International Journal of Engineering Research in Electronics and Communication Engineering (IJERECE) Vol 1, Issue 1, December 2014

Sensing vulnerabilities and multiple spoofing adversaries in wireless LAN

[1] S.karthika [2] A.kanagalakshmi
[1] PG student, ME Communication Systems, Sree Sastha institute of engg & tech, Chennai-123, [1] karthika.isro@gmail.com
[2] Assistant Professor ,Department of ECE, Sree Sastha institute of engg & tech,Chennai-123

Abstract- **Wireless spoofing attacks easy to launch and can significantly impact the performance of networks. The identity of a node verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. The spatial information of physical property associated with each node, hard to falsify and not reliant on cryptography, as the basis for detecting spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries. The formulation of determining the number of attackers as a multiclass detection problem. This project requires Request Storms (RS) algorithm to determine the number of attackers. This RS algorithm used for sending and receiving continuous packet transmission storms and detect malicious intruder using intensity based localization. The RS algorthim detect the unauthorized Internet Protocol / Medium Access Control (IP / MAC) and copy to the Access Control List (ACL), easy to detect and localize the intruder in the network. The integrated detection and localization system that can localize the positions of multiple attackers.**

Key words-**Spoofing,Internetprotocol,Medium access control protocol, Access control list.**

I. INTRODUCTION

A Wireless Local Area Network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. In 1997, Institute of Electrical and Electronics Engineers (IEEE) 802.11 was implemented as the first WLAN standard. It is based on radio technology operating in the 2.4 GHz. frequency and has a maximum throughput of 1 to 2 Mbps.

A.Overview

WLAN has been widely used in many sectors ranging from corporate, education, finance, healthcare, retail, manufacturing and warehousing. According to a study by the gartner group, approximately 74 percent of company laptops around the world will be equipped for WLAN by the end of 2013. It has increasingly becoming an important technology to satisfy the needs for installation flexibility, mobility, reduced cost of ownership and scalability.

Wireless networks are vulnerable to identity based attacks, including spoofing attacks, significantly impact the performance of networks. The generalized spoofing attack detection model generate unique identifier for each wireless nodes and a physical property associated with each node, as the basis for detecting spoofing attacks, finding the number of attackers when multiple adversaries masquerading as a same node identity and localizing multiple adversaries. Cluster based mechanisms are developed to determine the number of attackers.

In identity based spoofing attacks, an attacker can forge its identity to masquerade as another device or even create multiple illegitimate identities in the networks by masquerading as an authorized wireless Access Point (AP) or an authorized client. An attacker can launch Denial of Service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients. Therefore, identity based attacks will have a serious impact to the normal operation of wireless and sensor networks. Spoofing attacks can further facilitate a variety of traffic injection attacks such as attacks on access control lists, rogue AP attacks, and eventually DoS.

II. SECURITY THREATS OF WIRELESS LOCAL AREA NETWORK

Despite The Productivity, Convenience And Cost Advantage That Wlan Offers, The Radio Waves Used In Wireless Networks Create A Risk Where The Network Can Be Hacked. This Section Explains Three Examples Of Important Threats :Dos, Spoofing, And Eavesdropping.

A.*Denial Of Service*

In this kind of attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. Due to the nature of the radio transmission, the WLAN are very vulnerable against DoS attacks. The relatively low bit rates of WLAN can easily be overwhelmed and leave them open to DoS attacks. By using a powerful enough transceiver, radio interference can easily be generated that would enable WLAN to communicate using radio path. In computing, a DoS is an attempt to make a machine or network resource unavailable to its intended users. The target of a DoS attack vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend service of a host connected to the Internet. DoS attacks typically target sites or services hosted on high profile web servers such as banks, credit card payment gateways and even root nameservers.

B.Spoofing And Session Hijacking

This Is Where The Attacker Could Gain Access To Privileged Data And Resources In The Network By Assuming The Identity Of A Valid User. This Happens Because Ieee 802.11 Networks Do Not Authenticate The Source Address, Which Is Medium Access Control (Mac) Address Of The Frames. Attackers May Therefore Spoof Mac Addresses And Hijack Sessions. Moreover, Ieee 802.11 Does Not Require An Ap. This Facilitates Attackers Who May Masquerade As Ap. In Eliminating Spoofing, Proper Authentication And Access Control Mechanisms Need To Be Placed In The Wlan.

C.Eavesdropping

Eavesdropping involves attack against the confidentiality of the data that is being transmitted across the network. By their nature, WLAN intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any WLAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because the attacker can intercept the transmission over the air from a distance, away from the premise of the company.Eavesdropping can also be done over telephone lines, email, instant messaging and other methods of communication considered private. The communications is also vulnerable to electronic eavesdropping via infections such as trojans.

III. SPOOFING ATTACKS

More wireless networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin AP attacks. Attacker can easily break the wireless AP security and easily enter using some tools like cain and abel, wireshark and ethereal etc. When attacker entry is possible, then attacker wants to get some user credentials like username, password, balance amount, credit card number and other valuable information.

A.Possible Spoofing Attacks

Spoofing occurs when a hacker inside or outside a network impersonates the conversations of a trusted computer. Two general techniques are used during spoofing :

A hacker uses an Internet Protocol (IP) address that is within the range of trusted IP addresses.A hacker uses an authorized external IP address that is trusted.Spoofing is a technique an attacker send fake spoofed Address Resolution Protocol (ARP) messages onto a Local Area Network (LAN). Generally, the aim is to associate the attacker's MAC address with the IP address of another host (such as the default gateway) causing any traffic meant for that IP address to be sent to the attacker instead. A hacker uses an authorized external IP address that is trusted. ARP spoofing may allow an attacker to intercept data frames on a LAN, modify the traffic, or stop the traffic altogether. Often the attack is used as an opening for other attacks, such as DoS, man in the middle or session hijacking attacks.Session hijacking occurs in the context of a user, whether human or computer. The user has an on going connection with a server. Hijacking is said to occur when an attacker causes the user to lose connection and the attacker assumes identity and privileges for a period.Spoofing attacks are broadly classified into two types resource depletion attacks and masquerading attacks.

B.Resource Depletion Attack

In resource depletion attacks, an attacker sends high rate of request messages using random MAC values in order to emulate a high number of clients and consume scarce resources in the network.An attackerdepletes a resource to the point that the target's functionality is affected as shown in fig. 3.2. Virtually any resource necessary for the target's operation can be targeted in this attack. The result of a successful resource depletion attack is usually the degrading or denial of one or more services offered by the target. Resources required will depend on the nature of the resource to be depleted, the amount of the

resource the target has access to and other mitigating circumstances such as the target's ability to shift load, detect and mitigate resource depletion attacks.

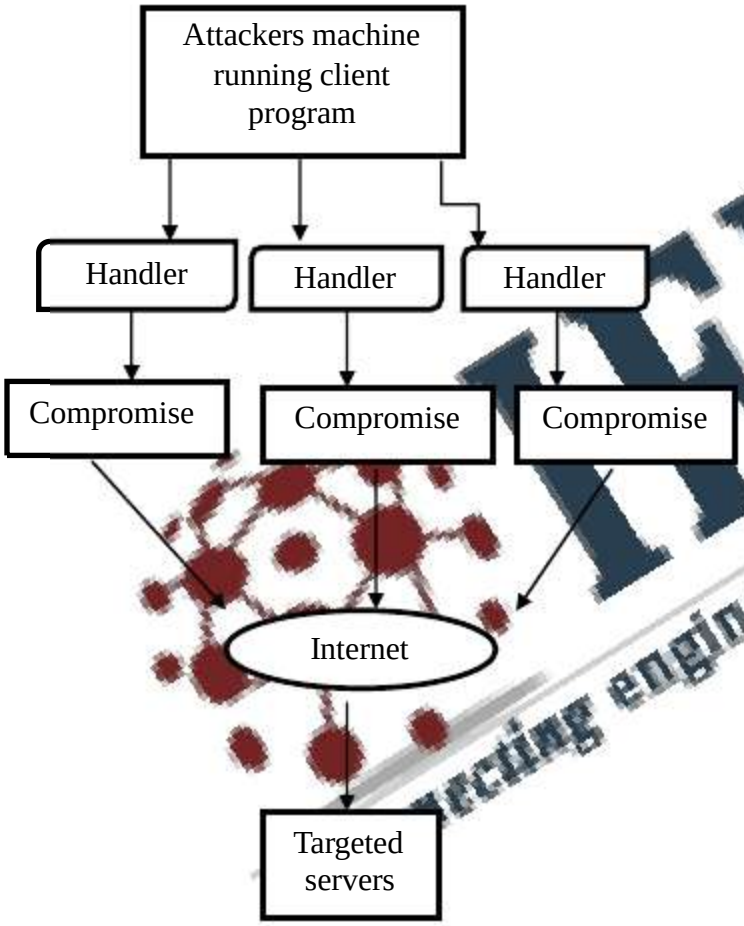

Fig. 1Resource Depletion Attack

Resource depletion can target endpoint hosts like servers and workstations as well as network resources like processing capability or memory consumption for normal operation. Resource depletion can also target exhaustion of bandwidth capabilities but the final goal is to make a DoS attack to the service. Virtually any resource necessary for the target's operation can be targeted in this attack. The more protected the resource and the greater the quantity of it that must be consumed, the more resources the attacker will need to have at their disposal.To prevent resource depletion monitor normal network activity and disable unnecessary services that could be used for undesired network device utilization. To avoid bandwidth exhaust should configure Quality of Service (QoS) at the perimeter of Wide Area Network (WAN) network to prioritize important traffic. If the network is at the edge of its capabilities because of bottlenecks in network should consider upgrading the weakest nodes or increasing the available bandwidth.

The result of a successful resource depletion attack is usually the degrading or denial of one or more services offered by the target. Resource depletion can target endpoint hosts like servers and workstations as well as network resources like processing capability or memory consumption for normal operation. The successful resource depletion attack is usually the degrading or denial of one or more services offered by the target. Vulnerable authentication is one of the other factors that can trigger a attack, as it helps the attacker to gain access much more easily.

C.Masquerading Attack

In masquerading attacks, an attacker targets a specific client by cloning its MAC address or the address of its AP. A masquerade attack is an attack that uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. If an authorization process is not fully protected, it can become extremely vulnerable to a masquerade attack.The attack can be triggered either by someone within the organization or by an outsider if the organization is connected to a public network.The amount of access masquerade attackers get depends on the level of authorization they have managed to attain. The target has access to, and other mitigating circumstances such as the target's ability to shift load. As such, masquerade attackers can have a full smorgasbord of cybercrime opportunities if they have gained the highest access authority to a business organization. Personal attacks, although less common, can also be harmful.

Masquerade attacks may happen in a number of ways. In case of an insider attack, a masquerade attacker gains access to the account of a legitimate user. Vulnerable authentication is one of the other factors that can trigger a masquerade attack, as it helps the attacker to gain access much more easily. Once the attackers gain access, they can get into all of the organization's critical data and can delete or modify it. For example, although a unique IP address is assigned to each individual computer, a hacker can convince another system that it is the authorized user through spoofing, essentially convincing the target computer that the hacker's computer has the same IP.

IV. PROPOSED SYSTEM

The proposed system will lead to develop Request Storms (RS) algorithm. In RS algorithm, the ARP duplicate IP address detection is already turned on by default and it have features to uncover the detect ARP, RS function. This function can also provide summaries of ARP flooding and ARP spoofing attack events as shown in fig 2. ARP flooding and spoofing attack is even capable of indicating which

frames should be further investigated because they were involved in an attack.

A.System Requirements

The requirements specification is a technical specification of requirements for the software products. It is the first step in the requirements analysis process it lists the requirements of a particular software system including functional, performance and security requirements. The hardware requirements consist of processor type, speed, Random Access Memory (RAM) and hard drive. The purpose of software requirements specification is to provide a detailed overview of the software project, its parameters and goals. This describes the project target audience and its user interface, hardware and software requirements.

B.Java

Java programming language was originally developed by Sun Microsystems which was initiated by James Gosling and released in 1995 as core component of Sun Microsystems' Java platform (Java 1.0). In java, everything is an object. Java can be easily extended since it is based on the object model.With Java's secure feature it enables to develop virus-free, tamper-free systems. Authentication techniques are based on public key encryption.Java is designed to be easy to learn.Java enables high performance.Java is designed for the distributed environment of the internet.

C.Java Swing

Swing is an advanced Graphical User Interface (GUI) toolkit. It has a rich set of widgets.Swing is a part of Java Foundation Classes (JFC). It is a collection of packages for creating full featured desktop applications. JFC consists of Abstract Window Toolkit (AWT), swing, accessibility, java 2Dimensional (2D), and drag and drop. The java platform has java2D library, which enables developers to create advanced 2D graphics and imaging.

There are basically two types of widget toolkits. Light weight and Heavy weight.

A heavyweight toolkit uses Operating Systems (OS) Application Programming Interface (API) to draw the widgets. For example Borland's Visual Computing Library (VCL), is a heavyweight toolkit.

V. ESTABLISHING WIRELESS NETWORK AND MONITORING

WPA is a mechanism provides pre shared key between AP and nodes. So using that key only, anyone can enter into the network. It also uses data integrity check. It is possible to easily analyze integrity of the received data. Establishing secure wireless networks is very important, because any intruder can poison the network at any time. Two kinds of authentication mechanisms used in Wired Equivalent Privacy (WEP). WPA provides pre shared key between AP

and nodes. So anyone can enter into the network. It is possible to easily analyze integrity of the received data.The status of system as shown in fig. 2 Establishing secure wireless networks is very important, because any intruder can poison the network at any time.

Fig.2 System Status

A. Cracking Wired Equivalent Privacy

A password and cryptography attack that does not attempt to decrypt any information, but continue to try a list of different passwords, words or letters. For example, a simple brute force attack may have a dictionary of all words or commonly used passwords and cycle through those words until it gains access to the account as shown in fig. 3.Although a brute force attack may be able to gain access to an account eventually, these attacks can take several hours, days, months and even years to run. The amount of time it takes to complete these attacks is dependent on the complexity of the password, the strength of the encryption, how well the attacker knows the target and the strength of the computers being used to conduct the attack.

Fig.3 Wireless Basic Settings

B. Attack Detection

The RS algorithm is used for sending and receiving continuous packet transmission storms and detects the malicious intruder using intensity based localization. From RS algorithm can get ARP flooding or ARP spoofing attack events. Using this, it is possible to add this detected IP / MAC to ACL. In this way, it is easy to detect and localize the intruder.

C. LOCALIZATION

In this phase, attacking the network using some tools, like wireshark, cain&abel. When anyone tries to intrude this secure network, the RS algorithm will detect the unauthorized IP / MAC and copy it to the ACL. So, it is very easy to detect and localize the intruder in a network as shown in fig. 4.

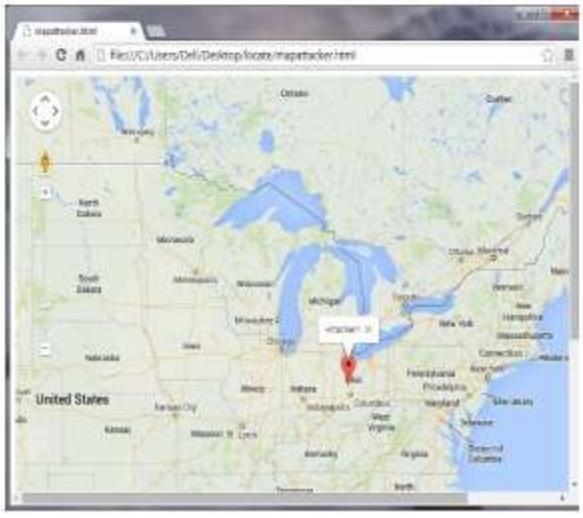

Fig.4Localization Attacker Using Internet Protocol

Based on the work the sensor energy levels at the individual nodes to calculate target object localizations and show that this does not add excessive amounts of computation or communication compared to a plain tracking algorithm such as envirotrack. On the contrary, knowing the current and past locations of the target objects also helped them with the tracking aspect as it enable to predict the object's future path.

CONCLUSION AND FUTURE WORK

As wireless networks are integrated with our daily social lives and there is an increasing need to support emerging mobile wireless applications. One serious class of threats that will affect the successful deployment of mobile wireless applications are spoofing attacks. In this work, proposed an unique approach to detect spoofing attacks in mobile wireless environments, which is a problem that has not been addressed in previous work. This approach can detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that it is possible to localize any number of attackers and eliminate them. Determining the number of adversaries is a particularly challenging problem. By developing a strong algorithm it will be possible to spoof vulnerabilities and detect number of adversaries in wireless LAN. Further, based on the number of attackers will be determined by this mechanism. The integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing strong evidence of the effectiveness of the approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries.This project can also be extended to applications such as military application and organization.

REFERENCES

1. Abu A. and Abed R. (2010) 'Enhancement of Passive MAC Spoofing Detection Techniques', (IJACSA) International Journal of Advanced Computer Science and Application, Vol. 1, No. 1, pp. 11-18.
2. Chandrasekaran and Francisco (2009) 'Detecting Identity Spoofs in IEEE 802.11e Wireless Networks', Global Telecommunications Conference, Vol. 1, No. 1, pp. 1-6.
3. Jieyang, Yingying and Trappe (2009) 'Detecting Spoofing Attacks in Mobile Wireless Environments', IEEE trans. Communications Society Conference on Digital Object Identifier, Vol. 2, No. 1, pp. 1-9.

4. Lifeng S. and Arora (2008) 'Spatial Signatures for Lightweight Security in Wireless Sensor Networks', IEEE International Conference on Computer Communications, Vol. 4, No. 1, pp. 17-23.
5. Misra and Gosh (2007) 'Detection of Identity Based Attacks in Wireless Sensor Networks Using Signal Prints', IEEE International Conference on Cyber, Physical and Social Computing, Vol. 7, No. 1, pp. 35-41.
6. Quing L. and Trappe (2007) 'Detecting Spoofing and Anomalous Traffic in Wireless Networks via Forge-Resistant Relationship', IEEE trans. Information on Forensics and Security, Vol. 2, No. 1, pp. 4-9.
7. Wool (2005) 'Lightweight Key Management for IEEE 802.11 WLAN With Key Refresh and Host Revocation', Springer Wireless Networks, Vol. 11, No. 2, pp. 677-686.
8. Yang and Trappe (2013) 'Detection and Localization of Multiple Spoofing Attackers in Wireless Networks', IEEE trans. Parallel and Distributed System, Vol. 9, No. 1, pp. 44-58.
9. Ying and wade T. (2013) 'Detecting and Localizing Identity Based Attacks in Wireless and Sensor Networks', IEEE trans. Vehicular Technology, Vol. 59, No. 1, pp. 62- 68.