Kurdistan Journal of Applied Research (KJAR) | Print-ISSN: 2411-7684 – Electronic-ISSN: 2411-7706 | kjar.spu.edu.iq
Volume 2 | Issue 3 | August 2017 | DOI: 10.24017/science.2017.3.48

Intrusion Detection and Prevention Systems in Wireless Networks

Ibrahim Al-Shourbaji
Computer Network Department, Computer
Science and Information System College,
Jazan University, 82822-
6649 Jazan, Kingdom of Saudi Arabia
ialshourbaji@jazanu.edu.sa

Samaher Al-Janabi
Department of Computer Science, Faculty of
Science for Women, University of Babylon,
Hilla 00964, Iraq
samaher@uobabylon.edu.iq

Abstract:***In society today, public and personal communication are often carried out through wireless technology. These technologies can be vulnerable to various types of attacks. Attackers can access the signal to listen or to cause more damage on the wireless networks. Intrusion Detection and Prevention System (IDPS) technology can be used to monitor and analyze the signal for any infiltration to prevent interception or other malicious intrusion. An overview description of IDPSs and their core functions, the primary types of intrusion detection mechanisms, and the limitations of IDPSs are discussed. This work perceives the requirements of developing new and sophisticated detection and prevention methods based on, and managed by, combining smart techniques including machine learning, data mining, and game theory along with risk analysis and assessment techniques. This assists wireless networks toremain secure and aids system administrators to effectively monitor their systems.***

Keywords: Wireless networks, intrusion-detection and prevention systems, technology, security, risk analysis

1. INTRODUCTION

Today, wireless technology plays a significant role in every aspect of our lives, both personal and public. However, the growth in the use of wireless technology has brought new challenges and limitations to user's privacy [1, 2]. This is because wireless networks are vulnerable to a number of attacks and threats; examples include unauthorized access, Denial of Service (DoS), and Distributed Denial of Service (DDoS) attacks. The intrusion problem in awireless network has become one of the leading causes of concern with the increaseduse of wireless networks [3, 4]. While the intrusion problem has existed for decades, the problem has been rising in intensity and vigor as more end-users use computers, the internet, The Web, mobile, and ad hoc wireless networks[5].

Wireless and mobile networks provide new challenges because of their nature to rely on network signals without exact or known boundaries. In addition, wireless systems are very competitive in regard to their performance, price, and convenience in connection [6]. However, there is a wide-spread, and connection convenience means that an attack can happen at multiple remote locations at any time [7]. Therefore, the field of wireless network and communication security has become essential and needs to be protected from attacks. Further, the integrity and availability of these systems must be protected to provide the necessary facilities to make them safe from unexpected attacks [8].

IDPSs can distinguish whether an activity is an attack attempt or normal system behavior. Such examples of these activities include trying to identify incidents of possible attacks, logging information of the attackers, and alerting the system administrator or trying to prevent them from succeeding. Therefore, by using IDPS, the wireless network activities can be controlled, possible attacks can be avoided, and the risk can be contained [9].

Because of a growing number of intrusion events, security threats, and the ways that the hackers can use to accomplish their goals, the need arises to use smarter IDPSs. This paper focuses on providing an overview of IDPSs, their role in detecting and preventing attacks from succeeding, and their drawbacks in wireless networks. The remainder of this research paper is structured as follows: Section 2 presents the attacks to thewireless network. Section 3 provides a brief outline about Intrusion detection and prevention systems (IDPSs) functions. Section 4 provides the IDPSs limitations. Section 5 provides a discussion of the paper. Section 6 concludes the article and provides future recommendations of this research.

2. LITERATURE REVIEW

There are several ways that attackers can infiltrate wireless networks. The first way is by targeting the various nodes, such as Access Points (AP) within the wireless network to get unauthorized access. The Second way is using a wireless card or Wi-Fi detection technique such as War Driving, which utilizes Nets tumbler, or Kismet [10]. These devices give attackers access to all the private information about the victim machine. Such examples include user identification, encryption method and the channel they are using. With this information, the attackers then can access and exploit the victim machine [11].

There are two main types of attacks on wireless networks, (DDoS) and (DoS). In recent years, there has been a rise in these attacks. For instance, there was a wave of DoS attacks on some big e-commerce and wireless information sites including Yahoo!, E'Trade, Buy.com, and Amazon.com [12]. According toanother recent report by Neustar, the effects of DDoS attacks on the business sector reach about £100,000 per hour [13]. These examples present and confirm the impact of these attacks on business sectors. Due to this, the organizations must take security seriously and cannot ignore security strategies.

Another common type of attack is a wormhole attack that involves an attacker copying messages or packets by channeling them to another network. They then send them to another faster destination node, so the copied packets reach the attacker's destination node before the original packets. Attackers do this using an invisible wormhole tunnel [14]. Figure 1 shows a wormhole attack scenario.

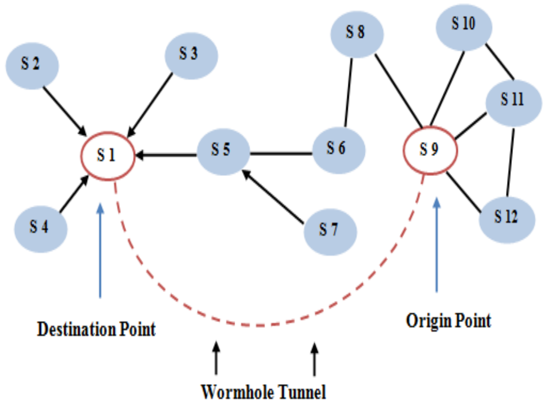

Figure 1 Wormhole Attack Scenario.

Hackers can also attack a wireless network system through Man-in-the-Middle attack. This can be achieved by introducing an authorized Access Point (AP) into the wireless networks. The attackers get access to the AP information of an active SSID by creating unauthorized AP. In this way, attackers can intercept the communication. If a TCP connects a client to a server, then the attacker will be the Man-in- the-Middle attack. In such a case, the attacker splits the TCP into two separate connections, with the common node being that of the attacker. This means that the first connection is from the client to the attacker, and the second will be from attacker to the server. Every response and request will take place between the client and server through the attacker.

Jamming is another type of attack that hackers can use to disallow legitimate users, marking them instead as unauthorized. Because of this attack, the system becomes "jammed" with all the illegitimate traffic signals until it cannot process the signals further. The effect is that no one can access or efficiently use the system – legitimate or otherwise [15].

Attackers may conduct "brute force dictionary" to determine the key or password that is in common with all shared wireless clients. In this approach, the attackers systematically try every possible key until the password is guessed and thenthe attacker can access the system. [16]Medium Access Control (MAC) address spoofing isanother way that attackers can launch wireless networks. Most importantly, it is hard to detect MAC address spoofing. Sequence Number (SN) tracking technique is mainly used to detect spoofing. This technique has a variety of disadvantages including that it cannot be used in systems with wireless cards that do not support standard 802.11 sequence number patterns.Italso may increase the number of false positives, and therefore, considerattack activities as normal system behaviors [17].

During the last decade, several solutions were proposed to overcome misuse and anomaly problems. Some researchers [18] proposed a hybrid detection approach to increase the capabilities of the current Wireless Intrusion Detection and Prevention System (WIDPS) by amalgamating two intelligent methods of misuse and anomaly. In another effort, a hybrid IDS has been proposed by incorporating the packet header anomaly detection and network traffic anomaly detection systems, which are ananomaly based IDSs with misuse-based IDS Snort [19]. The main goal behind their method is to identify known attacks by misuse while anomaly discovers unknown attacks. In another study, a hybrid method was proposed [20]. In this method, the authors integrate signature based (Snort) with anomaly based (Naïve Bayes) to enhance system security from attacks. The results showed that good performance was attained by their proposed method.

A two-stage classification system was developed [21]. The system uses Self-Organizing Map (SOM) neural networks and k-means algorithmto correlate the related alerts and to further classify the alerts into classes of true and false alarms. The experiments showed that all superfluous and noisy alertswere effectively reduced, which often contribute to more than 50% of false alarms.

A New Intrusion Detection Method Based on Antibody Concentration (NIDMBAC) was presented to reduce false alarm rate without affecting detection rate [22].The basic definitions of self, non-self, antigen, and detector ofthe intrusion detection domain were defined. Based on the antigen intrusion intensity, the change of antibody number is recorded from the process of clone proliferation for detectors based on the antigen classified recognition. The authors presented a probabilistic calculation technique for the intrusion alarm production, which rests on the correlation between the antigen intrusion intensity and the antibody concentration. The proposed method achieved better performance compared to traditional techniques.

A hybrid statistical approach using Data Mining and Decision Tree Classification was proposed [23]. The authors focus on detection involving statistical analysis of both attack and normal traffics. Because of their work, the statistical analysis can be manipulated to decrease misclassification of false positives and differentiate between attacks and false positives for the traffic data.

Other researchers have [24] proposed a network intrusion detection system based on acombinatorial algorithm (CA-NIDS). Their proposed algorithmemploys additional databases to enable thesignature based system to act as an anomaly based systemto detectnew attacks and speed up network traffic during traffic analysis. The final results show that better accuracy was achieved by the proposed algorithm.

From theabove-described research, it is clear that organizations need to employ IDPSs in their systems, and security should be part of an organization's overall security management and risk assessment plan. These systems can help them detect and prevent these attacks from succeeding.

3. IDPS FUNCTIONS

The conventional way for securing a wireless network is to design or to use a security mechanism, such as authentication mechanisms, Virtual Private Networks (VPN), and firewalls that create a protective barrier around the network. However, such security measures have inevitable vulnerabilities and are usually not sufficient to ensure that the systems are kept secure all the time. On the other hand, attackers always attempt to find ways to gain access to systems. This has resulted in the need for security technology that can monitor the systems, identify possible threats, and attempt to prevent them from succeeding [18].

IDPS can be used to complement the conventional security mechanisms. It provides four essential security functions.These functions include monitoring, analyzing, detecting, and preventing unusual and unauthorized activities [19]. IDPS aims at performing early detection of malicious activity to prevent more severedamage to the protected systems.

Intrusion Detection System (IDS) is a software or hardware that automatically detects intrusion into the system. An Intrusion Prevention System (IPS) detects intrusions and can also attempt to stop possible intrusions from succeeding. In addition, IPS can also compare signals to known signatures of previously detected intrusions on the current system as well as from a database of collected and published attack signatures. [20].

There are two general ways to detect intrusions based on signature, including signature-based and anomaly based detection. The signature-based approach can be easily compared to anti-virus software that analyzes and characterizes attack details to formulate signatures. Once the signatures are characterized, they can then besearched for and available information on the computer systems, such as audit data logs, can be compared. Conversely, anomaly detection notices unusual behavior on the network or in the system, compared to what is defined as “normal.” For this method, it is crucial to develop constructs for normal user, host, and network behavior through acompilation of normal data collected without intrusion. The event data that is monitored by the IDSs is compared to various activities to determine what is normal and what may be considered abnormal, and therefore cause for alarm. Table 1 summarizes pros and cons of the detection methodologies.

Table 1: The advantages and disadvantages of the Intrusion detection methodologies

Intrusion Detection techniques	**Advantages**	**Disadvantages**
Signature based	• Effective method and high detection accuracy to detect known attack • Low computational cost	• High false alarm for unknown attacks or vulnerabilitie s • Hard to keep knowledge base up to date
Anomaly based detection	• Effective to detect new vulnerabilities • Less dependent on Operating System (OS)	• Time-consuming to classify attacks • Difficultto activate alerts in proper time

Digital forensics is the process of investigating to identify, trace, and analyze illegal and fraudulent occurrences and provide proof to enforce laws against such events. IDPS can be used to provide, record, and document the information needed to identify suspicious early activities and may even lead to prevention of more serious damage [21]. Thus, an IDPS is not only very useful tool for collecting and interpreting digital evidences that may be used in a court of law, but also can draw the big picture of the activities of the system and can test the effectiveness of the controlenvironment by identifying policies and attributes that breach security and privacy.

In addition, IDPSs provide valuable information about how the attack took place, what the intruder achieved, and which methods the intruders used to accomplish their goals even if an IDPS fails to prevent an intrusion. A person, organization, or business can benefit from this additional information to quickly respond to abnormal activities within the system or repair security measures and try to prevent them from succeeding in proper time. Finally, it can be used to formulate continuous future security improvements.

4. LIMITATIONS OF INTRUSION DETECTION SYSTEMS (IDPS)

One of the main limitations of IDPS, specifically those that use anomaly based approach, is that it creates false alarms need to be tackled [22].The false alarm leads to complacency among those monitoring the alarms. Monitoring the alarms is also tiring because it is an ongoing activity. This reliance on human intervention is one of the main limitations of the wireless security systems. To be effective in detecting intrusions,IDPS systems should run in real time. If it is offline or after the event has occurred, IDPS will be useful only for audit, but it will not prevent an attack from happening.

The real time IDPS needs to be able to stream data across the network from sensors to a central point where the data can be stored and analyzed. This method is the correlation server. The additional concurrent running of traffic network may significantly affect network performance. For this reason, sufficient bandwidth is required. However, such tools as Air-Defense Guard may permit for set rate throttles on each sensor to bring transfer rates to the server to as low as 9.6 Kbps [23]. Another problem is that if the IDPS inaccurately classifies a normal system activity as an unusual one, the results can be very unfortunate since it will attempt to stop the activity or change it.

Some wireless intrusion detection systems such as, Air-Defense Guard and Air-Magnet Distributed are only good at preventing the system against known attack pattern recognition file given to them. They mostly utilize a signature recognition that can easily be misused. This is their major flaw in that the system offers protection only for what is a known to be an attack. This implies that new patterns of attacks easily go undetected, which underlines the need to come up with an efficient mechanism that can keep all network security components with signature or rule based tables up to thedate of known attack signature [24].

The efficiency of IDS is measured on how the detection method is capable of taking anaccurate decision as to whether an activity is an attack attempt or normal system behavior. There are three criteria to measure detection performance including detection rate, false negative rate, and false positive rate, which are given when detection results are reported. However, if the IDS take along time to detect or response for an intrusion, then there will be enough time available for the attacker to accomplish his/her desired goals.

5. DISCUSSION

In this age of technology of wireless networks, the best way to ensure security for the wireless network is by properly designing, installing, and securing the networks. The wireless network may require more careful management compared to wired networks because of its nature [25, 26]. Even minor activities that appear to be unrelated to computer networks may have a grave impact on the wireless network. For example, the installation of a new machine or the relocation of a potted plant may affect the wireless radio frequency signal, which may result in poor connectivity or slow speed of transmissions. Additionally, to overcome the issue of unauthorized intrusion, people responsible for the wireless network should frequently monitor and adjust wireless network settings, so that they can provide maximum performance to their clients. It is also of utmost importance to note that security requirement to provide safety measures for the wireless network is much different from that of wired networks. Implementing IEEE 802.11i/WPA2, and installing the latest wireless IDPS, and use of rogue access point (AP) discovery tools is one of the technical aspects of securing a wireless network. It is also a crucial step for making sure that the wireless network is safe from hackers.

Ideally, the IDPS system should be able to determine and prevent abnormal or authorized behaviors within the system in a real time [27]. Otherwise, intruders can access information and resources available on the system until prevention and not at the moment of detection. Another important issue that should be considered is to employ location anonymity as a part of seamless protection system to avoid detection of the access points and actual location identification. In this way, the wireless network will be protected by the IDPSs from unknown intrusion with limited human intervention and the system operation continuity would be ensured.

Risk management and assessment are the processes of classifying and evaluating risks by taking proper steps to minimize risk to an acceptable level and applying effective controls measures to preserve that level of risk for each information asset, vulnerability, and threat. These techniques not only assist the organizations to determine better the necessary security control and measures that need to be taken to minimize and contain the risk to an acceptable level, but also to make them capable and ready for meeting the needs of tomorrow. Due to this, risk management and assessment are crucial in building a uniform and effective architecture for IDPSs, which can secure the whole system and aid system administrator to control the system efficiently.

6. CONCLUSION AND FUTURE RECOMMENDATIONS

Wireless networks represent the next wave of networking because of their relevance in assisting an emerging mobile workforce in a growing information-oriented society. However, wireless networks also present many challenges in regard to application, software, hardware, network designers, and implementers. Unauthorized access, DoS, DDoS, Man in the Middle, Jamming, and Medium Access Control

(MAC) address spoofing, are the primary concern challenges to wireless networks. Attackers have the capacity to hear all conversations through trafficking networks, and therefore cause disrupted conditions by possible attacks. In this paper, an overview description of IDPSs and their core functions, primary types of intrusion detection mechanisms, and the limitations of IDPSshave been discussed. For the false alarm, IDPS should have a better and more accurate ability to identify the intrusion with a low rate of false positives.

Future work and development trends seem to be converging to include more intelligence techniques toward a model that is based on and managed by machine learning, data mining, and game theory along with risk analysis and assessment techniques together to help reducing false alarm rates. This will assist wireless networks toremain secure and able to face attacks that are more sophisticated and will aid system administrator to understand their systems behavior better. In addition, it will make IDPSs smarter. Some of the key issues that need more attention to overcome the limitations in wireless IDPSareto design a proactive and real-time prevention attack. Additionally, more attention should focus on seamless protection and anonymity location privacy. More research is needed to obtain new detection performance method and criteria to evaluate attack detection in awireless network to mitigate the delay time between detection and attack time that could be used by anadversary to damage the target system.

7. REFERENCE

[1] H. Bidgoli, Handbook of Information Security, Threats, Vulnerabilities, Prevention, Detection, and Management, John Wiley & Sons, New York.2006.

[2] I. AlShourbaji, “An overview of wireless local area network (WLAN),” International Journal of Computer Science and Information Security, pp. 46-53, 2013.

[3] D. Sivakumar, B.Sivakumar, “Detection and Localization of Attackers in Wireless Networks”, International Review on Computers and Software (IRECOS), pp. 854-864, 2014.

[4] I. AlShourbaji, R. AlAmeer, “Wireless intrusion detection systems (WIDS)”, Advances in Computer Science and its Applications (ACSA), 2013.

[5] M. M. Noor, W. H. Hassan, “Wireless networks: developments, threats and countermeasures”, International Journal of Digital Information and Wireless Communications (IJDIWC), pp.119-134., 2013.

[6] S. Al-Janabi , I. Al-Shourbaji , M. Shojafar, S. Shamshirband, “Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications”, Egyptian Informatics journal, pp. 113-122, 2017.

[7] M. P. M. Rathod, M. V. V.Parode, R.R.Keole, “SECURITY LIMITATIONS AND CHALLENGES IN WIRELESS NETWORKS”, International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE), pp. 42-45, 2012.

[8] S. Al-Janabi, I. Al-Shourbaji, “A Study of Cyber Security Awareness in Educational Environment in the Middle East”, Journal of Information & Knowledge Management,1650007, 2016.

[9] U. H.Rao, U.Nayak, “Intrusion Detection and Prevention Systems. The InfoSec Handbook, pp. 225-243, 2014.

[10] Y. Yu, K. Li, W. Zhou, P. Li, P,“Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures”, Journal of Network and Computer Applications, pp. 867-880, 2012.

[11] A. Mishra, A. K. Srivastava,“A Survey on Intrusion Detection System for Wireless Network”, International Journal of Computer Applications, pp.37-40, 2013.

[12] A. Wahid, P. Kumar, “A Survey on Attacks, Challenges and Security Mechanisms in Wireless Sensor Network”, International Journal for Innovative Research in Science and Technology, pp. 189-196, 2015.

[13] Neustar, “DDoS attacks pose biggest threat yet to European businesses”, available at: https://www.neustar.biz/about-us/news-room/press-releases/2015/ddos-attacks-pose-biggest-threat-yet-to-european-businesses. (Accessed 16 May 2015).

[14] T.Bin ,L.Qi, Y. X..Yang, L. Dong, X.Yang, “A ranging based scheme for detecting the wormhole attack in wireless sensor networks,” The Journal of China Universities of Posts and Telecommunications, pp. 6-10, 2012.

[15] W.Shen, P. Ning, X. He, H. Dai, Y. Liu, “MCR Decoding: A MIMO approach for defending against wireless jamming attacks”, In Proceedings of the IEEE on communications and Network Security (CNS), pp. 133-138, 2014.

[16] S.S.Ahamad, I. Al-Shourbaji, S. Al-Janabi, “A secure NFC mobile payment protocol based on biometrics with formal verification”, International Journal of Internet Technology and Secured Transactions, pp. 103-132, 2016.

[17] R.Vijayakumar, K. Selvakumar, K.Kulothungan, A. Kannan, “Prevention of multiple spoofing attacks with dynamic MAC address allocation for wireless networks”, In Proceedings of the ICCSP on communications and Signal Processing (ICCSP), pp. 1635-1639, 2014.

[18] S. S.Wang, K. Q Yan, S. C.Wang, C. W. Liu, “An integrated intrusion detection system for cluster-based wireless sensor networks”, Expert Systems with Applications, 38(12), pp.15234-15243, 2011.

[19] M. A. Aydın, A. H.Zaim, K. G.Ceylan, “A hybrid intrusion detection system design for computer network security”, Computers & Electrical Engineering, pp. 517-526. 2009.

[20] S. M.Hussein, F.H.M Ali, Z. Kasiran, “ Evaluation effectiveness of hybrid IDs using snort with naive Bayes to detect attacks”, In proceedings of the

IEEE on Digital Information and Communication Technology and it's Applications (DICTAP), pp. 256-260, 2012.

[21] G. C.Tjhai, S. M.Furnell, M. Papadaki, N. L.Clarke, “A preliminary two-stage alarm correlation and filtering system using SOM neural network and K-means algorithm”, Computers & Security, pp. 712-723, 2010.

[22] J. Zeng, T. Li, G. Li, H. Li , “A new intrusion detection method based on antibody concentration”, Emerging Intelligent Computing Technology and Applications. With Aspects of Artificial Intelligence, pp. 500-509, 2009

[23] N. B.Anuar, H. Sallehudin, A. Gan, O. Zakari , “Identifying false alarm for network intrusion detection system using data mining and decision tree”, In Proceedings of the World Scientific and Engineering Academy and Society (WSEAS) on Data networks, communications, computers. Stevens Point, Wisconsin, USA, pp. 22-28, 2008

[24] O. Folorunso, F.E. Ayo, Y.E. Babalola , “Ca-NIDS: A network intrusion detection system using combinatorial algorithm approach”, Journal of Information Privacy and Security, pp.181-196. 2016.

[25] S. H. Ali, “Novel Approach for Generating the Key of Stream Cipher System Using Random Forest Data Mining Algorithm”, In proceedings of the DeSE on Developments in eSystems Engineering (DeSE), pp. 259-269, 2013.

[26] M. Salman, B. Budiardjo, K. Ramli, “Key Issues and Challenges of Intrusion Detection and Prevention System: Developing Proactive Protection in Wireless Network Environment.", World Academy of Science, Engineering and Technology, pp. 521-524, 2011.

[27] K. Scarfone,. P. Mell, “Guide to intrusion detection and prevention systems (IDPS)”, Recommendations of the National Institute of Standards and Technology, National Institute of Standards and Technology, Maryland, 2007.

[28] M. E. Whitman, H.J.Mattord, Principles of Information Security”, Thomson Course Technology, Boston, MA, 2005.

[29] C. Y. Ho, Y. C.Lai, I. W.Chen, F. Y.Wang, W. H.Tai,“Statistical analysis of false positives and false negatives from real traffic with intrusion detection/prevention systems”, Communications Magazine, pp. 146-154,2012.

[30] M. P. M. Rathod, M. V. V. Parode, R. R. Keole, “SECURITY LIMITATIONS AND CHALLENGES IN WIRELESS NETWORKS”, International Journal of Electronics, Communication and Soft Computing Science & Engineering (IJECSCSE), pp. 42-45,2012.

[31] H. Chaouchi, M. Laurent-Maknavicius, Wireless and Mobile Networks Security, John Wiley & Sons, New York, 2013.

[32] M. Ahmad, S. Taj, T. Mustafa, M. Asri, “Performance analysis of wireless network with the impact of security mechanisms,” In proceedings the ICET of international on Emerging Technologies, pp. 1-6, 2012.

[33] A.Vindašius, “Security state of wireless networks, “Elektronikair Elektrotechnika, pp. 19-22, 2015.

P. S. Kenkre,.,A. Pai, L. Colaco, “Real Time Intrusion Detection and Prevention System”, In Proceedings of the Theory and Applications (FICTA) on Frontiers of Intelligent Computing, pp. 405-411, 2015.