Volume 7, Issue 2, February 2017 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

The Modern Approach in Wireless Intrusion Prevention System for Ad hoc Network: A Target Oriented Approach

S V Athawale*
Research Scholar, Department of Computer Engineering,
SGBAU, Amravati, Maharashtra, India

M A Pund
Department of Computer Engineering,
PRMIT & R, Amravati, Maharashtra, India

DOI: 10.23956/ijarcsse/V7I2/0127

Abstract— The wireless networks have revolutionized the way organizations work and offered a new range of possibilities, but at the same time they introduced new security threats. While an attacker needs physical access to a wired network in order to deploy an attack, a wireless network allows anyone within its range to passively monitor the traffic or even start an attack. One of the countermeasures can be the use of Wireless Intrusion Prevention Systems.

Keywords— network security, IDS, IPS, wireless intrusion detection, wireless intrusion prevention.

I. INTRODUCTION

Intrusion Detection was developed to recognize and report the attack in the late 1990s, as hacker's attacks and network worms began to affect the internet, it detected hostile traffic and sent alerts but did nothing to stop the attacks . It has been a long road for Intrusion Detection System (IDS), almost two decades since it has become a major issue [1]. In other words, Intrusion Detection is passive rather than active. It is not able to detect all malicious programmes and activities most of the time and incompatible to integrate with control restriction to restrict traffic inbound-outbound from attacking; which means it was only capable to detect attack actions, without prevention action. Intrusion Prevention System (IPS) is primarily a network-based defence system, with rising global network connectivity and combines the technique firewall with that of IDS properly with proactive techniques. This system is a proactive technique which prevents attacks before entering the network by examining numerous data record and detects demeanour pattern recognition sensor. When an attack is identified, intrusion prevention blocks and logs down the offending data. Currently, requirement for a system to provide early detection / warning from intrusion security violation with databases knowledge based has become a necessity.

This mechanism is activated to stop or allow packet data to process associated with the event. It prevents attack before it enters the network by examining various data records and prevents the demeanour of pattern recognition. Currently, requirement for a system to provide early detection / warning from intrusion security violation with knowledge based has become a vital necessity. Therefore, the system must be active and smart in classifying and distinguish the packet data, if curious or mischievous data are detected, alert is triggered and event alert response is executed [2, 3]. The main contribution of this paper is the enhancement of WIPS on the basis of behaviour so that attack can be prevent before it happen. The residual of the paper is structured as follows: we begin with Section 1 introduction then Section 2 represents related work in roadmap of intrusion detection, early detection, response and prevention system. Section 3 System flow and frame work. Section 4, intrusion prevention systems present work, additional works to be continued. Finally Section 5, experimental results and analysis.

II. RELATED WORK OF IPS

Based on the previous section, in order for places to counter security threat, this current needed an integrated solution that is renewable and not avoidable. The roadmap for development of detection, early detection and prevention system are represented in Figure 1. It started earlier in the IDS solution by [4], presenting the taxonomy and existing tools used of IDS. Furthermore, previous work by [5], proposes automatic early warning system to make prediction and advice regarding malware based on database and repository of threat. These early detection concepts has been introduced by [6], which describes differentiate types of operation mode IDS, IPS and Intrusion Response System (IRS), they compare it on the basis of literature product with features such as proactive, reactive and passive. Therefore, IRS can be categorised as a basic method of IPS. On the other hand, performed work by [7], outlines the future trends of IPS and its functionality such as: gateway appliance, perimeter defence appliance, all-in-all capability, and network packet inspection or prevention. Additionally, work from [8, 9], encountered challenges in intrusion detection of the early detection. The trend of behaviour analysis to efficient data collection is describe to improve the performance of sensors in the real-traffic network, due to the network traffic captured on high speed links is always a challenge to capacity issues. This means that early detection, protection and response system act as an elementary of IPS. The researcher strongly argued that the purpose of early detection and response system is the one of main concepts of IPS. It is expanded on the

functionality provided by IDS by enabling to prevent attack against of network. As mentioned previously, early detection and intrusion response has the fundamental part of intrusion prevention mechanism in recent network security challenge, this was confirmed performed. Responding to this issue, some researchers have proposed several different detections and response mechanisms to complement the existing prevention mechanism [10] they were declared intrusion response as having similar function as IDS and part of it, by maintaining detection, alerting and response to security operator. IPS functions as radar to monitor stream network traffic; detecting, identifying, and recognising any signal that could be regarded a security violation. With respect from proposal work by [11], they represent real-time intrusion prevention and anomaly system had predicted future of IPS technology, such as (i) having a better underlying intrusion detection, (ii) advancement in application-level analysis, (iii) more sophisticated response capabilities, and (iv) integration of intrusion prevention system into other security devices. Moreover, the prediction concerns on intrusion prevention technology which are very positive in market. Figure 2. Features of IPS previously, in 2004 [19], has predicted that IPSs have a bright future, this technology will continue to be used by a growing number of organizations to the point that it

Will become a commonplace as intrusion detection technology. More recently, performed work by [12], describes superior characteristic of host based IPS and use the term detection approach to show how IPSs work. As seen from Figure 2, the feature function of IPS is represented. Intrusion Prevention provides numerous capabilities at both the host level and the network level, but from a high-level perspective, the capabilities supplied by IPSs fall into two major categories: (i) Attack prevention, and (ii) Regulatory compliance.

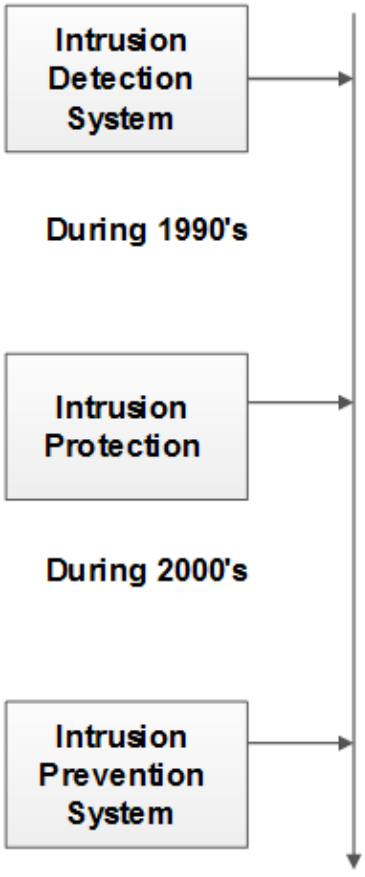

Fig. 1 Evolution of Intrusion Prevention system

Additionally, much type of IPSs potentially avoid the weakness of the signature-based intrusion detection systems and it can learn classes of harmful system activities and the types of events that they attempt to produce in targeted system. Therefore, it is much better to react appropriately to zero-day attacks. Hence, from this analysis, it is identified that IPS will also become more proficient than IDS because IDS, early detection, intrusion response is a fundamental aspect when intrusion prevention in developing. According to some reported work till now, [13,14] describes IDS and IPS fundamentally, currently IDS can be seen as a traditional second line of a defence system, it is becoming more difficult to apply security access control for it. On the contrary, IPS can be used to alarm for the attacks within a network and provide a platform for acting on attack preventive with Firewall and IDS function mechanism. In comparison to IDS and IPS with features of both depicted in [15, 16].

III. SYSTEM FLOW AND FRAME WORK

The selected sensor IEEE 802.11 authentication with the policies. If the policies are match then authenticates by intrusion prevention system, then latter sends to alert message from databases. Figure 1 shows the various phases and communication exchanged in each phase.

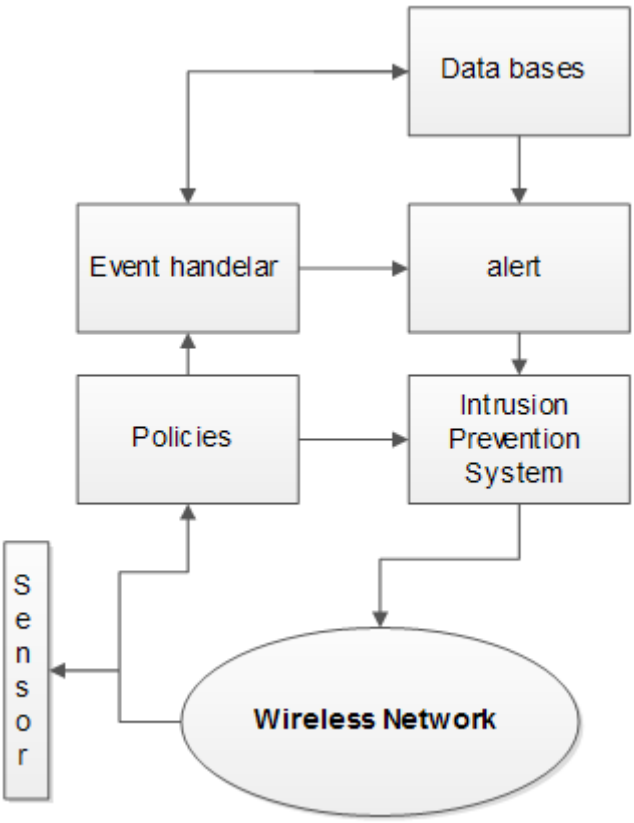

Fig. 1 System scenario and work flow

IV. INTRUSION PREVENTION SYSTEMS

Traditionally, firewalls and anti-virus programs try to block attacks but IDS tries to identify attacks as it occurs. Such techniques are critical to defence in depth approach to security, but have some limitations. A firewall can restrict services by blocking certain ports but it does very little to evaluate traffic that uses allowed ports. IDS can evaluate traffic that travels through these open ports but cannot restrict it. IPS can proactively block the attacks. Signature based approaches focuses on how an attack works, trying to detect certain strings in them. If an attacker makes minor changes by using the IDS evasion techniques discussed above, then previously written signatures no longer can detect the attack. IPS focuses prevention, instead on what an attack does, which does not change.

IPS popular Approaches

Some of the approaches being used are as follows

1. Software based heuristic approach - This approach is very similar to IDS anomaly detection using neural networks with additional ability to act against intrusions and block them.
2. *Sandbox* approach - Mobile code like ActiveX, Java applets and various other scripting languages are quarantined in a *sandbox* - an area with restricted access to rest of the system resources. The system runs the code in this *sandbox* and monitors it's activities. If the code violates a predefined policy it is stopped and prevented from executing, thwarting the attack.
3. Hybrid approach –On network-based IPS (NIPS), various detection methods, some of the proprietary including protocol anomaly, traffic anomaly, and signature detection work together to determine an imminent attack and block traffic coming from an inline router.
4. Kernel based protection approach – It is used on host-based IPS (HIPS). Most operating systems restrict access to the kernel by a user application. The kernel controls the access to system resources like memory, I/O devices, and CPU, thus preventing direct user access. In order to use resources user applications send requests or system calls to the kernel, which then carry out the operation. Any of the exploited code will execute at least one system call to gain access to privileged resources or services. Kernel based IPS prevents execution of malicious system calls in the system.

V. EXPERIMENTAL RESULTS AND ANALYSIS

We set up two local area networks (LAN) in the laboratory so as to simulate the environment of using our hybrid based IDPS. One network is a public WLAN which connects to the Internet while another network is a private LAN which connects to the IDPS host as shown in Figure 2. We have installed our IDPS on a computer. We generated DoS and 13 Probe attack types with the help of program tools as listed in Table 2. The network attacks are from public LAN to a victim computer in private LAN through the IDPS host. Moreover, computers on each LAN are required to generate normal network activities. In order to examine the performance of our real-time IDPS, the following values are

being used. The Total Detection Rate (TDR) is the percentage that IDPS can correctly detect DoS attacks, Probe attacks, and Normal network data.

The DoS Detection Rate (DDR) is the percentage that IDPS can correctly detect DoS attacks. The Probe Detection Rate (PDR) is the percentage that IDPS can correctly detect the Probe attacks. In the experiment, we use NS-2 for 70 nodes which is captured from simulation attacks in the network laboratory. We have run the experiment for 2 hours. During the test, number of threat detected and prevented are shown in fig 3.

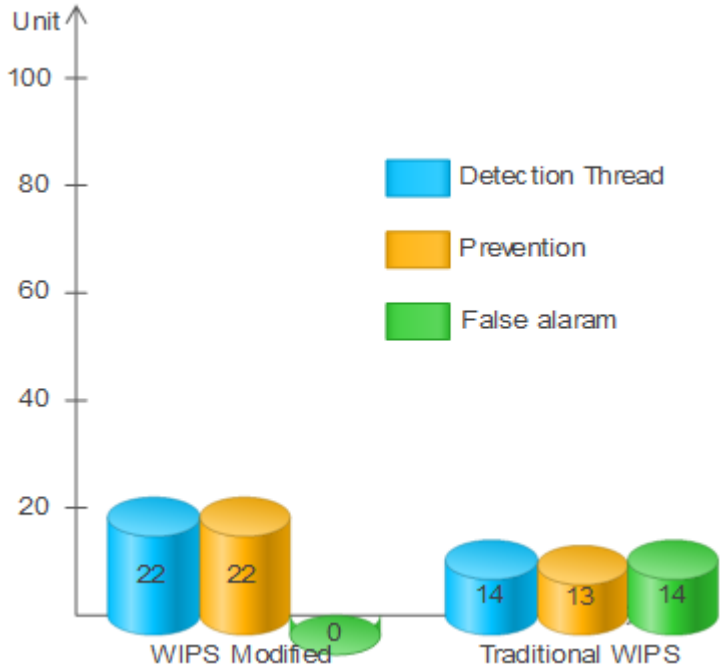

Fig. 3 Efficiency of Wireless Intrusion Prevention Systems at Detecting and Preventing Threats with negligible False Alarms

Table 1 gives a summary of threat presented which includes the number of malicious and external attacker nodes required for the launch each attack, the special capabilities of the new WIPS and the total threat protected in wireless environment are shown below.

Table I Wireless threat prevention summary

Threat Type	**New WIPS**	**Traditional WIPS**
Client misassociation	3 out of 3	3 out of 3
Adhoc networks	4 out of 4	2 out of 4
AP MAC address spoofing	YES	No
Remote AP MAC address spoofing	YES	Yes
Honeypot attack	YES	Yes
Misconfigured AP	YES	Yes
DoS attack	YES	No
Total Threat Protection	**22 out of 22**	**16 out of 22**

VI. CONCLUSIONS

As we see, the WLANs brought not only advantages, but also some specific security threats. For an organization using WLANs, it is obvious that they would need protection against wireless threats. However, a real-time wireless intrusion detection tool for detection/ removal of rogue access points is vital for any organization. The development of new wireless standards and security protocols is expected to improve the WLANs' security, but we also estimate that wireless intrusion prevention systems will continue to play a vital and important role in assuring the organization's security for the next generations.

ACKNOWLEDGMENT

The authors would like to thank Lalit patil and Navin Kumar for their proof-reading and valuable comments.

REFERENCES

[1] S V Athawale; D N Chaudhari," Towards effective client-server based advent intrusion prevention systemfor WLAN ", Computer, Communication and Control (IC4), 2015 International Conference on Year: 2015,pp 1 - 5, 2015.

[2] Guanlin Chen; Hui Yao; Zebing Wang," An Intelligent WLAN Intrusion Prevention System Based on Signature Detection and Plan Recognition ",Future Networks, 2010. ICFN '10. Second International Conference on Year: 2010,pp 168-172,2010.

[3] Yujia Zhang; et al. ," An overview of wireless intrusion prevention systems, Communication Systems, Networks and Applications (ICCSNA), pp 147-150,2010.

[4] Guanlin Chen; Hui Yao; Zebing Wang," Research of wireless intrusion prevention systems based on plan recognition and honeypot ", Wireless Communications & Signal Processing, 2009. WCSP 2009. International Conference, pp 1-5, 2009.

[5] A. Vartak; S. Ahmad; K N Gopinath," An Experimental Evaluation of Over-The-Air (OTA) Wireless IntrusionPrevention Techniques ", 2007 2nd International Conference on Communication Systems Software and Middleware,pp 1-7,2007.

[6] Mohamed Chahine Ghanem; Deepthi N. Ratnayake," Enhancing WPA2-PSK four-way handshaking after re-authentication to deal with de-authentication followed by brute-force attack a novel re-authentication protocol",2016 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (CyberSA),pp 1 - 7,2016.

[7] Sandeep B. Vanjale; P. B. Mane; Sandip V. Patil," Wireless LAN Intrusion Detection and Prevention system for Malicious Access Point",Computing for Sustainable Global Development (INDIACom), 2015 2nd International Conference,pp 487 – 490,2015

[8] Ghassan Kbar; Wathiq Mansoor," Securing the Wireless LANs that is based on Distributed Resource Management against internal attacks ", Innovations in Information Technology, 2007. IIT '07. 4th International Conference on pp 98 - 102, 2007.

[9] P. C. K. Raja; Suganthi." VLSI approach to wireless security mechanism ", IEEE International Conference on Personal Wireless Communications, pp 429-433,2005.

[10] Masakazu Fujii,"Intrusion Detection using Third-Parties Support",12th IEEE International Workshop on Future Trends of Distributed Computing Systems,pp 206-212,2008.

[11] Khalil El-Khatib,"Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems,"IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 8,pp 1143-1149.

[12] S.B.Vanjale, et al."Detecting & Eliminating Rogue Access Point in IEEE 802.11 WLAN,"International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) Volume-1,Issue-1,pp 108-112,2011.

[13] Sahil Seth, Anil Gankotiya,"Denial of Service attacks and Detection Methods in Wireless Mesh Networks,"2010 International Conference on Recent Trends in Information, Telecommunication and Computing,pp 238-240,2010.

[14] Yaqing Zhang,Srinivas Sampalli,"Client-based Intrusion Prevention System for 802.11 Wireless LANs",2010 IEEE 6th Intemational Conference on Wireless and Mobile Computing. Networking and Communications, pp 100-107,2010.

[15] Shikha Goel,Sudesh Kumar,"An Improved Method of Detecting Spoofed Attack in Wireless LAN",2009 First International Conference on Networks & Communications,pp 104-108,2009.

[16] Hua Li, et al."An Improved Defense Scheme Against Attacks On Wireless Security",pp 986-989,2007.

