ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Special Issue 2, April 2014

Attack Detection and Localizing Adversaries in Wireless Networks

Annapoorani.T[1], Kanchana.K [2]

PG Student [Embedded Systems], Dept. of EEE, Saveetha Engineering College, Chennai, Tamilnadu, India [1]

Assistant professor, Dept. of EEE, Saveetha Engineering College, Chennai, Tamilnadu, India [2]

ABSTRACT— Wireless Systems are now popular worldwide to help people and machines to communicate with each other irrespective of their location, where it has an endless quest for increased capacity and improved quality. Although there are many advantages but it still has some disadvantages. This paper deals with the vulnerabilities in the wireless systems. The vulnerabilities present in the wireless technology that are mostly related to threats and risks. Though much vulnerability are in the wireless systems this paper mainly deals with the spoofing attacks.

In wireless systems the adversaries can launch any type of attacks to steal the data and to slowdown the performance of the network. The main cause of this paper is to convey that wireless systems need a stronger mechanism. So we also propose to perform hardware implementation using a Zig bee transceiver which uses the standard (802.15.4) mainly based on Zigbee protocol Stack.

KEYWORDS- Spoofing Attack, Detection, Localization, Multiple Adversaries, Wireless Network Security.

I.INTRODUCTION

Wireless communication is the transfer of information such as voice or data between two or more nodes. Wireless communications which are involves in various types of applications such as radios, cellular telephones, PDA & wireless networking. In wireless communication different frequency are used for various applications. In this communication the information is transferred over both short and long distances.

Wireless communication, which mainly helps to get freedom from, wires which in saves the cost of installing wires. It provides instantaneous communication without physical connections setup eg: Bluetooth, Wi-Fi. It helps as communicate where wiring is infeasible or costly eg: rural areas, old building, battle field, vehicles. It has flexibility to stay connected anywhere at any time. It also have some disadvantages in which it need for stronger security mechanisms such as privacy, authentication and also it has higher probability of data corruption. This paper uses to detect and prevent the attacks happening in wireless communication field to provide stronger security.

An attack is an attempt by an unauthorized person to gain access to or modify information, assume control of an authorized session, disrupt the availability of service to authorized users. The targets are chosen based on attackers motivation, which causes several vulnerabilities in wireless systems. Generally they perform the steps in attacks Conduct reconnaissance, Scan, Research vulnerabilities, Perform the attack, Create a backdoor& Cover tracks. Some types of attacks in wireless communication are Denial-of-service, Backdoors/Trapdoors, Sniffing, Spoofing, Man-in-the-middle, Replay, TCP/IP hijacking, Password guessing, Attacks on encryption. However this paper, which mainly deals with, the spoofing, attacks in wireless systems.

The word "spoof" means to hoax, trick, or deceive. Therefore, in the IT world, spoofing refers tricking or deceiving computer systems or other computer users. Hiding one’s identity or faking the identity of another user on the Internet typically does this process. Spoofing can take place on the Internet in several different ways. One common method is through e-mail. E-mail spoofing involves sending messages from a bogus e-mail address or faking the e-mail address of another user. Fortunately, most e-mail servers have security features that prevent unauthorized users from sending messages. However, spammers often send spam messages from their own SMTP, which allows them to use fake e-mail addresses. Therefore, it is possible to receive e-mail from an address that is not the actual address of the person sending the message.

Another way spoofing takes place on the Internet is via IP spoofing. This involves masking the IP address of a certain computer system. By hiding or faking a computer's IP address, it is difficult for other systems to determine where the computer is transmitting data from. Because IP spoofing makes it difficult to track the source of a transmission, it is often used in denial-of-service attacks that overload a server. This may cause the server to either crash or become unresponsive to legitimate requests. Fortunately, software security systems have been developed that can identify denial-of-service attacks and block their transmissions.

As computing and networking are shifting from the static model of the wired Internet toward the new and exciting "anytime-anywhere" service model of the mobile Internet, wireless systems will become increasingly programmable, interfacing with converged devices, and supporting new mobile applications. One serious class of threats that will affect the successful deployment of mobile wireless technologies is spoofing attacks. Spoofing attacks can be launched with little effort. The reason stems from the shared nature of the wireless medium, where adversaries can perform passive monitoring of useful identity information and then masquerade as another device using the collected identity. Finally, spoofing can be done by faking an identity, such as an online username.

II.RELATED WORK

Recently, there has been much active research addressing spoofing attacks as well as those facilitated by adversaries masquerading as another wireless device.We cannot cover the entire body of works in this section. Rather, we give a short overview of traditional approaches and several new methods. We then describe the works most closely related to our work.
Recently, new approaches utilizing physical properties associated with wireless transmission to combat attacks in wireless networks have been proposed. Based on the fact that wireless channel response decorrelates quite rapidly in space, a channel-based authentication scheme was proposed to discriminate between transmitters at different locations, and thus to detect spoofing attacks in wireless networks focused on building fingerprints of 802.11bWLAN NICs by extracting radiometric signatures, such as frequency magnitude, phase errors, and I/Q origin offset, to defend against identity attacks. However, there is additional overhead associated with wireless channel response and radiometric signature extraction in wireless networks. The MAC sequence number has also been used to perform spoofing detection. Both the sequence number and the traffic pattern can be manipulated by an adversary as long as the adversary learns the traffic pattern under normal conditions. However, none of these approaches are capable of determining the number of attackers when there are multiple adversaries collaborating to use the same identity to launch malicious attacks. Further, they do not have the ability to localize the positions of the adversaries after attack detection.

Turning to studying localization techniques, in spite of its several meter-level accuracy, using RSS is an attractive approach because it can reuse the existing wireless infrastructure and is highly correlated with physical locations. Dealing with ranging methodology, range-based algorithms involve distance estimation to landmarks using the measurement of various physical properties such as RSS, Time of Arrival (TOA), Time Difference of Arrival (TDOA), and direction of arrival (DoA). Our work differs from the previous study in that we use the spatial information to assist in attack detection instead of relying on cryptographic-based approaches. Furthermore, our work is novel because none of the exiting work can determine the number of attackers when there are multiple adversaries masquerading as the same identity. Additionally, our approach can accurately localize multiple adversaries even when the attackers varying their transmission power levels to trick the system of their true locations.

III.PROPOSED SYSTEM

The block diagram of the proposed system is illustrated in Figure 1. The proposed system deals with wireless spoofing attacks, which causes significant impact in the performance of the network. The proposed model is more similar to the existing model, which in performs detection, determine, localize. In addition to the existing system this system, which eliminate the spoofing attacks. However the existing system is also performing to eliminate the spoofing attacks. The existing system does not provide the clear information about the hardware. They have only mentioned as a physical property which is hard to falsify.

The main aim of this proposed system is to detect and prevent unauthorized access of wireless data from spoofed using Zigbee technology. The CC2431 which is Zigbee transceiver, the CC2431 is a true System-On-Chip (SOC) for wireless sensor networking Zigbee IEEE 802.15.4 solutions. This Zig bee transceiver is performed on the Zigbee protocol stack. This system uses the spatial correlation of RSS inherited wireless nodes to detect the spoofing attacks. However the simulation process of proposed system is shown in the network simulator.

The proposed system which uses three nodes, one is specified as the master device which is connected to the personal computer. The other two nodes one is the authorized device which has the proper MAC address; the other one is the unauthorized device which has improper MAC address. The master node identifies the Mac address of slave nodes. The simulation of this process is done in network simulator using nine nodes.

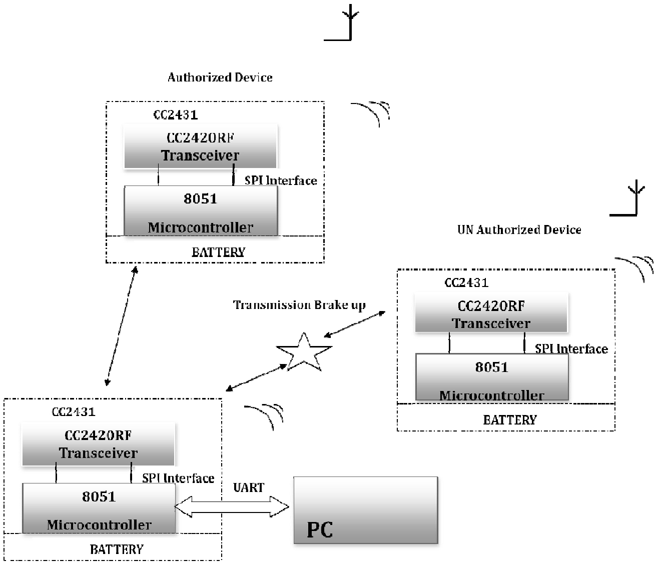

Figure 1. Block Diagram of Proposed System

IV.SYSTEM DESIGN IN NS-2

The system module which consists of Node creation, Gathering information about the nodes, Identifying the Mac Address, Data Transmission , Identifying the Hacker node.

A NODE CREATION

In NS-2, the network is constructed using nodes which are connected using links. Events are scheduled to pass between nodes through the links. Nodes and links can have various properties associated with them. Agents can be associated with nodes and they are responsible for generating different packets (e.g. TCP agent or UDP agent).

B. GATHERING INORMATION ABOUT NODES

When we have created the nodes, in this module we have to select the source and destination node from the regions, then we have ready for transmission the message to destination. When we ready to transmit message click transmit button, then it carefully selecting node for gather the information about each and every node of each region like neighbourhood of source node and who have highest energy in the neighbourhood, etc. Gathering information is to collect the information about very slave node, information are collected by the master node.

C. IDENTIFYING THE MAC ADDRESS

A media access control address (MAC address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as network address for most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sub layer of the OSI reference model. MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address (BIA). It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address.

A network node may have multiple NICs and each must have one unique MAC address per NIC.MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48, EUI-48, and EUI-64. The IEEE claims trademarks on the names EUI-48 and EUI-64, in which EUI is an abbreviation for Extended Unique Identifier. MAC address is collected from the source nodes and which is stored in the master node.

D. DATA TRANSMISSION

The Data transmission is done between the two nodes whether the transmission can be between the slave nodes to slave node or it can be fro master node to slave node. In this module the data transmission is happened between the two nodes node D and node E. The MAC address is identified by master node and it has all the information about the source nodes. The master node is represented as GOD in this module which knows about the transmission of the source nodes. Once the master identifies the proper Mac address of the source then it allows for the proper transmission.

E. IDENTIFYING THE HACKER NODE

In this module the hacker node is identified by the master node. The master node finds the MAC address requested by the hacker node is improper. In this module the hacker node is represented as node H. During the data transmission between the node D and node E the node H which finds the transmission and ready to attempt the spoofing. Once the master node identifies the hacker it gives the information to the slave nodes that the hacker is present in between the transmission path, this alerts the source nodes and to change the transmission path. This in turn moves on one the source node from current path to any other path. When the current path is changed the hacker cannot able to identify the changed path. So this enables the secure transmission.

V.CONCLUSION AND FUTURE WORK

We have proposed the system to detect and prevent the spoofing attacks in wireless communication. The simulation of this proposed system, which we have created nine nodes which indicates one master node and other slave nodes. The master node collects the information about the slave nodes including the MAC address of each slave node. The master node identifies the hacker node with improper MAC address. Overall the simulation which shows how the hacker node is identified and the secure data transmission is obtained. This system also gives the intimation about the hacker who is present in transmission path and provides the information to the nodes to change its transmission path. The advantage of this system is to provide the secure data transmission in the wireless system.

The simulation of this proposed system is simulated with nine nodes this can be implemented in hardware using Zigbee transceiver in each node as a future work. The Zigbee transceiver is associated with the Zigbee protocol stack, where it contains the necessary information regarding the transceiver. In this project we are going to implement with 3 nodes to detect the spoofing attacks. The nodes can also be added in case it is needed. Thus to prevent the spoofing attacks in secured areas this project can be implemented.

REFERENCES

1. Y. Chen, W. Trappe, and R.P. Martin, “Detecting and Localizing Wireless Spoofing Attacks,” Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), May 2007.
2. Y. Chen, W. Trappe, and R. Martin, “Attack Detection in Wireless Localization,” Proc. IEEE INFOCOM, Apr. 2007.
3. J. Yang, Y. Chen, and W. Trappe, “Detecting Spoofing Attacks in Mobile Wireless Environments,” Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), 2009.
4. Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, “Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength,” Proc. IEEE INFOCOM, Apr. 2008.
5. J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” Proc. USENIX Security Symp., pp. 15-28, 2003.
6. F. Ferreri, M. Bernaschi, and L. Valcamonici, “Access Points Vulnerabilities to Dos Attacks in 802.11 Networks,” Proc. IEEE Wireless Comm. and Networking Conf., 2004.