International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 11 | Nov -2016 www.irjet.net p-ISSN: 2395-0072

An Enhance Network Security by Inhibited way in Wireless Ad Hoc Network: A Review

R. U. Patil , Prof. S.V.Athavale

M.E. Computer Engineering,
Department Of Computer Engineering All India ShriShivaji
Memorial Society's College Of Engineering
Pune, Maharshtra, India
Asst. Professor, Department Of Computer Engineering All India ShriShivaji
Memorial Society's College Of Engineering
Pune, Mahatashtra, India

Abstract - *In commercial, military and different other domains in past some years is observed the incredible rise in the deployment of WLANs. In the employment of 802.3(LAN) and 802.11(WLAN) inconceivable grow has been observed for the sake of recompenses such as enhanced scalability and mobility of computer networks. IP address and MAC address can take part in an significant role in identifying such culprits. So This provokes illegitimate minds consequently creating an vital issue of precautions for IP address and MAC address. Simply spoofed several such implementations using IP and MAC address. This is the source to release of network security techniques similar to IPS (Intrusion Prevention System). We propose in this paper the approach is with the help of predefined applications or commands first inspect the entire network. Who is logging into the network is authorized user or not to test and verify that everyone, a new constraint propose in this paper which will be sole to every user.*

Key Words: 802.3; 802.11; IP; MAC; IPS

1.INTRODUCTION

The vast usage of Internet now days, the world becomes a single large unit because of the internet any human being can searching, communicating, sharing, working in different fields. Now days one of the basic needs for any human being has certainly become Internet. On the timeline of development of different technologies in the computer networks, there was an period in which Internet was accessed through physical wired connections but now-a-days, development of wireless networks there is no need of physical wired connections. This has happen to possible just because of the stunning grow in the development of wireless networks. Wireless network is very simple to setup. Network looks superior with no wires and increases elasticity too. wireless networks are taking a increasingly vital role in modern society the lack of valuable and affordable security measures made them easy targets [7]. There is no any need of a cable to pull, holes to drill, to connect other devices, just plug in your wireless Access Point (AP), and wireless connection manager be necessary to connect usually, and you are now online. Your AP is also online along with you, but this time every other person who finds a consign inside a broadcast range of your AP and here difficulty for you to starts. There are big risks the use of Wireless Networks which have been identified and have that the five aims viz., security, privacy reliability, accessibility, authenticity and non-repudiation cannot be met. when Moving one Access Point (AP) to another One has the main problems in IP communication. IP addresses, MAC addresses, SSID, WEP methodologies must be taken into account for security purpose. For standard level of safety used this different techniques. Also important information or data of users such as user account and simple password can simply be analyzed which will in revolve lead to a confused wireless network environment. Security for user this present 802.11 WLAN encryption techniques as well as WEP, WPA and WPA2 are all weak and unsatisfied. This network can also become weak because of MITM (Man in the Middle). If an unauthorized Access Point (AP) is form into the wireless networks, the perceptive information in the communication process is level to descent. Such in numerous problems set forth a test to the security purpose of wireless networks and hence form a new security technology known as Intrusion Prevention System (IPS). For network security an Intrusion Prevention System is used in the wireless network. This system provides various rules and policies for network traffic and or alerting system or network administrators to block doubtful traffic. For being alert admin can to take the

required action. Hence to identify and remove unauthorized hosts give an efficient and reliable approach and which attempt to retail the security and confidentiality of wireless networks. Thereby enhancing the security and consistency of WLAN the main purpose of my paper.

2. RELATED WORK

The creation of rouge access points, the open proxy servers are very risky as it inadvertently results. In recent network development Rogue Access Points (RAPs) is one of the primary security threats and if not handled correctly in time, then it could lead from small network faults to network failures. Rouge Access Points are the access points. And which are produced without any proper authorization. These access points in direct to support the scalability of the network which creates most of the times authorized users wrongly. But for this increase the difficulty to the network. In some domains Wireless Ad hoc and Sensor Networks (WASN) are becoming an significant platform [6]. According to a study in all project network rogue APs are present on about 40%. The reason is advancements in hardware and software have made AP installation, AP discovery, and AP negotiation an easy task for intruders[2]. In to a central location is to aggregate the task of monitoring rogue APs on several segments. Rogue access points (APs) represent the enterprise network to a stream of security susceptibility. Behind the firewall they are typically connected to a network port [1][4].A new class of attacks which is formed in wireless multi-hop ad hoc networks called stealthy packet dropping. Stealthy packet reducing can be simply launched against multi hop wireless ad hoc networks ([7], [6]). The least packed route instead of the shortest route is the benefit of AODV protocol. Also it supports both unicast and multicast packet transmissions still for nodes in stable movement[5].when attackers use high grow antennas to get information such as signal power, source type, and packet size occurs a traffic-analysis attack [7].

3. PROPOSED SYSTEM ARCHITECTURE

In the proposed system scanning phase is important as it arise as a safeguard to the network, by attending which users are already logged in, into the network and after that ones who desire to access the internet through the network. Any one of the user, who is demanding to access the internet, has to have directly by the administrator. In this case administrator refers the Controller. All the users want to be registered. The whole network is scanned in the scanning phase and by the administrator data is given brought together in the form of IP address, MAC address and the Unique Key. The proposed system will run the scanning of network always, so any user who arrives into the network and asks for the internet will be identified and thus will be limited to register with the controller. The next phase in this expected system is report generation. This phase of report generation is based on the data that is collected from another phase that is scanning phase. In this phase all the IP addresses and the MAC addresses collected are molded into a report. After that it is supplied to the Controller alias the administrator. The controller check this report and then verify the users are validated, as valid or invalid based on the data. After their IP and MAC addresses are found valid then valid users are timely to provide their unique key. After providing the Unique Key the user is allowed to use the internet, in the database is found non-conflicting with the other entries in the database after its access. Then set aside a catlog record which users are invalid to avoid any future consequences. Following cases are in this system arises.

Case 1: In the database such client needs to authenticate itself and obtain its own unique key but only if the scanned IP and MAC addresses are NOT PRESENT.

Case 2 In the database such client needs to give its unique key whenever asked for but only if the scanned IP and MAC addresses are PRESENT.

Case 3: If any of the scanned parameters that is IP or MAC address is found to difference integrity constraints in the database then such client is thought to be an intruder and will be blocked.

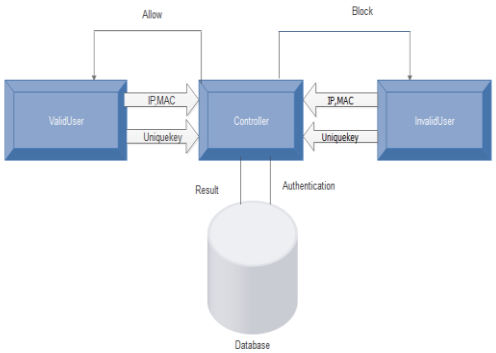

Fig 1.Proposed System Architecture

4.CONCLUSIONS

In this paper commence with the security of threat to the WLANs, then it overviews the existing intrusion prevention systems and limitations of them that have been tried to overcome in this paper. Proposed System to avoid illegal usage of internet, check of the whole network and keeps obstacle on non requested users with the help of their own uniqueness for security purpose. This proposed system shall be considered as a model for keeping frame between users and network resources. It is believed the proposed will bring an useful, more consistent, secure approach in network security. It is growing for IPS because of the way of interest and research is growing its rapidity in the field of network security so. I presented a system to identify APs from a central location using temporal traffic features. In my upcoming consideration work to develop this system in such a way that even other network resources will have opportunity to access only along with the Internet.

ACKNOWLEDGMENT

This paper involves number of respected helping hands. I am grateful to Prof. S. V. Athavale for his dedication and valuable guidance. I would like to thank the Department of Computer Engineering, AISSMS COE, Pune for their uninterrupted help and support.

REFERENCES

[1] S.B.Vanjale, Amol K. Kadam and Pramod A. Jadhav, 2011 Rogue Access Point Detecting & Eliminating in IEEE 802.11 WLAN, International Journal of Smart Sensors and AdHoc Networks (IJSSAN).

[2] Hitesh Thawani, VivekWaykule, and ShashiAthawale, 2013 Detection and Elimination of Unauthorized Hosts using MA based WIPS, International Journal of Computer Application.

[3] Ming Lei, Yang Xiao and Susan V. Vrbsky, 2008 Active Protection in Wireless Networking, The 4th International Conference on Mobile Ad-hoc and Sensor Networks by IEEE Computer Society.

[4] S.V. Athawale and S B Vanjale, 2011 802.11g Rouge Access Point Detection using MA, International Journal of Computer Science and Communication (ISSN 0973-7391).

[5] Yaqing Zhang and SrinivasSampalli, 2010 IPS for Client-based WLANs, 6th IEEE International Conference on Networking and Communications , Wireless and Mobile Computing.

[6] Issa Khalil and SaurabhBagchi, 2011 Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure, IEEE transactions.

[7] SamerFayssal and ByoungUk Kim, 2010 Performance Analysis Toolset for Wireless Intrusion Detection Systems, IEEE transactions.