НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ
январь–февраль 2017 Том 17 № 1 ISSN 2226-1494 http://ntv.ifmo.ru/
SCIENTIFIC AND TECHNICAL JOURNAL OF INFORMATION TECHNOLOGIES, MECHANICS AND OPTICS
January–February 2017 Vol. 17 No 1 ISSN 2226-1494 http://ntv.ifmo.ru/en

УДК 004.021

АНАЛИЗ СТАТИСТИЧЕСКИХ ДАННЫХ МОНИТОРИНГА СЕТЕВОЙ ИНФРАСТРУКТУРЫ ДЛЯ ВЫЯВЛЕНИЯ АНОМАЛЬНОГО ПОВЕДЕНИЯ ЛОКАЛЬНОГО СЕГМЕНТА СИСТЕМЫ

Н.А. Бажаев[a], И.С. Лебедев[a], И.Е. Кривцова[a]

[a] Университет ИТМО, Санкт-Петербург 197101, Российская Федерация
Адрес для переписки: nurzhan_nfs@hotmail.com

Информация о статье
Поступила в редакцию 04.10.16, принята к печати 20.11.16
doi: 10.17586/2226-1494-2017-17-1-92-99
Язык статьи – русский

Ссылка для цитирования: Бажаев Н.А., Лебедев И.С., Кривцова И.Е. Анализ статистических данных мониторинга сетевой инфраструктуры для выявления аномального поведения локального сегмента системы // Научно-технический вестник информационных технологий, механики и оптики. 2017. Т. 17. № 1. С. 92–99. doi: 10.17586/2226-1494-2017-92-99

Аннотация

Предложен метод мониторинга состояния информационной безопасности сегментов сетей маломощных устройств, персональных сетей «мягких пространств» («Умный дом», «Интернет вещей»). Проведен анализ характеристик систем, базирующихся на беспроводных технологиях, получаемых в результате пассивного наблюдения и активного опроса устройств, которые составляют инфраструктуру сети. Рассмотрен ряд внешних признаков попыток несанкционированного доступа к беспроводной сети со стороны потенциального нарушителя информационной безопасности. Модель для анализа состояний информационной безопасности основана на идентификационных, количественных, частотных, временных характеристиках. Ввиду особенностей устройств, обеспечивающих инфраструктуру сети, оценивание состояния информационной безопасности направлено на анализ нормального функционирования системы, а не на поиск сигнатур и характеристик аномалий при проведении различного рода информационных атак. Раскрыт эксперимент, обеспечивающий получение статистической информации о работе удаленных устройств беспроводной сети, где накопление данных для принятия решения происходит путем сравнения статистической информации служебных сообщений оконечных узлов в пассивном и активном режимах. Представлены результаты эксперимента по информационному воздействию на типовую систему. Предложенный подход к анализу статистических данных сетевой инфраструктуры на основе наивного байесовского классификатора может быть использован для определения состояний информационной безопасности.

Ключевые слова

информационная безопасность, беспроводные сети «мягких пространств», персональные сети, модель информационной безопасности

ANALYSIS OF STATISTICAL DATA FROM NETWORK INFRASTRUCTURE MONITORING TO DETECT ABNORMAL BEHAVIOR OF SYSTEM LOCAL SEGMENTS

N.A. Bazhayev[a], I.S. Lebedev[a], I.E. Krivtsova[a]

[a] ITMO University, Saint Petersburg, 197101, Russian Federation
Corresponding author: nurzhan_nfs@hotmail.com

Article info
Received 04.10.16, accepted 20.11.16
doi: 10.17586/2226-1494-2017-17-1-92-99
Article in Russian

For citation: Bazhayev N.A., Lebedev I.S., Krivtsova I.E. Analysis of statistical data from network infrastructure monitoring to detect abnormal behavior of system local segments. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2017, vol. 17, no. 1, pp. 92–99. doi: 10.17586/2226-1494-2017-17-1-92-99

Abstract

We propose a method of information security monitoring for a wireless network segments of low-power devices, "smart house", "Internet of Things". We have carried out the analysis of characteristics of systems based on wireless technologies, resulting from passive surveillance and active polling of devices that make up the network infrastructure. We have considered a number of external signs of unauthorized access to a wireless network by the potential information security malefactor. The model for analysis of information security conditions is based on the identity, quantity, frequency, and time characteristics. Due to the main features of devices providing network infrastructure, estimation of information security state is directed to the analysis of the system normal operation, rather than the search for signatures and anomalies during performance of

various kinds of information attacks. An experiment is disclosed that provides obtaining statistical information on the remote wireless devices, where the accumulation of data for decision-making is done by comparing the statistical information service messages from end nodes in passive and active modes. We present experiment results of the information influence on a typical system. The proposed approach to the analysis of network infrastructure statistical data based on naive Bayesian classifier can be used to determine the state of information security.

Keywords
information security, "soft space" wireless networks, personal networks, information security model

Введение

Появление большого количества мобильных устройств, подключаемых к сети Интернет, осуществление процессов приема, передачи, обработки поступающей с них информации вне контролируемой зоны обусловливают необходимость обеспечения процессов информационной безопасности относительно маломощных вычислительных систем, персональных сетей.

Особенно уязвимыми становятся беспроводные технологии, используемые в автоматизированных системах управления технологическим процессом, «Умных городах», «Умных домах», «Интернете вещей», «мягких пространствах». И, если в первых двух направления имеются типовые, адаптированные средства защиты, то в остальных, в связи с недостаточной стандартизацией и отсутствием регламентированных подходов, разработчики уделяют мало внимания решениям в области информационной безопасности [1–3].

Привычные бытовые «интеллектуальные» предметы («умные» микроволновки, кофеварки, стиральные машины), составляющие сегменты сетей «Интернета вещей» или «Умного дома», имеют ряд демаскирующих признаков, дающих возможность обнаружить и идентифицировать себя на основе структуры информационных сообщений, что предоставляет поле деятельности для потенциального злоумышленника. Унификация средств обеспечения взаимодействия отдельными производителями «умных» бытовых приборов и предоставление процессов настройки простым пользователям, не имеющим соответствующей квалификации, создают предпосылки для проведения различных атак, направленных на осуществление попыток управления такими устройствами извне [4, 5].

Обнаружение аномальных параметров сетевого трафика, неправильных или не соответствующих установленной ситуации команд, выявление большого числа повторных событий могут являться предвестниками попыток несанкционированного доступа [6, 7].

Таким образом, анализ информационных потоков с целью обнаружения отклонений различных их характеристик является одной из актуальных задач для персональных сетей.

В связи с этим возникает ряд задач, направленных на осуществление внешнего мониторинга событий информационной безопасности «интеллектуальных» устройств.

Постановка задачи

Типовым решением организации взаимодействия между устройствами является беспроводная сеть, состоящая из совокупности узлов. Такая система имеет инфраструктуру – набор физических и логических компонентов, которые обеспечивают связь, безопасность, маршрутизацию, управление, доступ и другие обязательные свойства сети [8, 9].

Компоненты сети, обеспечивающие сопряжения различных приборов и устройств «мягких пространств», позволяют осуществлять прием, обработку и передачу ограниченного типа сообщений. При внедрении сложных систем защиты информации может возникать ряд проблемных вопросов, связанных с необходимостью изменения архитектуры сети и увеличения вычислительных ресурсов отдельных узлов. В то же время большинство компонентов имеют конфигурационные возможности, позволяющие в течение ограниченного периода времени хранить статистическую информацию о своем функционировании. На начальном этапе эксплуатации после развертывания можно оценить различные характеристики интенсивности информационных, служебных пакетов, времена отклика на запросы, частоты нераспознанных и пропущенных сообщений. В связи с этим один из возможных подходов выявления аномального поведения – использование данных, отражающих состояния системы, которые могут быть применены в статистическом анализе [9, 10].

Исследуемые характеристики можно получить в результате как пассивного наблюдения, так и активного опроса устройств.

Таким образом, необходимо определить аномальное состояние относительно «нормального» функционирования на основе статистических данных характеристик множества элементов контролируемой системы.

Предлагаемый подход

Большая часть подходов к обнаружению попыток несанкционированного доступа предполагает выявление, обнаружение, идентификацию непредвиденных параметров сетевых пакетов (неправильные адреса, взведенные одновременно флаги сообщений и запросов соединений, непрогнозируемый рост

трафика сети) [11–13]. Однако анализ данных событий на низких уровнях сетевого взаимодействия с целью выявления инцидентов информационной безопасности является сложной задачей даже для специалистов, требует знаний сетевых протоколов и узкоспециализированных алгоритмов функционирования устройств конкретных производителей.

Один из возможных способов анализа состояний системы может осуществляться на основе статистических данных протоколов прикладного уровня взаимодействия узлов маломощных устройств путем пассивного и активного мониторинга. В первом случае производятся прослушивание сетевых устройств и статистический анализ событий приема и передачи различных типов сообщений. Во втором – выделяется узел системы мониторинга, от которого в определенные моменты времени отправляются запросы в виде различных команд, и осуществляется анализ временных задержек, изменений загрузки отдельных вычислительных ресурсов, сопоставление идентификационной информации и настроек.

Информация от датчиков и сенсоров, получнная путем пассивного прослушивания или активного мониторинга, скапливается в обрабатывающем узле, где осуществляется отслеживание ряда событий, связанных с изменением характеристик в сети, например:

- появление нераспознаваемых сообщений;
- появление повторных сообщений;
- увеличение числа сообщений о сбоях и отказах;
- увеличение широковещательных и служебных сообщений;
- возникновение задержек, влекущих статистическое изменение трафика информационных, служебных сообщений;
- изменение задержек откликов устройств на служебные широковещательные запросы для различных режимов работы;
- увеличение числа потерянных сообщений;
- изменение частот информационных и служебных сообщений.

Группирование приведенной выше совокупности событий позволяет рассмотреть анализ состояний информационной безопасности на основе идентификационных (I), количественных (N), частотных (f), временных (T) характеристик. В этом случае профиль функционирования системы будет определяться кортежем признаков:

$F=< I, N, f, T >$.

В зависимости от режима работы наблюдается изменение статистического портрета функционирования сети и устройств. Возникает возможность хранения признакового пространства, например, в виде таблиц событий реляционной базы данных устройств, которая наполняется по мере функционирования системы.

На рис. 1 и 2 представлена типовая система, где информация с датчиков и сенсоров анализируется на специально выделенном узле, и схема оценки состояния информационной безопасности, применяемая в системе мониторинга.

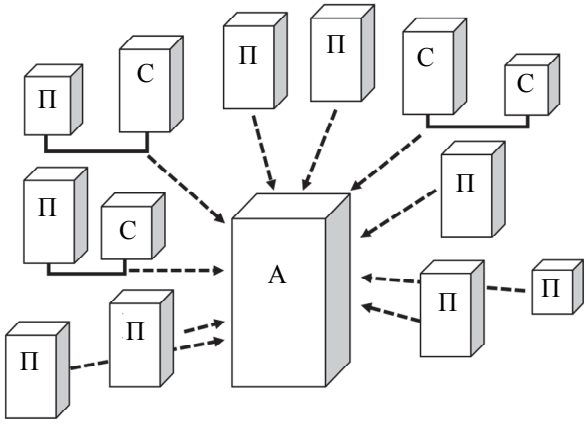

Рис. 1. Взаимодействие узлов сети: сенсоров (С), передатчиков (П) и блока анализа (А)

Для обнаружения «мягких» атак на маломощную сеть устройств особую важность приобретают признаки, которые можно представить в виде вектора значений, изменяемого во времени. Исходя из этого, для идентификации состояний возможно применение наивного байесовского классификатора, достоинством которого является малое количество данных для обучения:

$$C = \arg\max_{h \in H} \frac{p(X/h)p(h)}{p(X)},$$

где h, X – предсказываемое и предшествующее события, а значения функции p – вероятности этих событий и их следствий ($p=m/n$, где m – количество произошедших событий, n – количество всех событий).

В различных режимах работы системы могут наблюдаться аномалии, требующие более детального изучения на предмет возможности несанкционированного доступа [14, 15]. Определение количественных, частотных данных, показывающих нераспознанные, пропущенные сообщения, получение информации о конечном состоянии узлов на основе статистических данных протоколов прикладного уровня взаимодействия маломощных устройств путем пассивного и активного мониторинга позволяют осуществить построение классификатора.

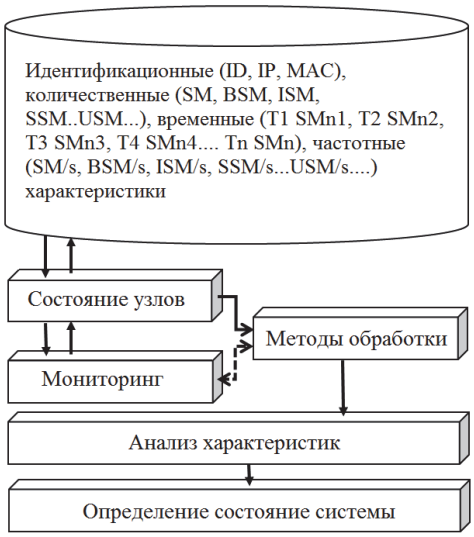

Рис. 2. Типовая схема оценки состояния информационной безопасности системы

На рис. 3 представлена анализируемая система. Информационные и служебные сообщения циркулируют между узлами $U_1 \ldots U_n$, устройство C предназначено для сбора информации. В первом случае устройство C прослушивает сеть и формирует выборку статистических данных, во втором – дополнительно осуществляет рассылку запросов на устройства и измеряет различные характеристики.

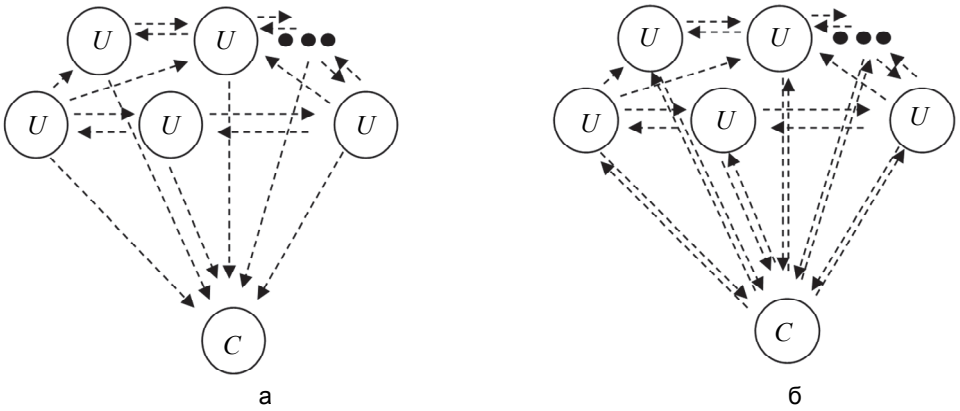

Рис. 3. Схема системы с пассивным (а) и системы с активным мониторингом (б)

Ввиду малой мощности устройств, обеспечивающих инфраструктуру сети, оценивание состояния информационной безопасности легче проводить, основываясь на профилях нормального функционирования системы.

Постановка эксперимента

На рис. 4 представлена архитектура модельной сети на базе устройств Zigbee Telegesis для проведения эксперимента и сбора статистической информации.

Анализируемое устройство представляет собой персональный компьютер с программным обеспечением, выполняющим функции монитора и тестера, которое осуществляет прием, передачу и анализ сообщений через присоединенный модуль Zigbee. Для имитации работы персональной сети тестирующая программа последовательно выдает информационные сообщения на устройство Zigbee по адресам узлов сети. Программа-монитор предназначена для анализа полученных сообщений, накопления статистических данных и их отправки на обрабатывающее устройство.

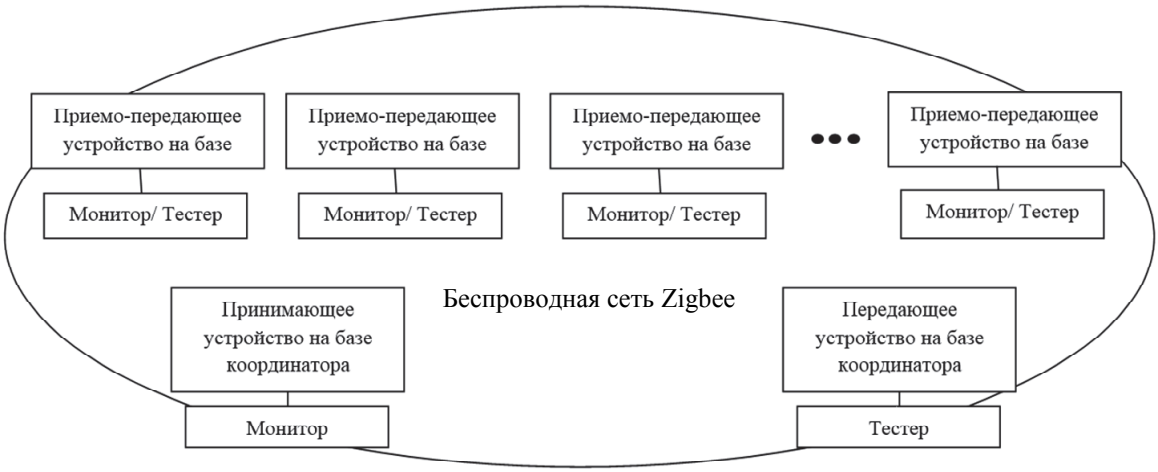

Рис. 4. Архитектура модельной сети на базе устройств Zigbee Telegesis для проведения эксперимента

При проведении испытаний выполнялась следующая последовательность действий.

1. Каждое приемо-передающее устройство под управлением программы-тестера независимо от других сетевых узлов последовательно выдает информационные сообщения по адресам узлов сети.
2. Каждое приемо-передающее устройство на прикладном уровне принимает сообщение, анализирует их корректность, периодически, по мере освобождения, после истечения определенного промежутка времени выдает информацию о своем состоянии.
3. Принимающее устройство в пассивном режиме слушает сеть, осуществляет распознавание типов переданных сообщений, выданных в эфир, анализирует внешние признаки, сравнивая с шаблонами, накапливает информацию на определенном интервале времени. В активном режиме, кроме перечисленных действий, устройством осуществляется опрос состояния приемо-передающих устройств, определяется среднее время задержки на сообщение.

После заданного временного периода «штатного функционирования» происходит имитация действий нарушителя. Вводится передающее устройство, которое во время работы сети с помощью тестирующей программы через случайные интервалы времени посылает на приемо-передающие устройства команды конфигурирования и управления модулями.

Результаты эксперимента

Накопление данных происходило путем сравнения статистической информации служебных сообщений оконечных узлов в пассивном и активном режимах.

На рис. 5 приведен пример графической интерпретации изменения вектора анализируемого состояния системы из 5 элементов Zigbee, рассматриваемой в эксперименте, показывающий значения отдельных параметров, снятых через интервал в 5 с. Результаты функционирования объединены в статистические данные по видам сообщений.

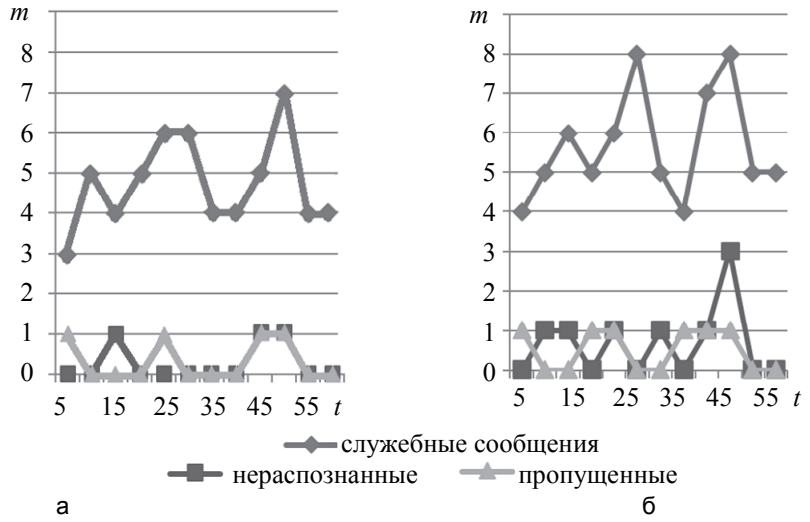

Рис. 5. Система в обычном состоянии (а) и система при активном мониторинге (б), где m – количество сообщений, t – время (с)

В эксперименте проведение атаки на прикладном уровне сводится к изменению интенсивности поступления сообщений (воспроизведение информационных сообщений, и наводнение служебными сообщениями, вызывающие процессы ассоциации, аутентификации, диссоциации, деаутентификации, запросы на подключение).

Для имитации попыток доступа к сети «потенциальному злоумышленнику» предоставлялись возможности по передаче сообщений конфигурирования и управления модулями и сетью (в приводимом эксперименте команды Zigbee Telegesis ATZ, AT+DASSL, AT+DASSR, AT+JPAN, AT+SJN и т.д.). Последовательность команд, отправляемых на функционирующие устройства, выбиралась случайным образом.

На статистической информации, полученной через определенные промежутки времени, связанные с функционированием устройств, строится типовой кортеж, отдельные компоненты которого приведены в таблице.

Параметр	5 с	10 с	…	*N* с
информационные сообщения	320	319	…	321
служебные сообщения	3	5	…	5
нераспознанные	0	0	…	0
пропущенные	1	0	…	0
…				
время задержки на сообщение	0,001	0,001	…	0,002

Таблица. Компоненты кортежа статистических данных системы

Обрабатывая наивным байесовским классификатором кортеж признаков через постоянные заданные промежутки времени, становится возможным определить аномальные состояния системы, на которые следует обратить более пристальное внимание.

В приводимом эксперименте для систем пассивного и активного мониторинга рассмотрены состояния:

- правильного распознавания штатного режима функционирования;
- правильного распознавания атаки на сеть;
- ложного распознавания атаки (при ее отсутствии);
- ложного распознавания нормального состояния (при проведении атаки).

Обучение классификатора происходило на основе данных при штатном режиме работы сети от 40 мин до 3,5 ч для каждого случая. Объем обучающей выборки k изменялся от 500 до 2500 кортежей. Результаты работы классификатора (где правильное распознавание состояний объединено) представлены на рис. 6.

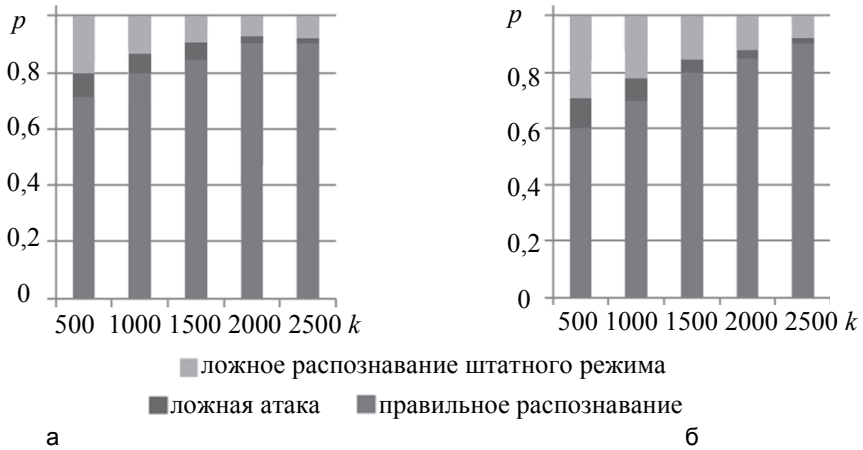

Рис. 6. Вероятностная оценка (P) работы классификатора состояний системы с пассивным (а) и активным мониторингом (б) на основе байесовского классификатора для различных объемов количества кортежей (k) обучающей выборки

Для оценки качественных характеристик необходим выбор различных показателей и их групп. В то же время предлагаемое решение не требует больших вычислительных затрат, подобная система может быть достаточно быстро обучена и использоваться в качестве решения, направленного на обнаружение аномальных параметров функционирования персональной сети. Однако даже статистика, полученная на основе проведенного эксперимента, показывает возможности вероятностного определения состояния информационной безопасности для подобных сетей.

Заключение

Таким образом, предложенный метод мониторинга состояния информационной безопасности сегментов сетей маломощных устройств, персональных сетей на основе статистических данных взаимодействия приемо-передающих устройств контроля функционирования прикладного уровня локальной информационной системы позволяет получать вероятностные характеристики состояния информационной безопасности. Особенностью подхода является возможность быстрой адаптации к локальным сетям маломощных устройств разных производителей «Интернета вещей», «Умного дома».

Для реализации данного вида мониторинга нет необходимости осуществлять разработку сложных системных приложений.

Предложенный метод может быть использован при поиске аномалий сегментов сетей. В то же время признаковое пространство требует дополнительного анализа и определения информативности отдельных характеристик для повышения точности и адаптации к системам обнаружения вторжений реального времени.

Литература

1. Kumar P., Ylianttila M., Gurtov A., Lee S.-G., Lee H.-J. An efficient and adaptive mutual authentication framework for heterogeneous wireless sensor networks-based applications // Sensors. 2014. V. 14. N 2. P. 2732–2755. doi: 10.3390/s140202732
2. Sridhar P., Sheikh-Bahaei S., Xia S., Jamshidi M. Multi agent simulation using discrete event and soft-computing methodologies // Proc. IEEE Int. Conf. on Systems, Man and Cybernetics. Washington, 2003. V. 2. P. 1711–1716.
3. Page J., Zaslavsky A., Indrawan M. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities // Proc. 1st Int. Workshop on Safety and Security in Multi-Agent Systems (SASEMAS). 2004. P. 85–101.
4. Зикратов И.А., Зикратова Т.В., Лебедев И.С. Доверительная модель управления безопасностью мультиагентных робототехнических систем с децентрализованным управлением // Научно-технический вестник информационных технологий, механики и оптики. 2014. № 2 (90). С. 47–52.
5. Zikratov I.A., Lebedev I.S., Gurtov A.V. Trust and reputation mechanisms for multi-agent robotic systems // Lecture Notes in Computer Science. 2014. V. 8638. P. 106–120. doi: 10.1007/978-3-319-10353-2_10
6. Wyglinski A.M., Huang X., Padir T., Lai L., Eisenbarth T.R., Venkatasubramanian K. Security of autonomous systems employing embedded computing and sensors // IEEE Micro. 2013. V. 33. P. 80–86. doi: 10.1109/MM.2013.18
7. Lebedev I.S., Korzhuk V.M. The monitoring of information security of remote devices of wireless networks // Lecture Notes in Computer Science. 2015. V. 9247. P. 3–10. doi: 10.1007/978-3-319-23126-6_1
8. Prabhakar M., Singh J.N., Mahadevan G. Nash equilibrium and Marcov chains to enhance game theoretic approach for vanet security // Advances in Intelligent Systems and Computing. 2013. V. 174 AISC. P. 191–199. doi: 10.1007/978-81-322-0740-5_24
9. Bazhayev N., Lebedev I., Korzhuk V., Zikratov I. Monitoring of the information security of wireless remote devices // Proc. 9th Int. Conf. on Application of Information and Communication Technologies. Rostov-on-Don, Russian Federation, 2015. P. 233–236. doi: 10.1109/ICAICT.2015.7338553
10. Nikolaevskiy I., Lukyanenko A., Polishchuk T., Polishchuk V.M., Gurtov A.V. isBF: scalable in-packet bloom filter based multicast // Computer Communications. 2015. V. 70. P. 79–85. doi: 10.1016/j.comcom.2015.05.002
11. Al-Naggar Y., Koucheryavy A. Fuzzy logic and Voronoi diagram using for cluster head selection in ubiquitous sensor networks // Lecture Notes in Computer Science. 2014. V. 8638. P. 319–330. doi: 10.1007/978-3-319-10353-2_28
12. Chehri A., Moutah H.T. Survivable and scalable wireless solution for e-health and emergency applications // Proc. 1st Int. Workshop on Engineering Interactive Computing Systems for Medicine and Health Care. Pisa, Italy, 2011. P. 25–29.
13. Krivtsova I., Lebedev I., Sukhoparov M., Bazhayev N., Zikratov I., Ometov A., Andreev S., Masek P., Fujdiak R., Hosek J.

References

1. Kumar P., Ylianttila M., Gurtov A., Lee S.-G., Lee H.-J. An efficient and adaptive mutual authentication framework for heterogeneous wireless sensor networks-based applications. *Sensors*, 2014, vol. 14, no. 2, pp. 2732–2755. doi: 10.3390/s140202732
2. Sridhar P., Sheikh-Bahaei S., Xia S., Jamshidi M. Multi agent simulation using discrete event and soft-computing methodologies. *Proc. IEEE Int. Conf. on Systems, Man and Cybernetics*. Washington, 2003, vol. 2, pp. 1711–1716.
3. Page J., Zaslavsky A., Indrawan M. Countering security vulnerabilities using a shared security buddy model schema in mobile agent communities. *Proc. 1st Int. Workshop on Safety and Security in Multi-Agent Systems, SASEMAS*, 2004, pp. 85–101.
4. Zikratov I.A., Zikratova T.V., Lebedev I.S. Trust model for information security of multi-agent robotic systems with a decentralized management. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2014, no. 2, pp. 47–52. (In Russian).
5. Zikratov I.A., Lebedev I.S., Gurtov A.V. Trust and reputation mechanisms for multi-agent robotic systems. *Lecture Notes in Computer Science*, 2014, vol. 8638, pp. 106–120. doi: 10.1007/978-3-319-10353-2_10
6. Wyglinski A.M., Huang X., Padir T., Lai L., Eisenbarth T.R., Venkatasubramanian K. Security of autonomous systems employing embedded computing and sensors. *IEEE Micro*, 2013, vol. 33, pp. 80–86. doi: 10.1109/MM.2013.18
7. Lebedev I.S., Korzhuk V.M. The monitoring of information security of remote devices of wireless networks. *Lecture Notes in Computer Science*, 2015, vol. 9247, pp. 3–10. doi: 10.1007/978-3-319-23126-6_1
8. Prabhakar M., Singh J.N., Mahadevan G. Nash equilibrium and Marcov chains to enhance game theoretic approach for vanet security. *Advances in Intelligent Systems and Computing*, 2013, vol. 174 AISC, pp. 191–199. doi: 10.1007/978-81-322-0740-5_24
9. Bazhayev N., Lebedev I., Korzhuk V., Zikratov I. Monitoring of the information security of wireless remote devices. *Proc. 9th Int. Conf. on Application of Information and Communication Technologies*. Rostov-on-Don, Russian Federation, 2015, pp. 233–236. doi: 10.1109/ICAICT.2015.7338553
10. Nikolaevskiy I., Lukyanenko A., Polishchuk T., Polishchuk V.M., Gurtov A.V. isBF: scalable in-packet bloom filter based multicast. *Computer Communications*, 2015, vol. 70, pp. 79–85. doi: 10.1016/j.comcom.2015.05.002
11. Al-Naggar Y., Koucheryavy A. Fuzzy logic and Voronoi diagram using for cluster head selection in ubiquitous sensor networks. *Lecture Notes in Computer Science*, 2014, vol. 8638, pp. 319–330. doi: 10.1007/978-3-319-10353-2_28
12. Chehri A., Moutah H.T. Survivable and scalable wireless solution for e-health and emergency applications. *Proc. 1st Int. Workshop on Engineering Interactive Computing Systems for Medicine and Health Care*. Pisa, Italy, 2011, pp. 25–29.
13. Krivtsova I., Lebedev I., Sukhoparov M., Bazhayev N., Zikratov I., Ometov A., Andreev S., Masek P., Fujdiak R., Hosek J. Implementing a broadcast storm attack on a mission-critical

Implementing a broadcast storm attack on a mission-critical wireless sensor network // Lecture Notes in Computer Science. 2016. V. 9674. P. 297–308.
14. Бажаев Н.А., Кривцова И.Е., Лебедев И.С. Исследование доступности удаленных устройств беспроводных сетей // Научно-технический вестник информационных технологий, механики и оптики. 2016. Т. 16. № 3. С. 467–473. doi: 10.17586/2226-1494-2016-16-3-467-473
15. Исакеев Д.Г., Зикратова Т.В., Лебедев И.С., Шабанов Д.П. Оценка безопасного состояния мультиагентной робототехнической системы при информационном воздействии на отдельный элемент // Вестник компьютерных и информационных технологий. 2015. № 1 (127). С. 43–49.

Авторы

Бажаев Нуржан Аманкулулы – аспирант, Университет ИТМО, Санкт-Петербург 197101, Российская Федерация, nurzhan_nfs@hotmail.com
Лебедев Илья Сергеевич – доктор технических наук, доцент, доцент, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, lebedev@cit.ifmo.ru
Кривцова Ирина Евгеньевна – старший преподаватель, Университет ИТМО, Санкт-Петербург, 197101, Российская Федерация, ikr@cit.ifmo.ru

wireless sensor network. *Lecture Notes in Computer Science*, 2016, vol. 9674, pp. 297–308.
14. Bazhayev N.A., Krivtsova I.E., Lebedev I.S. Availability research of remote devices for wireless networks. *Scientific and Technical Journal of Information Technologies, Mechanics and Optics*, 2016, vol. 16, no. 3, pp. 467–473. doi: 10.17586/2226-1494-2016-16-3-467-473. (In Russian).
15. Isakeev D.G., Zikratova T.V., Lebedev I.S., Shabanov D.P. The estimation of secure condition of multi-agent robotic system in case of information influence on the single component. *Herald of Computer and Information Technologies*, 2015, no. 1, pp. 43–49. (In Russian).

Authors

Nurzhan A. Bazhayev – postgraduate, ITMO University, Saint Petersburg, 197101, Russian Federation, nurzhan_nfs@hotmail.com

Ilya S. Lebedev – D.Sc., Associate professor, Associate professor, ITMO University, Saint Petersburg, 197101, Russian Federation, lebedev@cit.ifmo.ru
Irina E. Krivtsova – Senior lecturer, ITMO University, Saint Petersburg, 197101, Russian Federation, ikr@cit.ifmo.ru