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. 2, Issue 5, May 2014

Detection of Spoofing Attack and Localization of Multiple Adversaries in WSN

[1]R. Panchabi kesavan, [2]S.A. Ramesh kumar,

[1]P.G Scholar, Department of Computer Science and Engineering, Karpaga Vinayaga College of Engineering and Technology, Chengalpet, Tamil Nadu, India.

[2]Associate Professor, Department of Computer Science and Engineering, Karpaga Vinayaga College of Engineering and Technology, Chengalpet, Tamil Nadu, India.

ABSTRACT: Spoofing attack which easily attack the network and reduce the performance of the network. In this Paper, Spoofing attacks are detected, Finding the number of attackers that masquerade the node identity, Localizing all the attackers node and calculate the speed of a node, by using RSS (received signal strength) for spoofing detection. The number of attacker is determined by cluster- based method. Support Vector Machines (SVM) is to improve the accuracy of finding number of attackers. Evaluate our method in two real office, an 802.11 (WiFi) network and an 802.15.4 (ZigBee) network. Our method gives over 90 percent of Hit Rate.

KEYWORDS: Spoofing attack, masquerade, adversaries.

I. INTRODUCTION

In the wireless transmission medium, any transmission are monitored by adversaries. Adversaries are easily available in wireless device and used in common platform to launch a variety of attacks. Identity-based Spoofing attacks are easy to launch when compared to other attacks it cause the network performance. During passive monitoring easy to get MAC address for the attackers and modify its MAC address by using ifconfig command to masquerade as another device. In 802.11 security technique include Wired Equivalent Privacy (WEP), WiFi Protected Access(WPA) or 802.11i (WPA2) these methods can only protect the data frames. Still the Spoofing management or control frames to cause significant impact on networks by attackers. Spoofing attack can further in variety of attacks on access control list, rogue access point, Denial of Service (DOS). In a large network, multiple adversaries may masquerade as same identity and launch malicious attack like DOS. It is important to i) detect the Spoofing attack, ii) Determine the number of attackers and iii) localize multiple adversaries and eliminate them. Cryptographic method is not desirable, because its infrastructural, computational and management overhead. In this work we propose to use Received Signal Strength (RSS) based spatial correlation. Hard to falsefy and not reliant on cryptography for detecting spoofing attacks. We concerned with attackers who have different location than legitimate wireless node utilizing spatial information to address spoofing attacks has the unique power to not only identify the attacks but also localize adversaries. It will not require any additional cost or modification for detect the spoofing attacks. We addressed spoofing detection in mobile environment in our other work. The works are closely related to us Faria and cheriton[6] proposed the use of matching rule of signal prints for spoofing detection.

None of these approaches have the ability to determine the number of attackers, when multiple adversaries use the same identity. [9] Localize adversaries handle the case of single spoofing attacker and cannot localize different transmission power levels. The main contribution of our work are :

i) GADE: a Generalized Attack Detection model. Detect Spoofing attacks as well as determine the number of adversaries using cluster analysis method on RSS based spatial correlation.

Ii) IDOL : an Integrated Detection and Localization system. Detect attack as well as find the positions of multiple adversaries even it vary their transmission power levels. In GADE, the (PAM) Partitioning Around Medoids cluster analysis method is used to perform attack detection. Formulate the problem of determining the number of attackers as a multiclass detection problem, Determine the number of attacker by cluster based method. Further developed a mechanism

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. 2, Issue 5, May 2014

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 use the support vector Machines(SVM) to improve the accuracy of determining the number of attacker. IdOL utilize the results of number of attackers returned by GADE to further localize multiple adversaries. 802.11 and 802.15.4 network in two real office building, GADE is highly effective in Spoofing detection over 90 percent hit rate. IDOL can handle attacker using different transmission power levels, the effectiveness of localizing adversaries when there are multiple attackers in network.

II. RELATED WORK

To prevent the Spoofing attacks by using cryptographic – based authentication [13], [14] [4]. . . [13] introduced a Secure and efficient key management (SEKM) framework.
SEKM builds a Public Key Infrastructure (PKI) by applying secret sharing scheme. [14] implements a key management mechanism with periodic key refresh and host revocation for preventing compromise of authentication keys. [6], [15], [10] using RSS to defend against spoofing attacks are most closely related. [6] use of signal print rules matching for spoofing detection [15] RSS readings using Gaussian mixture model. [10] spatial "signature" include Received Signal Strength Indicatior (RSSI) and Link Quality Indicator (LQI) authenticate messages.

None of these approaches are capable of finding the number of attackers, when multiple attackers use the same identity to launch malicious attacks. They do not have the ability to localize the position detecting attackers. For Localizing techniques (several meter – level accuracy) using RSS is an attractive approach. Range- based Alogrithm which invole distance estimination such as RSS, Time of Arrival (TOR) [18], Time Difference of Arrival (TDOA), and Direction of arrival (DOA) [19]. [20] Range free algorithm to place bounds on candidate position. [18] distances to landmarks, while angulation uses the angle from landmarks. [16] scene matching strategies use a function that maps observed radio properties to location on already constructed signal map or database. [21] to perform detection of attacks on wireless localization. [19]] direction of arrival and received signal strength of the signals to localize adversary's sensor nodes. To identity the localization accuracy in multiple attackers by RSS Algorithm. None of the Existing work can find the number of attackers in multiple adversaries masquerading as same identity. It can accurately localize multiple adversaries even the attacker varying their transmission power level to system of their true location.

III. GENERALIZED ATTACK DETECTION MODEL

GADE which consist of attack detection and number determination number of adversaries.

A. Spatial correlation of RSS

Uniqueness of Spatial information is the challenge in spoofing detection, it does not using the attackers location directly position are unknown. RSS measured the landmarks through the transmitters physical location and governed by landmark distance.

B. Attack Detection using cluster Analysis

RSS reading from the same physical location belong to same cluster point. RSS reading from different location in signal space should form different cluster . The victim and the attacker using the same ID under spoofing attack to transmit data packets. RSS measured from each individual node (spoofing node or victim node). On the top of cluster analysis by RSS based spatial correlation to find the distance in signal space and detect the spoofing attackers.
H_o : normal (no spoofing attack)

C. Evaluation Strategy

To test the performance of attack detection in real office building environment. Evaluate in two office buildings,
Wireless Information Network Laboraatory (WINLAB) using an 802.11 (WiFi)
College using an 802.15.4 (zigbee) network.

The two floor sizes are 219ft x 169 ft and 200ft x 80 ft. have five landmarks in red stars in 802.11 network 802.15.4 the four landmarks deployed as red triangle landmark has important on detection performance. Linux machine is equipped in Athero miniPCI 802.11 as landmark. Both WiFi and zigbee networks Tmote sky measure the RSS readings. Small dots are the location for testing, 101 location for the 802.11 network and 94 location for 802.15.4 network. In day time, when people walk around 300 packet level RSS Samples are collected at each location. Various transmission power

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. 2, Issue 5, May 2014

levels from 30mW (15dBm) to 1mW (0 dBm) for 802.11. Randomly choose one point as position of original node, rest as the position of Spoofing node. Test through all possible combination of testing point for two or more attackers masquerading a same node identity.

Here use leave one – out method in localization algorithm, testing all node in one location where the rest of location as training data.

D. Result of Attack Detection

1. Impact of Attack Detection and Sampling Number

The cumulative Distribution Function of Dm both spoofing attack and Normal condition in signal space.

Under the spoofing attack the curve Dm shifted greatly to the right. The Spoofing attack is declare as when Dm>T.

2. Handling Different Transmission Power level

Transmission power is varied for an attacker from 30 mW (15dBm) to 1mW (0 dBm) in all cases Dm is larger.

10dB is the spoofing attacker transmission powewr to send packet, whereas the original node used 15dB power level. Dm curve under different power level shifts to larger Dm values, This attack is detected by GADE.

IV. DETERMINING THE NUMBER OF ATTACKERS

A. Problem Formulation

Do not know how many adversaries using the same node identity. Determining the number of attackers is a multicast detection problem, which similar to find number of cluster exist in RSS reaching.

C is the set of all classes C = {1, 2, 3, 1} C_i – Specific number of attackers, C_i = 3 define P_i as positive class of C_i others as negative Class N_i.

$P_i = C_i$

$N_i = U\ C_j$ € C

B. Silhouette Plot

1 Attacker number Determination

The graphical representation of cluster by Silhouette Plot, Silhouette use the following way to determine the number of attackers.

The RSS sample points S={ S_1, ... S_N} are the data set (where N is the total number of samples). Let C= (C_1, . . ., C_k) be its clustering into K cluster Let d (S_k, S_l) be the distance between S_k and S_L,

Let C_j = { S_1^j, ..., S_{mj}^j} be the jth cluster; j=1, ... k, where $m_j = |C_j|$.

C.System Evolution

The new method to find the cluster structures and the number of clusters is the System Evolution. By using twin cluster model are the two nearest cluster (eg. Cluster a and b) among all cluster (k) data set. It is used for calculate the energy. The border distance between the twin clusters are denoted by the partition Energy $E_p(k)$ Merging Energy Em(k) is the average distance between border region element in twin clusters.

The border region point out number of samples in cluster a by $n_a = \frac{M_a}{D_a}$, M_a total number of samples point $Da = \frac{\sqrt{M_a}}{2}$, same rule in cluster b, Partition Energy $E_p(k)$ and Merging Energy $E_m(k)$. When the number of attacker are find $E_m(k) \geq E_p(k)$ unless $E_p(k) > E_m(k)$. It stops when it reaches equilibrium state $K_{optimal}$ the optimal number is the number of attackers.

K=4 with $E_p(4) > E_m(4)$ and $E_p(5) < E_m(5)$ indicating four adversaries in 802.11 network, using same identity performing spoofing attacks.

D. The SILENCE Mechanism

Silhouette Plot is suitable for estimating the best partition, the Hit Rate decreases the number of attackers will increases when observed for Silhouette Plot and the System Evolution method. These are the reason for not tell difference between the real RSS by attackers at different position and fake RSS by outliers and variation of signal strength. Small

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. 2, Issue 5, May 2014

distance in Silhouette Plot for attackers in single physical location. The correct number of attackers and minimum distance of cluster from different location in System Evolution.

Based on these problem developed SILENCE, testing SILhouette Plot and System EvolutioN with minimum distance, this evaluate the minimum distance between the clusters, to improve the accuracy to find the number of attackers in pure cluster analysis.

E. Support Vector Machines – Based Mechanism

Some more methods are available for the number of attackers detection by System Evolution and SILENCE. To perform the higher detection rate by combine both the characters. SVM combine the intermediste results from various statistics method. Krneal – based method are set by SVM for classification of data.

V. IDOL: INTEGRATED DETECTION AND LOCALIZATION FRAMEWORK

In this method Spoofing attack detection, number of attacker determination and localize the multiple adversaries, The Attackers using a various transmission power.

A. Framework

RSS which is used to identify the position of anode. In this network the normal node and spoofing node have various location. RSS gets from SILENCE as input to find the normal node and attacker in the location.

The attacker using different transmission power level, it is difficult to identify the location exactly.

B. Algorithm

IDOL using these Algorithms, RADAR[15] – nearest neighbor matching in signal space, ABP[16] – Area Based Probability, BN[37] – multilateration Bayesian Networks

RADAR

Scene – matching localization by RADAR Gridded algorithm[15]. It uses interpolated signal map between (x,y) are the known location by RSS. Unknown location are read by RSS, the RADAR which gives the nearest signal map of x,y RSS point N – dimensional signal, where N is the number of landmark.

Area Based Probability

It also use the signal map but it divide the area by grid of equal – size tiles. Which calculate the Probability of each tiles L_i with i= 1,. . . . L using Bayes' rule.

$$P(L_i|S) = \frac{P(S|L_i)XP(L_i)}{P(s)}$$

ABP returns the mostly likely tiles as the adversaries.

VI. CONCLUSION

By using RSS reading for test statistic on cluster analysis, our method can both detect as well as find the number of adversaries and eliminate the spoofing node. The challenging problem is to find the number of attackers, by using SILENCE mechanism for greater accuracy of finding the number of attackers, when compare to other methods. Under Silhouette Plot and System Evaluation additionally using SVM to improve the accuracy. Validate our method in two networks WiFi (802.11 network) and ZigBee (802.15.4) in real office building. Further to calculate the speed of the node can be determined in our network.

REFERENCES

[1] Jie Yang, Yingying Chen, "Detection and Localization of Multiple Spoofing Attackers in Wireless Network," in Proc. IEEE IPDPS, Jan 2013.
[2] 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.
[3] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and practical solutions," in Proceedings of the USENIX Security Symposium, 2003, pp. 15 – 28.
[4] M. bohge and W. Trappe, "An authentication framework for hierarchical ad hoc sensor network," in Proceeding of the ACM Workshop on Wireless Security (WiSe), 2003, pp. 79-87.
[5] Y. Chen, W. Trappe and R. P. Martin, "Detecting and Localizing wireless spoofing attacks," in Proc. IEEE SECON, May 2007.
[6] D. Faria and D. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in Proceeding of the ACM Workshop on Wireless Security (WiSe), September 2006.

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. 2, Issue 5, May 2014

[7] F. Ferreri, M. Bernaschi and L. Valcamonici, "Access points vulnerabilities to dos attacks in 802.11 networks," in Proceedings of the IEEE Wireless Communications and Networking Conference, 2004.
[8] Q. Li and W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in Proc. IEEE SECON, 2006.
[9] Q. Li and W. Trappe, "Relationship-based detection of spoofing-related anomalous traffic in ad hoc networks," in Proc. IEEE SECON, 2006.
[10] L. Sang and A. Arora, "Spatial Signatures for LightweightSecurity in Wireless Sensor Networks,"Proc. IEEE INFOCOM, pp. 2137-2145, 2008.
[11] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in Proc. IEEE INFOCOM, April 2008.
[12] J. Yang, Y. Chen, and W. Trappe, "Detecting spoofing attacks in mobile wireless environments," in Proc. IEEE SECON, 2009.
[13] B. Wu, J. Wu, E. Fernandez, and S. Magliveras, "Secure and efficient key management in mobile ad hoc networks," in Proc. IEEE IPDPS, 2005.
[14] 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
[15] 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.
[16] P. Bahl and V. N. Padmanaban, "RADAR: An in-Building RF-Based User Location and Tracking System," Proc. IEEE INFOCOM, 2000.
[17] 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.
[18] P.Engr and P. Misra, Global Positioning System: Signal, Measurements and Performance. Ganga-Jamuna Press, 2001.
[19] Z. Yang, E. Ekici, and D.Xuan, "A Localization-Based Anti-Sensor Network System," Proc. IEEE INFOCOM, pp. 2396-2400, 2007.
[20] 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.
[21] Y.Chen, W. Trappe, and R. Martin, "Attack Detection in Wireless Localization," Proc. IEEE INFOCOM, Apr.2007.