ISSN: **1992-8645** www.jatit.org E-ISSN: **1817-3195**

A SURVEY AND OPEN ISSUES OF JAMMER LOCALIZATION TECHNIQUES IN WIRELESS SENSOR NETWORKS

[1,2]AHMED ABDULQADER HUSSEIN, [1]THAREK A. RAHMAN, [1]CHEE YEN LEOW

[1] Wireless Communication Centre (WCC), Faculty of Electrical Engineering, Universiti Teknologi Malaysia, UTM Skudai, Johor 81310, Malaysia

[2] University of Technology,Baghdad,Iraq

E-mail: ahmedabdulqaderhussein@gmail.com , tharek@fke.utm.my, bruceleow@fke.utm.my

ABSTRACT

Jamming sensor attacks localization is a significant area that acquires considerable research interest. This interest is expected to grow further with the prolifiration of wireless sensor network applications due to the physical share environment. Jamming attacks emitting a radio frequency signals by the adversaries and impact the wireless sensor network localization tactic. Also the jamming attacks are discovering swiftly techniques in a wide range of the intrusion in the wireless sensor network communications . Meanwhile the detection and localization of the jammer is being absolutely indispensable concern. This paper provides an overview of the jammer sensor localization techniques in wireless sensor networks and analyze the challenges in this field. The survey targets an important but mostly untouched open research issues in the future works .

Keywords: *Wireless Sensor Networks (WSNs), Jamming Attacks, Jammer Sensor Localization Technique.*

1. INTRODUCTION

The wireless sensor network localization is done by using different mechanisms like RSS, TOA, AOA, hop count . Most of these methods base on the wireless system's physical properties[1]. As more location based services getting deployed, there are a growing number of malicious attacks on the localization schemes. Most of attacks aim to affect the localization process so that the applications will be severely affected. Location infrastructure is subjected to various attacks from conventional to physical attacks [2],[3],[4].

Jamming attacks can be launched on these approches by merly causing signal attenuation or cutting the transmission path . The attacks results have a great deviations on the estimation of the wireless sensor network location values lead to a bigger measurement errors, due to these errors the application built on localization is affected. Jamming attacks can be inject a false messages or signals in the network on the grounds that of the share medium transmission . for example the jammer can emit signals to disrupt the communication between the transmitter and the target.

Radio interference attacks can be easily launched on wireless sensor network because of its shared nature of medium. An adversary continuously transmits on the wireless channel and disrupts the localization services. The intrusion with an appropriate wireless communication systems is the main goal of the jamming sensor attacks. Many types of these attacks are possible in the wireless networks. Localization methods using range based methods like RSS is severely affected by jamming attacks. The jammer transmits radio waves to the sensor and makes the distance method erroneous which relies on signal from the known anchors for RSS measurement [1], [5].

Definitely the detection and localizing the jammers plays an important key role in all the applications of the wireless sensor networks localization , so that the relevant literatures which have been selected in this work emphasizes on this significant topic only by analyzing the main characteristics and the drawbacks also for the jammer localization techniques. In addition, the previous review papers related to the wireless sensor networks under jamming attacks are focused in the direction of the jamming attacks defense and countermeasures strategies [6],[7],[8]. While the difference in our work is relied on the localizing the jammer in the network.

The essential criteria that have been adopted in this work for a comparison between approved studies are discussed according to the localization accuracy , network nodes density and the jammer transmission ranges. In the other side these works have been categorized into groups based on their mechanisms.

The main contribution of this paper is to explore the jammer sensor localization techniques through analyzing the current works interesting in this area and identify the challenges and the open research issues related to the localization of wireless sensor networks in the presence of jamming attacks , this issue is clearly highlighted in this survey.

2. SECURITY THREATS IN WIRELESS SENSOR NETWORKS

There are many attacks that have been specified by the researchers in wireless sensor networks . These security attacks can be categorized into several standards such as attack's domain and the technique that has been used . Consequently there are several kinds of attacks based on the goal and the nature of these attackers [9],[10] , the general significant classes can be summarized as:

2.1 Active and Passive Attacks

The attack classification of this kind is stand on r the damage level or access level for the wireless sensor network link layer. Active attacks comprise disturbance of the network activity such as obstruction , adjustment or innovation . Also this attack can be inserting erroneous informations into the wireless sensor network, jamming , replay message impersonating and run down the network.
While passive attacks comprise network information interchange without any communication obstruction, therefore this kind of attacks perform blockage , traffic monitoring and analysis .It is behaving as an ordinary node to eavesdrop , collect and steal information from the wireless networks so that it is normally used against privacy [11],[12].

2.2 External and Internal Attacks

This kind is based on the location of the attacker . It can be diffused either inside or outside the network. External attacks can be achieved by a node that are not within the wireless network transmission range , it can be launched attacks even without becoming authenticated , jamming the whole communication of the wireless sensor network and triggering Denial of Service attacks.In the other hand , Internal attacks are the major provocation in wireless sensor networks. It is diffused from inside the wireless network domain and can be access to all other sensor nodes placed within it's transmission ranges , including the access to the cryptography keys or other wireless sensor network codes and detecting the secret keys. Meanwhile internal attacks have a cruel effect in comparison with the external attacks through the knowledge of the secret and worthy information [13].

2.3 Mote Class versus Laptop Class Attacks

This kind of attack is based on the attacking devices and it can be employ several devices with various power , radio antenna and other abilities in order to attack the wireless sensor networks.

Mote class attacks the wireless sensor network by an adversary through a little number of nodes with the same functionalities that as of the network sensor nodes and it is happening from the internal domain of the wireless network . The aim of this attacker is to jam the radio link also stealing and get the access of the cryptography keys. While laptop class is an adversary using extra powerful devices like laptop , thus it can be get the access to a wide range of bandwidth with low passively communication channel and can be insert severe attacks into the network which will leads to severe damage [14] .

2.4 Stealthy Attacks versus Service Integrity

The main aim of this attacks is to infiltrate into the communication channel and inject a false information through the wireless sensor network.The most significant effect of this kind of attacks is the entire degradation also interruption of the functionalities and services of the wireless sensor networks [15].

2.5 Network Availability Attacks

Most of the research on this topic is revolved around security solutions using the layered approach. The layered approach is shown in the Figure 1. In layered approach the protocol stacks contains of the physical , data link , network , transport and application layers. These five layers and the three planes, i.e., the power management plane, mobility management plane and task management plane jointly forms the wireless layered architecture. The physical layer forms the hardware layer of the wireless communication path.

The transmission and reception of the signal are the responsibility of the physical layer. The next layer the data link layer takes care of the media access control MAC protocol which in turn manages communication over noisy channels. Network layer manages the data routing, and transport layer maintains the data flow. The application layer interacts with the final user [9].

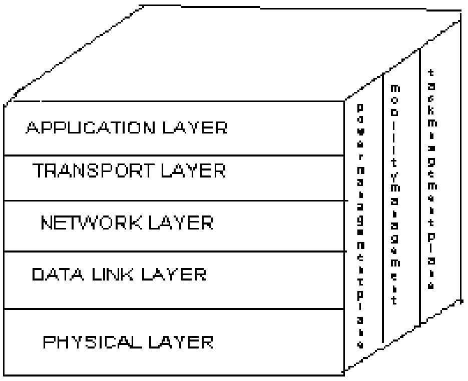

Figure 1. Layers Protocol architecture

The network availability attacks are usually indicated as a Denial of Service (DoS) attacks, which is going to make the wireless network unavailable , corrupt or disorder the network performance .Usually it can targets one of each layer of the open system interconnection (OSI) layer of the sensor network . Table 1 summarizes the threats on each layer [16].

Table 1 : Attacks types on the wireless sensor network

Layer	Attacks
Physical Layer	Jamming , Tampering
Data Link Layer	Jamming , Collision
Network Layer	Spoofing or replaying information, Selective forwarding or black holes, Sink holes, Sybil attacks, Node replication attacks, Wormholes Flooding, Attacks against privacy
Transport Layer	Injects false messages , Energy drain attacks
Application Layer	Attacks on reliability

layers.

3. PHYSICAL LAYER JAMMING ATTACKS

Definitely the RF signal transmission is used by most of the wireless communications. The broadcasting of a wireless signal over the channel can be absolutely blocked the receivers that are matched to the appropriate frequencies. Thus , the transmitted signal can be eavesdroped and a false messages can be inserted to the network . Jamming or interference can be targeting the radio signals lead to distort or lose the message . Therefore the generated signal for the powerful attacker's transmitter can easily overcome the target's signal and prevent the communication. Whereas the selection and generation of the carrier frequency , signal detection , modulation and encryption of the data are the main tasks of the physical layer in wireless sensor networks [17], and the jamming attacks have the access ability for the physical radio medium , so that it will be the real hazard for the sensor nodes expanded in a hesitant and risky environment[18] ,[19]. Figure 2. illustrate the sensor nodes in the jamming area that examine various degrees of jamming attacks [20].

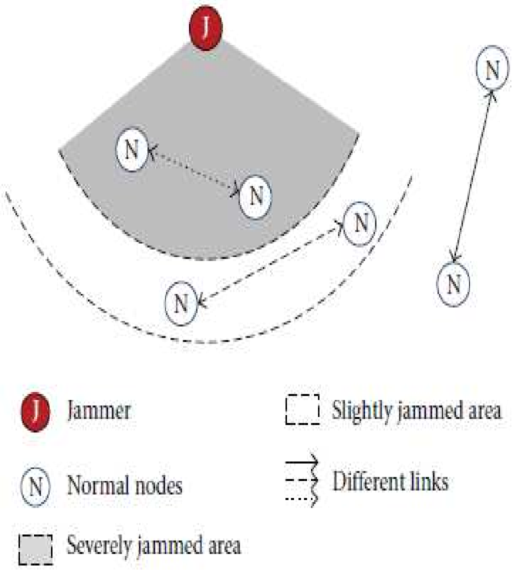

Figure 2. Illustration Of Varying Jamming Effects On Different Nodes.

4. JAMMING ATTACKS STRATEGIES

The jamming is a common type of the physical layer attacks , it can be disrupt the transmission communication opportunity. Therefore the main goal of the jamming attacks is to insert severe intervention to occupy the channels and miss the chances for the sensor nodes to communicate . Based on the jamming methods jammers are classified into following types [21], [22], [23].

- **Constant Jammer**: This kind of jammers continuously emits a radio signal.

- **Deceptive Jammer**: This type of jammers insert a typical packets continually into the transmission channel without any gap among these packets . As a consequence , an ordinary communication will be duped and trusting that there is an appropraite packets so that it will cheating the receiver to continue receive these fake packets.

- **Random Jammer**: This kind of jammers continuously alternate between jamming and sleep cycle. The operation of this jammers is to inject a packets into the channel for a certain time tj after that it will switched off it's radio and sleep for a time ts .

- **Reactive Jammer**: This kind of jammers remains silent through the idle status of the channel and will sending packets directly after the sensing of the channel activity .

5. RELATED WORK

There are many different works using a various techniques have been proposed to deal with the effect of the jammers in the wireless sensor networks through localizing the jammer in order to overcome it's effect. These different techniques are summarized into groups depend on their strategies as follow:

5.1 Network Topology Information Based Localization

A centroide based localization scheme that stratify centroide localization (CL) and weighted centroide localization (WCL) has been exploited to determine the jammer location [24]. (CL) achieves the location estimation without the collaboration of the victim nodes by using all neighboring nodes location information located within the transmission range of the targeted nodes. Hence this algorithm gather and average the jammed node coordinates in order to evaluate the jammer position , also this algorithm is powerful versus the environment propagation uncertainties but the accuracy of this algorithm is low and extremly sensitive to the jammed nodes distribution in the network. (WCL) is a consolidation form of (CL) . It performs improvement in the estimated position of the jammer than (CL) , it is also sensitive to the jammed nodes distribution and it needs all the jammed nodes to handover it's received signal strength RSS readings out of the jammed area. Meanwhile a development of a novel scheme , Virtual Force Iterative Localization (VFIL) algorithm [10] has been proposed to find the jammer location iteratively. This work uses the network topology information to get the approximate location of the jammer.This algorithm shows a high accuracy with less sensitive to the nodes density in the network and too much computation overhead than (CL) and (WCL) algorithms.

Z. Liu *etal* [25] proposed a hearing range based localization algorithm based on least square approch (LSQ) that exploits the network topology changes induced by jammer to evaluate it's position . This algorithm has a lower computational cost , one step instead of iterative search with a higher accuracy for localizing the jammer than VFIL algorithm. In addition this work depends on the noise level bounding (NLB) to localize the jammer accurately and it is not sensitive to the network node density . Finally this approach will fail if there is a multiple jammers or if a reactive jamming is present.

A non-iterative adaptive (LSQ) algorithm to localize a jammer has been presented in [26], this work takes the advantage of schedule differences for the node's neighbor which is induced by the jamming attacks . This work requires each node must be knows its neighbors so that if a random distribution is used for the sensor nodes in the network region, the neighbor list at each node is not possible to be kept.This algorithm is sensitive to the network node density and the changes of the hearing ranges induced by the jammer are too important .This work tests the challenges of the localization in a real system by taking into consideration the log normal shodowing model also evaluates the jammer position even in a complicated propagation circumference.

5.2 Jammed Nodes Boundary Based Localization

Tianzhen C. *etal* [27] has been proposed a scheme for jammer localization based on double circle localization (DCL) .This algorithm depends on two strategies , the first is called minimum bounding circle (MBC) , while the second is defined as maximun incribed circle (MIC) . Hence this work using the jammed and boundary information for calculating the average value of (MBC) and (MIC) to realize immovability the node allocation and the jammed region inconsistency. The estimation accuracy of the jammer position is high for this scheme while it is susceptible to the jamming transmission power and not suitable for a large scale networks.

Sun Y. *etal* [28] proposed a jammer localization scheme defined as minimum circle covering based localization (MCCL) . It relys on a reference data of a sensor nodes exist at the boundaries of the jammed region. This work applying minimum circle covering method in order to shape a sacrificial jamming area. The assumption of this work is that the location of all the sensor nodes is recognized in advance.the estimation accuracy of the jamme location is high while it fails if the is a multiple or mobile jammer in the network.

A novel range based jammer localization (RJL) approach has been presented in [29] . This approach is based on the basis of the sensing method known as CrowdLoc and it is fundamentelly including three steps : the first step using the received signal strength to register the reference data of the jammer through the behavior of the sensing task, these collecting information can be get from the sensor exist at the border of the jammer transmission region. In the second step all those border area sensors participate between each other to contribute in the jammer registered measurements. While the third step is to estimate the jammer location by applying the proposed approach .The estimation accuracy is low and it is close to the Cramer - Rao Bound (CRB) .Also this algorithm depends on the geometry condition of the node distribution .

An efficient scheme defined as Catch the Jammer (CJ) has been investigated in [30] . This algorithm based on the share location information between the jammed area and the one-hop neighboring nodes to evaluate the position of the jammer in the network. This approach calculates the convix hull for a group of the jammed nodes and reproduces identical minimum covering circle.It is sensitive to the change of the jammer position in the network , hence the boundary nodes performs more significan function of the jammer estimation process.

5.3 Jammer Power Range Based Localization

Yu Seung Kim [31] proposed a scheme to locate the position of the sensor node by getting the benefits of jamming attacks for the network. In the first step , this work employing the power adaptation technique to locate the jammer and utilize these characteristics to localize the sensor node. The assumption of this approach is based on a high transmission power for the locator which is not always the case for energy constrained sensor nodes. This algorithm is highly affected by the propagation power transmission and suffering from multipath phenomenon . In addition this scheme is not suitable for a large scale networks.

Zhenhua Liu *etal* [32] proposed a method to find the position of the jamming sensor node straight way through the jamming signal strength (JSS). The determination of JSS is a big challenge because of it will be a part of other interference signals . This approach devised an estimation mechanism depend on the ambient noise to filter out the JSS. This work performs a feedback measured valuation and codify jammer localization as a nonlinear optimization in order to reduce the estimation errors. The accuracy for the jammer's location estimation is high and it can achieve for one or multiple jammers in the network. The drawback of this work is that the location estimation errors increased with the increasing of the number of jammers in the network.

5.4 Other Techniques for Jammer Localization

K.Pelechrinis etal [33] presented a light weight jamming detection method based on packet delivery ratio (PDR). They used gradient descent minimization based scheme to locate the jammer. This approach is based on assumption that sensor nodes location is already known and the jammer location must be identified. This algorithm will be fail if there is a multiple jammers or reactive jammer , while the accuracy of localizing the jammer depends massively on the selection of the intial point (sensitivity to local minima) and it is suitable for the routing and not suitable for a large scale networks.

An X-ray algorithm has been developed to determine the multiple jammer location in [34] , which is characterize the jammed regions in a graphical process and measure the jammed position relied on the consequence points of the characterized jammed area. The basic concept of this approach contains of three phases , jammed area mapping , jammed area characterization and jammer position determination . In this work the convex polygon of the jammed nodes is computed as a distribution of the jammed region. The estimation accuracy of the jammer position shows improvent when the jammer transmission ranges increased , for the reason that is this approach heavly depends on the jammed area, hence the increasing of the jammer transmission ranges leads to larger jammed regions , then more sections of the jammed area characterization will be generated and more information of the jammer will be obtained. The drawback of this approach is that very hard to estimate the location of the jammer who is inside the jammed area and affecting by another jammer because of this algorithm obtain jammer's information needed to estimate it's location from the jammed area itself . Also this approach fails to estimate the location of multiple jammers at the same time .

The summarization of the main characteristic features and the drawbacks of the jammer localization techniques in wireless sensor networks has been shown in Table 2. and Table 3. Respectively.

6. CURRENT PROBLEMS , CHALLENGES AND OPEN RESEARCH ISSUES

The basic configuration for any jammer is to insert a radio signal into the communication channel in order to outface the signal between the transmitter and the receiver to cut the information transmission path . In wireless sensor networks , an attractive localization process is facing a widespread of the jamming attacks , many jamming attacks on localization are growing in development and also on a rise . However the jamming effects is a big problem in wireless sensor network localization , so that a lot of challenges still take deep intentions and hard efforts by most of the researchers to be overcome it.

There are a few works on the localization in the presence of jamming attacks , most of these works focusing on finding the location of the jammer in the network , while a very few works focusing on localizing the sensor nodes over jamming attacks environment. The aim of those works whose taking into consideration only localizing the jammer is to get a proper action or alarm the network system.In addition some of these works having impractical assumptions to localize the jammer , while the others can be used only for checking the effect of the jamming attacks on the wireless sensor network localization accuracy.

The real challenges and open issues in this important topic is to accept the existance of the jamming attacks in the network and dealing with this fact by detecting the jammers and eliminate it's influence through a new robust techniques.

Table 2 : The Main Characteristic Features Of The Jammer Localization Techniques In Wireless Sensor Networks

Algorithm	Accuracy	Network Node Density	Jammer Transmission Range
CL[24]	Low	Sensitive	Sensitive
WCL [24]	Medium	Extremly Sensitive	More Sensitive
VFIL [24]	High	Extremly Sensitive	More Sensitive
LSQ [25]	Very High	Non Sensitive	Sensitive
Adaptive LSQ [26]	High	Sensitive	Sensitive
DCL [27]	High	Less Sensitive	Sensitive
MCCL [28]	High	Less Sensitive	Sensitive
RJL [29]	Low	Sensitive	Sensitive
CJ [30]	High	Sensitive	Sensitive
Power Adaptation Technique [31]	High	Non Sensitive	Sensitive
JSS [32]	Very High	Non Sensitive	Non Sensitive
PDR [33]	Medium	Sensitive	Sensitive
X-ray [34]	Medium	Sensitive	Non Sensitive

Table 3 : The Drawbacks Of The Jammer Localization Techniques In Wireless Sensor Networks

Algorithm	Jammer Localization Capability	Drawbacks
CL [24]	Single jammer	needs the prior knowledge of the location coordinates for each node also the location of its neighbors
WCL [24]	Single jammer	Needs all the jammed nodes to handover it's received signal strength RSS readings out of the jammed area
VFIL [24]	Single jammer	Suffers from the impact of the jammer's position and involves too much computation overhead which is improper for constrained sensor networks
LSQ [25]	Single jammer	Depends on the noise level boundary (NLB) to localize the jammer accurately and suffers from the impact of the jammer's position
Adaptive LSQ [26]	Single jammer	Requires each node must be knows its neighbors , the changes of hearing ranges caused by the jammer is too significant
DCL [27]	Single jammer	susceptible to the jamming transmission power and not suitable for a large scale networks.
MCCL [28]	Single jammer	The location of all the sensor nodes is recognized in advance, it fails if the is a multiple or mobile jammer in the network.
RJL [29]	Single jammer	This algorithm depends on the geometry condition of the node distribution
CJ [30]	Single jammer	Sensitive to the change of the jammer position in the network, boundary nodes performs more significan function of the jammer estimation process
Power Adaptation Technique [31]	Single jammer	high transmission power for the locator which is not always the case for energy constrained sensor nodes, highly affected by the propagation power transmission and suffering from multipath phenomenon
JSS [32]	Single or Multiple jammers	location estimation errors increased with the increasing of the number of jammers in the network.
PDR [33]	Single jammer	Sensor nodes location is already known and the jammer location must be identified, This algorithm will be fail if there is a multiple jammers or reactive jammer and suitable for the routing and not suitable for a large scale networks.
X-ray [34]	Multiple jammers	Very hard to estimate the location of the jammer who is inside the jammed area and affecting by another jammer, this approach fails to estimate the location of multiple jammers at the same time .

7. CONCLUSION

Jammer localization is an extensive field that fetch a serious research interest. This paper summarizes the current techniques that were used to localize the jammer in the network , also analyzes the problems and the drawbacks of each technique. In fact that the localization accuracy of the sensor nodes in all the applications of the wireless sensor networks has a significant and priority , so that the focusing on localizing the jammer still not worthy if can not overcome it's influence on the network performance .

This paper hopes to open the door for the future works that give more efforts in the direction of localizing the sensor nodes accurately over the presence of the jamming attacks . Finally the open issues of this work motivates the researchers to propose an efficient solutions addressing this concern .

REFRENCES:

[1] Mao G.and Fidan B. , Localization Algorithms and Strategies for Wireless Sensor Networks; United States of America by Information Science Reference IGI Global ,2009.

[2] Chen Y., Kleisouris K., Li X. , Trappe W.and Martin, R. P. *A security and robustness performance analysis of localization algorithms to signal strength attacks* , *ACM Trans. Sens. Networks*, Vol. 5, 2009, pp. 1–37.

[3] Chen Y., Yang J., Member S., Trappe W.and M artin, R. P., *Detecting and Localizing Identity-Based Attacks in Wireless and Sensor Networks*,IEEE Transactions on vehicular Technology, Vol. 5 , no. 95, 2010, pp. 2418–2434.

[4] HUSSEIN AHMED ABDULQADER, THAREK A. RAHMAN, and CHEE YEN LEOW. "ROBUSTNESS OF LOCALIZATION ACCURACY FOR WIRELESS SENSOR NETWORKS UNDER PHYSICAL ATTACKS." Journal of Theoretical & Applied Information Technology, Vol. 66, Issue 1 , 2014, pp. 347-358.

[5] W. Xu et al., "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," MobiHoc '05: Proc. 6th ACM Int'l. Symp. Mobile Ad Hoc Net. and Comp., 2005, pp. 46–57.

[6] Mpitziopoulos, Aristides, et al. "A survey on jamming attacks and countermeasures in WSNs." Communications Surveys & Tutorials, IEEE Vol. 11, no.4 , 2009, pp. 42-56.

[7] Manojkumar, M. K., and D. Sathya. "A Survey on an Effective Defense Mechanism against Reactive Jamming Attacks in WSN." International Journal of Computer Trends and Technology (IJCTT), Vol. 7 , no. 3, 2014, pp. 143-146.

[8] Wenyuan Xu; Ke Ma; Trappe, W.; Zhang, Y., "Jamming sensor networks: attack and defense strategies," Network, IEEE , vol.20, no.3,2006, pp.41-47.

[9] Manju.V.C. , " A Survey on Wireless Sensor Network Attacks", International Journal of Engineering and Innovative Technology (IJEIT) Vol. 2, Issue 2, August 2012

[10] Shahriar Mohammadi , Hossein Jadidoleslamy, " A COMPARISON OF PHYSICAL ATTACKS ON WIRELESS SENSOR NETWORKS", International Journal of Peer to Peer Networks (IJP2P) Vol.2, No.2, April 2011

[11] Yick, Jennifer, Biswanath Mukherjee, and Dipak Ghosal. "Wireless sensor network survey." Computer networks , Vol.52, no. 12, 2008, pp. 2292-2330.

[12] Zhou, Yun, Yuguang Fang, and Yanchao Zhang. "Securing wireless sensor networks: a survey." Communications Surveys & Tutorials, IEEE Vol. 10, no. 3, 2008, pp. 6-28.

[13] Y. Wang, G. Attebury and B. Ramamurthy," A Survey of Security Issues in Wireless Sensor Networks", Communications Surveys & Tutorials, IEEE , Vol. 8, no.2, Second Quarter 2006, pp.2-23,

[14] Chaudhari H.C. and Kadam L.U., "Wireless Sensor Networks: Security, Attacks and Challenges" , International Journal of Networking Vol. 1, Issue 1, 2011.

[15] Muruganandam. A, Bagyalakshmi. P, " A Study on Threats in Wireless Sensor Networks", International Journal of Science and Research (IJSR), Vol. 3, Issue 3, March 2014 , pp. 413-418.

[16] Anitha S. Sastry, Sulthana Shazia; Vagdevi S. ,"Security Threats in Wireless Sensor Networks in Each Layer" , International Journal of Advanced Networking & Applications , Vol. 4, Issue 4, 2013, pp. 1657-1661.

[17] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks", IEEE Communications Magazine, Vol. 40, No. 8, August 2002 , pp. 102-114.

[18] Jaydip Sen , " A Survey on Wireless Sensor Network Security", International Journal of Communication Networks and Information Security (IJCNIS) , Vol. 1, No. 2, August 2009 , pp. 55-78.

[19] Kai Xing , Shyaam Sundhar Rajamadam Srinivasan, Manny Rivera , Jiang Li , Xiuzhen Cheng , " Attacks and Countermeasures in Sensor Networks: A Survey", NETWORK SECURITY, Springer , 2005 , pp. 251-272.

[20] Zhu, Yanmin, Xiangpeng Li, and Bo Li. "Optimal Adaptive Antijamming in Wireless Sensor Networks." International Journal of Distributed Sensor Networks , 2012 , pp. 1-9.

[21] Prakash J. Parmar, Sachin D. Babar," Survey of Jamming Attacks and Techniques in Wireless Sensor Networks",INDIAN JOURNAL OF APPLIED RESEARCH, Volume : 3, Issue : 8 ,Aug 2013 , pp. 270-274

[22] FARAZ AHSAN , ALI ZAHIR, SAJJAD MOHSIN, KHALID HUSSAIN," SURVEY ON SURVIVAL APPROACHES IN WIRELESS NETWORK AGAINST JAMMING ATTACK", Journal of Theoretical and Applied Information Technology, Vol. 30 No.1, August 2011 , pp. 55-67.

[23] Wenyuan Xu; Ke Ma; Trappe, W.; Zhang, Y., "Jamming sensor networks: attack and defense strategies," IEEE Network, vol.20, no.3, 2006 , pp.41-47.

[24] Hongbo Liu; Wenyuan X; Yingying Chen; Zhenhua Liu, "Localizing jammers in wireless networks, IEEE International Conference on Pervasive Computing and Communications, PerCom, 2009, pp. 1-6.

[25] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Wireless jamming localization by exploiting nodes' hearing ranges." Distributed Computing in Sensor Systems. Springer Berlin Heidelberg, 2010, pp. 348-361.

[26] Zhenhua Liu; Hongbo Liu; Wenyuan Xu; Yingying Chen, "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization, IEEE Transactions on Parallel and Distributed Systems, Vol..23, no.3, , March 2012, pp.547,555 .

[27] Tianzhen Cheng; Ping Li; Sencun Zhu, "An Algorithm for Jammer Localization in Wireless Sensor Networks", IEEE 26th International Conference on Advanced Information Networking and Applications (AINA), 2012 , pp. 724-731.

[28] SUN Yanqiang, WANG Xiaodong and ZHOU Xingming, " Jammer Localization for Wireless Sensor Networks " , Chinese Journal of Electronics Vol. 20, no. 4, Oct. 2011, pp. 735-738.

[29] Yanqiang Sun, Xiaodong Wang , Melek Önen, Refik Molva , " CrowdLoc: Wireless Jammer Localization with Crowdsourcing Measurements" ,UbiCrowd '11 Proceedings of the 2nd international workshop on Ubiquitous crowdsouring ACM New York, USA ,2011, Pp. 33-36.

[30] Yanqiang Sun; Molva, R., Onen, M., Xiaodong Wang, Xingming Zhou, "Catch the Jammer in Wireless Sensor Network" , IEEE 22nd International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), 2011, pp. 1156-1160.

[31] Yu Seung Kim; Mokaya, F.; Chen, E.; Tague, P., "All your jammers belong to us — Localization of wireless sensors under jamming attack", IEEE International Conference on Communications (ICC), 2012 pp.949-954.

[32] Zhenhua Liu; Hongbo Liu; Wenyuan Xu; Yingying Chen, "An Error-Minimizing Framework for Localizing Jammers in Wireless Networks," Parallel and Distributed Systems, IEEE Transactions on , vol.25, no.2, , 2014 , pp. 508-517.

[33] Pelechrinis, K.; Koutsopoulos, I; Broustis, I; Krishnamurthy, S.V., "Lightweight Jammer Localization in Wireless Networks: System Design and Implementation," Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE , vol., no., pp.1,6,Dec. 4 2009.

[34]Tianzhen Cheng; Ping Li; Sencun Zhu, "Multi-jammer Localization in Wireless Sensor Networks" , 2011 Seventh International Conference on Computational Intelligence and Security (CIS), 2011 , pp.736-740.