Middle-East Journal of Scientific Research
24 (Special Issue on Innovations in Information, Embedded and Communication Systems): 63-67, 2016
ISSN 1990-9233; © IDOSI Publications, 2016
DOI: 10.5829/idosi.mejsr.2016.24.IIECS.23141

Detection and Analysis of Spoofing Attackers in Wireless Sensor Networks

M. Srinivasaperumal, M. Jagadesh, T. Prabhu and K. Boopathi Raja

Department of ECE, SNS College of Technology, Coimbatore, India

Abstract: In recent days secure wireless communication over wireless sensor networks environment is one of the challenging tasks in real time applications. In this paper we discussed about the wireless spoofing attacks in wireless sensor networks. This kind of attacks is very easy to impose and may significantly impact the performance of networks. It may cause the serious problems in the network environments and makes huge data loss. The identification and detection of a node can be verified through different cryptographic authentication method and some conventional security approaches. But these methods are not always desirable because of their overhead requirements. Hence, here we use spatial correlation of Received Signal Strength (RSS) is very hard to falsify and also not reliant on cryptography. This method is used with cluster based mechanism to detect spoofing attacks and determine the number of attackers.

Key words: Wireless sensor networks · Security · Spoofing attacks · RSS · Cluster

INTRODUCTION

With the development of network technologies and applications, network attacks are greatly increasing both in number and severity [1, 2]. As a key technique in network security domain, Intrusion Detection System (IDS) plays vital role of detecting various kinds of attacks and secures the networks. Main purpose of IDS is to find out intrusions among normal audit data and this can be considered as classification problem. Intrusion detection systems (IDS) are an effective security technology, which can detect, prevent and possibly react to the attack. It performs monitoring of target sources of activities, such as audit and network traffic data in computer or network systems, requiring security measures and employs various techniques for providing security services. With the tremendous growth of network-based services and sensitive information on networks, network security is becoming more and more important than ever before [3].

Types of Network Attacks: Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself [4].

- Eaves dropping
- Data modification
- ID Address Spoofing
- Password based attacks
- Denial of Service attack
- Man in the middle attack
- Compromised key attack
- Sniffer attack
- Application layer attack

Spoofing: Many of the protocols in the TCP/IP suite do not provide mechanisms for authenticating the source or destination of a message [5, 6]. They are thus vulnerable to spoofing attacks when extra precautions are not taken by applications to verify the identity of the sending or receiving host. IP Spoofing and ARP Spoofing in particular may be used to leverage man-in-the-middle attacks against hosts on a computer network. Spoofing attacks which take advantage of TCP/IP suite protocols may be mitigated with the use of firewalls capable of deep packet inspection or by taking measures to verify the identity of the sender or recipient of a message [7].

802.11 Spoofing Based Attacks: A variety of 802.11 misbehaviors are based on MAC spoofing, some of which are benign to other users. For example, the spoofer may

Corresponding Author: M. Srinivasaperumal, Department of ECE, SNS College of Technology, Coimbatore, India.

want to use a randomly generated MAC address to hide their presence, or to masquerade as an authorized MAC address to circumvent AP's MAC address access-control list [8, 9]. Our focus, however, is on spoofing-based denial-of service (DoS) attacks, misbehaviors that impact other users by denying or degrading their network services. The IEEE 802.11 standard requires a two-step handshake before a wireless station (STA) can associate with an AP. When an STA is associated with an AP, the attacker can send a Deauthentication frame using the forged MAC address of the AP. The STA becomes disassociated and has to associate with the AP again. By continuously sending such spoofed Deauthentication frames, the attacker can break the wireless connectivity between the STA and the AP. Note that the attacker may also forge these frames using STA's MAC address.

Existing Methods: The existing method approaches to address potential spoofing attacks employ cryptographic schemes. Cryptography is an important and powerful tool for security services, namely authentication, confidentiality, integrity and non-repudiation [10]. It converts readable data (plaintext) into meaningless data (ciphertext). Cryptography has two dominant flavors, namely symmetric-key (secret-key) and asymmetrickey (public-key) approach. In symmetric-key cryptography, the same key is used to encrypt and decrypt the information, while in the asymmetric-key approach, different keys are used to convert and recover the information. Although the asymmetric cryptography approach possesses versatileness (authentication, integrity and confidentiality) and simplicity for key distribution, symmetric-key algorithms are generally more computation-efficient than the public-key approach. There is a variety of symmetric or asymmetric algorithms available, such as DES, AES, IDEA and RSA. Threshold cryptography is a scheme quite different from the above two approaches. In (k; n) secret sharing scheme, a secret is split into n pieces according to a random polynomial. The secret can be recovered by combining k pieces based on Lagrange interpolation. These cryptography tools are widely used in wired and wireless networks, obviously they could also be used in mobile ad hoc networks [11].

Proposed Method: The proposed method involves the use of received signal strength (RSS)-based spatial correlation. It is 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.

GADE: GADE is Generalized Attack Detection modEl 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. 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 and then applied cluster-based methods to determine the number of attacker.

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. In this section, we describe our Generalized Attack Detection ModEl. Which consists of two phases: Attack detection, which detects the presence of an attack and number determination, which determines the number of adversaries.

In GADE, following two methods are used to perform attacks and detections. They are Partitioning Around Medoids (PAM) and cluster analysis method. The problem of determining the number of attackers as a multiclass detection problem and then applied cluster-based methods to determine the number of attacker.

Partitioning Around Medoids: A clustering Algorithm that partitionates a dataset of n objects into a number k of clusters and works trying to minimize the error. This algorithm works with a matrix of dissimilarity, where its goal is to minimize the overall dissimilarity between the representants of each cluster and its members.The Partitioning Around Medoids Method to perform clustering analysis in RSS. The PAM Method is a popular iterative descent clustering algorithm. Compared to the popular K-means method the PAM method is more robust in the presence of noise and outliers. Thus, the PAM method is more suitable in determining clusters from RSS streams, which can be unreliable and fluctuating over time due to random noise and environmental bias.

Cluster the following data set of ten objects into two clusters i.e. k = 2. Table 1, consider a data set of ten objects as follows:

Table 1: Data set of ten objects

X1	2	6
X2	3	4
X3	3	8
X4	4	7
X5	6	2
X6	6	4
X7	7	3
X8	7	4
X9	8	5
X10	7	6

STEP 1

Initialize k centers.

Let us assume c1 = (3,4) and c2 = (7,4)

So here c1 and c2 are selected as medoids.

Calculate distance so as to associate each data object to its nearest medoid. Cost is calculated using Manhattan distance. Costs to the nearest medoid are shown bold in the Table 2 to 5.

Table 2: Cost from the Medoid (3,4)

I	c1		Data objects (Xi)		Cost (distance)
1	3	4	2	6	3
3	3	4	3	8	4
4	3	4	4	7	4
5	3	4	6	2	5
6	3	4	6	4	3
7	3	4	7	3	5
9	3	4	8	5	6
10	3	4	7	6	6

Table 3: Cost from the Medoid (7,4)

I	c2		Data objects (Xi)		Cost (distance)
1	7	4	2	6	7
3	7	4	3	8	8
4	7	4	4	7	6
5	7	4	6	2	3
6	7	4	6	4	1
7	7	4	7	3	1
9	7	4	8	5	2
10	7	4	7	6	2

Then the clusters become:

Cluster1 = {(3,4)(2,6)(3,8)(4,7)}

Cluster2 = {(7,4)(6,2)(6,4)(7,3)(8,5)(7,6)}

Since the points (2,6) (3,8) and (4,7) are closer to c1 hence they form one cluster whilst remaining points from another cluster. So the total cost involved is 20.Total cost is the summation of the cost of data object from its medoid in its cluster so here:

Totalcost={cost((3,4), (2,6)) + cost((3,4), (3,8)) + cost((3,4), (4,7))} + {cost((7,4), (6,2)) + cost((7,4), (6,4)) + cost((7,4), (7,3)) + cost((7,4), (8,5)) + cost((7,4), (7,6))}

STEP 2

Select one of the nonmedoids O'

Let us assume O' = (7,3)

So now the medoids are c1(3,4) and O'(7,3)

If c1 and O' are new medoids, calculate the total cost involved. By using the formula in the step 1

Table 4: Cost from the Medoid (3,4)

I	c1		Data objects (Xi)		Cost (distance)
1	3	4	2	6	3
3	3	4	3	8	4
4	3	4	4	7	4
5	3	4	6	2	5
6	3	4	6	4	3
7	3	4	7	4	4
9	3	4	8	5	6
10	3	4	7	6	4

Table 5: Cost from the Medoid(7,3)

I	O'		Data objects (Xi)		Cost (distance)
1	7	3	2	6	8
3	7	3	3	8	9
4	7	3	4	7	7
5	7	3	6	2	2
6	7	3	6	4	2
7	7	3	7	4	1
9	7	3	8	5	3
10	7	3	7	6	3

TOTAL COST= 3+4+4+2+2+1+3+3=22

So cost of swapping medoid from c2 to O' is

S=Current total cost-Past total cost=22-20=2>0

So moving to O' would be a bad idea, so the previous choice was good. So we try other nonmedoids and found that our first choice was the best. So the configuration does not change and algorithm terminates here (i.e. there is no change in the medoids). It may happen some data points may shift from one cluster to another cluster depending upon their closeness to medoid. In some standard situations, k-medoids demonstrate better performance than k-means. The most time-consuming part of the k-medoids algorithm is the calculation of the distances between objects. If a quadratic preprocessing and storage is applicable, the distances matrix can be precomputed to achieve consequent speed-up. See for example, where the authors also introduce a heuristic to choose the initial *k medoids*. A comparative study of *K-means* and *k-medoids* algorithms was performed for normal and for uniform distributions of data points. It was demonstrated that in the asymptotic of large data sets the k-medoids algorithm takes less time.

Simulation Results:

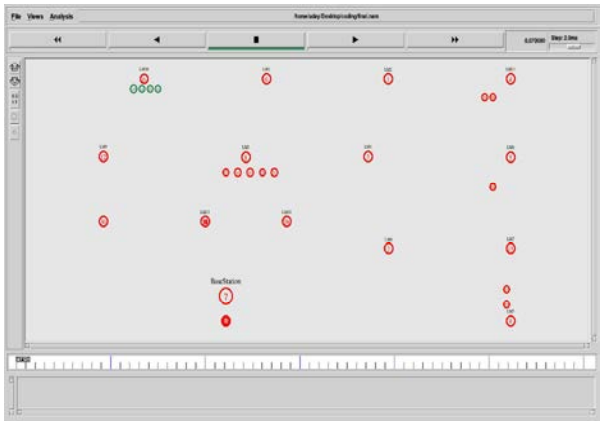

Fig. 1: Movement of Nodes from LM1

The Fig. 1 shows the movement of nodes 10,11,13 and 14 from Land Mark LM1 to the Land Mark LM2.

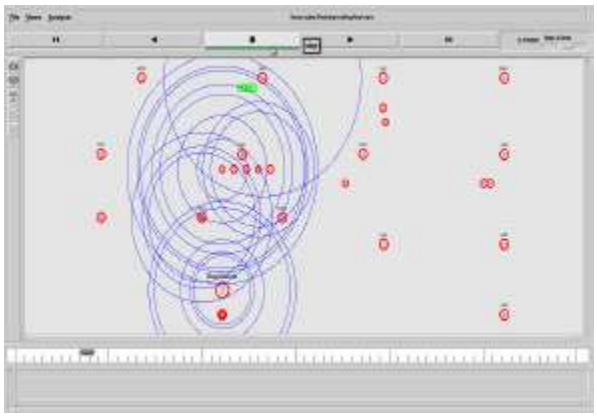

Fig. 2: Transmission of Packets

The Fig. 2 shows the transmission of packets between the nodes through the shortest path to the Base Station when it reaches Land Mark LM1.

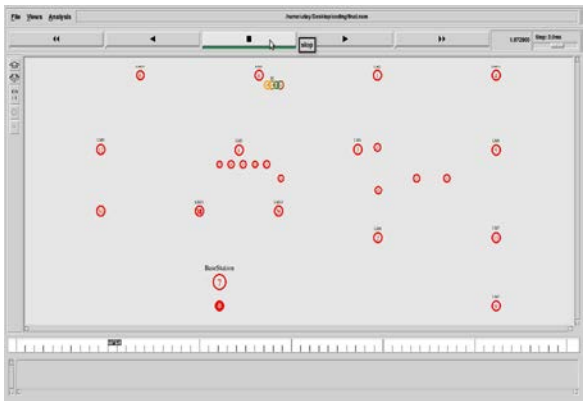

Fig. 3: Detection of Spoofing Attacker

The Fig. 3 explains the presence of a masquerade node where the 11th node masquerade like the 10th node with the ID of 10th node.

CONCLUSIONS

In this paper, we discussed about the 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. In future process the next stage includes the detection of number of attackers and localization of the attackers will be processed with NS2 and improve the accuracy of detecting the attackers in wireless sensor networks.

REFERENCES

1. Bellardo, J. and S. Savage, 2003. 802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions, Proc. USENIX Security Symp., pp: 15-28.
2. Chen, Y., W. Trappe and R.P. Martin, 2007. Detecting and Localizing Wireless Spoofing Attacks, Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON).
3. Faria, D. and D. Cheriton, 2006. Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," Proc. ACM Workshop Wireless Security (WiSe).
4. Ferreri, F., M. Bernaschi and L. Valcamonici, 2004. Access Points Vulnerabilities to Dos Attacks in 802.11 Networks, Proc. IEEE Wireless Comm. and Networking Conf.
5. Guo, F. and T. Chiueh, 2006. Sequence Number-Based MAC Address Spoof Detection, Proc. Eighth Int'l Conf. Recent Advances in Intrusion Detection, pp: 309-329.
6. Kaufman, L. and P.J. Rousseeuw, 1990. Finding Groups in Data: An Introduction to Cluster Analysis. Wiley Series in Probability and Statistics.
7. Young, M., 1989. The Technical Writer's Handbook. Mill Valley, CA: University Science.
8. Sheng, Y., K. Tan, G. Chen, D. Kotz and A. Campbell, 2008. Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength, Proc. IEEE INFOCOM.
9. Wool, A., 2005. Lightweight Key Management for IEEE 802.11 Wireless Lans With Key Refresh and Host Revocation, ACM/Springer Wireless Networks, 11(6): 677-686.

10. Wu, B., J. Wu, E. Fernandez and S. Magliveras, 2005. Secure and Efficient Key Management in Mobile Ad Hoc Networks, Proc. IEEE Int'l Parallel and Distributed Processing Symp. (IPDPS).
11. Yang, J., Y. Chen and W. Trappe, 2009. Detecting Spoofing Attacks in Mobile Wireless Environments, Proc. Ann. IEEE Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON).