MASKAY 6(1), Nov 2016
ISSN 1390-6712

Recibido (Received): 2016/09/24
Aceptado (Accepted): 2016/11/01

Estado del Arte en la detección de intrusiones en las redes 802.11i

The state of the art in intrusion detection in 802.11i networks

Carlos G. Romero, Luis A. Balseca, Fabián Sáenz, Javier Díaz

***Resumen*— En este artículo se presenta un análisis de los diversos mecanismos de seguridad existentes que agregan diferentes niveles de seguridad en las redes inalámbricas. Así también se describe una herramienta altamente empleada para la detección de intrusiones de red, los llamados sistemas de detección de intrusos inalámbricos (WIDS), finalmente se recopila información significativa y actualizada para identificar las diferentes técnicas desarrolladas para la detección de intrusiones en redes 802.11.**

***Palabras Clave*— Wifi, 802.11i, WIDS, detección de intrusiones, WPA2**

***Abstract*— In this paper an analysis of existing security mechanisms that improve security levels in wireless networks is presented. A highly used device for detecting network intrusion, called detection systems wireless intruders (WIDS) is also described, finally, meaningful and updated information is presented to identify different techniques developed for intrusion detection 802.11.**

***Index Terms*— Wifi, 802.11i, WIDS, Intrusion Detection, WPA2**

I. INTRODUCCIÓN

Con el amplio y rápido despliegue de las redes y de los dispositivos inalámbricos, han ido en aumento los retos concernientes a su seguridad. Con el anexo 802.11i de la IEEE [1], publicado en el año 2004, se lograron solventar en gran medida algunos problemas de seguridad en el ámbito de la confidencialidad y la integridad, pero los problemas asociados a la disponibilidad aún no han sido investigados con profundidad [2][3]. Adicionalmente, aparecen nuevas vulnerabilidades inherentes a la operación y la implementación de este estándar [4] [5], las cuales dan a lugar a posibles nuevos ataques.

El uso de IEEE802.11i RSN (*Robust Secure Network*) conlleva significativas mejoras en seguridad (Xing, Shakshuki, Benoit, & Sheltami, 2008) y el empleo de CCMP (*Counter Mode with Cipher Block Chaining MAC Protocol*) agrega confidencialidad e integridad a la comunicación, acompañado de 802.1x [7], permite la autenticación mutua entre el AP (*Access Point*) y la STA (*Station*).

Desafortunadamente, este estándar no ofrece protección a las tareas para la operación de la red que utilizan las tramas de control y de gestión, y no trata el tema de la disponibilidad para ninguno de los tres tipos de tramas (control, gestión y datos). Debido a que la información contenida en los paquetes de gestión y de control de la capa de enlace de datos o capa MAC (*Medium Access Control*) no está encriptada [1], se puede extraer y explotar la información de los protocolos y sus implementaciones para provocar ataques a la disponibilidad [8] [5], y al funcionamiento de la red.

Carlos G. Romero, Luis A. Balseca, Fabián Sáenz are with Departamento de Eléctrica y Electrónica, Universidad de las Fuerzas Armadas ESPE, Sangolquí, Av. General Rumiñahui s/n, 171-5-231B Ecuador. Javier Díaz is with Universidad Nacional de la Plata UNLP La Plata.

II. DETECCIÓN DE INTRUSIONES

A través del análisis del tráfico de la red se pueden detectar posibles ataques, especialmente aquellos que buscan alterar la disponibilidad de la información y de los servicios, para lo cual se han desarrollado herramientas de software y hardware llamadas Sistemas de Detección de Intrusiones (IDS). Estos sistemas pueden ser divididos en dos grandes categorías, dependiendo de la estrategia de análisis y detección de dichos eventos: los IDS basados en la detección de uso indebido y los basados en la detección de anomalías [9].

III. SISTEMAS DE DETECCIÓN DE INTRUSIONES EN REDES 802.11

Un sistema inalámbrico de detección de intrusiones (WIDS) está basado en un conjunto de sensores y un nucleo que recibe toda la información proporcionada en todas las areas de cobertura de los sensores inalámbricos.

A. Arquitectura

Un WIDS puede ser:

1. Centralizado

Basado en la combinación de sensores individuales los cuales recopilan y remiten todos los datos 802.11 a un analizador central, donde los datos son almacenados y procesados.

Ventajas.-
- Permite una fácil administración de protección a áreas grandes de redes 802.11. Expansiones a la red afectan solamente a él analizador.
- Permite una gran visión de lo que ocurre en todas las partes de la redes 802.11.

Desventajas.-
- Si el analizador falla, los sensores se vuelven inútiles y toda la red queda sin la protección.

2. Distribuido

Suele incluir uno o más dispositivos que se encargan tanto de la recolección y procesamiento de la información de los IDS.

Ventajas.-

- No hay un solo punto de fallo

Desventajas.-

- El costo de sensores con alta capacidad de procesamiento puede llegar a ser exagerado cuando muchos sensores son requeridos.

- La administración de múltiples sensores de procesamiento de información puede ser más difícil que la de un modelo centralizado.

- Expansiones en la red provocará una reprogramación en todos los sensores.

IV. TÉCNICAS EN LA DETECCIÓN DE INTRUSIONES EN REDES 802.11

A. Detección de uso indebido

La estrategia más utilizada para la detección de intrusiones consiste en la detección de uso indebido (patrones) para reconocer ataques previamente conocidos. La mayoría de los IDS disponibles en el mercado son de este tipo [10], donde algunos de los más populares son SNORT [11] y BRO IDS [12]. Dentro de este grupo se pueden destacar investigaciones como[13], donde se expone un método para la selección de las características más relevantes de las tramas para la detección de intrusiones basada en patrones, en redes con el estándar 802.11. Además, se muestra cómo emplear un número muy grande de características puede conllevar a una degradación de la razón de detección del IDS. En [14] [15] se describe cómo a través de modelos de transición de estados se puede representar intrusiones específicas y los autores implementan una herramienta llamada STATS (*State Transition Analysis Tool*) para la detección de intrusiones. Sin embargo, la detección de uso indebido puede acarrear varios problemas como la incapacidad de detectar los ataques nuevos y sus variantes.

La detección de usos indebidos se puede implementar de las siguientes formas:

1. Firmas Simples

La detección de firmas compara los eventos que ocurren, con las cadenas o firmas almacenadas en una base de datos de escenarios de ataque en busca de coincidencias. Su principal inconveniente es la necesidad de desarrollar e incorporar a la base de datos una firma nueva para cada nuevo tipo de ataque o vulnerabilidad descubierta.

2. Análisis de Transición de Estados

Se crean a partir de la construcción de una máquina de estados finitos. Los escenarios de ataques se representan como una secuencia de transiciones que caracterizan la evolución del estado de seguridad de un sistema. Cuando el autómata alcanza un estado considerado como una intrusión, se lanza la alarma. Algunas ventajas son las siguientes:

- Las transiciones ofrecen una forma de identificar una serie de patrones que conforman un ataque.
- El diagrama de estados define la forma más sencilla posible de definir un ataque. Así, el motor de análisis puede utilizar variantes del mismo para identificar ataques similares.
- El sistema puede detectar ataques coordinados y lentos.

Sin embargo, presentan algunas desventajas:
- El lenguaje utilizado para describir los ataques es demasiado limitado, y en ocasiones puede resultar insuficiente para recrear ataque más complejos.
- El análisis de algunos estados puede requerir más datos del objetivo, por parte del motor. Esto reduce el rendimiento del sistema.

3. Sistemas Expertos

Los sistemas expertos tienen el conocimiento codificado mediante reglas de implicación (condición-acción) de tipo *"if-then-else"*para examinar los datos. Realizan análisis mediante funciones internas al sistema, de forma completamente transparente al usuario.

Una de las ventajas más importantes de utilizar reglas *"if-then"* es que mantiene separados el control de razonamiento y la formulación de la solución del problema.

La principal desventaja que se plantea es que los patrones no definen un orden secuencial de acciones.

B. Detección de Anomalías

Los IDS basados en anomalías, por otro lado, detectan desviaciones en el comportamiento esperado o normal de los sistemas y las redes, las cuales pudieran constituir intentos de ataques. Por tal motivo, los IDS basados en el descubrimiento de anomalías son potencialmente capaces de detectar los ataques existentes y los nuevos, sin la necesidad de ser pre-configurados o actualizados de ninguna manera [16].

Los eventos de interés para los IDS basados en anomalías pueden estar definidos de dos maneras: por modelos estadísticos y por modelos *specification-based* [17][18].

1. *Modelos Estadísticos*

Los modelos estadísticos hacen uso de variables o características para estimar el comportamiento de la red, pero necesitan de un periodo de entrenamiento para determinar cuál es el comportamiento esperado o normal de la red.

Dentro de este tipo se pueden destacar las investigaciones de [19] y [20], donde se proponen modelos que consideran la variación temporal de ciertos parámetros del tráfico para determinar el comportamiento de un posible atacante en la red, aunque no hacen uso de ningún parámetro de control o de gestión. En [19] los autores se enfocan en múltiples comportamientos no esperados en WLAN 802.11 pero ponen énfasis en la detección del parámetro de *backoff*. El algoritmo de detección calcula y estima un tiempo promedio de *backoff* y genera una alarma si la estimación es sospechosamente baja.

En [21] Rong *et.al*. realizan una aproximación estadística, usando SPRT (*Sequential Probability Radio Test*) desarrollan un algoritmo para detectar estaciones fraudulentas que modifican sus tiempos de *backoff*. En [22] consideran el problema de un atacante que puede modificar su estrategia de intrusión (con inteligencia), por medio de la técnica "*min-max robust detection*", basándose en un número requerido de observaciones para la decisión, lo cual introduce demoras.

2. *Modelos basados en la especificación*

La detección de intrusiones *specification-based* fue sugerida inicialmente por Ko [23] y más recientemente aplicada en [17] [24] [25]. Este método se basa en describir el comportamiento normal y expresarlo a manera de especificaciones. Las desviaciones a estas especificaciones son tratadas como un evento anormal, pudiéndose tratar de una intrusión. Una especificación puede estar basada en la transición de estados que puede ocurrir durante el comportamiento normal y/o por una expresión específica basada en políticas de seguridad previamente declaradas.

Sekar *et.al*.[17] proponen un IDS para redes cableadas basado en modelación de la máquina de estados de los protocolos, combinado con técnicas estadísticas. En [18] Gill basa su investigación en redes WLAN IEEE802.11 tipo infraestructura y se centra en el esquema RSN, no toma en cuenta pre-RSN (sin el esquema de autenticación de 4 vías de RSN) ni técnicas de respuesta y no se basa en modelos estadísticos o matemáticos para la detección. Proponen como trabajo futuro extraer los modelos de transición de estados de manera automática desde los datos de entrenamiento y desarrollar un extensible y comprensible lenguaje de especificación para incorporar los modelos de transición de estados en una especificación.

En [17] y [26] los autores realizan un análisis temporal de la máquina de estados de redes WLAN 802.11i para la detección de intrusiones, pero aplicado a ataques conocidos.

V. EVALUACION DEL DESEMPEÑO DE IN WIDS

Dada la naturaleza de las redes inalámbricas, detectar intrusiones en WLAN 802.11 se convierte en un reto muy grande porque tanto los APs y como las STAs en la red se comportan de manera no determinada, dependiendo el tráfico que envíe o reciba cada nodo, así como la interferencia en el medio debido al número de nodos conectados o a fallas en la transmisión. El WIDS debe poder detectar eventos que se desvíen del comportamiento normal y determinar si ese comportamiento inusual se debe a una posible intrusión o a la interferencia en el medio de comunicación. Adicionalmente, debe detectar ataques en los protocolos usados en la red inalámbrica, por lo cual necesita concentrarse en protocolos de la capa física y de enlace de datos para detectar potenciales ataques[27] [28][3].

Para evaluar el desempeño de los IDS se utilizan varios criterios, pero si se requiere determinar su efectividad de un modo cuantitativo se han definido los términos de falsos positivos y falsos negativos [9].

Los IDS tradicionales como Snort [11] y su solución comercial Sourcefire [29], RealSecure [30], Cisco Intrusion Detection System [31] o Dragon [32], analizan en los paquetes la información correspondiente a la capa 3 (capa de red) y superiores, a diferencia de los WIDS (*Wireless* IDS), que además utilizan la información de la capa de enlace de datos (capa MAC).
Dentro de los WIDS existentes en el mercado se pueden destacar AirDefense [33], AirTight [34] y algunos de tipo académico como Kismetwireless [35] o Widz [36] los cuales, además de los análisis tradicionales en capa 3 y superiores, integran ciertos filtros que utilizan información la capa MAC para detectar ataques específicos en WLAN como son los APs no autorizados, el *WarDriving*, y las inundaciones.

La limitación de este tipo de herramientas es que, al basarse en la detección de mal uso, no detectan ataques nuevos o desconocidos [37].

Hasta aquí se puede concluir que han sido realizadas varias investigaciones con respecto a métodos y técnicas para la detección de intrusiones en redes WLAN [38]. Utilizando estrategias de detección de usos indebidos y de anomalías o una mezcla de ambas, se logra cierta efectividad en la detección de ataques específicos, previamente conocidos, mostrando bajas tasas de falsos positivos, pero con una incapacidad clara en la detección de ataques nuevos o no conocidos.

Además, dentro del campo de la modelación del comportamiento normal en redes 802.11i para la detección de intrusiones y más específicamente, con los paquetes de gestión y control de la capa MAC, es poco el trabajo realizado [39] [40] [41].

Adicionalmente, de los modelos que estiman el comportamiento normal de una red WLAN utilizando alguno o algunos parámetros de paquetes de gestión y control de la capa MAC, no se han obtenido resultados concluyentes. Ataques de denegación de servicios que afectan a la disponibilidad de las redes y los sistemas son todavía muy difíciles de detectar por los sistemas existentes.

Se ha identificado que para la detección de intrusiones en entornos inalámbricos, se requiere el uso de información de la capa MAC [13] [27] [28].

Por estas razones se hace necesario encontrar una solución científica mediante la cual se pueda estimar el comportamiento normal y anómalo en una red WLAN, en presencia o no de interferencia, utilizando los parámetros de paquetes de control y de gestión de la capa MAC, logrando detectar los ataques nuevos y los conocidos, y reducir el número de falsos positivos y negativos, permitiendo mejorar la efectividad del sistema de detección de intrusiones.

VI. CONCLUSIONES

Además de las vulnerabilidades existentes en los protocolos implementados para la seguridad en redes 802.11, tales como las de los protocolos WEP, WPA y WPA2, existen vulnerabilidades inherentes a la naturaleza del tráfico en una red inalámbrica que hacen posible la explotacion de estas vulnerabilidades a travez de ataques de denegación de servicio (DOS)

Se ve necesario la generación de mecanismos para detectar ataques de denegación de servicios en redes WLAN 802.11i, desde sus tramas básicas, es decir utilizando los parámetros de paquetes de control y gestión de capa MAC.

El desarrollo de WIDS que detectan intrusiones en la capa de enlace constituiría un gran avance en la solución de los problemas de seguridad de las redes inalámbricas, ya que la capa de enlace es la que caracteriza el acceso al medio inalámbrico.

VII. REFERENCIAS

[1] "IEEE Standard for Information Technology- Telecommunications and Information Exchange Between Systems- Local and Metropolitan Area Networks- Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements", *IEEE Std 802.11i-2004*, pp. 0_1 -175, 2004.

[2] Bell Labs. (2007) The Bell Labs security framework: Making the case of End to End Wifi Networks. [En línea]. http://www.forsitegroup.com/pdf/wp_lucent_wifi_security.pdf

[3] A. Tsakountakis, G. Kambourakis, y S. Gritzalis, "Towards effective Wireless Intrusion Detection in IEEE 802.11i", en *Security, Privacy and Trust in Pervasive and Ubiquitous Computing, 2007. SECPerU 2007. Third International Workshop on*, 2007, pp. 37-42.

[4] Songhe Zhao, C.A. Shoniregun, y C. Imafidon, "Addressing the vulnerability of the 4-way handshake of 802.11i", en *Digital Information Management, 2008. ICDIM 2008. Third International Conference on*, 2008, pp. 351-356.

[5] Jing Liu, Xinming Ye, Jun Zhang, y Jun Li, "Security Verification of 802.11i 4-Way Handshake Protocol", en *Communications, 2008. ICC '08. IEEE International Conference on*, 2008, pp. 1642-1647.

[6] Xinyu Xing, E. Shakshuki, D. Benoit, y T. Sheltami, "Security Analysis and Authentication Improvement for IEEE 802.11i Specification", en *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*, 2008, pp. 1-5.

[7] "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control", *IEEE Std 802.1X-2010 (Revision of IEEE Std 802.1X-2004)*, pp. C1 -205, 2010.

[8] Li Wang y B. Srinivasan, "Analysis and Improvements over DoS Attacks against IEEE 802.11i Standard", en *Networks Security Wireless Communications and Trusted Computing (NSWCTC), 2010 Second International Conference on*, vol. 2, 2010, pp. 109-113.

[9] C. F., & Pfleeger, S. L Pfleeger,. Upper Saddle River, NJ: Pearson Education, 2003.

[10] Urko ZURUTUZA, *Estado del Arte: Sistemas de detección de intrusos*.: Universidad Politécnica de Mondragón, Departamento de Informática, 2004. [En línea]. http://www.criptored.upm.es/guiateoria/gt_m399a.htm

[11] Snort IDS. (2010) [En línea]. www.snort.org

[12] BRO Intrusion detection system. (2010) [En línea]. http://www.bro-ids.org/

[13] M. Guennoun, A. Lbekkouri, y K. El-Khatib, "Selecting the Best Set of Features for Efficient Intrusion Detection in 802.11 Networks", en *Proc. 3rd Int. Conf. Information and Communication Technologies: From Theory to Applications ICTTA 2008*, 2008, pp. 1-4.

[14] K. Ilgun, R.A. Kemmerer, y P.A. Porras, "State transition analysis: a rule-based intrusion detection approach", *Software Engineering, IEEE Transactions on*, vol. 21, no. 3, pp. 181-199, 1995.

[15] Bin Dong y Xiu-Ling Liu, "An Improved Intrusion Detection System Based on Agent", en *Machine Learning and Cybernetics, 2007 International Conference on*, vol. 6, 2007, pp. 3164-3167.

[16] H. Debar and J.Viinikka, "Intrusion detection: Introduction", en *FOSAD 2004/2005*, 2005.

[17] R. Sekar et al., "Specification-Based anomaly detection: a new approach for detecting network intrusions", *ACM CCCS*, pp. 265-274, 2002.

[18] Rupinder Gill, Jason Smith, y Andrew Clark, "Specification-Based Intrusion Detection in WLANs", en *Proc. 22nd Annual Computer Security Applications Conf. ACSAC '06*, 2006, pp. 141-152.

[19] I Aad M. Raya, "DOMINO: a system to detect greedy behavior in IEEE 802.11 hotspots", en *Proceedings of the 2nd international conference on Mobile systems applications and services* , 2004, pp. 84-97.

[20] E. Sithirasenan y V. Muthukkumarasamy, "Detecting Security Threats in Wireless LANs Using Timing and Behavioral Anomalies", en *Networks, 2007. ICON 2007. 15th IEEE International Conference on*, 2007, pp. 66-71.

[21] Y. Rong, S.-K. Lee, y H.-A. Choi, "Detecting Stations Cheating on Backoff Rules in 802.11 Networks Using Sequential Analysis", en *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, 2006, pp. 1-13.

[22] A. Cardenas, S. Radosavac, y J. Baras, "Evaluation of Detection Algorithms for MAC Layer Misbehavior: Theory and Experiments", *Networking, IEEE/ACM Transactions on*, vol. 17, no. 2, pp. 605-617, 2009.

[23] C. Ko, "Execution Monitoring of Security-Critical Programs in a Distributed System: A Specification-based Approach", U.C. Davis, California, PhD Thesis 1996.

[24] C. Ko, H. Tseng, P. Balasubramayan, A. Chaudhary, K. Levitt T. Song, "Formal Reasoning About a Specification-Based Intrusion Detection for Dynamic Autoconfiguration Protocols in Ad Hoc Networks", *Formal Aspects in Security and Trust*, pp. 16-33, 2005.

[25] C. Tseng, T. Song, P. Balasubramayam, C. Ko, y K. Levitt, "A Specification-based Intrusion Detection Model for OLSR", en *RAID 2005*, vol. 3858, 2005.

[26] S. Fayssal, S. Hariri, y Y. Al-Nashif, "Anomaly-Based Behavior Analysis of Wireless Network Security", en *Mobile and Ubiquitous Systems: Networking Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on*, 2007, pp. 1-8.

[27] Zhiqi Tao y A.B. Ruighaver, "Wireless Intrusion Detection: Not as easy as traditional network intrusion detection", en *TENCON 2005 2005 IEEE Region 10*, 2005, pp. 1-5.

[28] K. El-Khatib, "Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems", *Parallel and Distributed Systems, IEEE Transactions on*, vol. 21, no. 8, pp. 1143-1149, 2010.

[29] Openfire CyberSecurity. (2010) [En línea]. http://www.sourcefire.com/

[30] RealSecure. (2010) IBM, Internet Security Systems. [En línea]. http://www.iss.net/

[31] Cisco Intrusion Prevention System. (2010) [En línea]. http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html

[32] Dragon IDS. (2010) [En línea]. http://www.enterasys.com/products/ids

[33] Motorola Airdefense Security Solutions. (2010) [En línea]. http://www.airdefense.net/

[34] AirTight Networks. (2010) [En línea]. http://www.airtightnetworks.com/

[35] Kismet IDS. (2010) KismetWireless. [En línea]. www.kismetwireless.net

[36] WIDZ. (2010) Fat-Loud-Blokes-Word-Of-Wierd. [En línea]. http://www.loud-fat-bloke.co.uk/tools.html

[37] Huan-Rong Tang, Rou-Ling Sun, y Wei-Qiang Kong, "Wireless Intrusion Detection for defending against TCP SYN flooding attack and man-in-the-middle attack", en *Proc. Int Machine Learning and Cybernetics Conf*, vol. 3, 2009, pp. 1464-1470.

[38] Hongyu Yang, Lixia Xie, y Jizhou Sun, "Intrusion detection for wireless local area network", en *Electrical and Computer Engineering, 2004. Canadian Conference on*, vol. 4, 2004, pp. 1949 - 1952 Vol.4.

[39] R. Gunasekaran, V. Rhymend Uthariaraj, R. Sudharsan, S. Sujitha Priyadarshini, y U. Yamini, "Detection and prevention of selfish and misbehaving nodes at MAC layer in mobile ad hoc networks", en *Proc. Canadian Conf. Electrical and Computer Engineering CCECE 2008*, 2008, pp. 1945-1948.

[40] S. Usha y S. Radha, "A collective network arbitration protocol to detect MAC misbehavior in MANETS", en *Proc. Int. Conf. Wireless Communication and Sensor Computing ICWCSC 2010*, 2010, pp. 1-5.

[41] R. D. Vallam, A. A. Franklin, y C. Siva Ram, "Modelling co-operative MAC layer misbehaviour in IEEE 802.11 ad hoc networks with heterogeneous loads", en *Proc. 6th Int. Symp. Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops WiOPT 2008*, 2008, pp. 197-206.