International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

# Detection and Localization of Multiple Spoofing Attackers in Wireless Networks

**Mr. Shadab A. Khan[1], Ms. Rupali S. Pophale[2]**

*Computer Engineering Department, CSMSS College of Polytechnic,India*

## ABSTRACT

*Wireless spoofing attacks are easy to launchand can significantly impact the performance of networks. Although the identity of a node can be verified throughcryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. This project is proposed to use spatial information, a physical property associated with each node, hard to falsify, and not reliant on cryptography, as the basis for 1) detecting spoofing attacks; 2) determining the number of attackers when multiple adversaries masquerading as the same node identity; and 3) localizing multiple adversaries. It is proposed to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. It formulates the problem of determining the number of attackers as a multi-class detection problem.*

*Cluster-based mechanisms are developed to determine the number of attackers. When the training data are available, the project explores using the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. In addition, it develops an integrated detection and localization system that can localize the positions of multiple attackers.*

*More Hit Rate and Precision percent is achieved when determining the number of attackers. The localization results use a representative set of algorithms that provide strong evidence of high accuracy of localizing multiple adversaries. In addition, a fast and effective mobile replica node detection scheme is proposed using the Sequential Probability Ratio Test. The project shows analytically and through simulation experiments that the scheme detects mobile replicas in an efficient and robust manner at the cost of reasonable overheads.*

***Keywords: Wireless network security, spoofing attack, attack detection, localization.***

## 1. INTRODUCTION

A Wireless network is a computer network that uses a wireless network connection such as a cell phone network, Wi-Fi local network or a terrestrial microwave network. Wireless networking is amethod which homes, telecommunications networks and enterprise(business) installations avoid the costly process of introducing cables into a building, or as a connection between variousequipment locations. Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.

### 1.1. Network Security

A wireless network is a computer network that uses a wireless network connection such as a cell phone network, Wi-Fi local network or a terrestrial microwave network.Wireless networking is a method in telecommunications Networks and enterprise (business) installations avoid the costly process of introducing cables into a building. Wireless telecommunications networks are generally implemented and administered using radio

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

communication. This implementation takes place at the physical level (layer) of the OSI model network structure.

### 1.2. Wireless Network Protection

Wireless technologies enable one or more devices to communicate without physical connections without requiring network or peripheral cabling. Wireless technologies use radio frequency transmissions as the means for transmitting data. Wireless technologies range from complex systems, such as Wireless Local Area Networks (WLAN) and cell phones tosimple devices such as wireless headphones, microphones, and other devices that do not process or store information. They also include infrared (IR) devices such as remote controls, some cordless computer keyboards and mice, and wireless hi-fi stereo headsets, all of which require a direct line of sight between the transmitter and the receiver to close the link.

**A) Wireless Lans**

WLANs allow greater flexibility and portability than do traditional wired local area networks (LAN). Unlike a traditional LAN, which requires a wire to connect a user's computer to the network, a WLAN connects computers and other components to the network using an access point device. An access point communicates with devices equipped with wireless network adaptors; it connects to a wired Ethernet LAN via an RJ-45 port. Access point devices typically have coverage areas of up to 300 feet (approximately 100 meters). This coverage area is called a cell or range. Users move freely within the cell with their laptop or other network device. Access point cells can be linked together to allow users to even with the users who are aside.

**B) Wireless Lans Device**

A wide range of devices use wireless technologies, with handheld devices being the most prevalent form today. Thisdocument discusses the most commonly used wireless handheld devices such as text messaging devices, PDAs, and smart phones.

**C) Wireless Standards**

Wireless technologies conform to a variety of standards and offer varying levels of security features. The wireless standards are the IEEE 802.11 and the Bluetooth standard. WLANs follow the IEEE 802.11 standards. Ad hoc networks follow proprietary techniques or are based on the Blue tooth standard.

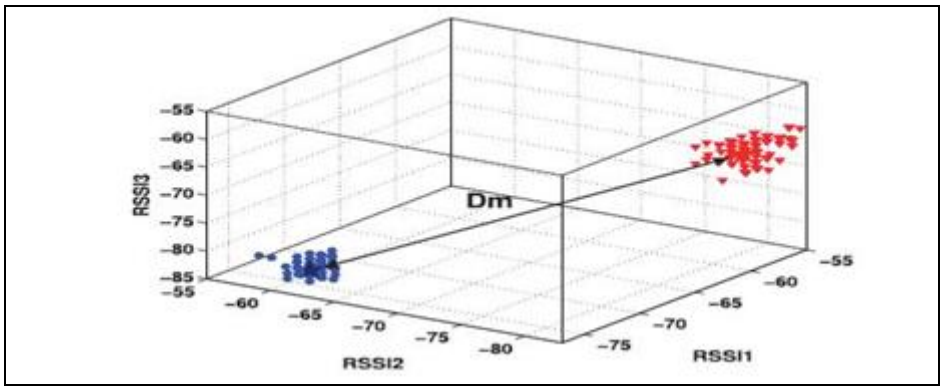
### 1.3. Emerging Wireless Technologies

Originally, handheld devices had limited functionality because of size and power requirements. However, the technology is improving, and handheld devices are becoming more feature-rich and portable. Smart phones are merging mobile phone and PDA technologies to provide normal voice service and email, text messaging, paging, Web access, and voice recognition. Next-generation mobile phones are quickly incorporating PDA, IR, wireless Internet, e-mail, and global positioning system (GPS) capabilities with device capable of delivering multiple services.

**D) Received Signal Strength**

In this work, they propose to use received signal strength (RSS)-based spatial correlation, a physical property associated with each wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346



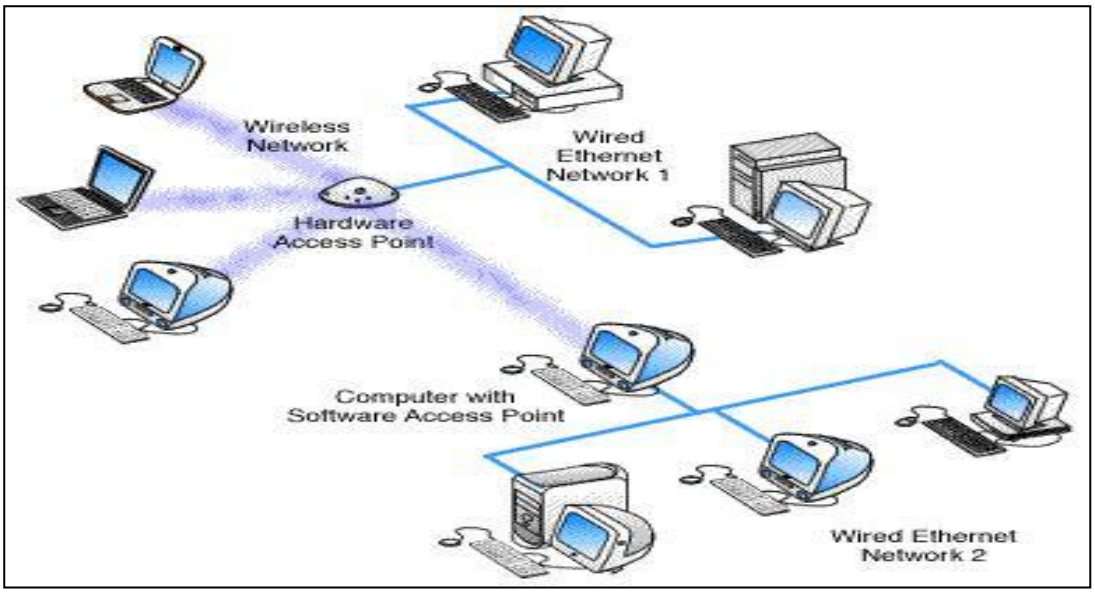

**E) Ieee 802.11 Architecture**

The IEEE 802.11 standard permits devices to establish either peer-to-peer (P2P) networks or networks based on fixed access points (AP) with which mobile nodes can communicate. Hence, the standard defines two basic network topologies: the infrastructure network and the ad hoc network.

The infrastructure network is meant to extend the range of the wired LAN to wireless cells. A laptop or other mobile device may move from cell to cell (from AP to AP) while maintaining access to the resources of the LAN. A cell is the area covered by an AP and is called a "basic service set" (BSS). The collection of all cells of an infrastructure network is called an extended service set (ESS).

**Fundamental 802.11 Wireless LAN Topology**

The Adhoc network, is meant to easily interconnect mobile devices that are in the same area (e.g., in the same room). In this architecture, client stations are grouped into a single geographic area and can be Internet-worked without access to the wired LAN (infrastructure network). The interconnecteddevices in the ad hoc mode are referred to as an Independent Basic service set (IBSS).



IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

**Wireless Networks**

APs may also provide a "bridging" function. Bridging connects two or more networks together and allows them to communicate—to exchange network traffic. Bridging involves either a point-to-point or a multipoint configuration.In a point-to-point architecture, two LANs are connected to each other via the LANs' respective APs.In multipoint bridging, one subnet on a LAN is connected to several other subnets on another LAN via each subnet AP.

**F) Attacks**

In many ways, network security can be destroyed. Attacks may occur through technical means such as specific tools designed for attacks or exploitation of vulnerabilities in a computer system. Attacks against information in electronic form have another interesting characteristic that is information can be copied, but it is not lost. It is just now resides in both the original owner's and the attacker's hands. This is not that damage is not done, but it may be much harder to detect since the original owner is not deprived of the information.

Network security attacks are typically divided into *passive* and *active* attacks. These two broad classes are then subdivided into other types of attacks.

**Passive Attack**—An attack in which an unauthorized party gains access to an asset and does not modify its content (i.e., eavesdropping). Passive attacks can be either eavesdropping or traffic analysis .

**Eavesdropping**—The attacker monitors transmissions for message content. An example of this attack is a person listening into the transmissions on a LAN between two workstations or tuning into transmissions between a wireless handset and a base station.

**Traffic analysis**—The attacker, in a more subtle way, gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages between communicating parties.

**Active Attack**—an attack whereby an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack but it may not be preventable. Active attacks may take the form of one of four types (or combination thereof): masquerading, replay, message modification, and denial-of-service (DoS). These attacks are defined below.

**Masquerading**—the attacker impersonates an authorized user and thereby gains certain Unauthorized privileges.

Replay The attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user.

**Message modification**—the attacker alters a legitimate message by deleting, adding to, Changing, or reordering it.

**Denial-of-service**—the attacker prevents or prohibits the normal use or management of Communicational facilities.

**G) Security of 802.11 Wireless Lans**

The IEEE 802.11 specification identified several services to provide a secure operating environment.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346


The security services are provided largely by the Wired Equivalent Privacy (WEP) protocol to protect link-level data during wireless transmission between clients and access points. WEP does not provide end-to-end security but provides security only for the wireless portion of the connection.

**Security Features of 802.11 Wireless LANS Per the Standard**

The three basic security services defined by IEEE for theWLAN environment are as follows:

Authentication: A primary goal of WEP was to provide a security service to verify the identity of communicating client stations. This provides access control to the network by denying access to client stations that cannot authenticate properly.

**Types of Authentication:**

Open-system authentication and shared-key authentication. Shared-key authentication, is based on cryptography. The open-system authentication technique is not truly authentication. The access point accepts the mobile station without verifying the identity of the station. The mobile station must trust that it is communicating to a real APConfidentiality/privacy: It was developed to provide "privacy achieved by a wired network." The intent was to prevent information compromise from casual eavesdropping (passive attack). The 802.11 standard supports privacy through the use of cryptographic techniques for the Wireless interface. The WEP cryptographic technique for confidentiality also uses the RC4 symmetric key, stream cipher algorithm to generate a pseudo-random data sequence. This "key stream" is simply added modulo 2 (exclusive-OR-ed) to the data to be transmitted. Through the WEP technique, data can be protected from disclosure during transmission over the wireless link. WEP is applied to all data above the 802.11 WLAN layers to protect traffic such as Transmission Control Protocol/Internet Protocol (TCP/IP), Internet Packet Exchange (IPX), and Hyper Text Transfer Protocol (HTTP).

**WEP Privacy Using RC4 Algorithm**

Integrity: Another goal of WEP was a security service developed to ensure that messages are not modified in transit between the wireless clients and the access point in an active attack.

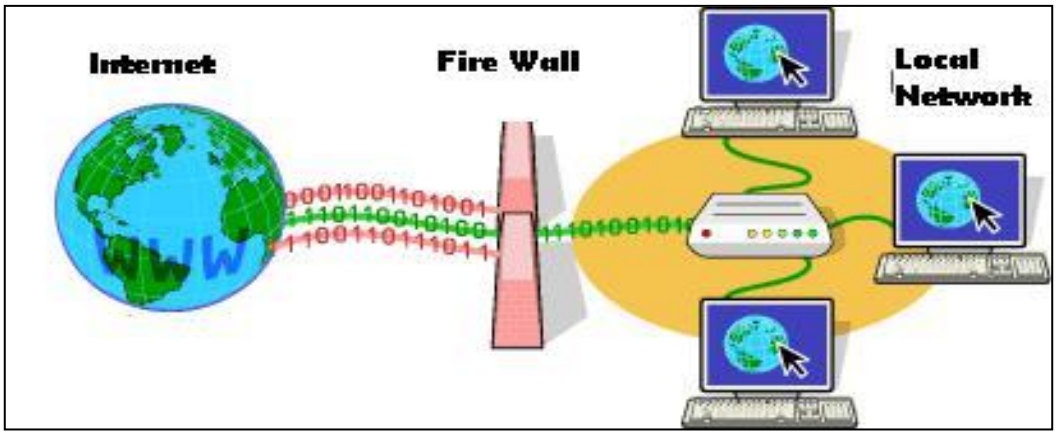
International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 09 , September 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

## II. SOFTWARE SOLUTIONS

### *A) Firewalls*

Firewalls are access control devices for the network and web that can assist in protecting an organization's internal network from external attacks. By their nature, firewalls are border security products, meaning that they exist on the border between the internal network and external network.

Properly configured, firewalls have become a necessary security device. A firewall is a network access control device that is designed to deny all traffic except that which is explicitly allowed. Firewall is a security device that can allow appropriate traffic to flow. Firewalls can perform a centralized security management function. Firewalls can be configured to allow traffic on the web based on the service, the IP address of the source or destination, or the ID of the user requesting service. Firewalls can also be configured to log all traffic.




**Encryption**

Encryption is simply to secure the information in web in such a way as to hide it from unauthorized individuals while allowing authorized individuals to see it. Individuals are defined as authorized if they have the appropriate key to decrypt the information. As long as the unauthorized individual does not have the key, the information would besafe. When a user encrypts a message in one key to create an output cipher text, decryption of that cipher text requires the use of the key to obtain the original message.

Through the use of encryption, we can provide portions of three security services:

**Confidentiality:** Encryption can be used to hide information from unauthorized individuals, either in transit or in storage.

**Integrity**: Encryption can be used to identify changes to information either in transit or in storage.

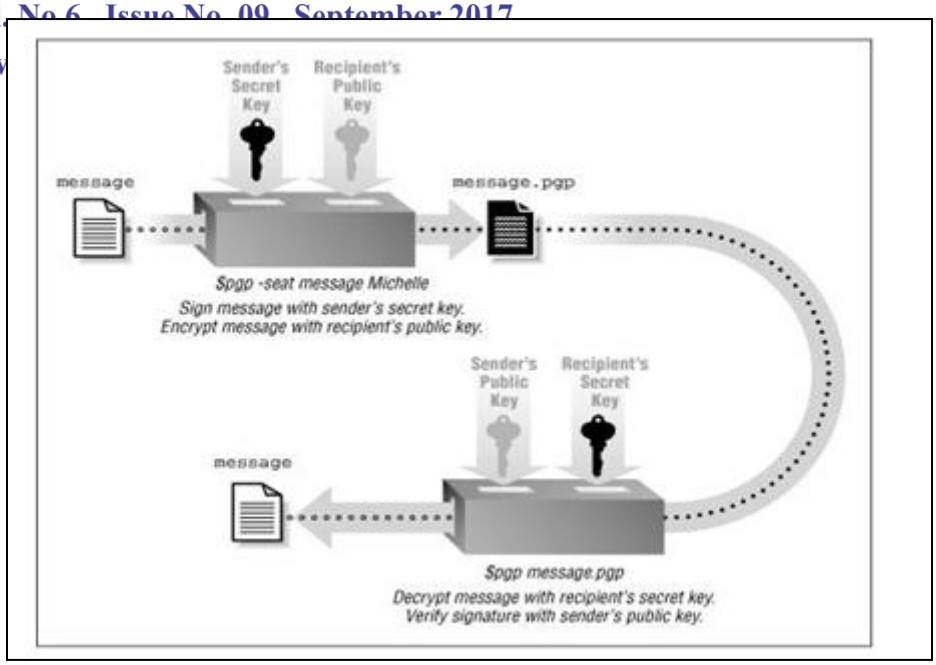
**Accountability:** Encryption can be used to authenticate the origin of information and prevent the origin of information from repudiating the fact that the information came from origin.

**Encryption:** Encryption is the process of converting readable information called plaintext into unreadable information called cipher text.

**Decryption:** Decryption is the process of reverting encrypted information (cipher text) back to plaintext.

**Key:** A key is the value that causes a cryptographic algorithm to run in a specific way and produce a specific cipher text. Key size, usually measured in bits. It is called key space.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346




## III. CONCLUSION

In signal strength-based spatial correlation, a physicalproperty associated with each wireless device that is hard to falsifyandnot reliant oncryptographyasthebasisfordetecting spoofing attacks in wireless networks. It providedtheoretical analysis of using the spatial correlation of RSSinherited from wireless nodes for attack detection. It derivedthe test statistic based on the cluster analysis of RSS readings.The approach can both detects the presence of attacks as wellas determine the number of adversaries, spoofing the samenode identity, so that we can localize any number of attackersand eliminate them.

## REFERENCES

[1] J.Bellardo and S. Savage, "802.11 Denial-of-Service Attacks. Real Vulnerabilities and Practical Solutions". In Proceedings of the 12thUSENIX Security Symposium, Washington, D.C., August 4-8, 2003.

[2] Bernard Aboba. IEEE 802.1X Pre-Authentication. Presentation to802.11 WGi,, July 2002.

[3] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop WirelessSecurity (WiSe), pp. 79-87, 2003.

[4] S. Capkun, L. Buttyan, and J. Hubaux. Self-Organized Publick-key Management for Mobile Ad Hoc Networks. IEEE Transactions on Mobile ComputingVol.2 NO.1 2003.

[5] Demirbas and Y. Song. An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks. In Proc. Of International Workshop on Advanced Experimental Activities on Wireless Networks and Systems, June 2006.

[6] A. Wool, "Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation," ACM/Springer Wireless Networks, vol. 11, no. 6, pp. 677686, 2005.

[7] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc. IEEE Int'l Paralleland Distributed Processing Symp. (IPDPS), 2005.