A Novel Technique For Detection of Both Spoofing And Jamming Attack In Wireless Networks

Dhivya T[1], Kalaivani K[2]
[1, 2] Dept of Computer science and Engineering
[1, 2] E.G.S Pillay Engineering College, Nagapattinam, India

Abstract- *Wireless Networks consist of numerous small home nodes and power production or other sensor nodes that can collect, and disseminate information for the processing of information from the nodes. Several of these applications involve the communication of sensitive information that must be protected from unauthorized parties. Although the wireless network communications could be secured via standard cryptographic methods, the communication patterns alone leak contextual information, which refers to event-related parameters that are inferred without accessing the report contents. Under a global model, all communications within the wireless networks are assumed to be intercepted and collectively analyzed. State-of-the-art countermeasures conceal traffic associated to real events by injecting dummy packets according to a predefined distribution. In these methods, real transmissions take place by substituting scheduled dummy transmissions,which decorrelates the occurrence of an event from the eavesdropped traffic patterns. However, concealment of contextual information comes at the expense of high communication overhead and increased end-to-end delay for reporting events. In this paper, we propose a general traffic analysis method using Received Signal Strength (RSS) for inferring contextual information from jamming attacks and spoofing attacks. Our method is meant as a baseline for evaluating the performance of protection mechanisms with varying underlying assumptions. Therefore, it relies on minimal information, namely the packet interception times, attackers' locations.*

Keywords- eavesdropped traffic patterns, Received signal strength,jamming attacks, spoofing attacks.

I. INTRODUCTION

Wireless networks are deployed, they will increasingly become tempting targets for malicious attacks. Due to the openness of wireless and sensor networks, they are especially vulnerable to spoofing attacks where an attacker forges its identity to masquerade as another device, or even creates multiple illegitimate identities. Spoofing attacks are a serious threat as they represent a form of identity compromise and can facilitate a variety of traffic injection attacks, such as evil twin access point attacks. It is thus desirable to detect the presence of spoofing and eliminate them from the network.

The traditional approach to address spoofing attacks is to apply cryptographic authentication. However, authentication requires additional infrastructural overhead and computational power associated with distributing, and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication. In addition, key management often incurs significant human management costs on the network.

In this paper, we take 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 and sensor nodes.Due to the shared nature of the wireless medium, attackers can gather useful identity information during passive monitoring and further utilize the identity information to launch identity-based attacks, in particular, the two most harmful but easy to launch attacks: 1) spoofing attacks and 2) Sybil attacks.

In identity-based spoofing attacks, an attacker can forge its identity to masquerade as another device or even create multiple illegitimate identities in the networks. For instance, in an IEEE 802.11 network, it is easy for an attacker to modify its Media Access Control (MAC) address of network interface card (NIC) to another device through vendor-supplied NIC drivers or open-source NIC drivers. In addition, by masquerading as an authorized wireless access point (AP) or an authorized client, an attacker can launch denial-of-service (DoS) attacks, bypass access control mechanisms, or falsely advertise services to wireless clients.

Therefore, identity-based attacks will have a serious impact to the normal operation of wireless and sensor networks. It is thus desirable to detect the presence of identity-

based attacks and eliminate them from the network. The traditional approach to address identity-based attacks is to apply cryptographic authentication.

However, authentication requires additional infrastructural overhead and computational power associated with distributing and maintaining cryptographic keys. Due to the limited power and resources available to the wireless devices and sensor nodes, it is not always possible to deploy authentication.

A. Overview of Spoofing Attacks

Due to the wireless medium nature, attackers can gain the useful identity information during passive monitoring.Attackers utilize the identity information to provide identity based spoofing attacks in wireless and sensor networks. For instance, in an 802.11 network, it is easy for a wireless device to acquire a valid MAC address and masquerade as another device. The IEEE 802.11 protocol suite provides insufficient identity verification during message exchange, including most control and management frames. Therefore, the adversary can request various services as if it were another user. Identity-based spoofing attacks are a serious threat in the network, because they represent a form of identity compromise and can facilitate a series of traffic injection attacks, including spoofing-based attacks.

An adversary can provide the authentication attack.If theclient chooses an AP for communication, client must authenticate itself to the AP before the communication session starts. The client and the AP are allowed to request thedeauthentication explicitly in order to avoid the existing authentication relationship with each other. Unfortunately, this de authentication message is not authenticated. Therefore, an attacker can gain this de authentication message, either on behalf of the client or on behalf of the AP. The adversary can completely prevent the client from transmitting or receiving by means of repeating this attack.

Furthermore, an attacker can utilize spoofing attack identity and provide the rogue AP attack against the wireless network. In the rogue AP attack, the adversary first sets up a rogue AP with the same MAC address and service set identifier as the legitimate AP but with a stronger signal. When a station enters the rogue AP coverage, it automatically associate with the rogue AP because of default network configuration, which has a stronger signal. Then, the adversary may involve in order toinfluence the communi-cation. For example, it can direct false traffic to the associated station or drop the requests made by the station. The adversary can performmore flooding attacks on APs by means of using spoofing identity, such as probe request, authentication request, and association request flooding attacks.

B. Overview of Jamming Attacks

Jamming is defined as the emission of radio signals aiming at disturbing the transceivers' operation [5]. The main difference between jamming and radio frequency interference (RFI) is that the former is intentional and against a specific target while the latter is unintentional, as a result of nearby transmitters that transmit in the same or very close frequencies (for instance, the coexistence of multiple WSNs on the same area using the same frequency channel may result in RFI). The key point in successful jamming attacks is Signal-toNoise Ratio (SNR), SNR= Psignal/Pnoise, where P is the average power. Noise simply represents the undesirable accidental fluctuation of electromagnetic spectrum, collected by the antenna. Jamming can be considered effective if SNR< 1. Existing jamming methods are described below.

Spot Jamming: The most popular jamming method is the spot jamming wherein the attacker directs all its transmitting power on a single frequency that the target uses with the same modulation and enough power to override the original signal. Spot jamming is usually very powerful, but since it jams a single frequency each time it may be easily avoided by changing to another frequency.

Sweep Jamming: In sweep jamming a jammer's full power shifts rapidly from one frequency to another. While this method of jamming has the advantage of being able to jam multiple frequencies in quick succession, it does not affect them all at the same time, and thus limits the effectiveness of this type of jamming. However, in a WSN environment, it is likely to cause considerable packet loss and retransmissions and, thereby, consume valuable energy resources.

Barrage Jamming: In barrage jamming a range of frequencies is jammed at the same time. Its main advantage is that it is able to jam multiple frequencies at once with enough power to decrease the SNR of the enemy receivers. However as the range of the jammed frequencies grows bigger the output power of the jamming is reduced proportionally.

Deceptive Jamming: Deceptive jamming can be applied in a single frequency or in a set of frequencies and is used when the adversary wishes not to reveal her existence. By flooding the WSN with fake data she can deceive the network's defensive mechanisms (if any) and complete her task without leaving any traces.

Deceptive jamming is a very dangerous type of attack as it cannot be easily detected and has the potential to flood the PE with useless or fake data that will mislead the WSN's operator and occupy the available bandwidth used by legitimate nodes.

C. Overview of Attack Detector

Received Signal Strength is widely available in deployed wireless communication networks, and its values are closely correlated with location in physical space. In addition, RSS is a common physical property used by a widely diverse set of localization algorithms. In spite of its several-meter-level localization accuracy, using RSS is an attractive approach, because it can reuse the existing wireless infrastructure, and it is sufficient to meet the accuracy requirement of most applications. For example, during health care monitoring, a doctor may only need to know in which room the tracked patient resides.

Although affected by random noise, environmental bias, and multipath effects, the RSS measured at a set of landmarks (i.e., reference points with known locations) is closely related to the transmitter's physical location and is governed by the distance to the landmarks. The RSS readings at different locations in physical space are distinctive.

D. Overview Of Localising Adversaries

If the spoofing attack detector detects the spoofing attack, we need to localize the adversaries and to eliminate the attackers from the network. We propose a real-time localization system that can be used in order to detect the location of the attackers.We have developed a general-purpose localization system to perform real-time indoor positioning. This system is designed with fully distributed functionality and easy to plug-in localization algorithms. It is built around 4 logical components: Transmitter, Landmark, Server, and Solver.

Transmitter: Transmitter transmits the packets can be localized. Often the application code need not to be altered on a sensor node in order to localize it.

Landmark: The Landmark component tracks the packet traffic and taken the RSS reading for each transmitter.

Then the RSS information is transmitted to the Server component. The Landmark is stateless component and is to access point with known locations.

Server:The Server component detects the spoofing attack and also it collects RSS reading from all the Landmark components. The Server calculates averaging or clustering by summarizing the RSS information, then forwards the information from Server component to the Solver component in order to estimate the localization.

Solver: A Solver component receives the input from the Server component.

Solverdetect the localization by means of using the localization algorithms and then sends the localization results back to the Server. There are multiple Solver can localize multiple transmitters simultaneously.

II. RELATED WORK

The problem of protecting the contextual information privacy has been studied under various scenarios. Threat models can be classified based on the adversary's network view (local vs. global) or the capabilities of the eavesdropping devices (packet decoding, localization of the transmission source, etc.). Eavesdroppers are assumed to intercept only a fraction of the WSN traffic under a local model. Hiding methods include adding of false-sources, random walks and pseudo-destinations, creation of routing loops, and flooding. These methods can provide few probability guarantees, because eavesdroppers locations are unknown. All communications within the WSN are assumed to be intercepted and collectively analysed under a global model.

In [20] the author proposed a random routing scheme (RRS) is proposed to provide path diversity. we combine dummy packet injection scheme (DPIS) and RRS with a in order to confuse the adversary. Finally, an anonymous communication scheme is proposed to hide theall nodes identity whichparticipate in packets transmission. Through the analysis of security and performance, we can see our proposed scheme can effectively prevent the traffic analysis attacks, and has the less delivery time and energy consumption.

In [16] the author proposed the novel approach.Because of tremendous usage of these technologies comes at the price of location privacy, Itobserving the communication patterns or the interface identifiers. The author describes a novel approach to location privacy at the link layer level. Used in conjunction with a pseudonym mechanism to prevent tracking by active communicating peers, which could be an interesting new direction for our work. Nevertheless, our approach provides privacy at the link layer without significantly undermining the performance of the network

In [21] the author proposed Source-Location Privacy While developing and evaluating our privacy-aware routing protocols, we jointly consider issues of location-privacy as well as the amount of energy consumed by the sensor network. By the observations, we propose a flexible routing strategy known as phantom routing. It protects the source's location. Investigations have shown that phantom routing is a powerful technique for protecting the location of the source during sensor transmissions

III. METHODOLOGY

Consider a network that consists of a source S, a destination D and a set of N trusted nodes S_N={1,. . .N}The source could be an independent node or an element of SN . The main objective of the nodes in SN is to send the information from the source to the destination. However, they can also cause interference to overhearing attacks by an eavesdropper, denoted by E. Links between the source and the destination as well as between the source and the eavesdropper are not considered; the direct links could be in deep shadowing or the destination and the eavesdropper could be outside the coverage area of the source.Source sends the message todestination.

E will tries to eavesdropping the confidential messages and also tries to jamming the process. In order to understand the concept consider a wireless network sends the confidential message from transmitter T to destination D. Eavesdroppers tries to eavesdrop the confidential messages and also tries to jamming the process as show in figure 2. At D accoding to its wiretap channel power gain channel.

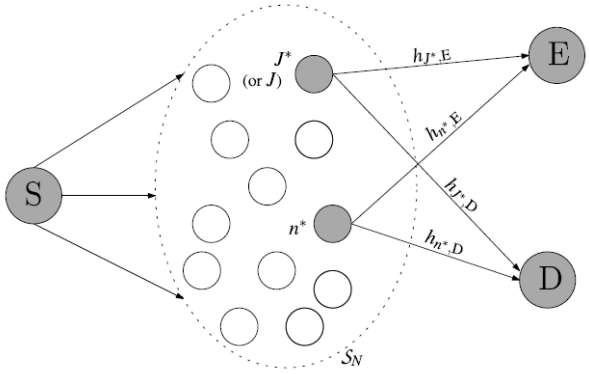

Fig. 1. Block diagram of the eavesdroppers attack

When the power gain is greater than a current thereshold it will eavesdrop the transmission T.Otherwise it will jam D to make T retransmit the confidential messages.the confidential messages is being retransmitted.

The eavesdroppers strategy can be summarised as follows

gte≥ ρ, Eavesdropping strategy
gte<ρ, Jamming strategy

wheregte is the channel power gain between T and E, and is a preset threshold that is determined by E in advance. Inorder to protect the confidential messages, D will adopt the Received Signal Strength method to detect E's action, and R will cooperate with legitimate user according to the detection results.

There are four possibilities states for eavesdropping attacks (i) the eavesdropper is jamming and correctly detected; (ii) the eavesdropper is eavesdropping and correctly detected; (iii) the eavesdropper is jamming and detected as eavesdropping action; and (iv) the eavesdropper is eavesdropping and detected as jamming action.

Received Signal Strength is calculated for each nodes. Eavesdroppers is detected by comparing Received Signal Strength of each node.

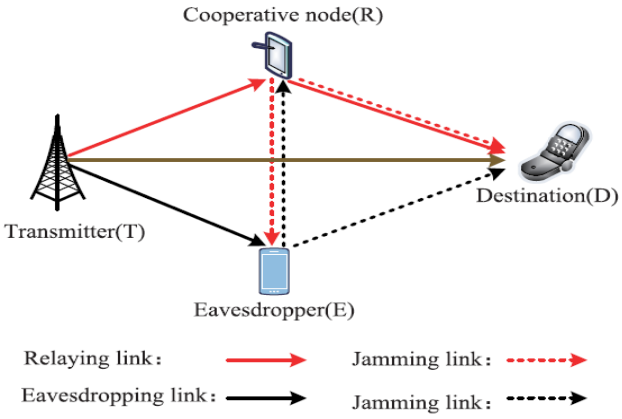

Fig. 2. The system diagram of our proposed secure communication scheme. The red line and the red dotted line denote the relaying link and jamming link of the cooperative node, respectively. The black line and the black dotted line denote the eavesdropping link and jamming attack link of the jamming-aided eavesdropper, respectively.

A. Received Signal Strength(RSS) Estimation

RSS is one of the types of localization algorithm.RSSThe RSS (Received Signal Strength) sometimes referred to RSSI (Received signal strength indicator). RSS is a measurement of the power present in a received radio signal.The RSS values are measured in dBm and have typical negative values ranging between 0 dBm (excellent signal) and -110 dBm (extremely poor signal). Measurement that is

ubiquitous in wireless systems is RSS. RSS based localization systems are less accurate than ToA based localization systems, but it can be implemented with little to no modication to existing systems. Specifically, received signal strength readings are obtainable in almost every wireless system without any extra hardware. Similar to ToA, in RSS, the user locates itself by receiving the signal from multiple access points. However, instead of measuring the ToA user computes the strength of the received signal. In RSS measurements the received signal strength represents the distance between the user and access point. Path loss model for the RSS measurements can be expressed as

$$R_i = R_o 10n^{\log \frac{di}{d}} \quad (1)$$

R_i is proportional to the received signal power (in dBm).R_O is the radiated power of the source (in dBm).d_i is the distance between the i^{th} receiver and the source.d is a reference distance.n is the path loss exponent (n=2 for free space propagation).Assuming that the signal strength and channel characteristics are known, three access points are required to locate a user in 2-dimensional space.

In the localization system used, the transmitted source power is unknown as well as the path loss index. As the equation above implies, the received power or equivalently the received signal strength, can be converted into distance. To overcome the problem of unknown parameters, a linear approximation is used. It is worth mentioning here that the performance of the RSS algorithm is very low when the geometric conditions are poor yielding an estimation error that becomes very large, especially at corners[14].

The algorithm executed as follows:

(i) initially assume a plausible path-loss index (e.g. n = 2, free space propagation).
(ii) Calculate the received power ratios at any two nodes to find the locus of possible source location.
(iii) establish an initial estimate of source location using intersecting loci from all measurements nodepairs.
(iv) calculate an improved estimate of source location using pairs of nodes corresponding to paths with nearly equal n. If necessary, iterate to converge on a final location estimate.

In Fig. 3 the flowchart of the algorithm is drawn

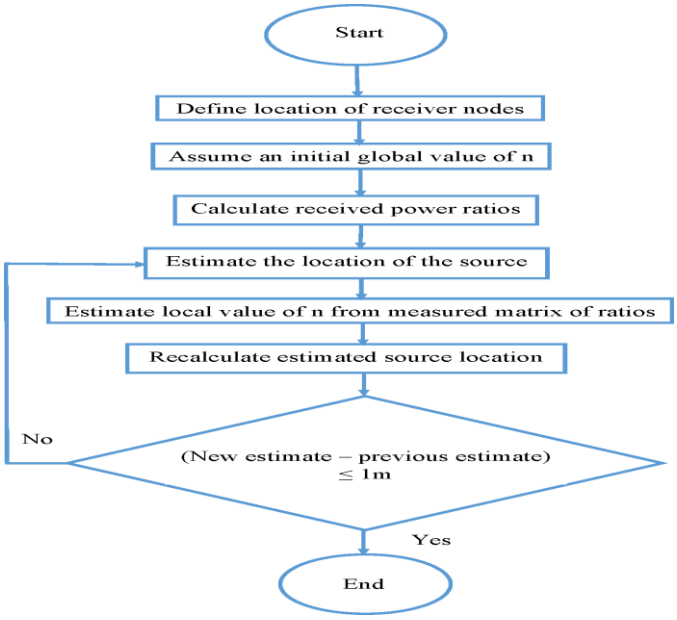

Fig. 2. Flowchart of the algorithm

In a noisy environment, the error should be less than 1 m between successive location to stop the algorithm. The main challenge is to optimize the value of the path loss exponent n for each path.

During the confidential message transmission,signal may be loss due to the noise.There is some path loss occurs during the transmission.It may varies slightly according to the enviroments.

IV. SYSTEM MODEL

Localization system used SILENCE as inputs to localization algorithms to estimate the positions of adversaries. The return positions from our system include the location estimate of the original node and the attackers in the physical space.

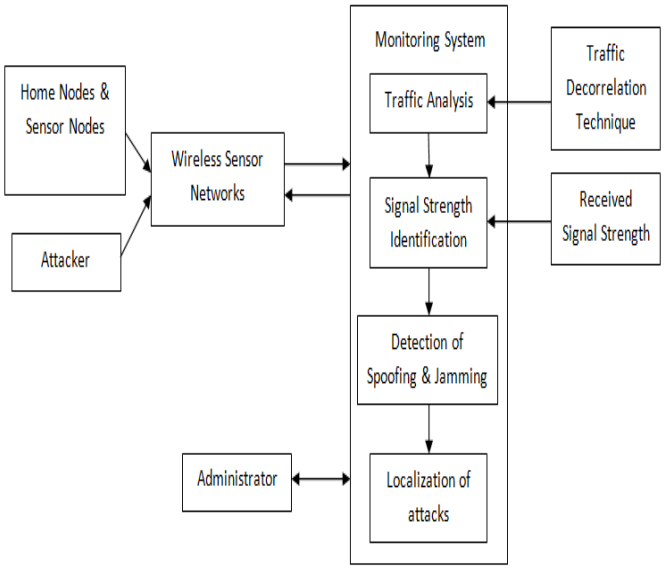

Fig. 3. System Architecture

We proposed the received signal strength based spatial correlation method, wireless device physical property is difficult to find and not useful for cryptography as the basis for detecting spoofing and jamming attacks in wireless networks.

Using received signal strength (RSS)-based spatial correlation, It is used to detect the both jamming and spoofing attacks. We need to find out theattackers different locations. Spatial information is used to detect the spoofing attacks has the unique power to not only identify the presence of these attacks but also localize adversaries. An advantage of using spatial correlation to detect spoofing attacks is that it will not require any additional cost or modification to the wireless devices themselves. Analysis showed that the RSS readings from a wireless node may cluster and fluctuate together.

Our approach can detect the presence of attacks and spoofing the same node identity. We can localize any number of attackers and eliminate them. The main challenging problem is determining the number of adversaries. We propose to use the spatial correlation of received signal strength (RSS) inherited from wireless nodes to detect both the spoofing and jamming attacks. Cluster-based mechanisms are developed to determine the number of attackers. The Support Vector Machines (SVM) method is also used if the training data is available. And it improves the accuracy of determining the number of attackers. We developed an localization system and integrated detection can localize the positions of multiple attackers.

The attacker and the victim are using the same ID to transmit data packets under the spoofing attack. The RSS readings of that ID is the mixture readings measured from each individual node (i.e., victim nodeor spoofing node). The RSS readings from the victim node and the spoofing and jamming attackers are mixed together under a spoofing attack. This observation suggests that analysis on top of RSS-based spatial correlation detect the presence of spoofing attackers in physical space and also find out the distance in signal space . The Partitioning around Medoids Method is used too 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.

V. CONCLUSION

In this paper, Received signal strength based spatial correlation method is used.RSS is used to detecting spoofing attacks in wireless networks. It provided theoretical analysis of using the spatial correlation of RSS inherited from wireless nodes for attack detection. It derived the test statistic based on the cluster analysis of RSS readings. Our approach can detect the presence of attacks as well as determine the number of adversaries, spoofing the same node identity, so that we can localize any number of attackers and eliminate them. It is difficult to detect the number of adversaries and it is one of the main challenging problem. The system developed with 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 such as Silhouette Plot and System Evolution that uses the cluster analysis method. Additionally, when the training data are available, we explored using Support Vector Machines-based mechanism to further improve the accuracy of determining the number of attackers present in the system.

REFERENCES

[1] V. C. C. Güngör and G. P. Hancke, “Industrial wireless sensor networks: Challenges, design principles, and technical approaches,” IEEE Trans. Ind. Electron., vol. 56, no. 10, pp. 4258–4265, Oct. 2009.

[2] W. Jiang, T. Kaiser, and A. J. H. Vinck, “A robust opportunistic relaying strategy for co-operative wireless communications,” IEEE Trans. Wire-less Commun., vol. 15, no. 4, pp. 2642–2655, Apr. 2016.

[3] A. Bletsas, A. Khisti, D. P. Reed, and A. Lippman, “A simple Cooper-ative diversity method based on network path selection,” IEEE J. Sel. Areas Commun., vol. 24, no. 3, pp. 659–672, Mar. 2006.

[4] J. Luo, J. Hu, D. Wu, and R. Li, “Opportunistic routing algorithm for relay node selection in wireless sensor

networks," IEEE Trans. Ind. Informat., vol. 11, no. 1, pp. 112–121, Feb. 2015.

[5] R. Madan, N. B. Mehta, A. F. Molisch, and J. Zhang, "Energy-efficient cooperative relaying over fading channels with simple relay selection," IEEE Trans. Wireless Commun., vol. 7, no. 8, pp. 3013–3025, Aug. 2008.

[6] J. Niu, L. Cheng, Y. Gu, L. Shu, and S. K. Das, "R3E: Reliable reactive routing enhancement for wireless sensor networks," IEEE Trans. Ind. Informat., vol. 10, no. 1, pp. 784–794, Feb. 2014.

[7] Z. Iqbal, K. Kim, and H.-N. Lee, "A cooperative wireless sensor network for indoor industrial monitoring," IEEE Trans. Ind. Informat., vol. 13, no. 2, pp. 482–491, Apr. 2017.

[8] I. Guvenc and C.-C. Chong, ``A survey on TOA based wireless localization and NLOS mitigation techniques," IEEE Commun. Surveys Tuts., vol. 11, no. 3, pp. 107_124, 3rd Qaurt., 2009.

[9] Y. Gu, A. Lo, and I. Niemegeers, ``A survey of indoor positioning systems for wireless personal networks," IEEE Commun. Surveys Tuts., vol. 11, no. 1, pp. 13_32, 3rd Qaurt., 2009.

[10] C. Nerguizian, C. Despins, and S. Affes, ``Geolocation in mines with an impulse response _ngerprinting technique and neural networks," IEEE Trans. Wireless Commun., vol. 5, no. 3, pp. 603_611, Mar. 2006.

[11] R. Barton, R. Zheng, S. Gezici, and V. Veeravalli, ``Signal processing for location estimation and tracking in wireless environments," EURASIP J. Adv. Signal Process., vol. 2008, p. 140, Jan. 2008. [Online].Available:https://www.hindawi.com/journals/misy/2016/7043235/

[12] G.Wang and K. Yang, ``A new approach to sensor node localization using RSS measurements in wireless sensor networks," IEEE Trans. Wireless Commun., vol. 10, no. 5, pp. 1389_1395, May 2011.

[13] L. Lazos and R. Poovendran, ``HiRLoc: High-resolution robust localization for wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 233_246, Feb. 2006.

[14] Y. Xu, Z. Jianguo and P. Zhang. "RSS-based source localization when path-loss model parameters are unknown." IEEE Communications Letters vol. 18, no 6, pp.1055-1058, 2014.

[15] F. Buckley and M. Lewinter, A Friendly Introduction to Graph Theory,1st ed. Prentice Hall, 2002.

[16] F. Armknecht, J. Girao and A. Matos, "Who said that? Privacy at link layer", IEEE International Conference on Computer Communications, pp. 0743-166X, may 2007.

[17] D. Niculescu and B. Nath, ``DV based positioning in ad hoc networks," J. Telecommun. Syst., vol. 22, pp. 265_280, Jan. 2003.

[18] Y. Shang and W. Ruml, ``Improved MDS-based localization," in Proc. IEEE Int. Conf. Computer Commun. (INFOCOM), Hong Kong, Mar. 2004, pp. 2640_2651.

[19] Y. Shang,W. Ruml, Y. Zhang, and M. Fromherz, ``Localization from mere connectivity," in Proc. ACM Mobihoc, Annapolis, MD, USA, Jun. 2003, pp. 201_212.

[20] P. Bahl, N. Padmanabhan, and V. Radar, ``An in-building RF based user location and tracking system," in Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM), Tel Aviv, Israel, Mar. 2000, pp. 775_784.

[21] Xi Luo, XuJi AND Myong-Soon ParkLocation Privacyagainst Traffic Analysis Attacks in Wireless Sensor Networks, IEEE Commun. Lett, pp. 2162-9048 June 2010.