

GMFAD and CDAL-M Models for Identification of Adversary Attacks in Wireless Sensor Network using RSS

Santosh S. Doifode¹, D. C. Mehetre²

¹Department of Computer Engineering, KJCOEMR, Pune, Maharashtra, India

²Professor, Department of Computer Engineering, KJCOEMR, Pune, Maharashtra, India

Abstract: *Wireless Sensor Networks are used worldwide across the Globe for communication in networks. Such Wireless Sensor Networks are easily vulnerable for range of attacks. The range of Adversaries attacks can also be easily launched in the wireless network. The paper presents the newly generated models GMFAD and CDAL-M which makes use of the physical property mainly Received Signal Strength associated with each node of network. It mainly focuses on received signal strength means the physical property instead of existing cryptographic techniques, which is hard or difficult to falsify and also independent of cryptographic techniques. This paper mainly focuses on detecting Identity based Adversaries attack and number of attackers in the cluster network also localizing the actual position of attackers. Also this paper can be used for Detecting Denial of Service attacks and localizing their position. The experimental results show that this advanced model doesn't require any additional efforts and also extra modifications to the existing. Hence topic depict that this models gives the advanced security management as compared to the existing cryptographic security techniques.*

Keywords: GMFAD, CDAL-M, RSS, DoS, WSN.

1. Introduction

In the current age of communication networks the more affection is laying towards the wireless sensor networks. It is usually assumed that an attacker may know the security mechanisms that are deployed in a sensor network. Attackers may be able to compromise a node or even physically capture a node. Most WSN nodes are viewed as non-tamper resistant due to the high cost of deploying tamper resistant sensor nodes. The attacker is capable of stealing the key materials contained within the compromised node. Base stations are regarded as trustworthy in WSNs. Most researchers focus on secure routing between sensors and the between base stations. Attacks in sensor networks can be classified into the following types Fig.1 indicate the types of attacks.

Outsider Vs. insider attacks: Outsider attacks are attacks from nodes which do not belong to a WSN. Insider attacks occur when legitimate nodes of a WSN behave in unintended or unauthorized ways.

Passive Vs. active attacks: Passive attacks include eavesdropping on or monitoring packets exchanged with in a WSN. Active attacks involve some modifications of the data stream or the creation of a false stream.

Mote-class Vs. Laptop-class attacks: An adversary attacks a WSN by using a few nodes with similar capabilities to the network nodes in mote-class attacks. Mote class attackers can jam the radio link in it's immediate vicinity.

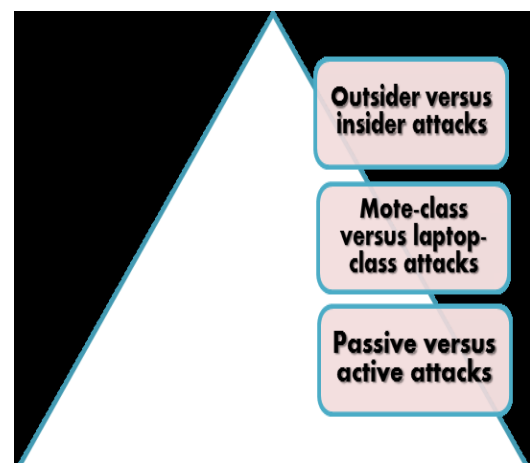


Figure 1: Attacks in WSN based on the capability of the attacker

As the wireless sensor networks are easily susceptible for various types of attacks, basically this paper focuses on Identity-based adversaries attacks [1] [2] [3] and the augmented and efficient techniques to secure from such attacks [4]. The existing technique involves the key computation cryptographic schemes, but such techniques are not always acceptable due to its key computation and extra overhead. Hence to enhance efficient security management this paper gives the innovative, improved and advanced technique to use the physical property based on Received Signal Strength. Received Signal Strength is the signal based non-cryptographic technique and physical property associated with each sensor node. The security technique based on advanced models such as GMFAD and CDAL-M used RSS and it doesn't require any additional improvement to the existing code. Also it is totally independent from the key based cryptographic technique, and hard to falsify. The objective which is find through the RSS-based security

techniques as like

- Detection of adversaries attack and number of adversaries attackers using GMFAD.
- Identified actual location of the attackers using the CDAL-M.
- Also Detects the Denial-Of-Service attack with location of attackers using GMFAD and CDAL-M model.

2. Existing Work

The existing approach makes use of cryptographic technique of Symmetric algorithm like either AES or 3-DES. Standard cryptographic technique are often too costly for the sensor network domain. Moreover, the distribution of shared secret keys poses another host of problems. This algorithm includes key distribution and management technique of overhead. Such cryptographic algorithms require a lot of efforts for reliable key management; further cryptography considers the Public Key Interface which can decrease the overhead of key management to some extent.

Cryptographic schemes requires reliable key distribution, management, and maintenance mechanisms also infrastructural, computational, and management overhead. These methods are susceptible to node compromise easily accessible and allowing their memory to be easily scanned[3] [4].

In wireless sensor network adversaries monitoring transmission medium and launch attacks with commonly available platform using the low cost wireless device Due to the openness of the wireless transmission medium, adversaries can monitor any transmission [3]. Existing survey presents the current state of affairs in the formulation of theoretical models for adversarial attacks in sensor networks and the different algorithmic remedies developed by the research community. Maxwell Young and Raouf Boutaba focus on jamming adversaries and Byzantine faults as these capture a wide range of benign faults as well as malicious attacks[4].

Further effort gives the hash technique and key revocation n key distribution implemented by Faria [5]. The detailed survey of attacks can be found in [6][7]. However due to limited facility on wireless devices and lacking of a fixed key management infrastructure in the wireless network, such cryptographic techniques are. This is what the cause that's why this paper makes use of newly advanced physical property associated with each node i.e. Received Signal Strength. Previously the RSS work was given by the Y Sheng and k Tan. He modeled the RSS readings using a Gaussian mixture model [12] and the Chen et al. used K-means cluster analysis and RSS to detect adversaries attacks. However, none of these approaches have the ability to determine the number of attackers when various adversaries use the same identity to launch attacks, which is the basis to further localize various adversaries after attack detection. Although Chen et al studied how to localize adversaries [10]; it can only handle the case of a single adversaries attacker and cannot localize the attacker if the adversary uses different transmission power levels.

3. Proposed Work

This paper has proposed mainly 2 models for detection and localization of Identity-based adversaries Attacks accordingly as like

3.1 Generalized Model For Attack Detection (GMFAD)

Basically this particular model mainly focuses on Detection of Identity based adversaries Attack for that purpose it consists of the new advanced technique is Partitioning around Medoids (PaM)[8]. As the adversaries attack detection could be performed by RSS-based spatial correlation from wireless sensor nodes. It also showed that the RSS readings from a wireless sensor node may fluctuate and should cluster together. In particular, the RSS readings over time from the similar physical location will belong to the similar cluster points in the n-dimensional signal space[9]. Also the RSS readings from different locations over time should form different clusters in signal space. The observation suggests that we may conduct cluster analysis on top of RSS-based spatial correlation so as to find out the distance in signal space and further identified the presence of Adversaries attackers in physical space[14]. In this work, we deploy the Partitioning around Medoids Method to perform clustering analysis in RSS.

3.1.1 Partitioning around Medoids

The according to PaM technique it consists of following mathematical steps:-

1. In the first step partition the RSS Vectors from the same node identity into 2 clusters.
2. Select the distance between two medoids as D_m .
3. Calculate $D_m = D_a - D_b$
4. If D_m is small

Then Adversaries Attack is not detected

5. Else if D_m is large

Then Adversaries Attack is detected.

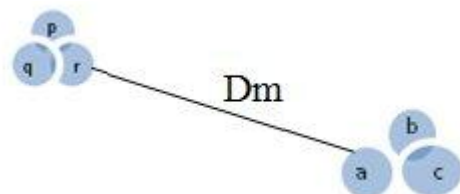


Figure 2: Distance between medoids.

In this way finally the objective to identified the presence of attacks should be done. Here M_a and M_b are the medoids of two clusters. Basically under normal conditions only one cluster from a single physical location. However, under a Adversaries attack, there is more than one node at different physical locations claiming the same node identity. As a result, more than one cluster will be formed in the signal space and D_m will be large as the medoids are obtained from the different RSS clusters associated with different locations in physical space.

3.1.2 System Evaluation

This technique is basically used for identified actual number of attackers in the wireless system. This method uses Twin-

Cluster Model[13]. It means this indicate that Twin-Cluster Model includes two closest clusters (e.g. clusters a and b) between K Potential clusters of a data set. Energy computation done by using twin cluster model. Mathematical model involve 2 types of energies—

1. Partition Energy ($E_p(K)$)
2. Merging Energy ($E_m(K)$)

The Partition Energy denotes the border distance between the twin clusters, whereas the Merging Energy is determined as the average distance between elements in the border region of the twin clusters. Here the border region includes a number of sample points chosen from clusters a and b that are nearest to its twin cluster than any other points within its own cluster. Then further equations of partition energy and merging energy denote. Where the value of K gives the actual number of Adversaries attackers in the system.

3.2 Coherent Detection and Localization Model (CDAL-M).

In this section, we present our integrated system that can use localize adversaries attackers. The experimental results are presented to evaluate the effectiveness of our approach, especially when attackers using different transmission power levels.

The conventional localization methods are based on averaged Received Signal Strength from each node identity inputs to estimate the position of a node. However, in wireless adversary attacks, the Received Signal Strength stream of a node identity may be mixed with Received Signal Strength readings of both the original node as well as attack nodes from different physical locations. The traditional method of averaging RSS readings cannot differentiate RSS readings from different locations and thus is not feasible for localizing adversaries.

Different from conventional localization approaches, our coherent detection and localization system utilizes the Received Signal Strength medoids as inputs to localization algorithms to estimate the positions of adversaries. The available positions from our system includes the location estimate of the original node and the attackers in the physical space. Here we use RADAR algorithm.

3.2.1 Radar Algorithm

The Radar-Gridded algorithm is expanded from scene-matching localization algorithm[11]. Here the proposed Radar-Gridded makes use of an interpolated signal map, which is built from a set of averaged RSS readings with known (X, Y) locations. From the observed RSS reading with an unknown location, Radar returns the x, y of the nearest neighbor in the signal map to the one to localize, where “nearest” is defined as the Euclidean distance of received signal strength points in an N-dimensional signal space, where N is the number of landmarks.

Further it makes use of Euclidean’s distance formula to obtain actual position (X, Y) co-ordinates of location. So gives the exact location of adversary attackers.

3.2.2 Bayesian networks

Bayesian Network localization is a multilateration algorithm. It encodes the signal-to-distance propagation model into the Bayesian Graphical Model for localization [15]. Fig. 3 shows the basic Bayesian Network. The vertices X and Y represent location and the vertex s_i is the received signal strength reading from the i th landmark. The vertex D_i represents the Euclidean distance between the location described by X and Y and the i th landmark. The value of s_i observe a signal propagation model $s_i = b_{0i} + b_{1i} \log D_i$, where b_{0i} , b_{1i} are the parameters specific to the i th landmark.

The distance depends on the location (X, Y) of the measured signal and the coordinates (x_i , y_i) of the i th landmark. The network models noise and described by modeling the s_i as a Gaussian distribution around the above propagation model.

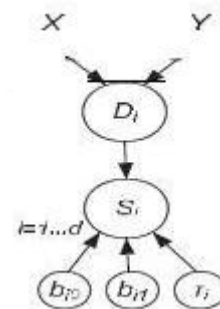


Figure 3: Bayesian graphical model

3.3 Detection of Denial of Service Attack

A denial-of-service (DoS) attack is an attempt to make a machine or network resource unavailable to its intended users. DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. Denial-of-service attacks are also common in business and responsible for website attacks.

In general terms, DoS attacks are implemented by either forcing the targeted computer to consuming its resources so that it can no longer provide its original service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

A denial-of-service attack may involve sending forged requests of some type to a very large number of nodes that will reply to the requests. Using Internet Protocol address attacks, the source address is set to that of the targeted victim, which means all the replies will go to the target.

The DSA Algorithm can be used further for detection of Denial of Service Attack.

Initially $i = \text{Request}$, $S = \text{Service}$;

1. For ($i=0$; $i \leq 2$; $i++$) a. $S++$
2. If ($i = \text{Infinity} \parallel \geq T$)
 // No response from Server $S = \text{NULL}$;
 // i.e. Denial of Service Attack is detected $D = \text{Attack Detected} = 1$;

// i.e. if attack is not detected D=0

3. Printf ("Dos attack is detected ");

This algorithm accurately detects the Denial of Service Attack. Experimental results show that this gives the efficient and effective way of Attack identification of type Denial of Service Attack.

4. Experimental Results and Comparison

Experimental results obtained from these models result into some effective graphs shows in Fig.5

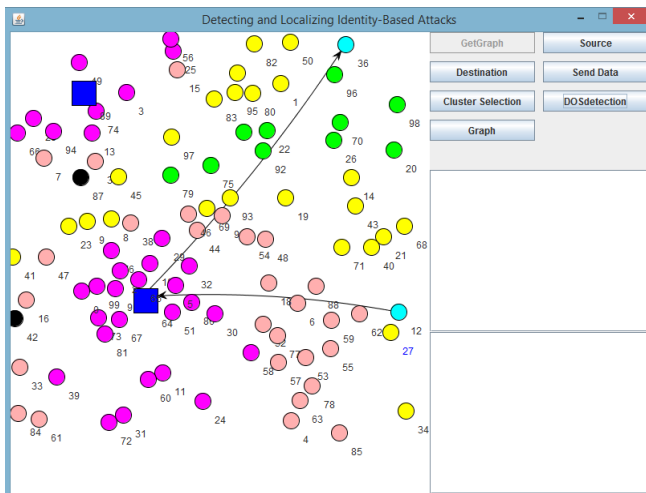


Figure 4: RSS based Cluster Selection

Also these techniques evaluated for Wi-Fi and Zigbee networks resulted into high detection rate as compared to previous approaches.

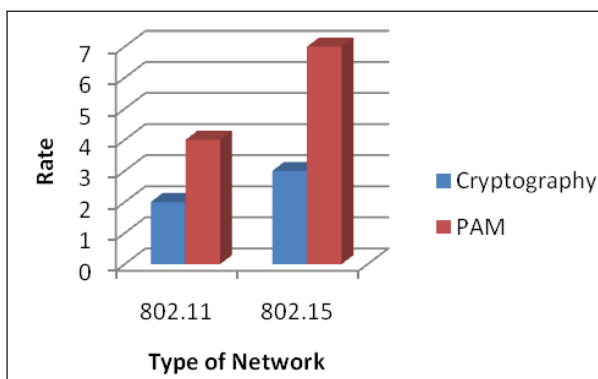


Figure 5: Graph for attack Detection Rate

Here the plotted graph indicates the Adversaries attack detection in both Previous and proposed techniques. The identification rate is higher in case of PAM (Partitioning around Medoids) showed that here the attacks are detected with more high speed as compared to previous one. Also the received signal strength based PAM needs less time than Cryptography hence it is more effective.

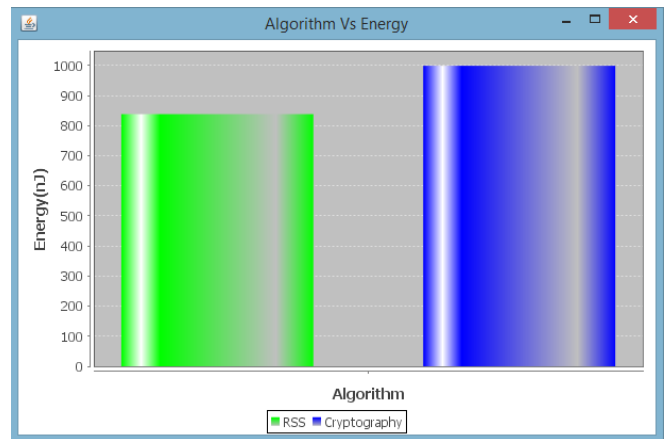


Figure 6: Algorithm Vs Energy Graph

Fig.6 shows the comparison among the energy consumption of each technique. Hence from the graph we come to the conclusion that RSS technique takes less time for all the computations than Cryptography.

5. Conclusion

Here we proposed to use GMFAD and CDAL-M model using Received signal strength (RSS) instead of previous approaches like Cryptography, so as to detect Identity-based Adversaries attacks and in advancement the Denial-of-Service attacks more effectively as compared to the existing one. Received signal strength it's a physical property associated with each node, which is hard to falsify and also not reliant on cryptography. Here we proposed PAM technique for Adversaries attack detection, further System Evaluation technique consist of twin-cluster model so as to obtain the exact number of adversaries attackers in the system (i.e.GMFAD) and also CDAL-M model to localize Adversaries attackers in the network. As enhancement here we also proposed algorithm to detect Denial-of-Service attack. Experimental results shows that all these proposed techniques are more efficient and effective than existing ones. Also that acceptably reduces the overhead requirements of existing approaches, as those proposed techniques don't require any additional implementations. Experimental result shows energy consumption and detection rate, additionally high accuracy of localizing multiple adversaries.

References

- [1] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and 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] Jie Yang, Yingying Chen, Wade Trappe and Jerry Cheng "Detection and Localization of Multiple Spoofing Attackers in Wireless Networks" IEEE Transactions on parallel and distributed systems, Vol. 24, No. 1, Jan 2013.
- [4] Yingying Chen, Member, IEEE, Jie Yang, Student Member, IEEE, Wade Trappe, Member, IEEE, and

- Richard P. Martin, Member, IEEE "Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks" IEEE Transactions vehicular technology, Vol. 59, No. 5, June 2010.
- [5] D. Faria and D. Cheriton, "Detecting Identity-Based Attacks in Wireless Networks Using Signalprints," Proc. ACM Workshop Wireless Security (WiSe), Sept. 2006.
- [6] 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.
- [7] 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
- [8] 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.
- [9] L. Kaufman and P.J. Rousseeuw, Finding Groups in Data: An Introduction to Cluster Analysis. Wiley Series in Probability and Statistics, 1990.
- [10] 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.
- [11] P. Bahl and V.N. Padmanabhan, "RADAR: An in-Building RF Based User Location and Tracking System," Proc. IEEE INFOCOM, 2000.
- [12] T. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, "A Survey of Various Propagation Models for Mobile Communication," IEEE Antennas and Propagation Magazine, vol. 45, no. 3, pp. 51-82, June 2003.
- [13] 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.
- [14] 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
- [15] 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.