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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

Support Vector Machine Based Determining Attackers and Localizing Adversaries in Wireless Networks

R.Sheela[1], R.Sudha[2]

PG Scholar-M.E, CSE, Gnanamani College of Engineering, Namakkal, T.N, India[1]

Assistant Professor, CSE, Gnanamani College of Engineering, Namakkal, T.N, India[2]

Abstract: Wireless spoofing attacks are easy to launch and can significantly impact the performance of networks. Although the identity of a node can be verified through cryptographic authentication, conventional security approaches are not always desirable because of their overhead requirements. The traditional approaches uses the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks and then formulate the problem of determining the number of attackers as a multiclass detection problem. Cluster-based mechanisms are developed to determine the number of attackers. In addition, they developed an integrated detection and localization system that can localize the positions of multiple attackers. The existing techniques are used to detect attackers but don't know how it attacks. In this paper, extend the RSS techniques to find out how attackers will attack by monitoring the attacker's activities.

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

I. INTRODUCTION

Among various types of attacks, identity-based spoofing attacks are especially easy to launch and can cause significant damage to network performance. For instance, in an 802.11 network, it is easy for an attacker to gather useful MAC address information during passive monitoring and then modify its MAC address by simply issuing an ifconfig command to masquerade as another device [2]. Spoofing attacks can further facilitate a variety of traffic injection attacks such as attacks on access control lists, rogue access point (AP) attacks, and eventually Denial of-Service (DoS) attacks. A broad survey of possible spoofing attacks can be found in. Moreover, in a large-scale network, multiple adversaries may masquerade as the same identity and collaborate to launch malicious attacks such as network resource utilization attack and denial-of-service attack quickly [1], [7].

Most existing approaches to address potential spoofing attacks employ cryptographic schemes. However, the application of cryptographic schemes requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply these cryptographic methods because of its infrastructural, computational, and management overhead. Further, cryptographic methods are susceptible to node compromise, which is a serious concern as most wireless nodes are easily accessible, allowing their memory to be easily scanned. In this work, we 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. Since we are concerned with attackers who have different locations than legitimate wireless nodes, utilizing spatial information to address spoofing attacks has the unique power to not only identify the presence of these attacks but also localize adversaries. An added advantage of employing spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves [5].

In generalized attack detection model (GADE), the Partitioning around Medoids (PAM) cluster analysis method is used to perform attack detection. We formulate the problem of determining the number of attackers as a multiclass detection problem. We then applied cluster-based methods to determine the number of attacker. We further developed a mechanism called SILENCE for testing Silhouette Plot and System Evolution with minimum distance of clusters, to improve the accuracy of determining the number of attackers. Additionally, when the training data are available, we propose to use the Support Vector [2].

Machines (SVM) method to further improve the accuracy of determining the number of attackers. Moreover, we developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries. As we demonstrated through our experiments using both an 802.11 network as well as an 802.15.4 network in two real office building environments, GADE is highly effective in spoofing detection with over 90 percent hit rate and precision.

Furthermore, using a set of representative localization algorithms, we show that IDOL can achieve similar localization accuracy when localizing adversaries to that of under normal conditions. One key observation is that IDOL can handle attackers using different transmission power levels, thereby providing strong evidence of the effectiveness of localizing adversaries when there are multiple attackers in the network [2], [6].

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

II. RELATED WORK

The traditional approach to prevent spoofing attacks is to use cryptographic-based authentication. They have introduced a secure and efficient key management (SEKM) framework. SEKM builds a Public Key Infrastructure (PKI) by applying a secret sharing scheme and an underlying multicast server group implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys [11]. An authentication framework for hierarchical, ad hoc sensor networks is proposed. However, the cryptographic authentication may not be always applicable because of the limited resources on wireless devices and lacking of a fixed key management infrastructure in the wireless network. 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. It focused on building fingerprints of 802.11b WLAN 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. It introduced a security layer that used forge resistant relationships based on the packet traffic, including MAC sequence number and traffic pattern, to detect spoofing attacks [15].

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. The works using RSS to defend against spoofing attacks are most closely related to us. We proposed to use the node's "spatial signature," including Received Signal Strength Indicator (RSSI) and Link Quality Indicator (LQI) to authenticate messages in wireless networks. 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). Whereas range-free algorithms [use coarser metrics to place bounds on candidate positions. The approaches to address potential spoofing attacks employ cryptographic schemes. However,

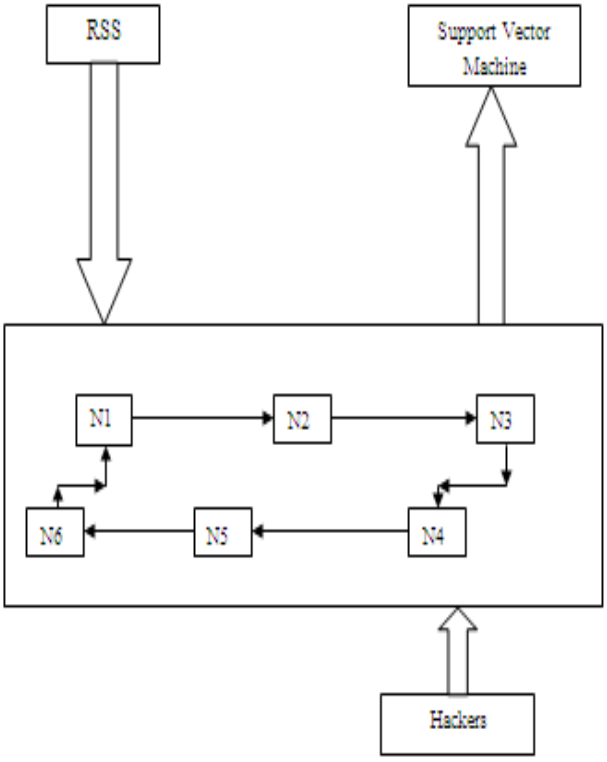

Fig.1 System Architecture

the application of cryptographic schemes requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply these cryptographic methods because of its infrastructural, computational, and management overhead [16].

III. PROPOSED METHOD

The approaches to address potential spoofing attacks employ cryptographic schemes. However, the application of cryptographic schemes requires reliable key distribution, management, and maintenance mechanisms. It is not always desirable to apply these cryptographic methods because of its infrastructural, computational, and management overhead. In proposed methods, we extend the RSS techniques to restrict the spoofing attacks as well as to find out how attackers will attack in wireless network and main reason of attack by monitoring the activities of each individual. By this method, we can automatically restrict spoofing attacks in wireless network.

A. Monitor for Received signal strength

The challenge in spoofing detection is to devise strategies that use the uniqueness of spatial information, but not using location directly as the attackers' positions are unknown. We propose to study RSS; a property closely correlated with location in physical space and is readily available in the existing wireless networks [4]. Although affected by random noise, environmental bias, and multipath effects, the RSS measured at a set of landmarks (i.e., reference points with known locations) is closely related to the transmitter's physical location and is governed by the distance to the landmarks. The RSS

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

readings at the same physical location are similar, whereas the RSS readings at different locations in physical space are distinctive. Thus, the RSS readings present strong spatial correlation characteristics. Turning to studying localization techniques, inspire 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. The works of RSS to defend against spoofing attacks are most closely related to us [10].

B. Detect the presence of spoofing attacks

The above analysis provides the theoretical support of using the RSS-based spatial correlation inherited from wireless nodes to perform spoofing attack detection. It also showed that the RSS readings from a wireless node may fluctuate and should cluster together. Recently, new approaches utilizing physical properties associated with wireless transmission to combat attacks in wireless networks have been proposed [4]. 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. In fig.2 a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage [8].

C. Determine the number of attackers

Different from traditional localization approaches, our integrated detection and localization system utilizes the RSS Medoids returned from SILENCE as inputs to localization algorithms to estimate the positions of adversaries. The return position from our system includes the location estimate of the original node and the attackers in the physical space. Determining the number of adversaries is a particularly challenging problem [12]. We developed SILENCE, a mechanism that employs the minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers than other methods under study, such as Silhouette Plot and System Evolution that use cluster analysis alone. Additionally, when the training data are available, we explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers present in the system [3].

D. Determine the number of attackers

Different from traditional localization approaches, our integrated detection and localization system utilizes the RSS Medoids returned from SILENCE as inputs to localization algorithms to estimate the positions of adversaries. The return position from our system includes the location estimate of the original node and the attackers in the physical space. Determining the number of adversaries is a particularly challenging problem [12]. We developed SILENCE, a mechanism that employs the

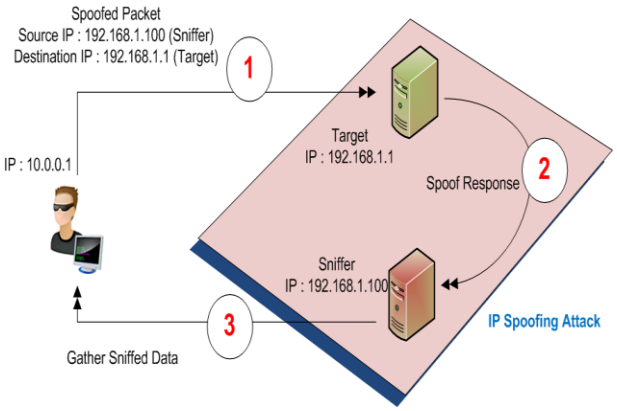

Fig.2 Spoofing attack

minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers than other methods under study, such as Silhouette Plot and System Evolution that use cluster analysis alone. Additionally, when the training data are available, we explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers present in the system [3].

E. Localize multiple adversaries

We developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries. By using a set of representative localization algorithms, we show that IDOL can achieve similar localization accuracy when localizing adversaries to that of under normal conditions. One key observation is that IDOL can handle attackers using different transmission power levels, thereby providing strong evidence of the effectiveness of localizing adversaries when there are multiple attackers in the network [9]. In fig.3 shows localization in wireless network connection.

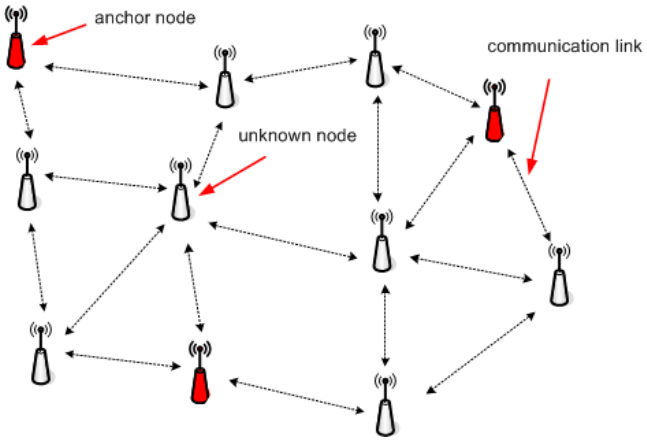

Fig.3 Localization in wireless network

F. Protection mechanism

Protection mechanisms are built into computer architecture to support the enforcement of security policies. A simple definition of a security policy is to set who may use what information in a computer system. We found that our detection mechanisms are highly effective

in both detecting the presence of attacks with detection rates over 98 percent and determining the number of adversaries, achieving over 90 percent hit rates and precision simultaneously when using SILENCE and SVM-based mechanism. Further, based on the number of attackers determined by our mechanisms, our integrated detection and localization system can localize any number of adversaries even when attackers using different transmission power levels. The performance of localizing adversaries achieves similar results as those under normal conditions, thereby, providing strong evidence of the effectiveness of our approach in detecting wireless spoofing attacks, determining the number of attackers and localizing adversaries [13], [14].

IV. CONCLUSION

We proposed to use received signal strength based spatial correlation, a physical property associated with each wireless device that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks in wireless networks. Provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. Derived the test statistic based on the cluster analysis of RSS readings. Approach can both detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that can localize any number of attackers and eliminate them [17]. Determining the number of adversaries is a particularly challenging problem. Developed SILENCE, a mechanism that employs the minimum distance testing in addition to cluster analysis to achieve better accuracy of determining the number of attackers than other methods under study, such as Silhouette Plot and System Evolution that use cluster analysis alone. Additionally, when the training data are available, explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers present in the system. Using extended RSS techniques to restrict the spoofing attacks as well as to find out how attackers will attack in wireless network and main reason of attack by monitoring the activities of each individual. By this method, it can automatically restrict spoofing attacks in wireless network.

REFERENCES

[1] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. USENIX Security Symp., pp. 15-28, 2003.

[2] 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.

[3] D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.

[4] 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.

[5] 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.

[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. 677-686, 2005.

[7] 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.

[8] 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.

[9] 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.

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

[11] 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.

[12] 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.

[13] L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2137-2145, 2008.

[14] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RFBased User Location and Tracking System," Proc. IEEE INFOCOM, 2000.

[15] E. Elnahrawy, X. Li, and R.P. Martin, "The Limits of Localization Using Signal Strength: A Comparative Study," Proc. IEEE Int'l Conf. Sensor and Ad Hoc Comm. and Networks (SECON), Oct. 2004.

[16] 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.

[17] J. Yang and Y. Chen, "A Theoretical Analysis of Wireless Localization Using RF-Based Fingerprint Matching," Proc. Fourth Int'l Workshop System Management Techniques, Processes, and Services (SMTPS), Apr. 2008.