ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

Detection and Localization of Multiple Spoofing Attackers Using Cluster Analysis in Wireless Network

[1]Deepak Bilolikar, [2]Shital Y Gaikwad

[1]M. E. (Second Year Student), Department of CSE, MPGI Institute of Engineering and Technology, Kupsurwadi, Nanded. (M.S.), India.

[2]Professor, Department of CSE, MPGI Institute of Engineering and Technology, Kupsurwadi, Nanded. (M.S.), India.

ABSTRACT: Wireless networks are vulnerable to spoofing attacks, which allows for many other forms of attacks on the networks. Although the authentication is not always possible because it requires key management and additional infrastructural overhead. In this paper describes method on detection and localization of multiple spoofing attackers in wireless networks. Author have spatial information a physical property of a node which have its no dependence on cryptography and hard to falsify for (1) detecting spoofing attacks; (2) determining the number of attackers when multiple adversaries masquerading as a same node identity; and (3) localizing multiple adversaries. Author propose to use Generalized Attack Detection Model (GADE) which has the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the presence of spoofing attacks. Using cluster-based mechanisms, developed to determine the number of attackers. When the training data is available, we explore using Support Vector Machines (SVM) method to improve the accuracy of determining the number of attackers. In addition, author developed an integrated detection and localization system that can localize the positions of multiple attackers. Author evaluated our techniques through two testbeds using both an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network in two real office buildings. Our experimental results show that our proposed methods can achieve over 90% Hit Rate and Precision when determining the number of attackers. Localization results using a representative set of algorithms provide strong evidence of high accuracy of localizing multiple adversaries.

KEYWORDS: Wireless network security, spoofing attack, attack detection, localization

1. INTRODUCTION

As computing and performing arts networks square measure shifting from wired infrastructure to the wireless, mobile and open communication networks, for increasing the speed of computation. However such networks square measure simply vulnerable for multiple and
style of opposer attacks like spoofing attacks. Essentially the identity based mostly spoofing attacks or masquerading attacks square measure simple to launch and additionally it will cause important injury to the network performance. Spoofing attacks additionally facilitate numerous sorts of traffic injection attacks, such as attacks on access management Lists (ACL), varlet access purpose (AP) attacks, and eventually Denial of- Service (DoS) attacks. The cryptographical techniques are wont to address such style of security violations. Therefore, it is necessary to

1) Detect the presence of spoofing attack
2) Determine the number of attackers
3) Localize multiple adversaries

Most existing approaches employ cryptographic schemes to address potential spoofing attacks [2], [1].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. This paper proposes to use RSS-based spatial correlation, a physical property associated with each wireless node that is hard

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Since the concern is on the 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.

Traditional approach to address spoofing attacks is to apply cryptographic authentication. Here cryptographic key requires maintains, distribution mechanism also authentication requires additional infrastructural overhead and computational power associated. Due to the limited power and resources available to the wireless devices, it is not always possible to deploy authentication. Also cryptographic methods are vulnerable to spoofing attacks as wireless nodes allow easy access to scan their memory In addition, key management often incurs significant human management costs on the network. Author takes 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 localizing the positions of the adversaries performing the attacks. Our approach utilizes the Received Signal Strength (RSS) measured across a set of access points to perform spoofing detection and localization. Our scheme does not add any overhead to the wireless devices. As we are dealing with attackers having different locations, spatial information helps in not only detecting spoofing attacks but also to localize the adversaries. [5] Shows spoofing attacks in mobile environments. Survey in [3][5][12] are closely related to our idea of detecting spoofing attacks.
[3]Deals with detecting spoofing attack using signal prints.[5]deals with using Gaussian mixture model and[12]deals with k-mean cluster analysis. however these methods would only detect spoofing attacks but could not handle nodes with different power levels.
Our focus is on methods

GADE: 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;
IDOL: an integrated detection and localization system that can both detect attacks as well as find the positions of multiple adversaries even when the adversaries vary their transmission power levels.
In 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. Author then applied cluster-based methods to determine the number of attacker.

Additionally, when the training data are available, Use the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. Finally, author developed an integrated system, IDOL, which utilizes the results of the number of attackers returned by GADE to further localize multiple adversaries. Furthermore, using a set of representative localization algorithms, 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. The scope of this paper is to detect spoofing attacks, determining the number of attackers when multiple adversaries masquerading as the same node identity and localizing multiple adversaries. The transmitted information from server is send to client in secure manner. If an intruder comes during transaction server discover and localize that specific system.

II. PROPOSED SYSTEM

The proposed framework utilizes Received Signal Strength (RSS)-based spatial connection, a physical (PAM) Method so as to perform clustering analysis in RSS. Property connected with every wireless node that is hard to falsify and not reliant on cryptography as the basis for detecting spoofing attacks. Since the concern is on the 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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

III. DESIGN OBJECTIVE AND RELATED WORK

Traditionally cryptographic authentication mechanism were used to detect spoofing attacks.[2][1][8] focus on the traditional approach of detecting spoofing attacks.

Wu etal. [2] 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. Wool [1] implemented a key management mechanism with periodic key refresh and host revocation to prevent the compromise of authentication keys. 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 decorelates 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 [7].Brik et al. [11] 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. Li and Trappe [10] 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. The MAC sequence number has also been used in [4] to perform spoofing detection. An adversary can manipulate both the sequence number and the traffic pattern as long as the adversary learns the traffic pattern under normal conditions. The works [3], [13], [6] using RSS to defend against spoofing attacks are most closely related to present work. Faria and Cheriton [3] proposed the use of matching rules of signalprints for spoofing detection. Sheng et al. [13] modeled the RSS readings using a Gaussian mixture model. Sang and Arora [6] 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, inspite of its several meter-level accuracy, using RSS [6], [9], 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 [6], [9], 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. Another method of classification describes the strategy used to map a node to a location. Lateration approaches use distances to landmarks, while angulation uses the angles from landmarks. Scene matching strategies [9] use a function that maps observed radio properties to locations on a pre-constructed signal map or database. Further, Chen proposed to perform detection of attacks on wireless localization and Yang proposed to use the direction of arrival and received signal strength of the signals to localize adversary's sensor nodes. In this work, we choose a group of algorithms employing RSS to perform the task of localizing multiple attackers and evaluate their performance in terms of localization accuracy. This work differs from the previous study in that here the spatial information is used to assist in attack detection instead of relying on cryptographic-based approaches. Furthermore, this 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, this approach can accurately localize multiple adversaries even when the attackers varying their transmission power levels to trick the system of their true locations.

IV. OVERVIEW OF TECHNIQUES

GADE (Generalized attack Detection Model):-

Here author used to propose RSS, a physical property closely correlated with location in physical space and also it is readily available in the existing wireless networks. As RSS can be affected due to random noise, environmental bias, and multipath effects then also the RSS measured at a set of landmarks is closely related to the transmitter's physical location. According to this the RSS readings present strong spatial correlation characteristics. The RSS vector is defined with value vector as-

S= {s1, s2, s3… sn }

Where n is the number of landmarks/access points that are monitoring the RSS of the wireless nodes and know their

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

locations. In case of spoofing attack, the two main elements are-

- Victim
- Attacker

Here both can transmit data packets by using same ID and the RSS readings of that ID is the mixture of readings measured from each individual node (i.e., spoofing node or victim node). Since under a spoofing attack, the RSS readings from the victim node and the spoofing attackers are mixed together, this observation suggests that we may conduct cluster analysis on top of RSS-based spatial correlation to find out the distance in signal space and further detect the presence of spoofing attackers in physical space. In this paper work, we propose to use Partitioning around Medoids The PAM Method is a popular iterative descent clustering algorithm. Also the evaluation results showed that PAM method is more robust than popular K-means clustering algorithm. Particularly our objective in this method is to detect the presence of attacks. Here null hypothesis indicates that no spoofing attack. T is the Test spec i.e. (Test specification) it is used to indicate weather observed data belongs to the null hypothesis or not. We then consider the distance between two medoids as Dm.

$$Dm = \| Mi - Mj \|$$

Where Mi and Mj are the medoids of two groups. Under typical conditions, the test detail Dm ought to be little following there is fundamentally standout bunch from a solitary physical area. Notwithstanding, under a mocking assault, there is more than one hub at distinctive physical areas asserting the same hub personality. Thus, more than one bunches will be shaped in the sign space and Dm will be extensive as the medoids are gotten from the distinctive RSS groups connected with diverse areas in physical space.

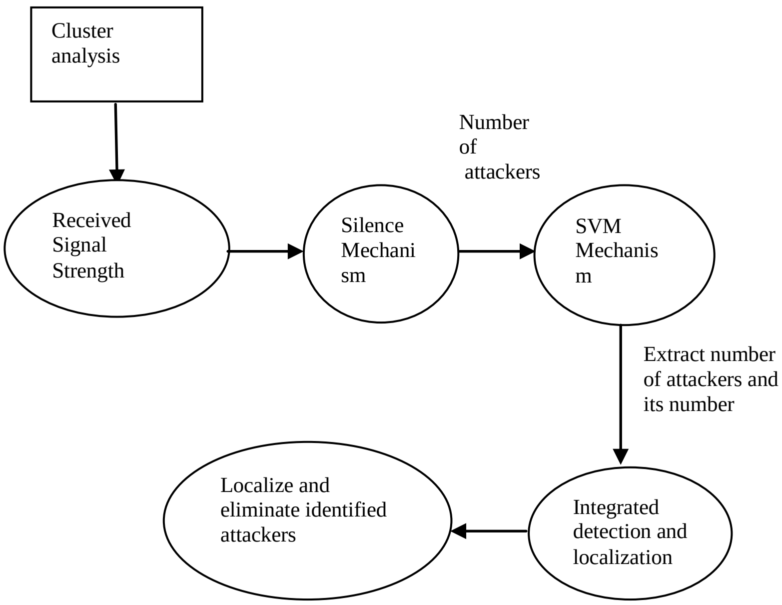

Fig.1 gives the overall pictorial presentation of this new security technique.

USING CLUSTER ANALYSIS IDENTIFYING THE ATTACK

Pi = Ci

The RSS-based spatial correlation transmitted from wireless

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

nodes to perform spoofing attack detection. It conjointly showed that the RSS readings from a wireless node could fluctuate and may cluster along. Particularly, the RSS readings over time from identical physical location can belong to identical cluster points within the n-dimensional signal area, whereas the RSS readings from completely different locations over time ought to kind different clusters in signal area. In Fig. 2, that presents RSS reading vectors of 3 landmarks (i.e., n = 3) from 2 completely different physical locations. underneath the spoofing attack, the victim and also the offender square measure victimization identical ID to transmit knowledge packets, and also the RSS readings of that ID is that the mixture readings measured from every individual node (i.e., spoofing node or victim node).Thus formulate spoofing detection as a applied math significance testing drawback, wherever the null hypothesis is H0: traditional (no spoofing attack):

In significance testing, a check data point T is employed to gauge whether or not discovered knowledge belong to the null-hypothesis or not.

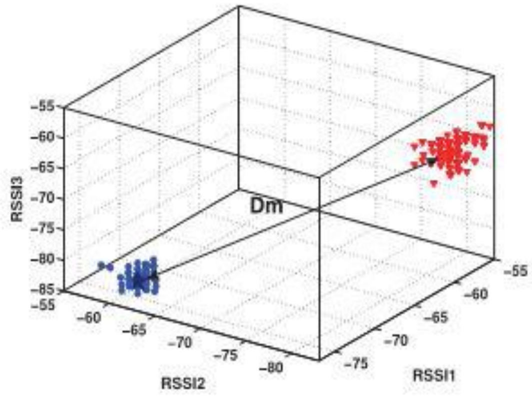

Fig.2 Illustration of RSS readings from two physical locations

MULTICLASS DETECTION PROBLEM

Multiclass detection problem includes determining number of attackers and similar in determining how many clusters existing in the RSS readings.

Ni = Ų cj € C

Here C is the set of all classes.ci is the specific number of attackers under particular class. Ni is the all other class as negative class. The related precision and F-measure are in. This gives the number of attackers in the system.

SILENCE Mechanism

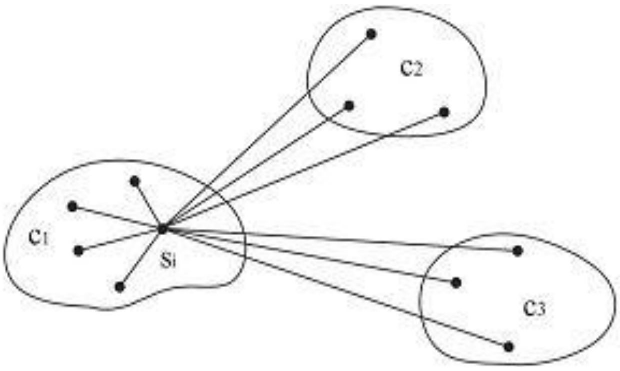

Fig.3.Cluster Representation view

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 4, April 2015

This SILENCE mechanism is basic Silhouette Plot for cluster is in. Based on this observation SILENCE, SILhouette Plot and System Evolution with minimum distance of cluster. This evaluates the minimum distance between clusters so as to improve the accuracy of determining the number of Attackers. SILENCE gives the K as number of attackers in the system. This K also depends on Dm-that's the distance between medoids.

Support Vector Machine (SVM) based mechanism.

SVM may be a set of kernel-based learning strategies for information classification that involves a coaching part and a testing part. Here every information instance within the coaching set consists of a target price (i.e., category label) and a number of other attributes (i.e., features). The performance of decisive variety of spoofing attackers may be improved additional by victimization SVM primarily based mechanism. During this section, Support Vector Machines is employed to classify the quantity of spoofing attackers and thus to enhance the detection rate. SVM accurately predicts the quantity of attackers by victimization model supported coaching information. The comparison between the results of SVM to those of Silhouette Plot, System Evolution and SILENCE strategies results in the ultimate call that SVM is that the best one because it provides important increase in Hit rate, preciseness etc.

V. CONCLUSION

Using received signal strength (RSS) 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. This approach can both detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that any number of attackers can be localized and can eliminate them. Determining the number of adversaries is a particularly challenging problem. This paper uses 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 is available, Support Vector Machines (SVM) based mechanism is used to further improve the accuracy of determining the number of attackers present in the system.

REFERENCES

[1] 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.
[2] 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.
[3]D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," Proc.ACM Workshop Wireless Security (WiSe), Sept. 2006.
[4]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.
[5] 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.
[6]L. Sang and A. Arora, "Spatial Signatures for Lightweight Security in Wireless Sensor Networks," Proc. IEEE INFOCOM, pp. 2137- 2145, 2008.
[7]L. Xiao, L.J. Greenstein, N.B. Mandayam, and W. Trappe, "Fingerprints in the Ether: Using the PhysicalLayer for Wireless Authentication," Proc. IEEE Int'l Conf.Comm. (ICC), pp. 4646-4651, June 2007.
[8]M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. ACM Workshop Wireless Security (WiSe), pp. 79- 87, 2003
[9]P. Bahl and V.N. Padmanabhan, "RADAR: An in- Building RFBased User Location and Tracking System," Proc. IEEE INFOCOM, 2000.
[10]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.
[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] 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.
[13] 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.