An Improved Intrusion Prevention Sytem for WLAN

S V Athawale
Assistent Professor, Department Of computer Engineering,
Pune University, AISSMS College of Engineering, Pune, India
svathawale@gmail.com

M A Pund
Professor Department of Computer Science & Engineering,
PRMIT & R, Badnera – Amravati.
dr.mapund@yahoo.com

Abstract— The volatile growth in wireless networks over the last few years resembles the rapid growth of the Internet within the last decade. The current IPS presents a less security. Unfortunately, our work combined with the work of others show that each of these mechanisms are completely futile. As a result, organizations with deployed wireless networks are vulnerable to illegal use of, and access to, their internal communications.

*****

I. INTRODUCTION

In recent times, there is a more prevalent use of wireless technology due to its convenience and low setup cost. However, it is becoming a challenge to provide security solutions for such a dynamically changing environment, often due to certain wireless network characteristics such as lack of infrastructure, low power availability and mobility [2]. Lack of WEP security has prompted the DoD and some businesses to prohibit wireless access to their critical LANs .But despite its well-documented weaknesses, many organizations continue to deploy wireless access. It has been estimated that by the end of 2002 more than half of all businesses and academic institutions will have wireless access to their institutional LANs. Lack of viable security makes these LANs vulnerable to a host of attacks such as “war driving” (driving down the street with a laptop looking for open 802.11 networks), and “parking lot attacks” (sitting in the parking lot eavesdropping on 802.11 communications) [6].

II. RELATED APPPOROCH

Wireless network security is different from wired security primarily because it gives potential attackers easy transport medium admission. This admission significantly increases the threat that any security architecture. Unfortunately, the early IEEE 802.11 standard failed to account for it. This, coupled with several design errors, led to the wave of security problems .Fortunately, newer architectures are becoming available to dramatically increase the security of 802.11-based networks [1].Security solution for wireless networks using a novel low cost Pseudo Random Number Generator (PRNG). The generated pseudo random numbers are also cryptographically secure and are thus suitable for security applications [2].Through the deep research on the wireless security crisis, using SSL VPN, AES and ECC expertise, puts forward a security strategy of wireless mobile office system.[3]. Temporal traffic characteristics to detect rogue APs at a middle location. This detection is free of the underlying wireless technology (802.11b, 802.11a, or 802.11g), is scalable, doesn’t have the inefficiencies of the current solutions, and is sovereign of the signal range of the rogue APs [4]. To quickly sweep all potential rogue APs, the verifier uses greedy algorithm to schedule the channels for the sniffers to listen . To work with the encrypted AP traffic, the sniffers use a probabilistic algorithm that only relies on observed packet size [5].SPRiNG, a simple protocol for secure point-to-point communication.SPRiNG makes use of synchronized pseudo random number generation to generate authenticator variables and fresh encryption keys on a per frame basis. A key design goal of SPRiNG was simplicity and compatibility with the existing 802.11b WEP protocol [6].Believe that the security provided by their deployed wireless access points is sufficient to prevent unauthorized access and use.While existing access points provide several security mechanisms, our work combined with those of others show that *ALL* of these mechanisms are completely in-effective [7]. Enhanced protection mechanism to reduce the number of extra frames used for channel reservation. The effectiveness solution to improve system performance in the mixed 802.11b and 802.11g WLAN is verified by simulation [8]. the system throughput by avoiding the costly RTSlCTS usage. Solution utilizes the characteristics of the existing MAC with a minimal rule change, which requires no change in the existing MAC implementations. When the 802.11g and 802.11bstations co-exist in the very same network. furthermore, our solution requires virtually no change in the existing MAC implementation [9]. The analytical, numerical and simulation results developed in our contribution allows to take into account in the channel load, net throughput, channel modeling, receiver structures and link analyses for IEEE 802.11 and 802.11e networks in an integrated way. The calculation of the good put since the transmission probability, the conditional collision probability, the cycle time and the packet success probability depend upon the traffic load, payload length, SINR per bit [10].

Study the performance of 802.11g and 802.11b standards in real-time while implementing an actual file transfer. The precise performance factors studied were protocol congestion, bandwidth and latency [11]. General mechanism, known as *packet leashes*, for detecting and, then shielding against wormhole attacks, and we present precise protocol, called TIK, that implements leashes. We also discuss topology-based wormhole detection, and demonstrate that it is unfeasible for these approaches to detect some wormhole topologies [12, 13, 14]. Your data might be subjected to an attack, in case your security measures and controls are not in place. Some attacks are active while others are passive, meaning information is monitored in case of passive attack whereas; in active attacks the information is altered with intent to corrupt or destroy the data or the network itself. Last couple

Sr. No.	***DNS as command-and-control***	***SSL slapped down***	***Hacktivism is back3***	Bonus trends
1	DNS affected	Digital Certificate is problem	New Thread	Malware, Social Networking Sites

III. HOW TO PERFORM NEW IPS

IPS will set into centralized monitoring mode for detecting any new IP enter to the nearest network block by system shown in Figure 1. Flowchart shows the flow of system. The IPS will check either it is belongs or other network traffic. If it is so then take appropriate action will execute and block the illegal user [13].

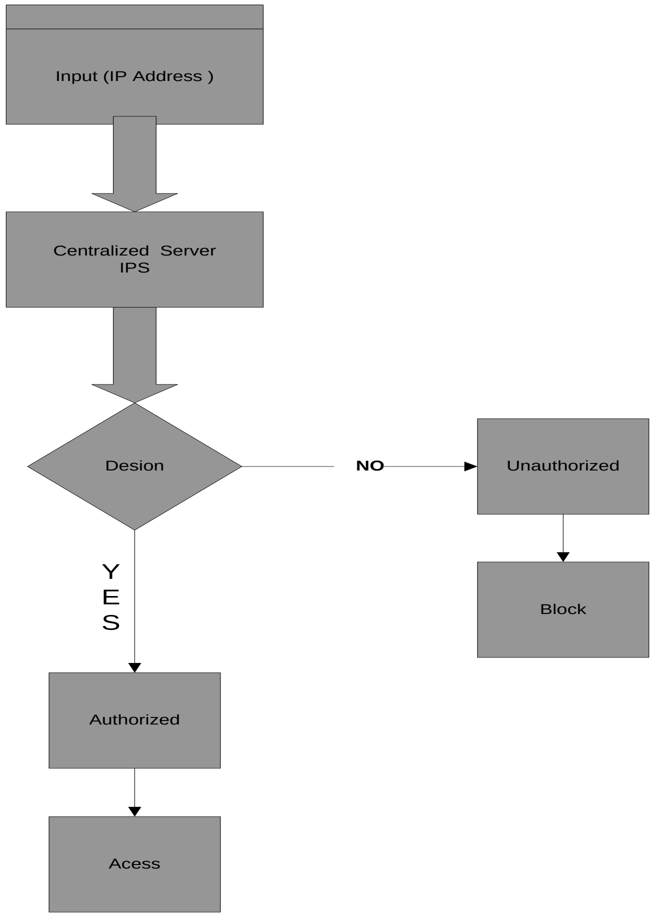
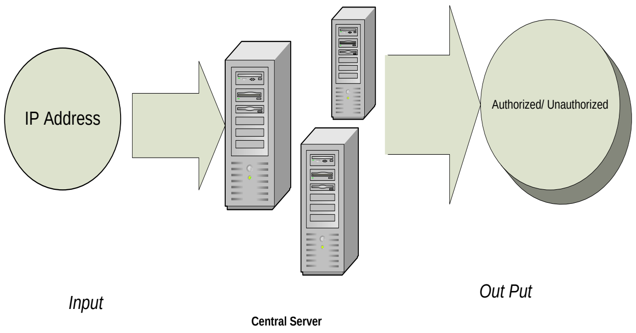


Figure 1. Flowchart of complete sysem.

Figure 1 shows the summary of flowchart used for preventing unauthorized access. So far there are no specific techniques available for how to detect illegal user using centralized server of years attacks on wireless LAN increased phenomenally, need a robust intrusion prevention system for your networks and data are [15], [16] vulnerable to any of the following new types of most dangerous attacks if you do not have a security plan in place.

As mentioned before, the only way of identifying either an IP address is legal or not is by checking with the central server. There are two choices how can it be identified; predefined allowed IP address run time prevention which is not yet develop [17],[18].

Present wireless network lacks network latency. System overhead, greater time and lack of reliability are also major concerns [19].However, in order to overcome the shortcomings; we need a centralized server security system. Unauthorized access point normally called rogue access point) to the network for their personal usage. Most users are unaware of the security threats that come along with this act. The unauthorized user or hacker can bypass the organization network defenses (i.e., firewall, access control) through the software the serious threat to the organization. It requires high administration and technical resources to execute the security audit on the wireless system. Therefore, this paper proposes the automate solution that will help administrator mitigating the threat. We provide the best practice for mitigate the threat over the network traffic. Shown in below Figure 2.



Proposed sytem scenario.

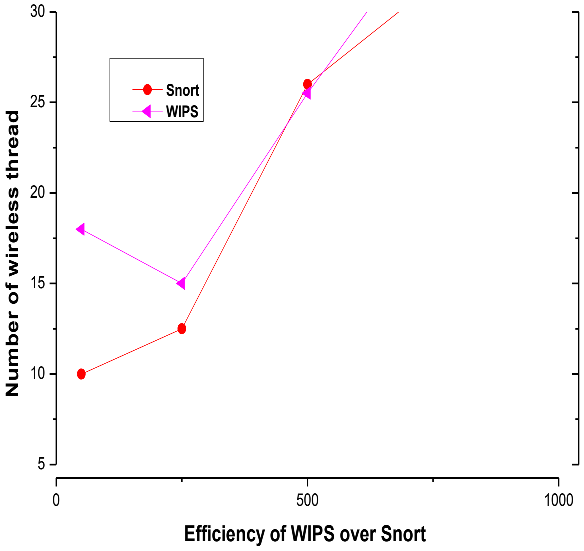
IV. TEST RESULT

In our experiments, we configured and setup on ns-2 , we concentrate main five threats such as , DoS attack, Rogue AP, MAC spoofing, MIM, WEP Decryption. and so on. Tests showed that the WIPS with Snort above 12 threats and prevented attackers from damaging the wireless network in these threats. Furthermore, it didn't generate any false alarms.

Snort-Wireless detected only 3 threats including, Dos Attack, Rogue AP and MAC Spoofing, 50 percent of the total, and prevented none of the threats. Moreover, Snort-Wireless yielded 1 false alarm with DoS when it was attacked by MIM (See Table 1).

TABLE I. WLAN THREAT PREVENTION

Test scenarios	***WIPS***	***SNORT***
Rouge acees point	YES	NO
Dos Attacks	YES	NO
MIM	YES	NO
MAC Spoofing	YES	NO
WEP Decryption	YES	NO



Performance of WIPS over Snort.

Figure 3 show that efficiency of these two WIPS atpreventing wireless threats. It can be seen from this figure that the WIPS with snort not only improves detection and prevention performance but also reduce false positives evidently.

V. CONCLUSION

We propose a new method to detect, protected unauthorized user. Internal network to the wireless edge and reports the address of confirmed legitimate user automatic blocking. With central based server system, we proposed that the verifier's workload may be amortized over time when monitoring a large number of active hosts. Using centralized testing theory, the verifier to test packets all over the network.In practice, our proposed method can quickly prevent the suspect.

ACKNOWLEDGMENT

The author is thankful to all the researchers of this field for giving him the required motivation to carry on with his work

REFERENCES

[1] William A. Arbaugh,"Wireless Security Is Different"University of Maryland at College Park,pp 99-100,August 2003.

[2] Karthik Ramakrishnan, Aruna Balasubramanian, Sumita Mishra2 and Ramalingam Sridhar," Wireless Security Protocol using a Low Cost Pseudo Random NumberGenerator",pp1-7,2004.

[3] Yin Zhiyu Zhang Linwei Li Wenna," Study on Security Strategy of Wireless Mobile Office System",pp 495-498,2009.

[4] Raheem Beyah, Shantanu Kangude, George Yu, Brian Strickland, and John Copeland," Rogue Access Point Detection using Temporal Traffic Characteristics",pp 2271-2275,2004.

[5] Hongda Yin, Guanling Chen, and Jie Wang," Detecting Protected Layer-3 Rogue APs",pp 1-10,2007.

[6] David L, Pepyne Yu-Chi (Larry) Ho, Qinghua Zheng," SPRiNG: Synchronized Random Numbers for Wireless Security",pp 2027-2032,2003.

[7] William A. Arbaugh,Narendar Shankar,Y.C. Justin Wan," Your 802.11 Wireless Network has No Clothes¤",pp 1-13.

[8] Yong Bai, Yifan Yu, Lan Chen," Enhanced Protection Mechanism for ImprovingCo-existence of IEEE 802.11b and IEEE 802.11gWireless LANs",pp 1-5,2009.

[9] Sunghyun Choi, Javier dei Prado Pavon," 802.1 lg CP: **A** Solution for IEEE 802.1 1 g and 802.1 lb Inter-Working",pp 690-694,2003.

[10] Roger Pierre Fabris Hoefel," IEEE WLANS: 802.11, 802.11e MAC AND 802.11a, 802.11b, 802.11g PHY CROSS

LAYER LINK BUDGET MODEL FOR CELL COVERAGE ESTIMATION",pp 1877-1882,2008.

[11] Victor Clincy, Ajay Sitaram, David Odaibo, Garima Sogarwal," A Real-Time Study of 802.11b and 802.11g',pp 1-3,2006

[12] Yih-Chun Hu, *Member, IEEE*, Adrian Perrig,*," Wormhole* Attacks in Wireless Networks*",pp 370-380,2006.*

[13] S V Athawale, Dr M A Pund."ACIPS: Improvement of Client-Server based Intrusion Prevention System for Wireless LAN", 4,pp.6868-6871,2017.

[14] S V Athawale1, M A Pund,"Intrusion Prevention System for Wireless LAN Security: A Study", International Journal of Advanced Research in Computer and Communication Engineering,(IJARCCE),Vol. 5, Issue 10,pp.421-423,2016.

[15] S V Athawale1, M A Pund,"A Novel Algorithm to Determine the Attacks Intention in Wireless Ad hoc Networks", International Journal Of Engineering And Computer Science, Volume 5 Issue 12, pp.19283-19287, 2016.

[16] S V Athawale1, M A Pund,"The Modern Approach in Wireless Intrusion Prevention System for Ad hoc Network: A Target Oriented Approach", International Journal of Advanced Research in Computer Science and Software Engineering,(IJARCSSE),Volume 7, Issue 2,pp.1-7,2017.

[17] S V Athawale1, M A Pund,"Comparative Performance Evaluation of Routing Protocols for Wireless Ad hoc Network", International Journal of Innovative Research in Science,Engineering and Technology,(IJIRSET),Volume 6, Issue 10,pp.19411-19416,2017.

[18] S V Athawale1, M A Pund,"Real-time Intrusion Prevention System to Increase Computer Security in Wireless LAN", nternational Journal for Research in Applied Science & Engineering Technology (IJRASET),Volume 5, Issue 9,pp.1428-1432,2017.

[19] S V Athawale1, M A Pund," NGIPS: The road map of next generation intrusion prevention system for wireless LAN", Ist IEEE International Conference on Intelligent Systems and Information Management (ICISIM), pp.276-280,2017.