Agent based IPS for WLAN

S V.Athawale
Department Of Computer Engineering All India Shri Shivaji Memorial Society's College Of Engineering
Pune, India

D N Chaudhari, Ph.D
Professor and Dean, Computer Engineering, JDIET,
Yavatmal, India

ABSTRACT
The growing technology of the Wireless LAN (WLAN) 802.11-based it also increases its threat of security attacks. This paper presents an overview and solution of better intrusion prevention system (IPS). We conducted experiments to comprehend the impact of various attacks, study the various probabilities under most dangerous attacks. However the earlier proposed solution to prevent the attacks on WLAN is not efficient. Its challenge to design such a system who gives us better result against the attacks. We propose an hybrid approach for deep packet inspection over network traffic resolve unauthorized, attacker. The experimental results yield satisfactory performance for the hybrid approach.

Keywords
LAN: Local Area Network, IPS: Intrusion prevention system WLAN: Wireless Local Area Networks.

1. INTRODUCTION
Nowadays Wireless network is very popular formed by many colleges, corporate, industry using it without major security policy some used policy but they are not up the mark so now time comes to design such wireless prevention system which adopt by many with minor changes in their existing setup now wireless media get increase phenomenally last few years. The 802.11 network used by many have some weakness in security system, fixed networking infrastructure, it can be applied to a limited range of application but in case Ad Hoc network scenarios, such network, uses in natural disaster, earthquake, and tsunami. Wireless network is particularly vulnerable to many attacks. The ability to deal with such attacks and maintain an acceptable level of prevention system in order to overcome such thread in presence of attack are the crucial issue in the design of a IPS for wireless network .Several complementary approaches are proposed in recent works to address this issue. For example, What are types of attacks and how to deal with such attacks, present intrusion system have some deficiencies [1].Intrusion detection system (IDS) can judge the destruction system and intrusion events by analyzing the network to transfer data. In some cases, simply using the firewall or authentication systems also can be broken. The detection system is a network-based intrusion detection system [2].A new architecture discuss of Wireless Intrusion Detection System (WIDS) for IEEE 802.11 wireless infrastructure networks[3].Security policy optimizer algorithms and their computational complicities need to optimize and optimize security policy manger notify Security policy Managers on each Access Point of the availability of a new Policy Database[4].After the explanation of these attacks, we discuss some defense techniques and an improved scheme against the attacks on wireless system will be implemented.

2. INTRUSION PREVENTION SYSTEM
Intrusion prevention System (IPS) is to manipulate the damage over network system and intruder events by analyzing packet activity all over territory. The traditional intrusion prevention system can only detect and respond to the destruction on the system. Today, intrusion prevention systems have been used in wireless local area network, to monitor and analyze various users' activities, determine the type of the invasion, detect illegal network behavior, and give an alert for abnormal network behavior. Wireless intrusion prevention system is similar to the traditional intrusion prevention systems, but only some change coverage and network latency are the key area .Today, most of the wireless intrusion prevention systems popular in the market are air defense monitor, watch and air defense guard.

3. RELATED WORK
The major wireless attack categories pertaining to IEEE 802.11 family networks and in particular the latest 802.11i security standard [1].Explained all kinds of the wireless attacks that have been performed on a wireless network in the past. Based on analyzing the drawbacks all attacks are targeted on, improved scheme for wireless network [11].Wireless IDS will be an important part of the WLAN. Although it still has some drawbacks, but overall the superior than others. New Wireless Intrusion Detection System (WIDS) for wireless networks. The WIDS can detect man-in-the-middle-attacks by analyzing the channel gap [3]. Performance analysis toolset remove the different weakness for wireless system [7]. After completing these initial jobs, the Security Manager helps to carry out these changes in policy while interacting with the underlying protocol stack, if there are any conflicts then the Security manager calls the adaptive security policy optimizer to remove some part of policy and maximizes the output [4].The mechanism is non-cryptographic, has less overheads and can be deployed in existing IEEE 802.11 WLANs [5]. The scanning it can detect such as DoS attacks and other Wlan attacks, tied with a strong security policy, can essentially meet the security requirements of a wireless LAN [2].Optimization of a wireless feature set has a significant impact on the efficiency and accuracy of the intrusion detection system [6].The system authenticates users on the basis of identity, rights & access hardware by distributed software agents that implement security policy and prevent unauthorized access[12].A Survey Study on Analysis of Attack Models via Unified Modeling Language in Wireless Sensor Networks [8].Precisely detecting a man-in-the-middle attack and successfully protecting AP from SYN Flood attack than other existing approaches [3].Optimal Wireless Network Restoration under Jamming Attack in a multi-hop multi-channel wireless network [9].

3.1 Proposed Algorithm for IPS
The equations show the time requirement for execution for the mobile agent.

$$T_{MINIMUM} = E\,t + A_T$$

Where Et =Execution Time

AT=Arrival Time

Our aim to minimize the function that are addition of the code execution time and agent query reporting time initially it start from 5 sec.In the algorithm of the agent minimizing the time of agent execute the particular task. In this paper, we take into account the amount of the data encounter by the agent each visited node over the network. And then give the response to the centralize IPS server. In the moving node is required message, and header, source, destination in second.

$$Tmin = \sum_{i=15}^{n} t.k \quad n \geq 57$$

The total life span of the agent to process and execute the particular query is the less than 57. Agent system gives the optimal solution scanning and prevention because it requires very less memory space as compare to other existing technology. There are various advantages why perform well because work on each port level with effective scanning and find out .The unauthorized person over the network. Thus all the communication now takes place effectively and locally. Then reduce the network traffic latency.

Table 1. Comparison with Existing Systems Time in Sec

Methods	Client Server	Agent Based System	Code On Demand	Remote Execution
Time	68	57	72	82

4. PROPOSED SYSTEM OVER VIEW FOR IPS

For new proposed system for intrusion prevention system is very simple and adopting in nature and give better result as compare to earlier approaches. Our systems mainly focused on centralized sever system, so that administrator can easily monitor due to agent based system and it take very less time complexity and reduce the network overhead.

Case 1*:* Suppose attacker tries to connect his laptop directly to networks .There is no IP address, MAC address found in data base hence not authorized user.

Case 2: Someone which inside in the network wants to do unwanted activity .Then we have runtime prevention systems who verifies MAC, SSID and IP along with unique ID.

Case 3: Some cases attacker want to connect with some readymade software. Then it's simple we trap with unique network ID, which manages my centralized server system.

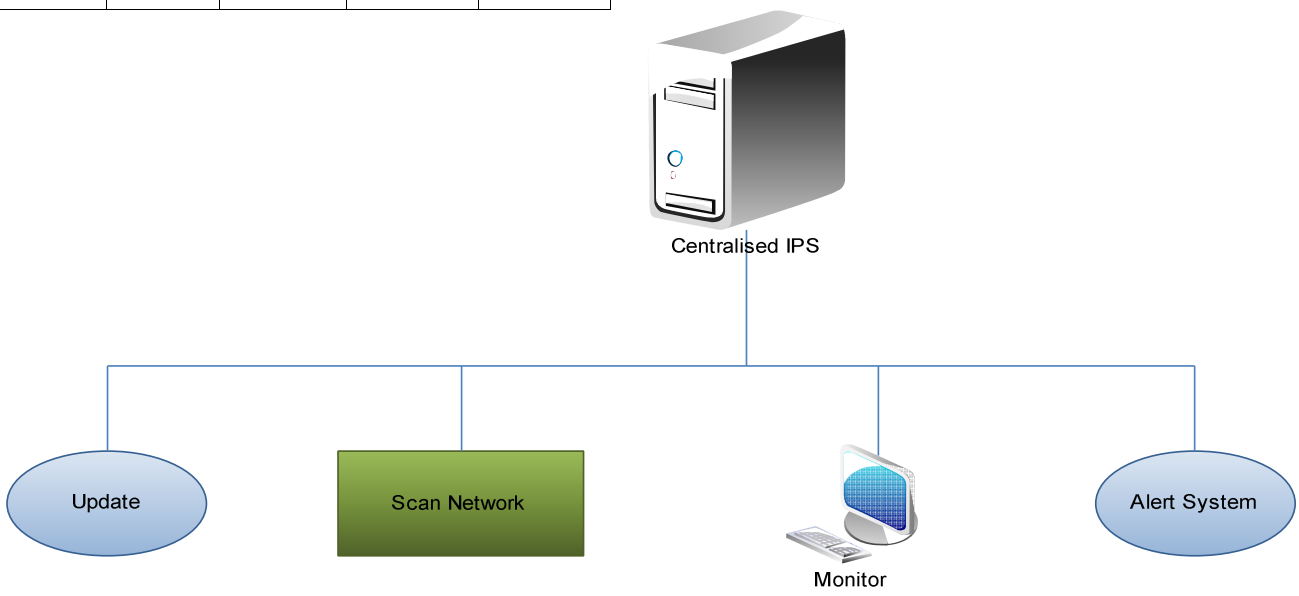

Fig 1: Proposed architecture for IPS

4.1 Experimental Results

In this paper, Experimental results were obtained using time and number of node interactions. The two types of classifications were trained using set of MAC address header attributes. The performance of the agent based IPS on the learning time and accuracy of the resulting classifiers. Experimental results clearly demonstrate that the performance of the classifiers trained with the reduced set of features is higher than the performance of the classifiers trained with the full set of features. Indeed, learning time is reduced by 57 percent.

The performance of the all four paradigm has shown in Table.1 of false positives and false negatives. The false positives rate is the percentage of frames containing normal traffic classified as intrusive frames. Likewise, the false negatives rate is the percentage of frames generated from wireless attacks which are classified as normal traffic. The false positives rate is reduced by an average of 24 percent when the reduced set of agent based system features is used as shown in figure 2.

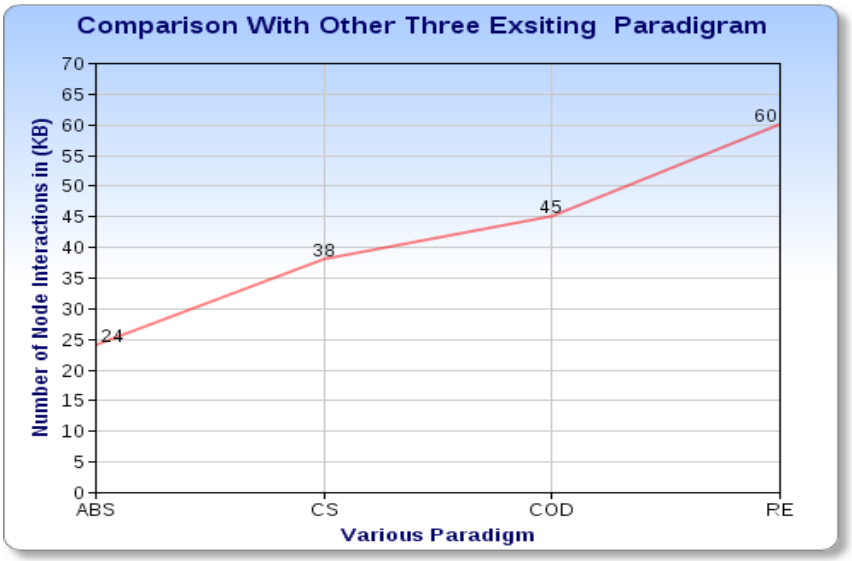

Fig 2: Total Number Node of Interactions

5. CONCLUSION AND FUTURE WORK

In this paper, we present the use of agent based communication over the network along with centralized server to improve performance by decreasing the false negative and false positive. The first, which we call network behavior, and works by forcing run time centralized server from network nodes to other clients. However, this centralized approach has been implemented in this above design will provide a much stronger security on networks. By structuring your wireless network to the above scheme, you will have an added level of security. It is required to develop a more efficient approach, which can detect the malicious packets and frame spoofing as well. Efficient methods are required to reduce network overhead associated with this method.

6. ACKNOWLEDGMENTS

First and foremost, I would like to thank Dr. D N Chaudhari for his most support and encouragement. He gently read my paper and offered precious detailed advices on motivate, organization, and the theme of the research paper.

7. REFERENCES

[1] Alexandros Tsakountakis, Georgios Kambourakis and Stefanos Gritzalis, 2007.Towards effective Wireless Intrusion Detection in IEEE 802.11i.

[2] Xiao qiang Peng,Cheng Zhang, Dian gang Wang, 2010.The intrusion Detection System design in WLAN based on Rogue AP.

[3] Huan—Rong Tang, Rou-Ling Sun, Wel-Qiang Kong,2009.Wireless Intrusion Detection For Defending Agaunst TCP SYN FLOODING ATTACK AND MAN-IN-THE-MIDDLE ATTACK.

[4] Debabrata Nayak, 2007.An Adaptive and Optimized Security Policy Manager for Wireless Networks.

[5] Yaqing Zhang,Srinivas ,2010.Client-based Intrusion Prevention System for Wireless LANs 802.11.

[6] Khalil El-Khatib, 2010.Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection Systems.

[7] Samer Fayssal,Byoung Uk Kim,2010.Performance Analysis Toolset for Wireless Intrusion Detection Systems.

[8] Sunghyuck Hong,Sunho Lim,2010.Analysis of Attack Models via Unified Modeling Language in Wireless Sensor Networks: A Survey Study.

[9] Shanshan Jiang and Yuan Xue, 2009.Optimal Wireless Network Restoration Under Jamming Attack.

[10] Ritu Chadha, Hong Cheng, Yuu-Heng Cheng, Jason Chiang, 2004.Policy-Based Mobile Ad Hoc Network Management*.

[11] Hua Li, Dimitri Reizvikh and Lucy (Liang) Lei,2007.An Improved Defense Scheme Against Attacks On Wireless Security.

[12] Larry Korba, 1998.Security System for reless Local Area Networks.