УДК 004.05

СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В СЕТЯХ ШИРОКОПОЛОСНОГО РАДИОДОСТУПА СТАНДАРТА IEEE 802.11

Д. В. Юркин[a], *канд. техн. наук, доцент*
В. Н. Никитин[a], *канд. техн. наук, доцент*
[a]*Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, РФ*

Постановка проблемы: *исследования разработчиков систем IDS и IPS определили типовую модель системы обнаружения вторжений, которая предназначена для обнаружения и блокировки типовых атак в проводной среде передачи данных. Однако, несмотря на повсеместное развертывание радиосетей передачи данных, проблема методов обнаружения вторжений и способов борьбы с ними недостаточно исследована. Целью работы является разработка методов автоматизации систем предотвращения вторжений в беспроводных сетях радиодоступа.* ***Методы:*** *сигнатурный и эвристический анализ сетевого трафика, корреляционный анализ попыток несанкционированного доступа.* ***Результаты:*** *разработаны основные принципы построения системы обнаружения вторжений в беспроводных сетях. Разработаны требования к реализации методов сбора и анализа данных IDS. Представлена технология обнаружения нарушителя в критических точках целевой IT-системы, использующая метод оценки уровня принятого сигнала RSSI и метод разности времен прихода сигнала TDoA. Разработаны методы сканирования радиоканала, позволяющие обнаруживать вторжения как в автономных системах, так и в системах с централизованной обработкой событий.* ***Практическая значимость:*** *результаты исследований позволяют повысить безопасность существующих распределенных сетей радиодоступа.*

Ключевые слова *— системы обнаружения вторжений, беспроводные сети передачи данных.*

Введение

В настоящее время бурного развития мультисервисных беспроводных сетей вопросам информационной безопасности уделяется большое внимание. В связи с особенностями организации сетей передачи данных с использованием оборудования широкополосного радиодоступа (ШРД) к сетям предъявляются повышенные требования по защите информации [1]. Наряду с методами криптографической инкапсуляции [2], аутентификации [3] и управления доступом к среде передачи данных на канальном уровне OSI/ISO также важны методы предотвращения злонамеренного воздействия средствами системы обнаружения вторжений (СОВ, Intrusion Detection System — IDS).

Для функционирования СОВ в сетях стандартов IEEE 802.11 может использоваться как одна, так и несколько точек доступа (ТД), причем с увеличением их числа точность позиционирования стороннего устройства увеличивается. Наиболее эффективной считается схема, в которой несколько ТД не участвуют в передаче данных абонентов, а используются только в режиме сенсора (Rogue Detector).

Специфика развертывания [4] сетей ШРД ставит следующие задачи перед СОВ [5] в мультисервисных распределенных сетях передачи данных стандарта IEEE 802.11:

1) обнаружение всех сторонних радиоустройств в пределах зоны покрытия радиосети;

2) классификация сторонних радиоустройств в пределах зоны покрытия радиосети;

3) подробный анализ активности сторонних устройств;

4) оценка степени угрозы, вызываемой активностью стороннего устройства;

5) определение физического местоположения стороннего устройства;

6) обезвреживание стороннего устройства с использованием как проводных, так и беспроводных алгоритмов.

Основные принципы реализации СОВ в сетях радиодоступа

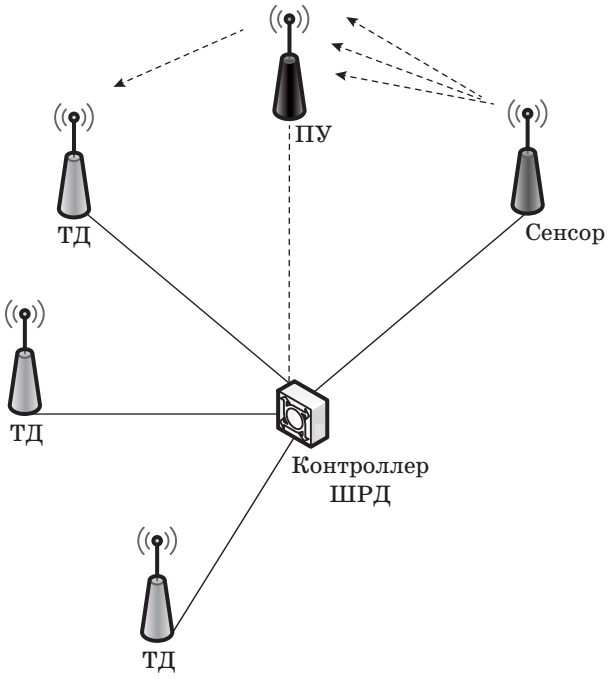
На примере реализации системы wIPS (wireless Intrusion Prevention System) (рис. 1) проиллюстрируем процесс детектирования [7] посторонних устройств (ПУ) ШРД.

Общая схема защиты от ПУ [5], работающих в зоне видимости сети ШРД, в которой работает СОВ, выглядит следующим образом.

Обнаружение [Detect] — обнаружение неинфраструктурных ТД и клиентов одноранговых подключений, а также ПУ стандарта IEEE 802.11n.

Классификация [Classify] — категорирование (over-the-air и on-the-wire) ПУ по уровню принятого сигнала RSSI (Receive Signal Strength Indications) и SSID (Service Set IDentifier), клиентам и пр., проверка нахождения ПУ в проводном сегменте, алгоритм Switch port tracing.

Обезвреживание [Mitigate] — изоляция (Shutdown, Contain и т. д.) нарушителей в радиоканале, отключение (Shutdown) порта на коммутаторе, обнаружение местоположения.



■ ***Рис. 1.*** Детектирование посторонних устройств ШРД

Локализация [Locate] — определение координат местоположения и типа радиоустройства в зоне развертывания беспроводной локальной вычислительной сети (БЛВС).

Согласно данной схеме, обнаружение ПУ [6] сенсором может осуществляться в режиме:

1) обслуживания клиентов с переключением на другие каналы для сканирования (local mode), где каждый канал прослушивается в течение времени T_{scan} в режиме сканирования всех каналов, или каналов данного регуляторного домена, или DCA-каналов;

2) сканирования Monitor Mode, в котором каждый канал прослушивается в течение времени T_{scan} и сканируются все каналы.

Согласно алгоритму работы экземпляра СОВ, любая ТД, которая имеет неизвестные значения RF Group name или mobility group, считается ПУ, при этом автономные ТД, управляемые беспроводным контроллером (БК), автоматически заносятся в список разрешенных устройств. В СОВ имеется система классификации ПУ по SSID и RSSI, основанная на анализе соответствия этих параметров условиям эксплуатации СОВ.

Режим ТД Rogue Detector предписывает отслеживание всех ARP-запросов от посторонних ТД и их клиентов, а БК в свою очередь делает запрос на Rogue Detector для определения наличия посторонних клиентов в проводном сегменте ЛВС.

Режим работы СОВ по протоколу Rogue Location Discovery Protocol (RLDP) обеспечивает обнаружение ПУ посредством подключения инфраструктурных ТД к ПУ в качестве клиента и отправки пакета на IP-адрес контроллера (функционирование возможно только для ПУ с open SSID).

Режим работы БК Switchport Tracing обеспечивает обнаружение ПУ способом определения CDP Neighbors для ТД, которая обнаружила ПУ, и просмотра CAM-таблиц коммутаторов на предмет наличия в них MAC-адресов и клиентов ПУ.

Основные методы обнаружения ПУ приведены в таблице.

Изоляция проводится после детектирования, обнаружения и классификации ПУ в режимах Local Mode, Monitor Mode и H-REAP. Подсистема изоляции ПУ осуществляет либо ручную, либо автоматическую блокировку сторонних ТД и клиентских устройств путем отправки De-Authentication пакетов блокируемому клиенту или широковещательных пакетов от блокируемой ТД.

■ Основные методы обнаружения ПУ wIPS

Алгоритм	Порядок действий	Объект детектирования	Оценка точности
Switchport Tracing	1. ТД детектирует ПУ в радиоканале 2. ТД уведомляет о коммутаторах 3. БК проверяет соседние коммутаторы 4. БК сообщает результаты в порядке их вероятности 5. Администратору предоставляется возможность отключить порт коммутатора	Open APs Secured APs NAT APs	Средняя
RLDP	1. ТД детектирует ПУ в радиоканале 2. ТД подключается к ПУ как клиент 3. ТД посылает RLDP-пакет 4. Если RLDP-пакет получен контроллером, то ПУ имеет выход в ЛВС	Open APs NAT APs	Гарантированная
Rogue Detector	1. Детектор подключается в режиме транка 2. Детектор получает набор MAC-адресов ПУ 3. Детектор ищет MAC-адреса ПУ в ARP-запросах	Open APs Secured APs	Высокая

Режимы сканирования радиоканала

Для обеспечения сбора информации об активности радиоустройств ТД должен вестись постоянный мониторинг передаваемых по радиоканалу данных как абонентскими устройствами, так и другими ТД. Данная задача решается путем перехода ТД в режим радиочастотного (РЧ) сканирования, в котором ТД передает анализатору СОВ следующие данные:

— MAC-адрес ПУ;

— MAC-адреса подключенных клиентов;

— кадры, инкапсулированные по протоколам WEP и WPA;

— преамбулы захваченных кадров;

— отношение сигнал/шум детектированных сигналов;

— мощность RSSI источника;

— номер канала ПУ;

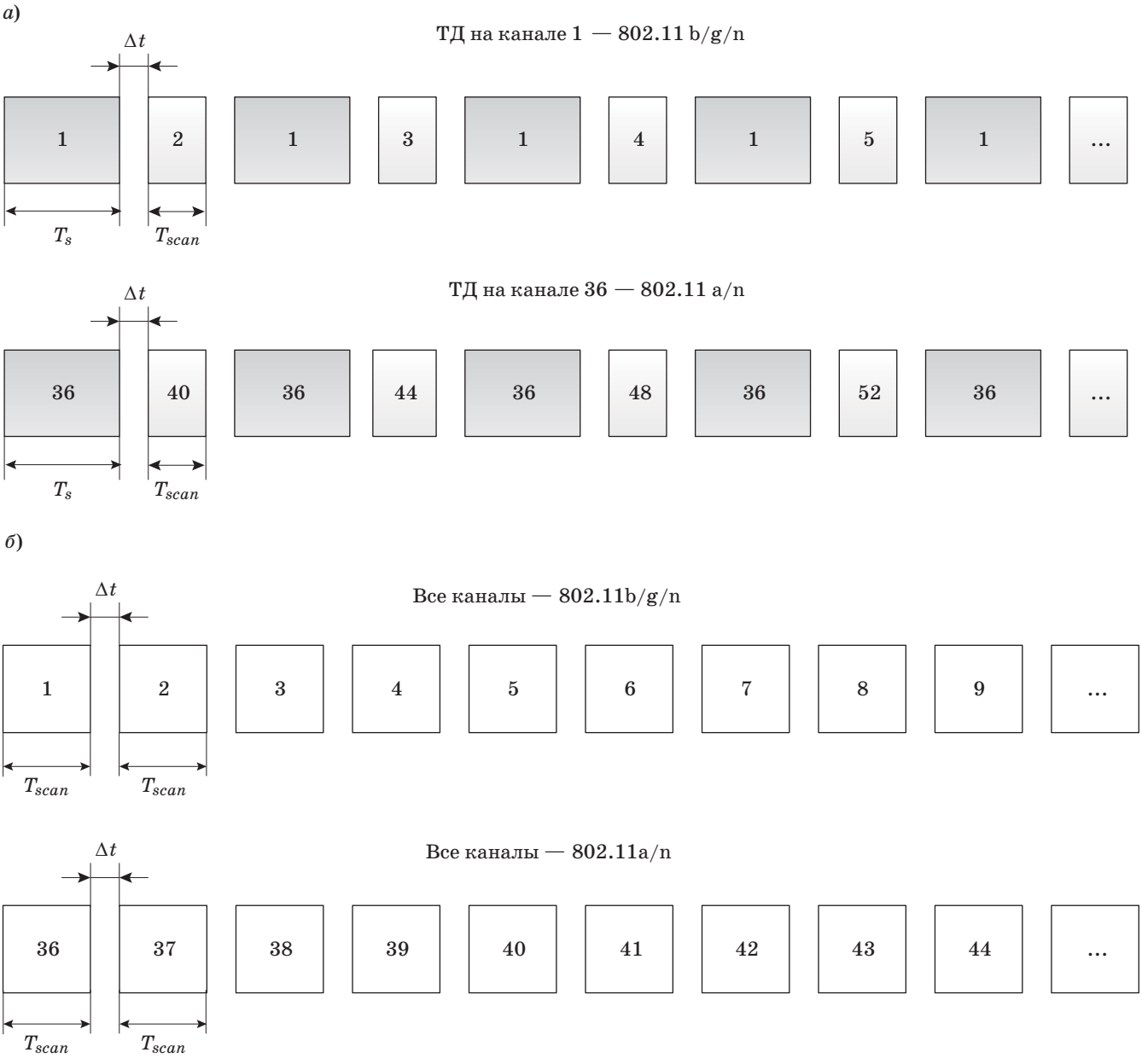
— SSID ПУ;

— IP-адрес ПУ;

— время обнаружения ПУ.

Требования [4] к современным мультисервисным сетям передачи данных оговаривают, что функционировать ТД могут в одном из следующих режимов: Local, H-REAP, Monitor, Rogue detector, Sniffer, Bridge.

Режим Local Mode РЧ-сканирования осуществляется по схеме рис. 2, *а*.



■ ***Рис. 2.*** Режим Local Mode (*а*) и Monitor Mode (*б*) РЧ-сканирования

Технология time-slicing H-REAP подразумевает приостановку обработки данных радиоканала, что позволяет прослушивать канал на протяжении T_{scan} каждые $T_s + \Delta t$ секунд без существенного влияния на качество оказания сервисов БЛВС (T_s — время передачи кадра).

Режим Monitor Mode РЧ-сканирования осуществляется по схеме рис. 2, *б*. Данная технология подразумевает отказ от обслуживания абонентов в пользу постоянного мониторинга радиоканала.

Особенности реализации адаптивных СОВ

Основным фактором, влияющим на топологию системы, является масштаб развертываемой БЛВС. В случае проектирования сети крупной организации, расположенной на площади, в несколько десятков раз превышающей зону покрытия одной ТД, необходимо развертывать сложную радиоканальную инфраструктуру. При этом следует учитывать тот факт, что атакующий [8, 9] субъект может перемещаться в пределах БЛВС или оказывать множественные воздействия на ее элементы.

Если в сети ШРД будет отсутствовать единый центр обработки событий сетевой активности, то множественные регистрируемые сенсорами ТД события будут иметь хаотичный характер, и по ним будет невозможно определить как источник, так и тип самого воздействия. Регистрация отдельных разрозненных событий сети ШРД не позволит администратору СОВ создать общую картину злонамеренных действий атакующего, и он может воспринять их как ложные срабатывания. Поэтому в данном случае необходимо использовать единый центр обработки данных событий БЛВС, соответствующих специальным корреляционным сигнатурам СОВ.

Обеспечить работу механизмов корреляции атак можно путем подключения всех контроллеров БЛВС по схемам, представленным на рис. 3, *а*, *б*.

В схеме, представленной на рис. 4, все сигналы от контроллеров БЛВС об обнаружении тревог консолидируются в едином узле, а после анализа их происхождения выдается сигнал обнаружения атаки в пределах контролируемой сети.

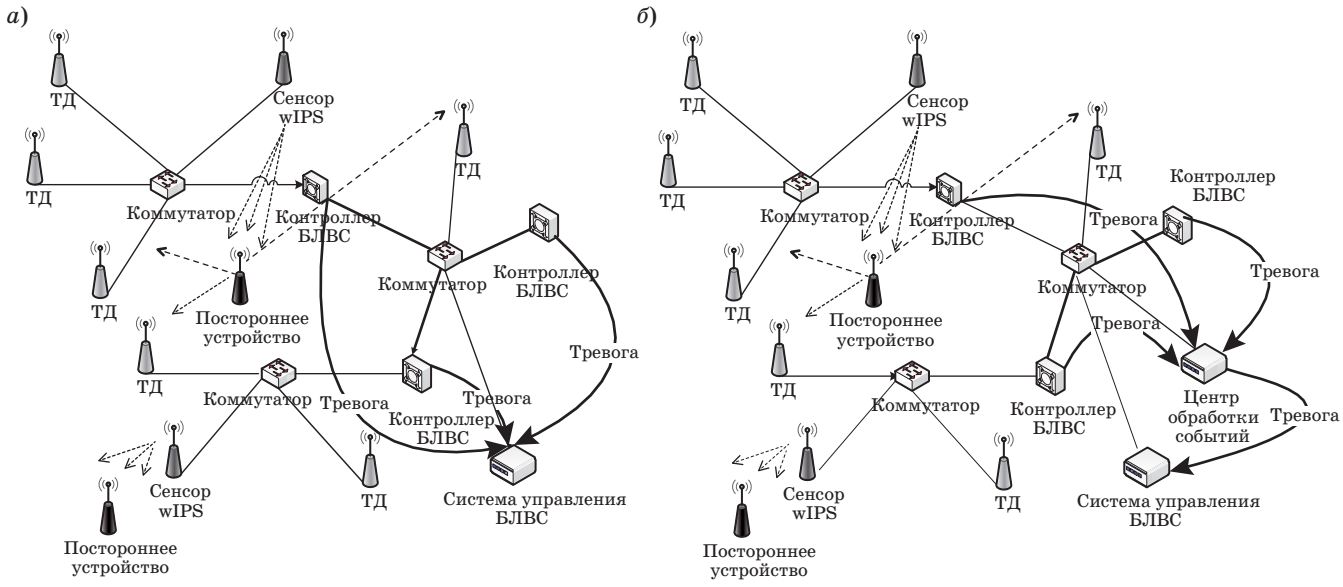
Система wIPS сохраняет всю информацию по передаваемым кадрам, составляющим обнаруженную угрозу, в соответствии с сигнатурой для ее дальнейшего анализа. Данная информация заносится в журнал отчетов, размещенный в центре обработки событий, и служит основным источником для формирования отчетности в системе управления БЛВС.

Для анализа уязвимостей БЛВС [10], защищаемой адаптивной СОВ, наиболее востребованными являются два типа отчетов — со списком wIPS-сигналов тревоги и идентификаторов ТД.

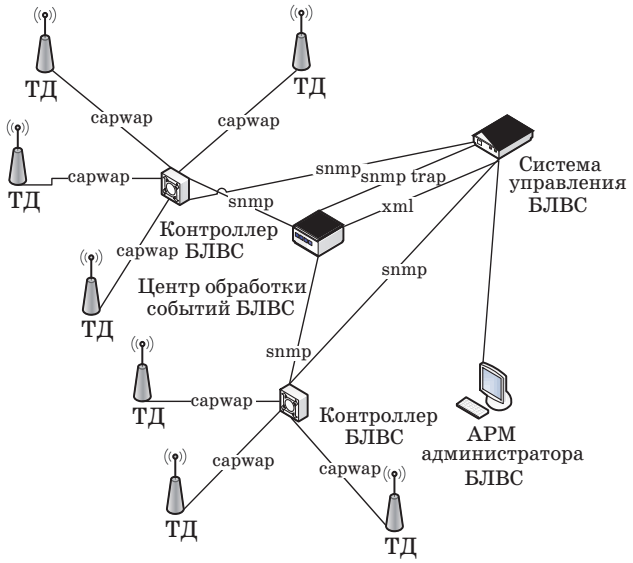
Отчет со списком wIPS-сигналов тревоги используется для отчетности об атаках и содержит:

1) сводный список сигналов тревоги;
2) тип сигнала тревоги;
3) SRC MAC;
4) идентификатор обнаружившей ТД;
5) время первого и последнего обнаружения.

Отчет со списком идентификаторов ТД используется для идентификации наиболее подверженных атакам зон радиопокрытия. Включает в себя рейтинг ТД с самым большим количеством ранжированных сигналов тревоги.



■ ***Рис. 3.*** Различия топологий БЛВС с базовой (*а*) и адаптивной (*б*) СОВ



■ ***Рис. 4***. Взаимодействие компонентов wIPS

Система определения местоположения устройств

В состав проектируемой защищенной БЛВС включается система определения местоположения радиоустройств. Эта подсистема может быть как установлена на сервер системы управления, так и включена в состав контроллера БЛВС. Данная подсистема обеспечивает определение местоположения клиентских абонентских устройств (как входящих в состав сети, так и сторонних ТД и их клиентов), осуществляет мониторинг активности и фиксирует маршруты перемещения устройств, находящихся в зоне радиопокрытия БЛВС.

В рамках стандартов IEEE 802.11a/b/g/ радиооборудование обеспечивает возможность определения местоположения активного радиоинтерфейса субъекта, решая такие задачи, как:

— реализация работы алгоритмов позиционирования;

— настройка и корректировка алгоритмов позиционирования;

— отправка информации о местоположении;

— хранение статистики информации о местоположениях;

— хранение информации о радиоустройствах с привязкой к географическим картам.

Система определения местоположения функционирует по двум технологиям:

— метод оценки RSSI;

— метод разности времен прихода сигнала TDoA (Time Difference of Arrival).

Метод оценки RSSI основан на измерениях RSSI элементами инфраструктуры БЛВС. Для функционирования системы определения местоположения клиентов требуется присутствие в БЛВС не менее трех ТД. С увеличением числа ТД в БЛВС точность определения увеличивается. Основными факторами, влияющими на точность определения местоположения, являются:

— плотность размещения ТД;

— расположение ТД друг относительно друга;

— параметры окружающей среды.

Метод различий времен прихода сигнала TDoA основан на разнице во временах получения радиосигнала абонента несколькими ресиверами TDoA. Этот способ обнаружения хорошо работает на открытых пространствах.

Заключение

Несмотря на то, что методы обнаружения и предотвращения вторжений в проводных сетях в настоящее время бурно развиваются, а производители телекоммуникационного оборудования предлагают большое количество эффективных IDS, интенсивность разработки средств обнаружения вторжений в сегменте сетей радиодоступа существенно уступает проводному сегменту. Исследования показывают, что с увеличением числа ТД точность определения местоположения и вероятность ложного обнаружения стороннего радиоустройства повышаются. В территориально распределенных системах обнаружения вторжений целесообразно использовать алгоритмы корреляции сигналов тревоги, при этом вероятность ложного срабатывания снижается, а точность обнаружения повышается.

Литература

1. **Зегжда Д. П., Коваленко С. Л.** Проблемы безопасности беспроводных сетей семейства IEEE 802.11a/b/g // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 45–49.
2. **Юркин Д. В., Никитин В. Н.** Анализ протоколов шифрования. Журнал радиоэлектроники. 2009. Т. 11. № 4. http://jre.cplire.ru/jre/apr09/5/text.html (дата обращения: 14.10.2013).
3. **Юркин Д. В., Никитин В. Н.** Улучшение способов аутентификации для каналов связи с ошибками // Информационно-управляющие системы. 2010. № 6. С. 24–29.
4. **Common** Criteria for Information Technology Security Evaluation. Part 1: Introduction and General Model, Version 3.1 // Common Criteria Portal. 2006. http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf (дата обращения: 20.10.2013).

5. **Common** Criteria for Information Technology Security Evaluation. Part 2: Security Functional Requirements, Version 3.1. // Common Criteria Portal. 2006. http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf (дата обращения: 20.10.2013).
6. **Watkins L., Robinson W. H., Beyah R. A.** A Passive Approach to Rogue Access Point Detection // Global Telecommunications Conf., Washington, 2007. P. 355–360.
7. **Chong E., Loo M., Christopher L., Marimuthu P.** Intrusion Detection for Routing Attacks in Sensor Networks // Intern. J. of Distributed Sensor Networks. 2006. Vol. 2. N 1. P. 313–332.
8. **Chung-Hsin L., Po-Cheng T., Chun-Lin L., Kuo-Hao L.** The Study of the Wireless Network Dos Attack // Proc. of the 2nd Intern. Conf. on Interaction Sciences: Information Technology, Culture and Human. N. Y., 2009. P. 418–421.
9. **Марков А. С., Рауткин Ю. В., Фадин А. А.** Состояние и перспективы анализа защищенности Wi-Fi сетей // Тр. Научно-исследовательского института радио. 2012. № 1. С. 85–90.
10. **Hongda Yin, Guanling Chen, Jie Wang.** Detecting Protected Layer-3 Rogue APs. Broadband Communications // Networks Broadband Communications: Networks and Systems. Raleigh, 2007. P. 449–458.

UDC 004.05

Intrusion Detection Systems in IEEE 802.11 Local Wireless Networks

Yurkin D. V.[a], PhD, Associate Professor, dvyurkin@yandex.ru
Nikitin V. N.[a], PhD, Associate Professor, vnikitin@rdnet.ru
[a]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, 22-1, Bolshevikov St., 193232, Saint-Petersburg, Russian Federation

Purpose: The research of developers of IDS and IPS has provided an operational model of an intrusion detection system which can detect and block typical wireless attacks in a wire system of data transfer. Yet the problem of techniques for monitoring, detecting and responding to information technology security breaches is very relevant in IEEE 802.11 radio networks. This research has been targeted at development of methods of system automation for preventing attacks on organization's wireless access points. **Methods:** signature and heuristic analysis of network traffic, correlation analysis of intrusion attempts. **Results:** There have been developed basic principles of constructing a system of intrusion detection in wireless networks. There have been worked out requirements for the methods of IDS data collection and analysis. There has been presented a technology of intruder detection at strategic points of a target IT system applying a method of evaluation of a received RSSI signal and a method of difference of TDoA signal arrival. There have been developed methods of radio channel scanning allowing detecting attacks in both autonomous systems and systems with central event processing. **Practical relevance:** The research results allow increasing the safety of the existing distributed radio networks.

Keywords — Intrusion Detection System, Wireless Local Networks..

References

1. Zegzhda D. P., Kovalenko S. L. Problems of Radio Networks Std. IEEE 802.11a/b/g security. *Problemy informatsionnoi bezopasnosti. Komp'iuternye sistemy*, 2006, vol. 1, no. 2, pp. 45–49 (In Russian).
2. Yurkin D. V., Nikitin V. N. Analyses of Encryption Protocols. *Zhurnal radioelektroniki,* 2009, vol. 11, no. 4. Available at: http://jre.cplire.ru/jre/apr09/5/text.html (accessed 20 October 2013) (In Russian).
3. Yurkin D. V., Nikitin V. N. Improving Authentication Methods for Error Prone Channels. *Informatsionno-upravliaiushchie sistemy*, 2010, no. 6, pp. 24–29 (In Russian).
4. Common Criteria for Information Technology Security Evaluation. Part 1. Introduction and General Model, Version 3.1. *Common Criteria Portal*, 2006. Available at: http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf (accessed 20 October 2013).
5. Common Criteria for Information Technology Security Evaluation. Part 2. Security Functional Requirements, Version 3.1. *Common Criteria Portal*, 2006. Available at: http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf (accessed 20 October 2013).
6. Watkins L., Robinson W. H., Beyah R. A. A Passive Approach to Rogue Access Point Detection. *Global Telecommunications Conf.* Washington, 2007, pp. 355–360.
7. Chong E., Loo M., Christopher L., Marimuthu P. Intrusion Detection for Routing Attacks in Sensor Networks. *International Journal of Distributed Sensor Networks,* 2006, vol. 2, no. 1, pp. 313–332.
8. Chung-Hsin L., Po-Cheng T., Chun-Lin L., Kuo-Hao L. The Study of the Wireless Network Dos Attack. *Proc. of the 2nd Intern. Conf. on Interaction Sciences: Information Technology, Culture and Human.* New York, 2009, pp. 418–421.
9. Markov A. S., Rautkin Iu. V., Fadin A. A. Status and Prospects of Security Analysis Wi-Fi Networks. *Trudy Nauchno-issledovatel'skogo instituta radio,* 2012, vol. 1, no. 12, pp. 85–90 (In Russian).
10. Hongda Yin, Guanling Chen, Jie Wang. Detecting Protected layer-3 Rogue APs. *Broadband Communications, Networks and Systems.* Raleigh, 2007, pp. 449–458.