Федеральное государственное бюджетное образовательное учреждение

высшего образования «Российский государственный гидрометеорологический университет»

На правах рукописи

Богданов Павел Юрьевич

Модели и методы обнаружения аномального трафика сетей интернета вещей

Специальность 05.12.13 - Системы, сети и устройства телекоммуникаций

Диссертация на соискание ученой степени кандидата технических наук

Научный руководитель: Татарникова Татьяна Михайловна доктор технических наук, профессор

Санкт-Петербург - 2022

2

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 4

ГЛАВА 1 ЭКОСИСТЕМА ИНТЕРНЕТА ВЕЩЕЙ 11

1. 1 Сенсорные и исполнительные устройства интернета вещей 11

1.2 Телекоммуникационная инфраструктура интернета вещей 13

1.3 Протоколы интернета вещей 16

1.4 Архитектура IoT 21

1.4.1 Архитектура IoT с применением промежуточных платформ 24

1.4.2 Архитектура IoT с применением туманных вычислений 26

1.4.3 Архитектура социального интернета вещей 29

1.4.4 Архитектура систем граничных вычислений 31

1.5 Характеристики интернета вещей 35

1.6 Постановка задачи 43

Выводы по первой главе 45

ГЛАВА 2 СИСТЕМА МЕТРИК ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ТРАФИКА СЕТИ ИНТЕРНЕТА ВЕЩЕЙ 47

2.1 Классификация атакующих воздействий на IoT-сети 47

2.2 Механизмы обеспечения безопасности сети интернета вещей 51

2.3 Система метрик обнаружения аномального трафика 55

2.4 Методы обнаружения атак в IoT-сетях 59

2.4.1 Сигнатурные методы выявления атак 61

2.4.2 Поведенческие методы выявления атак 63

2.4.3 Практические аспекты выявления атак 65

Выводы по второй главе 70

ГЛАВА 3 МЕТОДЫ ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ТРАФИКА СЕТЕЙ ИНТЕРНЕТА ВЕЩЕЙ 71

3.1 Обнаружение атак на уровне IoT-устройства 71

3.2 Обнаружение атак на уровне сетевых сегментов 76

3.2.1 Применение глубоких автоэнкодеров для детектирования аномалий 77

3.2.2 Формирование поведенческого снимка IoT-устройства 82

3

3.2.3 Методика детектирования аномального поведения IoT-устройства 84

3.2.4 Обучение автоэнкодера и анализ результатов 87

3.3 Обнаружение аномального трафика на уровне сети 90

3.3.1 Применяемые методы обучения 92

3.3.2 Оценки эффективности моделей классификации 96

3.3.2 Характеристика обучающей выборки (data set) 101

3.3.3 Предложения по снижению влияния малых объемов data set и количества информационных признаков на качество обучения 107

3.4 Описание работы системы обнаружения атак 114

Выводы по третьей главе 117

ГЛАВА 4 ИМИТАЦИОННЫЕ МОДЕЛИ ФУНКЦИОНИРОВАНИЯ СЕТИ ИНТЕРНЕТА ВЕЩЕЙ 119

Заключение

ВходедиссертационногоисследованиябыларешенаважнаянаучнаязадачазаключающаясявразработкемоделейиметодовобнаруженияаномальноготрафикасетейинтернетавещейОсобоевниманиевработеуделенонесколькимнаправлениям систематизацииметрическиххарактеристик

позволяющихоценитьстатустрафикаинтернетавещейнормальныйилианомальныйиприменениюмоделейглубокогообученияприпостроениисистемыобнаруженияатаксучетомметрическиххарактеристик

Проведенныевработеисследованияпозволили

 Рассмотретьархитектурыобусловливающиеиерархическуюструктурупостроениясистемыобнаруженияатакнаузлыинтернетавещей

 Выделитьхарактеристикиособенныедляинтернетавещейтакиекаксвязностьикластеризациясенсорныхустройствсрокслужбысенсорнойсети

 Сформулироватьзадачудиссертационногоисследованиякакоптимизационнуюзадачупозволяющуюпредложитьвыбратьмеханизмыобнаруженияаномальноготрафиканавсехучасткахиерархическоговзаимодействияустройствиузловинтернетавещей

 Классифицироватьатакинасетиинтернетавещейимеханизмовобеспеченияпротиводействиясетевыматакам

 Предложитьсистемудиагностическихпрогнозирующихиретроспективныхметрикобусловливающуюсвоевременноеобнаружениеотклоненияпоказателейаномальноготрафикаотнормального

 Предложитьструктурусистемыобнаруженияатакдлясетейинтернетавещейсописаниемкомпонентучаствующихвпроцесседетектированияаномальноготрафика

 Предложитьметоддетектированияаномальногоповедениясенсорныхустройствкоторыйопираетсянаглубокиеавтоэнкодерыотдельнодлякаждого





устройстваобученногонастатистическихфункцияхизвлеченныхизнезараженноготрафика

 Систематизироватьоценкиэффективностиметодовмашинногообучениясцельювыборамоделиклассификаторасетевыхатак

 Выбратьэкспериментальнымпутеммодельклассификаторасетевыхатакнауровнесети

 Разработатьимитационнуюмодельсетидлядемонстрациинеобходимостивнедрениямеханизмовобнаруженияаномальноготрафикаатакисточающихэнергию

 Продемонстрироватьувеличениесрокаслужбысетиикоэффициентадоставкипакетовадресатувсетисвнедрениеммоделиоценкидоверияузлампосравнениюссетьювкотороймеханизмыобнаруженияаномальноготрафикаотсутствуют