ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

ACIPS: Improvement of Client-Server based Intrusion Prevention System for Wireless LAN

S V Athawale, Dr M A Pund

Assistant Professor, Dept. of Computer, AISSMS College Engg, Savitribai Phule Pune University, India

Professor, Dept. of Computer, Prof. Ram Meghe Institute of Technology & Research, Badnera, Amravati, India

ABSTRACT: The expansion of wireless network and its application increased rapidly and that way raise new security concern. Mobile Ad Hoc Networks (MANET) is the hotspot of every attacker nowadays. To maximize security in wireless intrusion detection (IDS) and prevention system (IPS) system the conventional routing protocols do not take into consideration, the energy of the nodes while routes are being selected which leads to early exhaustion of nodes and partitioning of the network. In this paper, we discuss the main wireless attacks and its prevention we concerning only 802.11i family network. We designed client server based WIDPS system and our test result show that the proposed system is capable to detect attack effectively and stop most of wireless attacks . The proposed method has meagre network overheads and can be easily employed in existing IEEE 802.11 wireless LAN.

KEYWORDS: Mobile Ad Hoc Networks (MANET); intrusion detection system (IDS); intrusion prevention (IPS); Local area network (LAN).

I. INTRODUCTION

Wireless network is growing at a rapid pace and consumers across the globe and all people want to improve mobility and productivity. Due to wide coverage, this wireless LAN introduces a new threat broadcasting. The challenge of wireless LAN is to securely broadcast data in the wireless environment became the serious issue and now a days most of portable devices such as mobile ,laptop support wireless function and these devices support all most all operating system platform. Therefore, the challenge people faced is no longer just to ensure secure “wireless space”, but also to protect your computer connections with the outside world. The threats from WLAN are many, such as spying, denial service attacks, monitoring attacks, intermediary (MITM) attacks, intrusion from client to the client, Rogue AP, flooding attacks, and so on, in this paper focus on current threads on wireless.

There are many tools available for Wi-Fi such Wi-Fi manager, [1] Air sort these tools worked on windows as well as open source environment. In fact, especially for wireless network intrusion detection and prevention for WLAN is key area for future computing because future belongs to wireless networks.

Background

A. Overview Intrusion Detection and Prevention System

IDS (Intrusion Detection System) can be divided into host-based intrusion Maintenance System (HIDS) and network-based Intrusion Detection System (NIDS). HIDS uses files on the host (in particular log file or host network to send and receive data packets) as a data source. HIDS first appeared in the 21st century, the early'80s, when the network topology is simple and the intrusion is rare. HIDS focuses on post-mortem analysis attacks. HIDS is still primarily through the records to verify, but enhance the degree of automation, also to achieve accurate detection and rapid response. Different from HIDS, NIDS using the original network packets as a data source, which found signs of intrusion. It can detect and response to the intrusion without prejudice to the use of performance.

II. RELATED WORK

In the field of correspondence and knowledge reposition over the net, security has been the key focus of diverse analysts throughout the coming years. The Denial of Service (DoS) and Distributed Denial of Service (DDoS) area unit the kinds of attacks that have modified the purpose of read of system security. By these varieties [2] of attacks even superior limit servers are often pounded. attributable to the trusting method of information science, the supply location of a packet isn't valid thus it's hard for the victim to acknowledge the wellspring of DoS/DDoS attack. One of the foremost relevant problems within the construction of a Layer three protocol for wireless unplanned networking is security. The technology's potential to be a key resource in several mission essential applications will solely be consummated once the [3] network may be created resistant, if not fast, to attacks that hinder its operation. the matter of securing routing, already a tough one to resolve in wired networks, is exaggerated by Associate in Nursing order of magnitude in wireless networks, In order to make sure that the network is [4] not being compromised, a network administrator monitors the network in time period. Hardware support from AirDefense permits directors to add a sensing element next to their APs which is able to gather network info on a day after day and report any irregularity occurring on the network. They [5] gift the utilization of transmission rate along with FRR technique to boost this technique by decreasing the false negative and false positive. Presently available spoof noticeion ways unable to detect the adversary presence if victim not human activity. This results in false negative alarms. the answer to false negative is given in FRR-RA technique by causation periodic probing. Optimal wireless solution [6] linear programming issues and perform intensive performance evaluations to review the impact of various electronic jamming eventualities in a very multi-hop multi-channel wireless network. They proposed [7] mechanism is noncryptographic, has low overheads and can be deployed in existing IEEE 802.11 WLANs. The management of multi-threaded [8] processing and reporting sensors will spend more time than centralized wireless intrusion detection system. In this paper [9] they tend to discuss the major wireless attack classes regarding IEEE 802.11 family networks and above all the most recent 802.11i security commonplace. In this paper, they were propose a new architecture [10] of Wireless Intrusion Detection System (WIDS) for IEEE 802.11 wireless infrastructure networks. The WIDS then detects the man-in-the-middle-attacks by analyzing the channelizing gap.

A. Framework of Wireless IDPS

The framework of wireless intrusion detection and prevention system as shown in Fig1. It is rationally divided into seven parts first scan wireless network so that all IP address MAC are checked and compare second module is data bases which compare with existing authorised list third and it is most important part intrusion detection and prevention system with policies based on IP, MAC, SSID if these all three key parameter are match then finally we come to conclusion that whether it is authorised or its unauthorised.

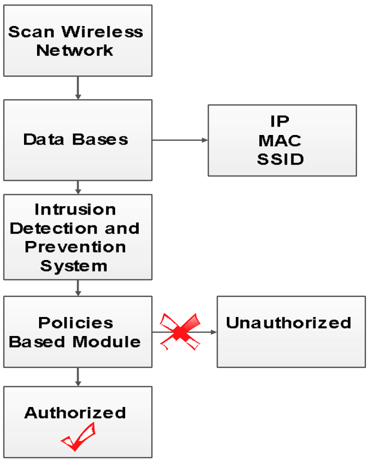

Fig.1. framework of wireless intrusion detection and prevention system

III. PROPOSED ALGORITHM

A. *Policy selection Algoritm:*

```
• Algorithm  Optimize PolicySelection: rule set,
• 1:Dmax=20
• 2.WNlist=visited=0
• 3:pool List=scan_nodes=0
• 4:for i=0 to 20 do
• 5:if(WNlist $\in$ ip AND WNlist $\in$ mac AND WNlist $\in$ ssid)
• 6:insert WNlist into pool_list
• 7:else insert WNlist into prevention list
• 8:i=i+1
• 9:end if
• 10:end for
• 11:return pool_list(authorised list)
```

B. *Description of the Proposed Algorithm:*

The main aim of the proposed algorithm is to maximize the wireless security and reduce the total transmission energy in terms of accuracy, bit width and time with efficient routes to transmit the packet all over the wireless network. The proposed algorithm is consists of two main formula .

Calculating Transmission Energy:

The transmission accuracy (T) of each node relative to its distance coverage with another node is calculated by using.

$$T= T_{node} \div R_{node} \times 100 \qquad \text{eq. (1)}$$

where ÷ is constant and n is node.

IV. PSEUDO CODE

```
Step 1: Scan all the wireless node in network.
Step 2:  The maximum wireless node 20
Step 3:  Check the below condition for each scan till last node available on wireless to transmit the packet.
             if (WNlist $\in$ ip AND WNlist $\in$ mac AND WNlist $\in$ ssid)
                     Make sure the wireless node pool list.
            else
                  Insert WNlist in to into prevention list nodes
            end
Step 4:  Calculate the total transmission energy for all 20 nodes.
Step 5: Select the energy efficient route on the basis of minimum total transmission energy of the route.
Step 6:  Calculate the TA transmission accuracy for each node of the selected route using eq.  (1).
Step 7: End.
```

V. SIMULATION RESULTS

This model is implemented by expanding the general-purpose network simulator NS2. The simulation model thus implemented is used to study the behaviour and deportment of wireless network with limited node (20) where they are believed to have better performance. Wireless trade-off between decoding accuracy and channel covertness. The channel was set with a = 15, *f = 7, mlow = 3,* and *mhigh* = 7. Accuracy tends to decrease, as shown in Fig, with an increase in *t.* This makes sense because as *D* monitors for longer time periods, given that the attacker is transmitting at very small values of a and *f,* the covert portion of traffic is hidden easily amidst the relatively large trace and anomalies are hard to detect. Figure 2. Detection accuracy having said that the scheme is able to detect with up to 90% accuracy even for increasingly stealthy attacker operation.

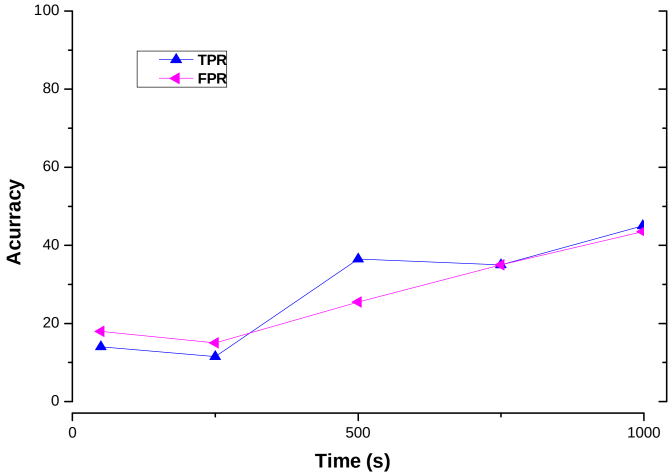

Fig. 2. Detection accuracy

Experiments were performed Figure 3. On the WLAN for both 802.11b and 802.11g specifications by configuring the AP to operate in the required mode. For each network type and protocol, 20 node and 50 sets of 1000 data packets. The detections from the 20 trials were used in determining TPR/FPR measures for the experiments. Accordingly, we tested our classifier with different input sizes and observed that it works with optimum accuracy for a minimal input trace of 1000 data packets

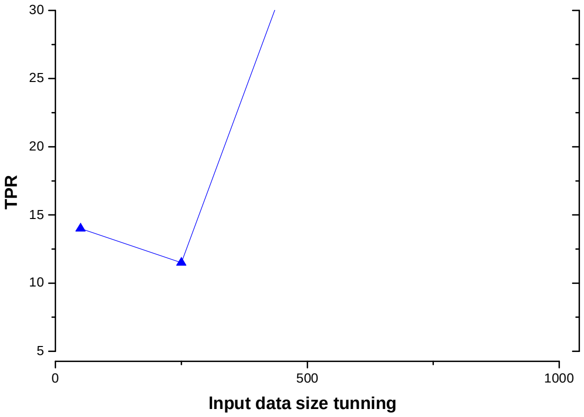

Fig .3. Data size tunning

In Figure 4, note that with an increase in bin width the accuracy drops, which makes sense as the classifier works better with a higher number of bins. The optimal bin width of 20μs was chosen, as it gives the minimum FPR of 0.1 and maximum TPR of 98.

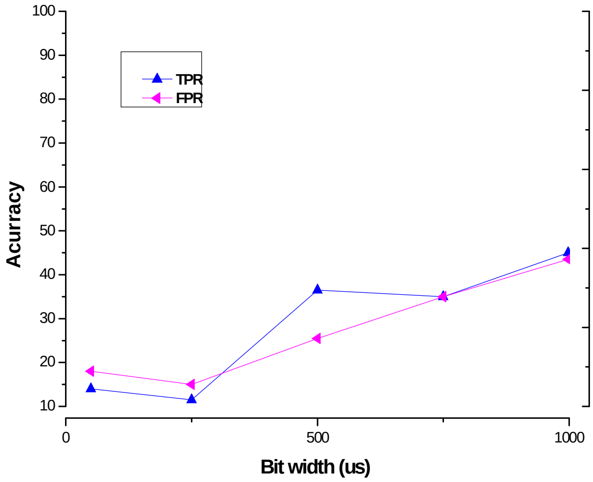

Fig .4. Bit width tunning scenario

VI. CONCLUSION AND FUTURE WORK

Our simulation results showed that the proposed Client-Server based Intrusion Prevention System for Wireless LAN performs better with the total Detection accuracy, Data size tunning, Bit width tuning scenario, this paper we have propounded an approach for constructing an intrusion prevention system for WLAN using specified policies based intrusion detection and prevention system this system implemented for attack detection and policy based monitoring its unique contribution of this work. The simulation results showed that the proposed algorithm performs better with the total transmission energy in term of accuracy and bit width and TPR and FPR metric than the maximum number of hops metric. The proposed algorithm provides energy efficient path for data transmission. We have used very small network of 20 nodes, in ns-2 all in one environment as number of nodes increases the complexity will increase. We can increase the number of nodes and analyze the performance if we increase number of node definitely increase network overhead and latency.

REFERENCES

1. S V Athawale,D N Chaudhari, “Towards effective Client-Server based Advent Intrusion Prevention system for WLAN”,pp.1 - 5,2015.
2. Anushree, Priyanka Baviskar,et.al., “Defence Mechanism to Mitigate DDoS Attack For Wireless LAN”,Volume – 5 Issue -02,pp.15714-15718,2016.
3. L. Felipe Perrone, Samuel C. Nelson, “A Study of On-Off Attack Models for Wireless Ad Hoc Networks”, pp.1 - 10, 2006.
4. Hua Li, Dimitri Reizvikh , Lucy (Liang) Lei, “An Improved Defense Scheme Against Attacks On Wireless Security”,pp.986-989,2007.
5. Shikha Goel,Sudesh Kumar, “An Improved Method of Detecting Spoofed Attack in Wireless LAN”,pp.104-108,2009.
6. Shanshan Jiang and Yuan Xue, “Optimal Wireless Network Restoration under Jamming Attack”, pp.1-6, 2009.
7. Yaqing Zhang,Srinivas Sampalli, “Client-based Intrusion Prevention System for 802.11 Wireless LANs”,pp.100-107,2010.
8. Xiao qiang Peng ,Cheng Zhang, Dian gang Wang, “The intrusion Detection System design in WLAN based on Rogue AP”,pp.432-436,2010.
9. Alexandros Tsakountakis et.al, “Towards effective Wireless Intrusion Detection in IEEE 802.11i”, pp.37-42, 2007.
10. HUAN-RONG TANG et.al, “WIRELESS INTRUSION DETECTION FOR DEFENDING AGAINST TCP SYN FLOODING ATTACK AND MAN-IN-THE-MIDDLE ATTACK”, pp.1464-1470, 2009.

BIOGRAPHY

Shashikant V. Athawale M Tech, CSE, in 2011, currently teaches graduate and postgraduate level Students in Computer Science and Engineering at Pune University in Pune Maharashtra, India.
He is currently a Ph.D candidate in computer science at the Sant Gadge Baba Amravati University in Maharashtra, India. He has worked extensively in both the wired and wireless network sectors to improve the network security of their critical information systems. His research focuses on developing the security of computer and wireless & Ad hoc network systems.

Dr. Mahendra A Pund is working as Professor in Computer Engineering Department at Prof. Ram Meghe Institute of Technology & Research, Badnera-Amravati, India. He has 22 years experience in teaching profession. Total 24 papers are published in International &National Conferences and International Journals. His research interest is in the areas of wireless network, ad hoc network and security issues, Image processing, Machine Learning, Image Processing and Pattern Recognition, Feature Extraction. He is guiding many research scholars and he is a member of CSTA, New York, CSI, ISTE, Associate Member of I.E, IACSIT, Singapore and IAENG, Hong Kong. Also, he is Advisory consultant to CapeArc Solutions Pvt. Ltd. (www.capearcsolutions.com),Consultant to New Gen Systems pvt.ltd.