International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
*ISSN (Online)*2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP445-449

IP Spoofing and Stepping Stone Attacks in Wireless Networks: Detection, Localization and Prevention

Ashwini Kokate[1], Sneha Bhalerao[2], Sapana Dikonda[3], Kajol Ingawale[4], R. T. Umbare[5]
[1 2 3 4 5]*(Computer, JSPMs Rajarshi Shahu College of Engineering, India)*

Abstract :- Wireless network are openness in nature and it is easy for spoofing attacker to launch wireless spoofing attackers which causes threat for data security and impact performance of network. In traditional security cryptographic authentication is used to verify the nodes which are not desirable because of network overhead requirement. In this paper we use physical property associated with each node for special information, as it does not depend on cryptography and hard to falsify. This physical property can be used for detection of spoofing attackers which are present in the network for determining the number of attacker when multiple adversaries masquerade as the same node identity as that of other node and localizing adversaries. Then the multiclass detection problem is formulated for determining number of attackers. Cluster-based mechanisms are developed to determine the number of attackers. Support Vector Machines (SVM) method is used to further improve the accuracy of determining the number of attackers when training data is made available. In addition to integrated detection and localization system is used to localize the positions of multiple attackers.

Keywords: -Attack Detection, Localization, Spoofing Attack, Wireless network security.

I. INTRODUCTION

In wireless network it is very difficult to identify multiple spoofing attacks because wireless network has openness in nature and each and every node have their own node identity which is very essential to recognize and differentiate one node from other node. As wireless and sensor networks are deployed more, they will become tempting targets for malicious attacks.

As the openness of sensor and wireless networks, which are especially vulnerable to spoofing attacks in which an attacker forges its identity to masquerade as another device or creates multiple fake user. Spoofing attacks are a serious threat as they represent a form of identity compromise and variety of traffic injection attacks can be facilitated, such as evil twin access point attacks. It is very easy for an attacker to purchase a low price wireless device and can use these platforms to launch various type of wireless spoofing attack which are commonly available.

There are different types of attacks which can be performed by attackers, among this attacks identity-based attacks are easy to launch and cause significant damage to network performance. Therefore, to determine number of attackers, it is important to detect the presence of spoofing attackers and to localize multiple adversaries and eliminate them. The traditional approach is to address spoofing attacks using cryptographic authentication. Authentication requires additional infrastructural overhead and computational poor associated with cryptographic keys for maintaining and distributing. Due to the limited, poor resources available to the wireless devices and sensor nodes which is not always possible to deploy authentication, key management often incurs significant human management costs on the network. In this paper, we take a different approach by using the physical properties associated with wireless transmissions to detect spoofing.

Specifically, we propose a scheme for both detecting spoofing attacks, as well as the adversaries performing the attacks localizing their positions. Our approach utilizes the Received Signal Strength (RSS) and a physical property associate with each wireless node that is hard to falsify and cryptography as the basis for detecting spoofing attacks

thus not reliant. Using spatial information to address spoofing attackers has the unique power to not only identify the presence of these attackers but also localize adversaries.

It does not require additional cost or modification to wireless device to identify spoofing attacks. In this we proposed to use a general attack detection module (GADE) that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis and an integrated detection and localization system (IDOL) which can detect both attacker as well as position of multiple attacker even when the attacker vary their power level.

II. SCOPE

The scope of this paper is determining the number of attacks when multiple adversaries masquerading as the same node identity, detecting spoofing attacks and localizing multiple adversaries in network. Intruder if comes during transaction, then the server will discover and localize that particular system. So that the data transmitted by the sender can be receive only by authenticated receiver not by the attacker who masquerades as the same identity of original node and to eliminate the attack to make data transmission secure.

III. EXISTING SYSTEM

In the existing system cryptographic scheme is used for node identification, as number of nodes increase in an wireless network it is very difficult to provide security to each and every nodes because it require reliable key distribution, management, and maintenance mechanism. It is not always desirable to apply these cryptographic methods because of its management, computational and infrastructural overhead. Further, cryptographic methods are susceptible to node compromise. This is a serious concern as most wireless nodes are accessible, allowing their memory to be easily scanned. In a wireless network such as 802.11 networks attacker can easily attack to gather useful MAC address information during passive monitoring and then modifying its MAC address by simply issuing an*" ifconfig "*command to masquerade as another device [3].

IV. ATTACKERS IN EXISTING SYSTEM

4.1 Resource Depletion Attacks

This is essentially a DOS attack. The attacker sends unnecessary requests in large amount to flood the network, which consumes large amount of computational power, network bandwidth and memory.

The attacker goes one step ahead and attempts to mask its identity by spoofing its MAC or IP address. Therefore, mechanisms based on IP or MAC addresses for security will fail to identify the DOS attack. As signal prints cannot be spoofed easily, to detect such attack a mechanism based on signal prints is used [3].

4.2 Masquerade Attacks

In a masquerade attack, the attacker poses as a valid member node. Many techniques involve spoofing IP or MAC address, so as to acquire the privileges of another member node which is valid. This will allow the attacker to enter and access a network to which person is unauthorized. Identity-based security mechanisms that use IP or MAC address – or any information that the sender sends as a part of data – cannot detect such security violations. However, owing to the properties of signal prints, it is very difficult for the attacker to defeat a security mechanism based on signal prints.

V. PROPOSED SYSTEM

In the proposed system we proposed to use a generalized attack detection model (GADE) that can both detect spoofing attacks as well as determine the number of adversaries using cluster analysis methods grounded on RSS-based spatial correlations among normal devices and adversaries; and an integrated detection and localization system (IDOL) that can both detect attacks as well as find the positions of multiple adversaries even when the transmission power levels are varied by adversaries. In GADE, the Partitioning around Medoids (PAM) cluster analysis method is used to perform attack detection. Later we formulate the problem of determining the number of

attackers as a multiclass detection problem and then we applied cluster-based methods to determine the number of attacker [2].

To improve the accuracy of determining the number of attackers a mechanism known as SILENCE is used. The use of Support Vector Machines (SVM) method is used to further improve the accuracy of determining the number of attackers, when training data available. We developed IDOL, an integrated system, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries.

By this method it is possible to determining the number of attackers when multiple adversaries masquerading as the same node identity, detecting spoofing attacks and localizing multiple adversaries without causing overhead in wireless network.

Detection mechanisms are effective highly in both detecting attacks with detection rate 98 percent and determining number of adversaries; by achieving 90 percent precision and hit rates simultaneously using SILENCE and SVM based mechanism. By analysing RSS readings from each MAC address using the algorithm K-means Cluster Algorithm. It is found that the distance between the centroids in the signal space can be used as a good test statistics for detecting effectively, and then it also describes how to combine K-means spoofing detectors inside a real time indoor localization system. A general approach named K-means approachin which almost all RSS-based localization algorithms are used [2].

Fig.1.Proposed system architecture

Modules Used:

- Identification Module
  Identification of IP and MAC address is done using RSS readings. The calculation of RSS is based on accuracy, time and power.
- Detection Module
  Multiple users with same node identity are detected.
- Localization Module
  Physical location in x, y coordinates of attacker detected in previous module is located.
- Prevention Module
  The user profile is blocked, for further uploading the machine can also be blocked.

5.1.Detection

1. In this Module, system A, which forms a cluster, is divided into k-disjoints is no. of partions.
2. Centriod is calculated.
3. To calculate RSS values, consider three attributes.

- Packet delivery ratio (PDR):

$$\text{PDR} = \frac{\sum \text{Received packets at destinations}}{\sum \text{Sent packets by sources}} \quad (1)$$

- Routing Overhead (RoH):

$$\text{RoH} = \frac{\sum \text{Routing transmissions}}{\sum \text{Data trasmission} + \sum \text{Routing transmission}} \quad (2)$$

- Average end-to-end delay (AED)

$$\text{AED} = \frac{\sum_1^N (\text{T}_{Received} - \text{T}_{Sent})}{\text{N}} \quad (3)$$

The RSS readings are distinctive at different physical space location. One node claiming the same MAC address at different physical location is detected as Spoofing attack.
K-means cluster analysis is used to identify spoofing attack [1].

5.2 Localization

RSS obtained is forwarded and given to server. Server collects information then spoofing detection is performed. Using RADAR-gridded algorithm localization is done using solver. There can be many solvers are available which can detect multiple transmitters simultaneously. Radio map is plotted against known location. Localization is performed by measuring transmitters RSS at each landmark then compared to radio map and attackers will is localized.

VI. SURVEY ON EXISTING SYSTEM

Wireless networks are vulnerable to many identity-based attacks in which a malicious device uses forged MAC addresses to masquerade as a septic client or to create illegitimate multiple identities. For example, several link-layer services which are in IEEE 802.11 networks have been shown to be vulnerable to such attacks even if 802.11i/1X and other security mechanisms are deployed [1].We can show that a transmitting device can be robustly indentured by its signal print, topple of signal strength values reported by access points acting as sensors. We show that, deferent from other packet contents or MAC address, attackers do not have as much control regarding the signal prints they produce.

VII. CONCLUSION

Theoretical analysis for attack detection by using the spatial correlation of RSS inherited from wireless nodes is used.Based on the cluster analysis of RSS readings the test statistics can be derived. Our approach can detect the presence of attacks as well as spoofing the same node identity, determine the number of adversaries so that we can localize any number of attackers and remove them.Challengingproblem is to determining the number of adversaries. SILENCE mechanism to cluster analysis is used for determining the number of attackers to achieve better accuracy. Advantage of GADE and IDOL algorithm is GADE can detect both number of adversaries using cluster analysis and spoofing attacks. GADE cannot detect attacks at low transmission levels this drawback is overcome by IDOL can detect attacks and find position of multiple attackers even when transmission power is low.
Additionally, when the training data is made available, it is explored using Support Vector Machines (SVM) based mechanism to further improve the accuracy of determining the number of attackers which are present in the system. The approach can detect multiple wireless Spoofing attacks and can also, determining the number of attackers and localizing adversaries. Can be used is Cyber Cell Security.

REFERENCES

[1] Jie Yang, Student Member, IEEE, Yingying (Jennifer) Chen, Senior Member, IEEE, Wade Trappe, Member, IEEE and Jerry Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks", *IEEE Transaction on Parallel and Distributed System, Vol. 24, No. 1, January 2013.*

[2] 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.*

[3]Yong Sheng3, keren Tan1, Guanling Chen2 David Kotz1, Andrew Campbell Institute for Security Technology Studies, Dartmouth College; 2 Department of Computer Science, University of Massachusetts Lowell; 3Google, Inc. (at Dartmouth ISTS during this work), "Detecting 802.11 MAC Layer Spoofing using Received Signal Strength", IEEE *INFOCOM 2008.*