АНТИПЛАГИАТ
ТВОРИТЕ СОБСТВЕННЫМ УМОМ

Отчет о проверке на заимствования №1

Автор: Соленая Оксана Ярославовна osolenaya@list.ru / ID: 12
Проверяющий: Соленая Оксана Ярославовна (osolenaya@list.ru / ID: 12)
Организация: Санкт-Петербургский государственный университет аэрокосмического приборостроения

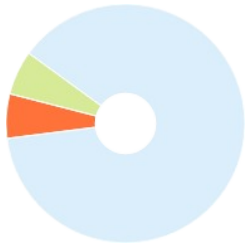
Отчет предоставлен сервисом «Антиплагиат» - http://guap.antiplagiat.ru

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 1055
Начало загрузки: 18.10.2019 20:10:56
Длительность загрузки: 00:00:35
Корректировка от 18.10.2019 20:17:26
Имя исходного файла: Коржук_ДР
Размер текста: 3746 кБ
Тип документа: Кандидатская диссертация
Символов в тексте: 320667
Слов в тексте: 37323
Число предложений: 2616

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 18.10.2019 20:11:32
Длительность проверки: 00:00:46
Комментарии: [Автосохраненная версия]
Модули поиска: Модуль поиска ИПС "Адилет", Модуль выделения библиографических записей, Сводная коллекция ЭБС, Коллекция РГБ, Цитирование, Модуль поиска переводных заимствований, Коллекция eLIBRARY.RU, Коллекция ГАРАНТ, Модуль поиска "ГУАП", Модуль поиска Интернет, Коллекция Медицина, Модуль поиска перефразирований eLIBRARY.RU, Модуль поиска перефразирований Интернет, Коллекция Патенты, Модуль поиска общеупотребительных выражений



ЗАИМСТВОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
6,42%	6,31%	87,27%

Заимствования — доля всех найденных текстовых пересечений, за исключением тех, которые система отнесла к цитированиям, по отношению к общему объему документа.
Цитирования — доля текстовых пересечений, которые не являются авторскими, но система посчитала их использование корректным, по отношению к общему объему документа. Сюда относятся оформленные по ГОСТу цитаты; общеупотребительные выражения; фрагменты текста, найденные в источниках из коллекций нормативно-правовой документации.
Текстовое пересечение — фрагмент текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника.
Источник — документ, проиндексированный в системе и содержащийся в модуле поиска, по которому проводится проверка.
Оригинальность — доля фрагментов текста проверяемого документа, не обнаруженных ни в одном источнике, по которым шла проверка, по отношению к общему объему документа.
Заимствования, цитирования и оригинальность являются отдельными показателями и в сумме дают 100%, что соответствует всему тексту проверяемого документа.
Обращаем Ваше внимание, что система находит текстовые пересечения проверяемого документа с проиндексированными в системе текстовыми источниками. При этом система является вспомогательным инструментом, определение корректности и правомерности заимствований или цитирований, а также авторства текстовых фрагментов проверяемого документа остается в компетенции проверяющего.

№	Доля в отчете	Доля в тексте	Источник	Ссылка	Актуален на	Модуль поиска	Блоков в отчете	Блоков в тексте
[01]	4,12%	4,39%	Постановление Главы Инсарского мун..	http://municipal.garant.ru	11 Мар 2019	Коллекция ГАРАНТ	13216	78
[02]	0,01%	4,25%	Постановление Администрации Инсар..	http://ivo.garant.ru	04 Мар 2019	Коллекция ГАРАНТ	45	100
[03]	0%	2,77%	Браницкий, Александр Александрович...	http://dlib.rsl.ru	15 Окт 2019	Коллекция РГБ	0	57
[04]	2,53%	2,77%	http://www.spiiras.nw.ru/dissovet/wp-co..	http://spiiras.nw.ru	06 Ноя 2018	Модуль поиска Интернет	8103	57
[05]	0,3%	1,16%	Постановление Правительства Хабаро..	http://ivo.garant.ru	21 Июн 2019	Коллекция ГАРАНТ	957	27
[06]	0%	0,95%	ИДЕНТИФИКАЦИЯ АТАК НА БЕСПРОВО..	http://elibrary.ru	16 Июл 2018	Коллекция eLIBRARY.RU	0	75
[07]	0,82%	0,95%	Постановление Кабинета Министров Ч.	http://ivo.garant.ru	28 Фев 2018	Коллекция ГАРАНТ	2631	54
[08]	0,23%	0,79%	Постановление администрации Омсук..	http://municipal.garant.ru	02 Мар 2018	Коллекция ГАРАНТ	743	24
[09]	0%	0,67%	П О С Т А Н О В Л Е Н И Е - PDF	https://docplayer.ru	23 Июн 2019	Модуль поиска Интернет	5	17
[10]	0,3%	0,6%	Модели и методы обнаружения наруш.	http://spiiras.nw.ru	06 Ноя 2018	Модуль поиска Интернет	948	19
[11]	0%	0,59%	Викснин, Илья Игоревич Модели и ме...	http://dlib.rsl.ru	15 Окт 2019	Коллекция РГБ	0	20
[12]	0%	0,58%	Выпуск №2 2018	http://ntvp.ru	29 Мар 2018	Модуль поиска Интернет	0	26
[13]	0%	0,5%	https://esu.citis.ru/dissertation/CTF0KYQ..	https://esu.citis.ru	10 Мая 2018	Модуль поиска Интернет	0	11
[14]	0,36%	0,48%	Методы обеспечения целостности инф.	https://sut.ru	06 Ноя 2018	Модуль поиска Интернет	1145	12
[15]	0,01%	0,47%	https://esu.citis.ru/dissertation/BT9BCPU.	https://esu.citis.ru	21 Мар 2018	Модуль поиска Интернет	22	18
[16]	0,09%	0,46%	Штеренберг, Станислав Игоревич Обн..	http://dlib.rsl.ru	15 Окт 2019	Коллекция РГБ	298	11
[17]	0,37%	0,46%	A survey of intrusion detection in wireles..	https://doi.org	18 Июн 2019	Модуль поиска Интернет	1185	23
[18]	0,12%	0,42%	Браницкий, Александр Александрович...	http://dlib.rsl.ru	01 Янв 2018	Коллекция РГБ	391	16

[19]	0,16%	0,42%	SESSION SECURITY AND ALLIED TECHNO..	http://worldcomp-proceedings.cc	12 Июл 2017	Модуль поиска Интернет	502	20
[20]	0,03%	0,41%	АНАЛИЗ И КЛАССИФИКАЦИЯ МЕТОДО..	http://elibrary.ru	05 Авг 2016	Коллекция eLIBRARY.RU	103	19
[21]	0,04%	0,39%	Методы и алгоритмы количественной...	https://ugatu.su	06 Ноя 2018	Модуль поиска Интернет	144	13
[22]	0,01%	0,36%	Колчин, Максим Александрович Мето...	http://dlib.rsl.ru	19 Фев 2018	Коллекция РГБ	38	7
[23]	0,19%	0,36%	Воробьева, Алиса Андреевна Методик...	http://dlib.rsl.ru	15 Дек 2017	Коллекция РГБ	613	11
[24]	0%	0,32%	Диссертационная работа (Добавлен 24..	https://sibsutis.ru	25 Дек 2017	Модуль поиска Интернет	0	8
[25]	0,26%	0,3%	RESEARCH at ITMO University	http://research.ifmo.ru	18 Окт 2018	Модуль поиска Интернет	830	10
[26]	0,16%	0,27%	Годовой отчет 2016 года	http://spiiras.nw.ru	раньше 2011	Модуль поиска Интернет	518	8
[27]	0%	0,27%	Компоненты риска физической безоп...	http://elibrary.ru	19 Сен 2019	Коллекция eLIBRARY.RU	0	9
[28]	0,11%	0,26%	MIPRO'2015. 38th International Convent..	http://elibrary.ru	11 Июл 2015	Коллекция eLIBRARY.RU	341	11
[29]	0,25%	0,25%	не указано	http://standartgost.ru	01 Янв 2017	Модуль поиска перефразирований Интернет	787	1
[30]	0,12%	0,24%	13_reference.pdf	http://shodhganga.inflibnet.ac.in	07 Авг 2018	Модуль поиска Интернет	376	11
[31]	0%	0,2%	Сивачев, Алексей Вячеславович Метод..	http://dlib.rsl.ru	15 Окт 2019	Коллекция РГБ	0	7
[32]	0%	0,2%	ВЕСТНИК МОРДОВСКОГО УНИВЕРСИТ...	https://docplayer.ru	22 Фев 2019	Модуль поиска Интернет	0	2
[33]	0,12%	0,2%	http://vestnik.mrsu.ru/content/pdf/18-1...	http://vestnik.mrsu.ru	23 Мая 2018	Модуль поиска Интернет	370	2
[34]	0,08%	0,18%	Катаева, Алина Владимировна Извлече.	http://dlib.rsl.ru	05 Авг 2019	Коллекция РГБ	250	8
[35]	0%	0,18%	Анализ угроз информационной безоп...	http://elibrary.ru	16 Июл 2018	Коллекция eLIBRARY.RU	0	7
[36]	0,11%	0,17%	Addressing Security and Privacy Challeng..	http://arxiv.org	03 Дек 2018	Модуль поиска Интернет	364	8
[37]	0%	0,17%	https://dissov.pnzgu.ru/files/dissov.pnzg..	https://dissov.pnzgu.ru	04 Июн 2019	Модуль поиска Интернет	0	6
[38]	0,09%	0,17%	Диссертация Финогеева Егора Алексее..	http://dissov.pnzgu.ru	19 Янв 2018	Модуль поиска Интернет	304	6
[39]	0,09%	0,16%	Чечулин, Андрей Алексеевич Построен.	http://dlib.rsl.ru	17 Ноя 2014	Коллекция РГБ	279	6
[40]	0%	0,15%	Финогеев, Егор Алексеевич Модели и м.	http://dlib.rsl.ru	22 Фев 2019	Коллекция РГБ	0	5
[41]	0%	0,14%	Перспективы научно-исследовательск...	http://elibrary.ru	16 Июл 2018	Коллекция eLIBRARY.RU	0	3
[42]	0%	0,14%	A Systematic Hands-On Approach to Gen.	https://link.springer.com	06 Мая 2019	Модуль поиска Интернет	0	5
[43]	0%	0,13%	Дойникова, Елена Владимировна Оцен.	http://dlib.rsl.ru	19 Фев 2018	Коллекция РГБ	0	4
[44]	0%	0,12%	Определение актуальных угроз безоп...	http://elibrary.ru	02 Янв 2018	Модуль поиска перефразирований eLIBRARY.RU	15	2
[45]	0%	0,11%	231269	http://biblioclub.ru	19 Апр 2016	Сводная коллекция ЭБС	0	4
[46]	0,02%	0,11%	Ку Тхань Фонг Разработка беспроводн..	http://dlib.rsl.ru	04 Дек 2017	Коллекция РГБ	51	5
[47]	0,07%	0,11%	Шейкин, Трифон Юрьевич Повышени...	http://dlib.rsl.ru	22 Авг 2019	Коллекция РГБ	212	5
[48]	0,06%	0,11%	Амелин Р.В. Государственные и муниц...	http://ivo.garant.ru	21 Фев 2019	Коллекция ГАРАНТ	195	13
[49]	0,05%	0,1%	Дунин, Вадим Сергеевич диссертация ...	http://dlib.rsl.ru	31 Мар 2015	Коллекция РГБ	150	3
[50]	0%	0,1%	ОСНОВНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ..	http://elibrary.ru	раньше 2011	Коллекция eLIBRARY.RU	0	3
[51]	0,04%	0,1%	Актуальные проблемы инфотелекомм..	http://elibrary.ru	05 Дек 2015	Коллекция eLIBRARY.RU	113	3
[52]	0,04%	0,09%	КОМПЬЮТЕРНАЯ ОПТИКА. Том 41 №1 ...	https://book.ru	03 Июл 2017	Сводная коллекция ЭБС	137	3
[53]	0,04%	0,09%	Исследование угроз и организация ме..	http://elibrary.ru	02 Янв 2018	Модуль поиска перефразирований eLIBRARY.RU	125	2
[54]	0%	0,09%	Ложников, Павел Сергеевич Методоло..	http://dlib.rsl.ru	15 Окт 2019	Коллекция РГБ	0	4
[55]	0%	0,08%	Laboratory of Computer Security Proble...	http://comsec.spb.ru	08 Янв 2018	Модуль поиска переводных заимствований	0	1
[56]	0%	0,08%	Чудинова, Ксения Владиславовна Упра..	http://dlib.rsl.ru	22 Фев 2019	Коллекция РГБ	0	4

[57]	0,07%	0,07%	К выявлению групп менеджеров.	http://elibrary.ru	28 Авг 2014	Коллекция eLIBRARY.RU	239	3
[58]	0%	0,07%	Теория вероятностей и математическа.	https://book.ru	03 Июл 2017	Сводная коллекция ЭБС	0	2
[59]	0%	0,07%	Организация и технологии защиты ин..	http://bibliorossica.com	27 Дек 2016	Сводная коллекция ЭБС	0	4
[60]	0%	0,07%	Организация и технологии защиты ин..	http://ibooks.ru	09 Дек 2016	Сводная коллекция ЭБС	0	4
[61]	0%	0,07%	Организация и технологии защиты ин..	http://biblioclub.ru	20 Апр 2016	Сводная коллекция ЭБС	0	4
[62]	0%	0,07%	66085	http://e.lanbook.com	09 Мар 2016	Сводная коллекция ЭБС	0	4
[63]	0,03%	0,07%	Белобров, Андрей Петрович диссертац..	http://dlib.rsl.ru	30 Июл 2012	Коллекция РГБ	97	3
[64]	0,04%	0,06%	Bandwidth saving system and method fo.	http://freepatentsonline.com	04 Ноя 2016	Коллекция Патенты	136	4
[65]	0%	0,06%	Беспроводные сети датчиков на основ..	http://elibrary.ru	28 Авг 2014	Коллекция eLIBRARY.RU	0	4
[66]	0,06%	0,06%	Методы и средства анализа информат...	http://swsys.ru	05 Янв 2017	Модуль поиска перефразирований Интернет	202	1
[67]	0%	0,06%	Критически важные объекты и киберт..	http://ibooks.ru	09 Дек 2016	Сводная коллекция ЭБС	0	4
[68]	0%	0,06%	Ле Тхи Чанг Линь Оптимальные много.	http://dlib.rsl.ru	22 Фев 2019	Коллекция РГБ	0	3
[69]	0,03%	0,06%	КОМПАРИРОВАНИЕ МЕТОДОВ КЛАССИ.	http://elibrary.ru	04 Июл 2015	Коллекция eLIBRARY.RU	99	2
[70]	0%	0,05%	Определение актуальных угроз безоп...	http://elibrary.ru	04 Мая 2017	Коллекция eLIBRARY.RU	0	1
[71]	0,04%	0,05%	Multimedia Computing and Networking ...	http://elibrary.ru	28 Авг 2014	Коллекция eLIBRARY.RU	114	2
[72]	0,05%	0,05%	ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИ.	http://elibrary.ru	02 Янв 2018	Модуль поиска перефразирований eLIBRARY.RU	169	1
[73]	0,05%	0,05%	Полная версия научной работы	http://scienceforum.ru	29 Янв 2017	Модуль поиска перефразирований Интернет	164	1
[74]	0%	0,05%	Подход к анализу состояния информац.	http://elibrary.ru	02 Мая 2017	Коллекция eLIBRARY.RU	0	2
[75]	0,02%	0,05%	CERTIFICATING VEHICLE PUBLIC KEY WIT..	http://freepatentsonline.com	09 Ноя 2016	Коллекция Патенты	65	2
[76]	0%	0,05%	Intrusion detection signature analysis us..	http://freepatentsonline.com	04 Ноя 2016	Коллекция Патенты	0	2
[77]	0%	0,05%	Intrusion detection signature analysis us..	http://freepatentsonline.com	04 Ноя 2016	Коллекция Патенты	0	2
[78]	0%	0,05%	Multilayered intrusion detection system...	http://freepatentsonline.com	07 Ноя 2016	Коллекция Патенты	0	2
[79]	0%	0,05%	Domain mapping method and system - C.	http://freepatentsonline.com	06 Ноя 2016	Коллекция Патенты	0	2
[80]	0%	0,05%	Method and system for adaptive networ..	http://freepatentsonline.com	06 Ноя 2016	Коллекция Патенты	0	2
[81]	0%	0,05%	Network intrusion detection signature a...	http://freepatentsonline.com	06 Ноя 2016	Коллекция Патенты	0	2
[82]	0%	0,05%	Intrusion detection system and method...	http://freepatentsonline.com	06 Ноя 2016	Коллекция Патенты	0	2
[83]	0%	0,05%	Method and system for adaptive networ..	http://freepatentsonline.com	06 Ноя 2016	Коллекция Патенты	0	2
[84]	0%	0,05%	Method and system for dynamically dist...	http://freepatentsonline.com	06 Ноя 2016	Коллекция Патенты	0	2
[85]	0%	0,05%	System and method for consolidating an..	http://freepatentsonline.com	07 Ноя 2016	Коллекция Патенты	0	2
[86]	0%	0,05%	Method and system for providing tampe..	http://freepatentsonline.com	09 Ноя 2016	Коллекция Патенты	0	2
[87]	0%	0,05%	Parallel intrusion detection sensors with...	http://freepatentsonline.com	04 Ноя 2016	Коллекция Патенты	0	2
[88]	0%	0,05%	WIRELESS SENSOR NETWORK AND ADAP..	http://freepatentsonline.com	08 Ноя 2016	Коллекция Патенты	0	2
[89]	0%	0,05%	Выпуск журнала № 2 за 2014, Современ.	http://science-education.ru	29 Янв 2017	Модуль поиска перефразирований Интернет	0	1
[90]	0%	0,04%	ПОСТРОЕНИЕ МОДЕЛИ ДАННЫХ ДЛЯ С.	http://elibrary.ru	17 Дек 2016	Коллекция eLIBRARY.RU	0	1
[91]	0%	0,04%	ЭКСПЕРИМЕНТАЛЬНЫЕ ИССЛЕДОВАНИ.	http://elibrary.ru	14 Дек 2016	Коллекция eLIBRARY.RU	0	1
[92]	0,04%	0,04%	РАЗРАБОТКА ТРЕБОВАНИЙ К СОСТАВУ..	http://elibrary.ru	02 Янв 2018	Модуль поиска перефразирований eLIBRARY.RU	116	1
[93]	0%	0,03%	Лечение больных с метастазами коло...	http://emll.ru	21 Дек 2016	Коллекция Медицина	0	1
[94]	0,03%	0,03%	Компьютерные сети. 5-е изд.	http://ibooks.ru	09 Дек 2016	Сводная коллекция ЭБС	109	1

[95]	0%	0,03%	КОМПЬЮТЕРНАЯ ОПТИКА. Том 41 №2 ...	https://book.ru	03 Июл 2017	Сводная коллекция ЭБС	0	1
[96]	0,03%	0,03%	Герменевтическая методология интег...	http://elibrary.ru	16 Июл 2018	Коллекция eLIBRARY.RU	107	1
[97]	0,03%	0,03%	ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСН..	http://elibrary.ru	01 Янв 2017	Коллекция eLIBRARY.RU	104	1
[98]	0%	0,03%	SCHEDULING ALGORITHM FOR WIRELES..	http://freepatentsonline.com	09 Ноя 2016	Коллекция Патенты	0	1
[99]	0,03%	0,03%	Башкин, Владимир Анатольевич диссе..	http://dlib.rsl.ru	раньше 2011	Коллекция РГБ	91	1
[100]	0%	0,02%	The analitic approach to choice of the ne...	http://elibrary.ru	11 Мая 2018	Коллекция eLIBRARY.RU	0	1
[101]	0%	0,02%	OBJECT AND SPATIAL LEVEL QUANTITATI..	http://freepatentsonline.com	09 Ноя 2016	Коллекция Патенты	0	1
[102]	0%	0,02%	Combinational pixel-by-pixel and object-...	http://freepatentsonline.com	09 Ноя 2016	Коллекция Патенты	0	1
[103]	0,02%	0,02%	253183	http://biblioclub.ru	19 Апр 2016	Сводная коллекция ЭБС	64	1
[104]	0%	0,02%	253607	http://biblioclub.ru	19 Апр 2016	Сводная коллекция ЭБС	0	1
[105]	0%	0,02%	Дорошенко, Александр Юрьевич Мето.	http://dlib.rsl.ru	15 Окт 2019	Коллекция РГБ	2	1
[106]	0%	0,02%	Разработка механизма адаптивной ма..	http://elibrary.ru	11 Янв 2017	Коллекция eLIBRARY.RU	0	1
[107]	0%	0,02%	Collaborative location and activity recom..	http://freepatentsonline.com	09 Ноя 2016	Коллекция Патенты	0	1
[108]	0%	0%	не указано	не указано	раньше 2011	Модуль выделения библиографических записей	0	1
[109]	0,1%	0%	не указано	не указано	раньше 2011	Цитирование	331	3
[110]	0,66%	0%	не указано	не указано	раньше 2011	Модуль поиска общеупотребительных выражений	2117	82

Текст документа

1

федеральное государственное автономное образовательное учреждение

высшего образования 110 «Санкт-Петербургский 15 национальный исследовательский

университет информационных технологий 110 , механики и оптики 110 »

УДК 004.056

На правах рукописи 10

Коржук Виктория Михайловна

Модель и метод идентификации атак сетевого уровня на беспроводные

сенсорные сети на основе поведенческого анализа

05.13.19 – Методы и системы защиты информации, информационная

безопасность 110

Диссертация на соискание ученой степени

Кандидата технических наук

Научный руководитель

кандидат 14 технических наук, доцент 22

Заколдаев Данил Анатольевич

Санкт-Петербург – 2019

2

Оглавление

4

Введение

Актуальность работы. Современный этап развития информационных технологий характеризуется повсеместным внедрением и использованием различных киберфизических систем (КФС). В качестве основы для таких систем нередко используются беспроводные сенсорные сети (БСС), и защита информации в этих сетях является новой и актуальной задачей. Важность решения задачи идентификации атак на БСС обусловлена спецификой БСС в КФС и непрерывным ростом количества разнообразных сетевых угроз, реализация которых может привести к финансовым, репутационным и даже человеческим потерям. По данным аналитической компании International Data Corporation, расходы в исследуемой области в 2019 году достигнут 745 млрд долларов, а к 2022-му году превысят 1 трлн долларов [109]. Согласно долгосрочному прогнозу научно-технологического развития РФ до 2030 года к 2020 году в мире будет 30,1 млрд беспроводных устройств, включая системы автоматизации производства (Индустрия 4.0), системы автоматизации зданий [131] и помещений (Умный дом) [125], носимые устройства, в т.ч. медицинского назначения, системы мониторинга состояния окружающей среды и т. д. [20]

Текущий уровень развития научно-методического аппарата (НМА) не позволяет 10 обеспечивать необходимый уровень целостности и доступности информации, циркулирующей в БСС. Ввиду таких особенностей функционирования устройств БСС, как малый объем памяти, вычислительных мощностей, а также ограничений в электропитании, существующие методы защиты информации и классические системы обнаружения вторжений (СОВ) оказываются недостаточно эффективными. В процессе разработки и анализа модели угроз и модели нарушителя для БСС в соответствии с базой данных угроз ФСТЭК было выявлено, что наиболее вероятными угрозами с наиболее высоким уровнем ущерба являются атаки сетевого уровня (атаки, соответствующие сетевому уровню модели OSI).

Мониторинг состояния сети и обнаружение сетевых атак на основе анализа аномалий является одним из самых популярных методов, однако чаще всего исследователи используют семантическую составляющую передаваемых пакетов в трафике. В таких случаях достаточно велика вероятность ложного срабатывания, так как не представляется возможным точно определить причину аномалии: вызвана ли она атакой, программным сбоем или действительным изменением окружающей среды. Сигнатурный анализ также используется часто, однако здесь возникает вопрос хранения и дополнения базы данных сигнатур. Алгоритмы обнаружения атак, основанные на управлении репутацией или доверии показывают высокую точность, но являются вычислительно сложными, что не подходит под ограничения БСС, связанных с малым объемом памяти, энергоемкости и вычислительных ресурсов. Поэтому в данном диссертационном исследовании используется поведенческий анализ. Под поведением понимается набор характеристик сети в конкретный момент времени. Такой подход является не в полной мере исследованным. В соответствии с этим задача идентификации атак сетевого уровня на беспроводные сенсорные сети является актуальной, а предлагаемый в настоящем диссертационном исследовании научно-методический аппарат направлен на ее решение.

Степень разработанности темы. Значительный вклад в решение проблемы идентификации атак на компьютерные сети внесли такие отечественные исследователи, как И.А. Зикратов, П.Д. Зегжда, Е.С. Басан, Т.И. Гришечкина, А.А. Браницкий, И.И. Викснин и зарубежные исследователи Ю. Эль Мураби, Г. Калнур, Ш. Зонг, Х. Ку, Ма и др. В частности, задачей обеспечения информационной безопасности БСС посвящены работы И.В. Котенко, И.Б. Саенко, И.С. Лебедева, Е.Е. Бессоновой и А. Да Силвы, М.Р. Ахмеда, И. Альмомани, С. Син-гха и др. Анализ работ в этой области показал, что существующие решения позволяют идентифицировать от одной до четырех атак сетевого уровня на БСС, ограничиваются использованием единственного классификатора и не имеют гибкой методики идентификации сетевых атак. Соответственно, диссертационная работа направлена на повышение

эффективности к идентификации атак на БСС с помощью анализа поведения сети, что и определяет актуальность исследования, его теоретическую и практическую значимость.

Научная задача состоит в разработке и обосновании научно-методического аппарата по идентификации атак сетевого уровня на БСС на основе анализа новой комбинации признаков, характеризующего поведение такой сети.

Объектом исследования являются системы обеспечения информационной безопасности БСС.

Предметом исследования являются модели и методы идентификации атак сетевого уровня на БСС.

Цель диссертационного исследования: повышение эффективности

идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа. Для достижения цели сформулированы и решены следующие частные задачи:

1) Провести исследование и анализ существующих методов идентификации атак на БСС, выявить показатели эффективности идентификации.

2) Разработать модель профиля поведения устройств БСС.

3) Разработать метод идентификации атак сетевого уровня на БСС на основе анализа поведения сети с использованием совокупности методов машинного обучения.

4) Разработать методику идентификации атак на БСС, содержащую дополнительные этапы настройки и классификации и .

5) Провести вычислительный эксперимент и обосновать применимость разработанной модели профиля поведения БСС, метода и методики идентификации атак.

6) Сравнить разработанные модель, метод и методику с существующими исследованиями и сформулировать выводы о результатах диссертационной работы.

Научную новизну диссертации составляют:

1) Модель профиля поведения БСС отличается от известных использованием новой комбинации признаков поведения сети, таких как общее количество пакетов, переданных в сети, максимальное количество отправленных узлом пакетов, максимальное и минимальное количество полученных узлом пакетов и соотношение между количеством созданных и полученных пакетов.

2) Метод идентификации атак сетевого уровня на БСС на основе поведенческого анализа сети отличается от известных применением совокупности алгоритма «случайного леса» и вероятностного классификатора и введением параметра степени уверенности.

3) Методика идентификации атак на беспроводные сенсорные сети отличается от существующих использованием разработанных модели профиля поведения БСС и метода идентификации атак сетевого уровня на БСС, а также использованием программной модели реализации атак, программы оценки информативности и программы вычисления апостериорных распределений дискретного параметра распределения многомерной случайной величины по статистической выборке.

Теоретическая и практическая значимость. Разработанные модель, метод и методика предназначены для повышения эффективности идентификации сетевых атак на БСС, что позволит обеспечить необходимый уровень целостности и доступности информации. Предложенные модель и метод позволяют выявить в среднем на 9 атак больше, по сравнению с другими исследованиями, количество сетевых атак на БСС. Использование параметра степени уверенности в процессе идентификации сетевых атак предоставляет возможность получить необходимую точность классификации при неполном наборе признаков, что позволяет снизить затраты временных и вычислительных ресурсов. Применение разработанной методики идентификации атак и программных продуктов в системе обнаружения вторжений позволяет повысить гибкость системы и обеспечить необходимый уровень защищенности информационных систем. Результаты диссертационной работы могут быть использованы для дальнейшего развития подходов к обеспечению ИБ 10 в БСС в целом и БСС в контексте КФС в частности.

Методология и методы диссертационного исследования. Для решения сформулированных в работе задач использовались следующие методы исследования: методы теории информационной безопасности и методологии защиты информации, методы теории информации, положения теории вероятности, методы математической статистики и вычислительного

эксперимента.

Положения, выносимые на защиту:

1) Разработанная модель профиля поведения беспроводной сенсорной сети позволяет идентифицировать большее по сравнению с существующими исследованиями, количество атак.

2) Разработанный метод идентификации атак сетевого уровня на БСС на основе анализа профиля поведения позволяет обеспечить высокую точность идентификации при использовании неполного набора признаков профиля поведения.

3) Предложенная методика идентификации атак на беспроводные сенсорные сети позволяет повысить эффективность идентификации атак.

Обоснованность и достоверность полученных результатов достигается использованием апробированного математического аппарата и подтверждается проведением сравнительного анализа с существующими методами; серией практических экспериментов по идентификации 23 атак на БСС; согласованностью результатов, полученных при теоретическом исследовании с результатами проведенных экспериментов, а также непротиворечивостью достигнутых результатов и результатов работ других авторов; практической апробацией 23 в процессе реализации грантов, деятельности производственных организаций и одобрением на научно-технических конференциях.

Реализация результатов работы 10. Результаты, представленные в диссертационной работе, были реализованы в рамках выполнения следующих научно-исследовательских работ: проекта Минобрнауки России « Разработка методов агрегации, нормализации, анализа и визуализации больших массивов гетерогенных структурированных, полуструктурированных и 26

9

неструктурированных данных для мониторинга и управления безопасностью распределенной сети электронных потребительских устройств 26 No14-604-21-0147 (2014-2016); НИР-ПРИКЛ « Исследование уязвимостей систем для защиты от атак по сторонним каналам 14 » No713552 (2014-2016); грант для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга 14 (2015); гранта РНФ « Управление инцидентами и противодействие целевым киберфизическим атакам в распределенных крупномасштабных критически важных системах с учетом облачных сервисов и сетей Интернета вещей 26 » No15-11-30029 (2015-2017); НИР «Технологии киберфизических систем: управление, вычисления, безопасность» No617026 (2018); НИР-ФУНД «Исследование перспективных методов и технологий защиты киберпространства в банковской сфере» No59880 (2019); НИР-ФУНД «Методы, модели, методики, алгоритмы, протоколы и приложения для обеспечения информационной безопасности киберфизических систем» No717075 (2017-2019). Результаты работы использовались при разработке системы мониторинга информационной безопасности компании АК «Реактор». Полученные результаты используются в образовательном процессе факультета БИТ Университета ИТМО по

направлениям подготовки 110 бакалвариата 10.03.01 и магистратуры 10.04.01 по дисциплинам «Основы информационной безопасности», « Теория информационной безопасности и методология защиты информации», «Комплексные системы защиты информации 96 ».

Апробация результатов работы. Основные результаты работы были представлены и обсуждены на следующих конференциях и семинарах:

1) 15 th International Conference NEW2AN 2015 and 8th Conference ruSMART 26 ;

2) 18th Conference of Open Innovations Association FRUCT (2016);

3) Конференция Information Security and Protection of Information

Technology в рамках Conference of Open Innovations Association FRUCT (2015);

10

4) Молодежная научная школа «Безопасные информационные технологии» в рамках XIV Санкт-Петербургской межрегиональной конференции 10 «Региональная информатика» (2014);

5) IX и X Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России 10 » (2015, 2017);

6) IV, V, VI, VII, VIII Конгресс молодых ученых (2014, 2015, 2016, 2017, 2018);

7) XLIV, XLV Научная и учебно-методическая конференция Университета ИТМО (2015, 2016);

8) Круглый стол для победителей конкурсов грантов (Университет ИТМО – по техническому направлению) в рамках Конкурса грантов для студентов вузов, расположенных на территории Санкт-Петербурга, аспирантов вузов, отраслевых и академических институтов, расположенных на территории Санкт-Петербурга 14 (2015). 16

Публикации. Основные результаты, полученные в ходе диссертационного исследования, изложены в 17 печатных 4 работах, три из которых опубликованы 4 автором в журналах, рекомендованных ВАК 4 , восемь – в зарубежных изданиях, индексированных в Web of Science и Scopus 4 , шесть – в прочих изданиях. Получено три свидетельства о 4 государственной регистрации программ для ЭВМ 110 . 105

Личный вклад. Все результаты, представленные в диссертационной работе, получены лично автором в процессе выполнения научно-исследовательской 4 работы.

Структура и объем диссертационного 4 исследования

Диссертация 110 состоит из введения, трех глав, заключения 110 и 5 приложений. Основной материал изложен на 184 страницах. Полный объем диссертации составляет 206 страницы с 43 рисунками и 32 таблицами. Список литературы содержит 221 наименование.

Содержание работы 18 . Первая глава 4 включает в себя представление концепции БСС в контексте КФС, обзор существующих методов идентификации атак в БСС и постановку научной задачи. Во второй главе описана разработанная

11

модель профиля поведения БСС, произведена оценка информативности используемых в модели признаков. Также представлен метод идентификации атак, включающий в себя разработанную модель, алгоритм машинного обучения «случайный лес», вероятностный классификатор и параметр степени уверенности. Третья глава содержит изложение методику идентификации атак, включающую в себя разработанные модель профиля поведения и метод идентификации сетевых атак, а также рекомендации по применению разработанных в процессе диссертационного исследования программ. Кроме этого, в третьей главе представлены расширенные эксперименты и оценка модели, метода и методики по сравнению с существующими исследованиями.

12

Глава 1 Постановка задачи идентификации атак на беспроводные сенсорные сети

1.1 Обзор концепции беспроводных сенсорных сетей

Беспроводные сенсорные сети (БСС) относятся к группе пространственно-распределенных и специализированных датчиков и подчиненных им актуаторов для мониторинга [188], регистрации и реакции на физические условия окружающей среды и организации собранных данных в центральном месте. БСС измеряет такие условия окружающей среды как температура, звук, уровни загрязнения, влажность, ветер, и т.д. БСС зачастую являются основой для более

сложных и комплексных автоматизированных систем – так называемых кибер-физических систем (КФС).

В соответствии с [76; 179] КФС – система, объединяющая физические («аналоговые», аппаратные элементы, другие физические системы и среду, в которой функционирует КФС) и информационные (выполняющие вычисления, обеспечивающие функционирование и контроль алгоритмов и реализующие передачу данных) компоненты (рисунок 1.1) [154]. Использование КФС позволяет повышать эффективность производственного процесса благодаря полной интеграции вычислительных устройств с механизма предприятия 10 [197]. В основном, БСС применяются в таких системах, как:

- системы автоматизации производства (Индустрия 4.0) [185];
- системы автоматизации зданий и помещений (Умный дом) [125];
- медицинские системы автоматизации и раннего прогнозирования;
- носимые устройства, в том числе медицинского назначения;
- системы мониторинга состояния окружающей среды и макроскопического экологического контроля [163];
- системы транспортного обеспечения и управления городской логистикой [184];
- военные разведывательные системы и т.д.

Рисунок 1.1 – Система отношений в КФС

С началом активного применения БСС возрастают и риски, связанные с обеспечением информационной безопасности сети. БСС тесно связывают инфраструктуру физических объектов с информационными сетями, поэтому любая атака, осуществленная на них через информационные сети, в особенности глобальные инфокоммуникационные сети, такие как Интернет, будет нести огромные риски, временные и материальные потери на объектах энергоснабжения, химической обработки и национальной безопасности [157]. БСС обычно подвержены атакам в большей степени ввиду использования ими беспроводных каналов связи, поэтому проблемы обеспечения доверия между узлами, доступности, целостности и конфиденциальности информации должны учитываться еще с этапа разработки таких сетей [200].

Важность задачи обеспечения информационной безопасности обусловлена спецификой БСС в киберфизических системах и непрерывным ростом количества разнообразных сетевых угроз [27], реализация которых может привести к финансовым, репутационным и даже человеческим потерям [158]. По данным аналитической компании International Data Corporation, расходы в исследуемой области в 2019 году достигнут 745 млрд долларов, а к 2022-му году превысят 1

трлн долларов. Согласно долгосрочному прогнозу научно-технологического развития РФ до 2030 года и исследованиям НИУ ВШЭ к 2020 году в мире будет 30,1 млрд беспроводных устройств, включая системы автоматизации производства (Индустрия 4.0), системы автоматизации зданий и помещений (Умный дом), носимые устройства, в том числе медицинского назначения, системы мониторинга состояния окружающей среды и т.д. В это же время, эксперты «Лаборатории Касперского» отмечают, возрастает количество целевых атак на индустриальные предприятия и промышленность, а также на компоненты системы автоматизации, представленные киберфизическими системами и беспроводными сенсорными сетями. При этом на обнаружение атак 34% опрошенных компаний тратит несколько дней, а 20% – до нескольких недель [32]. Более того, снижается сложность осуществления активных атак на БСС [6], поскольку увеличивается количество программного-аппаратных средств мониторинга и тестирования сетей [73], которые чаще всего используются злоумышленниками для несанкционированного подключения к беспроводному каналу связи.

Развитие концепции БСС является одним из приоритетных направлений 110, что подтверждается ускоряющимися темпами их внедрения и включением в программы национальных стратегических исследований [189]. Способность БСС эффективно осуществлять мониторинг за параметрами среды, особенно в тех случаях, когда 110 вручную это сделать ресурсозатратно, физически невозможно либо опасно для жизни и здоровья человека 110, обеспечила их возрастающую популярность. Простейшая схема БСС приведена на рисунке 1.2.

Технологические особенности БСС делают применение хорошо изученных методов обеспечения безопасности в сетевых структурах трудным или неоправданным. Защита против сложных видов атак типа атаки Сивиллы или отказа в обслуживании сетевых узлов [172], демонстрирующих аномальное поведение, в данный момент не удовлетворительна. Поскольку цель защиты БСС – обеспечение безопасности как информации, циркулирующей внутри сети, так и самих ресурсов, возможные требования к достижению этой цели очень высокие:

доступность, целостность, наличие механизмов авторизации и аутентификации, анонимность, конфиденциальность, актуальность данных, защита индивидуальных узлов, неотказуемость и другие [7].

Рисунок 1.2 – Простейшая схема БСС

В будущем ожидается дальнейшее масштабирование размеров БСС и более тесная интеграция с сетями глобального информационного обмена, что только усложнит задачи обеспечения информационной безопасности [179] (рисунок 1.3).

Рисунок 1.3 – Три варианта объекта назначения передаваемой информации

В Российской Федерации на данный момент БСС не распространены настолько широко, как в западноевропейских и североамериканских странах, однако законодательным органом уже осознаны проблемы защиты критически

важных информационных систем: 26.07.2017 был принят Федеральный закон No 187-ФЗ « О безопасности критической информационной инфраструктуры Российской Федерации» [109 41]. В статье 2 пункте 8 определено, что в число субъектов критической информационной инфраструктуры попадают в том числе российские юридические лица и индивидуальные предприниматели 110, использующие информационно-телекоммуникационные системы и сети, а также автоматизированные системы управления в топливно-энергетическом комплексе, сферах обороны, атомной энергии, ракетно-космической, здравоохранения, транспорта, энергетики, горной, металлургической и химической промышленности [50; 74]. Учитывая, что в будущем ожидается внедрение БСС именно в эти области, в частности интеграция с автоматизированными системами промышленного управления и включение БСС в схемы информационного обмена на предприятиях, проблемы обеспечения информационной безопасности в них приобретают острый, масштабный характер и переходят из разряда исследовательской практики в класс проблем, требующих практического решения [8].

Как упоминалось ранее, БСС – сеть распространенных, сообщающихся между собой датчиков, собирающих данные о параметрах окружающей среды и/или контролирующих их, обеспечивая взаимодействие людей и/или компьютеров с окружающей средой [52]. Типовая структура простой одноранговой БСС представлена на рисунке 1.4.

С технической точки зрения, сенсор, или датчик, – это устройство, преобразующее физические, химические или биологические параметры среды в электрический сигнал. Объединенные в распространенную сеть, где они располагаются в узлах, сенсоры выполняют сбор и обработку информации о параметрах среды, а также ее передачу по протоколам связи другим узлам в сети. Большие количества сенсорных узлов (до 65 536 единиц в одной сети),

распределенные по области мониторинга, образуют самоорганизующуюся сеть [166]. В таких сетях процесс передачи информации происходит от одного узла к

17

другому по достижении сетевого шлюза, откуда информация транслируется на управляющий узел, где выполняется настройка сети ее пользователями [47].

Сенсорный узел – один из основных компонентов БСС. Архитектура сенсорного узла представлена на рисунке 1.5. Аппаратная составляющая сенсорного узла, как правило, содержит четыре части:

- объединенный блок питания и управления энергопотреблением;
- датчик;
- микроконтроллер;
- беспроводный трансивер, или приемопередатчик.

Рисунок 1.4 – Типовая структура одноранговой БСС

Рисунок 1.5 – Архитектура сенсорного узла

18

Блок питания и управления энергопотреблением должен обеспечивать стабильное энергопитание системы. Сенсор собирает данные о состоянии среды и, преобразуя их в электрические сигналы, передает их на микроконтроллер, обрабатывающий данные по заданным правилам. Беспроводной трансивер затем передает данные, обеспечивая таким образом физическую реализацию коммуникации в БСС в частности и в КФС в целом (рисунок 1.6) Главная особенность сенсорного узла – его малые размеры, ограниченное питание и малая мощность.

В настоящий момент существует большое разнообразие сенсоров, способных измерять перемещение, скорость, ускорение, давление, механическое напряжение, звук, свет, электромагнитные волны, температуру, значение водородного показателя pH и др. Размеры таких модулей не превышают нескольких миллиметров [117; 130].

Рисунок 1.6 – Определение сенсора в рамках КФС

Кроме того, разработаны технологии накопления энергии из внешних источников в окружающей среде, использующиеся в энергоснабжении автономных сенсоров. Такие системы достаточно компактны и требуют малое количество энергии, но могут быть ограничены зависимостью от заряда батареи. Технологии автономных сенсоров основаны на заряде от солнечного света,

19

пьезоэлектрических кристаллах, микроосцилляторах, генераторах термоэлектрической энергии или приемниках электромагнитных волн и др.

Поскольку для широкого и экономичного с точки зрения затрат развертывания БСС наиболее оптимально использование серийных коммерческих беспроводных коммуникаций и инфраструктур, современные БСС использует ограниченный набор технологий беспроводных коммуникаций [167].

В БСС используются два диапазона частот: семейство диапазонов ISM (англ. Industrial, Scientific, and Medical – индустриальный, научный и медицинский), определенное в Регламенте радиосвязи Международного союза электросвязи, и семейство диапазонов U-NII (англ. Unlicensed National Information Infrastructure – нелицензированная национальная информационная инфраструктура [94]), регулируемое Федеральной комиссией по связи США (FCC), также известное как диапазон 5 ГГц.

Ввиду естественных источников и явлений (потери, ослабление сигнала, затухания, многолучевое распространение и др.), а также использования открытых частот другими пользователями поблизости, в БСС возникают помехи, вне зависимости от того, используются ли технологии IEEE PAN, LAN, MAN или другие более общие радиотехнологии. Например, мобильные устройства с технологией Bluetooth [134], разделяющие рабочие частоты с беспроводными

сенсорами, могут оказать влияние на работу сети в закрытых пространствах; СВЧ-печи, функционирующие на частоте 2.45 ГГц, могут повлиять на работу беспроводной связи на частотах около 2.4 ГГц диапазона ISM; неправильно настроенная фильтрация электрических моторов может вызвать появление электрического шума, достаточного, чтобы беспроводные коммуникации стали ненадежными [221]; существенные потери в сигнале может вызвать физическое расположение трансивера.

Тем не менее, технологии IEEE PAN, LAN, MAN на данный момент наиболее широко применяются в большинстве коммерческих БСС. Для их реализации необходима поддержка протоколов связи, среди которых распространены:

- IEEE 802.15.1 (Bluetooth);
- IEEE 802.15.4 (Zigbee и другие спецификации) [100, 101];
- IEEE 802.11 (Wi-Fi);
- IEEE 802.16 (WiMax);
- RFID (радиочастотная идентификация).

На рисунке 1.7 представлено сравнение различных протоколов по дальности действия, энергопотреблению, скорости передачи данных и стоимости [33].

Рисунок 1.7 – Сравнение протоколов связи

IEEE 802.15.4 – наиболее полный стандарт WPAN-сетей с низкой скоростью передачи данных, имеющий несколько подкатегорий. Данный стандарт был направленно разработан для применения в случаях низкоскоростного мониторинга и управления, при необходимости низкого энергопотребления и продолжительной работы устройств. Базовый обновленный стандарт – IEEE 802.15.4a/b, его вариации – IEEE 802.15.4c–g [203].

Этот стандарт определяет физический уровень (PHY) и уровень MAC сетевой модели OSI. Уровень PHY определяет частоты, энергопотребление, модуляцию и другие характеристики беспроводной связи, уровень MAC

определяет формат обработки данных. Остальные уровни в сетевой модели определяют другие методы обработки данных и связанные надстройки протокола, включая уровень приложений.

Основная задача стандарта – предоставление базового формата, к которому могут быть добавлены другие протоколы и функции в качестве уровней 3–7 сетевой модели. Самый широко используемый диапазон частот – 2.4 ГГц. Определена модуляция методом прямой последовательности для расширения спектра (DSSS) [128], устойчивая к шумам и помехам, а также предоставляющая возможность кодирования для повышения надежности связи. Стандартная двоичная фазовая манипуляция применяется для двух низкоскоростных версий, в то время как квадратурная фазовая манипуляция, с помощью которой возможно снизить энергопотребление, – для высокоскоростной версии. В отношении канального доступа, в IEEE 802.15.4 применяется протокол множественного доступа с контролем несущей и избеганием коллизий (CSMA/CA [47]), позволяющий нескольким пользователям или узлам получить доступ к одному каналу в разное время без помех. Большинство передач происходит редко, короткими пакетами, при непродолжительном включении, что минимизирует энергопотребление, при этом радиус передачи разнится и может достигать 1 км, в то время как многие реализации покрывают меньший радиус: от 10 до 75 м.

В IEEE 802.15.4 определены две базовые топологии сети: топология звезды, где связь между узлами осуществляется через центральный координирующий узел, и топология одноранговой сети (P2P), которая может быть расширена в другие топологии на более высоких уровнях сетевого взаимодействия, среди них достаточно популярна ячеистая топология. Топологии приведены на рисунках 1.8 и 1.9.

Самая распространенная спецификация протоколов верхнего уровня для IEEE 802.15.4 – Zigbee, разрабатываемая Zigbee Alliance [53; 207]. Именно данная спецификация исследуется в диссертационной работе. Она определяет на сетевом уровне и уровне приложений сетевой модели дополнительные функции связи, которые включают в себя аутентификацию легитимных узлов, безопасное

шифрование и маршрутизацию данных, обеспечивающую функционирование на основе ячеистой топологии. Ее основное преимущество состоит в способности любого узла сообщаться с другим узлом напрямую либо через ретрансляцию сигнала через несколько дополнительных узлов, поэтому такая сеть может протягиваться на большое расстояние. Более того, такая топология увеличивает надежность связи, предоставляя несколько путей передачи сигнала от одного узла к другому. Ячеистые сети Zigbee являются самонастраивающимися и самовосстанавливающимися [51; 208]. Некоторые из преимуществ БСС на основе Zigbee:

- надежность и самовосстановление [98];
- поддержка большого количества узлов;
- простота развертывания;
- большое время жизни батареи;
- низкое энергопотребление;
- низкая цена;
- простота настройки и отладки;
- гибкая сетевая структура [176].

Рисунок 1.8 –Топологии IEEE 802.15.4

Рисунок 1.9 – Ячеистая топология

Несмотря на то что Zigbee – самая известная спецификация базового стандарта IEEE 802.15.4, разработаны другие протоколы для определенного целевого использования:

1. WirelessHART, технология БСС на основе беспроводной версии протокола HART, применяемого в системах автоматизации и управления производственными процессами. Определяет протокол мультиплексирования с разделением по времени;
2. ISA100.11a, стандарт промышленного контроля, используемый в системах управления производственными процессами. Определяет опции смены рабочего канала, мультиплексирования с переменным разделением по времени и ячеистую топологию;
3. 6LoWPAN (RFC 5933, RFC 4919), с помощью которого возможно настроить устройства на передачу 128-битных адресов протокола IPv6. Эта спецификация применяет компрессию хедеров и методы передачи адресов так, что устройства на основе IEEE 802.15.4 могут получить доступ к сети Интернет. Пакеты IPv6 сжимаются и инкапсулируются для соответствия стандартным размерам. 6LoWPAN упрощает применение IEEE 802.15.4 в технологиях интернета вещей, умных сетей электроснабжения и межмашинного взаимодействия.

1.2 Специфика обеспечения информационной безопасности в беспроводных сенсорных сетях

Ввиду архитектурных особенностей, БСС имеют ограниченные вычислительные возможности, малую емкость памяти, низкую пропускную способность, ограниченные энергоресурсы и малые размеры аппаратных средств [75], что накладывает жесткие ограничения на методы обеспечения безопасности в сетях [93] и делают применение некоторых из них невозможным [142]. Основные ограничения в БСС, накладываемые на средства защиты

информации, можно классифицировать следующим образом:

1. Ограниченность ресурсов

- Ограниченность вычислительных ресурсов;
- Ограниченность энергетических ресурсов.

2. Ненадежность связи

- Ненадежная передача
- Конфликты
- Задержки

3. Непредвиденные случаи

Ниже приведены пояснения к каждому ограничению.

Ограниченность вычислительных ресурсов. Будучи миниатюрными ЭВМ, сенсоры оснащены процессором, модулем оперативной памяти, урезанной операционной системой с минимальным набором инструкций и очень небольшой доступной свободной памятью, поэтому алгоритмы обеспечения безопасности не могут требовать от сенсоров выполнения вычислительно сложных и затратных по памяти операций без риска препятствования выполнению основной конструктивной задачи – сбора и передачи данных [147].

Ограниченность энергетических ресурсов. Энергия в сенсорах тратится на три основных компонента: модуль датчика, трансивер и микропроцессор. Сложные алгоритмы дополнительно загружают процессор, при выполнении множества вычислений, и модуль связи, при необходимости интенсивного обмена

данными. При этом микропроцессор выполняет около 800–1000 операций в секунду, но энергетические затраты на передачу данных гораздо больше по сравнению с ее обработкой в ЦП. Практика применения сенсоров предусматривает их установку и использование на протяжении длинных временных промежутков с увеличенным периодом замены батареи, поэтому методы обеспечения безопасности, заметно сокращающие этот период, не практичны и избегаются [148].

Ненадежная передача. БСС – большое количество связанных в сеть сенсоров, где передача данных зачастую происходит в виде сетевых пакетов от одного сенсора к другому. Ввиду природы беспроводной коммуникации и структуры сети, пакеты могут быть или повреждены из-за ошибок и помех в канале передачи, или отброшены чрезмерно загруженными узлами. В сети, построенной без применения протоколов обнаружения и исправления таких ошибок, возрастают риски потерять критически важные пакеты, содержащие особо ценную информацию о среде или информацию, необходимую для осуществления процедур безопасности, например, криптографические ключи.

Конфликты. В сетях с высоким количеством сенсоров на единицу площади могут возникать конфликты беспроводной связи, приводящие к неполной передаче пакета или ее прекращению, что осложняет применение методов обеспечения безопасности, полагающихся на стабильность связи и полноту передаваемых данных.

Задержки. Зачастую из-за особенностей развертывания БСС невозможно построить такую архитектуру сети, где была бы возможна глобальная адресация одного узла другим. Более того, в таких сетях, как правило, предусматривается поток информации через несколько узлов к одному общему узлу сбора данных. Все это приводит к специальному проектированию топологии сети, где имеют значение расположение узлов в пространстве и их связи друг с другом. Топологические особенности, такие как различная удаленность от узла сбора информации, непредвиденные выходы из строя отдельных узлов, различная загруженность, неизбежно приводят к пересылке пакетов, перестройке маршрутов

их передачи и задержках в доставке. Работа некоторых СЗИ в таких условиях

может оказаться неустойчивой и неэффективной.

Непредвиденные ситуации. БСС напрямую взаимодействуют с окружающей их средой, поэтому они часто применяются в открытых, крупномасштабных, иногда враждебных пространствах, где невозможно контролировать любые незначительные изменения. Отсюда вытекает ряд проблем, связанных с физической целостностью сенсоров как устройств, среди которых случайный выход из строя, физический ущерб, резкое изменение условий среды и др. Получение надежных данных в сложных условиях от физически удаленных сенсоров к конечному пользователю бывает само по себе непростой задачей. К примеру, типичной является модель сенсора HBE-ZibgeX II от Hanback Electronics, оснащенная 8-битным микроконтроллером ATmega128L с максимальной тактовой частотой 8 МГц, оперативной памятью типа SRAM 4 КБ, flash-памятью 128 КБ [191]; трансивером CC2420 от Texas Instruments, поддерживающим стандарты IEEE 802.15.4 и Zigbee, работающим на частоте 2.4 ГГц, оснащенным DSSS-модемом со скоростями 1 Мчип/с и 250 Кб/с; батареями напряжениями в 1.2 В и 1.5 В; а также TinyOS – встраиваемой компонентной операционной системой.

Обеспечение информационной безопасности в БСС из-за поставленных ограничений имеет ряд особенностей [193; 135; 165; 206]:

1) Сложные криптографические протоколы являются ресурсозатратными и плохо подходят для концепции маломощных устройств без постоянного источника питания.

2) Ресурсоемкие надстроенные протоколы также привносят дополнительную нагрузку и влияют на передачу информации между устройствами.

3) Процесс обеспечения информационной безопасности сети напрямую зависит от квалификации администратора. Более того, в некоторых случаях при большом количестве устройств в сети практически невозможно обеспечить необходимый уровень безопасности встроенными средствами.

4) Неприспособленность устройств к агрессивной внешней среде.

Необходимо учитывать также природу беспроводных коммуникаций: используя существующие средства мониторинга [29] и тестирования состояния сети, злоумышленники не только могут прослушивать трафик [16], но и подключиться к сети и реализовывать различные атаки [95]. Самым простым примером такого средства является Wireshark, который с помощью простых манипуляций позволяет производить парсинг сети [33]. При добавлении нового устройства к сети происходит передача ключа на сетевом уровне, при перехвате которого возможно подключение к сети [168], прослушивание всего трафика и проведение различных сетевых атак, которые и рассматриваются в данном исследовании [34; 122]. Снимок экрана, представленный на рисунке 1.10, подтверждает эту возможность.

Рисунок 1.10 – Локация сетевого ключа при анализе пакетов

Необходимо отметить, что фреймы подтверждения (acknowledgement frame), используемые для подтверждения принятия данных, не шифруются и не имеют кода целостности сообщения (MIC – message integrity code), поэтому могут быть использованы для проведения атаки «отказ в обслуживании» или «затопления».

Еще одна уязвимость БСС на ZigBee состоит в том, что при 110 отсутствии проверки целостности сообщения узлом возможно подделать значения счетчика кадров, и, соответственно, валидный пакет будет отброшен, так как его значение не будет совпадать со счетчиком узла [45, 46].

Помимо этого, возможны различные варианты подключения к БСС. Злоумышленник может создать ложный координатор сети, в результате чего

действительный координатор сменит адрес сети (PAN ID) на какое-то иное значение [209]. Поскольку узлы сети остаются привязанными к старому адресу, нарушается доступность и целостность сети. В прикладном значении это значит, что датчики не смогут вовремя отреагировать на изменения измеряемых показателей и соответствующие действия не будут осуществлены (особо опасным представляется такое воздействие на системы реагирования, например, на пожарную сигнализацию и датчики дыма).

Среди программно-аппаратных средств для «мониторинга и тестирования» [60] сетей спецификации ZigBee могут быть выделены следующие:

1) KillerBee – программная платформа и утилиты для атак на сети стандарта IEEE 802.15.4 со спецификацией ZigBee [115]. В списке поддерживаемой аппаратной части представлены такие средства, как Atmel RZ RAVEN USB Stick и присутствует поддержка Texas Instruments CC2531.

2) Attify ZigBee Framework – схожая с KillerBee платформа, имеющая преимущество в виде графического интерфейса [116].

3) SecBee – средство тестирования безопасности, использующее в своем составе Scapy-radio, KillerBee и GNU Radio block. Особенность в том, что для ее функционирования нужна программно-определяемая радиосистема, например, USRP (Universal Software Radio Peripheral) [77].

4) Z3sec – платформа для тестирования безопасности, для полноценной работы которой требуется большое количество дополнительных пакетов. Поддерживаются такие аппаратные средства, как Ettus USRP и средства, совместимые с KillerBee [115].

В общем, атаки на БСС можно проклассифицировать по трем признакам [18; 104]:

1. Уровень активности атакующего: пассивные атаки / активные атаки.
2. Отношение нарушителя к системе: внешние атаки/ внутренние атаки;
3. Уровень сетевой модели (уровни представлены на рисунке 1.11).

Ниже приведены пояснения к каждому виду атак.

Рисунок 1.11 – Стандартный вид стека протоколов для БСС

Пассивные атаки, в основном, нарушают конфиденциальность данных. Нарушитель прослушивает незащищенный трафик и ищет в нем информацию, которую можно использовать для осуществления других типов атак [144.] К пассивным атакам относятся анализ трафика, прослушивание коммуникаций, расшифровывание слабозащищенного трафика и перехват учетных данных. Пассивный перехват сетевых операций дает нарушителям возможность предугадывать следующие действия в сети. Последствия пассивных атак – раскрытие информации или данных без согласия и разрешения пользователя БСС.

При осуществлении активных атак нарушитель принимает активные меры к получению контроля над сетью. Некоторые из атак, входящих в эту категорию, – это отказ в обслуживании (DoS), изменение данных, отброс пакетов (packet drop), воспроизведение передачи (replay), ложное информирование о данных маршрутизации (sinkhole attack) [137], подмена (spoofing), затопление (flooding), создание пробок в маршрутах (jamming), перегрузка (overwhelm), червоточина (wormhole), подделывание (fabrication), ложное объявление о маршрутах (hello

flood) [181], диверсия узлов (node subversion), недостаточность взаимодействия (lack of cooperation), модификация (modification), атака «человек посередине» (man-in-the middle), выборочное перенаправление (selective forwarding), и ложные узлы (false nodes).

Внешние атаки могут реализовать пассивное прослушивание трансмиссий данных, а также внедрять в сеть ложную информацию для расходования системных ресурсов и подготовки атак отказа в обслуживании.

Внутренние нарушители могут скрытно оказывать ущерб сети, потому что оперируют в обход процедур аутентификации и авторизации, так как являются легитимными узлами и имеют доступ к информации в сети, поэтому сложно предсказать закономерности их атак. Внутренние нарушители могут осуществлять целый ряд атак, противостоять которым довольно сложно, потому что трудно распознать, возникла ли аномалия из-за случайных факторов или внутреннего нарушителя [80; 83]. При таких атаках наблюдается подавление важной информации, которая не достигает базовой станции, что существенно ухудшает сетевую производительность, например, скорость доставки пакетов из-за их повторяющихся сбросов. К такому типу атак принадлежат отброс пакетов (packet drop), отброс пакетов с некоторой вероятностью (grayhole) [177], атака с сохранением уровня доверия к узлу (on-off attack) [62].

Атаки на физическом уровне разнятся от захвата и повреждения узлом до глушения канала радиовещания [178]. Иногда физические атаки обнаружить сложнее, чем программные, из-за отсутствия физического контроля над каждым отдельным узлом. Глушение – одна из самых важных атак на физическом уровне: нарушитель может в постоянном режиме транслировать радиосигналы по беспроводному каналу или передавать сигналы высоких энергий для блокирования беспроводной среды и препятствования связи между сенсорными узлами, что приведет к атаке отказа в обслуживании.

Функции протоколов канального уровня – координация соседних узлов в целях обеспечения доступа к разделяемым беспроводным каналам и предоставление абстракции связи для верхних уровней. Атакующие имеют

возможность преднамеренно нарушить предусмотренный протоколом алгоритм на канальном уровне. Например, вызов конфликтов прерыванием передачи пакета, израсходование энергии узлом постоянной передачей данных или перехват и анализ сообщений в целях получения информации из закономерностей связи. Данные действия возможны, даже если сообщения зашифрованы и не могут быть расшифрованы без ключа.

На сетевом уровне и на уровнях выше разнообразие атак увеличивается. Следует отметить атаки отказа в обслуживании, а также ряд атак, напрямую направленных на изменение маршрутной информации: ее имитация, изменение, перенаправление, что создает проблемы с трафиком в сети [3]. Также перехват одного из узлов теоретически позволяет нарушителю получить контроль над всей сетью [136].

Характерная угроза на транспортном уровне – израсходование ресурсов узлов и сети посредством непрерывного запроса на подключение, до достижения предельного количества подключений. В результате легитимные узлы не могут эффективно обрабатывать и передавать данные.

На прикладном уровне могут быть осуществлены атаки перегрузки (overwhelm), отказа (repudiation), повреждения данных и выполнение вредоносного кода.

В результате разработки модели угроз и модели нарушителя на основе базы данных угроз ФСТЭК было выявлено, что атаки сетевого уровня на БСС являются актуальными и представляют интерес для специалистов по обеспечению информационной безопасности (Приложение А). [19; 1; 58]

Более подробно описание исследуемых атак приводится в Главе 2.

Одним из наиболее простых и эффективных способов обеспечения ИБ БСС является мониторинг состояния сети [61]. Для этих целей применяются системы обнаружения вторжений (СОВ) (системы обнаружения атак [9; 35; 113]). В данной работе под обнаружением также понимается идентификация атак. [153; 19; 103].

Исследователи предлагают различные варианты техник обнаружения и

идентификации атак в сетях:

1) на основе анализа аномалий [133]. Подходы к обнаружению вторжений на основе анализа аномалий ищут необычные показатели среды [119; 90]. Основное преимущество подходов, основанных на аномалиях, заключается в том, что они 110 не ищут что-то конкретное [159]. Это устраняет необходимость точного указания всех известных векторов атак. Одним из основных недостатков этой категории является восприимчивость к ложным срабатываниям. [195; 171].

2) на основе анализа сигнатур. Подходы к обнаружению вторжений на основе сигнатур ищут набор параметров, соответствующих определенному шаблону неправильного поведения. Эти подходы реагируют только на известное некорректное поведение. Ключевым недостатком этой категории является сложность обновления словаря векторов атак. Сигнатура атаки может быть одномерной последовательностью данных: например, байты, передаваемые по сети, история системных вызовов программы или информационные потоки, относящиеся к конкретному приложению (например, измерения датчиков БСС). Одной из сложностей является объединение простых последовательностей данных в многомерную последовательность данных [91]. Важной исследовательской задачей в этой области является создание эффективного словаря атак [120]. Длина сигнатуры является показателем эффективности для таких подходов: более длинные сигнатуры предполагают более высокие требования к памяти и использованию микропроцессора.

3) на основе управления репутацией. Основная цель данного подхода – обнаружение узлов, проявляющих эгоистичное или зловредное поведение [118]. Исследователи в этой области добились высоких результатов [82; 111], однако для реализации таких подходов требуются большие вычислительные мощности, что не вписывается в ограничения данного исследования.

4) на основе анализа поведения [217]. Этот подход анализирует данные об узле или сети в целом, чтобы определить, скомпрометирован ли узел/сеть []. Отличие анализа поведения от анализа сигнатур состоит в учете временных

изменений признаков сети: предполагается, что для идентификации атак с высокой точностью необходимо наблюдение за изменением параметров во времени. Одним из основных преимуществ использования такого подхода является масштабируемость. Еще одним важным преимуществом использования подхода, основанного на анализе поведения, является децентрализация, то есть возможность исследования поведения одного узла, группы узлов или сети в целом. Одним из основных недостатков основанного на поведении объединения является то, что каждый узел должен выполнять дополнительную работу по сбору и/или анализу, своих данных, что является критичным в сетях с ограниченными ресурсами [186]. В данном диссертационном исследовании применяется именно метод анализа поведения сети.

Различные методы обнаружения и идентификации атак на БСС будут рассмотрены в следующем разделе.

1.3 Существующие методы идентификации атак на беспроводные сенсорные сети

В процессе анализа существующих методов обнаружения и идентификации атак на БСС были изучены материалы следующие исследования:

1) Да Силва и др. [180] предложили централизованную СОВ на основе анализа трафика. Достоинством метода являются малые энергозатраты, а недостатком – низкая точность (30%), ошибки первого рода 50% и невозможность обнаружения неизвестных атак. Авторы рассматривают 8 атак: задержку сообщения, воспроизведение сообщения, червоточину, джэмминг, атаки «черная дыра» и «серая дыра».

2) М.Р. Ахмед [67] предлагает метод защиты БСС от внутренних атак на основе мультиагентной системы. Рассматривается 18 различных атак, точность

обнаружения варьируется от 75% до 95%. В качестве исследуемой системы используется модель БСС на основе MatLab и J-Sim.

3) Дрозда и соавт. [105] предлагают подход к обнаружения вторжений на основе биологии. Это полу-контролируемая конструкция на основе аномалий.

34

Авторы использовали симулятор JiST / SWANS для моделирования сети с 1718 узлами, обменивающимися трафиком с низкой постоянной скоростью передачи данных (272 бит/с). Были исследованы атаки типа «серая дыра». Точность обнаружения для их метода колеблется от 41.14% до 99.94% и ошибки первого рода от 2.22% до 62,07%.

4) Гришечкина [18] предлагает анализировать 6 типов атак в большой сети (предполагаемо, до 65 тыс. устройств) на основе уязвимостей в сетевом протоколе.

5) Альмомани и соавт. [69] разработали набор данных для идентификации 4 атак (затопление, черная дыра, серая дыра и scheduling) в сети с кластерной топологией. Эксперименты проводились на модели сети, состоящей из 7 устройств. При использовании 23 признаков, точность идентификации составила 97,5%.

6) Бессонова и соавт. [38] предлагали идентифицировать 3 атаки (человек посередине, повторная пересылка и распределенный отказ в обслуживании) на основании 4 признаков и использовании искусственной нейронной сети [57]. Точность предложенного метода составила 91%. Для тестирования применялся симулятор OMNeT++, однако количество устройств в сети не превышало трех.

7) Сяо и соавт. [199] предлагают полуавтоматическую СОВ с использованием Байесовского классификатора. Обнаружение происходит на каждом узле для предотвращения дискредитации потока сетевых данных через агрегацию или другую внутрисетевую обработку. Исследователи ограничили набор для идентификации тремя параметрами, и рассматривают только атаки с воспроизведением пакетов.

8) Эль Мураби и соавт. [155] разработали СОВ на основе алгоритмов анализа данных. Предполагается, что система может с точностью до 99,9% обнаружить 16 различных атак на основе 41 признака. Для классификации использовался алгоритм «Случайный лес». Однако данное исследование имеет

35

недостаток: для обучения и тестирования алгоритма использовался набор данных на основе KDD 99.

9) Чен и соавт. [96] предложили метод обнаружения атаки «отказ в обслуживании» на основе объединения преобразования Гильберта-Хуанга и оценки доверия. В эксперименте использовалась модель БСС на основе NS2 simulator, однако в качестве обучающего набора данных был использован KDD Cup 99.

10) Калкха и соав. [138] описывают процесс обнаружения и предотвращения атаки «Черная дыра» на БСС с помощью скрытых Марковских моделей [88]. Достоинством данной модели является набор данных, полученный от реальной сети из 50 устройств на территории площадью 786x460 м.

11) Ма и соавт. [150] предлагают СОВ на основе некооперативной теории игр. Недостатком этого исследования является относительно низкая точность идентификации, которая составляет всего 70%. Авторы рассматривают такие атаки, как джэмминг, истощение, изменение маршрутизации и затопление.

12) Гур и соавт. [126] разработали метод идентификации атак на основе избыточных перекрестных проверок. Кластеры выбирают агрегатор, который пересылает данные датчиков в приемник на основе оценок надежности. Достоинством этого метода является формула достоверности, которая основана

на 4 параметрах: расстоянии, количестве и качестве производимых данных и оставшейся энергии. Недостаток данного исследования заключается в том, что 110 модель угроз не рассматривает сотрудничество вредоносных узлов. Основное внимание авторы уделяют атакам на обработку данных.

13) Цзиньхуэй и соавт. [132] рассматривают СОВ для гибридных атак типа «отказ в обслуживании» и для обнаружения используют показатели энергопотребления узла. Исследования проводились с помощью симулятора NS-2 на кластерной топологии сети. Точность обнаружения составила 80%.

14) Абрамов и Басан [1] в процессе разработки модели защищенной кластерной БСС использовали такие показатели, как среднее количество энергии, уровень доверия [89] и др. Модель позволяет обнаружить 11 атак.

36

15) Барати и соавт. [78] осуществляют обнаружение атаки типа «отказ в обслуживании» с помощью различных техник классификации. Основным классификатором является алгоритм «случайный лес», точность достигает 96,7%. Для получения и анализа данных использовался NS-2 с 100 узлов, разделенных на 5 кластеров.

16) Кальнур и соавт. [139] предлагают метод обнаружения злоумышленника с помощью КМП-алгоритма. Исследователи не приводят деления на конкретные атаки, но предполагают, что с помощью анализа аномалий могут с точностью до 87% обнаружить практически любое зловредное воздействие.

17) Жу и соавтр. [205] описывают способ обнаружения атаки «выборочная пересылка» на основе адаптивного автомата и эффективности коммуникации. Для проведения экспериментов использовался симулятор OMNeT++, была построена сеть из 151 устройства. Авторы достигли точности идентификации, равной 97,1%.

18) Ганеривал и соавт. [111] предлагают метод обнаружения атак, который вычисляет оценки репутации на основе сходства данных, сообщаемых датчиками с избыточным покрытием. Здесь используется обнаружение выбросов на основе плотности для генерации оценок репутации и снижение показателей доверия с течением времени при отсутствии обновления. Достоинством данного метода является экспериментальное проектирование: авторы моделируют свою конструкцию, реализуют ее и собирают данные как в лабораторных, так и в эксплуатационных условиях.

19) Чэнь [97] предлагает СОВ на основе уровней доверия, однако отсутствие численных результатов не позволяет оценить качество работы. Автор рассматривает переадресацию пакетов, рассинхронизацию времени и атаки на обработку данных.

20) Онат и Мири [162] оценивают уровень принимаемого сигнала и скорость поступления пакетов от доверенного узла. Обнаруживаются такие атаки, как спуфинг и истощение ресурсов.

37

21) Замани и соавт. [201] разработали метод обнаружения атак на основе поиска сигнатур в трафике. Подход авторов основывался на распределенной природе биологической иммунной системы. В методе фигурируют несколько объектов: неподвижные агенты (по аналогии с тимусом, костным мозгом, лимфатическими узлами) действуют как обычные ткани тела и специальные движущиеся агенты (особые клетки) играют роль иммунных клеток. Критерии обнаружения представляют собой взвешенную сумму уровней безопасной концентрации, уровней опасной концентрации и плотности совпадающих молекулярных паттернов. Ошибки первого и второго рода составляют 40% и 8,23% соответственно. Модель фокусируется на DDoS-атаки.

22) Иоаннис и соавт. [129] предлагают СОВ на основе множественного доверия и анализе трафика. Обнаруживаются 2 атаки: «черная дыра» и «серая

дыра». Авторы анализируют отношение скорости и количества проявления нарушений.

Приведенный выше перечень проанализированных исследований не является полным и исчерпывающим, однако является достаточным для понимания существующих подходов и сравнения с результатами данной работы. Таким образом, было выявлено, что в большинстве случаев исследования направлены на выявление в среднем 5-6 разновидностей атак. Используются различные признаки для осуществления классификации. Точность обнаружения и идентификации также варьируется в среднем от 50 до 90 процентов.

1.4 Показатели эффективности идентификации атак на беспроводные сенсорные сети

Для оценки эффективности системы обнаружения вторжений и идентификации атак используется множество различных характеристик [31; 42]. Чаще всего используются следующие характеристики [критерии выбора систем] [2; 123]:

1) архитектура СОВ (единая, модульная);
2) место размещения;

3) поддерживаемые операционные системы и сетевые протоколы;
4) доступный перечень источников информации (возможность получения информации о событиях в сети);
5) доступный перечень вариантов реагирования на атаки (возможность предпринимать различные действия в ответ на обнаруженные атаки) [124];
6) возможность удаленного управления;
7) обеспечение отказоустойчивости связи между агентами СОВ и основным модулем;
8) оперативность и качество обновления;
9) возможность добавления пользовательских сигнатур и правил (если планируется доработка системы обнаружения атак под нужды конкретной, не вполне типовой информационной системы, именно такая возможность является залогом потенциальной тонкой настройки системы обнаружения атак [204];
10) удобство работы и настройки;
11) производительность;
12) стоимость.

Вследствие того, что в данном исследовании не разрабатывается полноценная СОВ, а лишь ее составляющие части, необходимые для мониторинга состояния сети, не все из приведенных выше характеристик подходят для оценки [196]. Соответственно, было принято решение составить новый перечень для оценки эффективности [85] идентификации атак на БСС.

На основании проведенного анализа существующих исследований был составлен предполагаемый перечень показателей:

1) количество идентифицируемых атак;
2) количество признаков, необходимых для идентификации;
3) точность, аккуратность, полнота идентификации;
4) топология сети;
5) влияние на сеть (активный или пассивный мониторинг);
6) сложность алгоритма анализа;
7) возможность расширения;

8) использование актуального набора данных.

Однако, такое количество показателей для оценки эффективности не является целесообразным [102], поэтому было принято решение сократить перечень до 4 признаков:

1) количество идентифицируемых атак;

2) количество идентификационных признаков;

3) точность (precision);

4) полнота (recall).

Также выявленным показателям были присвоены весовые коэффициенты в зависимости от частоты появления в существующих исследованиях. В таблице 1 представлен перечень показателей и присвоенные веса.

Таблица 1 – Показатели эффективности идентификации атак

Показатель эффективности	Присвоенный вес, %
количество идентифицируемых атак	15
количество идентификационных признаков	25
точность (precision)	30
полнота (recall)	30

Таким образом, формулу для оценки эффективности идентификации можно представить следующим образом:

$Q = q1 * 0,15 + q2 * 0,25 + q3 * 0,3 + q4 * 0,3$

Суммарный вес всех показателей равен 100%.

1.5 Постановка задачи исследования

В соответствии с вышеизложенным, существует необходимость разработки научно-методический аппарата для идентификации атак сетевого уровня на БСС. Для идентификации атак предлагается использовать поведенческий анализ, основанный на мониторинге характеристик (признаков) поведения сети. Под

поведением сети в данной работе понимается совокупность характеристик (признаков) сети в определенный момент времени.

Научная задача данной работы состоит в разработке и обосновании научно-методического аппарата по идентификации атак сетевого уровня на беспроводные сенсорные сети на основе анализа новой комбинации признаков, характеризующего поведение такой сети. Ключевым элементом научной задачи является идентификация атак. Идентификация представляет собой сопоставление текущего поведения сети с известным поведением (нормальное поведение, типы поведения под атаками: «затопление», «повторная передача» и др.). Задача идентификации сводится к задаче классификации, которую рассмотрим далее.

В классическом виде постановку задачи классификации можно представить в следующем виде [110] . Существует некое множество всевозможных объектов – $X = \{x1,..., xn\}$ и его подмножество, содержащее исследуемы объекты Xc . Под исследуемыми объектами понимаются те, которые рассматриваются в рамках решаемой задачи. Также определено множество классов $Y = \{C0,..., Cm\}$, каждый из которых представляет собой [110] набор объектов, являющийся подмножеством Os, и объединённых некоторой связью: $\forall Ci \in Y (Ci \subset Xc)$.

Введём вспомогательное отображение $\lambda : C \rightarrow \{0, ..., m\}$ – которая ставит каждому классу его номер (метку): $\forall Ci \in Y \lambda(Ci) = i, i = 0, m$.

Будем считать, что каждому объекту x соответствует один класс, то ест существует неизвестная целевая зависимость $y*:Xc \rightarrow \lambda(Y)$. В связи с этим множество Xc является дизъюнктивным объединением множеств, объединяющих различные классы $Ci(i = 0, ..., m)$: $Xc = \bigvee_{i=0}^{m} Ci$. В случае возникновения задачи мультиклассификации, когда одному объекту соответствует несколько классов, необходимо её свести к задаче классификации за счёт введения дополнительных признаков, которые бы позволили обеспечить однозначное выполнение целевой зависимости $y*$.

Каждый объект $x \in Xc$ представлен набором признаков $x = (x1,... ., xk)$ – то есть представляет собой вектор признаков.

Тогда для решения задачи классификации необходимо построить алгоритм,

относящийся к множеству всех алгоритмов A, такой что a : Xc → {1, ..., m},
который максимизирует отношение верно классифицированных объектов к
общему количеству объектов x ∈ Xc:
Ω(a, Xc) =
1
#Xc
· #{x | (∃Ci ∈ C,x ∈ Ci)∧ a(x) = λ(x)}x∈Xc → max
a ∈A
Задача, поставленная в данной диссертационной работе, может быть
сформулирована следующим образом [110]. Дано множество классов поведений сети C:
нормальное поведение, поведение под атакой (атака «затопление», и др.); K –
множество признаков поведения сети, и множество исследуемых поведений сети
Xc. Выделим из множества K подмножество наиболее информативных признаков:
KI ⊆ K. Каждое поведение представлено вектором признаков размерностью k =
#KI . Пусть тогда XcKI – исследуемые объекты, представленные вектором из
признаков k ∈ KI. С помощью некоего правила R построена обучающая выборка:
набор маркированных векторов признаков поведения сети ΞXc
L = {(x'
i,ci)}i=0
M =
∪∪ x∈Ci∩Xc (x, λ (C))
Ci∈C L, где Xc
L ⊆ Xc – множество обучающих векторов, а xi
' ∈
Cici
– отношение принадлежности.
Тогда для решения задачи идентификации атак на БСС, на базе обучающей
выборки ΞXc
L нужно решить следующую оптимизационную задачу. Введём
дополнительное множество G = {KI1,..., KIk}, где KIi ⊆ KI,#KIi = i, и
дополнительную вспомогательную функцию ψ:G → {XcKI1
, ..., XcKIk
}, где XcKIi
–
исследуемые объекты x ∈ Xc, представленные с помощью вектора длиной i.
Необходимо при заданном уровне эффективности σ идентификации свести к
минимуму количество используемых признаков k ∈ KI:
Λ(a,Xc,σ) = min
i ∈{1,...,k}
{#KIi | KIi ∈ G,Ω(a, ψ(Ki)) ≥ σ},
где Λ(a,Xc,σ) – функция оценки минимального набора признаков поведения, σ –
наперёд заданное положительное число.

Выводы по главе 1

1) Рассмотрена концепция беспроводных сенсорных сетей в рамках
киберфизических систем, выявлены особенности функционирования
беспроводных сенсорных сетей, такие как малый объем памяти и вычислительных
мощностей устройств беспроводных сенсорных сетей и ограниченные
энергоресурсы. Сформулированы ограничения исследования, касающиеся
используемой спецификации, уровня передачи данных и исследуемых атак. В
работе рассмотрен сетевой уровень спецификации ZigBee. Предполагается
пассивный вид мониторинга поведения сети.

2) Выполнен анализ существующих подходов к идентификации атак на
беспроводные сенсорные сети. В рамках осуществленного анализа предложена
оценка эффективности идентификации атак. Эффективность представляет собой

совокупность таких параметров, как количество идентифицируемых атак, количество идентификационных признаков, точность (precision) и полнота (recall).

3) Выполнена постановка задачи диссертационного исследования, которая заключается в разработке научно-методического аппарата для идентификации атак сетевого уровня на БСС на основе поведенческого анализа.

43

Глава 2 Модель профиля поведения беспроводной сенсорной сети. Метод идентификации атак на беспроводные сенсорные сети, основанный на поведенческом анализе

2.1 Модель профиля поведения беспроводной сенсорной сети

Под профилем поведения в данном исследовании понимается совокупность основных параметров, характеризующих состояния сети.

Пусть

M =< x1,x2,..., xn >,

где M - модель профиля поведения БСС, с помощью которой можно охарактеризовать состояние сети как нормальное поведение сети или поведение сети под атакой, xi - некоторый признак состояния сети, а n - количество используемых признаков.

Соответствующее признаковое пространство для разработки модели было сформировано из 51 признака [214; 216]. Источниками для составления набора признаков являлись стандарт IEEE802.15.4 [207] и спецификация ZigBee [208], существующие исследования [68; 81; 108] и результаты практического использовании.

Для получения результатов практического использования были экспериментально исследованы характеристики модулей ZigBee ETRX357 трех видов (со встроенной антенной, с возможностью подключения внешней антенны и со встроенным усилителем мощности) с отладочными платами, на которых располагаются датчики света и температуры [164]. Фотография устройств представлена на рисунке 2.1. Благодаря наличию интерфейса «Telegesis Terminal», представленного на рисунке 2.2, возможно управление модулями с помощью AT-команд, а также получение данных о сети и данных с сенсоров.

Также, признаки выбирались в соответствии с возможными вариантами совершения атак на БСС. Выделенные признаки сгруппированы следующим образом:

44

1. Количественные признаки – представлены в таблице 2;

2. Сводные признаки – представлены в 3 (для всех признаков собираются три значения: max – максимальное, min – минимальное, avg – усредненное по количеству узлов в сети);

Рисунок 2.1 – Используемые модули ZigBee ETRX357, отладочные платы и USB-шлюз

Рисунок 2.2 – Интерфейс «Telegesis Terminal»

3. Признаки-соотношения – представлены в таблице 4. Для этих признаков формируются три значения: max– максимальное, min– минимальное, avg– усредненное по количеству узлов в сети. Если один (любой) из элементов

45

соотношения равен нулю, к нулю приравнивается и соотношение – вне зависимости от того, в какой части соотношения оказался нуль (в числителе или знаменателе).

Таблица 2 – Количественные признаки поведения БСС

Признак Описание

num_frames Общее количество кадров, переданных в сети по стандарту IEEE802.15.4

num_frames_avg Общее количество кадров, переданных в сети по стандарту IEEE802.15.4, усредненное по числу PAN в сети

num_packets Общее количество пакетов, переданных в сети по спецификации ZigBee

num_packets_avg Общее количество пакетов, переданных в сети по спецификации ZigBee, усредненное по числу PAN в сети

num_route_msgs Количество переданных маршрутных сообщений (RREQ, RREP) по стандарту IEEE 802.15.4

num_forwarded_packets Общее количество пересланных сообщений в сети в рамках протокола маршрутизации пакетов

Таблица 3 – Сводные признаки поведения БСС

Признак	Описание
num_packets_out	Количество пакетов, отправленных каждым узлом (собственных и пересланных)
num_packets_in	Количество пакетов, полученных каждым узлом (адресованных узлу и подлежащих пересылке)
weighted_num_packets_in	Взвешенное по числу узлов-получателей количество пакетов, полученных каждым узлом (адресованных узлу и подлежащих пересылке)
num_packets_equal_src	Количество полученных пакетов, в которых в качестве отправителя указан один и тот же узел

num_packets_equal_src_pan	Количество полученных пакетов, в которых в качестве PAN отправителя указан один и тот же PAN
num_packets_equal_dest	Количество полученных пакетов, в которых в качестве получателя указан один и тот же узел
num_packets_equal_dest_pan	Количество полученных пакетов, в которых в качестве PAN получателя указан один и тот же PAN
num_frames_out	Количество кадров, отправленных каждым узлом (собственных и пересланных)
num_frames_in	Количество кадров, полученных каждым узлом (адресованных узлу и подлежащих пересылке)
weighted_num_frames_in	Взвешенное по числу узлов-получателей количество кадров, полученных каждым узлом (адресованных узлу и подлежащих пересылке)
num_forwarded_packets	Количество пересылаемых узлом пакетов
num_packets_created	Количество пакетов, созданных узлом

Таблица 4 – Признаки-соотношения поведения БСС

Признак	Описание

frac_packets_in_out Соотношение для каждого узла количества полученных и переданных в сеть пакетов

frac_packets_in_out_pa
n

Соотношение для каждой PAN количества полученных и переданных в сеть пакетов

frac_packets_created_a
cquired

Соотношение между количеством пакетов, созданных узлом, и количеством полученных пакетов, в которых в качестве источника указан данный узел

Было выдвинуто предположение, что с помощью данной модели возможно идентифицировать следующие состояния сети:

1) Нормальное поведение сети.

2) Атака «отказ во сне» (Denial of Sleep). Атакующий узел генерирует и отправляет пакеты определенному узлу в сети, что приводит к истощению источника питания узла [174].

3) Атака «затопление» (Flood). При такой атаке осуществляется передача пакетов на конкретный адрес с частотой выше, чем в нормальном состоянии.

4) Классический вариант атаки «повторная передача» (Repeated transmission). Для этой атаки характерна пересылка некоторых пакетов: каждый k-й пакет дублируется во внутренней очереди, а повторная передача из очереди каждого следующего пакета происходит каждые L секунд.

5) Атака «повторная передача» для конкретного узла. Осуществляется по аналогии с предыдущей, с тем отличием, что во внутренней очереди сохраняются пакеты для определенного узла.

6) Атака «повторная передача» от конкретного узла. Во внутренней очереди сохраняются пакеты, отправленные определенным узлом.

7) Классический вариант атаки «выборочная пересылка» (Selective forwarding). Данная атака позволяет отбросить каждый k-й пакет вместо пересылки.

8) Атака «выборочная пересылка» пакетов для конкретного узла. Действует по аналогии с классическим вариантом, но отбрасываются лишь пакеты, адресованные определенному узлу.

9) Атака «выборочная пересылка» пакетов от конкретного узла. Эта атака действует также, как две предыдущие, но отбрасываются лишь те пакеты, которые сгенерированы одним узлом.

10) Атака «воронка» (Sinkhole). Особенность данной атаки заключается в «перетягивании» всего трафика на скомпрометированный узел.

11) Классический вариант атаки «подмена» (Spoofing). Эта атака представляет собой подмену адресов отправителя и получателя на случайные для каждого k-го генерируемого пакета.

12) Атака «подмена» для конкретного узла. Данный вариант атаки предусматривает изменение адреса узла-отправителя на случайный, а адреса узла-получателя на конкретный узел.

13) Атака «подмена» от конкретного узла. Эта атака происходит по аналогии с предыдущей, но указывается конкретный адрес узла-отправителя, и случайный для узла-получателя.

14) Атака Сивиллы (Sybil). В данной атаке происходит создание большого количества зловредных узлов, которые выдают себя за легитимные.

15) Атака «червоточина» (Wormhole). Характеризуется построением «туннеля» и ретрансляцией пакетов злоумышленников в желаемом направлении.

По данным Positive Technologies, приведенных в материалах « Беспроводные

указанные атаки не требуют большого объема вычислительных и программно-аппаратных ресурсов, и, соответственно, легко доступны для злоумышленников [135]. Результатом таких атак является нарушение доступности и целостности информации, циркулирующей в БСС.

2.2 Формирование набора данных об атаках на беспроводные сенсорные сети

В процессе диссертационной работы было выявлено, что часть исследователей использовали набор данных KDD'99 – набор данных, разработанный для конкурса по интеллектуальному анализу данных в 1999 году [140] на основании 1998 DARPA Intrusion Detection Evaluation Program [127]. Задача конкурса состояла в том, чтобы построить детектор сетевых вторжений и атак для локальной сети [13], способный различать нормальное поведение и различные атаки [152]. Эта база данных содержит стандартный набор данных, который включает в себя широкий спектр вторжений, моделируемых в среде военной сети [151].

Некоторые исследования использовали адаптированные наборы данных, представляющие собой в основном модельные данные [170; 192]. Однако либо

указанные наборы не были представлены в общем доступе, либо отражали лишь 1-4 атаки [59; 70]. Соответственно, было принято решении о разработке программной модели реализации атак на БСС [64].

Существует большое количество средств имитационного моделирования и моделирования сетей, из которых чаще всего используются AnyLogic, OMNeT++, ns, OPNET, NetSim и GNS3. Некоторые программные модели БСС [28] представлены в коммерческих проектах и имеют закрытый исходный код, что исключает возможность создания атакующих сеть узлов без осуществления обратного анализа кода этих проектов. Другие средства моделирования представляют собой упрощенную реализацию стандарта IEEE 802.15.4, поверх которой строится стек протоколов TCP/IP – как значительно более распространенный и широко используемый [99]. Более того, часто средства моделирования направлены на изучение вопросов энергоэффективности модулей и корректности используемых протоколов БСС. При этом реализуются лишь наиболее простые топологии сети – «звезда», «дерево» и «точка-точка», которые, хотя и применяются на практике, представляют собой лишь частный случай беспроводных сенсорных сетей, исключающий возможность проведения многих атак, возможных в сетях с топологиями «кластерное дерево» и «ячеистая сеть» [49].

Сравнительная характеристика средств моделирования на основании критериев, важных с точки зрения разработки модели проведения атак на беспроводные сенсорные сети приведена в таблице 5.

Таблица 5 – Сопоставление средств моделирования

OMNeT++	NetSim	ns	AnyLogic	GNS3
Лицензия	Academic	Proprietary	GPLv2	Proprietary	GNU GPL
OS	Linux, Unix, Windows (MinGW), Mac OS	Windows	Linux, Unix, Mac OS	Windows, Linux, Mac OS	Windows, Linux, Mac OS

50

OMNeT++ NetSim ns AnyLogic GNS3

Тип Библиотека и

фреймворк

Средство

симуляции

Симулятор для

дискретно-

событийного

моделирования

Средство

имитационного

моделирования

Эмулятор

сетевых

взаимодейст

вий

Назначен

ие

Создание

моделей сетей

Создание

моделей сетей

Создание

моделей сетей

Создание

имитационных

моделей

Создание

моделей

сетей

Язык C++ C C++ Java -

IDE + + - +/- -

Визуализ

ация

+ + + + +

Таким образом, были проанализированы различные средства симуляции и моделирования [21; 37] и было выявлено, что наиболее актуальным является симулятор (среда моделирования) OMNeT++, так как он представляет собой объектно-ориентированную библиотеку, в которой определены классы для объектов сетевого взаимодействия (узлов сети) и сообщений, пересылаемых между ними. Преимуществами данного симулятора являются доступный язык программирования, присутствие среды интегрированной разработки и наличие лицензии.

Симулятор OMNeT++ позволяет осуществлять дискретно-событийное моделирование. Для этого используется концепция очереди сообщений. Все взаимодействия между объектами осуществляются с помощью пересылки сообщений. При этом каждому сообщению соответствует время его доставки, в соответствии с которым сообщения помещаются в очередь с приоритетом: чем ближе значение времени доставки к текущему, тем ближе к началу очереди сообщение. При каждом извлечении сообщения из очереди глобальная переменная времени принимает значение, соответствующее времени доставки сообщения.

Как уже было отмечено ранее [110], главной целью осуществляемого

моделирования атак на БСС является получение [121] статистики сетевых

51

отправлений и исследование статистических характеристик сети при совершении атак на целостность и доступность. При этом существенное внимание требуется уделять детализации моделирования процессов, протекающих как в рамках отдельных узлов, так и в масштабах всей сети [219].

В модели предполагается, что скорость передачи между любыми двумя узлами (через один хоп) является одинаковой. При этом в рамках алгоритма построения маршрута в ячеистой сети используется критерий количества промежуточных узлов до узла назначения [175]. Этот способ часто используется и на практике [145].

Необходимо рассмотреть две сети с одинаковыми топологией, количеством узлов, средней частотой генерации новых пакетов, частотным диапазоном (и, соответственно, одинаковой скоростью передачи) [43, 44].

Пусть максимальное количество сетевых пакетов, передаваемых в такой сети за время t равно k. Предположим, что за время t первая сеть создает k пакетов, а вторая сеть – k+m пакетов. В сети работает сбор статистики: через каждые N×t единиц времени записывается, например, общее количество пакетов, переданных в сети за это время. Динамика работы сети представлена в таблице 6. Приведенные значения для момента времени N×t выведены на основе метода математической индукции.

Таблица 6 – Динамика работы в зависимости от частоты генерации пакетов

Время	Сеть 1			Сеть 2		
	Создано	Передано	Очередь	Создано	Передано	Очередь
t	k	k	-	k+m	k	m
2×t	k	k	-	k+m	k	2×m
…	…	…	…	…	…	…
N×t	k	k	-	k+m	k	N×m

В момент времени N×t происходит запись накопленной статистики. При этом в выборку заносятся лишь те значения, которые были получены на основании реально переданных в среду пакетов, количество пакетов в очереди игнорируется [156]. Следовательно, для достижения целей имитационного

52

моделирования нет необходимости детально описывать процесс передачи данных через среду. Если число пакетов превышает максимально допустимое для данных характеристик сети, излишки будут помещены в очередь, статистика же будет соответствовать аналогичной при характеристиках, допускающих передачу всех пакетов в узел назначения. Иными словами, с точки зрения сборщика статистики о передаваемых по сети пакетах, сеть, работающая с максимально допустимой частотой генерации пакетов, и сеть, превышающая эту частоту, выглядят одинаково. Стоит отметить, что для корректного построения и использования модели с таким предположением необходимо оценить максимально допустимую среднюю частоту генерации пакетов.

Под частотой генерации пакетов понимается величина, обратная периоду – временному промежутку между созданием новых пакетов. Естественно предположить, что в беспроводных сенсорных сетях период между генерацией последовательных пакетов является либо постоянной, либо незначительно изменяющейся величиной. Поэтому в модели период генерации пакетов для любого узла подчиняется нормальному распределению, причем значения математического ожидания и стандартного отклонения задаются пользователем. Фактически числитель частоты – количество пакетов, генерируемых за промежуток времени в знаменателе. При приведении к общему знаменателю всех частот в числителях оказывается количество пакетов, создаваемых каждым из узлов за промежуток времени в знаменателе. При этом сумма этих значений

представляет собой количество пакетов, созданных во всей сети за тот же временной отрезок. Следовательно, совокупная частота создания новых пакетов получается алгебраической суммой частот создания пакетов каждым из узлов в отдельности:

{

T1 = k

T2 = l

T3 = m

□

{

v1 =

1

k

v2 =

1

l

v3 =

1

m

⇒

{

v1 =

lm

klm

v2 =

kl

klm

v3 =

km

klm

⇒ vобщ =

lm + kl + km

klm

Разрабатываемая модель имеет еще одну особенность – предполагается мгновенная передача сообщений между двумя последовательными узлами маршрута [56]. Для простоты написания программы вместо воспроизведения фактической передачи данных через среду реализована задержка отправки каждого пакета в среду на время, высчитанное методом, представленным ниже. На сбор статистики это предположение влияния не оказывает, поскольку в модели, как и в реальной системе, сообщение считается переданным только после успешной передачи последнего информационного бита. Единственное значимое следствие – явное предположение отсутствия коллизий, которое также обосновывается приведенными ниже математическими выкладками.

В первую очередь рассматривается процесс передачи сообщения между двумя соседними узлами сети ZigBee. В стандарте IEEE 802.15.4-2015 определен формат пакета на физическом уровне [143], представленный на рисунке 2.3.

Рисунок 2.3 – Пакет физического уровня IEEE 802.15.4

Было теоретически рассчитано максимальное время передачи пакета. Стандарт предлагает несколько методов модуляции сигнала, из которых в работе рассматриваются два – BPSK (Binary Phase-Shift Keying) и O-QPSK (Offset Quadrature Phase-Shift Keying). Использовавшийся ранее метод ASK (Amplitude Shift Keying) в настоящее время признан устаревшим, а остальные методы пока что используются реже, чем выделенные. Скорости передачи информации и символов приведены в таблице 7. Здесь и далее для O-QPSK рассматриваются

только частотные диапазоны 2,4 ГГц и 868 МГц. Стандарт определяет и другие частотные диапазоны, для которых скорости передачи либо совпадают со скоростями для диапазона 2,4 ГГц, либо попадают в промежуток между значениями, соответствующими 2,4 ГГц и 868 МГц.

54

Таблица 7 – Характеристики среды передачи данных

Модуляция Число октетов в символе

Частота Скорость передачи символов

Скорость передачи данных

BPSK 1 868 МГц 20 Ксимв/с 20 Кбит/с

915 МГц 40 Ксимв/с 40 Кбит/с

O-QPSK 2 868 МГц 25 Ксимв/с 100 Кбит/с

2,4 ГГц 62,5 Ксимв/с 250 Кбит/с

В сети без использования слотов координатор и маршрутизаторы обычно не переходят в спящий режим и подключены к сетям электропитания. Взаимодействие с конечными устройствами (RFD) осуществляется по принципу «запрос-ответ»: конечные узлы автономны, проводят большую часть времени в спящем режиме, но иногда «просыпаются» и либо непосредственно осуществляют передачу данных по алгоритму CSMA/CA (множественный доступ с контролем несущей и избеганием коллизий), либо запрашивают у координатора PAN (Private Area Network) маячок [198]. Координатор отправляет маячок, в котором содержатся сведения о наличии информации, предназначенной для конечного узла. Затем – осуществляется стандартная передача с помощью того же CSMA/CA. При этом передающий узел:

1. ожидает в течение случайного промежутка времени от 0 до 2BE-1, где BE – Backoff Exponent (эта величина по умолчанию равна 3);
2. прослушивает среду на наличие активной передачи – в течение времени aCcaTime (по умолчанию – 8 символов);
3. в зависимости от состояния среды:

a. если среда занята – увеличивает значение BE на 1 и переходит к пункту 1;

b. если среда свободна – передает данные;

c. если количество повторных попыток превысило допустимый рубеж (macMaxCsmaBackoffs, по умолчанию, 4), то прекращает попытки пересылки и возвращает ошибку.

55

Общее время передачи складывается из следующих величин:

1. Период начального ожидания – InitialBackoff;
2. Передача данных – TransmissionTime;
3. Переключение из режима прослушивания в режим передачи – Rx-Tx;
4. Передача подтверждения (без использования CSMA/CA).

$$InitialBackoff = (2^3 - 1) * aUnitBackoffPeriod + aCcaTime$$

$$= 7 * (aTurnaroundTime + aCcaTime) + aCcaTime$$

$$= 7 * 20 \text{ символьных периодов} + 8 \text{ символьных периодов}$$

$$= 148 \text{ символьных периодов}$$

$$DataSize = 133 * 8 = 1064 \text{ бит}$$

Минимальное и максимальное время передачи одного пакета в сети без слотов представлено в таблицах 8 и 9 соответственно.

Таблица 8 – Минимальное время передачи одного пакета в сети без слотов

O-QPSK BPSK

2,4 ГГц 868 МГц 915 МГц 868 МГц

InitialBackoff

148

62500

= 2,368 мс

148

25000

= 5,92 мс

148

40000

= 3,7 мс

148

20000

= 7,4 мс

TransmissionTime

1064

250000

= 4,256 мс

1064

100000

= 10,64 мс

1064

40000

= 26,6 мс

1064

250000

= 53,2 мс

Rx-Tx

12

62500

= 192 мкс

12

25000

= 480 мкс

12

40000

= 300 мкс

12

20000

= 600 мкс

AckTime

88

250000

= 352 мкс

88

100000

= 880 мкс

88

40000

= 2,2 мс

88

20000

= 4,4 мс

Total 7,168 мс 17,92 мс 32,8 мс 65,6 мс

Также необходимо оценить максимальное время передачи одного пакета.

Как было отмечено ранее, если по истечении интервала InitialBackoff среда

остается занятой, BE увеличивается на 1, и снова начинается интервал ожидания. Цикл может пройти до 4 итераций. Тогда максимальное время ожидания:

InitialBackoff

= (23 − 1) ∗ aUnitInitialBackoffPeriod + aCcaTime + (24 − 1)

∗ aUnitInitialBackoffPeriod + aCcaTime + (25 − 1)

∗ aUnitInitialBackoffPeriod + aCcaTime + (26 − 1)

∗ aUnitInitialBackoffPeriod + aCcaTime

= aUnitInitialBackoffPeriod ∗ (7 + 15 + 31 + 63) + 4 ∗ aCcaTime

= 116 ∗ 20 + 4 ∗ 8 = 2352 символьных периода

Таблица 9 – Максимальное время передачи пакета в сети без слотов

O-QPSK BPSK

2,4 ГГц 868 МГц 915 МГц 868 МГц

InitialBackoff

2352

62500

= 37,632 мс

2352

25000

= 94,08 мс

2352

40000

= 58,8 мс

2352

20000

= 117,6 мс

... ...

Total 42,432 мс 106,08 мс 87,9 мс 181,2 мс

Следовательно, в наихудшем случае максимально загруженной сети пакет будет передан быстрее, чем через 1 секунду после создания (иначе – будет возвращена ошибка, а в модели предполагается отсутствие таких ошибок). Это, в частности, объясняет предположение о крайне малой вероятности коллизии, сделанное ранее: даже если произойдет коллизия, повторная передача займет не более 181,2 мс в наихудшем случае, что значительно меньше исследуемых в модели временных промежутков. Коллизия возможна только в случае, изображенном на рисунке 2: узлы, POS (private operating space) которых пересекаются менее, чем наполовину, одновременно отправляют сообщения третьему узлу, и тем самым нарушают передачу друг друга.

Рисунок 2.4 – Коллизия CSMA/CA

В такой сети с использованием слотов (сети с маячками) особое значение имеют типы устройств и сообщений. Координаторы периодически посылают в сеть сообщения специального типа – маячки, которые, во-первых, передают конфигурационную информацию, а во-вторых – выполняют функцию синхронизации. Разделение среды между координаторами разных PAN может осуществляться по-разному: разделением времени, передачей в разных частотных диапазонах и т.д.

Временной интервал между маячками делится на активную и неактивную части. Активная часть называется суперфреймом и состоит из 16 слотов. Первый слот занимает маячок. Временем начала первого слота считается время начала передачи первого информационного бита полезной нагрузки пакета физического уровня. В рамках суперфрейма осуществляется конкурентный доступ к слотам по алгоритму CSMA/CA. Последние 7 слотов могут быть выделены для передачи данных без конкуренции, но этот случай рассматриваться не будет.

Следовательно, отличие от предыдущего случая заключается в следующем:

1. Имеется жестко заданное разделение на активный и неактивный промежутки времени;

2. По умолчанию прослушивание канала осуществляется в течение времени CW*aCcaTime, где CW по умолчанию – 2;

3. Большую часть времени все устройства сети проводят в спящем режиме.

Для сети со слотами справедливы следующие соотношения:

BeaconInterval = BI = aBaseSuperframeDuration ∗ 2macBeaconOrder

SuperframeDuration = SD

= aBaseSuperframeDuration ∗ 2macSuperframeOrder

aBaseSuperframeDuration = aBaseSlotDuration ∗ aNumSuperframeSlots

= 60 символов ∗ 16 = 960 символов

macBeaconOrder и macSuperframeOrder могут принимать значения от 0 до 14, причем macSuperframeOrder должен быть меньше, чем macBeaconOrder.

Максимальные и минимальные значения BI (BeaconInterval) и SD (SuperframeDuration) при этом приведены в таблице 10.

Таблица 10 – Максимальные и минимальные значения BI и SD

	O-QPSK	BPSK	
	2,4 ГГц	868 МГц	915 МГц	868 МГц
aBaseSlotDuration	15,36 мс	38,4 мс	24 мс	48 мс
BImax и SDmax	251,65824 с	629,1456 с	393,216 с	786,432 с
BImin и SDmin	15,36 мс	38,4 мс	24 мс	48 мс

Рассматривать простейший случай системы, в которой каждая PAN функционирует на собственном канале бессмысленно, поскольку в этом случае принципиальной разницы со случаем сети без слотов нет: в каждой сети маячки могут посылаться даже одновременно. Поэтому приведем вычисления для случая разделения во времени. Требуется оценить минимальный интервал между маячками главного координатора, при условиях:

1. В сети может быть 10, 15 или 20 PAN;

2. Каждая PAN включает 5 узлов;

3. Коллизии исключены.

InitialBackoffbest = (23 − 1) ∗ aUnitBackoffPeriod + CW ∗ aCcaTime

= 7 ∗ (aTurnaroundTime + aCcaTime) + CW ∗ aCcaTime

= 7 ∗ 20 символьных периодов + 2 ∗ 8 символьных периодов

= 156 символьных периодов

DataSize = 133 ∗ 8 = 1064 бит

InitialBackoffworst

= (23 − 1) ∗ aUnitInitialBackoffPeriod + CW ∗ aCcaTime

+ (24 − 1) ∗ aUnitInitialBackoffPeriod + CW ∗ aCcaTime

+ (25 − 1) ∗ aUnitInitialBackoffPeriod + CW ∗ aCcaTime

+ (26 − 1) ∗ aUnitInitialBackoffPeriod + CW ∗ aCcaTime

= aUnitInitialBackoffPeriod ∗ (7 + 15 + 31 + 63) + 4 ∗ CW

∗ aCcaTime = 116 ∗ 20 + 4 ∗ 2 ∗ 8 = 2384 символьных периода

Время передачи для одного пакета и требуемы BI приведены в таблицах 11 и 12 соответственно.

Таблица 11 – Время передачи одного пакета в сети со слотами

	O-QPSK	BPSK	
	2,4 ГГц	868 МГц	915 МГц	868 МГц
InitialBackoff best	2,496 мс	6,24 мс	3,9 мс	7,8 мс
InitialBackoff worst	38,144 мс	95,36 мс	59,6 мс	119,2 мс
TransmissionTime	4,256 мс	10,64 мс	26,6 мс	53,2 мс
Rx-Tx	195 мкс	480 мкс	300 мкс	600 мкс
Ack	352 мкс	880 мкс	2,2 мс	4,4 мс

Total best 7,296 мс 18,24 мс 33 мс 66 мс

Total worst 44,544 мс 107,36 мс 88,7 мс 177,4 мс

Исходя из предположений о количестве PAN и количестве узлов в каждой PAN оценим требуемую продолжительность BI для сети с модуляцией O-QPSK с частотным диапазоном 2,4 ГГц и сети с модуляцией BPSK и частотным диапазоном 868 МГц:

$$BImin = \sum_{i=1}^{NPAN} Nузлові$$

60

Таблица 12 – Требуемый BI для сети со слотами

	O-QPSK (2,4 ГГц)		BPSK (868 МГц)	
N	best	worst	best	worst
10	437,76 мс	2,67264 с	3,96 с	10,644 с
15	656,64 мс	4,00896 с	5,94 с	15,966 с
20	875,52 мс	5,34528 с	7,92 с	21,288 с

Полученные значения определяют минимальный требуемый интервал между маячками координатора. При этом каждый узел в сети успешно передаст как минимум один пакет. Стоит отметить, что рассмотренный случай – наихудший из всех возможных, поскольку предусматривает полное пересечение всех POS. На практике PAN, отстоящие друг от друга на расстояние 110, превышающее POS, могут использовать для передачи пакетов один и тот же момент 110 времени. Управление разделением времени осуществляется координатором на основании данных о пространственном расположении устройств.

Как уже было отмечено ранее 110, в модели учитывается задержка передачи пакета между узлами: пакет передается следующему узлу мгновенно, но по истечении таймера на время передачи, вычисленное для разных характеристик сети выше. Для обеспечения полной адекватности модели следует выбирать период генерации пакетов и период сбора статистики большие, чем максимальное время передачи в пределах хопа. В этом случае все созданные в течение периода пакеты либо будут переданы, либо не будут переданы вообще. Также рекомендуется соблюдать соотношение:

$$\frac{1}{vобщ} > Tmin,$$

где Tmin – минимально необходимое время для гарантированной передачи пакета. Тогда гарантируется, что новый пакет не появится до того, как будет передан предыдущий пакет, созданный любым другим узлом в сети. Тем не менее, это ограничение является слишком жестким и должно быть использовано только в 110

61

том случае, если 110 POS всех узлов полностью пересекаются и при передаче информационного сигнала его получение осуществляется всеми узлами. Кроме того, по соображениям энергоэффективности в беспроводных сенсорных сетях ZigBee пакеты практически никогда не создаются чаще, чем раз в несколько секунд.

В рамках модели исследуются вопросы нарушения целостности маршрутизации и доступности [30]. Функционал автоматического перестроения сети не реализуется, поскольку не позволяет в общем случае судить о наличии или отсутствии вредоносного воздействия на сеть: свидетельством, допустим, атаки «воронка» является изменение частоты отправления кадров к определенному узлу относительно частоты в нормальном режиме работы, а не предшествующая операция перестроения. Кроме того, в некоторых случаях способом проведения той же атаки может стать намеренный вывод из строя части

маршрутизаторов. При этом перестроение сети может и не происходить, поскольку узлам достаточно обновить связанные с маршрутизацией таблицы.

В модели используются три вероятностных распределения:

1. Промежутки времени между последовательными созданиями пакетов распределены нормально с параметрами, определяемыми пользователем;
2. Количество кадров канального уровня в каждом пакете сетевого уровня – подчиняется геометрическому распределению;
3. Адреса пункта назначения и целевой PAN ID выбираются случайно из равномерного распределения.

Были реализованы две топологии сети – «ячеистая сеть» и «кластерное дерево», поскольку остальные топологии явно сводятся к этим двум наиболее общим топологиям сети [182]. Для этих топологий реализованы разные объекты взаимодействия и способы адресации. Кроме того, для каждой топологии были реализованы атакующие узлы.

В рамках модели с топологией «ячеистая сеть» реализованы два типа объектов:

1. Узел сети – представляет собой маршрутизатор, к которому присоединены несколько конечных устройств. Передача к конечным устройствам осуществляется в канале, отличном от используемого для маршрутизации между координаторами. Явно предполагается, что конечные устройства подключены к координаторам своих PAN по схеме «звезда».
2. Коллектор – узел-сборщик статистики, который раз в T секунд записывает в файл накопленную информацию о сетевых пересылках.

Для этой модели реализован алгоритм поиска маршрута AODV (Ad-hoc On-demand Distance Vector algorithm). При создании нового пакета узел проверяет таблицу маршрутизации на наличие записи о следующем узле в маршруте для заданного адреса назначения. Если такой записи нет, осуществляется широковещательный запрос, который повторяется каждым получившим его узлом до тех пор, пока не достигнет узла с заданным адресом. Этот узел на основании информации из широковещательного пакета (она обновляется каждым узлом) отправляет пакет обратно узлу-источнику запроса. Затем может осуществляться пересылка сообщения, поскольку информация о маршруте содержится во всех узлах, входящих в этот маршрут [81].

Скриншот сети из 15 узлов с ячеистой топологией приведен на рисунке 2.5.

Рисунок 2.5 – Ячеистая топология сети

В модели с топологией «кластерное дерево» используется упрощенная схема маршрутизации. Каждому узлу координатор выделяет домен адресов, который узел может на свое усмотрение делить между подключенными к нему устройствами – и так далее. Реализованы объекты трех типов:

1. Узел сети – аналогично узлу из ячеистой топологии;
2. Коллектор – аналогично узлу из ячеистой топологии;
3. Адресатор – узел, выполняющий вспомогательные функции адресации.

Для подсчета границ домена адресов используются следующие соотношения (собственный адрес – удаляется из выделенного домена, общее количество адресов – задается пользователем):

Для потомка i (i ∈ [0; NumChildren]):

$$First = FirstChildAddress + i * \left[\frac{1 + LastChildAddress - FirstChildAddress}{NumChildren} \right],$$

$$Last = FirstChildAddress + (i + 1) * \left[\right.$$

1 + LastChildAddress − FirstChildAddress

NumChildren

] − 1,

где:

NumChildren – число потомков узла;

FirstChildAddress – первый адрес из домена (по умолчанию на 1 больше собственного адреса координатора PAN);

LastChildAddress – последний адрес из домена;

First – первый адрес домена, выделяемого i-му потомку;

Last – последний адрес домена, выделяемого i-му потомку.

Например, если главному координатору был выделен домен из 50 адресов (0 – 49), то он сам получает адрес 0, а оставшиеся адреса делятся поровну между потомками (для упрощения кластерное дерево считается сбалансированным).

Пусть имеется 3 потомка:

FirstChildAddress ≔ 1

LastChildAddress ≔ 49

64

i = 0 ⇒ First = 1; Last = 1 + 1 ∗ [

1 + 49 − 1

3

] − 1 = 16;

i = 1 ⇒ First = 1 + 1 ∗ [

1 + 49 − 1

3

] = 17; Last = 1 + 2 ∗ [

1 + 49 − 1

3

] − 1 = 32;

i = 2 ⇒ First = 1 + 2 ∗ [

1 + 49 − 1

3

] = 33; Last = 1 + 3 ∗ [

1 + 49 − 1

3

] − 1 = 48.

Адрес «49» остается неиспользованным. В результате все потомки получают в пользование домен из 16 адресов, первый из которых они назначат себе, а остальные – разделят между своими потомками.

Адресация выполняется просто: если адрес пункта назначения в полученном или вновь созданном пакете принадлежит домену, то осуществляется передача потомку, иначе пакет передается родителю. Гарантии присутствия узла с указанным в пакете адресом назначения предоставляет Адресатор.

Пример топологии «кластерное дерево» приведен на 2.6.

Рисунок 2.6 – Кластерное дерево

Для демонстрации работы модели приведены графики простейших характеристик сети – совокупного количества пакетов и количества пакетов, связанных с маршрутизацией для обеих топологий с числом узлов, равным 15. Это значение было выбрано из соображений моделирования атак типа «воронка» и «червоточина» в кластерном дереве. Учитывая то, что большая часть пакетов проходит через корневой узел, требуется обеспечить достаточную высоту дерева.

65

Если предположить, что количество потомков в каждом узле равно 2, 15 узлов требуется для получения дерева глубины 3 (на 0 уровне – 1 узел, на 1 уровне – 2 узла, на 2 уровне – 4 узла, на 3 уровне – 8 узлов). Результаты представлены на 2.7

и 2.8.

Рисунок 2.7 – Статистика ячеистой сети

Рисунок 2.8 – Статистика сети топологии «кластерное дерево»

При эксперименте использовались следующие параметры:

1. Количество узлов – 15;

2. Для всех узлов период генерации пакетов подчиняется нормальному распределению с параметрами:

a. Математическое ожидание – 10.0;

b. Среднеквадратичное отклонение – 1.0;

3. Начало генерации пакетов для каждого узла подчиняется равномерному распределению и принимает целочисленные значения от 0 до 20.

4. Размер пакета в кадрах определяется геометрическим распределением с константой 0.8;

5. Количество конечных устройств в каждой PAN – 5;

6. Период сбора статистики – 10 секунд.

Учитывая отсутствие перестроений в сети после начала работы маршрутные сообщения пересылаются в большом количестве только в первые несколько секунд после генерации первых сообщений. Поскольку количество узлов невелико, а пакеты появляются относительно часто, в дальнейшем маршрутные сообщения в сети не наблюдаются.

Для моделирования атак, упомянутых в предыдущем разделе, используются NED-файлы – файлы описания сети, которые хранят в себе топологическую структуру сети и используется для описания логической структуры сети, которая моделируется в программе. Соответственно, для того, чтобы использовать разработанную модель проведения атак на БСС, необходимо модифицировать файлы omnetpp.ini [160].

Ниже приведен перечень настроек, необходимые для функционирования модели. Перечень подразделяется на общие настройки и настройки, характерные для некоторых атак. Предполагается, что аутентификация злоумышленника в сети

произошла успешно.

Общие настройки:

- **.delay – задержка перед отправкой пакета;
- **.node_name.address – адреса узлов (не должны модифицироваться);
- **.packet_generation_period – период генерации пакетов, подчиненный нормальному распределению;
- **.dev_packet_generation_period – стандартное отклонение нормального распределения;

- **.packet_size_parametr_geometric – параметр геометрического распределения, определяющий размер пакета в кадре;
- **.numRFDs – количество устройств в сети: предполагается, что каждый узел представляет собой подсеть из роутера и нескольких конечных устройств; возможно иметь до 10 конечных устройств в такой подсети;
- **.numNodes – количество узлов в сети;
- **.collector.period – период генерации пакетов.

Атака «Отказ во сне» (Denial of sleep):

- **.attack_address – адрес для проведения атаки;
- **.attack_pan – адрес сети (PAN) для проведения атаки.

Атаки «Выборочная пересылка» (Selective forward) и «повторная передача» (repeated transmission):

**.select_period – период выборки пакетов;

**.select_address – адрес выборки;

**.select_pan –выбор адреса сети (PAN) для выборки;

**.repeat_period – период повтора.

Атака «Подмена» (Spoofing)

**.spoof_period – период подмены пакетов;

**.spoof_address – адрес для атаки;

**.spoof_pan – адрес сети (PAN) для атаки.

Атака «червоточина» (Wormhole):

**.wormhole_period – период дупликации пакетов;

**.wormhole_node.my_num – системная переменная: 1 – для первого узла-червоточины, 2 для второго.

После настройки модели были сформированы различные выборки данных для нормального поведения и 14 атак в формате файлов .csv. Для начала, была выбрана сеть с ячеистой топологией из 15 узлов. Период создания нового пакета каждым узлом был подчинен нормальному распределению с математическим ожиданием 10 и среднеквадратичным отклонением, равным 1. При этом для выявления возможной зависимости классификации от размеров пакетов [22]

также было введено геометрическое распределение с параметром 0,8, определяющее количество кадров в каждом пакете. Был рассмотрен идеальный случай работы сети со средней задержкой в 0,007168 секунд. Каждый маршрутизатор представляет PAN из 5 узлов. Предполагается, что каждая PAN имеет топологию «звезда», и передача осуществляется в канале отличном от используемого для взаимодействия между маршрутизаторами. Выборки длиной 500 записей были получены для различных периодов сбора статистики: 5 с, 10 с, 20 с, 50 с, 100 с, 10 мин., 1 час. Также количество записей в выборках варьировалось для : 500, 1000 и 2500 записей для каждого состояния сети. Пример выборки представлен на рисунке 2.9.

Рисунок 2.9 – Пример сгенерированной выборки

При обработке статистических данных вручную были получены процентные соотношения средних отклонений каждого признака при атаке от соответствующего признака при нормальном поведении. В таблице 13

представлены такие данные для атаки типа «отказ во сне». В приложении Б представлена расширенная таблица для всех типов поведения.

Таблица 13 – Средние отклонения признаков при атаке «отказ во сне»

Признак	min	max
num_frames	97,04%	97,11%
num_frames_avg	97,04%	97,11%
num_packets	97,05%	97,34%
num_packets_avg	97,04%	97,37%
num_packets_out_avg	103,21%	104,31%
num_packets_out_max	93,23%	94,23%
num_packets_out_min	99,76%	100,00%
num_packets_in_avg	98,08%	98,56%
num_packets_in_max	92,24%	95,54%
num_packets_in_min	82,76%	91,31%
weighted_num_packets_in_avg	97,19%	102,33%
weighted_num_packets_in_max	90,92%	100,66%
weighted_num_packets_in_min	94,02%	107,28%
frac_packets_in_out_avg	69,57%	81,58%
frac_packets_in_out_max	100,00%	100,00%
frac_packets_in_out_min	100,00%	100,00%
frac_packets_in_out_pan_avg	40,53%	100,00%
frac_packets_in_out_pan_max	100,00%	100,00%
frac_packets_in_out_pan_min	100,00%	100,02%
num_packets_equal_src_avg	104,76%	106,35%
num_packets_equal_src_max	418,48%	497,33%
num_packets_equal_src_min	86,84%	100,00%
num_packets_equal_src_pan_avg	99,99%	100,00%
num_packets_equal_src_pan_max	99,74%	100,01%
num_packets_equal_src_pan_min	99,73%	100,00%
num_packets_equal_dest_avg	100,00%	100,00%
num_packets_equal_dest_max	490,43%	552,63%
num_packets_equal_dest_min	86,49%	92,35%
num_packets_equal_dest_pan_avg	99,99%	100,00%
num_packets_equal_dest_pan_max	173,79%	177,78%
num_packets_equal_dest_pan_min	92,70%	93,65%
num_frames_out_avg	103,69%	103,86%
num_frames_out_max	93,60%	94,45%
num_frames_out_min	91,49%	99,41%
num_frames_in_avg	97,81%	98,07%
num_frames_in_max	92,17%	96,33%
num_frames_in_min	91,64%	96,77%
weighted_num_frames_in_avg	97,13%	101,65%
weighted_num_frames_in_max	92,10%	102,37%
weighted_num_frames_in_min	94,09%	101,34%
num_route_msgs	100,00%	101,59%
num_forwarded_packets	98,87%	100,10%
num_forwarded_packets_avg	98,82%	100,00%
num_forwarded_packets_max	91,41%	92,71%
num_forwarded_packets_min	98,80%	106,82%
num_packets_created_avg	100,00%	106,01%
num_packets_created_max	316,18%	497,33%
num_packets_created_min	86,84%	100,00%
frac_packets_created_acquired_avg	99,02%	100,00%
frac_packets_created_acquired_max	100,00%	100,00%

frac_packets_created_acquired_min 100,00% 100,00%

2.3 Оценка информативности признаков модели профиля поведения беспроводной сенсорной сети

Принимая во внимание объем выборок, было принято решение по возможности произвести сокращение признакового пространства [4]. Для этого необходимо оценить информативность признаков, то есть способность признака принимать разные значения для объектов разных классов и схожие значения для объектов одного класса. [11] Под классом здесь понимается конкретное поведения сети: нормальное поведение или поведение под разными видами атак.

Для оценки информативности признаков было разработано и зарегистрировано специализированное программное обеспечение (No 2018618975 от 24.07.2018). Оно может быть использовано для оценки и сокращения признакового пространства в задачах машинного обучения и анализа данных 110 [84; 87]. В программе используется подход к информативности с позиций теории информации и функционально реализованы следующие алгоритмы:

1. Подсчет информативности методом Шеннона для N классов;
2. Подсчет информативности методами Шеннона, Кульбака и накопленных частот для любых двух классов из представленного множества мощностью N;
3. Удаление из выборки неинформативных признаков;
4. Сортировка подсчитанных значений информативности;
5. Выбор наиболее информативных признаков для K из N классов.

Метод Кульбака заключается в оценке меры расхождения между классами (дивергенции). Преимуществом метода является независимость от объема выборок, а недостатком – невозможность оценки информативности при делении на более, чем два класса. Формула метода Кульбака представлена ниже:

I(x) = ∑ [Pi1 − Pi2] ∗ log2

Pi1

Pi2

G

i=1,

Pik =

mik

∑ mik

G

i=1

, k = 1; 2,

где:

G – количество градация признака x;

mi,k – количество объектов класса k, у которых признак принимает значение градации i;

Pi,k – доля объектов класса k среди всех объектов, у которых признак принимает значение градации i.

Метод Шеннона оценивает информативность с точки зрения теории информации – как средневзвешенное количество информации (меры снижения неопределенности знания), приходящееся на разные градации некоторого

признака [11; 17; 25]. При этом информативность признака оценивается следующим образом:

I(x) = 1 + ∑(Pi ∗ ∑Pi,k ∗ logK Pi,k

K

k=1

)

G

i=1

,

где:

G – количество градация признака x;

K – количество классов;

N – количество объектов всех классов;

mi,k – количество объектов класса k, у которых признак принимает значение градации i;

Pi – частота появления градации i среди всех объектов выборки;

Pi,k – доля объектов класса k среди всех объектов, у которых признак принимает значение градации i.

Среди существенных преимуществ метода Шеннона выделяют следующие:

1. Возможность оценки информативности для нескольких классов.

2. Абсолютное значение величины информативности: от 0 до 1.

3. Объемы выборок по разным классам могут быть различны.

Метод накопленных частот применяется для случаев классификации на два класса. При этом требованием являются одинаковые объемы выборок для двух классов. Метод заключается в построении эмпирических распределений для объектов обоих классов в одинаковых координатных осях. Затем для каждого интервала на координатной оси подсчитывается накопленная частота – сумма всех частот от первого до текущего интервала. Здесь явно прослеживается аналогия с нахождением функции вероятностного распределения [5] путем интегрирования плотности распределения. Оценкой информативности является максимальная разность частот для двух классов (среди всех интервалов).

В таблице 14 приведены способы перевода критериев информативности в интуитивно понятную шкалу для разных методов подсчета информативности.

Таблица 14 – Перевод значений информативности в шкалу рангов

Шкала рангов	Метод Шеннона	Метод Кульбака	Метод накопленных частот
очень высокий (ОВ)	(0,8; 1,0]	(xmin + 4 ∗ xmax − xmin 5 ; xmax)	
высокий (В)	(0,6; 0,8]	(xmin + 3 ∗ xmax − xmin 5 ; xmin + 4 ∗ xmax − xmin 5)	
средний (СР)	(0,4; 0,6]	(xmin + 2 ∗ xmax − xmin 5 ; xmin + 3 ∗ xmax − xmin 5)	
ниже среднего (НС)	(0,2; 0,4]	(xmin + xmax − xmin 5 ; xmin + 2 ∗ xmax − xmin 5)	
низкий (Н)	(0; 0,2]	(xmin;xmin +	

xmax − xmin

5

)

Основное назначение этой шкалы – обоснование для установления границ при отсечении неинформативных признаков и выборе наиболее информативных признаков.

Соответственно, было принято решение оценить информативность признаков в зависимости от параметров модели.

Было решено выявить зависимости между средним периодом создания нового пакета и периодом сбора статистики. Для этого была создана модель сети с ячеистой топологией из 15 узлов. Период создания нового пакета каждым узлом был подчинен нормальному распределению с математическим ожиданием 10 и среднеквадратичным отклонением, равным 1. При этом для выявления возможной зависимости классификации от размеров пакетов также было введено геометрическое распределение с параметром 0.8, определяющее количество кадров в каждом пакете. Рассматривался случай работы сети со средней задержкой в 0.007168 секунд.

В течение эксперимента были получены выборки длины 500 записей для следующих периодов сбора статистической информации (T=10 секунд – средний период генерации нового пакета в сети):

1. 5 секунд (0.5*T);
2. 10 секунд (1*T);
3. 20 секунд (2*T);
4. 50 секунд (5*T);

5. 100 секунд (10*T);
6. 10 минут (60*T);
7. 1 час (360*T).

Результаты эксперимента представлены в таблице 15. Для каждого из периодов сбора указан наиболее информативный признак и его информативность. На рисунке 2.10 приведен график информативности для периода 360T.

Таблица 15 – Максимальная информативность при разных периодах сбора статистики

Период	Признак	Информативность (по методу Шеннона)
0.5*T	num_packets_equal_src_pan_max	0.0743
1*T	num_forwarded_packets	0.0983
2*T	num_forwarded_packets_max	0.1330
5*T	num_forwarded_packets_max	0.1933
10*T	num_packets_equal_src_pan_min	0.2365
60*T	num_packets_out_avg	0.3594
360*T	num_packets_out_avg	0.4421

При анализе полученных данных сделаны следующие выводы:

1. Информативность признаков существенным образом зависит от периода сбора статистики: чем больше период, тем больше значение информативности;
2. Признаки, информативные при небольших периодах сбора статистической информации могут оказаться неинформативными при больших периодах и наоборот.

Стоит отметить, что при использовании признаков в качестве основы для создания СОВ допустимо реализовывать обнаружение аномального поведения для нескольких периодов сбора статистики [63; 65]. Так, например, если средний период генерации пакета в системе составляет 10 секунд, то можно собирать статистику с периодами 10 секунд, 2 минуты, 10 минут, 30 минут и 1 час. Для каждого периода дается своя оценка поведения системы [218], причем чем больше период, тем больше доверия к возвращаемой СОВ информации о состоянии сети.

Рисунок 2.10 – Информативность признаков при периоде сбора статистики 3600 с

Фактически оценка информативности с помощью метода Шеннона

применяется для оценки способности признака разделять выборку на классы.

0 0,05 0,1 0,15 0,2 0,25 0,3 0,35 0,4 0,45 0,5

num_frames

num_frames_avg

num_packets

num_packets_avg

num_packets_out_avg

num_packets_out_max

num_packets_out_min

num_packets_in_avg

num_packets_in_max

num_packets_in_min

weighted_num_packets_in_avg

weighted_num_packets_in_max

weighted_num_packets_in_min

frac_packets_in_out_avg

frac_packets_in_out_max

frac_packets_in_out_min

frac_packets_in_out_pan_avg

frac_packets_in_out_pan_max

frac_packets_in_out_pan_min

num_packets_equal_src_avg

num_packets_equal_src_max

num_packets_equal_src_min

num_packets_equal_src_pan_avg

num_packets_equal_src_pan_max

num_packets_equal_src_pan_min

num_packets_equal_dest_avg

num_packets_equal_dest_max

num_packets_equal_dest_min

num_packets_equal_dest_pan_avg

num_packets_equal_dest_pan_max

num_packets_equal_dest_pan_min

num_frames_out_avg

num_frames_out_max

num_frames_out_min

num_frames_in_avg

num_frames_in_max

num_frames_in_min

weighted_num_frames_in_avg

weighted_num_frames_in_max

weighted_num_frames_in_min

num_route_msgs

num_forwarded_packets

num_forwarded_packets_avg

num_forwarded_packets_max

num_forwarded_packets_min

num_packets_created_avg

num_packets_created_max

num_packets_created_min

frac_packets_created_acquired_avg

frac_packets_created_acquired_max

frac_packets_created_acquired_min

360T

75

Поэтому, если в выборке присутствует класс, который не может быть по тем или иным причинам 110 выделен с помощью никакого из признаков, общее значение информативности будет «проседать» для всех признаков. Поэтому необходимо дополнительно произвести оценку способности каждого признака делить выборку всего на два класса: нормальное поведение сети и поведение под атакой. Для этого был произведен еще один эксперимент: для каждой пары выборок «нормальное поведение/атака» были посчитаны значения информативности каждого признака для трех периодов – 10T, 60T и 360T. Результаты для класса атаки типа «отказ во сне» представлены в таблицах 16-18.

Таблица 16 – 5 наиболее информативных признаков по методу Шеннона

Период Признак Информативность

10T num_packets_equal_dest_max 0.993084

num_packets_equal_src_max 0.947495

num_packets_equal_dest_pan_max 0.326937

num_packets_out_avg 0.063563

num_frames_out_avg 0.056685

60T num_packets_equal_src_max 1

num_packets_equal_dest_max 1

num_packets_equal_dest_pan_max 1

num_packets_created_max 1

num_packets_out_avg 0.449877

360T num_packets_equal_src_avg 1

num_packets_equal_src_max 1

num_packets_equal_dest_max 1

num_packets_equal_dest_pan_max 1

num_packets_created_max 1

Таблица 17 – 5 наиболее информативных признаков по методу Кульбака

Период Признак Информативность

10T num_packets_equal_dest_max 9.465693477

num_packets_equal_src_max 6.099388733

num_packets_equal_dest_pan_max 2.490051765

num_packets_out_avg 0.547426314

76

num_frames_out_avg 0.452548685

60T num_frames_out_avg 3.578476423

frac_packets_in_out_avg 2.987830226

frac_packets_in_out_pan_avg 2.596515492

num_forwarded_packets_max 2.100943134

num_packets_out_max 1.919809395

360T num_frames_avg 8.393924912

num_packets_equal_dest_pan_min 5.926747972

num_frames_in_avg 4.500561628

frac_packets_in_out_avg 3.296978144

weighted_num_packets_in_max 2.116442256

Таблица 18 – 5 наиболее информативных признаков по методу накопленных частот

Период Признак Информативность

10T num_packets_equal_dest_max 799

num_packets_equal_src_max 789

num_packets_equal_dest_pan_max 505

num_frames_out_avg 214

frac_packets_in_out_avg 167

60T num_packets_equal_src_max 250

num_packets_equal_dest_max 250

num_packets_equal_dest_pan_max 250

num_packets_created_max 249

num_packets_out_avg 162

360T num_packets_equal_src_avg 168

num_packets_equal_src_max 168

num_packets_equal_dest_max 168

num_packets_equal_dest_pan_max 168

num_packets_created_max 168

В силу большого объема полученных данных приводятся лишь основные выводы:

1. Для большинства типов атак (за исключением вариаций «повторной передачи» и «выборочной пересылки») существуют признаки, позволяющие однозначно отличить поведение сети под атакой от нормального поведения (но при этом не гарантируется идентификация конкретного типа атаки);
2. Чем больше период сбора статистики, тем больше в общем случае максимально информативных признаков;
3. Методы Шеннона и накопленных частот чаще всего возвращают одни и те же результаты, а результаты метода Кульбака часто отличаются.

Низкая информативность признаков в случае атак типов «повторная передача» и «выборочная пересылка» может быть объяснена двумя факторами:

1. Для признаков-соотношений используется предположение: если один из элементов соотношения равен 0, то все соотношение приравнивается к 0. В результате, например, для «выборочной пересылки» может возникнуть ситуация, при которой атакующий отбросил все пакеты, отправленные некоторым узлом. Тогда количество полученных узлом назначения пакетов от этого узла будет равно нулю. Соотношение между количеством отправленных узлом пакетов и количеством полученных от узла пакетов будет приравнено нулю, что не будет отличаться от ситуации, когда пакеты вообще не передавались. Решение проблемы – использование машинной константы INT_MAX в случае, если знаменатель соотношения принимает в качестве значения нуль;
2. Чтобы «выборочная пересылка» и «повторная передача» реализовались, необходимо, чтобы через атакующий узел проходили пакеты от атакуемого узла. В эксперименте исследовались три случая для каждого типа атаки – отбрасывались или повторно отправлялись либо все пакеты, либо пакеты от определенного источника, либо пакеты для определенного узла. Если первый случай отслеживается даже в случае периода 60T, то второй и третий – практически не отслеживаются. Причина в том, что адрес назначения выбирается случайно (из равномерного распределения). Поэтому через атакующий узел пакеты, которые могли бы быть отправлены повторно или отброшены, вообще не проходят. А случай, когда пакеты проходят через атакующий узел, встречается

настолько редко, что изменение значений признаков-отношений мало отличается от изменения в случае, когда передача до узла назначения не успевает завершиться на момент сбора статистики. Предполагаемое решение проблемы может заключаться в исследовании адаптированной к атаке топологии сети, когда через атакующий узел проходит большая часть пакетов от атакуемого узла. Такой случай чаще всего встречается на практике.

Большую часть приведенных признаков возможно собирать для каждой PAN в отдельности, а окончательные значения вычислять, исходя из полученных значений для подсетей. В этом случае для передачи многих признаков может хватить всего 8 байт (размерность integer на современных вычислительных

машинах).

Следующий эксперимент, проведенный в рамках исследования – оценка зависимости информативности признаков от размеров выборки. Например, методы Шеннона и Кульбака оперируют частотами, которые могут измениться при увеличении мощности множества объектов. Закономерным следствием является проверка наличия зависимости и ее формализация.

В целях получения ответа на поставленный вопрос было получено три выборки различной мощности для периода 2T: 500, 1000 и 2500 (для нормального режима работы сети и каждого типа атаки). Затем была получена оценка информативности методом Шеннона. Результаты представлены в таблице 19.

Таблица 19 – Наиболее информативные признаки при разных объемах выборки

Длина выборки (для каждой атаки)	Признак	Информативность
500	num_forwarded_packets_max	0.1361
	num_packets_out_max	0.1217
	num_forwarded_packets	0.1163
	num_packets_equal_src_pan_max	0.1066
	num_frames_out_max	0.1015
1000	num_forwarded_packets_max	0.1330
	num_packets_out_max	0.1202
	num_forwarded_packets	0.1136
	num_packets_equal_src_pan_max	0.1070

	num_frames_out_max	0.1005
2500	num_forwarded_packets_max	0.1330
	num_packets_out_max	0.1202
	num_forwarded_packets	0.1136
	num_packets_equal_src_pan_max	0.1070
	num_frames_out_max	0.1005

Следовательно, при больших значениях мощности выборки информативность практически не повышается при увеличении количества объектов. Поэтому оптимальное количество обучающих объектов либо подбирается опытным путем, либо диктуется используемым методом машинного обучения. Так, например, при обучении методом стохастического градиента намеренно используется лишь часть обучающей выборки – количество объектов, достаточное для достижения состояния алгоритма, при котором дальнейшие градиентные шаги не приводят к значительному повышению точности классификации.

Хотя до использования конкретных методов машинного обучения трудно сказать, насколько эти признаки способны идентифицировать конкретный тип атаки, можно предположить, что в данном случае классификация высокой точности может быть достигнута с использованием композиций алгоритмов (бустинга), в частности, логических классификаторов, хорошо работающих лишь на части выборки.

Еще одной переменной, связанной с информативностью, является параметр дискретизации. Известно, что методы оценки информативности оперируют признаками с конечными дискретными множествами значений. Для того, чтобы осуществить перевод значений признака в дискретную шкалу из конечного числа значений осуществлялись следующие действия:

1. Поиск максимального и минимального элементов;
2. Вычисление шага дискретизации как частного от разности максимального и минимального элементов и параметра дискретизации.

В данной диссертационной работе используется параметр дискретизации равный 10. Стоит отметить, что в некоторых случаях величина параметра может

иметь существенное значение. Например, если значения признака изменяются в пределах меньших (максимальный и минимальный элементы – выбросы), чем выбранный шаг дискретизации, то даже если каждому классу соответствует собственное множество значений признака, не пересекающееся с множествами значений признака других классов, подсчитанная информативность окажется нулевой: все значения признаки окажутся приведены к одному значению. Для анализа зависимости информативности от параметра дискретизации [23] была произведена оценка всех признаков, кроме тех, которые попадают в ранг информативности «низкий» для двух топологий при периоде сбора статистики 360*T. Результаты представлены на рисунке 2.11. Сделаны следующие общие выводы:

1. Чем больше параметр дискретизации, тем больше значения информативности признаков;
2. Чем больше параметр дискретизации, тем больше признаков относятся к более высоким рангам информативности.

На основании оценок, полученных методом Шеннона, можно произвести сокращение признакового пространства. Было принято решение исключить из выборки следующие признаки:

1. Для всех сетей:
1. num_packets_out_min;
2. num_packets_in_min;
3. weighted_num_packets_in_avg;
4. frac_packets_in_out_min;
5. frac_packets_in_out_pan_min;
6. frac_packets_in_out_pan_max;
7. num_packets_equal_dest_min;
8. num_frames_out_min;
9. num_frames_in_min;

10. weighted_num_frames_in_avg;
11. num_route_msgs;
12. num_packets_created_avg;
13. num_packets_created_min;
14. frac_packets_created_acquired_max;
15. weighted_num_packets_in_min;
16. weighted_num_frames_in_min;
17. frac_packets_in_out_max.

Рисунок 2.11 – Информативность и параметр дискретизации в ячеистой сети

В данной диссертационной работе среди прочих исследуются линейные методы классификации – метод опорных векторов [161], метод стохастического градиента и логистическая регрессия. Все эти методы так или иначе строят разделяющую гиперплоскость между двумя классами. При этом все эти методы

frac_packets_in_out_avg

weighted_num_packets_in_max

num_packets_equal_dest_avg

weighted_num_frames_in_max

num_packets_equal_src_min

Ячеистая сеть. Информативность и параметр дискретизации

Discr=10 Discr=100

крайне чувствительны к наличию линейной зависимости между признаками. Существует множество способов, позволяющих с определенной долей точности судить о наличии корреляционной зависимости между признаками. Формально используемый далее метод является не совсем корректным с точки зрения математической статистики. Дело в том, что понятия «линейная независимость» и «некоррелированность» не являются взаимозаменяемыми: из первого следует второе, но из второго не следует первое. В данном случае этот принцип нарушается, что, однако, не оказывает значительного негативного влияния на классификацию [54].

В работе используется коэффициент корреляции Пирсона [17; 25]. Эта величина позволяет судить (с определенной долей точности) о силе линейной зависимости между признаками. Рассмотрим две выборки X = (x1,..., xm) и Y = (y1,..., ym). Для них коэффициент корреляции Пирсона может быть рассчитан по формуле (где x и y – средние значения):

rxy =

∑ m (xi − x)(yi − y)

i=1

√∑ m (xi − x)2

i=1 + ∑ m (yi − y)2

i=1

При равенстве или близости коэффициента корреляции Пирсона к единице говорят о линейной зависимости признаков, а к нулю – о их линейной независимости. Сокращение на основе отсечения линейно зависимых признаков, теоретически, не должно оказывать негативное влияние на точность классификации, поскольку линейно зависимые признаки вносят в итоговый результат один и тот же вклад.

Осуществим сокращение пространства признаков. Для этого из двух линейно зависимых признаков оставим тот, который проще интерпретируется или который проще получить в процессе сбора статистики. Так, например, среди признаков num_frames, num_packets, num_frames_avg и num_packets_avg, для которых наблюдается сильная корреляционная зависимость, оставлен лишь последний, поскольку:

1. Сбор признаков на сетевом уровне проще, чем на канальном (а количество кадров изначально вводилось лишь для того, чтобы избежать использования параметра «размер пакета»).
2. Усредненная по числу узлов характеристика снижает зависимость от количества узлов, что в перспективе может привести к упрощению построения более сложных систем обнаружения аномального поведения [66].

Из 34 признаков были отобраны 11 наиболее подходящих, которые составили набор признаков «независимые»:

1. num_packets_avg,
2. num_packets_out_max,
3. frac_packets_in_out_avg,
4. frac_packets_in_out_pan_avg,
5. num_packets_equal_src_min,
6. num_packets_equal_src_pan_max,

7. num_packets_equal_src_pan_min,

8. num_packets_equal_dest_pan_min,

9. weighted_num_frames_in_min,

10. frac_packets_created_acquired_avg,

11. frac_packets_created_acquired_min.

Соответственно, можно говорить о сокращении признакового пространства для формирования модели профиля поведения БСС для идентификации атак сетевого уровня с 51 признака до 11 признаков.

2.4 Метод идентификации атак на основе алгоритма «случайного леса»

В рамках диссертационной работы было принято решение изучить различные классификаторы [15], поскольку существующие исследования разнятся в выбранных алгоритмах и методах [173]. В качестве инструментария был выбран язык Python и библиотека Scikit-learn [36; 169].

Еще один набор признаков был получен уже в процессе применения методов машинного обучения. Реализованные в ней классификаторы после

обучения способны оценить степень влияния каждого из признаков на окончательный результат. Приведенный ниже набор был получен с помощью такой оценки классификатора «случайный лес» и включает лишь пять признаков:

1. num_packets_avg,

2. num_packets_out_max,

3. num_packets_equal_src_pan_max,

4. num_packets_equal_src_pan_min,

5. frac_packets_created_acquired_avg.

Следовательно, модель профиля поведения сети может быть представлена вышеуказанными пятью признаками.

Необходимо отметить, что данные признаки в своем большинстве актуальны только для БСС и спецификации ZigBee и прямых аналогов в беспроводных локальных сетях (БЛС) и беспроводных персональных сетях (БПС) не имеют. Описание используемых признаков и возможность использования в БЛС и БПС [55] представлены в таблице 20.

Таблица 20 – Возможность использования выбранных признаков в различных сетях

Признак	Описание	Аналоги в БЛС	Аналоги в БПС
num_ packets_avg	Общее количество пакетов, переданных в сети по спецификации ZigBee, усредненное по числу PAN в сети.	Прямых аналогов нет ввиду отсутствия понятия PAN (англ. Personal Area Network — персональная сеть, здесь фигурирует как часть спецификации ZigBee) в БЛС. Возможно усреднение общего количества переданных в сети пакетов по количеству отдельных точек доступа, только когда их несколько.	В общем случае нет.

Только при
использовании
спецификации ZigBee.
num_packet_
out_max
Максимальное
количество пакетов,
отправленных каким-
либо узлом
(собственных и
пересланных).
Максимальное количество
пакетов, отправленных
каким-либо из
подключенных к сети
устройств.
Максимальное
количество пакетов,
отправленных каким-
либо из подключенных к
сети устройств или
узлов.
num_packets_ Максимальное Прямых аналогов нет. В общем случае нет.

85
equal_src_
pan_max
количество
полученных каким-
либо узлом пакетов,
в которых в качестве
PAN-отправителя
указана одна и та же
PAN.
Измерение количества
пакетов, получаемых
устройствами от устройств,
подключенных к другим
точкам доступам,
нецелесообразно и является
некорректным
переложением принципов
устройства сетей БСС на
БЛС.
Только при
использовании
спецификации ZigBee.
num_packets_
equal_src_
pan_min
Минимальное
количество
полученных каким-
либо узлом пакетов,
в которых в качестве
PAN-отправителя

	указан один и тот же PAN.	
	Прямых аналогов нет.	
	Измерение количества пакетов, получаемых устройствами от устройств, подключенных к другим точкам доступам, нецелесообразно и является некорректным переложением принципов устройства сетей БСС на БЛС.	
	В общем случае нет.	
	Только при использовании спецификации ZigBee.	
frac_packets_ created_ acquired_avg	Соотношение между количеством пакетов, созданных узлом, и количеством полученных пакетов, в которых в качестве источника указан данный узел, усредненное по сети.	Признак возможно реализовать в БЛС только при организации системы опроса устройства о количестве созданных им пакетов, однако это некорректное переложение принципов работы БСС на БЛС. В случае корректной работы точки доступа данный признак бесполезен.
	В общем случае признак возможно реализовать в БПС только при организации системы опроса устройства или узла о количестве созданных им пакетов, однако не всегда данная интерпретация будет корректной с точки зрения принципов работы сети.	

В работе используются классификаторы, которые условно могут быть разделены на две группы [110] : многоклассовые классификаторы и линейные классификаторы [183]. Первые – обеспечивают классификацию непосредственно

на несколько классов, вторые – на лишь два класса. В работе используется схема обобщения на многоклассовую классификацию One-vs-Rest. Она предполагает решение задач классификации по отделению каждого класса от всех остальных. Ответом считается тот класс, для которого уверенность классификации

86

оказывается максимальной [110; 149]. Кратко опишем используемые методы классификации [86; 92; 114].

Решающее дерево [146]. Этот метод классификации считается одним из наиболее простых во всем машинном обучении и относится к группе логических классификаторов. Работа метода сводится к построению бинарного дерева, во внутренних узлах которого располагаются предикаты, а в листах – либо метки классов, либо статистическое соотношение для объектов, когда-либо попадавших в этот лист. Выбор предикатов осуществляется с помощью критериев информативности, которых существует множество [94]. В работе был использован критерий Джини, оценивающий способность предиката передавать объекты одного класса в одну и ту же ветвь. Классификация осуществляется двумя способами: либо для объекта доступен путь через предикаты, который приводит в лист с однозначной меткой класса, либо вычисляется вероятность отнесения объекта к каждому из классов, а в качестве ответа указывается наиболее вероятный класс.

Градиентный бустинг является один из способов построения композиции классификаторов. Такие методы стремятся итеративно, с помощью последовательного добавления новых классификаторов, компенсировать ошибки ранее работавших классификаторов. Суть обучения сводится к следующему процессу. Сначала выбранный алгоритм обучается на обучающей выборке. Затем производится оценка эффективности классификации. Веса тех объектов, на которых алгоритм чаще ошибается – увеличиваются, а тех, на которых классификация уверенная – уменьшаются. Затем на тех же данных, но с учетом изменившихся весов обучается следующий алгоритм классификации – и так далее, до тех пор, пока общее качество классификации не перестанет существенно изменяться от итерации к итерации. В работе использован как полноценный градиентный бустинг, так и его частный случай AdaBoost.

«Случайный лес» – это усовершенствованный вариант градиентного бустинга, в котором в качестве базовых алгоритмов используются решающие деревья, а также введены два важных вероятностных правила [48; 202]:

87

1. Каждый классификатор обучается на случайном подмножестве признаков.
2. Каждый классификатор обучается на случайном подмножестве объектов.

Для разработки метода идентификации [211] в качестве основы использовался алгоритм «случайный лес», представляющий собой коллекцию случайных деревьев, показавший наиболее высокий показатель точности (precision), аккуратности (accuracy) и полноты (recall), что не противоречит существующим исследованиям в этой области:

$$F = \{h(X, \Psi s), s = 1, \dots\},$$

где $h(X, \Psi s)$ – решающее дерево, $\{\Psi s\}$ – независимые одинаково распределенные случайные векторы, X – выборка признаков x, подающаяся на вход.

Рисунок 2.12 – Точность классификации различных алгоритмов

Кроме описанных выше исследовались следующие алгоритмы:

1. Логистическая регрессия [194].
2. Метод опорных векторов.
3. Метод ближайшего соседа.
4. Метод k-ближайших соседей.

60

70

80

90

100

Точность различных алгоритмов на профилях поведения

различной размерности

total informative uncorrelated minimum

88

5. Метод парзеновского окна.

На рисунке 17 показана точность при многоклассовой классификации для четырех наборов признаков.

Сделаны следующие выводы:

1) точность классификации значительно не изменяется при сокращении признакового пространства, что подтверждает исключительную важность признаков, попавших в набор «minimum».

2) наиболее высокую точность продемонстрировал алгоритм «случайного леса».

2.5 Обоснование применения вероятностного классификатора и введения параметра уверенности для улучшения эффективности метода идентификации атак

Поскольку «случайный лес» показывает высокую точность только на больших периодах сбора статистики, была предпринята попытка сократить время, необходимое для идентификации при условии использования неполного набора признаков модели профиля поведения БСС.

В качестве основного вычислительного блока в алгоритме обнаружения вторжений будет использоваться вероятностный классификатор [112]. Далее последует обзор основного теоретического минимума, необходимого для его разработки.

В машинном обучении вероятностный классификатор – классификатор, способный предсказать на основе предоставленного значения распределение вероятностей множества классов, по сравнению с другими методами 110 , предсказывающими лишь наиболее вероятный класс, которому может принадлежать наблюдение.

Вероятностные классификаторы обобщают понятие классификатора как функции от значения, выводящей предполагаемый класс как результат [187]. Вместо этого, вероятностный классификатор рассчитывает условные

89

распределения, определяющие вероятность принадлежности наблюдения каждому из возможных классов:

Pr Y y i | X x, i : y Y

где X – множество наблюдений,

Y – множество возможных классов,

x – данное наблюдение,

yi – i-ый класс из множества Y.

Задача построения вероятностного классификатора, таким образом, в первую очередь состоит в составлении условных распределений вероятностей для всех наблюдений. Один из самых популярных способов основан на применении теоремы Байеса [79]:

|

|

P B A P A

P A B

PB

где A и B – некоторые события, при этом

PB 0

,

P A | B

– (условная) вероятность события A при наступлении B,

P B | A

– (условная) вероятность события B при наступлении A,

PA

и

PB

– вероятности наблюдения события A и B независимо друг

от друга, также известные как частные распределения.

В контексте классификации больших объемов данных на несколько классов

формула приобретает иную интерпретацию. Положим, что

x – единичное измерение, которое может быть случайным вектором x,

X xx 1,, n

– набор данных, полученный из n независимых одинаково

распределенных случайных величин xi,

θ – параметр распределения величины x: p(x | θ), или класс.

Тогда при предположении, что распределение x меняется в зависимости от

класса, вероятность принадлежности измерения классу вычисляется как

90

|

|

pp

p

p

X

X

X

(2.1)

где

P | X

– апостериорная вероятность принадлежности измерения классу θ

при известных данных X,

p X |

– вероятность получения данных X в классе θ,

p

– априорная вероятность класса θ,

p X

– вероятность получения данных X.

При классификации на основе теоремы Байеса [107] генерируется

достаточно большая обучающая выборка X с назначенными классами θ, на основе

которой вычисляются значения

p X |,

а также определяются априорные

вероятности классов. В результате применения (2.1) ко всей обучающей выборке

вычисляется матрица вида

11 12 1

21 22 2

12

m

m

n n nm

p p p

p p p

p p p

(2.2)

где n – количество уникальных значений в выборке,

m – количество классов.

В случае, если классификация проводится по нескольким признакам, т.е.

1

1

,,

,,

u

n

xx

x

X x x

возникают проблемы, связанные с вычислением члена

p X |,

который

может быть переписан в соответствии с правилом разложения условных

вероятностей:

p x 1,, x u | p x 1 | x 2,, x u, p x 2 | x 3,, x u, p x u |

(2.3)

Вычисление каждого члена в разложении (2.3) может быть слишком

сложным и затратным по времени и памяти. В наивном Байесовском

классификаторе для упрощения вычислений делается предположение о

независимости, а именно что каждый признак

x i

независим от любого другого

x j

, ij :

p x i | x i 1,, x u, p x i |

В этом случае

1

11

1 1

,,,

|,,,,, |

,,

n

u

u u i

u i

p x x

p x x p x x p p x

p x x

Однако, как показывает практика, зачастую в признаковом пространстве

сетевых моделей несколько признаков показывают корреляцию между собой,

поэтому Ошибка! Источник ссылки не найден. не верно в случае

классификации по взаимозависимым признакам.

Вычисление члена

p X

в (2.1) самого по себе также представляется

трудной задачей, поэтому в классификаторах, основанных на теореме Байеса,

используются нормализующие константы, вытекающие из формулы полной

вероятности:

1

|

1

m

ii

i

pp

p

X

X

1

|

m

ii

i

p p p

XX

В результате формула Ошибка! Источник ссылки не найден. приобретает вид

1

|

|

|

m

ii

i

pp

p

pp

X

X

X

В классификаторах, основанных на применении теоремы Байеса, также возникает проблема определения априорных вероятностей классов: члена

p

в (2.1) [39]. Априорная вероятность – математическое выражение знания либо предположения о том, с какой частотой встречается класс. В зависимости от ее

значений, получаемые условные (апостериорные) распределения вероятностей классов могут существенно измениться и повлиять на процесс решения, к какому классу следует отнести наблюдения. В целом существует два подхода к решению этой проблемы, основанных на интерпретации вероятности:

1. частотная вероятность;
2. байесовская вероятность.

При понимании априорный вероятностей как частотных необходимо иметь большие объемы данных, представляющих собой репрезентативную статистику, на основе которой возможно определить частоты проявления классов. Во многих случаях сбор такой статистики представляется невозможным по нескольким причинам:

недостаточная изученность области знаний;

чрезмерная сложность моделирования;

невозможность проведения эксперимента в реальном мире;

слишком большое время сбора данных;

этические ограничения.

Даже после сбора статистики в ряде случаев возникают вопросы к ее правдоподобности, отсутствии систематических отклонений и др. Тем не менее, при имеющихся данных процесс определения апостериорных вероятностей заметно упрощается, а сами результаты более объективны и обоснованы наблюдениями и экспериментами.

Байесовская вероятность представляет собой (в объективном понимании) разумное ожидание, отражающее меру знаний о событии, либо личную степень уверенности в наступлении события (в субъективном понимании). Сложность объективного определения байесовской вероятности состоит в необходимости составления процесса байесовского вывода, где первоначальные гипотезы (т.е. априорные вероятности) обновляются новыми данными [10]. Субъективное же понимание определяется лишь личными убеждениями и мнениями. Для определения субъективной вероятности используются системы экспертных оценок, основанные на выдвижении предположений группой людей. При

достаточном обосновании таких предположений экспертные оценки могут успешно применяться.

При отсутствии какого-либо источника информации об априорных вероятностях принимается неинформативное априорное распределение [190], а именно такое распределение, которое отражает размытую или общую картину о переменной [12]. Среди таких распределение самое простое и часто используемое – равновероятное:

1

pi i,

m

,

где m – количество классов.

Возможность его использования без существенного изменения значений апостериорных распределений обусловливается большей информативностью члена

p X |

в (2.1), также называемого функцией правдоподобия, по сравнению с априорным распределением.

В качестве среды разработки алгоритма вычисления вероятностей был выбран пакет прикладных программ MATLAB 2017b, обладающий собственным интерпретируемым языком программирования и предоставляющий множество доступных функций [26] в интегрированной среде.

При разработке были учтены требования к разнообразию параметров, от которых зависит вычисление распределений условных вероятностей, а также эффективность в отношении использования ресурсов памяти и времени выполнения программы. На рисунке ниже представлена блок-схема базового алгоритма программы вероятностной классификации. В блок-схему включены крупные структурные элементы программы без подробной спецификации отдельных операций.

Исходный код программы представлен в приложении В. Рассмотрим подробнее функциональность алгоритма и заложенные в него процедуры и принципы классификации. Алгоритм представлен на рисунке 2.13.

На ввод (элемент 1 блок-схемы) программой принимаются:

3. CSV-файлы данных

Каждый файл содержит данные работы модели сети в одном из 15 состояний. Главное требование к файлам – использование одного признакового пространства так, что в каждом файле содержится произвольное количество наблюдений, представляющими собой кортеж значений, соответствующий кортежу признаков:

1 11 12 1

2 21 22 2

12

’’’

’’’

’’’

u

u

n n n nu

x x x

x x x

x x x

x

x

x

4. Вектор априорных вероятностей

Должен содержать все значения априорных вероятностей, соответствующие 15 состояниям модели сети. Сумма значений не играет роли, так как вектор автоматически нормализуется в процессе работы программы так, что сумма введенных вероятностей становится равной 1.

a a 12, a,, a m

5. Подвектор признакового пространства

Содержит выбранные из признакового пространства признаки, для которых будут составляться частные распределения:

v x j, x j 1,, x l, v x x 1, x 2,, x u, v

6. Комбинации признаков из подвектора

Содержит натуральные числа, определяющие, в сочетаниях с каким количеством признаков следует составлять условные распределения вероятностей:

k k 12 k, k t, i : k i, k i l

(2.4)

где l – количество членов подвектора признакового пространства.

Перед вычислением условных вероятностей как таковых выполняется первоначальная обработка данных (элемент 2). Поскольку на выходе необходимо предоставить универсальную шкалу, предусматривающую все возможные

значения признака из наблюдаемых в любом состоянии, но также могущую предоставить информацию об отклонении значения признака от некоторой нормы, используется стандартизация, или вычисление z-оценок.

Рисунок 2.13 – Блок-схема программы вероятностного классификатора

При этом вместо индивидуальных значений медиан и стандартных отклонений применяются значения, вычисленные для нормального состояния. Это позволит сравнивать значения признака в разных состояниях и видеть, насколько сильно отклонение в различных состояниях системы.

norm

norm

xx

x

s

где x – старое (необработанное значение признака),

x – новое (обработанное) значение признака,

x norm

– медианное значение признака при нормальном функционировании,

s norm

– стандартное отклонение значений признака при нормальном

функционировании.

Начало

Импорт и проверка исходных данных

Предварительная обработка данных

Расчет апостериорных распределений

Цикл для каждого уникального значения combo

Перейти к следующему значению в цикле 4

Перейти к следующей комбинации в цикле 3

Цикл для каждой комбинации признаков combo

Вывести матрицу распределений

Останов

1

2

3

4

5

6

96

В качестве стандартного отклонения принимается квадратный корень несмещенной оценки дисперсии:

2 2

1

1

11

n

i

i

n

s x x

nn

где n – количество наблюдений в выборке,

22

1

1 n

i

i

xx

n

– выборочная дисперсия,

xi – i-ое наблюдение,

x

– медианное значение признака.

Если стандартное отклонение равно нулю, значения признака для всех 15 состояний оставляются прежними, так как их предварительная обработка в этом случае невозможна.

Кроме того, в процессе предварительной обработки после стандартизации (если она осуществлялась) берутся лишь целые части z-оценок с помощью функции floor (пол):

x max n | n x

В будущем это поможет предотвратить чрезмерную дезинтеграцию данных на отдельные значения, не позволяющие сделать общих заключений. С математической точки зрения, данная операция уплотняет шкалу значений признака посредством расширения диапазонов уникальных значений.

Изначально алгоритмом предусматривается расчет апостериорных распределений сочетаний (комбинаций) признаков из подвектора (т.е.

определенного признакового пространства классификации) по k элементов, указываемых в векторе k (2.4), для каждого k. При этом количество таких сочетаний будет равным

11

!

!!

i

tt

k

n

ii ii

n

CC

k n k

(2.5)

Значение (2.5) определяет количество итераций в цикле (элемент 3) и влияет на время выполнения алгоритма: оно растет линейно с ростом C.

97

f C O C

Однако C в общем случае зависит экспоненциально от размерности u подвектора признакового пространства, поэтому

f u O c u, c u u ;2

В лучшем случае

,

u

f u O u u O u

если для классификации используется лишь один признак, в худшем –

f u O 2u

, если используются все, так как

1

21

n

kn

n

k

CC

.

Функции правдоподобия, равные в формуле (2.1) члену

p X |

считаются в программе (элемент 5) по формуле

1

1

„ |

„ |

|

ui

ui

i

n x x

p x x

n

x

X

,

где

n x x 1,, x ui |

– количество наблюдений уникального значения, когда

система находилась в состоянии θ,

n x | i

– количество всех наблюдений, когда система была в состоянии

θ.

Центральное предположение наивного байесовского классификатора о том, что признаки независимы друг от друга [141], было отброшено как некорректно представляющее сетевую модель. Поэтому разложение (2.3) не выполнялось, а взамен него были взяты комбинации уникальных значений (элемент 4), для которых подсчитывалось число их появлений в выборке. Таким образом удалось сохранить зависимость признаков друг от друга:

1

1,,

u

ii

i

n c c u xc

x

x Λ

,

где Λ – оператор конъюнкции,

[ ] – оператор Айверсона.

Для каждой комбинации признаков из подвектора апостериорные распределения объединяются в матрицу вида (2.2), в дополнение к которой формируется матрица уникальных значений комбинации, служащая индексом к рядам матрицы (элемент 6), а также представляющая из себя стандартизированную шкалу (или их вложенное сочетание). В дальнейшем матрицы апостериорных вероятностей будут использоваться как составная часть алгоритма обнаружения вторжения в качестве классификатора [24], в то время как матрица-индекс будет использоваться как инструмент поиска необходимого распределения.

При предварительном анализе статистики были обнаружены аномальные скачки и резкие возрастная значений признаков на первых нескольких снятых наблюдениях. Это вызвано тем, что при первоначальном запуске сетевой модели не установлены данные о соседних устройствах, а сеть в целом еще не выстроена, поэтому происходит интенсивный обмен данными между сенсорными узлами для установления связи между ближайшими устройствами и организации сети. При выполнении классификации данные значения будут представлять собой единичные выбросы, которые могут не только ухудшить точность классификации, но и сместить шкалу значений признака посредством изменения медианы. На рисунках 2.14 и 2.15 представлены графики, иллюстрирующие аномальные скачки.

В результате выполнения алгоритма были получены единообразные матрицы, содержащие вероятностные распределения по 15 классам в стандартизированной относительно нормального состояния шкале. Представлены на рисунке 2.16.

Стандартизированная шкала слева от матрицы отражает отличие от медианного значения признака при нормальном функционировании модели сети в стандартных отклонениях. Пример распределения апостериорной вероятности для значений [1σ;2σ) признака num_packets_equal_src_pan_max при периоде

наблюдения 10T в топологии mesh представлен на рисунке 2.17.

99

Рисунок 2.14 – Лепестковые диаграммы первых 24 наблюдений признакового пространства сетевой модели в состоянии normal, период T, топология mesh

Рисунок 2.15 – Диаграммы изменения значений признака num_packets_avg во времени, начиная с первого наблюдения, в различных состояниях сети, период 10T, топология mesh

Из первичного анализа статистики и условных распределений вероятности можно заметить, что некоторые типы атак можно детектировать с высокой степенью уверенности, выражаемой апостериорной вероятностью появления

100

атаки, используя лишь один признак из сокращенного признакового пространства.

Рисунок 2.16 – Матрица апостериорных распределений вероятностей классов-атак в стандартной шкале признака num_packets_equal_src_pan_max, период 10T, топология mesh

Так, например, (не)осуществление атаки flood можно обнаружить со 100% точностью в ячеистой топологии, используя лишь значение признака num_packets_equal_src_pan_max, посчитанное при периоде 10T (см. рисунок 4 выше). В матрицах условных распределений для двух и более признаков количество таких значений еще больше. Ввиду этого выдвигается гипотеза о том, что некоторые наблюдения возможно классифицировать, используя подпространство признакового пространства классификации, не ухудшая при этом ее точность.

Для проверки предположения о том, что в некоторых случаях для классификации достаточно использовать несколько признаков из числа всех доступных, предлагается использовать отдельный алгоритм классификации. Два основных требования, предъявляемых к нему, – это

101

7. использование частичного признакового пространства классификации;
8. определенная точность классификации.

Рисунок 2.17 – Столбчатая диаграмма распределения апостериорной вероятности классов-атак для значений [1σ;2σ) признака num_packets_equal_src_pan_max, период 10T, топология mesh

Требование 1 представляет собой ограничение сверху на количество данных, необходимых определения состояния БСС, в то время как требования 2 – ограничение снизу на точность системы обнаружения вторжений. Таким образом, алгоритм должен работать так, чтобы снизить нагрузку на доступные вычислительные ресурсы сети, при этом не теряя в эффективности обнаружения атак и не вызывая чрезмерного количества ложных срабатываний [71]. Проблема удовлетворения требования 1 заключается в принятии решения, какое подпространство (т.е. какую комбинацию признаков) использовать для классификации следующего наблюдения. Это решение должно быть обосновано прогнозом того, насколько хорошо данное подпространство поможет выявить класс, т.е. сможет удовлетворить требование 2.

Составление такого прогноза, или точнее, их системы, предполагает исследование эффективности каждой комбинации признаков применительно к

102

обнаружению каждого класса с высокой точностью и дальнейшее формирование набора комбинаций, которые будут использоваться в СОВ. При этом выбор определенной комбинации при поступлении очередного наблюдения должен диктоваться двумя критериями:

9. вероятность возникновения атаки;

10. предполагаемый класс, в котором находится система в данный момент.

Критерий 1 необходим для разработки статистической модели выбора и выражает собой априорную вероятность класса, подсчет или установление которой, как уже говорилось, очень сложен. Критерий 2, в свою очередь, предполагает составление дополнительной системы правил, определяющих, какое подпространство использовать, базируясь на знаниях о предполагаемых состояниях системы при предыдущих наблюдениях. Поэтому формирование системы прогнозов очень сложно и не гарантирует определенности, а применение методов работы с неопределенностью еще больше усложняет ее.

В данной работе вместо разработки системы прогнозов предлагается основываться на предположении о зависимости точности классификации от используемого признакового подпространства: чем больше количество признаков, используемых для классификации, тем больше ее точность. В зависимости от того, как 110 рассматривать данное предположение, оно объясняется следующими причинами:

11. Большее количество признаков означает получение большего количества информации о состоянии системы. Поскольку информация может рассматриваться как мера снятия определенности, увеличение ее объема приводит к возможности более точной классификации.

12. Чем больше признаков используется, тем специфичнее становится общая характеристика состояния системы. Чем более данные, характеризующие различные классы, отличаются, чем легче их различить, т.е. проклассифицировать.

Если сменить формулировку предположения, то основной прогноз об эффективности пространства – чем больше размерность подпространства, тем оно эффективнее в плане точности классификации. Если необходима более точная классификация состояния системы, нужно увеличить количество признаков, по которым она проводится.

Следует также отметить различную природу требований 1–2. Поскольку требование 1 к точности классификации (обнаружения атак) в контексте обеспечения безопасности важнее, оно необходимо должно быть удовлетворено в любом решении об использовании комбинации признаков, в то время как исполнение требования 2 желательно: не исключено использования всего признакового пространства, если это действительно необходимо. Это обусловливает процесс поиска такого решения: логичным будет среди самых желательных относительно требования 2 найти такое, которое необходимо удовлетворяет требованию 1. Если таких решений нет, происходит поиск среди менее желательных, и т.д.

На основе изложенного выше предлагается метод итеративной классификации, контролируемый двумя параметрами:

13. количество признаков;

14. параметр степени уверенности [210].

Рассмотрим подробнее параметр 2. Так как объективно сказать, насколько хорошо используемое пространство, в особенности при общности принятого прогноза, сможет обеспечить требуемую точность, достаточно сложно, предлагается ограничиться субъективным параметром степени уверенности, показывающим, насколько можно быть уверенным, что класс наблюдения именно таков, какой был определен. В прикладном смысле применения вероятностного классификатора этот параметр отражает апостериорную вероятность определенного класса.

Процесс итеративной классификации, таким образом, будет заключаться в классификации при расширении подпространства (увеличении значения

параметра 1) в ожидании повышении степени уверенности в определенном на нем классе. При этом для процесса определены два стоп-правила:

15. достижение показателем степени уверенности заданного значения параметра 2;
16. подпространство расширилось до всего пространства (значение параметра 1 максимально возможное).

Для проверки выдвинутых предположений был разработан алгоритм итеративной классификации наблюдения (рисунок 2.18). Исходный код алгоритма представлен в приложении В.

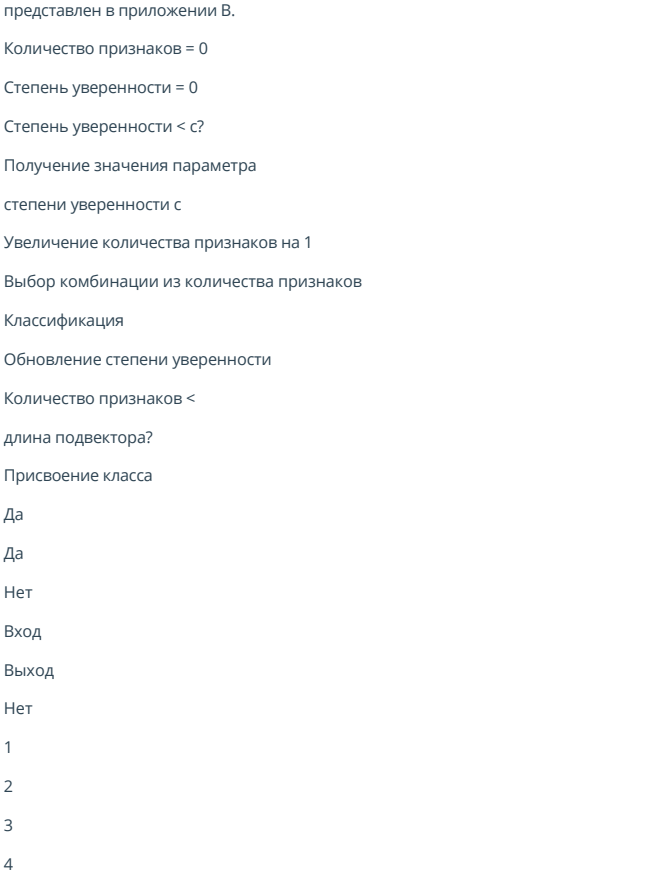


Рисунок 2.18 – Блок-схема алгоритма итеративной классификации наблюдения

Рассмотрим, как в структурных элементах алгоритма были реализованы принятые положения об итеративной классификации. Алгоритм выполняется для каждого нового измерения признакового пространства БСС. Способ определения параметра 2 устанавливается в программе СОВ, для которой данный алгоритм

разрабатывался как составная часть (элемент 1). Предварительно перед запуском цикла значение каждого параметра инициализируется (элемент 2), после чего выполняется проверка (элемент 3) стоп-правила 1: достижение определенным классом установленной степени уверенности. При его удовлетворении измерению присваивается окончательный класс (элемент 9), после чего алгоритм завершает свою работу. В противном случае происходит увеличение размерности подпространства (элемент 4) и его определение как комбинации признаков (элемент 5). По заданным признакам происходит классификация измерения с помощью таблиц апостериорных вероятностей, сгенерированных вероятностным классификатором. Определение класса выполняется по правилу оптимального решения:

$$y \hat{} \operatorname{argmax} p \mid x$$

где

y ^

– определенный класс,

argmax

– аргумент максимизации, или аргумент, при котором значение

выражения достигает наибольшего значения,

θ – один из 15 классов (состояний/атак) системы,

Θ – множество всех классов,

px |

– апостериорная вероятность класса θ при измерении x (2.1).

При этом также записывается само значение апостериорной вероятности (элемент 7), необходимое для принятия решения о следующей итерации. Перед этим выполняется проверка стоп-правила на текущую размерность подпространства (элемент 8): в случае, если ее можно увеличить, происходит дальнейшая проверка значения показателя степени уверенности (элемент 3), если нельзя – наблюдению присваивается класс (элемент 9), определенный при помощи всех допустимых признаков, и алгоритм завершает работу.

Тестирование работы алгоритма проводилось на данных о функционировании сети в топологии mesh при модельном периоде 360T. Данный период сам по себе обеспечивает высокий уровень точности, так как на большом периоде несущественные отличия между значениями признаков при малых

периодах наблюдения аккумулируются, тем самым упрощая различение классов. Значение параметра степени уверенности устанавливалось равным 0,85. Распределение априорных вероятностей полагалось равновероятным за неимением объективных данных, позволяющих судить о частоте или возможности осуществления атаки на БСС.

В таблице 21 и на рисунке 110 2.19 представлена точность классификации с помощью относительного количества измерений, классифицированных как тот или другой класс.

Таблица 21 – Количество классификаций в процентном выражении

Индекс определенного состояния

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Индекс состояния

1 99% - - - - - - - - - - 1% - - -

2 - 100% - - - - - - - - - - - - -

3 1% - 90% - 1% - - 7% - - - - - - 1%

4 - - - 99% - - - - - - - - - - 1%

5 - - - 1% 99% - - - - - - - - - -

6 - - - - - 99% - - - - 1% - - - 1%

7 1% - - - - - 99% - - - - - - - -

8 - - 15% - - - - 85% - - - - - - -

9 1% - - - - - - 1% 98% - - - - - -

10 - 1% - - - - - - - 99% - - - - -

11 - - - - - - - - - - 99% 1% - - -

12 1% - - - - - - - - - - 99% - - -

13 - - - - - - - - - - - - 100% - -

14 - - - - 1% - - - - - - - - 99% -

15 - - - - - - - 1% 1% 1% - - - - 97%

Как видно из таблицы 21 и рисунка 2.19, для большинства состояний точность классификаций приближается к 100%, при этом ни одно состояние не показывает точность меньше, чем заданный параметр степени уверенности 85%. Также следует заметить, что состояния «normal» и «selective_forward_dest» были проклассифицированы одно как другое, что можно объяснить близостью

некоторых групп данных одного класса к другому, а именно присутствие в статистике атаки типа «selective_forward_dest» значений, близких к нормальным. Следует отметить, что при такой высокой точности множество измерений было классифицировано с количеством признаков меньше пяти (рисунок 2.20). Чем легче определить атаку, тем, как правило, меньше требуется для этого признаков (например, атаки типа «flood» и «spoof_dest» на рисунке 2.20).

107

Определение нормального состояния сети было относительно трудным, что демонстрируется высоким количеством измерений, проклассифицированных с использованием всех пяти признаков. Это объясняется тем, что зачастую в статистике атак встречаются значения, подходящие под нормальные, в особенности для тех типов атак, которые обладают свойствами маскировать свою активность.

Рисунок 2.19 – Столбчатые диаграммы относительного числа классификаций измерений как определенного класса для всех состояний

Возможность сокращения числа признаков классификации в некоторых случаях обусловлена различными значениями признаков для различных типов атак, когда эти значения отличаются от нормальных. На рисунке ниже представлен график относительного количества классификаций атаки типа «flood» по определенному количеству признаков в зависимости от z-оценки отклонения признака num_packets_avg от нормы. Количество значений, входящих в пределы 3σ и определявшихся с помощью пяти признаков, иногда доходит до 20%, в то время как значения, выходящие за 3σ, не классифицировались более чем тремя признаками, что отображено на рисунке 2.21.

Для 12 состояний количество признаков, потребовавшихся для классификации, не превысило трех, что видно на рисунке 2.22.

108

Рисунок 2.20 – Относительное число классификаций, проведенных по определенному количеству признаков

Рисунок 2.21 – Относительное число классификаций атаки flood по определенному числу признаков в зависимости от значения отклонения признака num_packets_avg от нормы

109

Рисунок 2.22 – Среднее количество потребовавшихся признаков классификации измерений для различных классов (типов поведения)

Трудно определяемые состояния normal (No 3) и selective_forward_dest (No 8) тоже показали сокращение в среднем количестве признаков (около 4,3), хоть и небольшое.

Поскольку степень уверенности в классе (т.е. его апостериорная вероятность) играет ключевую роль в итеративном цикле, были исследованы ее показатели при определении класса. Чего и требовалось ожидать, во всех случаях средний показатель степени уверенности был больше заданного параметра (рисунок 2.23), однако для состояний 3 и 8 были обнаружены значения показателя для отдельных измерений, которые были значительно меньше требуемых (рисунок 2.24). В связи с эти были сделаны два заключения о влиянии параметра степени уверенности на значение апостериорной вероятности (показатель степени уверенности) присваиваемого класса:

17. Параметр степени уверенности не гарантирует классификацию с определенной апостериорной вероятностью в отдельных случаях;

110

18. В среднем по времени (по измерениям) значение показателя степени уверенности остается равным или превышающим значение заданного параметра степени уверенности.

Рисунок 2.23 – Среднее значение апостериорной вероятности определенного

класса при различном количестве признаков классификации

Рисунок 2.24 – Относительное число классификаций измерений с определенной апостериорной вероятностью (степенью уверенности)

111

На рисунке 2.25 представлены графики изменения апостериорной вероятности определенного класса при увеличении размерности пространства для нескольких серий работы алгоритма итеративной классификации.

Рисунок 2.25 – Графики изменения апостериорной вероятности предполагаемого класса по итерациям для нескольких классификации

Из графиков видна не только общая тенденция повышения степени уверенности, но и ее скорость, а также те состояния, которые требуют большего количества итераций. На рисунке также видно, как в состояниях normal и selective_forward_dest некоторые измерения при использовании пяти признаков классифицируются с более низкой степенью уверенности.

После тестирования алгоритма при фиксированном значении параметра степени уверенности было проведено исследование зависимости от него точности и среднего числа признаков классификации. На рисунке 2.26 можно заметить, что зависимость между параметром степени уверенности и точностью классификации не строго линейная, однако при возрастании первого возрастает и второе. При этом каждый класс обладает минимально возможной точностью классификации и максимально возможной, к которой точность асимптотически приближается при повышении значения параметра степени уверенности.

112

Следует сказать, что в большинстве случаев при необходимости обеспечения в среднем заданной точности классификации значение данного параметра не должно быть обязательно равно требуемой точности: он может быть несколько меньше, в пределах 30%.

Рисунок 2.26 – Графики зависимости средней точности классификации от значения параметра степени уверенности

Если не принимать во внимание 110 отдельные показатели точности в тех случаях, когда значение параметра степени уверенности близко к 0 или 1, можно сформировать заключение: параметр степени уверенности гарантирует среднюю точность классификации, равную ему или превышающую его. Это заключение тесно связано с заключением 2 о влиянии параметра степени уверенности на апостериорную вероятность определяемого класса и обосновывается применения правила оптимального решения Ошибка! Источник ссылки не найден.. Это правило гарантирует выбор такого класса, который, по сравнению с другими, чаще всего будет правильным. При увеличении параметра степени уверенности увеличится и апостериорная вероятность присваиваемого класса, т.е., в конечном итоге, частота правильной классификации.

113

На рисунке 2.27 представлены графики зависимости среднего количества признаков классификации от параметра степени уверенности. Как и в случае с точностью классификации, при возрастании одного – возрастает и другое. Однако характер зависимости более линейный. Более того, на множестве классов рост количества признаков происходит достаточно медленно, откуда следует вывод, что сокращенное количество используемых признаков классификации обусловливается в первую очередь природой статистики и только во вторую – значением параметра степени уверенности.

Очевидно, что при низкой скорости прироста значений зависимостей, как показано на 2.27, при выборе параметра степени уверенности следует в большей степени руководствоваться зависимостью от него точности классификации, так

как при небольшом изменении этого параметра можно обеспечить желаемое повышение точности при небольшом изменении требуемого числа признаков в среднем. С другой стороны, для таких состояний, как 3 и 8, имеет смысл руководствоваться теми зависимостями, какие более приоритетны, так как скорость изменения количества признаков для них высока, что может быть критично для СОВ.

Рисунок 2.27 – Графики зависимости среднего числа признаков классификации от значения параметра степени уверенности

Наконец, по данным, сгенерированным для исследования зависимостей, упомянутых выше, были построены графики на рисунке 2.28, отражающие общие тенденции зависимости точности классификации от среднего количества признаков.

Рисунок 2.28 – Точечные диаграммы корреляции среднего количества признаков и количества правильных классификаций

Данные показатели явно демонстрируют положительную корреляцию между собой, а это значит, что центральное предположение, принятое и выраженное в пункте 3.1 данной работы, о прогнозе, необходимом для принятия решения, какую комбинацию признаков использовать, верно. Поэтому прогноз о повышении точности классификации с увеличением размерности используемого признакового подпространства можно принять как основной прогноз системы принятия решения об используемой комбинации.

Было проверено и/или установлено несколько основных принципов и положений, характеризующих алгоритм обнаружения вторжений на основе вероятностной классификаций:

19. Некоторые наблюдения возможно классифицировать, используя подпространство признакового пространства классификации, не ухудшая при этом ее точность;

20. При повышении размерности используемого признакового подпространства классификации увеличивается ее точность;
21. При использовании итеративной классификации возможно добиться высокой степени точности распознавания типов атак при существенном сокращении среднего количества используемых для этого признаков;
22. В среднем значение апостериорной вероятности присвоенного класса не меньше значения заданного параметра степени уверенности;
23. Параметр степени уверенности обеспечивает точность классификации не ниже его значения;
24. Возможность использования сокращенного количества признаков из пространства обусловливается в первую очередь природой статистики и только во вторую – значением параметра степени уверенности;
25. Возможно сократить среднее число признаков классификации при сохранении высокой точности.

Выводы по главе 2

В главе 2 были решены следующие задачи:

1) предложена модель профиля поведения беспроводной сенсорной сети, позволяющая идентифицировать 14 типов атак сетевого уровня на беспроводные сенсорные сети. Модель профиля поведения отличается от известных использованием новой комбинации признаков, таких как общее количество пакетов, переданных в сети, максимальное количество отправленных узлом пакетов, максимальное и минимальное количество полученных узлом пакетов и соотношение между количеством созданных и полученных пакетов.
2) обоснован и описан процесс получения набора данных о поведении беспроводной сенсорной сети. Создан набор данных, который использовался для обучения и тестирования алгоритмов классификации. Набор был получен с

помощью разработанной программной модели атак на БСС. Описанная модель удовлетворяет характеристикам стандарта IEEE 802.15.4;

116

3) проведено сравнение различных алгоритмов классификации на основе разработанной модели профиля поведения и предложен метод идентификации атак на основе алгоритма «случайный лес», вероятностного классификатора и параметра степени уверенности. Новизна метода идентификации состоит в совместном использовании алгоритма «случайного леса» и вероятностного классификатора. Алгоритм «случайный лес» позволяет добиться высокой точности идентификации (97%) на разработанной модели профиля поведения сети и условии продолжительного сбора статистики (один час при условии, что средний период генерации пакетов равен 10 с). Вероятностный классификатор с введением параметра степени уверенности позволяет достигать заданного уровня точности при использовании неполного набора признаков модели профиля поведения и меньшего периода сбора статистики.

117

Глава 3 Методика идентификации атак на беспроводные сенсорные сети. Проведение экспериментов и оценка результатов

3.1 Методика идентификации атак на беспроводные сенсорные сети

Методика идентификации атак позволяет использовать предложенные модель и метод для идентификации атак сетевого уровня, поскольку возможно произвести настройку предложенных решений для различных характеристик сети. В качестве составляющих элементов методики используются такие разработки автора, как модель профиля поведения БСС и метод идентификации атак. Особенность модели профиля поведения заключается в использовании новой комбинации признаков идентификации атак, составленной на основе стандарта 802.15.4 и спецификации ZigBee; особенность метода идентификации состоит в совместном использовании алгоритма «случайный лес», вероятностного классификатора и введения параметра степени уверенности.

Также, в процессе проведения исследования были разработаны: программная модель проведения атак на БСС (No2018617190 от 20.06.2018), позволяющая получить набор данных для анализа; программа подсчета информативности признаков статистической выборки (No 2018618975 от 24.07.2018), необходимая для автоматизированного сокращения признакового пространства идентификации; и программа вычисления апостериорных распределений дискретного параметра распределения многомерной случайной величины по статистической выборки (No2018619014 от 25.07.2018), используемая на этапе обучения вероятностного классификатора и формирования рекомендаций для его применения [212].

Разработанная методика описывает процесс идентификации атак на БСС на основе анализа поведения сети. Общая схема методики представлена на рисунке 3.1.

Подготовительный этап методики начинается с настройки программной модели атак на беспроводные сенсорные сети в соответствии с характеристиками защищаемой сети (рисунок 3.2).

118

Рисунок 3.1 – Общая схема методики идентификации атак на БСС

При этом, возможно корректировка и изменение таких параметров, как: топология сети (ячеистая или кластерная); количество узлов в сети; профили поведения сети (нормального поведения и атак, которые необходимо идентифицировать); и набор признаков, характеризующих поведение сети.

119

Рисунок 3.2 – Этап настройки методики идентификации

После настройки программной модели осуществляется генерация статистических данных о нормальном поведении сети и поведении сети под атаками. Возможна корректировка модели поведения сети в соответствии с реальными данными в случае необходимости.

На основе полученных данных далее формируется модель профиля поведения сети. Данный подпункт включает в себя и снижение размерности набора признаков, необходимых для идентификации. Это реализуется с помощью вышеуказанной программы, которая подсчитывает информативность признаков по формулам Шеннона, Кульбака и методу накопленных частот.

120

После оценки корреляции между признаками, применяется алгоритм машинного обучения из библиотеки SciKitLearn для финального, минимального достаточного для идентификации набора признаков.

После формирования модели профиля поведения и оценки информативности, происходит формирование определенных профилей поведения сети и, при необходимости, занесение сформированных профилей в базу данных.

Следующий шаг – настройка метода идентификации атак на БСС. На данном шаге указываются следующие:

- параметра степени уверенности;
- период сбора данных с узлов сети;
- больший и меньший временные периоды для сбора данных о состоянии сети в целом.

Следует отметить, что 110 период характеризует количество итераций сбора данных о работе сети. Рекомендуется для большого временного периода выбирать Tb = 360T, а для малого Ts = 60T. T задается администратором сети (предыдущие работы автора предлагают T=10 с). Два периода стоит выбирать только в том случае, если 110 выбран подход с последовательным применением вероятностного классификатора и «случайного леса». В другом случае можно использовать один временной период. Имеет смысл выбирать величину малого периода такой, чтобы она была кратна большему периоду.

Выбор априорной вероятности нормального состояния. В результате проведения рядя экспериментов (для обеспечения высокой точности классификации нормального поведения сети и 14 атак) установлено, что необходимо, чтобы значение параметра степени уверенности было выше значения апостериорной вероятности нормального состояния на ~30% и нет необходимости в использовании апостериорной вероятности нормального состояния, превышающей 20%.

После этого происходит обучение алгоритма «случайный лес» и вероятностного классификатора.

Непосредственно этап идентификации атак представлен на рисунке 3.3.

121

Предполагается, что для идентификации можно использовать любой из упомянутых классификаторов или же использовать их совместно. Вероятностный классификатор стоит использовать в тех случаях, когда важную роль играет энергоэффективность: он позволяет идентифицировать атаки на неполном наборе признаков с заданной точностью (экспериментально было выявлено, что возможно достижение точности 95% при использовании только одного признака). Этот вариант применим, когда, например, узлы сети не обладают постоянным источником питанием (в частности, узлом, осуществляющим мониторинг [220] поведения, может быть шлюз, собирающий данные о поведении сети, также работающий от собственного источника питания).

Классификатор «случайный лес» менее энергоэффективен, но в то же время показывает более высокую точность работы: он демонстрирует хорошие результаты на наборе статистических данных, собранных за более длительный промежуток времени (экспериментально было выявлено, что длительность

периода сбора статистики, при которой достигается максимальная точность, равняется 360T (одному часу при соответствующих настройках)).

В связи с этим, предполагается целесообразным совместное использование двух классификаторов: на длительном промежутке «случайный лес», а на более коротких – вероятностный – для примерной оценки поведения сети. Следующую конфигурацию методов идентификации атак следует рассматривать в качестве рекомендаций.

Анализ неполного набора признаков из профиля поведения сети вероятностным классификатором производится каждые Ts . В этом случае вероятностный классификатор будет работать с растущим объемом набора данных: Ts,2Ts,3Ts,..., nTs, где nTs < Tb.

Результаты анализа предоставляются администратору сети. При соответствии показателя уверенности и результатов сравнения признака(ов) выводится результат идентификации (поведение под атакой или наиболее вероятные варианты атак, близкие к идентифицируемой по исследуемому признаку).

122

Рисунок 3.3 – Этап идентификации атак

123

В случае, если результатов достаточно и идентификация является положительной (вероятность конкретного поведения больше заданного параметра степени уверенности), администратор может завершить этап идентификации атак и, в случае необходимости, перейти к мерам по противодействию атаке. Если полученные результаты меньше или равны показателя степени уверенности, то запрашивается дополнительный признак из признакового пространства и происходит следующая попытка идентификации. При несоответствии показателя уверенности и использовании всех признаков состояния сети происходит завершение анализа поведения вероятностным классификатором. Возможно также завершение процесса идентификации, если администратор сети предполагает, что полученных результаты являются удовлетворительными.

Необходимо отметить, что классификация изначально осуществляется на небольших по сравнению с Tb периодах сбора данных. Поэтому на начальном этапе работы стоит выбирать не столь большие величины параметра степени уверенности: при большом значении параметра степени уверенности, например, 85-99%, классификатор будет использовать в среднем больше признаков для классификации, что увеличит нагрузку на устройства. Результаты на небольших наборах данных, как показывает практика, менее информативны, поэтому расходование энергии устройств на этом этапе нецелесообразно. Тем не менее, на каждой последующей итерации работы вероятностного классификатора набор данных и, соответственно, информативность признаков будут расти. В связи с этим предлагается 110 использование прогрессирующего параметра степени уверенности от 60% до 90%.

После этого производится анализ полного набора признаков профиля поведения, собранного за Tb и выполняется классификация с помощью классификатора «случайный лес». При положительной идентификации выводится результат (тип атаки), при невозможности идентификации выводится сообщение о неизвестном аномальном поведении.

124

3.2 Эксперимент при изменении параметров сети

Для подтверждения результатов, полученных в работе, был проведен ряд дополнительных экспериментов, направленных на оценку зависимости информативности признаков от следующих характеристик сети:

1. Топологии;

2. Периодов генерации пакетов;

3. Степени случайности выбора адресов назначения.

Аналогично пункту 2.3 в главе 2, была произведена оценка информативность признаков для кластерного дерева. Результаты приведены на рисунке 3.4 и в таблицах 22-24. Можно сделать вывод, что 110 наблюдается тенденция к общему увеличению информативности признаков при увеличении периода сбора статистики. Кроме того, еще раз подтверждается существование признаков, способных отделить аномальное поведение от нормального.

Для сопоставления наиболее информативных признаков для разных топологий (ячеистой сети и кластерного дерева) был выбран максимальный период сбора статистики – 360Т. На рисунке 3.5 представлены наиболее информативные признаки.

На рисунке 3.6 представлена зависимость признаков от параметра дискретизации для сети с топологией кластерное дерево.

При анализе результатов можно сделать следующие выводы:

1. В общем случае информативность признаков для топологии сети «кластерное дерево» выше, чем информативность для ячеистой сети;
2. Для сети с топологией «кластерное дерево» и ячеистой сети информативными, по большей части, являются одни и те же признаки.

Следующий эксперимент реализован путем назначения для каждого узла собственных значений математического ожидания для нормальных распределений, определяющих период генерации пакетов. Математические ожидания в первом случае одинаковые и равны 10 (что рассматривалось выше), во втором случае назначены произвольно (значения представлены в таблице 25).

125

Рисунок 3.4 - Информативность признаков для сети топологии «кластерное дерево» по методу Шеннона

Таблица 22 – 5 наиболее информативных признаков по методу Шеннона для сети топологии «кластерное дерево»

Период Признак Информативность

10Т num_packets_equal_src_max 1

num_packets_equal_dest_max 1

num_packets_created_max 1

num_packets_equal_dest_pan_max 0.388859

num_packets_in_max 0.101423

0 0,1 0,2 0,3 0,4 0,5 0,6

num_frames

num_packets

num_packets_out_avg

num_packets_out_min

num_packets_in_max

weighted_num_packets_in_avg

weighted_num_packets_in_min

frac_packets_in_out_max

frac_packets_in_out_pan_avg

frac_packets_in_out_pan_min

num_packets_equal_src_max

num_packets_equal_src_pan_avg

num_packets_equal_src_pan_min

num_packets_equal_dest_max

num_packets_equal_dest_pan_avg

num_packets_equal_dest_pan_min

num_frames_out_max

num_frames_in_avg

num_frames_in_min

weighted_num_frames_in_max

num_route_msgs

num_forwarded_packets_avg

num_forwarded_packets_min

num_packets_created_max

frac_packets_created_acquired_avg

frac_packets_created_acquired_min

Кластерное дерево

360T 60T 10T

126

Период Признак Информативность

60T num_packets_equal_src_max 1

num_packets_equal_dest_max 1

num_packets_created_max 1

num_packets_equal_dest_pan_max 0.995858

frac_packets_in_out_avg 0.549236

360T num_packets_equal_src_avg

1

num_packets_equal_src_max 1

num_packets_equal_dest_max 1

num_packets_equal_dest_pan_max 1

num_packets_created_max 1

Таблица 23 – 5 наиболее информативных признаков по методу Кульбака для сети

топологии «кластерное дерево»

Период Признак Информативность

10T num_packets_equal_dest_pan_max 2.277001901

num_packets 0.867413464

num_packets_in_max 0.85058403

frac_packets_in_out_avg 0.786712173

num_packets_avg 0.739905533

60T frac_packets_in_out_avg 5.286882719

frac_packets_in_out_pan_avg 4.510871542

num_packets 3.857940948

num_packets_in_max 3.316789377

num_packets_avg 3.200612921

360T num_packets 13.49451084

num_forwarded_packets_max 11.24762801

num_frames 11.08580809

num_packets_out_max 10.57995196

num_frames_avg 10.36466165

Таблица 24 – 5 наиболее информативных признаков по методу накопленных

частот для сети топологии «кластерное дерево»

Период Признак Информативность

10T num_packets_equal_src_max 500

num_packets_equal_dest_max 500

num_packets_created_max 500

num_packets_equal_dest_pan_max 316

num_packets 165

60T num_packets_equal_src_max 500

num_packets_equal_dest_max 500

num_packets_created_max 500

num_packets_equal_dest_pan_max 499

frac_packets_in_out_avg 390

360T num_packets_equal_src_avg 167

num_packets_equal_src_max 167

num_packets_equal_dest_max 167

num_packets_equal_dest_pan_max 167

num_packets_created_max 167

127

Рисунок 3.5 – Информативные признаки для топологии «кластерное дерево»

и ячеистой сети

Рисунок 3.6 – Информативность и параметр дискретизации в сети с топологией

«кластерное дерево»

0 0,1 0,2 0,3 0,4 0,5 0,6

num_packets_out_max

num_frames_out_max

num_packets_avg

num_frames_avg

num_packets

num_forwarded_packets_avg

num_packets_equal_dest_pan_max

num_frames

num_frames_out_avg

num_packets_equal_dest_pan_avg

frac_packets_in_out_pan_avg

num_packets_equal_dest_max

num_packets_equal_dest_avg

num_packets_equal_src_pan_max

frac_packets_created_acquired_min

weighted_num_packets_in_min

num_packets_equal_dest_pan_min

Ячеистая сеть и кластерное дерево

Mesh Tree

0 0,1 0,2 0,3 0,4 0,5 0,6 0,7

num_packets_out_avg

num_forwarded_packets_max

num_packets_avg

frac_packets_created_acquired_avg

num_frames_avg

num_forwarded_packets

frac_packets_in_out_avg

num_packets_equal_src_pan_min

num_packets_equal_src_pan_avg

weighted_num_frames_in_max

weighted_num_packets_in_min

num_packets_equal_src_min

num_packets_equal_dest_pan_min

Кластерное дерево. Информативность и параметр

дискретизации

Discr=10 Discr=100

128

Таблица 25 – Математические ожидания для нормального распределения

Узел Математическое

ожидание

Узел Математическое

ожидание

Node 0 5 Node 8 15

Node 1 10 Node 9 20

Node 2 15 Node 10 10

Node 3 10 Node 11 15

Node 4 20 Node 12 10

Node 5 15 Node 13 10

Node 6 5 Node 14 10

Node 7 20

Вторая часть эксперимента заключается в назначении для каждого узла сети (за исключением одного – координатора) адреса, которому направляются все генерируемые этим узлом пакеты. Маршруты пересылки сообщений настроены так, чтобы атаки типа «выборочная пересылка», «повторная передача» и «воронка» имели смысл. В таблице 26 представлены маршруты для каждого узла сети.

Таблица 26 – Детерминированные маршруты для ячеистой сети

Узел Получатель пакетов Узел Получатель пакетов

Node 0 Random Node 8 Node 10

Node 1 Node 0 Node 9 Node 12

Node 2 Node 0 Node 10 Node 14

Node 3 Node 12 Node 11 Node 10

Node 4 Node 0 Node 12 Node 14

Node 5 Node 0 Node 13 Node 12

Node 6 Node 10 Node 14 Node 0

Node 7 Node 11

Стоит отметить, что для случая детерминированной пересылки не осуществляется моделирование атак типа selective_forward_dest и

repeated_transmission_dest, поскольку эти атаки в подобных сетях [40] сводятся к обычным выборочной пересылке и повторной передаче.

Обобщенные результаты эксперимента представлены на рисунке 3.7. Так же, как и в случае сравнения кластерного дерева и ячеистой сети, изображены признаки, не относящиеся к рангу неинформативных. Стоит отметить, что были получены и оценки тремя методами оценки информативности для любой пары классов «нормальное-аномальное поведение». В работе эти результаты не приводятся ввиду большого объема информации. Общий вывод тот же, что и для аналогичной оценки древовидной структуры: для большинства типов атак существуют абсолютно информативные признаки, что теоретически обуславливает высокую точность методов классификации, основанных на композициях алгоритмов.

Из анализа приведенной информации следуют выводы:

1. Информативность признаков в сети с детерминированными маршрутами обычно выше, чем информативность в стохастической сети;
2. Количество информативных признаков в сети с детерминированными маршрутами обычно больше, чем количество в стохастической сети;
3. Информативность мало зависит от соотношения периодов генерации пакетов разными узлами, что еще раз подчеркивает справедливость формулы для подсчета совокупной частоты генерации пакетов. Обратная величина – средний период генерации пакетов – имеет исключительную важность, поскольку частично определяет величину периода сбора статистики.

Полученные данные показывают, что значительной разницы с результатами оценки информативности, приведенной в Главе 2, нет. Следовательно, можно сделать вывод о том 110 , что 110 для большинства вариантов, вне зависимости от степени случайности выбора адресов и иных характеристик, наиболее информативные признаки одинаковы.

Как уже было отмечено ранее 110 , среди классов поведения есть частные случаи атак на беспроводные сенсорные сети, которые в выборке были обозначены суффиксами _exact_dest и _exact_src. Эти частные случаи соответствуют

применению вредоносного воздействия к пакетам, соответствующим определенному адресу отправителя или получателя.

Рисунок 3.7 – Информативность признаков в сети с ячеистой топологией в зависимости от различных параметров сети

Для того, чтобы атакующий узел мог осуществить атаку, необходимо, чтобы через него проходили пакеты со строго определенным адресом отправителя или получателя. В случае сети со стохастической адресацией это происходит достаточно редко. Так, например, при пяти узлах в некоторой PAN лишь каждый пятый пакет будет соответствовать требуемому условию. При этом атакующий узел не может, например, отбрасывать все пакеты, соответствующие определенному адресу и проходящие через него, так как в этом случае 110 он будет быстро обнаружен атакуемым узлом. Поэтому чаще всего атакующие осуществляют аномальное воздействие выборочно, лишь на часть пакетов. В

0 0,1 0,2 0,3 0,4 0,5 0,6 0,7 0,8

num_packets_out_avg

num_frames_out_avg

num_frames_avg

num_packets_in_max

num_frames_out_max

num_frames_in_max

num_packets_equal_src_pan_min

num_packets_in_avg

num_packets_equal_dest_avg

num_packets_equal_dest_pan_avg

frac_packets_in_out_avg

num_packets_equal_dest_max

num_packets_equal_dest_pan_min

num_frames

frac_packets_in_out_pan_max

num_packets_equal_src_pan_max

num_packets_equal_src_max

weighted_num_frames_in_avg

Информативность в ячеистой сети

Determined Var periods Stochastic

131

результате статистически некоторые типы атак могут не проявиться даже при периоде сбора статистики продолжительностью один час.

Рассмотрим точность классификации при отсечении вариаций (частных случаев) атак. Результаты приведены на рисунках 3.8 и 3.9.

Рисунок 3.8 – Точность многоклассовой классификации при отсечении частных случаев

Рисунок 3.9 – Точность линейной классификации при отсечении частных случаев

Следовательно, точность классификации при отсечении частных случаев значительно увеличивается и достигает 97% даже для ранее плохо работавших алгоритмов машинного обучения. Таким образом, можно сделать промежуточный вывод: предложенная модель профиля поведения позволяет практически со 100% точностью определять поведение БСС.

Рассмотрим работу классификаторов при изменении количества узлов и средних периодов генерации пакетов. Классификатор был обучен на выборке,

50

60

70

80

90

100

AdaBoost Decision Tree Extra Trees classifier Gradient Boosting RandomForest

Точность классификации при отсечении вариаций атак

total informative uncorrelated minimum

40

50

60

70

80

90

100

Stochastic Gradient Linear Support Vector

Machine

Support Vector Machine Logistic Regression

Точность класиификации при тсечении вариаций атак

total informative uncorrelated minimum

полученной для 15 узлов со средним периодом генерации пакетов 10 секунд. В качестве тестовых выборок были использованы:

1. Выборка, полученная для 20 узлов со средним периодом генерации пакетов 10 секунд.
2. Выборка, полученная для 15 узлов со средним периодом генерации пакетов 5 секунд.

Точность классификации для решающего дерева и стохастического леса представлена на рисунках 3.10 и 3.11. На рисунках 3.12 и 3.13 представлена точность классификации при отсечении частных видов атак.

Рисунок 3.10 – Обобщающая способность DecisionTree

Рисунок 3.11 – Обобщающая способность RandomForest

0

10

20

30

40

50

60

70

changed frequency changed num_nodes

Обобщающая способность дерева решений

total informative uncorrelated minimum

0

10

20

30

40

50

60

70

80

90

changed frequency changed num_nodes

Обобщающая способность "случайного леса"

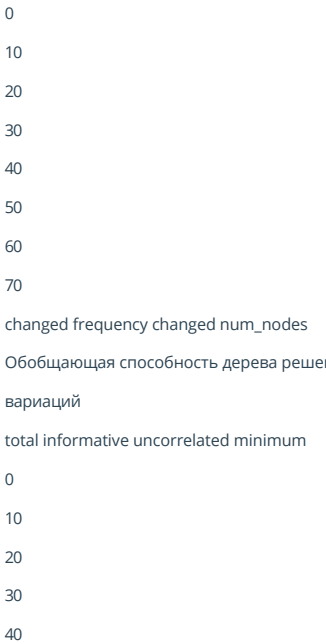
total informative uncorrelated minimum

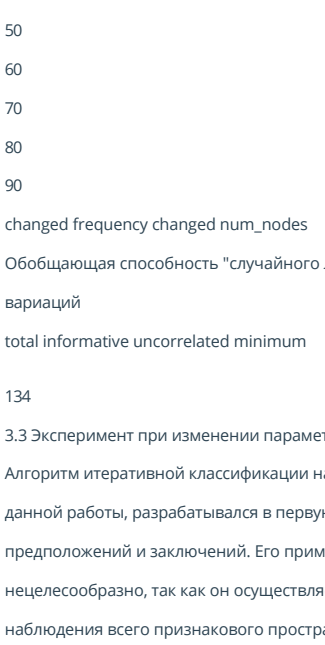
Рисунок 3.12 – Обобщающая способность DecisionTree при отсечении частных случаев

Рисунок 3.13 – Обобщающая способность RandomForest при отсечении частных

случаев

На основании всего вышеперечисленного, можно сделать вывод, что 110 изменение количества узлов оказывает на классификатор менее пагубное влияние, чем изменение средних периодов генерации пакетов. В то же время, точность классификации значительно ниже, чем полученная ранее для случая неизменных количества узлов и статистических характеристик.





134

3.3 Эксперимент при изменении параметра степени уверенности

Алгоритм итеративной классификации наблюдения, описанный в пункте 2.3 данной работы, разрабатывался в первую очередь для проверки сделанных ранее предположений и заключений. Его применение в таком виде в реальных условиях нецелесообразно, так как он осуществляет классификацию единственного наблюдения всего признакового пространства. Это означает, что реального снижения количества признаков, чьи значения измеряются с определенным периодом, не произойдет, так как для алгоритма требуется полное наблюдение. Более того, классификация займет больше времени и вычислительных ресурсов системы, так как, по сравнению со стандартной схемой классификации, на одно значение требуется больше одной итерации, а значит, больше компьютерных операций [72].

Таким образом, по сравнению с классическим методом классификаций, где используется фиксированное признаковое пространство, на каждое наблюдение которого требуется определенное количество операций, нет никакого преимущества. Однако ранее было сделано заключение 7 о возможности применения алгоритма итеративной классификации для сокращения среднего количества используемых признаков, поэтому данный алгоритм необходимо адаптировать для применения в реальных условиях. В связи с этим предлагается 110 переработка алгоритма для классификации серии измерений. Далее будут рассмотрены принципы функционирования адаптированного алгоритма, а также будет проведено его тестирование.

В обобщенном виде адаптированный алгоритм представлен на рисунке 3.14. Как и прежде, в первую очередь алгоритм получает значение параметра степени уверенности (элемент 1), в общем случае – дополнительными средствами СОВ. Инициализация цикла происходит за счет обнуления значений двух ключевых параметров: количества признаков подпространства и показателя степени уверенности (элемент 2). Перед каждой следующей классификацией происходит проверка удовлетворения двух стоп-правил: достижения значения параметра

степени уверенности (элемент 3) – в первую очередь, максимального расширения подпространства (элемент 4) – во вторую. Срабатывание стоп-правила приводит к принятию решения о состоянии, в котором на данный момент находится сеть (элемент 10). Это состояние определяется как класс, присвоенный последнему наблюдению, за которым последовало срабатывание стоп-правила.

Рисунок 3.14 – Блок-схема разработанного метода идентификации атак на основе вероятностного классификатора

В случае, если наблюдение классифицировано с низкой степенью уверенности и его подпространство можно расширить, количество признаков увеличивается (элемент 5). По нему выбирается комбинация (элемент 6), значения

признаков которой запрашиваются алгоритмом: такая процедура позволит ограничиться сбором (элемент 7) сокращенного количества данных с самой БСС, уменьшая нагрузку на ее ресурсы.

136

Классификация (элемент 8) и обновление степени уверенности производятся на базовой станции БСС, где были собраны данные о работе сети и хранятся таблицы апостериорных вероятностей. Такой метод организации системы обнаружения вторжений обладает рядом преимуществ, среди которых:

26. отсутствие высоких требований к вычислительным ресурсам сенсорных узлов;
27. возможность собирать статистику работы БСС на носители данных и анализировать ее;
28. облегченная модификация параметров классификации или вероятностного классификатора.

Главный недостаток такой схемы – централизация алгоритма обнаружения вторжений в одном месте, из-за чего безопасность информации может быть подвергнута угрозе при компрометации базовой станции или нарушению доступности, целостности данных на ней.

Алгоритм проектировался для постоянной работы, т.е. непрерывного мониторинга безопасности БСС на предмет атак, однако после принятия каждого решения (элемент 10) предусмотрена возможность завершить его работу (элемент 11), что выполняется средствами администрирования СОВ. Такая остановка может быть необходима, например, для изменения конфигурации сети, СОВ, вероятностного классификатора или параметра алгоритма обнаружения вторжений.

Перед проведением серии экспериментов были изменены некоторые параметры алгоритма. Во-первых, был изменен метод выбора комбинации признаков (элемент 6). В алгоритме итеративной классификации наблюдения данный выбор (элемент 5) происходил с учетом текущего подпространства, а именно случайно выбирался дополнительный признак из числа тех, что не использовались, в дополнение к уже присутствующим в подпространстве:

w 0, w i w i 1 vv, v \ w i 1

,

где v – подвектор признакового пространства БСС; признаковое пространство классификации,

137

w i

– подпространство v; i-ое подпространство классификации (размерности i),

v – новый признак классификации.

При этом обязательно выполняется

i : ww ii 1

(3.1)

В адаптированном же алгоритме выбор всего подпространства классификации происходит случайно, т.е. без учета текущего:

i j, j

j

wv vv

Поэтому (3.1) не обязательно выполняется для всех i.

Во-вторых, было принято решение увеличить априорную вероятность нормального состояния в десять раз (0,67), чтобы выразить ожидание работы сети в нормальном состоянии в большинстве случаев. Априорные вероятности атак были равны равномерно распределенной между ними разнице 1 0,67 0,33

0,33 14 0,024

:

1 3

, 3

i 1

p

pi

m

,

(3.2)

где

p i

– априорная вероятность i-ого состояния (атаки/класса),

p 3

– априорная вероятность нормального состояния,

m – количество различных состояний БСС.

Значение параметра степени уверенности осталось равным 85%.

В ходе тестирования адаптированного алгоритма записывались те же ключевые характеристики, что и ранее: точность и среднее число признаков классификации. На рисунке 3.15 представлены столбчатые диаграммы, отражающие разницу в относительной точности классификации по сравнению с предыдущей серией экспериментов. Из него видно, прежде всего, что количество правильных классификаций нормального состояния увеличилось, а неправильных – уменьшилось, при этом для некоторых типов атак, из которых более всего

выделяется selective_forward_dest, верное обратное. Такое отличие объясняется принятым значением априорной вероятности нормального состояния: его значение было достаточно велико, чтобы значительно повысить приоритет нормального состояния по сравнению с атаками, что привело к большему количеству правильных определений самого нормального состояния, но также и к неправильной классификации атак. Особенно низкие результаты для состояния No8 обусловлены большим количеством наблюдений в статистике этого состояния нормальных значений.

Рисунок 3.15 – Столбчатые диаграммы разницы в относительном числе классификаций как определенного класса между второй и первой серией экспериментов

Соответственно, среднее количество признаков классификаций снизилось по сравнению с первой серией экспериментов, что представлено на рисунках 3.16 и 3.17. Примечательно, насколько сильно упала частота использования пяти признаков для определения данных нормального состояния: если считать, что в большинстве случаев состояние сети будет действительно нормальным, то этот результат обеспечит существенное снятие нагрузки с БСС.

При этом среднее количество признаков, использованных при классификации, упало практически для всех состояний. Данный показатель

снизился для нормального состояния на единицу, т.е. в среднем по измерениям для классификации нормального состояния требуется не более 4 признаков.

Рисунок 3.16 – Столбчатые диаграммы разницы в относительном числе классификаций с использованием определенного количества признаков между второй и первой серией экспериментов

Рисунок 3.17 – Столбчатые диаграммы разницы в среднем количестве использованных признаков классификации между второй и первой серией экспериментов

Данное отличие видно также на рисунке 3.18, отображающем количество

использованных признаков классификации для различных измерений нормального состояния при первой серии экспериментов, где априорная вероятность нормального состояния была 0,067 (верхний график), и второй, где она была равна 0,67 (нижний). В последнем случае за 100 измерений пять признаков были использованы лишь пять раз.

Рисунок 3.18 – Графики количества использованных признаков классификации при первой серии экспериментов (верхний) и второй (нижний)

Поскольку результаты тестирования данного алгоритма существенно отличались от результатов для предыдущего, преимущественно из-за другого значения априорной вероятности нормального состояния, дополнительно было проведено исследование зависимости точности классификации от его значения. Из графика этой зависимости (рисунок 3.19) для состояния normal видно, что точность достигает предела в 100% процентов при значении априорной вероятности 0,2 и не меняется при его увеличении, в то время как для других атак - уменьшается, поэтому можно заключить, что применение значений априорной вероятности normal выше 0,2 нецелесообразно. Следует принять во внимание

состояние 8 (selective_forward_dest), точность определения которого зависит от априорной вероятности normal практически линейно: атака этого типа показывают самую большую скорость понижения точности среди всех других.

Рисунок 3.19 – Графики зависимости количества правильных классификаций от значения априорной вероятности нормального состояния

Кроме того, были получены данные о зависимости среднего количества использованных признаков классификации от апостериорной вероятности нормального состояния (рисунок 3.20). Для состояний 3 и 8 эти зависимости практически идентичны и демонстрируют высокую скорость уменьшения среднего количества признаков классификации при повышении априорной вероятности состояния normal. Для большинства атак наблюдается относительное постоянство значений зависимости на диапазоне от 0 до 0,7±0,1, после чего происходит резкое снижение, соответствующее резкому ухудшению качестве классификации. Здесь выделяются состояния repeated_transmission и spoof_dest, для которых графики зависимости демонстрируют практически полное отсутствие зависимости от априорной вероятности нормального состояния: в их статистике практически (или совсем) отсутствуют значения, походящие на нормальные.

Рисунок 3.20 – Графики зависимости среднего количества использованных признаков классификации от априорной вероятности нормального состояния

3.4 Эксперимент при изменении априорной вероятности нормального поведения и параметра степени уверенности

Во время разработки метода были выявлены два параметра, существенно влияющих на точность обнаружения вторжений и, закономерно, количество признаков классификации: параметр степени уверенности, задаваемый для итеративного процесса классификации, и априорная вероятность нормального состояния, изменяющая распределения апостериорных вероятностей, по которым проводится определение класса. Ранее влияние этих параметров на классификацию исследовалось по отдельности, однако для более полного понимания зависимостей необходима проверка их совместного влияния на характеристики классификации.

Перед проведением серии экспериментов было сформулировано правило пересчета апостериорных распределений при изменении апостериорного распределения вероятности возникновения классов. Данное правило позволило ограничиться операциями линейной алгебры для изменения вероятностного классификатора без необходимости проводить генерацию распределений с нуля.

143

1

diag 11

T

T

P P m P

1

,

(3.3)

где P – имеющаяся матрица апостериорных вероятностей вида (2.2),

diag 1,, m

– матрица прежних значений априорной вероятности,

diag 1,, m

– матрица новых значений априорной вероятности,

diag vv 1,, n

– диагональная матрица вида

av ij i ij

,

ij

– символ Кронекера,

1m – вектор

1,,1

m

.

Формула (3.3) является выражением в элементарных операциях деление каждого члена матрицы на прежнее значение априорной вероятности соответствующего класса, умножение на новое и дальнейшее нормирование ряда матрицы, т.е. значений одного апостериорного распределения.

В ходе исследования при изменении априорной вероятности нормального состояния априорные вероятности атак считались по формуле (3.2). При этом для каждой пары различных значений параметра степени уверенности и априорной вероятности нормального состояния производилась серия тестов, направленная на установление упомянутых выше характеристик классификации. Таким образом, для каждого состояния было получено две матрицы: в первой записаны показатели точности классификации, во второй – среднее количество использованных признаков.

На рисунке 3.21 изображены графические представления матриц зависимости точности классификации от параметра степени уверенности и априорной вероятности нормального состояния. Каждое значение в матрице определяет цвет, закрашивающий точку, координатами которой являются значения параметров. В качестве легенды к соответствию цвета точки и значению предоставлена цветовая шкала: чем ниже значение, тем темнее окрашивается точка, чем оно выше, тем цвет точки светлее.

144

Рисунок 3.21 – Графические представления матриц зависимости точности классификации от параметра степени уверенности и априорной вероятности нормального состояния

Необходимо сказать о тенденции, усматриваемой почти для всех видов атак: для обеспечения высокой точности классификации необходимо, чтобы значение параметра степени уверенности было выше значения апостериорной вероятности нормального состояния приблизительно на 30%. Области высокой точности на рисунке – светлые треугольники в левом верхнем углу. Матрица для нормального состояния отличается от других, но только потому, что его апостериорная вероятность была опорной при исследовании. Значения матрицы подтверждают ранее сделанное наблюдение: нет необходимости в использовании

апостериорной вероятности нормального состояния, превышающей 20%.

Были также получены аналогичные графические представления матриц для среднего количества признаков классификации, представленные на рисунке 3.22. Наиболее важное свойство данных, проиллюстрированное на данном рисунке, – это отсутствие необходимости более чем в ≈3 признаках классификации для всех атак, кроме selective_forward_dest при любых значениях параметра степени уверенности и априорной вероятности нормального состояния. Нормальное состояние в некоторых случаях требовало всех пяти признаков.

145

Рисунок 3.22 – Графические представления матриц зависимости среднего числа использованных признаков классификации от параметра степени уверенности и априорной вероятности нормального состояния

На основе данных о зависимости среднего количества признаков классификации можно выдвинуть гипотезу, что возможно определить такое признаковое пространство классификации, что для определения каждого класса не потребуются лишь его подпространство при любых параметрах классификации. Иными словами, возможно для каждого класса найти такую комбинацию признаков, что она однозначно определяет этот класс из числа всех других, и составить из каждой такой комбинации признаковое пространство, которое не будет использоваться в полной мере. Исследование данной гипотезы выходит за рамки данной работы и потому не будет проводиться.

Полученные матрицы сами по себе могут носить рекомендательный характер и служить как руководство к выбору параметров, однако в данной работе для формирования рекомендаций предлагается пользоваться простым алгоритмом поиска значений параметров, обеспечивающих требуемые характеристики классификации. Пусть A – матрица точности классификации для различных значений параметра степени уверенности и априорной вероятности нормального состояния, N – матрица среднего количества признаков, c – соответствующее числу в матрице значение параметра степени уверенности, а p –

146

соответствующее ему значение априорной вероятности нормального состояния. Тогда алгоритм поиска требуемых c и p следующий:

Шаг 1. Выбрать требуемую точность классификации a;

Шаг 2. Найти в A все значения не меньше a и записать их индексы;

Шаг 3. Среди значений в N, находящихся на соответствующем месте записанных индексов, выбрать минимальное(-ые);

Шаг 4. Присвоить c и p индекс (один из индексов) минимального(-ых) значения(-ий), найденного(-ых) в предыдущем шаге.

Данный алгоритм гарантирует нахождение таких c и p, что они удовлетворяют требованию на желаемую точность классификации при использовании минимально возможного количества признаков. Следует отметить, что алгоритм прост и ищет оптимальное решение с точки зрения двух параметров, однако во внимание не принимаются матрицы для других классов или поиск среди найденных в шаге 3 минимальных значений наилучшего по какому-то иному критерию. В таблицах 27, 28, 29 представлены результаты работы этого алгоритма для требуемых значений точности в самой простой его реализации.

Таблица 27 – Алгоритмически сформированные рекомендации по выбору значения параметра степени уверенности при требуемой точности классификации для различных классов

Индекс класса (состояния/атаки)	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Требуемая точность классификации															
5%	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01
10%	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,01
15%	0,01	0,01	0,01	0,01	0,01	0,01	0,01	0,02	0,01	0,01	0,01	0,01	0,01	0,01	0,01

20% 0,01 0,01 0,01 0,01 0,01 0,01 0,01 0,02 0,01 0,01 0,01 0,01 0,01 0,01 0,01

25% 0,01 0,01 0,01 0,01 0,01 0,01 0,01 0,02 0,01 0,01 0,01 0,01 0,01 0,01 0,01

30% 0,01 0,01 0,01 0,01 0,01 0,01 0,01 0,02 0,02 0,01 0,01 0,01 0,01 0,01 0,01

35% 0,01 0,01 0,01 0,01 0,01 0,01 0,01 0,02 0,02 0,01 0,01 0,01 0,01 0,01 0,01

40% 0,01 0,02 0,01 0,01 0,01 0,01 0,01 0,21 0,02 0,01 0,01 0,01 0,01 0,02 0,01

45% 0,02 0,02 0,01 0,01 0,03 0,01 0,01 0,21 0,02 0,01 0,01 0,01 0,01 0,02 0,01

50% 0,02 0,02 0,01 0,01 0,03 0,01 0,01 0,21 0,02 0,03 0,01 0,01 0,03 0,02 0,02

55% 0,07 0,02 0,02 0,01 0,09 0,01 0,01 0,21 0,02 0,03 0,09 0,01 0,03 0,02 0,02

60% 0,38 0,02 0,02 0,01 0,02 0,01 0,01 0,21 0,02 0,07 0,05 0,01 0,04 0,03 0,02

65% 0,71 0,02 0,01 0,01 0,06 0,01 0,01 0,21 0,13 0,07 0,05 0,04 0,05 0,03 0,09

70% 0,44 0,04 0,01 0,01 0,06 0,01 0,01 0,25 0,13 0,08 0,24 0,04 0,08 0,03 0,05

75% 0,37 0,04 0,01 0,01 0,06 0,32 0,01 0,31 0,16 0,13 0,36 0,05 0,2 0,03 0,1

80% 0,37 0,08 0,01 0,01 0,19 0,42 0,07 0,31 0,23 0,22 0,47 0,05 0,26 0,02 0,12

85% 0,39 0,13 0,1 0,01 0,36 0,17 0,06 0,34 0,23 0,22 0,47 0,28 0,53 0,14 0,3

90% 0,85 0,27 0,1 0,01 0,36 0,25 0,13 0,34 0,23 0,32 0,32 0,36 0,87 0,36 0,39

95% 0,85 0,25 0,1 0,03 0,23 0,24 0,15 0,34 0,23 0,39 0,51 0,46 0,96 0,36 0,39

100% 0,65 0,22 0,17 0,05 0,27 0,47 0,39 0,5 0,74 0,33 0,51 0,46 0,96 0,36 0,49

147

Таблица 28 – Алгоритмически сформированные рекомендации по выбору значения априорной вероятности нормального состояния при требуемой точности классификации для различных классов

Индекс класса (состояния/атаки)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Требуемая точность классификации

5% 0.01 0.01 0.07 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01

10% 0.01 0.01 0.07 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01

15% 0.01 0.01 0.07 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01

20% 0.01 0.01 0.07 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01

25% 0.01 0.01 0.07 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01

30% 0.01 0.01 0.07 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01

35% 0.01 0.01 0.07 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01 0.01

40% 0.01 0.01 0.07 0.01 0.01 0.01 0.01 0.05 0.01 0.01 0.01 0.01 0.01 0.01 0.01

45% 0.01 0.01 0.07 0.01 0.01 0.01 0.01 0.05 0.01 0.01 0.01 0.01 0.01 0.01 0.01

50% 0.01 0.01 0.07 0.01 0.01 0.01 0.01 0.05 0.01 0.01 0.01 0.01 0.01 0.01 0.01

55% 0.03 0.01 0.07 0.01 0.01 0.01 0.01 0.05 0.01 0.01 0.01 0.01 0.01 0.01 0.01

60% 1 0.01 0.07 0.01 0.02 0.01 0.01 0.05 0.01 0.01 0.11 0.01 0.01 0.01 0.01

65% 1 0.01 0.08 0.01 0.02 0.01 0.01 0.05 0.01 0.01 0.11 0.01 0.03 0.01 0.01

70% 0.29 0.01 0.08 0.01 0.02 0.01 0.01 0.01 0.01 0.01 0.24 0.01 0.09 0.01 0.02

75% 0.2 0.01 0.08 0.01 0.02 0.53 0.01 0.01 0.07 0.01 0.35 0.02 0.21 0.01 0.03

80% 0.2 0.02 0.08 0.01 0.03 0.57 0.02 0.01 0.01 0.02 0.47 0.02 0.63 0.05 0.07

85% 0.03 0.19 0.09 0.01 0.13 0.03 0.35 0.02 0.01 0.02 0.47 0.05 0.9 0.08 0.03

90% 0.4 0.2 0.09 0.01 0.13 0.07 0.05 0.03 0.01 0.06 0.05 0.32 0.75 0.19 0.2

95% 0.4 0.65 0.09 0.01 0.03 0.05 0.07 0.05 0.01 0.21 0.21 0.66 0.71 0.19 0.2

100% 0.01 0.02 0.13 0.13 0.03 0.08 0.08 0.04 0.17 0.05 0.21 0.66 0.71 0.19 0.01

Таблица 29 – Алгоритмически найденные минимальные количества признаков, необходимых для обеспечение требуемой точности классификации для различных классов

Индекс класса (состояния/атаки)

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Требуемая точность классификации

5% 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

10% 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

15% 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

20% 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

25% 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

30% 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

35% 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1

40% 1 1 1 1 1 1 1 1.4 1 1 1 1 1 1 1

45% 1 1 1 1 1 1 1 1.4 1 1 1 1 1 1 1

50% 1 1 1 1 1 1 1 1.4 1 1 1 1 1 1 1

55% 1 1 1 1 1 1 1 1.4 1 1 1 1 1 1 1

60% 1 1 1 1 1 1 1 1.4 1 1 1 1 1 1 1

65% 1 1 1 1 1 1 1 1.4 1.2 1 1 1 1 1 1

70% 1.4 1 1 1 1 1 1 1.75 1.2 1 1 1 1 1 1

75% 1.55 1 1 1 1 1 1 1.75 1.4 1.1 1 1 1 1 1

80% 1.55 1 1 1 1.25 1 1 1.75 1.5 1.25 1.1 1 1 1 1.15

85% 1.7 1 1 1 1.45 1.35 1 1.95 1.5 1.25 1.1 1 1.1 1.2 1.2

90% 1.75 1 1 1 1.45 1.4 1.1 2 1.5 1.3 1.3 1 1.2 1.25 1.3

95% 1.75 1 1 1 1.5 1.45 1.15 2.05 1.5 1.4 1.4 1.3 1.25 1.25 1.3

100% 1.9 1.05 1 1 1.55 1.75 1.25 2.95 1.75 1.55 1.4 1.3 1.25 1.25 1.55

Необходимо заметить, что представленные на таблицах выше значения рассчитывались с учетом минимизации количества используемых признаков

классификации и носят больше демонстративный характер. При отсутствии требования на абсолютную минимизацию количества признаков или при наличии требования на обеспечение определенной точности по всем признакам данные значения могут меняться. Таким образом, необходимо руководствоваться матрицами, графические представления которых представлены на РИСУНКАХ и применять описанный выше простой алгоритм, видоизменяя его под предъявляемые требования. В целом, основная цель формирования рекомендации – обеспечение приемлемой точности при использовании наименьшего количества признаков.

3.5 Оценка результатов и практические рекомендации

Для того, чтобы произвести оценку разработанных модели профиля поведения БСС и метода и методики идентификации атак сетевого уровня на БСС, предлагается сравнить их с существующими аналогами по эффективности. Под эффективностью понимается комплекс параметров, включающих в себя количество атак, количество признаков, precision и recall.

В целом, предложенные модель профиля поведения, метод и методика идентификации показали гибкость настройки параметров и возможность удовлетворять требуемые показатели точности классификации при снижении среднего количества признаков, необходимых для ее проведения. Тем не менее, остаются несколько направлений его дальнейшего исследования и доработки. Актуальным является исследование функционирования метода на малых периодах собираемых данных и анализ динамики изменения апостериорной вероятности предполагаемого класса или присвоенных измерениям классам. Следует исследовать адаптацию разработанных метода и методики к другим методам итеративной классификации. В данной работе использовалось простейшее вычисление апостериорной вероятности классов, однако существуют более сложные методы обработки данных, показывающих лучшие результаты по сравнению с классификаторами, использующими только теорему Байеса. Не

исключено, что при применении другого вероятностного классификатора в основе алгоритма удастся сделать его более качественным.

Необходимо исследование алгоритма в динамических условиях, т.е. условиях постепенного изменения значения признакового пространства сети при переходе от нормального состояния к состоянию атаки. В данной работе использовались данные статического функционирования модели сети в заранее определенных условиях.

Оценка качества разработанной методики производилась в сравнении с существующими исследованиями. Результаты сравнения приведены в таблице 30.

Таблица 30. Сравнение результатов существующих исследований с предложенными в диссертационной работе

Автор количество признаков количество атак percision recall

I. Almomani 23 4 0,98 0,98

H. Qu 13 4 0,97 0,96

M.A. Abdullah 19 5 0,97 0,89

M. Zamani 9 1 0,96 0,95

Разработанные модель, метод

и методика 5 14 0,97 0,97

Для более наглядной визуализации было произведена суммарная оценка эффективности идентификации предложенных решений с существующими. Результаты сравнения приведены на рисунке 3.24.

В соответствии с диаграммой, можно судить о повышении эффективности идентификации атак сетевого уровня на беспроводные сенсорные сети.

В соответствии с приведенными данными можно утверждать, что эффективность идентификации атак сетевого уровня повысилось примерно на 20%.

В качестве завершающего раздела диссертационного исследования сформулированы дополнительные практические рекомендации по применению разработанных модели профиля поведения, метода и методики идентификации атак, не описанные в предыдущих пунктах.

150

Рисунок 3.23 – Сравнение эффективности разработанной методики с существующими исследованиями

Задача сбора статистической информации в реальной сети в данном исследовании не ставилась, но представляется возможным сформулировать несколько возможных вариантов:

1. Использование встроенных возможностей управляющего интерфейса.

В качестве примера можно привести 110 Telegesis Terminal, который позволяет получить некоторую статистическую информацию о работе сети.

2. Использование отдельного мобильного узла, который будет функционировать как сниффер: прослушивать сеть, не влияя на ее активность, и анализировать полученные данные о поведении сети.

3. Использование дополнительной «служебной» БСС для прослушивания и сбора данных. Однако в этом случае возникают задачи обеспечения информационной безопасности и обслуживания служебной БСС.

4. Использование протоколов или надстроек на более высоких уровнях модели OSI.

Поведение, которое является нормальным в одной сети, в другой может оказаться аномальным, например, соответствовать атаке типа «затопление». При этом процесс построения СОВ поведения много времени не занимает.

0

0,1

0,2

0,3

0,4

0,5

0,6

0,7

0,8

0,9

1

I. Almomani H. Qu M.A. Abdullah M. Zamani Разработанные

модель, метод и
методика
атаки признаки percision recall

151

Соответственно, вполне допустимо заново получать выборки данных и обучать классификаторы при изменении частотных характеристик сети или количества узлов. Эти изменения могут быть выявлены с помощью того же протокола, который используется для первичного сбора параметров сети: вовсе не обязательно прекращать его работу после сбора достаточного количества информации.

В качестве завершающего раздела диссертационной работы сформулированы практические рекомендации по применению разработанных модели профиля поведения, метода и методики идентификации атак, не описанные в предыдущих пунктах.

Задача сбора статистической информации в реальной сети в данном исследовании не ставилась, но представляется возможным сформулировать несколько возможных вариантов:

1. Использование встроенных возможностей управляющего интерфейса.

В качестве примера можно привести 110 Telegesis Terminal, который позволяет получить некоторую статистическую информацию о работе сети.

2. Использование отдельного мобильного узла-детектора [14], который будет функционировать как сниффер: прослушивать сеть, не влияя на ее активность, и анализировать полученные данные о поведении сети.

3. Использование дополнительной «служебной» БСС для прослушивания и сбора данных. Однако в этом случае возникают задачи обеспечения информационной безопасности и обслуживания служебной БСС.

4. Использование протоколов или надстроек на более высоких уровнях модели OSI.

Учитывая вышеизложенное, сформулированы следующие рекомендации к программно-аппаратной части мобильного узла:

1. возможность накопления информации: должно быть обеспечено накопление статистической информации в табличном виде (для каждого фрейма должны быть сохранены следующие поля: время передачи, размер, отправитель, получатель, характер передачи (отправлен, принят, переслан) и т.д.;

152

2. возможность проверки и подтверждения целостности информации;

3. возможность получения произвольной выборки данных. Это необходимо при учете ограничений на производительность и ресурсоемкость БСС;

4. возможность расчета средних, максимальных, минимальных и др. значений характеристик по накопленным за произвольный промежуток времени данным. Данная рекомендация также относится к ограничениям БСС, связанных с малым объемом памяти и энергоемкости;

5. возможность обнаружения аномалий в БСС. Поскольку данная работа направлена непосредственно на идентификацию атак, а процесс обнаружения аномального поведения и запуск процесса идентификации атак явно не рассматривались, предполагается использование встроенных механизмов обнаружения аномального поведения СОВ и осуществление управления процессом идентификации сетевым администратором;

6. возможность проведения аудита и сбора статистики при условии, что узлы БСС изначально не имеют функции накопления и отправки статистических сведений. Необходимо учитывать возможные настройки сети и используемые протоколы передачи данных;

7. достаточная вычислительная мощность и запас памяти. При

проектировании внешнего мобильного узла мониторинга и аудита поведения сети, необходимо обеспечить требуемую вычислительную мощность для работы алгоритмов машинного обучения и анализа данных 110 и накопления и хранения данных.

Как правило, узлы БСС реализуют на базе микроконтроллеров, так как последние обычно имеют достаточно вычислительной мощности для выполнения возлагаемых функций (сбор данных с сенсора и отправка их в сеть), в то же время имея малое энергопотребление. При этом основной вклад в энергосбережение вносит возможность узлов большую часть времени находиться в режиме сна (пониженного энергопотребления, в котором отключается большая часть функций модуля), в котором потребление узлом энергии падает на несколько порядков. За

153

счет этого достигается возможность работы от автономного источника питания на протяжении нескольких месяцев. Однако, для выполнения функции мониторинга узлу-детектору необходимо постоянно прослушивать эфир, что исключает возможность использования режима сна как способа энергосбережения.

В данном случае полагается разумным использовать другой класс вычислительных устройств, объединяющий в себе компактность и наличие аппаратных интерфейсов, присущих микроконтроллерам, и вычислительную мощь полноценных ЭВМ – одноплатные компьютеры.

Исходя из выбранных выше компонент предложена следующая модель узла-детектора, представленная на рисунке 3.24. К одноплатному компьютеру подключено специальное System-on-Chip решение – устройство-сниффер или адаптированный приемопередатчик, настроенное на рабочие каналы сети и осуществляющее мониторинг [213]. Из собранных устройством данных генерируется статистическая информация, которая записывается в СУБД. В то же время в режиме обучения или режиме анализа на компьютере работает алгоритм классификации, который соответственно обучается или анализирует собранную информацию. Результат анализа выводится через интерфейс.

Рисунок 3.24 – Модель узла-детектора

Для реализации такого узла могут быть использованы такие программно-аппаратные решения, как разработки NordicSemiconductor и модули ZigBee ETRX-357.

154

Среди средств для мониторинга и тестирования можно выделить следующие:

a. KillerBee;

b. Attify ZigBee Framework;

c. SecBee;

d. Z3sec;

e. WireShark.

Поведение, которое является нормальным в одной сети, в другой может оказаться аномальным, и, например, соответствовать атаке типа «затопление». При этом процесс построения СОВ поведения много времени не занимает [106]. Соответственно, вполне допустимо заново получать выборки данных и обучать классификаторы при изменении частотных характеристик сети или количества узлов. Эти изменения могут быть выявлены с помощью того же протокола, который используется для первичного сбора параметров сети: вовсе не обязательно прекращать его работу после сбора достаточного количества информации.

В соответствии с этим, можно представить перечень действий администратора сети, соответствующий разработанной методике для применения результатов работы:

1) анализ защищаемой сети и исследование ее характеристик;

2) настройка программной модели проведения атак на БСС в симуляторе OmNet++ с учетом характеристик защищаемой сети. Необходимо учитывать спецификацию стандарта, топологию сети, количество устройств, скорость передачи и среднее время генерации пакетов. При этом, администратор имеет возможность добавить атаки сетевого уровня, меняя в модели содержание файлов omnetpp.ini;
3) оценка информативности признаков с помощью представленного в работе ПО и составление профилей поведения сети на основе предложенной модели профиля поведения;

4) обучение классификаторов и задание параметра степени уверенности. Необходимо учитывать, что параметр степени уверенности гарантирует среднюю точность классификации, равную ему или превышающую его. Также необходимо, чтобы значение параметра степени уверенности было выше значения апостериорной вероятности нормального состояния на ~30% и нет необходимости в использовании апостериорной вероятности нормального состояния, превышающей 20%;
5) применение метода идентификации и принятие решения о соответствии результатов текущему поведению сети: предполагается совместное применение алгоритма «случайный лес» и вероятностного классификатора. В начале процесса идентификации и на малом периоде сбора данных предлагается использовать вероятностный классификатор: он позволяет с некоторой точностью на основании неполного набора признаков (от 1 в начале процесса идентификации до 5) утверждать, нормальное ли поведение у сети или же сеть находится под атакой. За время работы вероятностного классификатора накапливаются статистические данные, которые при необходимости обрабатывает алгоритм «случайный лес», при этом точность достигает 97%;
6) при получении результатов о возможной атаке рекомендуется принять меры по противодействию атаке.
Исследованный перечень атак сетевого уровня на БСС не является исчерпывающим, и предполагаются дальнейшие исследования в области идентификации и противодействия атакам на БСС.
Приведенные рекомендации позволяют с помощью поведенческого анализа обнаружить нарушения целостности и доступности информации, циркулирующей в КФС, основой которых являются БСС, и повысить эффективность идентификации сетевых атак на БСС.
В качестве перспектив дальнейшей разработки тематики следует указать исследования, связанные с развитием модели профиля поведения беспроводной сенсорной сети и доработки программной модели реализации атак на БСС для увеличения количества идентифицируемых атак и улучшения показателей

идентификации. Другим направлением является расширение и апробация разработанных модели профиля поведения, программной модели реализации атак и метода идентификации для различных сетевых протоколов в БСС. Кроме того, представляется значимой разработка методов противодействия исследованным атакам. Также возможно использование описанных в работе модели, метода и методики для разработки мобильных программно-аппаратных средств мониторинга состояния БСС.
Выводы по главе 3
В данной главе были решены следующие задачи:
1) предложена методика идентификации атак на беспроводные сенсорные сети на основе поведенческого анализа, включающая в себя разработанную модель профиля поведения беспроводной сенсорной сети, программную модель проведения атак на беспроводную сеть, программу оценки информативности, а также предложенный метод идентификации атак и

программу вычисления апостериорного распределения

2) проведена проверка работоспособности предложенных модели профиля поведения и метода идентификации для различных топологий (ячеистая сеть и кластерное дерево), характеристик беспроводной сенсорной сети (период генерации пакетов, степень случайности выбор адресов узлов назначения), изменении параметра степени уверенности и изменении априорной вероятности нормального поведения;

3) осуществлена оценка эффективности процесса идентификации атак с использованием разработанной модели профиля поведения, метода и методики идентификации на беспроводные сенсорные сети по сравнению с существующими исследованиями. Прирост эффективности составляет 20%;

4) разработаны практические рекомендации про применению модели профиля поведения, метода и методики идентификации атак на беспроводные сенсорные сети, включающие в себя варианты сбора статистической информации о поведении беспроводной сенсорной сети, рекомендации к предлагаемой

157

программно-аппаратной части системы обнаружения вторжений, набор средств тестирования и мониторинга сети и перечень действий администратора. Сформулированы перспективы области, состоящие в развитии и проработке предложенный модели, метода и методики, а также в разработке методов противодействия исследованным атакам.

158

Заключение

В диссертационной работе решена задача разработки научно-методического аппарата для идентификации атак сетевого уровня на беспроводные сенсорные сети на основе поведенческого анализа, имеющая большое значение для обеспечения информационной безопасности киберфизических систем. Основные результаты представлены ниже:

1. Рассмотрены существующие методы идентификации атак на беспроводные сенсорные сети, проведен их анализ, выявлены достоинства и недостатки данных методов. Проанализированы условия и ограничения применения каждого из методов 23 .

2. Разработана модель профиля поведения беспроводной сенсорной сети, позволяющая идентифицировать 14 атак сетевого уровня на беспроводные сенсорные сети.

3. Разработана программная модель реализации атак, позволяющая адаптировать разработанную модель к конкретным условиям и получить модельные статистические данные, что упрощает процесс обеспечения информационной безопасности беспроводных сенсорных сетей.

4. Разработан метод идентификации атак сетевого уровня на беспроводные сенсорные сети на основе анализа профиля поведения сети, использующий комбинацию алгоритмов «случайный лес» и вероятностного классификатора, обладающий более высокой точностью по сравнению с исследованными методами, использующий неполный набор признаков и позволяющий задавать необходимую точность идентифицировать атаки на беспроводные сенсорные сети.

5. Разработана методика идентификации атак на беспроводные сенсорные сети, позволяющая повысить эффективности идентификации и, соответственно, уровень защищенности беспроводных сенсорных сетей благодаря гибкой настройке на основе разработанных модели профиля поведения, программной модели проведения атак и метода идентификации атак, программы

159

подсчета информативности признаков статистической выборки и программы вычисления апостериорных распределений дискретного параметра распределения

многомерной случайной величины по статистической выборке.

Представленный научно-методический аппарат для идентификации атак сетевого уровня на беспроводные сенсорные сети на основе анализа поведения такой сети позволяет повысить эффективность идентификации атак на беспроводные сенсорные сети и может быть использован в качестве 110 основы для построения системы обнаружения вторжений.

Рекомендации по применению разработанного научно-методического аппарата для идентификации атак сетевого уровня на беспроводные сенсорные сети включают в себя указания по использованию модели профиля поведения беспроводной сенсорной сети, настройке программной модели реализации атак на беспроводные сенсорные сети и применению метода и методики идентификации атак, а также разработку подходов, направленных на повышение эффективности процесса идентификации атак. Основываясь на сформулированных рекомендациях, представляется вероятной возможность применения полученных результатов в системах обнаружения вторжений в целом и в рамках концепции кибер-физических систем в частности, так как разработанные модель профиля поведения, метод и методика идентификации позволяют обнаружить нарушения целостности и доступности информации, циркулирующей в таких системах.

В качестве перспектив дальнейшей разработки тематики следует указать исследования, связанные с развитием модели профиля поведения беспроводной сенсорной сети и доработки программной модели реализации атак на беспроводные сенсорные сети для увеличения количества идентифицируемых атак и улучшения показателей идентификации. Другим направлением является расширение и апробация разработанных модели профиля поведения, программной модели реализации атак и метода идентификации для различных сетевых протоколов в беспроводных сенсорных сетях. Кроме того, представляется значимой разработка методов противодействия исследованным атакам. Также возможно использование описанных в работе модели, метода и методики для

160

разработки мобильных программно-аппаратных средств мониторинга состояния беспроводной сенсорной сети.

Соответствие паспорту специальности. Проведенное исследование и полученные в его ходе результаты соответствуют п. 3 « Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса» и п. 14 « 16 Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности» 109 определения специальности 05.13.19 паспорта специальностей ВАК (технические науки).

161

Список сокращений и условных обозначений

БЛС - беспроводные локальные сети

БПС - беспроводные персональные сети

БСС - Беспроводные сенсорные сети

ИБ - информационная безопасность

КФС - кибер-физическая система

СВЧ – сверхвысокочастотный

СЗИ - система защиты информации

СОВ - система обнаружения вторжений

ЦП – центральный процессор

ЭВМ – электронно-вычислительная машина

CSMA/CA - Carrier-sense multiple access with collision avoidance 103

DDoS - distributed denial-of-service attack

DoS - Denial of Sleep

DSSS - direct-sequence spread spectrum

FCC – Federal Communications Commission

IEEE – Institute of Electrical and Electronics Engineers

ISM - Industrial, Scientific, and Medical

LAN - local area network

MAN - Metropolitan area network

OSI - Open Systems Interconnection

P2P - Peer-to-peer

PAN - personal area network

PHY – physical layer

POS - private operating space

RFC - Request for Comments

162

Список литературы

1. Абрамов, Е. С. Разработка модели защищенной кластерной беспроводной сенсорной сети / Е.С. Абрамов, Е.С. Басан //Известия Южного федерального университета. Технические науки. – 2013. – No. 12 (149).

2. Абрамов, Е. С. Выбор характеристик систем обнаружения атак для выработки заключения о функциональных возможностях / Е.С. Абрамов, И. Ю. Половко //Известия Южного федерального университета. Технические науки. – 2011. – Т. 125. – No. 12.

3. Ажмухамедов, И. М. Определение аномалий объема сетевого трафика на основе аппарата нечетких множеств / И.М. Ажмухамедов, А. Н. Марьенков // Вестник Астраханского государственного технического университета . — Астрахань, 2011. — No 1 (51). — С. 48—50.

4. Айвазян, С. А. Прикладная статистика: классификация и снижение размерности / С. А. Айвазян, В. М. Бухштабер, И. С. Енюков, Л. Д. Мешалкин. — М. : Финансы и статистика , 1989. — 607 с.

5. Айвазян, С. А. Теория вероятностей и прикладная статистика, 2-е издание / С. А. Айвазян, В. С. Мхитарян. Т. 1. — М. : Юнити-Дана , 2001. — 656 с.

6. Басан, А. С. Метод противодейсвитя активным атакам злоумышленника в беспроводных сенсорных сетях / А.С. Басан, Е.С. Басан, О.Б. Макаревич // Известия Южного федерального университета. Технические науки. — 2017. — No. 5 (190). С. 16—25.

7. Баскаков, С. С. Беспроводные сенсорные сети: вопросы и ответы — М. : Автоматизация в промышленности, 2008. —No 4. — С. 34—35.

8. Большаков, А. Беспроводной промышленный мониторинг / А. Большаков, В. Шашкин [Электронный ресурс]. — 2008. — URL: http://www.ipmce.ru/img/release/is_sensor.pdf (дата обращения: 29.09.2019).

9. Браницкий, А. А. Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, И. В. Котенко // Труды СПИИРАН . — 2016. —Т. 2, No 45. — С. 207—244.

163

10. Бююль, А. SPSS: искусство обработки информации. Анализ статистических данных и восстановление скрытых закономерностей / А. Бююль, П. Цефель. — СПб . : ДиаСофтЮП, 2005. — 608 с.

11. Быкова, В.В. Методы и средства анализа информативности признаков при обработке медицинских данных / В.В. Быкова, А.В. Катаева // Программные продукты и системы . – 2016. – No. 2 (114).

12. Вапник, В. Н. Восстановление зависимостей по эмпирическим данным / В. Н. Вапник. — М. : Наука , 1979. — 448 с.

13. Васильев, В. И. Обнаружение атак в локальных беспроводных сетях на основе интеллектуального анализа данных / В. И. Васильев, И. В. Шарабыров — СПб. : Известия ЮФУ. Технические науки, 2014. — No 2 (151). — С. 57—67.

14. Виноградова, М. М. Прототип модуля обнаружения сетевых атак с нечетким выводом // Дипломная работа. — СПб., 2015. — 55 с.

15. Воронцов, К.В. Машинное обучение: курс лекций // К. В. Воронцов [Электронный ресурс]. — 2010. — URL: http://www.machinelearning.ru (дата обращения : 30.09.2019).

16. Выборнова, А.И. Исследование характеристик трафика в беспроводных сенсорных сетях: Автореф. дис. канд. техн. наук . — СПб., 2014.

17. Голованова, И. С. Выбор информативных признаков. Оценка информативности // Методические указания к лабораторной работе по дисциплине «Методы обработки биомедицинских данных». — Томск , 2003. — 18 с.

18. Гришечкина, Т. А. Анализ атак на сетевые протоколы в мобильных сенсорных сетях ad hoc // Известия Южного федерального университета. Технические науки. – 2012. – Т. 137. – No. 12 (137).

19. Десницкий, В. А. Моделирование и анализ защищенности коммуникационной сети управления в чрезвычайных ситуациях на базе устройств XBEE // Региональная информатика и информационная безопасность. – 2017. – С. 221-223.

20. Долгосрочный прогноз научно-технологического развития РФ до 2030 года

164

[Электронный ресурс] — 2013. — URL: https://prognoz2030.hse.ru (visited on 23.09.2019)

21. Дядюнов, А.Н. Моделирование беспроводных сенсорных сетей / А. Н. Дядюнов, К. Н. Кузнецов — М. : Научный вестник МГТУ ГА, 2009. — No 139. — С. 63—69.

22. Журавлев, Ю.И. Об алгебраическом подходе к решению задач распознавания или классификации / Ю. И. Журавлев // Проблемы кибернетики . — 1978. — Т. 33. — С. 5—68.

23. Загоруйко, Н.Г. Прикладные методы анализа данных и знаний. / Н. Г. Загоруйко. — Новосибирск: Изд-во ИМ СО РАН, 1999. — 270 с.

24. Зубков, Е.В. Методы интеллектуального анализа данных и обнаружение вторжений / Е. В. Зубков, В. М. Белов // Вестник СибГУТИ. — Новосибирск, 2016. — No 1. — С. 118—133.

25. Колесникова, С.И. Методы анализа информативности разнотипных признаков / С.И. Колесникова // Вестник Томского государственного университета: Управление, вычислительная техника и информатика. — 2009. — No 1 (6). — С. 69—80.

26. Колмогоров, А. Н. О представлении непрерывных функций нескольких переменных суперпозициями непрерывных функций меньшего числа переменных / А. Н. Колмогоров // Докл. АН СССР . Т. 114. — 1957. — С. 953—956.

27. Кондратьев, А. А. Методологическое обеспечение интеллектуальных систем защиты от сетевых атак / А. А. Кондратьев, А. А. Талалаев, И. П. Тищенко, В. П. Фраленко, В. М. Хачумов // Современные проблемы науки и образования . — 2014. — No 2.

28. Котенко, Д.И. Методы и средства моделирования атак в больших компьютерных сетях: состояние проблемы / Д.И. Котенко, И.В. Котенко, И.Б. Саенко // Труды СПИИРАН. – 2012. – Т. 22. – No. 0. – С. 5-30.

29. Котенко, И.В. Новое поколение систем мониторинга и управления инцидентами безопасности / И.В. Котенко, И.Б. Саенко, Р.М. Юсупов // Научно-технические ведомости Санкт-Петербургского государственного

165

политехнического университета. Информатика. Телекоммуникации. Управление . – 2014. – No. 3 (198).

30. Котенко, И.В. Построение модели данных для системы моделирования сетевых атак на основе онтологического подхода / И.В. Котенко, О.В.

Полубелова, А.А. Чечулин // Труды СПИИРАН 39 . – 2013. – Т. 3. – No. 26. – С. 26-39.
31. Критерии выбора систем обнаружения и предотвращения компьютерных атак [Электронный ресурс] — 2019. — URL: https://www.coursera.org/lecture/management-informacionnoi-bezopasnosti/kritierii-vybora-sistiem-obnaruzhieniia-i-priedotvrashchieniia-komp-iutiernykh-m4L9G (дата обращения: 18.09.2019)
32. «Лаборатория Касперского»: число целевых атак на предприятия выросло на 40% [Электронный ресурс] — 2019. — URL: //cnews.ru/link/n380331 (дата обращения: 22.03.2018)
33. Литвинов, Е. Полет пчелы. Как работают сети ZigBee и как искать уязвимости в них [Электронный ресурс] — 2019. — URL: https://xakep.ru/2019/09/30/zigbee-exploits/ (дата обращения: 1.10.2019)
34. Лоднева, О.Н. Анализ трафика устройств Интернета вещей / О. Н. Лоднева, Е. П. Ромасевич — М. : Современные информационные технологии и ИТ-образование, 2018. — No 1. (дата обращения: 13.09.2019)
35. Лукацкий, А.В. Обнаружение атак / А. В. Лукацкий. — СПб. : БХВ-Петербург, 2003. — 608 с.
36. Маккинни, У. Python и анализ данных / У. Маккинни. — М. : ДМК Пресс, 2015. — 482 с.
37. Махров, С.С. Использование систем моделирования беспроводных сенсорных сетей NS 2 и OMNET++ // T-Comm-Телекоммуникации и Транспорт. – 2013. – Т. 7. – No. 10.
38. Настека, А. В. Выявление аномалий в беспроводных сенсорных сетях системы / А. В. Настека, А. Н. Канев, Е. Е. Бессонова // Научно-технический вестник информационных технологий, оптики и механики. — СПб., 2017. — Т. 17. — No 3. — С. 450—456.

39. Николенко, С.И. Байесовские классификаторы / С. И. Николенко [Электронный ресурс]. — 2004. — URL: https://logic.pdmi.ras.ru/~sergey/teaching/mlaptu11/03-classifiers.pdf. (дата обращения: 22.03.2018).
40. Норткат, С. Обнаружение нарушений безопасности в сетях, 3-е издание / С. Норткат, Д. Новак. — М. : Издательский дом «Вильямс 4 », 2003. — 448 с.
41. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 110 26 июля 2017 No 187-ФЗ // Собрание законодательства. — 2017. — No 31 (31.07). — ст. 4736.
42. Половко, И.Ю. Анализ функциональных требований к системам обнаружения вторжений / И. Ю. Половко, О. Ю. Пескова // Известия Южного федерального университета. Технические науки 4 . — 2014. — No 2 (151). — С. 86—92.
43. Прокопьев, А.В. Разработка и исследование моделей нагрузки в беспроводных сенсорных сетях: Автореф. дис. канд 47 . тех. наук. — СПб., 2012. — 19 с.
44. Проничев, А.П. Моделирование мультиагентной системы кибер-физических устройств для решения проблем управления и контроля безопасности периметра / А.П. Проничев, Л.А. Виткова // Международный научно-исследовательский журнал. – 2019. – No. 9 (87) Часть 1. – С. 14-19.
45. Пушкарев, О. Безопасная передача данных в сети ZigBee на примере радиомодулей Xbee / О. Пушкарев [Электронный ресурс]. — 2011. — URL: http://www.russianelectronics.ru/leader-r/review/2187/doc/57691/ (дата обращения: 27.09.2019).
46. Пушкарев, О. Построение Zigbee-сети на базе готовых устройств компании Digi — М. : Беспроводные технологии, 2011. — Т. 3. — No 24. — С. 74—77.
47. Рудаков, К. А. Беспроводные сенсорные сети: принципы организации, алгоритмы выбора головного узла и кластеризации // ВКР. — Челябинск, 2018. — 46 с.

48. Рыжков, А. М. Композиции алгоритмов, основанные на случайном лесе // Дипломная работа. — М., 2015. — 51 с.

49. Салим, А. А. Э. А. Разработка алгоритмов выбора головного узла в кластерных беспроводных сенсорных сетях 97 : Автореф. дис. канд. тех. наук. — СПб., 2010. — 27 с.

50. Сетевая инфраструктура системы РТЛС [Электронный ресурс]. — 2012. URL: http://www.rtlsnet.ru/technology/view/3 (дата обращения: 27.09.2019).

51. Скуснов, А. ZigBee: взгляд вглубь — М. : Компоненты и технологии, 2005. — No 4. — С. 144—148.

52. Смурыгин, И.М. Концепция организации беспроводных сенсорных сетей и их применение // Молодежный научно-технический вестник. – 2012. – No. 9. – С. 31-31.

53. Стек протоколов ZigBee 802.15.4 на платформе Freescale Semiconductor [Электронный ресурс]. — 2004. — URL: https://myprez.ru/no_category/94156 (дата обращения 26.09.2019).

54. Стренг, Г. Линейная алгебра и ее применения / Г. Стренг. — М. : Мир, 1980. — 454 с.

55. Таненбаум Э. Компьютерные сети / Э. Таннгбаум, Д. Уэзеролл — СПб.: Питер, 2013. — 960 с.

56. Тараканов, Е.В. Экспериментальные исследования протокола передачи данных с приоритетами в беспроводной сенсорной сети в системе TOSSIM // Известия Томского политехнического университета 72 . —Томск, 2012. — Т.321. — No 5. — С. 223-227.

57. Тимофеев, А. Исследование и моделирование нейросетевого метода обнаружения и классификации сетевых атак / А. Тимофеев, А. Браницкий // International Journal Information Technologies & Knowledge 18 . – 2012. – Т. 6. – No. 3. – С. 257-265.

58. Финогеев, А.Г. Оценка информационных рисков в распределенных системах обработки данных на основе беспроводных сенсорных сетей / А. А. Финогеев, А. Г. Финогеев, И. С. Нефедова // 38 Известия высших учебных заведений. Поволжский регион. Технические науки 110 . — Пенза 38 , 2016. — No 2 (38). — С. 49—60.

59. Финогеев, А.Г. // Анализ и классификация атак через беспроводные 38

168

сенсорные сети в SCADA системах / А. Г. Финогеев 38 , И. С. Нефедова, Е. А. Финогеев, В. Т. Куанг, П. В. Ботвинкин // Прикаспийский журнал: управление и высокие технологии 110 . — Астрахань, 2014. — No 1 (25). — С. 12—23.

60. Чечулин, А.А. Комбинирование механизмов защиты от сканирования в компьютерных сетях / А.А. Чечулин, И.В. Котенко // Информационно-управляющие системы 49 . – 2010. – No. 6.

61. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. — М. : ИД «Форум»: ИНФРА 4 -М, 2008. — 416 с.

62. Шахов, В.В. Моделирование воздействия атаки Black Hole / В. В. Шахов, А. Н. Юргенсон, О. Д. Соколова // Программные продукты и системы. — Тверь, 2017. — No 1. — С. 34—49.

63. Шелухин, О.И. Обнаружение аномальных вторжений в компьютерные сети статистическими методами / О.И. Шелухин, А.С. Филинова, А.В. Васина 16 —М. : T-Comm: Телекоммуникации и транспорт, 2015. — Т. 9. — No 10. — С. 42—49.

64. Шилов, И.М. Оценка аномального поведения узлов беспроводной сенсорной сети на основе статистических методов // Выпускная квалификационная работа бакалавра. Университет ИТМО. — СПб. —2017.

65. Abraham, A. Distributed intrusion detection systems: a computational intelligence approach / A. Abraham, J. Thomas // Applications of Information Systems to Homeland Security and Defense. — IGI Global, 2006. — Pp. 107–137.

66. Agarwal, B. Hybrid approach for detection of anomaly network traffic using data

mining techniques / B. Agarwal, N. Mittal // Procedia Technology. — 2012. — Vol. 6. — Pp 4 . 996–1003.

67. Ahmed, M. R. Protecting Wireless Sensor Networks from Internal Attacks / M. R. Ahmed Thesis // Faculty of Education, Science, Technology and Mathematics University of Canberra. — Canberra, Australia, 2014. — 161 p.

68. Akyildiz I. F. et al. Wireless sensor networks: a survey //Computer networks. – 2002. – T. 38. – No. 4. – C. 393-422.

69. Almomani, I. WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks / I. Almomani, B. Al-Kasasbeh, M. AL-Akhras // Journal of Sensors.

169

— 2016. — 16 p.

70. Alrajeh, N. A. Intrusion Detection Systems in Wireless Sensor Networks: A Review / N.A. Alrajeh, S. Khan, B. Shams // International Journal of Distributed Sensor Networks. — 2013. — Vol. 9, no 30 . 5. — 7 p.

71. Amini, M. Effective intrusion detection with a neural network ensemble using fuzzy clustering and stacking combination method / M. Amini, J. Rezaeenour, E. Hadavandi // Journal of Computing and Security. — 2014. — Vol. 1, no. 4. — Pp 4 . 293—305.

72. Amudha, P. Classifier Model for Intrusion Detection Using Bio-inspired Metaheuristic Approach / P. Amudha, S. Karthik, S. Sivakumari // International Journal of Computer Science and Information Technologies 28 . — Tamilnadu, India, 2014. — Pp. 7637—7642.

73. Anderson, J. P. [et al.] Computer security threat monitoring and surveillance / J. P. Anderson: tech. rep 4 . — 1980.

74. Astapov, S. Object Detection for Military Surveillance Using Distributed Multimodal Smart Sensors / S. Astapov, J.–S. Preden, J. Ehala, A. Riid // Proceedings of the 19 48 th International Conference on 48 Digital Signal Processing — IEEE. 2014. — Pp. 366—371.

75. Baghyalakshmi, D. Low Latency and Energy Efficient Routing Protocols for Wireless Sensor Networks / D. Baghyalakshmi, J. Ebenezer, S.A.V. Satya Murty // Wireless Communication and Sensor Computing, 2010. — IEEE. 2010. — Vol. 6. — Pp.45—50.

76. Baheti, R. Cyber-physical systems / R. Baheti, H. Gill //The impact of control technology. – 2011. – T. 12. – No. 1. – C. 161-166.

77. Banday, M. T. Security in Context of the Internet of Things: A Study //Cryptographic Security Solutions for the Internet of Things. – IGI Global, 2019. – C. 1-40.

78. Barati M. et al. Distributed Denial of Service detection using hybrid machine learning technique //2014 International Symposium on Biometrics and Security Technologies (ISBAST). – IEEE, 2014. – C. 268-273.

170

79. Barbara, D. Detecting novel network intrusions using bayes estimators / D. Barbara, N. Wu, S. Jajodia // In Proceedings of the 2001 SIAM International Conference on Data Mining. — SIAM. 2001. — Pp. 1–17.

80. Barford, P. Characteristics of Network Traffic Flow Anomalies / P. Barford, D. Plonka // In Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. — ACM. 2001. — Pp 4 . 69—73.

81. Baronti, P. Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards 36 / P. Pillai, V. W. C. Chook, S. Chessa, A. Gotta 36 , Y. Fun Hu // Computer Communications. — 2007. — Pp.1655— 1695.

82. Bella, G. Managing reputation over manets / G. Bella, G. Costantino, S. Riccobene // 2008 The Fourth International Conference on Information Assurance and Security 17 . – IEEE, 2008. – C. 255-260.

83. Bhojannawar, S. S. Anomaly Detection Techniques for Wireless Sensor

Networks – A Survey / S. S. Bhojannawar, C. M. Bulla, V. M. Danawade //

International Journal of Advanced Research in Computer and Communication Engineering 4 . — IEEE. 2010. — Vol. 2. — Pp. 3582—3857.

84. Bishop, C. M. Pattern recognition and machine learning / C. M. Bishop. — Springer, 2006. — 738 pp.

85. Boyce, C. A. P. A Comparison of Four Intrusion Detection Systems for Secure E-Business / C. A. P. Boyce, A. N. Zincir-Heywood // In Proceedings of the International Conference on Electronic Commerce Research. — 2003. — Pp 4 . 302—314.

86. Branitskiy, A. Network attack detection based on combination of neural, immune and neuro-fuzzy classifiers / A. Branitskiy, I. Kotenko // In Proceedings of the 18th IEEE International Conference on Computational Science and Engineering (IEEE CSE2015). — IEEE. Oct. 2015. — Pp 4 . 152— 159.

87. Breiman, L. Random Forests / L. Breiman // Machine Learning. — 2001. Vol. 45, no. 1. — Pp. 5—32.

88. Brindasri, S. Evaluation of Network Intrusion Detection Using Markov Chain / S. Brindasri, K. Saravanan // International Journal on Cybernetics & Informatics (IJCI). — 2014. — Vol. 3, no. 2. — Pp 4 . 11—20.

171

89. Chae, Y. Trust Management for Defending On-off Attacks / Y. Chae, L.C. DiPippo, Y.L. Sun // Transactions on Parallel and Distributed Systems. — IEEE.2015. — Vol. 26, no 4. — Pp. 1178—1191.

90. Chandola, V. Anomaly detection: A survey / V.Chandola, A. Banerjee, V. Kumar // ACM computing surveys (CSUR 52). – 2009. – T. 41. – No. 3. – C. 15.

91. Chandola, V. Anomaly detection 52 for discrete sequences: A survey / V.Chandola, A. Banerjee, V. Kumar // IEEE Transactions on Knowledge and Data Engineering. – 2010. – T. 24. – No. 5. – C. 823-839.

92. Chandrasekhar, A. M. Intrusion detection technique by using k-means, fuzzy neural network and SVM classifiers / A. M. Chandrasekhar, K. Raghuveer // In Proceedings of International Conference on Computer Communication and Informatics (ICCCI). — IEEE. 2013. — Pp 4 . 1—7.

93. Chaudhari, H. Wireless Sensor Networks: Security, Attacks and Challenges / H. Chaudhari, L. Kadam // International Journal of Networking. — 2011. — Vol. 1, no 1. — Pp. 4—16.

94. Cheikhrouhou, O. LNT: A Logical Neighbor Tree for Secure Group Management in Wireless Sensor Networks / A. Koubaa, G. Dini, H. Alzaid, M. Abid // Procedia Computer Science. — 2011. — Vol. 5. — Pp. 198—207.

95. Chelli, K. Security Issues in Wireless Sensor Networks: Attacks and Countermeasures / K. Chelli // Proceedings of the World Congress on Engineering. — London, UK. — 2015. — Vol. 1. — Pp. 519—524.

96. Chen, H. et al. A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation //IEEE Access. – 2019. – T. 7. – C. 32853-32866.

97. Chen, H. Task-based trust management for wireless sensor networks 17 //International Journal of Security and its applications. – 2009. – T. 3. – No. 2. – C. 21-26.

98. Cheng-tai, Y. Dynamic Recofiguration Techniques for Wireless Sensor Networks / Y. Cheng-tai // Masters Theses 1896. — 2014. — 96 p.

172

99. Comer, D. E. Internetworking with TCP/IP / D. E. Comer // Principles, Protocols, and Architecture. — 2014. — 733 p.

100. Cuomo, F. Performance analysis of IEEE 802.15. 4 wireless sensor networks: An insight into the topology formation process / F. Cuomo, E. Cipollone, A. Abbagnale // Computer Networks. — Pp. 3057—3075.

101. Cuomo, F. Topology formation in IEEE 802.15.4: cluster-tree characterization /

F. Cuomo, S. Della Luna, E. Cipollone, P. Todorova, T. Suihko // Computing and Communications. — 2008. — Pp. 276—281.

102. Debar, H. Towards a taxonomy of intrusion-detection systems / H. Debar, M. Dacier, A. Wespi // Computer Networks. — 1999. — Vol. 31, no. 8. — Pp. 805— 822.

103. Denning, D. E. An intrusion-detection model / D. E. Denning // IEEE Transactions on software engineering 4 . — IEEE.1987. — no. 2. — Pp. 222— 232.

104. Dharamkar, B. A Review of Cyber Attack Classification Technique Based on Data Mining and Neural Network Approach / B. Dharamkar, R. Ranjan Singh // International Journal of Computer Trends and Technology. — Bhopal, India, 2014. — Vol. 7, no. 2. — Pp. 100—105.

105. Drozda, M. Bio-inspired error detection for complex systems / M. Drozda, I. Bate, J. Timmis //2011 IEEE 17th Pacific Rim International Symposium on Dependable Computing. – IEEE, 2011. – С. 154-163.

106. Ennert, M. Testing of IDS model using several intrusion detection tools / M. Ennert 4 , E. Chovancova, Z. Dudlakova // Journal of Applied Mathematics and Computational Mechanics. — 2015. — Vol. 14, no. 1. — Pp 4 . 55—62.

107. Fan, Z. Bayesian analysis / Z. Fan [Электронный ресурс]. — 2016. — URL: https://stats200.stanford.edu/Lecture20.pdf (visited on 22.03.2018).

108. Farid, D. Md. Adaptive Network Intrusion Detection Learning: Attribute Selection and Classification / D. Md. Farid, J. Darmont, N. Harbi, N. Huu Hoa, M. Z. Rahman // International Journal of Computer and Information Engineering. — Bangkok, Thailand, 2009. — Vol. 3, no. 12. — 5 p.

109. Framingham, Mass. IDC Forecasts Worldwide Spending on the Internet of Things to Reach $745 Billion in 2019, Led by the Manufacturing, Consumer,

Transportation, and Utilities Sectors [Электронный ресурс] — 2019. — URL: https://www.idc.com/getdoc.jsp?containerId=prUS44596319 (visited on 25.09.2019)

110. Galar, M. An overview of ensemble methods for binary classifiers in multi-class problems: Experimental study on one-vs-one and one-vs-all schemes / M. Galar 4 , A. Fernandez, E. Barrenechea, H. Bustince, F. Herrera // Pattern Recognition. — 2011. — Vol. 44, no. 8. — Pp 4 . 1761—1776.

111. Ganeriwal, S. Reputation-based framework for high integrity sensor networks 10 / S. Ganeriwal, L. Balzano., M. Srivastava 10 //ACM Transactions on Sensor Networks (TOSN). – 2008. – Т. 4. – No. 3. – С. 15.

112. Garg, A. Understanding Probabilistic Classifiers / A. Garg, D. Roth // Machine Learning: ECML 2001. ECML 2001. Lecture Notes in Computer Science. — Springer, Berlin, Heidelberg 75 , 2001. — Vol. 2167. — Pp. 179–191.

113. Ghorbani, A. A. Network intrusion detection and prevention: concepts and techniques / A. A. Ghorbani, W. Lu, M. Tavallaee. Vol. 47. — Springer Science & Business Media 4 , 2009. — 212 p.

114. Govindarajan, M. Intrusion detection using an ensemble of classification methods / M. Govindarajan, R. M. Chandrasekaran // In Proceeding of the World Congress on Engineering and Computer Science. Vol 4 . 1. — 2012. — Pp 20 . 459—464.

115. Gupta, A. Exploiting ZigBee and BLE //The IoT Hacker's Handbook. – Apress, Berkeley, CA, 2019. – Pp. 265-309.

116. Gupta, A. Performing an IoT Pentest //The IoT Hacker's Handbook. – Apress, Berkeley, CA, 2019. – Pp. 17-37.

117. Hać, A. Wireless Sensor Network Designs / A. Hać // John Wiley & Sons Ltd. — Chichester, United Kingdom, 2003. — I. 1. — 410 p.

118. Haddadi, F. Wireless Intrusion Detection System Using a Lightweight Agent 17 / F. Haddadi, M. A. Sarram // Second International Conference on Computer and Network Technology. — Bangkok, Thailand, 2010. — Pp 17 . 84—87.

119. Hall, J. Anomaly-based intrusion detection using mobility profiles of public transportation users / J. Hall, M. Barbeau, E. Kranakis // WiMob'2005), IEEE

International Conference on Wireless And Mobile Computing, Networking And Communications 17 , 2005. – IEEE, 2005. – T. 2. – C. 17-24.

120. Han, H. Using data mining to discover signatures in network-based intrusion detection 17 / H. Han, X.L. Lu, L.Y. Ren 17 // Proceedings. International Conference on Machine Learning and Cybernetics. – IEEE, 2002. – T. 1. – C. 13-17.

121. Hastie, T. The Elements of Statistical Learning / T. Hastie, R. Tibshirani, J. Friedman // Springer 69 -Verlag. — New York, USA, 2009. — I. 2. — 763 p.

122. He, H.-T. Detecting anomalous network traffic with combined fuzzy-based approaches / H.-T. He, X.-N. Luo, B.-L. Liu // Advances in Intelligent Computing. — 2005. — Pp 4 . 433—442.

123. Hodo, A. Shallow and Deep Networks Intrusion Detection System: A Taxonomy and Survey / Bellekens, A. Hamilton, C. Tachtatzis, R. Atkinson [Электронный ресурс]. — 2017. — URL: https://www.semanticscholar.org/ paper/Shallow-and-Deep-Networks-Intrusion-Detection-A-and-Hodo-Bellekens/193a4f04b007840571c96ac9b84b09f215063c97 (visited on 26.09.2019).

124. Hu, H. Security Metric Methods for Network Multistep Attacks Using AMC and Big Data Correlation Analysis / H. Hu, Y. Liu, H. Zhang, and Y. Zhang // Security and Communication Networks. — 2018. — Vol. 2018. — 14 p.

125. Huang, H. A Remote Home Security System Based on Wireless Sensor Network and GSM Technology / H. Huang, S. Xiao, X. Meng, Y. Xiong // NSWCTC 2010 – The 2nd International Conference on Networks Security, Wireless Communications and Trusted Computing. — IEEE 19 .2010. — Pp. 535—538.

126. Hur, J. et al. Trust management for resilient wireless sensor networks //International Conference on Information Security and Cryptology. – Springer, Berlin, Heidelberg, 2005. – C. 56-68.

127. Hussain, J. Designing a Data Cube for NSL-KDD data set to improve the quality of network intrusion detection / J. Hussain, P. Kalita // International Conference on Frontiers in Mathematics (Gauhati University). — Guwahati, Assam, India. — Pp. 78—81.

128. IEEE 802.15.4 – 2015. IEEE Standard for Low-Rate Wireless Networks. — Введ. 22.04.2016. — Piscataway, IEEE: 2016. — 709 p.

129. Ioannis, K.Towards intrusion detection in wireless sensor networks / K. Ioannis, T. Dimitriou, F.C. Freiling // Proc. of the 13th European Wireless Conference. – 2007. – C. 1-10.

130. Izadi, D. Enhancing Wireless Sensor Networks Functionalities / D. Izadi [Электронный ресурс]. —2014. — URL: — http://dro.deakin.edu.au/eserv/DU:30072876/izadi-enhancingwireless-2014A.pdf (visited on 26.09.2019).

131. Jabbar, M. A. Cyber Physical Systems for Smart Cities Development / M. A. Jabbar, S. Samreen, R. A. D. K. K. Reddy // International Journal of Engineering & Technology. – 2018. – T. 7. – No. 4.6. – C. 36-38.

132. Jinhui, X. et al. Intrusion detection system for hybrid DoS attacks using energy trust in wireless sensor networks //Procedia computer science. – 2018. – T. 131. – C. 1188-1195.

133. Jyothsna, V. A review of anomaly based intrusion detection systems / V. Jyothsna, V. R. Prasad, K. M. Prasad // International Journal of Computer Applications. — 2011. — Vol. 28, no. 7. — Pp 4 . 26—35.

134. Kanwar, A. ZigBee: The New Bluetooth Technology / A. Kanwar, A. Khazanchi // International Journal of Engineering and Computer Science. — 2012. — Vol. 1, no 2. — Pp. 67—74.

135. Karlof 19 , C. Secure routing in wireless sensor networks: Attacks and countermeasures 19 / C. Karlof, D. Wagner // Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications 30 , 2003. – IEEE, 2003. – C. 113-127.

136. Karlof, C TinySec: a link layer security architecture for wireless sensor networks / C. Karlof, N. Sastry, D. Wagner // Proceedings of the 2nd international conference on Embedded networked sensor systems . – ACM, 2014. – C. 162-175.
137. Kaur, M. Detection and Mitigation of Sinkhole Attack in Wireless Sensor Network / M. Kaur, A. Singh // Proceedings – 2016 International Conference on Micro-

Electronics and Telecommunication Engineering, ICMETE 2016. — IEEE. 2016. — Pp. 217— 221.
138. Kalkha, H. Preventing Black Hole Attack in Wireless Sensor Network Using HMM / H. Kalkha, H. Satori, K. Satori // Procedia computer science. – 2019. – T. 148. – C. 552-561.
139. Kalnoor, G. Pattern matching intrusion detection technique for Wireless Sensor Networks / G. Kalnoor, J. Agarkhed //2016 2nd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB). – IEEE, 2016. – C. 724-728.
140. KDD Cup 1999 Data [Электронный ресурс] — 1999. — URL: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99 (дата обращения: 27.09.2019)
141. Keller, F. Naive Bayes Classifiers / F. Keller [Электронный ресурс]. — 2003. — URL: http://www.coli.uni-saarland.de/~crocker/Teaching/Connectionist/lecture10_4up.pdf (visited on 24.03.2018).
142. Khan, M.A. Challenges for security in Wireless sensor networks (WSNs) / M.A. Khan, G.A. Shah, M. Sher. // International Journal of Computer and Information Engineering. — 2011. —Vol. 5, no 8. — Pp. 848—854.
143. Kim, S. S. Statistical techniques for detecting traffic anomalies through packet header data / S. S. Kim, A. Reddy // IEEE/ACM Transactions on Networking (TON). — 2008. — Vol. 16, no. 3. — Pp . 562—575.
144. Kolias, C. Intrusion Detection in 802.11 Networks: Empirical Evaluation of Threats and a Public Dataset / C. Kolias, G. Kambourakis, A. Stavrou, S. Gritzalis // IEEE Communications Surveys & Tutorials. — IEEE. 2016. — Vol. 18, no. 1— Pp. 184—208.
145. Kotenko, I. A cyber attack modeling and impact assessment framework / I. Kotenko, A. Chechulin //2013 5 th International Conference on Cyber Conflict (CYCON 2013). – IEEE, 2013. – C. 1-24.
146. Kruegel, C. Using decision trees to improve signature-based intrusion detection / C. Kruegel, T. Toth // In Proceedings of the 6th International Workshop on the Recent Advances in Intrusion Detection. — Springer, 2003. — Pp . 173–191.

147. Kumar, V. Wireless Sensor Networks: Security Issues, Challenges and Solutions / V. Kumar, A. Jain, P.N. Barwal // International Journal of Information & Computation Technology. — 2014. — Vol. 4, no 8. — Pp. 859— 868.
148. Lewis, F. L. Wireless Sensor Networks / F.L. Lewis // Smart Environments. — Hoboken, NJ, 2005. Pp. 11—46.
149. Lorena, A. C. A review on the combination of binary classifiers in multiclass problems / A. C. Lorena, A. C. De Carvalho, J. M. Gama // Artificial Intelligence Review. — 2008. — Vol. 30, no. 1. — Pp . 19—37.
150. Ma, Y. The intrusion detection method based on game theory in wireless sensor network / Y. Ma, H. Cao, J. Ma //2008 First IEEE International Conference on Ubi-Media Computing. – IEEE, 2008. – C. 326-331.
151. Mahoney, M. An analysis of the 1999 DARPA/Lincoln Laboratory evaluation data for network anomaly detection / M. Mahoney, P. Chan // In Proceedings of the 6th International Symposium on Recent advances in intrusion detection (RAID 2003). — Springer, 2003. — Pp. 220—237.
152. McHugh, J. Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by Lincoln laboratory / J.

McHugh // ACM Transactions on Information and System Security (TISSEC). — 2000. — Vol. 3, no. 4. — Pp 4 . 262—294.
153. Mitchell, R. A survey of intrusion detection in wireless network applications 17 / R. Mitchell, I.-R. Chen // Computer Communications. — 2014. — Vol. 42. — Pp. 1—23.
154. Mo Y. et al. Cyber–physical security of a smart grid infrastructure //Proceedings of the IEEE. – 2011. – T. 100. – No. 1. – C. 195-209.
155. Mourabit, Y. Intrusion Detection Techniques in Wireless Sensor Network using Data Mining Algorithms: Comparative Evaluation Based on Attacks Detection / Y. Mourabit, A. Toumanari, A. Bouirden, N. Moussaid // International Journal of Advanced Computer Science and Application. —Agadir, Morocco, 2015. — Vol. 6, no. 9. — Pp. 164—172.
156. Mouradian, A. Formal Verification of Real-Time Wireless Sensor Networks Protocols with Realistic Radio Links / A. Mouradian, I. Augé-Blum // RTNS '13

Proceedings of the 21 48 st International conference on 48 Real-Time Networks and Systems. 2013. — Pp. 213 — 222.
157. Nadir, I. et al. An Auditing Framework for Vulnerability Analysis of IoT System //2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). – IEEE, 2019. – C. 39-47.
158. Neuman, C. Challenges in security for cyber-physical systems 36 //DHS workshop on future directions in cyber-physical systems security. – 2009. – C. 22-24.
159. Oluwasanya, P. Anomaly Detection in Wireless Sensor Networks / P. Oluwasanya [Электронный ресурс]. — 2017. — URL: https://arxiv.org/abs/1708.08053 (дата обращения 25.09.2019).
160. OMNeT++ simulatiom manual [Электронный ресурс]. — 2018. — URL: https://omnetpp.org/doc/omnetpp/manual/ (дата обращения 27.09.2019).
161. Omrani, T. Fusion of ANN and SVM Classifiers for Network Attack Detection / T. Omrani, A. Dallali, B. Chibani Rhaimi, J. Fattahi // 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering. —IEEE. 2017. — Pp. 374-377.
162. Onat, I. An intrusion detection system for wireless sensor networks 17 / I. Onat, A. Miri //WiMob'2005), IEEE International Conference on Wireless And Mobile Computing, Networking And Communications 17 , 2005. – IEEE, 2005. – T. 3. – C. 253-259.
163. Othman, M.F. Wireless Sensor Network Applications: A Study in Environment Monitoring System / M. F. Othman, K. Shazali // Procedia Engineering. — 2012. – Vol. 41. — Pp. 1204—1210.
164. Panousopoulou, A. Feature Selection for Performance Characterization in Multi-hop Wireless Sensor Networks / A. Panousopoulou, M. Azkune, P. Tsakalides // Ad Hoc Networks. — 2016. — Vol. 49. — Pp. 70—89.
165. Pathan, A. S. K. Security in Wireless Sensor Networks: Issues and Challenges 30 / A. S. K. Pathan, H.-W. Lee, C. S. Hong // The 8th International Conference on Advanced Communication Technology 28 . — IEEE.2006. —Vol.3. — Pp. 1043—1048.

166. Pathan A. S. K. (ed.). Security of self-organizing networks: MANET, WSN, WMN, VANET. — CRC press, 2016. — 595 p.
167. Patil, S. Security Issues and Challenges in Wireless Sensor Networks / S. Patil, P. Lilhare // Proceedings of Recent Advances in Interdisciplinary Trends in Engineering & Applications (RAITEA) – 2019.
168. Paxson, V. Bro: a system for detecting network intruders in real-time / V. Paxson // Computer networks. — 1999. — Vol. 31, no. 23. — Pp 4 . 2435–2463.
169. Pedregosa, F. et al. Scikit-learn: Machine learning in Python //Journal of machine learning research. – 2011. – T. 12. – No. Oct. – C. 2825-2830.
170. Petersen, R. Data Mining for Network Intrusion Detection / Independent degree

project - first cycle Bachelor's thesis // Mid Sweden University, Department of Information and Communication Systems. — Sundsvall and Östersund, Sweden, 2015. — 61 p.

171. Porras, P. A. EMERALD: Event monitoring enabling response to anomalous live disturbances / P.A. Porras, P.G. Neumann // Proceedings of the 20th national information systems security conference . – 1997. – T. 3. – C. 353-365.

172. Ptacek, T. H. Insertion, evasion, and denial of service: Eluding network intrusion detection / T. H. Ptacek, T. N. Newsham: tech. rep. / SECURE NETWORKS INC CALGARY ALBERTA . — 1998.

173. Qu, H. An Adaptive Intrusion Detection Method for Wireless Sensor Networks / H. Qu, Z. Qiu, X. Tang, M. Xiang, P. Wang // International Journal of Advanced Computer Science and Applications . — Chongqing, China, 2017. — Vol. 8, no. 11. — Pp. 27—36.

174. Raymond, D.R. Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols / D.R. Raymond, R. C. Marchany, M. I. Brownfield , S. F. Midkiff // IEEE Transactions on Vehicular Technology. — IEEE. 2009. — Vol. 58, no 1. — Pp. 367— 380.

175. Roy, A. K., Khan A. K. Architectural and Security Prospective of Wireless Mesh Network //International Journal of Computational Intelligence & IoT. – 2019. – T. 2. – No. 1.

180

176. Rødfoss, J. T. Comparison of open source network intrusion detection systems / J. T. Rødfoss: MA thesis / Rødfoss, Jonas Taftø. — University of Oslo, Department of Informatics , 2011. — 85 p.

177. Sen, J. A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks / M. G. Sandra, S. G. Harihara, H. Reddy, B. Purushothaman // 2007 6th International Conference on Information, Communications & Signal Processing. — IEEE. 2007. — Vol. 53, no 16.

178. Sheth, A. MOJO: A Distributed Physical Layer Anomaly Detection System for 802.11 WLANs / C. Doerr, D. Grunwald, R. Han, D. Sicker // Conference: Proceedings of the 4 th International Conference on Mobile Systems, Applications, and Services (MobiSys 2006). — Uppsala, Sweden, 2006. — Pp. 191— 204.

179. Siddesh G. M. et al. (ed.). Cyber-Physical Systems: A Computational Perspective. — CRC Press, 2015.

180. da Silva A. P. R. et al. Decentralized intrusion detection in wireless sensor networks // Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks . – ACM, 2005. – C. 16-23.

181. Singh, V.P. Hello Flood Attack and its Countermeasures in Wireless Sensor Networks / V.P. Singh, S. Jain, J. Singhai // International Journal of Computer Science Issues. — 2010. — Vol. 7, no 3. — Pp . 23–27.

182. Sohraby, K. Wireless Sensor Networks: Technology, Protocols, and Applications / K. Sohraby, D. Minoli, T. Znati // John Wiley & Sons, Inc. — New York, USA, 2007. — 308 p.

183. Sommer, R. Outside the closed world: On using machine learning for network intrusion detection / R. Sommer, V. Paxson // In Proceedings of the IEEE Symposium on Security and Privacy. — IEEE. 2010. — Pp . 305–316.

184. Stankovic, J. A. Realistic Applications for Wireless Sensor Networks / J.A. Stankovic, A.D. Wood, T. He // Theoretical Aspects of Distributed Computing in Sensor Networks. Monographs in Theoretical Computer Science. An EATCS Series. — Springer, Berlin, Heidelberg , 2011. — Pp. 835 —863.

181

185. Syed, D. et al. Security for Complex Cyber-Physical and Industrial Control Systems: Current Trends, Limitations, and Challenges // PACIS. — 2017. — C. 180.

186. Tao, Z. Wireless Intrusion Detection: Not as easy as traditional network intrusion detection / Z. Tao, A.B. Ruighaver //TENCON 2005-2005 IEEE Region 10 Conference.

– IEEE, 2005. – С. 1-5.

187. Tartakovsky, A. Sequential Analysis: Hypothesis Testing and Changepoint Detection / A. Tartakovsky, I. Nikiforov, M. Basseville. // Chapman and Hall/CRC. — New York, USA, 2014. — 603 p.

188. The Bro Network Security Monitor. Load Balancing [Электронный ресурс]. — 2011. — URL: https://www.bro.org/documentation/load-balancing.html (visited on 28/09/2019).

189. The Evolution of Wireless Sensor Networks [Электронный ресурс]. — 2015. — URL: https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf (visited on 15.03.2018).

190. Tokdar, S. T. Choosing a Prior Distribution / S. T. Tokdar [Электронный ресурс]. — 2013. — URL: https://www2.stat.duke.edu/courses/Spring13/sta732.01/priors.pdf (visited on 24.03.2018).

191. Ubiquitous Sensor Network HBE-ZigbeX II [Электронный ресурс]. — 2015. — URL: http://www.hanback.co.kr/board/download_file.php?ASN=138_1452376260&BDN=BD1142&IDX=6 (visited on 27.02.2018).

192. Vermaa, A. Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection Systems using Distance-based Machine Learning / A. Vermaa, V. Rangaa // Procedia Computer Science. — Kurukshetra, India, 2018. — Pp. 709—716.

193. Walters J. P. et al. Wireless sensor network security: A survey //Security in distributed, grid, mobile, and pervasive computing . – 2007. – Т. 1. – С. 367.

194. Werbos, P. J. Beyond regression: New tools for prediction and analysis in the behavioral sciences / P. J. Werbos: PhD thesis / Werbos, Paul John. — Harvard University, MA, 1974.

195. White , G. B. Cooperating security managers: A peer-based intrusion detection system / G.B. White., E.A. Fisch, U.W. Pooch // IEEE network. – 1996. – Т. 10. – No. 1.

182

– С. 20-23.

196. White, J. S. Quantitative analysis of intrusion detection systems: Snort and Suricata / J. S. White, T. Fitzsimmons, J. N. Matthews // SPIE Defense Security and Sensing Cyber Security Conference. — 2013. — Vol . 8757.

197. Wolf W. H. Cyber-physical systems //IEEE Computer. – 2009. – Т. 42. – No. 3. – С. 88-89.

198. Wyglinski, A. M. Security of autonomous systems employing embedded computing and sensors / A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T.R. Eisenbarth. — IEEE. 2013. — no. 6504448. — Pp. 80—86.

199. Xiao, Z. An anomaly detection scheme based on machine learning for WSN / Z. Xiao, C. Liu, C. Chen // 2009 First International Conference on Information Science and Engineering. – IEEE, 2009. – С. 3959-3962.

200. Yinbiao, S. Internet of Things: Wireless Sensor Network / S. Yinbiao [Электронный ресурс]. — 2014. — URL: http://www.iec.ch/whitepaper/pdf/ iecWP-internetofthings-LR-en.pdf (visited on13.03.2018).

201. Zamani, M. et al. A DDoS-aware IDS model based on danger theory and mobile agents //2009 International Conference on Computational Intelligence and Security . – IEEE, 2009. – Т. 1. – С. 516-520.

202. Zhang, J. Network Intrusion Detection using Random Forests / J. Zhang, M. Zulkernine // Twelfth International Multi-Conference on Information Processing-2016 (Queen's University). — Ontario, Canada, 2016. — Pp. 213—217.

203. Zheng, J. A comprehensive performance study of IEEE 802.15.4, in: Sensor Network Operations / J. Zheng, M. J. Lee. — IEEE. 2006. — Pp. 218 —237.

204. Zhong, S. Clustering Approach to Wireless Network Intrusion Detection / S. Zhong, T. M. Khoshgoftaar, S. V. Nath // Proceedings of the 17 th IEEE International Conference on Tools with Artificial Intelligence (ICTAI '05). —IEEE. 2005. — Pp. 189—196.

205. Zhu, H. et al. Detection of selective forwarding attacks based on adaptive learning automata and communication quality in wireless sensor networks 28 183 //International Journal of Distributed Sensor Networks 28 . – 2018. – Т. 14. – No. 11. – С. 1550147718815046.
206. Zia, T. Security issues in wireless sensor networks / T. Zia, A. Zomaya //2006 International Conference on Systems and Networks Communications (ICSNC 19 '06). – IEEE, 2006. – С. 40-40.
207. ZigBee Alliance [Электронный ресурс] — 2005. — URL: https://zigbee.org (visited on 2.06.2019)
208. ZigBee Specification 053474r20. ZigBee Specification. — 19.09.2012. — San Ramon, ZigBee Standards Organization. — 622 p.
209. Zillner, T. Zigbee exploited. The good, the bad and the ugly / Tobias Zillner // Cognosec. — Vienna, Austria, 2015. — 8 p.
210. Коржук, В.М. Введение параметра степени уверенности в процесс идентификации атак на киберфизические системы / В. М. Коржук, А. В. Грозных, Д. А. Заколдаев // Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки 110 ». — 2019. — No10. — С. 57-64.
211. Коржук, В. М. Идентификация атак на беспроводные сенсорные сети на основе анализа аномального поведения сети / В.М. Коржук, П. Бонковски // Научно-технический вестник Поволжья. — 2018. — No 2. — С. 83-85.
212. Коржук, В.М. Методика идентификации атак на беспроводные сенсорные сети на основе анализа поведения сети Современная наука: актуальные проблемы теории и практики. Серия «Естественные и технические науки 110 » (в печати). — 2019. — No11.
213. Коржук, В. М. Обеспечение информационной безопасности каналов связи на основе многофункционального специализированного программно-аппаратного решения 25 / М. Е. Сухопаров, И. С. Лебедев, И. Е. Кривцова, С. А. Печеркин // Проблемы информационной безопасности. —2016. — No 2. — С. 70—74.
214. Korzhuk, V. M. Formalization of the Feature Space for Detection of Attacks on Wireless Sensor Networks / I.A. Zikratov, V. Korzhuk, I. Shilov, A. Gvozdev // 2017 20th Conference of Open Innovations Association (FRUCT). — IEEE. 2017. — Pp. 526—533.

215. Korzhuk, V. M. Identification of Attacks against Wireless Sensor Networks Based on Behaviour Analysis / V. M. Korzhuk, A. Groznykh, A. Menshikov, M. Strecker // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications 20 . — Saint-Petersburg, 2019. — Vol. 10, no. 2. — Pp. 1—21.
216. Korzhuk V. Reduction of the Feature Space for the Detection of Attacks of Wireless Sensor Networks / V. Korzhuk, I. Shilov, J. Torshenko // 2017 20th Conference of Open Innovations Association (FRUCT). — IEEE, 2017. – Pp. 195—201.
217. Korzhuk, V. M. The Analysis of Abnormal Behavior of the System Local Segment on the Basis of Statistical Data Obtained from the Network Infrastructure Monitoring 25 / I. S. Lebedev, I. E. Krivtsova, V. M. Korzhuk, N. Bazhayev, M. E. Sukhoparov, S. Pecherkin, K. Salakhutdinova 25 // Lecture Notes in Computer Science. — Saint-Petersburg, 2016. — Vol. 9870. — Pp. 503—511.
218. Korzhuk V. M. The Estimation of Secure Condition of Multi-Agent Robotic System in Case of Information Influence on the Single Element 25 / I. A. Zikratov, I. S. Lebedev, V. M. Korzhuk 25 // Proceedings of the 17th Conference of Open Innovations Association FRUCT 14 . — Yaroslavl, 2015. — Pp. 362— 367.
219. Korzhuk, V. M. The Model of the Attack Implementation on Wireless Sensor Networks / V. M. Korzhuk, I. Krivtsova, I. Shilov // 2017 20th Conference of Open Innovations Association (FRUCT). — IEEE. 2017. — Pp. 187—194.

220. Korzhuk, V. M. The Monitoring of Information Security of Remote Devices of Wireless Networks 25 / I. S.Lebedev, V. M. Korzhuk // Lecture Notes in Computer Science. — Saint-Petersburg, 2015. — Vol. 9247. — Pp. 3—10.

221. Korzhuk, V. M. Using Preventive Measures for the Purpose of Assuring Information Security of Wireless Communication Channels 25 / V. M. Korzhuk, I. E. Krivtsova, K. Salakhutdinova, M. E. Sukhoparov, D. Tikhonov 25 // Proceedings of the 18th Conference of Open Innovations Association FRUCT 14 . —- Saint-Petersburg, 2016. — Pp. 167—173.

Приложение А Модель угроз и нарушителя для БСС

Таблица 31 – Модель угроз и нарушителя для БСС

No	Код	Название	Описание	Обусловлена	Условия реализации	Объект воздействия	Источник(и) и потенциал	Вероятность реализации	Опасность реализации	Актуальность	Последствия реализации
1	УБИ .003	Угроза анализа 7 криптографических алгоритмов и их реализации	Угроза заключается в возможности выявления слабых мест в криптографических алгоритмах или уязвимостей в реализующем их программном обеспечении. 1 слабостями криптографических алгоритмов, а также ошибками в программном коде криптографических средств, их сопряжении с системой или параметрах их настройки.	в 1 случае наличия у нарушителя сведений об применяемых в системе средствах шифрования, реализованных в них алгоритмах шифрования и параметрах их 1 настройках	Метаданные,						

системное
программное
обеспечение
Внешний
нарушитель со
средним
потенциалом
Средняя Низкая Средняя Нарушение
конфиденциа
льности
Нарушение
целостности
2 УБИ
.006

Угроза
внедрения
кода или
данных
Угроза заключается в
возможности внедрения
нарушителем в
дискредитируемую
информационную систему
или IoT-устройство
вредоносного кода, который
может быть в дальнейшем
запущен «вручную»
пользователями,
автоматически при
выполнении определённого
условия (наступления
определённой даты, входа
пользователя в систему и
т.п.) или с использованием
аутентификационных
данных, заданных «по
умолчанию», а также в
возможности
несанкционированного
внедрения нарушителем
некоторых собственных
данных для обработки в
дискредитируемую
информационную систему,
фактически осуществив
незаконное использование
чужих вычислительных
ресурсов, и блокирования
работы устройства при
выполнении определенных
команд. 1
наличием уязвимостей
программного обеспечения;
слабостями мер
антивирусной защиты и

разграничения доступа; 5

наличием открытого Telnet-

порта на IoT-устройстве

(только для IoT-устройств).

в 5 случае работы

дискредитируемого

пользователя с файлами,

поступающими из

недоверенных источников;

при наличии у 5 него 9

привилегий установки

программного обеспечения;

в случае неизмененных

владельцем учетных

данных IoT-устройства

(заводских пароля и

логина) 5

Системное

программное

обеспечение,

прикладное

программное

обеспечение,

сетевое

программное

обеспечение 7

Внешний

нарушитель с

низким

потенциалом 7

Средняя Высокая Высокая Нарушение

конфиденциа

льности

Нарушение

целостности

Нарушение

доступности

3 УБИ Угроза Угроза заключается в слабостью технологий при условии подключения Сетевой узел Внутренний Высокая Высокая Высокая Нарушение

186

.011 деавториза

ции

санкциони

рованного

клиента

беспроводн

ой сети

возможности

автоматического разрыва

соединения беспроводной

точки доступа с

санкционированным

клиентом беспроводной сети. 1

сетевого взаимодействия по

беспроводным каналам

передачи данных –
сведения о MAC-адресах
беспроводных клиентов
доступны всем участникам
сетевого взаимодействия. 1
нарушителем к
беспроводной сети
устройства, MAC-адрес
которого будет полностью
совпадать с MAC-адресом
дискредитируемого
санкционированного
клиента 1
нарушитель с
низким
потенциалом
Внешний
нарушитель с
низким
потенциалом 7
доступности
4 УБИ
.023
Угроза
изменения
компонент
ов системы
Угроза заключается в
возможности получения
нарушителем доступа к сети
Интернет (при его отсутствии
в системе), к хранимым на
личных мобильных
устройствах файлах,
внедрения закладок и т.п.
путём несанкционированного
изменения состава
программных или
аппаратных средств
информационной системы,
что в дальнейшем позволит
осуществлять данному
нарушителю (или другому –
внешнему, обнаружившему
несанкционированный канал
доступа в систему)
несанкционированные
действия в данной системе. 1
слабостями мер контроля за
целостностью аппаратной
конфигурации
информационной системы. 1
при условии успешного
получения нарушителем
необходимых полномочий в

системе 1
Информацион
ная система,
сервер,
рабочая
станция,
виртуальная
машина,
системное
программное
обеспечение,
прикладное
программное
обеспечение,
аппаратное
обеспечение 7
Внутренний
нарушитель с
низким
потенциалом 7
Средняя Высокая Высокая Нарушение
целостности
Нарушение
доступности
5 УБИ
.034
Угроза
использова
ния

слабостей
протоколов
сетевого/ 2 ло
кального

обмена
данными 2
Угроза заключается в
возможности осуществления
нарушителем
несанкционированного
доступа к передаваемой в
системе защищаемой
информации за счёт
деструктивного воздействия
на протоколы
сетевого/локального обмена
данными в системе путём
нарушения правил
использования данных
протоколов. 1
слабостями самих
протоколов (заложенных в
них алгоритмов),
ошибками, допущенными в
ходе реализации
протоколов, или

уязвимостями,
внедряемыми
автоматизированными
средствами
проектирования/разработки
.
в 1 случае наличия слабостей
в протоколах
сетевого/локального обмена
данными 1
Системное
программное
обеспечение,
сетевое
программное
обеспечение,
сетевой
трафик 7
Внутренний
нарушитель с
низким
потенциалом
Внешний
нарушитель с
низким
потенциалом 7
Средняя Низкая Средняя Нарушение
конфиденциа
льности
6 УБИ
.069
Угроза
неправоме
рных
действий в
каналах
связи
Угроза заключается в
возможности внесения
нарушителем изменений в
работу сетевых протоколов
путём добавления или
удаления данных из
информационного потока с
целью оказания влияния на 1
слабостями сетевых
протоколов,
заключающимися в
отсутствии проверки
целостности и подлинности
получаемых данных. 1
при условии осуществления
нарушителем
несанкционированного
доступа к сетевому трафику 1

Сетевой

трафик

Внешний

нарушитель с

низким

потенциалом 5

Средняя Высокая Высокая Нарушение

конфиденциа

льности

Нарушение

целостности

187

работу дискредитируемой

системы или получения

доступа к конфиденциальной

информации, передаваемой

по каналу связи.

7 1 УБИ

.073

Угроза

несанкцион

ированного

доступа к 53

активному

и (или)

пассивном

у

виртуально

му и (или)

физическо

му

сетевому

оборудован

ию из

физическо

й и (или)

виртуально

й сети

Угроза заключается в

возможности изменения

вредоносными программами

алгоритма работы

программного обеспечения

сетевого оборудования и

(или) параметров его

настройки путём

эксплуатации уязвимостей

программного и (или)

микропрограммного

обеспечения указанного

оборудования.

ограниченностью

функциональных

возможностей (наличием

слабостей) активного и (или) пассивного виртуального и (или) физического сетевого оборудования, входящего в состав виртуальной инфраструктуры, наличием у данного оборудования фиксированного сетевого адреса.

при условии наличия уязвимостей в программном и (или) микропрограммном обеспечении сетевого оборудования

Сетевое оборудование 29, микропрограммное обеспечение, сетевое программное обеспечение, виртуальные устройства

Внутренний нарушитель со средним потенциалом

Внешний нарушитель со средним потенциалом 7

Средняя Высокая Высокая Нарушение конфиденциальности

Нарушение целостности

Нарушение доступности

8 УБИ.092

Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам

Угроза заключается в

возможности получения
нарушителем привилегий
управления системой путём
использования удалённого
внеполосного (по
независимому
вспомогательному каналу 1
TCP/IP) доступа

невозможностью контроля
за механизмом,
реализующего функции
удалённого доступа на
аппаратном уровне, на
уровне операционной
системы, а также
независимостью от
состояния питания
аппаратных устройств, т.к.
данный механизм
предусматривает процедуру
удалённого
включения/выключения
аппаратных устройств. 1
наличия в системе
аппаратного обеспечения,
поддерживающего
технологию удалённого
внеполосного доступа;
наличия подключения
системы к сетям общего
пользования (сети
Интернет) 1
Информацион
ная система,
аппаратное
обеспечение
Внешний
нарушитель с
высоким
потенциалом
Низкая Высокая Средняя Нарушение
конфиденциа
льности
Нарушение
целостности
Нарушение
доступности
9 УБИ
.098
Угроза
обнаружен
ия
открытых
портов и
идентифик

ации
привязанн
ых к 53 нему
сетевых
служб
Угроза заключается в
возможности определения
нарушителем состояния
сетевых портов
дискредитируемой системы
(т.н. сканирование портов)
для получения сведений о
возможности установления
соединения с
дискредитируемой системой
по данным портам,
конфигурации самой системы 1
уязвимостями и ошибками
конфигурирования средств
межсетевого экранирования
и фильтрации сетевого
трафика, используемых в
дискредитируемой системе. 1
при условии наличия у
нарушителя подключения к
дискредитируемой
вычислительной сети и
специализированного
программного обеспечения,
реализующего функции
сканирования портов и
анализа сетевого трафика 1
Сетевой узел,
сетевое
программное
обеспечение,
сетевой
трафик 7
Внешний
нарушитель с
низким
потенциалом 7
Средняя Низкая Средняя Нарушение
конфиденциа
льности

188

и установленных средств
защиты информации, а также
других сведений,
позволяющих нарушителю
определить по каким портам
деструктивные программные
воздействия могут быть
осуществлены напрямую, а
по каким – только с

использованием специальных
техник обхода межсетевых
экранов.
10 1 УБИ
.099
Угроза
обнаружен
ия хостов
Угроза заключается в
возможности сканирования
нарушителем
вычислительной сети для
выявления работающих
сетевых узлов. 1
слабостями механизмов
сетевого взаимодействия,
предоставляющих клиентам
сети открытую
техническую информацию
о сетевых узлах, а также с
уязвимостями и ошибками
конфигурирования средств
межсетевого экранирования
и фильтрации сетевого
трафика, используемых в
дискредитируемой системе. 1
при условии наличия у
нарушителя подключения к
дискредитируемой
вычислительной сети и
специализированного
программного обеспечения,
реализующего функции
анализа сетевого трафика 1
Сетевой узел,
сетевое
программное
обеспечение,
сетевой
трафик 7
Внешний
нарушитель с
низким
потенциалом 7
Высокая Низкая Средняя Нарушение
конфиденциа
льности
11 УБИ
.103
Угроза
определени
я типов
объектов
защиты
Угроза заключается в

возможности проведения нарушителем анализа выходных данных дискредитируемой системы с помощью метода, позволяющего определить точные значения параметров и свойств, однозначно присущих дискредитируемой системе (данный метод известен как «fingerprinting», с англ. «дактилоскопия»). Использование данного метода не наносит прямого вреда дискредитируемой системе. Однако сведения, собранные таким образом, позволяют нарушителю выявить слабые места дискредитируемой системы, которые могут быть использованы в дальнейшем при реализации других угроз. 1

ошибками в параметрах конфигурации средств межсетевого экранирования, а также с отсутствием механизмов контроля входных и выходных данных.

в 1 случае наличия у нарушителя сведений о взаимосвязи выходных данных с конфигурацией дискредитируемой системы (документация на программные средства, стандарты передачи данных, спецификации и т.п.) 1

Сетевой узел, сетевое программное обеспечение, сетевой трафик 7

Внешний нарушитель с низким потенциалом 7

Высокая Низкая Средняя Нарушение конфиденциа льности

12 УБИ .113

Угроза

перезагруз

ки

Угроза заключается в

возможности сброса

пользователем 1

свойством оперативной

памяти обнулять своё

состояние при выключении 1

как аппаратным способом

(нажатием кнопки), так и

программным (локально 1

Системное

программное

обеспечение,

Внутренний

нарушитель с

низким

Высокая Низкая Средняя Нарушение

целостности

Нарушение

189

аппаратны

х и

программн

о-

аппаратны

х средств

вычислите

льной

техники

(нарушителем) состояния

оперативной памяти

(обнуления памяти) путём

случайного или намеренного

осуществления перезагрузки

отдельных устройств, блоков

или системы в целом.

и 1 перезагрузке.

или удалённо) при

выполнении следующих

условий:

наличие в системе

открытых сессий работы

пользователей;

наличие у нарушителя прав

в системе (или физической

возможности) на

осуществление

форсированной

перезагрузки 1

аппаратное

обеспечение

потенциалом

Внешний нарушитель с низким потенциалом доступности

13 УБИ.125

Угроза подключения к беспроводной сети в обход процедуры 1 аутентификации

Угроза заключается в возможности осуществления нарушителем перехвата трафика беспроводной сети или других неправомерных действий путём легализации нарушителем собственного подключения к беспроводной сети в полуавтоматическом режиме (например, WPS) без ввода ключа шифрования. 1 слабостями процедуры аутентификации беспроводных устройств в ходе полуавтоматического подключения 1 при условии наличия у нарушителя физического доступа к беспроводной точке доступа, поддерживающей полуавтоматический режим подключения 1

Сетевой узел, сетевое программное обеспечение 7

Внешний нарушитель с низким потенциалом 7

Высокая Средняя Высокая Нарушение конфиденциальности Нарушение целостности Нарушение доступности

14 УБИ

.132

Угроза получения предварительной информации об объекте защиты

Угроза заключается в возможности раскрытия нарушителем защищаемых сведений о состоянии защищённости дискредитируемой системы, её конфигурации и потенциальных уязвимостях и др., путём проведения мероприятий по сбору и анализу доступной информации о системе.

Данная угроза 1 отличается от угрозы перехвата данных и других угроз сбора данных тем, что нарушитель активно опрашивает дискредитируемую систему, а не просто за ней наблюдает 1 наличием уязвимостей в сетевом программном обеспечении, позволяющим получить сведения о конфигурации отдельных программ или системы в целом (отсутствие контроля входных данных, наличие открытых сетевых портов, неправильная настройка политик безопасности и т.п.). 1

при условии получения информации о дискредитируемой системе с помощью хотя бы одного из следующих способов изучения дискредитируемой системы:

анализ реакций системы на сетевые (в т.ч. синтаксически неверные или нестандартные) запросы к открытым в системе сетевым сервисам, которые могут стать

причиной вызова
необработанных
исключений с подробными
сообщениями об ошибках,
содержащих защищаемую
информацию (о
трассировке стека, о
конфигурации системы, о
маршруте прохождения
сетевых пакетов)
анализ реакций системы на
строковые URI-запросы (в
т.ч. неверные SQL-запросы, 1
Сетевой узел,
сетевое
программное
обеспечение,
сетевой
трафик,
прикладное
программное
обеспечение 7
Внешний
нарушитель со
средним
потенциалом 7
Средняя Средняя Средняя Нарушение
конфиденциа
льности

190
альтернативные пути
доступа к файлам).
15 УБИ
.139
Угроза
преодолени
я
физическо
й защиты
Угроза заключается в
возможности осуществления
нарушителем практически
любых деструктивных
действий в отношении
дискредитируемой
информационной системы
при получении им
физического доступа к
аппаратным средствам
вычислительной техники
системы путём преодоления
системы контроля
физического доступа,
организованной в здании
предприятия. 1

уязвимостями в системе контроля физического доступа (отсутствием замков в помещении, ошибками персонала и т.п.). 1

при условии успешного применения нарушителем любого из методов проникновения на объект (обман персонала, взлом замков и др.) 1

Сервер, рабочая станция, носитель информации, аппаратное обеспечение 7

Внешний нарушитель со средним потенциалом 7

Высокая Высокая Высокая Нарушение конфиденциальности

Нарушение целостности

Нарушение доступности

16 УБИ.140 7

Угроза приведения системы в состояние «отказ в обслуживании» 44

Угроза заключается в возможности отказа дискредитированной системой в доступе легальным пользователям при лавинообразном увеличении числа сетевых соединений с данной системой. 1

для обработки каждого сетевого запроса системой потребляется часть её ресурсов, а также слабостями сетевых технологий, связанными с ограниченностью скорости

обработки потоков сетевых запросов, и недостаточностью мер контроля за управлением соединениями. 1 при условии превышения объёма запросов над объёмами доступных для их обработки ресурсов дискредитируемой системы (таких как способность переносить повышенную нагрузку или приобретать дополнительные ресурсы для предотвращения их исчерпания). Ключевым фактором успешности реализации данной угрозы является число запросов, которое может отправить нарушитель в единицу времени: чем больше это число, тем выше вероятность успешной реализации данной угрозы для дискредитируемой системы 1 Информацион ная система, сетевой узел, системное программное обеспечение, сетевое программное обеспечение, сетевой трафик 7 Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом 7 Высокая Высокая Высокая Нарушение доступности 17 УБИ .143 Угроза 7 программн ого выведения из строя

средств
хранения,
обработки
и (или)
ввода/ 1 выво
да/передач

Угроза заключается в
возможности прерывания
нарушителем технологии
обработки информации в
дискредитируемой системе
путём осуществления
деструктивного
программного (локально или
удалённо) воздействия на
средства хранения (внешних,
съёмных и внутренних 1
наличием уязвимостей
микропрограммного
обеспечения средств
хранения, обработки и
(или)
ввода/вывода/передачи
информации. 1
при наличии у нарушителя
прав на отправку команды
или специально
сформированных входных
данных на средства
хранения, обработки и
(или)
ввода/вывода/передачи
информации 1
Носитель
информации,
микропрограм
мное

обеспечение,
аппаратное
обеспечение 7
Внутренний
нарушитель со
средним
потенциалом
Внешний
нарушитель со
средним
потенциалом 7
Низкая Высокая Средняя Нарушение
доступности

191
и
информаци
и

накопителей), обработки (процессора, контроллера устройств и т.п.) и (или) ввода/вывода/передачи информации (клавиатуры и др.), в результате которого объект защиты перейдёт в состояние «отказ в обслуживании». При этом вывод его из этого состояния может быть невозможен путём простой перезагрузки системы, а потребует проведения 1 ремонтно-восстановительных работ.

18 УБИ .145 Угроза пропуска проверки целостности программного обеспечения

Угроза заключается в возможности внедрения нарушителем в дискредитируемую систему вредоносного программного обеспечения путём обманного перенаправления запросов пользователя или его программ на собственный сетевой ресурс, содержащий вредоносное программное обеспечение, для его «ручной» или «автоматической» загрузки с последующей установкой в дискредитируемую систему от имени пользователя или его программ.

слабостями механизмов проверки целостности файлов программного обеспечения и/или проверки подлинности источника их получения.

при условии успешного использования обманных техник одного из следующих методов: «ручного метода» –

нарушитель, используя обманные механизмы, убеждает пользователя перейти по ссылке на сетевой ресурс нарушителя, что приводит к запуску вредоносного кода на компьютере пользователя, или убеждает пользователя самостоятельно загрузить и установить вредоносную программу (например, под видом игры или антивирусного средства); «автоматического метода» – нарушитель осуществляет деструктивное воздействие переадресацию функции автоматического обновления дискредитируемой программы на собственный вредоносный сервер

Системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение 7

Внутренний нарушитель с низким потенциалом

Внешний нарушитель с низким потенциалом 7

Низкая Высокая Средняя Нарушение целостности

Нарушение доступности

19 УБИ .157

Угроза физическог о

выведения из строя средств хранения, обработки 1

Угроза заключается в возможности умышленного выведения из строя внешним нарушителем средств хранения, обработки и (или) ввода/вывода/передачи информации, что может привести к нарушению 1

слабостями мер контроля физического доступа к средствам хранения, обработки и (или) ввода/вывода/передачи информации. 1

при условии получения нарушителем физического доступа к носителям информации (внешним, съёмным и внутренним накопителям), средствам обработки информации (процессору, контроллерам 1

Сервер, рабочая станция, носитель информации, аппаратное обеспечение 7

Внешний нарушитель с низким потенциалом 7

Высокая Средняя Высокая Нарушение целостности Нарушение доступности

192

и (или) ввода/вывода/передачи информации

доступности, а в некоторых случаях и целостности защищаемой информации. 1

устройств и т.п.) и средствам ввода/вывода информации (клавиатура и т.п.)

20 1 УБИ .160

Угроза хищения

средств
хранения,
обработки
и (или)
ввода/ 7 выво
да/передач
и
информаци
и

Угроза заключается в
возможности осуществления
внешним нарушителем кражи
компьютера (и
подключённых к нему
устройств), USB-
накопителей, оптических
дисков или других средств
хранения, обработки,
ввода/вывода/передачи
информации. 1
слабостями мер контроля
физического доступа к
средствам хранения,
обработки и (или)
ввода/вывода/передачи
информации 1
при условии наличия у
нарушителя физического
доступа к носителям
информации (внешним,
съёмным и внутренним
накопителям), средствам
обработки информации
(процессору, контроллерам
устройств и т.п.) и
средствам ввода/вывода
информации (клавиатура и
т.п.) 1
Сервер,
рабочая
станция,
носитель
информации,
аппаратное
обеспечение 7
Внешний
нарушитель с
низким
потенциалом 7
Высокая Высокая Высокая Нарушение
конфиденциа
льности
Нарушение
доступности
21 УБИ

.165

Угроза включения в проект не достоверно испытанных компонентов

Угроза заключается в возможности нарушения безопасности защищаемой информации вследствие выбора для применения в системе компонентов не в соответствии с их заданными проектировщиком функциональными характеристиками, надёжностью, наличием сертификатов и др.

недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. 1

при условии выбора для применения в системе компонентов по цене, разрекламированности и др.

Программное обеспечение, техническое средство, информационная система, ключевая система информационной инфраструктуры

Внутренний нарушитель со средним потенциалом

Низкая Средняя Средняя Нарушение конфиденциальности Нарушение целостности Нарушение доступности

22 УБИ

.166

Угроза внедрения системной избыточности

Угроза заключается в возможности снижения скорости обработки данных (т.е. доступности) компонентами программного обеспечения (или системы в целом) из-за внедрения в него (в неё) избыточных компонентов (изначально ненужных или необходимость в которых отпала при внесении изменений в проект). 1

недостаточностью мер по контролю за ошибками в ходе проектирования систем, связанных с безопасностью. 1

при условии внесения изменений в перечень задач, решаемых проектируемым программным обеспечением (проектируемой системой) 1

Программное обеспечение, информационная система, ключевая система информационной инфраструктуры

Внутренний нарушитель со средним потенциалом

Средняя Высокая Высокая Нарушение доступности

23 УБИ.178

Угроза несанкционированного использования системных

и сетевых
утилит
Угроза заключается в
возможности осуществления
нарушителем деструктивного
программного воздействия на
систему за 5 счёт

использования имеющихся
или предварительно 5
внедрённых стандартных
наличие в системе
стандартных системных и
сетевых утилит или
успешное их внедрение
нарушителем в систему и
сокрытие (с
использованием
существующих архивов,

Системное
программное
обеспечение 7
Внутренний
нарушитель с
низким
потенциалом
Внешний
нарушитель с
низким
потенциалом 7
Низкая Высокая Средняя Нарушение
конфиденциа
льности
Нарушение
целостности
Нарушение
доступности

193
(известных и обычно не
определяемых
антивирусными программами
как вредоносных) системных
и сетевых утилит,
предназначенных для
использования
администратором для
диагностики и обслуживания
системы (сети). 5
атрибутов «скрытый» или
«только для чтения» и 5 др.);
наличие у нарушителя
привилегий на запуск таких
утилит
24 5 УБИ
.182

Угроза физического устаревания аппаратных компонентов
Угроза заключается в возможности нарушения функциональности системы, связанной с безопасностью, вследствие отказов аппаратных компонентов этой системы из-за их физического устаревания (ржавление, быстрый износ, окисление, загрязнение, отслаивание, шелушение и др.)
влиянием физической окружающей среды (влажности, пыли, коррозийных субстанций).
возрастает при использовании пользователями технических средств в условиях, не удовлетворяющих требованиям заданных их производителем
Аппаратное средство
Внутренний нарушитель с низким потенциалом
Низкая Низкая Низкая Нарушение доступности
25 УБИ.183
Угроза перехвата управления автоматизированной системой управления технологическими процессами и

Угроза заключается в

возможности осуществления нарушителем несанкционированного доступа к информационной инфраструктуре за счёт получения нарушителем права управления входящей в её состав автоматизированной системой управления технологическими процессами путём эксплуатации уязвимостей её программного обеспечения или слабостей технологических протоколов передачи данных 33 . наличием у автоматизированной системы управления технологическими процессами 110 программных сетевых интерфейсов взаимодействия и, как следствие, возможностью несанкционированного доступа к данной системе, а также недостаточностью мер фильтрации сетевого трафика и антивирусной защиты. при условии наличия у нарушителя прав на осуществление взаимодействия с автоматизированной системой управления технологическими процессами 110 . Реализация данной угрозы может привести к: блокированию или искажению (некорректность выполнения) алгоритмов отработки заданий управления технологическими процессами, непосредственного управления оборудованием предприятия; нарушению штатного хода технологических процессов;

частичному или полному
останову технологических
процессов без (или с)
выхода(-ом) оборудования
из строя;
Программное
обеспечение
автоматизиро
ванной
системы
управления
технологическ
ими
процессами

Внутренний
нарушитель со
средним
потенциалом
Внешний
нарушитель с 7
высоким
потенциалом
Низкая Высокая Средняя Нарушение
целостности
Нарушение
доступности

194
аварийной ситуации в
критической системе
информационной
инфраструктуры
26 УБИ
.185
Угроза
несанкцион
ированного

изменения
параметров
настройки
средств
защиты 8
информаци
и

Угроза заключается в
возможности осуществления
нарушителем
несанкционированного
изменения параметров
настройки средства защиты
информации. 8
слабостями мер
разграничения доступа к
конфигурационным файлам

средства защиты информации. 8 при условии получения нарушителем прав доступа к программному интерфейсу управления средством защиты информации, а также при наличии у нарушителя сведений о структуре и формате файлов конфигурации средства защиты информации 8 Средство 7 защиты информации Внутренний нарушитель с низким потенциалом Внешний нарушитель с низким потенциалом 7 Низкая Средняя Средняя Нарушение конфиденциальности Нарушение целостности Нарушение доступности 27 УБИ .187 Угроза несанкционированного воздействия на средство защиты информации

Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к 8 программной среде управления средством защиты информации и 8 изменения режима его функционирования. наличием у средств защиты информации программной среды управления и взаимодействия с

пользователями системы

при условии получения

нарушителем прав доступа

к программному

интерфейсу управления

средством защиты

информации 8

Средство

защиты

информации

Внутренний

нарушитель со

средним

потенциалом

Внешний

нарушитель со

средним

потенциалом 7

Низкая Средняя Средняя Нарушение

конфиденциа

льности

Нарушение

целостности

Нарушение

доступности

Приложение Б Средние значения признаков поведения под атаками

Таблица 32 Средние значения признаков поведения под атаками по отношению к значениям признаков нормального поведения

Тип поведения

dos flood normal

repeated_tr

ansmission

repeated_tran

smission_dest

repeated_tra

nsmission_sr

c

selective

_forward

selective_f

orward_des

t

selective_f

orward_sr

c

sinkhole spoof

spoof_de

st

spoof_sr

c

sybil

wormhol

e

num_frames 97,11% 107,79% 100,00% 106,06% 99,99% 100,18% 93,78% 99,85% 99,66% 106,44% 99,90% 95,70% 99,98% 193,76% 103,12%

num_frames_avg 97,11% 107,79% 100,00% 106,06% 99,99% 100,18% 93,78% 99,85% 99,66% 106,44% 99,90% 95,70% 99,97% 132,12% 103,12%

num_packets 97,19% 107,93% 100,00% 106,13% 100,07% 100,26% 93,87% 99,93% 99,74% 106,44% 99,97% 95,78% 100,01% 193,85% 103,41%

num_packets_avg 97,19% 107,94% 100,00% 106,14% 100,07% 100,26% 93,87% 99,93% 99,74% 106,44% 99,97% 95,78% 100,01% 132,18% 103,41%

num_packets_out

_avg

103,83% 119,45% 100,00% 104,65% 100,10% 100,23% 95,40% 99,92% 99,83% 104,88% 99,31% 96,97% 104,15% 124,15% 101,76%

num_packets_out

_max

93,58% 170,75% 100,00% 108,02% 99,98% 100,37% 94,97% 100,00% 99,61% 193,39% 99,81% 93,59% 99,94% 155,30% 103,77%

num_packets_out

_min

99,76% 99,58% 100,00% 99,99% 99,99% 99,99% 99,99% 99,99% 99,99% 100,00% 57,55% 57,86% 99,26% 97,46% 99,23%

num_packets_in_

avg

98,08% 112,77% 100,00% 106,69% 100,12% 100,30% 93,34% 99,92% 99,74% 104,85% 100,01% 96,08% 100,02% 124,27% 103,32%

num_packets_in_

max

92,24% 166,65% 100,00% 109,20% 99,85% 100,45% 93,49% 99,85% 99,26% 190,37% 99,77% 92,08% 100,94% 153,62% 105,77%

num_packets_in_

min

91,31% 90,80% 100,00% 104,22% 98,89% 98,89% 81,67% 98,93% 98,93% 100,00% 99,74% 91,08% 91,31% 96,87% 100,15%

weighted_num_pa

ckets_in_avg

97,19% 113,34% 100,00% 106,28% 100,01% 100,23% 92,28% 99,66% 99,19% 101,74% 101,05% 96,99% 102,72% 127,75% 99,10%

weighted_num_pa

ckets_in_max

99,46% 126,59% 100,00% 110,23% 102,15% 102,36% 92,65% 101,40% 100,50% 118,89% 102,79% 101,81% 105,17% 142,66% 102,26%

weighted_num_pa

ckets_in_min

94,02% 93,44% 100,00% 103,73% 100,11% 100,56% 95,63% 100,11% 99,46% 88,49% 97,08% 91,58% 102,27% 93,35% 82,76%

frac_packets_in_o

ut_avg

74,17% 79,12% 100,00% 136,33% 101,26% 101,28% 66,23% 101,29% 101,36% 100,00% 117,42% 90,79% 82,66% 100,91% 95,16%

frac_packets_in_o

ut_max

100,00% 317,86% 100,00% 100,60% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 165,48% 160,12% 100,00% 100,60% 100,00%

frac_packets_in_o

ut_pan_avg

40,53% 41,02% 100,00% 162,86% 100,21% 101,35% 33,59% 100,65% 99,33% 100,00% 106,66% 40,82% 107,53% 97,86% 135,75%

frac_packets_in_o

ut_pan_max

100,00% 200,60% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00%

frac_packets_in_o

ut_pan_min

100,00% 0,00% 100,00% 0,00% 100,60% 100,60% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00%

num_packets_equ

al_src_avg

106,34% 132,22% 100,00% 108,48% 100,13% 100,12% 92,04% 100,00% 100,00% 100,00% 100,00% 100,00% 106,35% 100,00% 100,00%

num_packets_equ

al_src_max

463,60%

2178,99

%

100,00% 118,10% 100,61% 103,65% 96,68% 100,09% 100,25% 100,00% 103,20% 103,00% 309,56% 101,38% 99,43%

num_packets_equ

al_src_min

99,20% 99,21% 100,00% 103,96% 100,17% 99,83% 79,59% 99,24% 92,63% 100,00% 56,85% 57,21% 99,21% 97,26% 98,44%

num_packets_equ

al_src_pan_avg

99,99% 124,65% 100,00% 108,34% 100,31% 100,30% 91,66% 99,67% 99,69% 100,00% 100,01% 99,99% 100,00% 100,01% 99,87%

num_packets_equ

al_src_pan_max

100,01% 465,31% 100,00% 127,31% 100,62% 103,61% 99,58% 99,84% 99,96% 100,00% 104,27% 104,31% 148,50% 100,11% 99,97%

num_packets_equ

al_src_pan_min

99,96% 100,06% 100,00% 100,42% 100,15% 100,02% 72,12% 99,36% 96,29% 100,00% 53,91% 53,88% 50,50% 99,90% 99,00%

num_packets_equ

al_dest_avg

100,00% 125,13% 100,00% 108,48% 100,13% 100,12% 92,04% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00% 100,00%

num_packets_equ

al_dest_max

525,23%

2207,44

%

100,00% 116,78% 104,53% 100,30% 94,70% 99,84% 99,67% 100,00% 100,55% 524,36% 100,19% 101,82% 99,76%

num_packets_equ

al_dest_min

92,35% 91,81% 100,00% 106,36% 100,44% 100,56% 81,47% 95,29% 99,97% 100,00% 100,08% 92,05% 100,63% 98,00% 100,91%

num_packets_equ

al_dest_pan_avg

99,99% 124,65% 100,00% 108,34% 100,31% 100,30% 91,66% 99,67% 99,69% 100,00% 100,01% 99,99% 100,00% 100,01% 99,87%

num_packets_equ

al_dest_pan_max

177,78% 518,42% 100,00% 119,31% 101,23% 100,68% 95,50% 100,28% 100,24% 100,00% 100,10% 177,33% 100,35% 101,19% 100,01%

num_packets_equ

al_dest_pan_min

92,87% 92,81% 100,00% 104,95% 100,00% 100,20% 78,58% 99,19% 99,51% 100,00% 99,65% 93,08% 99,89% 99,11% 99,61%

num_frames_out_

avg

103,72% 119,29% 100,00% 104,53% 100,01% 100,12% 95,30% 99,84% 99,74% 104,84% 99,26% 96,87% 104,09% 124,08% 101,70%

num_frames_out_

max

93,60% 170,57% 100,00% 108,14% 100,00% 100,39% 94,84% 100,01% 99,64% 193,37% 99,74% 93,48% 99,92% 155,14% 103,69%

num_frames_out_

min

99,41% 99,41% 100,00% 99,91% 99,91% 99,91% 99,87% 99,87% 99,87% 100,00% 58,47% 58,42% 99,49% 97,09% 99,27%

num_frames_in_a

vg

97,97% 112,65% 100,00% 106,59% 100,02% 100,21% 93,23% 99,83% 99,67% 104,85% 99,92% 95,99% 99,97% 124,17% 102,92%

num_frames_in_

max

92,17% 166,50% 100,00% 109,17% 99,87% 100,46% 93,33% 99,87% 99,28% 190,35% 99,79% 91,99% 100,81% 153,46% 105,25%

num_frames_in_

min

91,64% 90,44% 100,00% 104,90% 99,07% 99,07% 82,51% 99,05% 99,05% 100,00% 100,29% 90,49% 91,45% 96,90% 99,66%

weighted_num_fr

ames_in_avg

97,13% 113,23% 100,00% 106,17% 99,90% 100,11% 92,17% 99,55% 99,09% 101,73% 100,97% 96,92% 102,68% 127,69% 98,65%

weighted_num_fr

ames_in_max

99,33% 126,42% 100,00% 110,05% 101,97% 102,18% 92,56% 101,23% 100,33% 118,87% 102,72% 101,57% 104,92% 142,47% 101,69%

weighted_num_fr

ames_in_min

94,09% 93,29% 100,00% 103,60% 99,98% 100,41% 95,49% 99,98% 99,35% 88,30% 97,09% 91,31% 102,01% 93,07% 82,25%

num_route_msgs

101,59% 102,60% 100,00% 104,50% 104,50% 104,50% 103,87% 103,87% 103,87% 107,14% 101,99% 101,72% 102,85% 286,18%

1225,88

%

num_forwarded_p

ackets

99,36% 115,65% 100,00% 110,17% 100,22% 100,44% 89,84% 99,79% 99,57% 110,66% 102,19% 97,17% 102,22% 224,57% 103,72%

num_forwarded_p

ackets_avg

99,37% 115,66% 100,00% 110,18% 100,22% 100,44% 89,84% 99,79% 99,57% 110,67% 102,19% 97,17% 102,23% 153,13% 103,72%

num_forwarded_p

ackets_max

91,76% 190,96% 100,00% 110,30% 99,99% 100,49% 93,53% 100,01% 99,52% 220,01% 99,76% 91,76% 99,92% 171,04% 104,85%

num_forwarded_p

ackets_min

100,48% 101,02% 100,00% 102,81% 102,81% 102,81% 102,81% 102,81% 102,81% 0,00% 102,08% 102,53% 101,77% 117,02% 102,44%

197

num_packets_cre

ated_avg

106,01% 137,70% 100,00% 100,87% 100,87% 100,87% 100,27% 100,27% 100,27% 100,00% 96,45% 96,17% 103,28% 101,09% 100,55%

num_packets_cre

ated_max

462,00%

2170,09

%

100,00% 100,31% 100,31% 100,31% 100,31% 100,31% 100,31% 100,34% 100,38% 99,88% 231,24% 101,70% 100,12%

num_packets_cre

ated_min

99,20% 99,21% 100,00% 99,75% 99,75% 99,75% 99,75% 99,75% 99,75% 100,00% 56,85% 57,21% 99,21% 97,26% 98,89%

frac_packets_crea

ted_acquired_avg

99,99% 100,00% 100,00% 28,42% 83,09% 99,00% 100,01% 99,99% 100,00% 100,01% 20,46% 17,96% 98,99% 100,02% 100,00%

frac_packets_crea

ted_acquired_max

100,00% 100,00% 100,00% 99,41% 100,00% 100,00% 100,00% 100,00% 100,00% 100,59% 100,00% 100,00% 100,00% 100,59% 100,00%

frac_packets_crea

ted_acquired_min

100,00% 100,00% 100,00% 0,00% 0,00% 0,60% 100,00% 100,00% 100,00% 100,00% 0,00% 0,00% 0,00% 100,00% 100,00%

198

Приложение В Листинги программ

Листинг В1 – Алгоритм итеративной классификации наблюдения

признакового пространства

```
01 % Data used for algorithm testing
02 mat = mesh360;
03
04 % The algorithm is tested for every class
05 for att=1:15
06
07 % Number of tests
08 n = 70;
```

```
09
10 % Starting point in the data
11 start=floor(rand()*n)+1;
12
13 % Structure designed to store prediction data
14 prediction(att).label=zeros(1,n);
15 prediction(att).prob=zeros(1,n);
16 prediction(att).num=zeros(1,n);
17 prediction(att).stor.label=zeros(n,5)/0;
18 prediction(att).stor.prob=zeros(n,5)/0;
19
20 % Conduct a test for all observations
21 for obs=start:start+n-1
22
23 % Completely available feature space is assumed
24 combo=vars;
25
26 % Initializing the loop
27 vect=[];
28 cert=0;
29 i=0;
30
31 % Start the iterative classification loop; stop-rules
32 while all(cert<prec) && i<length(vars)
33
34 % Expand the available feature space
35 i=i+1;
36
37 % Randomly choose a new classification feature
38 newvar=randperm(length(combo),1);
39
40 % Add the new feature to ones already used
41 vect=sort([vect combo(newvar)]);
42
43 % Reduce the available feature choices
44 combo(newvar)=[];
45
46 % Preprocessing the current observations
47 val=mat(obs-start+1,vect,att);
48 val=val-nmu(vect);
49 for j=1:length(val)
50 if ns(vect(j)) ~= 0
51 val(j)=floor(val(j)./ns(vect(j)));
52 end
53 end
54
55 % Constructing a guide to posterior probability matrices data storage
56 group='';
57 for j=1:length(vect)
58 group = [group num2str(vect(j)) '_'];
```



```
59 end
60 group = ['v' group(1:end-1)];
61
62 % Searching for the corresponding posterior distribution
```

```
63 [~,~,idx]=intersect(val,A.(genvarname(group)).ix,'rows');
64 distr=A.(genvarname(group)).p(idx,:);
65
66 % Making the optimal decision
67 [cert,result]=max(distr);
68
69 % Storing the current values for later analysis
70 prediction(att).stor.prob(obs-start+1,i) = cert;
71 prediction(att).stor.label(obs-start+1,i) = result;
72 end
73
74 % Updating the prediction
75 prediction(att).label(obs-start+1)=result;
76 prediction(att).prob(obs-start+1)=cert;
77 prediction(att).num(obs-start+1)=i;
78 end
79 end
```

Листинг В2 – Алгоритм обнаружения вторжений на основе вероятностного классификатора

```
01 % Data used for algorithm testing
02 mat=mesh360;
03
04 % The algorithm is tested for every class
05 for att=1:15
06
07 % Number of tests
08 n = 70;
09
10 % Starting poing in the data
11 start=floor(rand()*n)+1;
12
13 % Structure designed to store prediction data
14
15 prediction(att).label=zeros(1,n);
16 prediction(att).prob=zeros(1,n);
17 prediction(att).num=zeros(1,n);
18 prediction(att).stor.label=zeros(n,5)/0;
19 prediction(att).stor.prob=zeros(n,5)/0;
20
21 % Conduct a test for all observations
22 for obs=start:start+n-1
23
24 % Initializing the loop
25 i=1;
26
27 % Start the iterative classification loop; accuracy stop-rule
28 while prediction(att).prob(obs-start+1)<prec
29
30 % Choose a new feature subspace
31 newvars=vars(sort(randperm(length(vars),i)));
32
33 % Obtain a new observation
34 vect=mat(obs-start+1+i-1,newvars,att);
35
36 % Preprocessing the current observations
```

```
37 vect=vect-nmu(newvars);
38 for l=1:length(vect)
```



```
39 if ns(newvars(l)) ~= 0
40 vect(l) = floor(vect(l)./ns(newvars(l)));
41 end
42 end
43
44 % Constructing a guide to posterior probability matrices data storage
45 group='';
46 for l=1:length(newvars)
47 group = [group num2str(newvars(l)) '_'];
48 end
49 group = ['v' group(1:end-1)];
50
51 % Searching for the corresponding
52 [~,~,idx]=intersect(vect,A.(genvarname(group)).ix,'rows');
53 distr=A.(genvarname(group)).p(idx,:);
54
55 % Making the optimal decision
56 [cert,result]=max(distr);
57
58 % Storing the current values for later analysis
59 prediction(att).stor.label(obs-start+1,i)=result;
60 prediction(att).stor.prob(obs-start+1,i)=cert;
61
62 % Updating the prediction
63 prediction(att).label(obs-start+1)=result;
64 prediction(att).prob(obs-start+1)=cert;
65 prediction(att).num(obs-start+1)=i;
66
67 % Number of features stop-rule
68 if i<5
69 i=i+1;
70 else
71 break
72 end
73 end
74 end
75 end
```


Приложение Г Свидетельства о регистрации программ для ЭВМ

Приложение Д Копии актов внедрения