International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 495-499 1 May 2014

Multiple Spoofing Adversaries Detection and Localization in Wireless Networks

[1]S.Devi Rahini, [2]R.Ravi, [3]Dr. Beulah Shekhar
[1]PG Scholar, Department of Network Engineering, Francis Xavier Engineering College, Tirunelveli.
[2]Professor& Head, Department of Computer Science and Engineering, Francis Xavier Engineering College,Tirunelveli, Tamil Nadu State, India.
[3]Associate Professor, Department of Criminology and Criminal Justice, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu State, India.
[1]devirahini26@gmail.com,[2]csehod@francisxavier.ac.in, [3]fxhodcse@gmail.com

Abstract: ***The openness of wireless networks enables adversaries to deception as other devices. Spoofing attacks are vulnerable in wireless network, which are allowed the many form of attacks in the network. Wireless spoofing attacks are effortless to start and can extensively impact the performance of networks. A physical property coupled with each node is proposed which uses spatial information, hard to forge, and not contingent on cryptography, as the beginning for, detecting spoofing attacks, determining the number of attackers when multiple adversaries hidden as the same node identity and localizing multiple adversaries. To use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect the spoofing attacks. Cluster-based mechanisms are developed to determine the number of attackers. When the training data are available, we explore using the Support Vector Machines (SVM) method to further improve the accuracy of determining the number of attackers. An integrated detection and localization system is developed to localize the positions of multiple attackers.***

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

I. INTRODUCTION

In wireless network spoofing attack is when malicious party masquerade as the another devices or user in order to launch the variety of attacks against the hosts such as spread malware, bypass the access control and steal data. Spoofing attack is the generally hack technique in the network attacks. Network hackers just explore into this fault and devised many various network attacks, either spoofing themselves as reasonable clients or original servers. The attacker can monitor any transmission in wireless network. Further, attackers can easily purchase low-cost wireless device and use these normally existing platform to begin a variety of attacks with little effort. Most common method for the spoofing attacks are IP spoofing, ARP spoofing, DNS server spoofing.

IP SPOOFING :

Internet Protocol (IP) is the protocol used for transmitting messages over the Internet [1]; it is a network protocol operating at layer 3 of the OSI model. IP address spoofing is the one of the most frequently used spoofing attack methods. In an IP spoofing attack, an attacker sends IP packet from spoofed source address in order to masquerade itself. Denial of service attack often use the IP spoofing to overload the network and devices with packets that appears to be form legitimate source IP addresses.

II.RELATED WORK

The cryptographic techniques can be used to deal with such type of security violations. However, the application of cryptographic schemes [2] [3] require reliable key distribution, management, and maintenance mechanisms. It is not always attractive to apply these cryptographic methods because of its infrastructural, computational, and management. Further, these cryptographic methods are also vulnerable to node compromise, which is a serious disquiet as most wireless nodes are easily reachable, allowing their memory to be simply scanned.

We propose to use received signal strength (RSS)-based spatial correlation. It can be used mainly for detecting the presence of spoofing attacks, formative the number of attackers and localizing multiple adversaries and abolish them. We focus on static nodes in this work, which are familiar for spoofing scenario [4]. We addressed spoofing detection in mobile environments in our further work [5].

The works that are closely related to us are [1], [4], [6]. Faria and Cheriton [1] planned the use of matching rules of signalprints for spoofing detection, Sheng et al. [4] model the RSS reading using a Gaussian mixture model and Chen et al. [3] used RSS and K-means cluster analysis to detect spoofing attacks. However, not any of these approach have the ability to determine the number of attackers when multiple adversaries use the same identity to begin attacks, which is the basis to further localize several adversaries after attack detection.

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 495-499 1 May 2014

While Chen et al. [4] studied how to localize adversaries; it can only handle the case of a single spoofing attacker and cannot localize the attacker if the adversary uses different transmission power levels.

To study the localization techniques, in spite of its more than a few meter-level accuracy, using RSS [7], [8], [9], [10] is an attractive approach because it can reprocess the existing wireless infrastructure and is highly associated with physical locations. Trading with ranging methodology, range-based algorithms absorb distance evaluation to landmarks using the measurement of various physical properties such as RSS [7], [8], Time Of Arrival (TOA) [11], Time YANG ET AL.: DETECTION AND LOCALIZATION OF MULTIPLE SPOOFING ATTACKERS IN WIRELESS NETWORKS 45 Difference Of Arrival (TDOA), and direction of arrival (DoA) [12]. Range-free algorithms [13] use coarser metrics to place bounds on candidate positions.

One more method of classification explain the approach used to map a node to a location. Alteration approaches [11] use distances to landmarks, while angulations' used for the angles from landmarks. Scene matching strategies [7] use a function that maps experiential radio properties to locations on a recreate signal map or database. Further, Chen et al. [14] projected to perform detection of attacks on wireless localization and Yang et al. [12] 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 calculate their performance in terms of localization accuracy
The main focus of our work is a) A generalized attack detection model (GADE): It can detect the spoofing attack in the network as well as can determine the number of spoofing attackers in the same system. Here the attack detection can be present using Partitioning around Medoids (PAM) which calculates the medoids distance. If the medoid distance value is small it means that spoofing attack is not detected but if it is large then it signifies that spoofing attack is detected.

Then we used cluster based Multiple attack detection problem to determine number of spoofing attackers. Also we residential and used the SILENCE mechanism to improve the accuracy of finding number of attackers in the network. b) Integrated detection and localization system (IDOL):-IDOL can be used to detect the attacks and also can exactly localize the positions of spoofing adversaries or attackers.

GADE model results are returned to the IDOL. IDOL can handle attackers using by different transmission power levels, and hence provides strong evidence of the efficiency of localizing adversaries when there are multiple attackers in the network.

III.PROPOSED SYSTEM

3.1 GADE (Generalized Attack Detection Model)

Generalized attack model is consists of two method. They are detecting the spoofing attack and determining the presence of attackers in the network.

3.1.1Attack detection using cluster analysis

In a spoofing attack, the intruder mail messages to a computer indicating that the message has come from a trusted system. To be unbeaten, the intruder must first find out the IP address of a trusted system, and then change the packet headers to that it show that the packets are coming from the trusted system. The nature of attacker is spoofing the isolated computer into believing that they are a legitimate member of the network. The goal of the attack is to found a connection that will consent to the attacker to gain root access to the host, allowing the design of a backdoor entry path into the target system.

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 objective space.

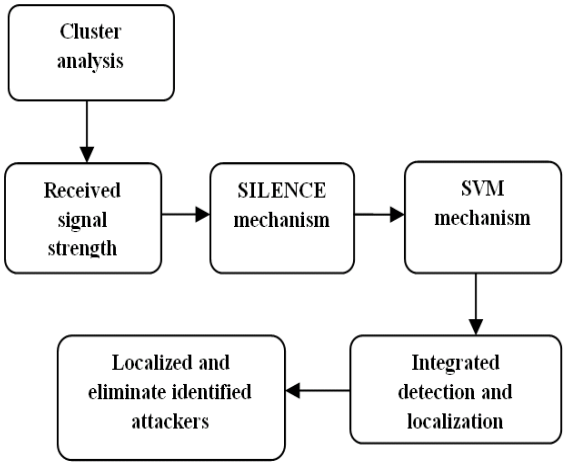

Fig 1 System architecture

3.1.2 Received Signal Strength

Received signal strength measured across a set of access point to carry out the spoofing detection and localization. The received signal strength (RSS) is a measurement that is hard to falsify capriciously and it is highly associated to the transmitter's location**.** Assuming the attacker and the victim are divided by a sensible distance, RSS can be used to make different them to identify spoofing attack. RSS is the signal strength of a received frame measured at the receiver's antenna. Many commercial 802.11 chipsets present per-frame RSS measurements. RSS is interrelated to the

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 495-499 1 May 2014

transmission power, the distance between the transmitter and the receiver, and the radio location because of multi-path and inclusion effects. The further than the attacker is from its victim, the more possible their RSS pattern vary extensively and the easier to detect the spoofing attacks.

In GADE method use Partitioning Around Medoids (PAM) Method so as to perform clustering analysis in RSS. The PAM Method is a accepted iterative descent clustering algorithm [15]. Also the estimate outcome showed that PAM method is more forceful than popular K-means clustering algorithm [16]. In scrupulous, attack detection phase, we separation the RSS vectors from the same node identity into two clusters (i.e., K = 2) regardless of how many attackers are using this characteristics, since our objective in this phase is to detect the incidence of attacks. We then choose the distance between two medoids Dm as the test statistic T in our significance testing for spoofing detection,

$$Dm -= |Mi - Mj|,$$

where Mi and Mj are the medoids of two clusters. In usual setting, the test statistic Dm should be small since there is basically only one cluster from a single physical location. However, under a spoofing attack, there is multiple node at different physical locations claiming the same node identity. As a result, multiple clusters will be formed in the signal space and Dm will be large as the medoids are derived from the different RSS clusters associated with different locations in physical space.

IV.FIND OUT THE NUMBER OF ATTACKER

4.1SILENCE Mechanism:

This SILENCE mechanism's basic Silhouette Plot for cluster is in [20][21].Based on this observation we developed SILENCE,SILhouette Plot and System EvolutioN with minimum distanCE of cluster. This mechanism estimates the minimum distance between clusters accordingly when to improve the accuracy of determining the number of Attackers. SILENCE gives the K as number of attackers in the system. This K depends on the distance between medoids.[17]

4.2 SUPPORT VECTOR METHOD

Support vector method is used to improve the accurateness of determining the number of attackers. This method collect the training data during the offline period,and also improve the performance of find out the number of spoofing attackers. We combine the characteristics of support vector method and SILENCE mechanism, to improve the higher detection rate. SVM method is kernal based learning method for classification, which involves a training phase and testing phase each data request in the training set consists of a target value and several attributes.

The advantage of using SVM is that it can combine the intermediate results (i.e. features) from different statistic methods to build a model based on training data acquired from cluster, to precisely expect the number of attackers. On detecting a attacker in the wireless network, SVM increment the target Value by '1', else '0'. SVM can be applied to solve classification and regression problems.

V.IDOL

Integrated detection and localization system is detect the spoofing attack, find out the number of attacker, and also localize the position of the attacker.

The proposed model builds use of three localization algorithms:-

- RADAR Grid algorithm
- Area Based Probabilistic algorithm
- Multi lateration algorithm

1. RADAR Grid:

This algorithm is the scene matching algorithm given in [18].It uses an interpolated signal map, which is build from a set of averaged RSS readings with known (x, y) locations. It returns the x, y of the near neighbor in the signal map to the one to localize, where "nearest" is defined as the Euclidean distance of RSS points in an N-dimensional signal space, where N is the number of familiar sight.

2. Area Based Probabilistic algorithm:

This algorithm is given in [19].Then here it is further extended to give value of P (Li/S). Here the given experimental area is divided into a regular grid of equal-sized strips. ABP imagine the allocation of RSS for each landmark track a Gaussian distribution with mean as the estimated value of RSS reading vector s. ABP then compute the probability of the wireless device being at each tile Li, with i = 1 . . .L, On the floor using Bayes' rule

$$P (Li/S) = P(S/Li) \times P (Li) / P(S)$$

This algorithm gives the probable area of location where the attackers or adversaries may be present. From this probable location authentic position of adversaries can be obtain in terms of x and y synchronize using multilateration algorithm.

3. Multilateration algorithm:

Bayesian network localization is the multilateration algorithm [22].This proposed algorithm encodes signal to space propagation model into Bayesian Graphical Model for localization.

Here Di correspond to the Euclidean space between the location particular by X and Y. (xi, yi) be the manager of the landmark.

$$Di = \sqrt{(X-xi)\ 2 + (Y-yi)\ 2}$$

This find out the original position of adversaries in network.

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 495-499 1 May 2014

.

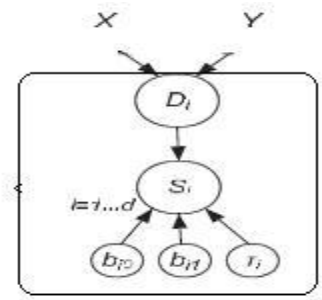

Fig 2 Bayesian Model Overview

VI.RESULT

If a spoofing attacker sends packets at a different transmission power level from the original node, based on our cluster analysis there will be two distinct RSS clusters in signal space (i.e., Dm will be large).In this graph, distance between two medoids in X axis and probablity in Y axis. spoofing attacks launched by using different transmission power levels will be detected effectively in GADE.

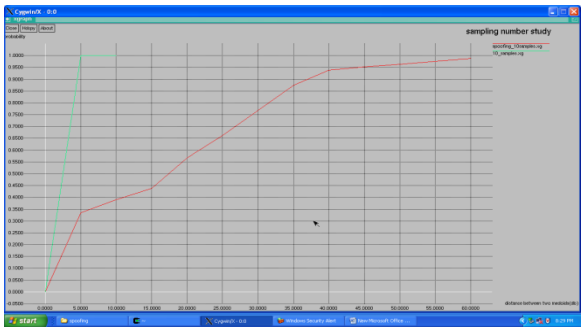

Fig 3Distance between two medoids vs probablity

This figure explain about the detection rate as a function of the distance between the original node and spoofing node. X axis represents the distance between the nodes,Y axis represents the spoofing attack detection rate.

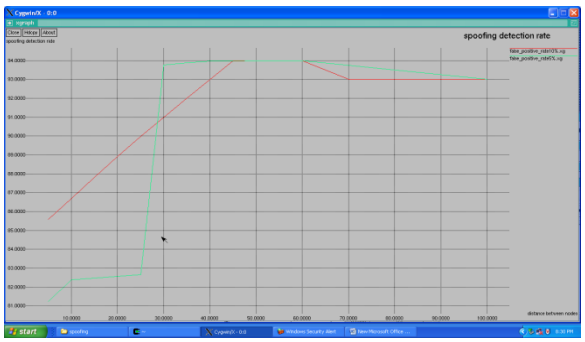

Fig 4 Distance between nodes vs spoofing detection rate

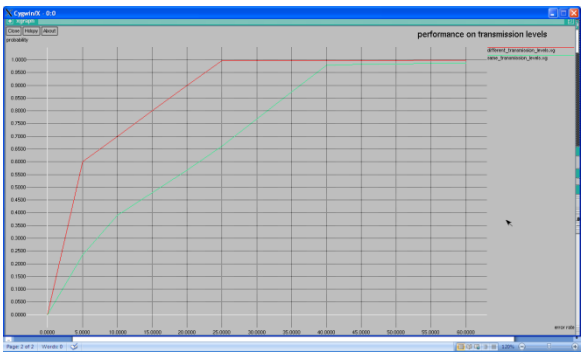

Fig 5Error rate vs probablity

The performance of using the difference of returned medoids in handling adversaries using different transmission power levels is comparable to the results when adversaries used the same transmission power levels as the original node. Fig 5 is explained about the adversaries used the same transmission power levels as the original node and the returned medoids ; and also adversaries changed their transmission power level from 15 to 10 dB and the returned medoids. IDOL method is highly effective with or without changing their transmission level in localization of multiple adversaries. In this graph error rate in the X axis, and probability in the Y axis.

VII.CONCLUSION

This project presented by the detecting the spoofing attack, determine the numbers of attacker and localizing the multiple attackers. This method used the received signal strength to find the detection of spoofing attack. Spoofing attacks launched by using different transmission power levels will be detected effectively in GADE. And also the Silence mechanism used to improve the accuracy of determining the number of attacker. This project is achieve the high performance of localization the spoofing attacker in the wireless network using IDOL . 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

REFERENCES

i. Diana Jeba Jingle, Elijah Blessing Rajsingh, “Defending IP Spoofing Attack and TCP SYN Flooding Attack in Next Generation Multi-hop Wireless Networks”, *International Journal of Information & Network Security*,vol 2 No.2 2013, pp.160-166.

ii. 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.

iii. 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.

International Journal of Scientific Engineering and Technology (ISSN : 2277-1581)
Volume No.3 Issue No.5, pp : 495-499 1 May 2014

iv. 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.
v. 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.
vi. 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.
vii. P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RFBased User Location and Tracking System," Proc. IEEE INFOCOM, 2000.
viii. 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.
ix. 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.
x. 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.
xi. P. Enge and P. Misra, Global Positioning System: Signals, Measurements and Performance. Ganga-Jamuna Press, 2001.
xii. Z. Yang, E. Ekici, and D. Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.
xiii. T. He, C. Huang, B. Blum, J.A. Stankovic, and T. Abdelzaher, "Range-Free Localization Schemes in Large Scale Sensor Networks," Proc. MobiCom '03, 2003.
xiv. Y. Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc. IEEE INFOCOM, Apr. 2007.
xv. L. Kaufman and P.J. Rousseeuw, Finding Groups in Data: An Introduction to Cluster Analysis. *Wiley Series in Probability and Statistics*, 1990.
xvi. G. Zhou, T. He, S. Krishnamurthy, and J.A. Stankovic, "Models and Solutions for Radio Irregularity in Wireless Sensor Networks,"*ACM Trans. Sensor Networks*, vol. 2, pp. 221-262, 2006.
xvii. Jie Yang, Yingying Chen, and Jerry Cheng, "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" in IEEE transactions on parallel and distributed systems, Vol 24, no.1, january 2013 .
xviii. P. Bahl and V.N. Padmanabhan, "RADAR: An in- Building RFBased User Location and Tracking System," *Proc. IEEE INFOCOM*, 2000.
xix. 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.
xx. P. Rousseeuw, "Silhouettes: A Graphical Aid to the Interpretation and Validation of Cluster Analysis," *J. Computational and Applied Math., vol*. 20, no. 1, pp. 53-65, Nov. 1987.
xxi. K. Wang, "Estimating the Number of Clusters via System Evolution for Cluster Analysis of Gene Expression Data," *Technical Report NO. 2007-258, Computer Science Dept., Xidian Univ., P.R. China*, 2007.
xxii. D. Madigan, E. Elnahrawy, R. Martin, W. Ju, P. Krishnan, and A.S. Krishnakumar, "Bayesian Indoor Positioning Systems," *Proc. IEEE INFOCOM, pp*. 324- 331, Mar. 2005. 1875

AUTHOR(S) PROFILE

S.Devi Rahini is presently studying M.E second year Network Engineering in Francis Xavier Engineering College. She has completed her B.E Electronics and Communication Engineering from J.P College of engineering. Her field of interests are Network security, Wireless network**.**

R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor & Head and Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkatta. He has 18 years of experience in teaching as Professor and Head of department in various colleges. He published 12 International Journals, 1 National Journal. His areas of interest are Virtual Private networks, Networks, Natural Language Processing and Cyber security.

Dr. Beulah Shekhar is a Coordinator for Victimology & Victim Assistance, in the Department of Criminology and Criminal Justice Sciences; she is presently working as a Associate Professor in the Department of Criminology and Criminal Justice Sciences. And her areas of interest are Crimes against Women Empowerment, Human Rights, and Police Training.