Detecting Spoofing Attacks in Wireless Network

Sudha Khusboo Surin¹, Preetha Mary Ann², D. Sarvanan³

¹Final Year MCA. Sathyabama University, Chennai, India
²&³Assistant Professor, Sathyabama University, Chennai, India.

ABSTRACT

Due to the openness of the wireless transmission medium, it is easy to launch spoofing attack and can significantly reduce the performance of networks. Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance. This paper proposes a mechanism for detecting and preventing these harmful attacks. This mechanism is based on physical data which include IP address, MAC address and signal strength values reported by access point to detect spoofing attack. The physical data are correlated with the physical location of a node. Assuming that the attacker and the genuine stations are separated by a distance, the physical data can differentiate them and help us to detect spoofing attack. This mechanism would require very less deployment cost since it uses physical data, a property associated with each node and does not require any additional tools.

Keywords: Spoofing attack, IP address, MAC address, Signal strength, wireless network.

1. INTRODUCTION

Today Internet plays a very vital role in our everyday life. Therefore using wireless network is very common. This paper explores the mechanism for defending against spoofing attack. It has become one of the major threats to the operation of internet today. Among various types of attacks, identity-based spoofing attacks are very easy to launch and can cause significant damage to network performance. Two devices in a network using same identity are treated as a single client, even if they generate conflict or inconsistent request. Spoofing attack is when a malicious party impersonates another device or user to launch attacks against network host, steal data or spread malware. Therefore for a secure transaction over a network it is important to detect spoofing attack and prevent the attackers.

This paper propose to use physical data which includes IP Address, MAC address and signal strength values reported by access point to detect spoofing attack. This physical data is correlated with the physical location of a node allowing detection of large number of attackers. Any information transmitted over the network link contains IP address, MAC address and signal strength sensed by access points within range. A table is constructed by aggregating all details reported transmitted at different locations produced distinct values with distance, which allows the server to distinguish genuine client located geographically apart.

2. PROBLEM DEFINITION

2.1 Existing System

The basic approach for detecting spoofing attacks uses cryptographic schemes. Cryptographic-based authentication has introduced a secure and efficient key management (SEKM) framework. Recently many techniques have been proposed by various researchers based on radiometric signature and forge-resistant relationship. However, these techniques increase over head as it requires reliable key management and maintenance. Therefore, it may not be always applicable as it has high cost and provides less security.

2.2 Proposed System

The proposed work introduces physical data which is associated with each node in the network for detecting the presence of spoofing attack. This data is not reliant on cryptography and is very hard to falsify. This physical data includes MAC address, IP address and signal strength value, which is sent by the user to the server with the request. If the server finds that two nodes having same id but different physical data then it means that there occurs spoofing attack. The MAC address may be forged but signal strength cannot be forged assuring the determination of spoofing attack in worst conditions also.

Figure 1 Proposed System Architecture
3. EXPERIMENTAL SETUP

3.1 Attack Model
Assume that the malicious users are provided with wireless network and have the information about each outgoing request sent over the network. This allows them to launch attacks against network host, steal data or spread malware. In terms of their physical location, assume that the attackers can move freely around the area covered by wireless network.

3.2 Attack Detection
In this section physical data that are strongly correlated with the physical location of a node allows the detection of large number of attackers. For each data sent to the server the IP address, MAC address and signal strength is extracted and analyzed. If the server finds same node ID but different physical data then it means spoofing attack has taken place. An added advantage of employing this technique to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves.

Procedure 1: (SENDREQUEST) is executed when any information is transmitted over the network link, contains its own MAC address, IP address and signal strength, which is specific for each node in the network.

Procedure 2: (RECVREQUEST) is executed when server is ready to receive data. A table is constructed by aggregating all the details transmitted at different locations produced by distinct signal. To determine the occurrence of attack we observed data. If there exists any request send by same node identity but different physical data, as a result we can identify that an attack has been launched since, under a spoofing attack, there is more than one node at different physical locations claiming the same node identity.

 Procedure 2: (RECVREQUEST)
Creating Table
For each received data
Find initial SS value SSi
Create table
ID[n] = NodeID
IP[n] = IPAddress
MAC[n] = MACAddress
SS[n] = SIG
End For
Detecting Spoofing Attack
If ID == CurID && MAC == CurMAC
Ds = SS[0] – SS[1]
If SSi > Ds
Spoofing attack has taken place
Else if ID == CurID && IP == CurIP
Ds = SS[0] – SS[1]
If SSi > Ds || MAC != CurMAC
Spoofing attack has taken place
Endif
Endif
Endif
Else
No Spoofing Attack
Endif

Procedure 3: (SENDRESPONSE) is executed when spoofing detection is done and attacker is identified. The server sends the response to the genuine user by using MAC address of the genuine user.

4. EXPERIMENTAL RESULTS
The experiment performed by this work gives the following results: the normal user sends the requests to the server including physical data and the server provider identifies the occurrence of spoofing attack by using physical data, the malicious node is avoided and the response is transmitted to the genuine user.
5. CONCLUSION AND FUTURE WORK
This work proposed the use physical property associated with each wireless device for detecting spoofing attacks in networks. It provided the mechanism to identify spoofing attack using same identity in the network. This approach can be also used to determine the number of attackers using same node identity.
The future work is to detect anonymous nodes that enter any anonymous node to communicate in the network.

References


