ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

RSS and Spatial Correlation Based Approach to Detect and Localize Spoofing Attackers in Wireless Networks

P.Naveen Sundar Kumar, V.B.Sekhar

Department of CSE, RGMCET, Nandyal, India

Abstract--Wireless networks are vulnerable to attacks due to shared medium and mobility besides resource constrained nature. Spoofing attacks are one kind of attacks that can be launched easily on wireless networks. Cryptography can be used to overcome this problem. However, conventional security approaches cannot be directly used with wireless networks as they cause overhead. Without depending on cryptography, recently Yang et al. proposed a method that uses spatial information to detect spoofing attacks, find number of attackers involved in the attacks and also localizing the adversaries. Spatial correlation of received signal strength is used in order to achieve this. SVM and cluster based mechanism are used to know number of attackers and improve accuracy of detection. In this paper we build a prototype network application that simulates the wireless networks. It is used to demonstrate the detection and localization of spoofing attackers. The empirical results reveal that the proposed application is capable of detecting attacks besides localizing attackers.

Index Terms – Wireless networks, spoofing attacks, localization, and attack detection

I. INTRODUCTION

Wireless networks are widely used in the real world as they provide simple and easy solutions to communications. However, they are vulnerable to various kinds of attacks due to the open medium and mobility. Adversaries can launch attacks on such networks using low cost devices with less effort. Among the attacks launched by them, identity based attacks are easier to launch and such attacks cause problems to wireless networks. Masquerade with another device is possible with MAC address change in 802.11 networks. The protocols like WEP, WPA and WPA 2 are used to protect wireless networks. The security methodologies of these protocols also cause problems and they are vulnerable to spoofing attacks. Other attacks possible include traffic injection attacks DoS attacks and rogue access point attacks. In this context, it is essential to have mechanisms to detect the spoofing attacks, find out the number of attackers involved and localize those attackers or adversaries and get rid of them. Traditionally cryptographic schemes were used to secure communications in networks. However, they cause heavy overhead on the network. Key distribution mechanisms are costly and the security mechanisms used for conventional networks do not work directly with wireless networks. For this reason it is important to understand the feasibility of traditional cryptographic solutions with respect to their computational and infrastructural overhead. Node compromises another serious problem with cryptographic methods. To overcome these issues, Yang et al. [1] proposed a solution based on the received signal strength and spatial correlation. When a physical property which is associated with each node is used for security, it is not easy to falsify it. This approach does not depend on cryptographic primitives. With respect to spoofing attacks, it is essential that identifying the number of attacks and their location. In this paper we design and implement a network application that simulates wireless nodes that have communication among them. We also demonstrate spoofing attacks launched and their prevention mechanisms without using cryptographic primitives. Received signal strength is used in order to find the attacks, know the number of attackers involved and the location of all the adversaries. The remainder of the paper is structured as follows. Section II provides review of literature on prior works. Section III provides the proposed approach towards handling spoofing attacks. Section IV presents prototype application and experimental results while section V concludes the paper.

II. RELATED WORKS

Security has been a major concern in all wireless networks. The traditional cryptographic solutions [2], [3], [4] were not able to solve security problems in wireless networks as they cause overhead. A framework was introduced in [4] named SEKM with public key infrastructure. In [3] a key management scheme was implemented in which key is refreshed periodically to protect communication network. In [2] a hierarchical network is used for experiments and an authentication framework was proposed for security. Recently some approaches came into existence that focused on the physical properties of the underlying networks. One such work is in [5] which take care of spoofing attacks in wireless networks.

Later on in [6] biometrics such as fingerprints is used for protecting WLAN. In [7] a forge resistant solution was given to detect spoofing attacks. In [8] MAC sequence number is used in order to perform spoofing detection. However, traffic pattern approaches and sequence numbers can be manipulated by adversaries.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

The work which is close to the work of this paper includes the works based on RSS for detecting spoofing attacks [9], [10], [11]. Matching rules concept was used in [11] while Gaussian mixture model for RSS was used in [10]. Spatial signature concept was introduced in [14]. With respect to localization, RSS has been performing well and many researches came into existence [12], [13], and [14]. The Time of Arrival concept is used in [15]. Matching strategies are used in [14] with pre-defined values in order to detect spoofing attack. Direction of arrival concept is used in [16] along with received signal strength to detect spoofing attack. Localization of adversaries was explored in [17]. In this paper we focused on RSS and other techniques for detecting and localization of spoofing attackers.

III. PROPOSED SOLUTION

In this section we describe our approach in solving the problem of detection and localization of multiple spoofing attacks. Received signal strength is widely used for finding or estimating the location of a node from which signals are received. Based on the signal strength it is achieved. However, it might not be as accurate as expected. To overcome this problem in [1] RSS is used along with spatial correlation. The RSS readings provide details about spatial correlations. This will help in finding exact location of the mobile device. The detection and localization of spooling attackers is achieved using RSS and its spatial correlations. More details about the solution can be found in [1]. In this paper we built a prototype application that demonstrates the concept of detection and localization of multiple spoofing attackers.

The application was built using Java platform. The nodes are built as graphical programs that simulate the functionality of wireless nodes. The application runs in networking environment. The application is basically a network application where multiple wireless nodes can run and there are common communication scenarios among the nodes. However, we built an attack model as well to demonstrate the detection and localization of multiple spoofing attackers. With attack model, the application is able to demonstrate the proof of concept.

IV. EXPERIMENTAL RESULTS

The environment used for experiments is multiple PCs with 2 GB RAM and core 2 dual processor running in a network. In each PC a graphical program runs which simulates as a wireless node. The nodes running different machines can communicate with each other. The general communication characteristics are provided in the network application besides the simulation of attack model. The application supports the selection of number of nodes in the network and generates the nodes as follows besides having a graphical program for each node.

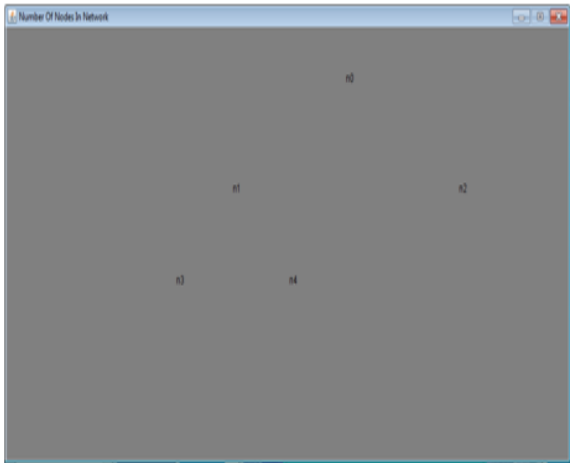

Figure 1 – Simulation of wireless nodes

As can be seen in Figure 1, it is evident that the selected number of nodes is created. However, each node has its graphical window as well that simulates the node functionality. Afterwards, it is possible to calculate Euclidian distance as shown in Figure 2.

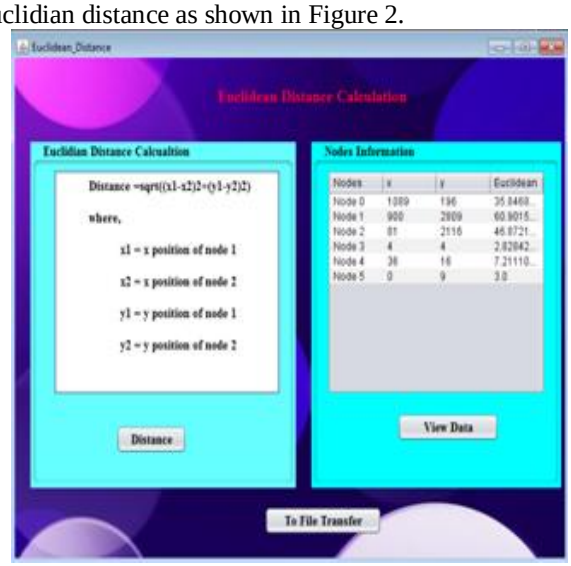

Figure 2 – Euclidian distance calculation

As can be seen in Figure 2, it is evident that the Euclidian distance is computed and the nodes information is presented.

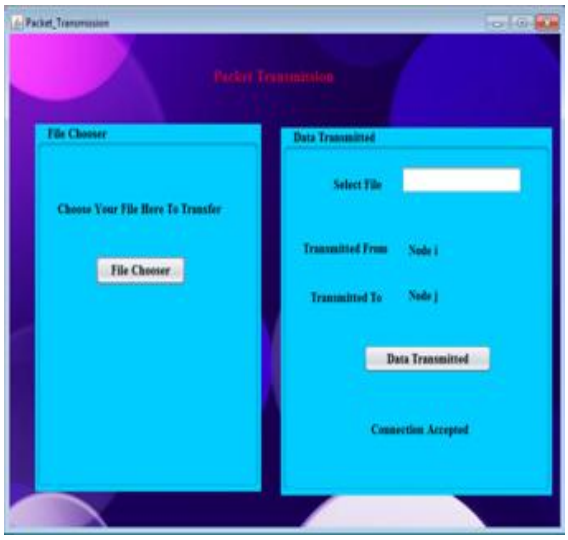

Figure 3 – Packet transmission

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

As can be seen in Figure 3, the packet transmission process in the normal scenario is demonstrated.

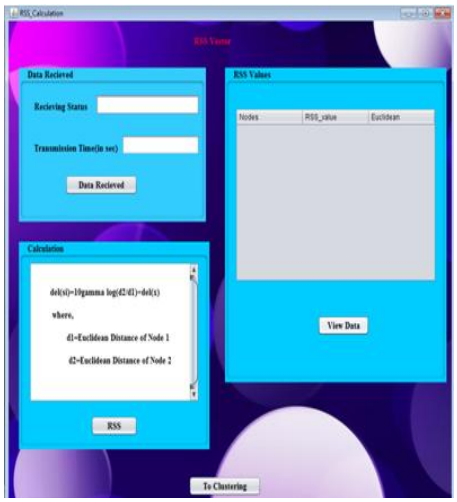

Figure 4 – RSS vector

As seen in Figure 4, RSS vector is generated and it is used for computing the required values in order to perform detection and localization of attackers.

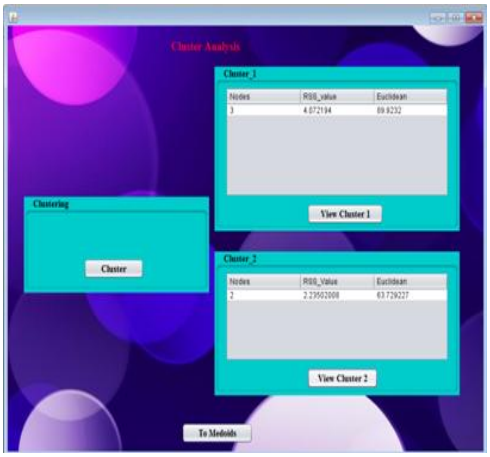

Figure 5 – Cluster analysis

As can be seen in Figure 5, the cluster analysis is made for understanding the nodes, their positions and the cluster to which they belong. These cluster dynamics are further used later for detection and localization.

Figure 6 – Spoofing attack detection

As can be seen in Figure 6, the application is able to demonstrates multiple spoofing attacks and able to detect spoofing attacks.

Figure 7 - Finding number of attackers

As can be seen in Figure 7, the application is able to detect the number of attackers. The attackers and other details are computed.

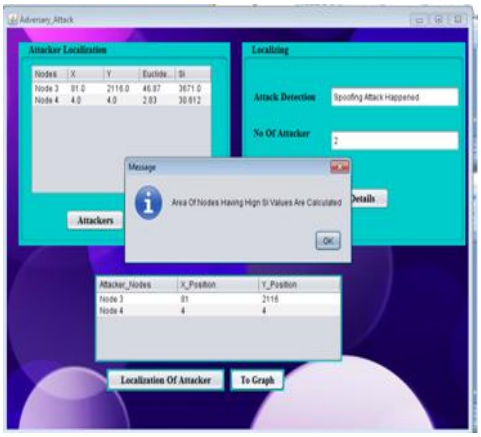

Figure 8 – Attacker localization

As can be seen in Figure 8, the attackers are localized. The number of attackers involved in spoofing attack and their location is found.

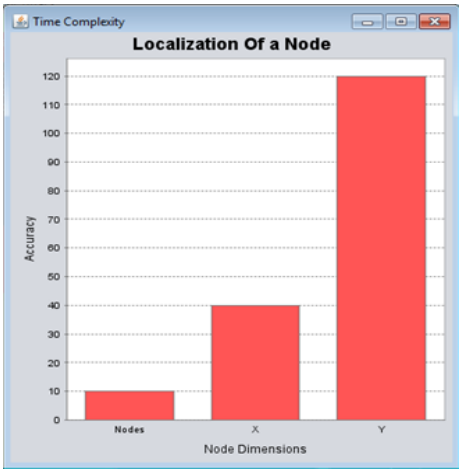

Figure 9 – Node localization dynamics

As can be seen in Figure 9, it is evident that the node localization dynamics are visualized. The horizontal axis takes nodes, x and y dimensions while the vertical access presents accuracy.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

V. CONCLUSION AND FUTURE WORK

In this paper, we studied the problem of detection and localization of multiple spoofing attackers in wireless networks. It is a challenging problem to detect and localize multiple spoofing attackers. Recently Yang et al. [1] proposed a solution for this. They used received signal strength along with spatial correlation and physical property of mobile device. This approach is hard to falsify. They provided theoretical analysis and also simulated analysis to prove the solution. Their solution is able to protect wireless networks from spoofing attacks. It detects multiple spoofing attackers and localizes them. In this paper we built a networking application, a prototype that demonstrates the concept of detection and localization of multiple spoofing attackers. The application was built using Java programming language with SWING and networking API in order to demonstrate the proof of concept. The experimental results reveal that the application is useful to understand how detection and localization of multiple spoofing attackers can be made. In our future work, we intend to implement such solution in real networks

REFERENCES

[1] Jie Yang, Yingying (Jennifer) Chen, Senior Member, IEEE, Wade Trappe and Jerry Cheng. (2013). Detection and Localization of Multiple Spoofing Attackers in Wireless Networks. *IEEE*. 24 (1), p44-58.
[2] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79-87, 2003.
[3] 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. 677-686, 2005.
[4] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and Efficient Key Management in Mobile Ad Hoc Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS), 2005.
[5] L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the Physical Layer for Wireless Authentication," Proc. IEEE Int'l Conf. Comm. (ICC), pp. 4646-4651,June 2007.
[6] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless Device Identification with Radiometric Signatures," Proc. 14th ACM Int'l Conf. Mobile Computing and Networking, pp. 116-127, 2008.
[7] Q. Li and W. Trappe, "Relationship-Based Detection of Spoofing Related Anomalous Traffic in Ad Hoc Networks," Proc. Ann. IEEE Comm. Soc. on IEEE and Sensor and Ad Hoc Comm. and Networks (SECON), 2006.
[8] F. Guo and T. Chiueh, "Sequence Number-Based MAC Address Spoof Detection," Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection, pp. 309-329, 2006.
[9] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 21372145, 2008.
[10] 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.
[11] D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.
[12] Y. Chen, J. Francisco, W. Trappe, and R.P. Martin, "A Practical Approach to Landmark Deployment for Indoor Localization," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Sept. 2006.
[13] E. Elnahrawy, X. Li, and R.P. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," Proc. IEEE Int' Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.
[14] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RFBased User Location and Tracking System," Proc. IEEE INFOCOM, 2000.
[15] P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001.
[16] Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.
[17] Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc. IEEE INFOCOM, Apr. 2007.