Published in the Russian Federation
Vestnik policii
Has been issued since 1907.
ISSN: 2409-3610
E-ISSN: 2414-0880
Vol. 7, Is. 1, pp. 38-44, 2016

DOI: 10.13187/vesp.2016.7.38
www.ejournal21.com

UDC 004.056

Automation Device Authentication at «Smart Home»

[1] Anton N. Kanev
[2] Alexander V. Nasteka
[3] Catherine E. Bessonova

[1] ITMO university, Russian Federation
197101 Saint Petersburg, Kronverkskiy prospekt, 49
E-mail: kanev.a.n@mail.ru
[2] ITMO university, Russian Federation
97101 Saint Petersburg, Kronverkskiy prospekt, 49
E-mail: nasteka.av@gmail.com
[3] ITMO university, Russian Federation
197101 Saint Petersburg, Kronverkskiyprospekt, 49
PhD in Engineering sciences, Assistant
E-mail: merom812@gmail.com

Abstract

This article brings to light the problem of anomaly detection in the object of protection automation systems. The article illustrates the method of anomaly detection using hybrid neural network, and the performed experiment. The result of the research is software that implements the anomaly detection mechanism.

Keywords: information security; smart home; automation device; artificial neural network.

Введение

В настоящее время одной из основных гарантией сохранности имущества в охраняемых помещениях является установка различных систем сигнализации и вывод тревожного сигнала на пульты частных охранных предприятий. Правоохранительных органы используют встраиваемое оборудование для создания контролируемых зон [1, 2]. При физическом проникновении или ином отслеживаемом действии (вскрытие двери и т.п.) со стороны нарушителя, данные устройства успешно сообщают о нем.

Однако, если «наезд» идет непосредственно на датчик или узел охранной сети, то они не имеют возможности контролировать и реагировать на внешние программные и физические воздействия, которые не вписываются в стандартную модель поведения нарушителей.

В связи с развитием комплексов домашней автоматизации (“Умный дом”) охранные устройства все чаще внедряются в существующую инфраструктуру, где становятся еще более уязвимыми элементами сети и подвержены стандартным атакам типа DDoS [4, 5]. Реализация таких атак приводит к возникновению аномалий в системе. Таким образом,

задачей исследования является разработка программного комплекса для выявления аномалий системы “Умный дом”.

Материалы и методы

Основным источником для написания статьи послужили исследования в области обеспечения информационной безопасности систем домашней автоматизации, обеспечения информационной безопасности беспроводных сенсорных сетей, а также материалы по искусственным нейронным сетям [1, 6, 7].

Методологическую основу работы составил общенаучный метод анализа. В статье даются рекомендации по практическому использованию искусственных нейронных сетей для выявления аномалий в системе “Умный дом”.

Обсуждение

Общая схема возможного воздействия на устройства системы “Умный дом” представляет собой две стороны: злоумышленник и атакуемые устройства (см. рисунок 1).

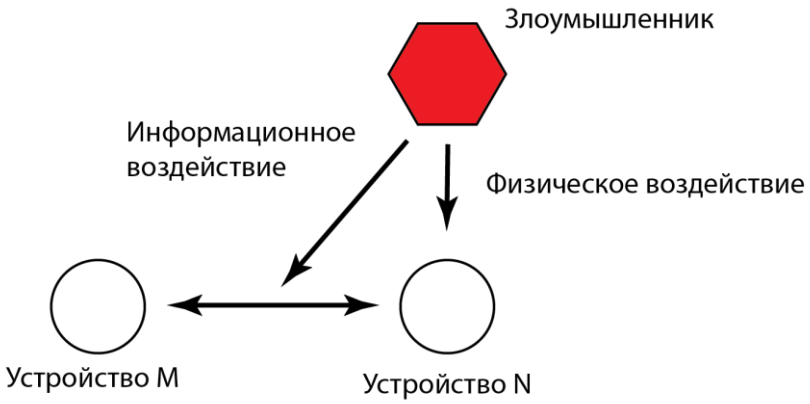

Рис. 1. Схема воздействия на устройства системы “Умный Дом”

Злоумышленник имеет возможность физического вмешательства в работу Устройства N (его отключение). В этом случае Устройством M может быть зарегистрирована аномалия в виде недоступного Устройства N. Основным воздействием является информационное, которое направлено на информационный поток между устройством N и M. В случае, если устройством N ведется мониторинг активности сети, в частности активность сетевого общения Устройством M, то базовые атаки типа Man-in-the-middle, replay-атаки также приведут к образованию аномалий, которые злоумышленник не в состоянии скрыть [8].

Каждое из представленных выше воздействий тем или иным образом влияет на характеристики сети системы “Умный дом”. Для решения поставленной задачи в первую очередь необходимо определить совокупность тех характеристик, которые будут анализироваться механизмом выявления аномалий (т.е. определить метрики).

Данные метрики различаются в зависимости от исследуемой аномалии [9]. В данной работе были выделены те из них, которые встречаются наиболее часто:

– количество входящих/исходящих пакетов за единицу времени;

– количество потерянных пакетов/ошибок за единицу времени;

– мощность исходящего сигнала;

– потребление электроэнергии за единицу времени.

Также требуется хранить значения метрик в течение некоторого периода времени с целью выявления их изменений. Согласно [9] является использование метрик соседних узлов сети. Таким образом, каждый узел сети системы “Умный дом” можно представить, как набор метрик, распределенных во времени.

Рассмотренный выше набор метрик является непостоянным и индивидуальным для конкретной реализации системы “Умный дом”. Учитывая данные факторы, предлагается использовать искусственные нейронные сети как механизм обнаружения аномалий сети.

В работе используется гибридная нейронная сеть, объединяющая две модели искусственных нейронных сетей: самоорганизующуюся сеть с конкуренцией (слой Кохонена) и многослойный персептрон [3]. Структура гибридной нейронной сети представлена на рисунке 2.

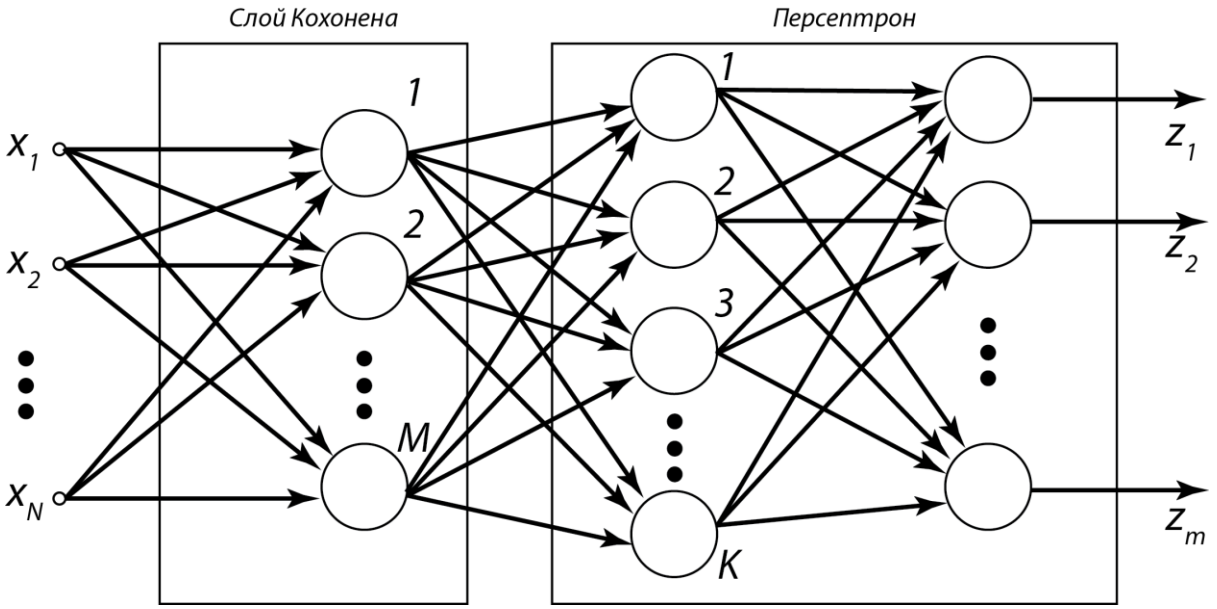

Рис. 2. Структура гибридной нейронной сети

Главным достоинством слоя Кохонена является высокая скорость обучения в сравнении с нейронными сетями с учителем. При заданной структуре он позволяет выделить наиболее важные входные данные (свойство локализации). Затем результирующий вектор передается на вход многослойному персептрону, функция которого состоит в определении, является ли переданный вектор аномальным или нет. В данном случае используется свойство аппроксимации персептронной сети.

Обучение гибридной сети проводится в несколько этапов: на первом обучается слой Кохонена, на втором - многослойный персептрон, при этом обучающая выборка подается через слой Кохонена. Методом обучения персептрона является метод обратного распространения ошибки.

В описанной выше модели используется следующий математический аппарат.

Значение каждого нейрона в слое Кохонена:

$$u_i = \sum_j w_{ji} x_j \,, \tag{1}$$

где u_i – значение нейрона i, w_{ji}– вес связи i-го нейрона с j-м входом, x_j– j-й вход.

В слое выбирается «победитель»: $u_{\max} = \max\{u_i\}$, где $u_{\max}$ – «победитель». При этом используется механизм утомления для активации «мертвых» нейронов [3].

ВыходслояКохонена:

$$y_i = \exp\left(-\frac{\left|u_{\max} - u_i\right|^2}{\sigma^2}\right), \tag{2}$$

гдеy_i – i-йвыход, σ – подбираемоезначение.

В ходе обучения слоя Кохонена веса «победителя» корректируются:

$$w_{ji} = w_{ji} + \alpha\left(x_j - w_{ji}\right), \quad (3)$$

гдеα – скоростьобучения.

Значение нейронов в персептроне:

$$z_i^{(k)} = \sum_j w_{ji}^{(k)} y_j^{(k-1)}, \quad (4)$$

где$z_i^{(k)}$ – значениеi-гонейронавk-мслое, $w_{ji}^{(k)}$ – вессвязиi-гонейронаk-гослоясj-мнейроном$(k-1)$-гослоя, $y_j^{(k-1)}$ – значениеj-гонейронав$(k-1)$-мслое, k = 0 – вход.

Результаты

Для практической реализации было разработано два самостоятельных модуля, которые в дальнейшем объединятся в единую систему по выявлению аномалий в системе “Умный дом”.

Первым модулем является искусственная нейронная сеть, разработанная на языке C++. Она полностью повторяет представленную модель искусственной нейронной сети и требует основные этапы для возможности работы:

1. обучение слоя Кохонена;
2. обучение сети персептрона;

После обучения искусственная нейронная сеть готова к работе и способна на основании входящих данных выносить решения о принадлежности текущего состояния узла сети к аномальному или обычному с ошибкой в 91,47%.

Второй модуль представляет собой реализацию модели системы “Умный дом” в специальной среде моделирования (см. рисунок 3). Для разработки данного модуля использовалась IDE Omnet++, которая позволяет создавать различные топологии сетей, задавать логику их работы [10].

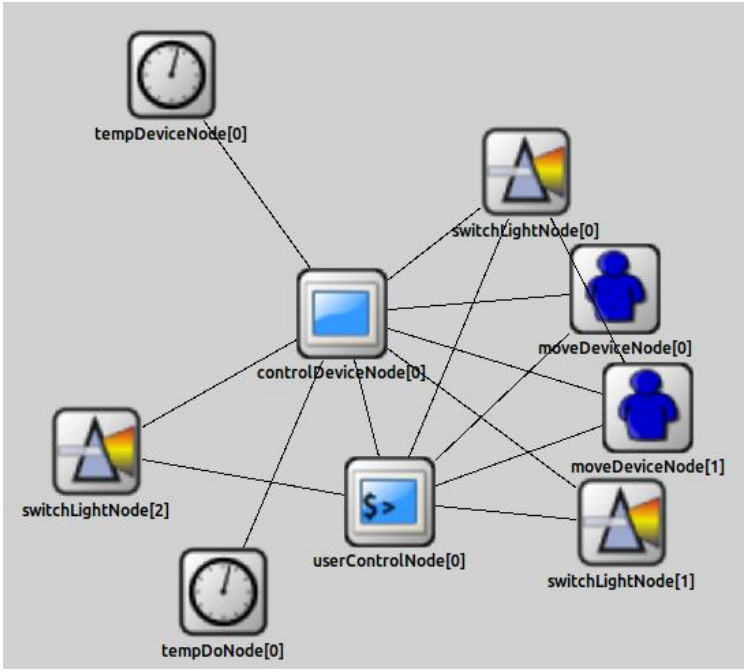

Рис. 3. Упрощенная модель системы “Умный дом”

Для проведения эксперимента был создан сценарий по которому модель системы “Умный дом” давала данные об информационных потоках в сети, а искусственная нейронная сеть выносила решения на основе предоставленных данных.

В модели “Умный дом” было использовано два ключевых устройства: controlDeviceNode (устройство с детектором аномалий) и tempDeviceNode (источник

аномального трафика). Была смоделирована ситуация, когда в трафик сети встраивались дополнительные потоки данных, отсутствующие при нормальном режиме работы. Так, если опрос всех устройств с их данными (отправка запроса на получение пакета) проходит каждые 5 минут, то источник tempDeviceNode начинал передавать случайным адресатам сообщения каждую минуту. Полученные данные позволяют провести анализ количества входящих пакетов за единицу времени на промежуточном узле controlDeviceNode с помощью искусственной нейронной сети. [11]

Конфигурация искусственной нейронной сети:

1. слой Кохонена: размер входного вектора - 2, количество нейронов в слое - 2; скорость обучения - 0,25; размер обучающей выборки - 10000;
2. персептрон: размер входного вектора - 2; количество слоев - 2; количество нейронов в каждом слое 10 и 5 соответственно; скорость обучения - 0,5; размер обучающей выборки - 10000;

Для тестирования были созданы обучающая и тестовая выборки размером в 10000 каждая. В тестовой выборке содержалось 129 аномальных состояний. Аномалией считалось состояние, для которой результат искусственной нейронной сети не ниже 0,9. Результаты обработки данных представлены в таблице.

Таблица 1

Результаты эксперимента

		Смоделированное состояние	
		Аномалия	Не аномалия
Результат работы искусственной нейронной сети	Аномалия	118	11
	Не аномалия	0	9871

Вычислим точность L = 100% * 118/(11+118) = 91,47%

Заключение

В работе представлен механизм выявления аномалий сети системы “Умный дом” на основе искусственной нейронной сети. Предложенный метод позволит вневедомственным подразделениям обеспечить контроль за внутренним состоянием критических узлов системы сигнализации с точностью 91,47% определения постороннего вмешательства и своевременное реагирование на попытки взлома их программной составляющей.

На данный момент определены метрики сети системы “Умный дом”, определена структура искусственной нейронной сети, а также разработан программный комплекс для выявления аномалий.

Для реализованного метода проведен эксперимент в системе моделирования IDE Omnet++.

Примечания:

1. Бессонова Е.Е., Ефремов А.А., Настека А.В., Овсяникова В.В., Салахутдинова К.И., Трофимов А.А. Россия, Санкт-Петербург, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики Анализ защищенности систем «Умный Дом» // Региональная информатика «РИ-2014» Материалы конференции 2014. (124). [Электронный ресурс]. URL: http://spoisu.ru/files/ri/ri2014/ri2014_materials.pdf
2. Настека А.В., Бессонова Е.Е., Аутентификация устройств автоматизации в системе “Умный дом” // Вестник Полиции, 2015, Том (4), издание. 2, 68-74 с.

3. Осовский С. Нейронные сети для обработки информации / Пер. с польского И.Д. Рудинского. М.: Финансы и статистика, 2002. 344 с.

4. Стариковский А.В. Исследование уязвимостей систем умного дома [Текст] / А.В. Стариковский, И.Ю. Жуков, Д.М. Михайлов, А.М. Толстая, Ф.В. Жорин, В.В. Макаров, А.Б. Вавренюк // Спецтехника и связь. 2012. №2. С. 55-57.

5. Безопасность АСУЗ. Можно ли взломать Умный дом? [Электронный ресурс]. URL: http://www.cnews.ru/reviews/?2011/01/24/424494

6. СТО НП "АВОК" 8.1.2-2008 Стандарт АВОК. Автоматизированные системы управления зданиями. Часть 2. Технические средства.

7. СТО НП "АВОК" 8.1.3-2007 Стандарт АВОК. Автоматизированные системы управления зданиями. Часть 3. Функции.

8. Mario B.B., Candid W, Insecurity in the Internet of Things // SECURITY RESPONSE. 2015. P 9-14.

9. Raja Jurdak, X. Rosalind Wang, Oliver Obst, Philip Valencia, Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies // Intelligence-Based Systems Engineering. 2011. P 309-325, ISBN 978-3-642-17931-0

10. User Manual OMNeT++ version 4.6 [Электронныйресурс] URL: https://omnetpp.org/doc/omnetpp/manual/usman.html

11. Нырков А.П., Каторин Ю.Ф., Соколов С.С., Ежгуров В.Н. Основные принципы построения защищенных информационных систем автоматизированного управления транспортно-логическим комплексом. //Проблемы информационной безопасности. Компьютерные системы. 2013. № 2 (2). С. 54-58.

References:

1. Bessonova E.E., Efremov A.A., Nasteka A.V., Ovsyanikova V.V., Salakhutdinova K.I., Trofimov A.A. Rossiya, Sankt-Peterburg, Sankt-Peterburgskii natsional'nyi issledovatel'skii universitet informatsionnykh tekhnologii, mekhaniki i optiki Analiz zashchishchennosti sistem «Umnyi Dom» // Regional'naya informatika «RI-2014» Materialy konferentsii 2014. (124). [Elektronnyi resurs]. URL: http://spoisu.ru/files/ri/ri2014/ ri2014_materials.pdf

2. Nasteka A.V., Bessonova E.E., Autentifikatsiya ustroistv avtomatizatsii v sisteme “Umnyi dom” // Vestnik Politsii, 2015, Tom (4), izdanie. 2, 68-74 s.

3. Osovskii S. Neironnye seti dlya obrabotki informatsii / Per. s pol'skogo I.D. Rudinskogo. M.: Finansy i statistika, 2002. 344 s.

4. Starikovskii A.V. Issledovanie uyazvimostei sistem umnogo doma [Tekst] / A.V. Starikovskii, I.Yu. Zhukov, D.M. Mikhailov, A.M. Tolstaya, F.V. Zhorin, V.V. Makarov, A.B. Vavrenyuk // Spetstekhnika i svyaz'. 2012. №2. S. 55-57.

5. Bezopasnost' ASUZ. Mozhno li vzlomat' Umnyi dom? [Elektronnyi resurs]. URL: http://www.cnews.ru/reviews/?2011/01/24/424494

6. STO NP "AVOK" 8.1.2-2008 Standart AVOK. Avtomatizirovannye sistemy upravleniya zdaniyami. Chast' 2. Tekhnicheskie sredstva.

7. STO NP "AVOK" 8.1.3-2007 Standart AVOK. Avtomatizirovannye sistemy upravleniya zdaniyami. Chast' 3. Funktsii.

8. Mario B.B., Candid W, Insecurity in the Internet of Things // SECURITY RESPONSE. 2015. P 9-14.

9. Raja Jurdak, X. Rosalind Wang, Oliver Obst, Philip Valencia, Wireless Sensor Network Anomalies: Diagnosis and Detection Strategies // Intelligence-Based Systems Engineering. 2011. P 309-325, ISBN 978-3-642-17931-0

10. User Manual OMNeT++ version 4.6 [Elektronnyiresurs] URL: https://omnetpp.org/doc/omnetpp/manual/usman.html

11. Nyrkov A.P., Katorin Yu.F., Sokolov S.S., Ezhgurov V.N. Osnovnye printsipy postroeniya zashchishchennykh informatsionnykh sistem avtomatizirovannogo upravleniya transportno-logicheskim kompleksom. //Problemy informatsionnoi bezopasnosti. Komp'yuternye sistemy. 2013. № 2 (2). S. 54-58.

УДК 004.056

Выявление аномалий в системах автоматизации объектов охраны

[1]Антон Николаевич Канев
[2]Александр Владимирович Настека
[3]Екатерина Евгеньевна Бессонова

[1] Университет ИТМО, Российская Федерация
197101 Санкт-Петербург, Кронверкский проспект, 49
E-mail: kanev.a.n@mail.ru
[2] Университет ИТМО, Российская Федерация
197101 Санкт-Петербург, Кронверкский проспект, 49
E-mail: nasteka.av@gmail.com
[3] Университет ИТМО, Российская Федерация
197101 Санкт-Петербург, Кронверкский проспект, 49
Кандидат технических наук, ассистент
E-mail: merom812@gmail.com

Аннотация. Данная статья рассматривает проблему выявления аномалий в системе автоматизации объектов охраны. Подробно рассмотрен метод выявления аномалий на основе использования гибридной нейронной сети, а также описывается программный комплекс, реализующий механизм выявления аномалий, и проведенный эксперимент.

Ключевые слова: информационная безопасность, домашняя автоматизация, устройства автоматизации, искусственная нейронная сеть.