www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-3, Issue-2, Apr- 2015
Research Paper

Int. J. Sci. Res. in Network Security and Communication
ISSN: 2321-3256

Proposed Jamming Removal Technique for Wireless Sensor Network

Amr M. Kishk[1*], Nagy W. Messiha[2], Nawal A. El-Fishawy[3], Abdelrahman A. Alkafs[4] and Ahmed H. Madian[5]

[1*]Reactor Department/Egyptian Atomic Energy Authority (EAEA)/Egypt and amr.kishk@yahoo.com
[2]Electronics and Communication Engineering/Faculty of Electronic Engineering (FEE)/Egypt and dr.nagy_wadie@hotmail.com
[3]Computer Engineering/ Faculty of Electronic Engineering (FEE)/Egypt and nelfishawy@hotmail.com
[4]Reactor Department/Egyptian Atomic Energy Authority (EAEA)/Egypt and alkafs@yahoo.com
[5]Reaction Engineering/ Egyptian Atomic Energy Authority (EAEA)/Egypt and ah_madian@hotmail.com

Received: 04 Mar 2015 | Revised: 16 Mar 2015 | Accepted: 10 Apr 2015 | Published: 30 Apr 2015

***Abstract*—**This electronic docum Wireless Sensor Network (WSN) is exposed to many threats to destroy data confidentiality during the transmission in the communication channel. The Jamming is one of these threats. To face this threat, we should discuss this problem from many directions. The discussion includes jamming types and its effects, jamming detection techniques, disturber localization methods, and defensive techniques. The reduction or removal of the effectiveness of jamming from the reconstructed data at the receiver enhances the performance of WSN. The techniques used to face this threat are discussed in this paper. The enhancements of these techniques are introduced in this paper which are extracted from their drawbacks. The weakness point of the disturber is the inability to jam the signal frequency which leads us to propose a defensive technique to remove the effectiveness of jamming completely from the reconstructed data at the receiver. The proposed defensive technique guides us to remove the attached redundancy of the coding techniques from the packets. And also, it reduces the transmission time of the transmitted message. So, the overall performance of WSN is improved due to jamming removal.

Keywords- Disturber Types; Victim Nodes; Jamming Detection Techniques; Disturber Localization Methods; Defensive Techniques.

I. Introduction

Wireless networks have been becoming more affordable and deployed in different modalities [1]. Wireless Sensor Network (WSN) is one of these modalities which constitutes a set of light-weight devices called sensor nodes. Each node in WSN is equipped with a radio transceiver [2]. WSN is growing extremely and becoming more and more attractive for a variety of application areas such as surveillance of information, industrial secrets, air pollution monitoring, and many more. WSN is mostly used for gathering application specific information from the surrounding environment. The primary weakness shared by all wireless application and technologies is the vulnerability to security threats [3]. A denial-of-service (DoS) attack is typically one of these threats used by illegitimate users to reduce the functionality and the overall performance of the network [4]. DoS from jamming is difficult to remove it from the reconstructed signal at the receiver with the limit resources available to WSN nodes [5].

Jamming can occur either unintentionally in the form of interference, noise, or collision to disrupt or prevent the signal transmission in WSN [6]. And Also, jamming can exhaust the battery energy of the nodes due to multiple retransmission processes. The disturber has many forms and it can be summarized into four types: constant disturber, deceptive disturber, random disturber, and reactive disturber [7]. These types can be differentiated from each other from their definitions. Constant disturber continually emits a radio signal into WSN channels. Deceptive disturber constantly injects regular packets without any gap between subsequent packet transmissions. Random disturber alternates between sleeping and jamming. Finally, reactive disturber emits a radio signal into WSN channels as soon as it senses an activity on the channel. From the definitions of the disturber types, all disturber types except reactive disturber are active attacks because they try to block the channel irrespective of the traffic pattern on the channel while reactive channel depends on traffic status. So, reactive disturber may be harder to detect than the others. The Jammed nodes are called victim nodes while the non jammed nodes are called the boundary nodes which are the neighbors of the victim nodes. The nodes which active the reactive nodes are called trigger nodes as shown in Fig. 1.

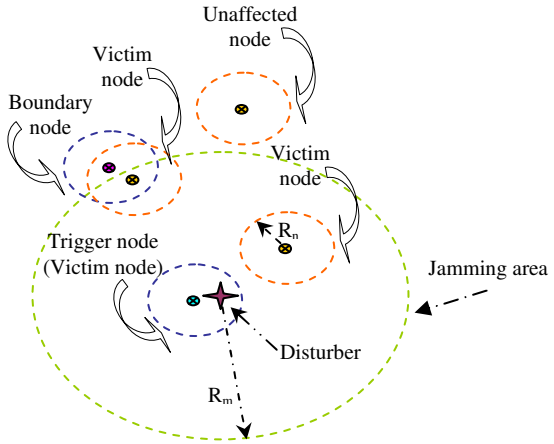

Figure 1. Sensor nodes types in the presence of disturber.

To protect the network from jamming, many mechanisms have been proposed to defeat or diminish the effectiveness of jamming. Jamming detection, its localization methods, and the defensive techniques are discussed in this paper. The detection of the jamming beside the disturber localization enforce the ability of defensive mechanisms to defeat or diminish the effectiveness of jamming. The two most popular defensive mechanisms are Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) [1]. The weakness point of these techniques introduces their proposed enhancements. These enhancements are explained and compared with the traditional techniques. The proposed detection technique prolongs the battery lifetime of the sensor nodes. The proposed localization method specifies the disturber position exactly in comparison with the traditional methods. This enhancement guides us to remove the disturber manually from the network or change the data route. The paper introduces two defensive techniques. One of them removes the effectiveness of jamming completely from the reconstructed data. So, the sensor network can send and receive without dependence on detection techniques or localization methods. Jamming removal enhances the performance of WSN.

The organization of the paper is as follows: section II introduces the related work of the jamming detection techniques, localization methods, and defensive techniques while their enhancements and the results are discussed in sections III and IV respectively. Finally, the conclusions of these discussions are shown in the end of this paper.

II. Related Work

A. Jamming detection techniques

WSN is a self-configuring network of small sensor nodes communicating among themselves using radio signals deployed in quantity to sense, monitor, and understand the physical world [8]. Disturber negatively affects the sensor nodes in its inability to send its packets correctly to BS; causing multiple retransmission processes due to multiple Negative Acknowledgements (NACKs) or no received ACKs from the receiver. These problems guide the sensor nodes to use jamming detection technique to take a decision to prevent the exhaustion of battery energy. The objective of the jamming detection techniques is to minimize the number of required observation samples to derive a decision about existence of disturber in the communication channels [6]. Some of them depend on measurements of the regular transmission and the others assign periodic time to detect the presence of jamming within the communication channel using an assignment detection packet. The jamming detection measurements depend on the side type: sender or receiver.

A.1. Jamming detection measurements

Jamming detection measurements at the sender side

The disturbers can prevent a legitimate source from sending out packets because of the channel might appear constantly busy to the source. In this case, the sensor nodes spend waiting time until the channel become idle. The technique used for jamming detection in this case is namely by carrier sensing time. The sensor nodes declare the existence of disturber in the communication channel when the carrier sensing time is above a threshold time specified by the network operator. In most forms of wireless Medium Access Control (MAC), governing rules decide who can transmit and which time. One popular class of MAC protocols are those based on Carrier Sense Multiple Access (CSMA) [1]. The carrier sense time with MAC protocols is suitable to detect both constant disturber and deceptive disturber but, it is not suitable to detect the other disturber types: random disturber and reactive disturber because the later types jam the communication channel under conditions while the first types jam the communication channel all the time. So, the need to another detection technique guides the problem to Packet Send Ratio (PSR) which is defined as the ratio of packets that are successfully send out by a legitimate traffic source compared to the number of packets it intends to send out at the MAC layer [1] or it can be defined as the ratio of number of received ACK by the total number of packets. Depending on a comparison PSR with a specified threshold, the sender can declare the existence of disturber in the communication channel to stop the retransmission processes. Until now, PSR is the popular technique at the sender side to detect all the disturber types and guides the sensor nodes to the defensive mechanisms to minimize the effectiveness of jamming on the communication channel as possible.

Jamming detection measurements at the receiver side

The senor node as a receiver does not spend more energy like the sender side in the jamming detection. The main objective of the disturber with respect to the receiver is the packet disrupting before the receiving process. The signal strength does not consider a real metric used to declare the existence of the jamming in the communication channel because the disturber can reduce the signal strength at the sender side before reach the receiver and also he can amplify

the signal strength at the receiver side as an expected matter because of his high energy in comparison with the transmitting energy of the sensor node. The distributed received packets means the receiver will request packets retransmission and can cause exhaustion to the node battery. It has been thought about another measure namely by Packet Delivery Ratio (PDR). PDR is much like PSR and is defined as the ratio of the number of packets that are successfully delivered to the destination compared to the number of packets that have been sent out by the sender. The number of packets that are successfully delivered to a destination is measured from number of packets that pass the CRC check while the number of packets that have been sent out by the sender is defined from the received packet header. Until now, PDR is the popular technique at the receiver side to detect all the disturber types. So, the sensor nodes should use a suitable defensive mechanism to minimize the effectiveness of jamming on the communication channel as possible.

A.2. Periodic jamming detection

Periodic jamming detection prevents energy consumption in the data transmission and multiple retransmission processes in the presence of jamming. The periodic jamming detection has assigned a detection packet between the nodes in the communication channels. This packet is sent between sensor nodes periodically before regular transmission. The contents of the detection packet are different from of technique to another technique. These techniques can be summarized as follows:

DoS check timer

One of these detection packet is a packet of size 31-bytes. This detection packet is suggested to send it to the other node in the communication area periodically depending on a time specified by the application layer namely by DoS check timer. The delay in the reply or receiving NACK from the other node means the presence of jamming [9]. So, the sender only who specify the presence of disturber in the communication channel. This technique was applied on three different topology: two-party radio communication, infrastructure network, and Ad hoc network.

Radio Interference Detection (RID)

Two packets were suggested by Radio Interference Detection (RID) technique for jamming detection process: High Power Detection packet (HD) and Normal Power Detection packet (ND) [10]. The sender used a HD-ND detection by sending out a HD-packet of size 2-bytes which only contains its ID followed by ND packet after certain time namely by Minimal Hardware Wait Time (MHWT). The absence of ND or disrupted ND packet at the receiver side means the presence of disturber. To ensure from the result, this process was repeated many times. And also, the enhancement of RID is namely by RID-B which uses TDMA protocol with RID to separate the multi transmission collision from the effectiveness of jamming from the results.

A Query-based Jamming Detection Algorithm (QUJDA)

A Query-based Jamming Detection Algorithm (QUJDA) is an anomaly-based and distributed algorithm by which jamming attacks can be detected by exchange a QUERY and REPLY packets of size 7-bytes each among the neighbors periodically [11]. The packet disruption or receiving NACK refers to the presence of disturber in the communication channel. Both the sender and the receiver share to detect the jamming.

Broadcasting a beacon

Instead of detecting the jamming between two neighbor nodes, it is suggested to carry out the jamming detection in each cluster. Each node in a cluster broadcasts a beacon that carries its ID periodically. From the absence of ACK or the presence of NACKs, the jamming can be detected [12]. So, each node, as a sender, can specify the jamming location.

PROBE message

The assumption of the presence of jamming in the communication channel has been assumed and measured by some way. After that, the nodes outside the jamming area, boundary nodes, prevent the communication with the nodes inside the jammed area, victim nodes [13]. The boundary nodes test the communication channel with the victim nodes periodically using PROBE message. So, the communication with the victim nodes in the future means no jamming between them.

B. Disturber localization methods

Disturber localization in WSN is important so as to take security actions against the disturber and restore the network communication [14]. The victim nodes in jamming area can be specified by their received packets using jamming detection technique. It has been suggested to analysis this jamming area to discover the disturber type with the victim nodes [15]. The trigger nodes localization is one of the methods used to locate one type of the disturbers, reactive disturber, in WSN [16]. This technique partitioned the victim nodes into groups and each node in these groups uses a detection technique to specify the trigger nodes. Instead of locating the jamming area or the trigger nodes, it was estimated different methods to specify the disturber position to deal with him manually or to reconfigure WSN topology such as: Centroid Localization (CL) [17], Weighted Centroid Localization (WCL) [18], Virtual Force Iterative Localization (VFIL) [19], and Double Circle Localization (DCL) [14]. These methods have based on the known location of the victim nodes.

B.1. Centroid Localization (CL)

CL has depended on the victim nodes only to estimate the disturber location by determination the average of x and y values of the victim nodes as in (1).

$$(\hat{x}_{\text{disturber}}, \hat{y}_{\text{disturber}}) = \left(\frac{\sum_{i=1}^{N} x_i}{N}, \frac{\sum_{i=1}^{N} y_i}{N} \right) \quad (1)$$

B.2. Weighted Centroid Localization (WCL)

It is a CL enhancement by adding the weighting factor into CL method. So, the disturber position can be estimated as in (2) where: $w_i = 1/d_i^2$, and d_i^2 is the distance between the i[th] neighbor node and the disturber node.

$$(\hat{x}_{\text{disturber}}, \hat{y}_{\text{disturber}}) = \left(\frac{\sum_{i=1}^{N} w_i x_i}{\sum_{i=1}^{N} w_i}, \frac{\sum_{i=1}^{N} w_i y_i}{\sum_{i=1}^{N} w_i} \right) \quad (2)$$

B.3. Virtual Force Iterative Localization (VFIL)

It is a another CL enhancement by adjusting the estimation of disturber position by applying iterations on two forces types: pull force, F_{pull}^{i}, and push force, F_{push}^{j}. These forces adjust the estimated disturber position by applying multiple iterations on the determination of F_{pull}^{i} and F_{push}^{j} beside $F_{jo\text{int}}$ as in (3-5) where: (x_i, y_i), (x_j, y_j), and $(\hat{x}_o, \hat{y}_o)$ are the position of the victim nodes, boundary nodes, and the estimated disturber position using CL method.

$$F_{pull}^{i} = \left(\frac{x_i - \hat{x}_o}{\sqrt{(x_i - \hat{x}_o)^2 + (y_i - \hat{y}_o)^2}}, \frac{y_i - \hat{y}_o}{\sqrt{(x_i - \hat{x}_o)^2 + (y_i - \hat{y}_o)^2}} \right) \quad (3)$$

$$F_{push}^{j} = \left(\frac{\hat{x}_o - x_j}{\sqrt{(\hat{x}_o - x_j)^2 + (\hat{y}_o - y_j)^2}}, \frac{\hat{y}_o - y_j}{\sqrt{(\hat{x}_o - x_j)^2 + (\hat{y}_o - y_j)^2}} \right) \quad (4)$$

$$F_{jo\text{int}} = \frac{\sum_{i \in J} F_{pull}^{i} + \sum_{j \in B} F_{push}^{j}}{\left| \sum_{i \in J} F_{pull}^{i} + \sum_{j \in B} F_{push}^{j} \right|} \quad (5)$$

B.4. Double Circle Localization (DCL)

Both CL and WCL are sensitive to node distribution and network density, and VFIL has difficulties in disturber transmission range estimation. To avoid these drawbacks, DCL is based on Minimum Boundary Circle (MBC) and Maximum Inscribed Circle (MIC) to enhance the disturber position estimation.

C. Defense techniques

Jamming is one of the threats which interferes with the radio frequencies used by sensor nodes and may be viewed as a special case of DoS attacks [20]. Jamming is divided into four types: constant disturber, deceptive disturber, random disturber, and reactive disturber [7]. To face this interference, it must be gather information on the presence of disturber in the communication channel, its type and its location, to assist the defense techniques to face these attacks. There are two ways to face the jamming: avoid dealing with the victim nodes or dealing with them using defense techniques. Some of ideas were suggested to avoid dealing with the victim nodes: spatial retreats [9], the use of the trigger nodes as a receiver only [16], changing the data route using ant system [4], and no data transmission with the victim nodes until jamming removal [13]. The other way of use defense technique has many different ideas: regulated transmitted power, FHSS, DSSS, hybrid FHSS/DSSS, Ultra Wide Band (UWB) technology, antenna polarization, directional transmission [20], wired pairs, uncoordinated channel hopping [21], frame masking defense, packet fragmentation, and redundant encoding [15].These techniques are discussed as follows:

C.1. Frequency Hopping Spread Spectrum (FHSS)

FHSS is a spread spectrum method of the transmitting radio signal by rapidly switching a carrier among many frequency channel using a shared algorithm known at the transmitter and the receiver [20]. The sensor nodes in WSN environments comply with the ZigBee communication protocol [20]. All ZigBee devices are required to comply with the two versions of IEEE 802.15.4:2003 and 2006. The communication between sensor nodes is in the unlicensed 2.4GHz, 902-928 MHz (North America), and 868MHz (Europe) Industrial, Scientific, and Medical (ISM) bands. The comparison between two versions of ZigBee communication protocol is shown in table 1. The comparison shows that: FHSS is suitable for the unlicensed 2.4GHz and 915MHz bands because of multiple channels in these bands while 868 band is not suitable for FHSS because no enough channels for hopping process. The capability of disturber to jam the transmitted data at some channel guides the defensive techniques to change the transmitting frequency to another channel. And also, the probability of jamming multiple channels guides us to use FHSS.

Table 1. WSN communication protocols

	Unlicensed 2.4GHz	902-928MHz (North America)	868MHz (Europe)
No of channels	16 channels and each channel occupying 3MHz	10 channels and extended to 30 channels in	1-Channel and extended to 2-Channels

	with 5MHz channel spacing	version 2006 with 2MHz channel spacing	in version 2006
Data rate	250 Kbps per channel	40 Kbps per channel	20 Kbps
Modulation technique	Offset Quadrature Phase-shift keying (O-QPSK) that transmits 2-bits per symbol	Binary Phase Shift Keying (BPSK) and both O-QPSK and the combination between binary keying and Amplitude Shift Key (ASK) are added in version 2006	
Transmission range	10 to 75m		
Maximum output power	0dBm (1mW)		

C.2. Frequency hopping pairs

Because of diminishing the impact of jamming whenever far from its center, it has been thought to link some nodes pairs by wire connection to transfer the data from the jamming area to the outside. The wire connection is shielded by insulating layer which prevent the jamming from the outside signals. Although the idea of wired pairs solved the jamming problem significantly, the problem of wire connection is added to WSN. So, the direction to the wireless solutions has been taken by use FHSS instead of wire connection. Not all sensor nodes use FHSS but the wired pairs is replaced by FHSS only because the need for synchronization may be a major reason against the usage of FHSS in multihop WSN [21].

C.3. Direct Sequence Spread Spectrum (DSSS)

DSSS transmissions are performed by multiplying the data being transmitted by a Pseudo Noise (PN) digital signal. This PN digital signal is a pseudorandom sequence of 1 and -1 values at a frequency much higher than that of the original signal [20]. PN digital signal aids the decoder to recover the jammed bits depending on the acting of each bit by multiple bits.

C.4. Hybrid FHSS/DSSS

Hybrid FHSS/DSSS refers to use an advanced radio unit by adding FHSS unit after DSSS unit in the sensor node namely by Ares node [20]. The communication within Ares nodes is the unlicensed 5GHz band (5470-5725 MHz) instead of 2.4 GHz band because of the heavily use of 2.4 GHz band. In the 5GHz band, there is 255 MHz of bandwidth available for spread spectrum transmission. Ares nodes uses 51 frequency channels for FHSSS with 5 MHz of bandwidth available for DSSS. The data rate used in this band is 252 Kbps per channel. Ares nodes have the ability to perform frequency hops up to 100,000 per second. A sequence of channels used was determined by a channel sequence generation algorithm that used as a seed secret key. This secret key was derived from a secret word, known only to the nodes and the sink, using Password-Based Key Derivation Function 2 (PBKDF2) [22] or the combination of Mersenne Twister (MT199937) algorithm [23] with a Secure Hash Algorithm 1 (SHA-1). The secret key scheme used here for enhanced security. The encryption key may change upon sink request or in specific time intervals or arbitrary depending on nodes computational power and available energy. For even more enhanced security, the PN code may be changed periodically. This scheme has used Flooding Time Synchronization Protocol (FTSP) which is designed especially for WSN and it has an average precision of 0.5μs per hop in a multihop case. The scheme did not use Global Positioning System (GPS) for synchronization purpose because GPS signals are highly vulnerable to face the jamming and also GPS receivers would drastically increase the Ares node cost. The hybrid FHSS/DSSS enhances the performance of both FHSS and DSSS separately.

C.5. Packet fragmentation

The sensor node breaks the outgoing application payload into fragments to be transmitted separately on different channels and with different Start of Framer Delimiter (SFD) sequence [15]. The last fragment contains a Frame Check sequence (FCS) for the entire payload. The redundancy and correction overhead may be reduced by using near-optimal erasure codes which can be efficiently implemented in hardware or software [24].

C.6. Popular defensive techniques

Regulated transmitted power

Higher transmitted power implies higher resistance against jamming because a stranger jamming signal is needed to overcome the original signal.

Ultra Wide Band (UWB) technology

UWB technology is a modulation technique based on transmitting very short pulses simultaneously [25]. The use of very short pulses resists the effects of both multipath and jamming.

Antenna polarization

The antenna polarization is the orientation of the electric field with respect to the earth's surface [20]. The receiver must have the same antenna polarization as the transmitter to be able to receive the transmitted signal. Hence, if the sensor nodes are capable of changing the polarization of their antennas when they sense interference, they will be able to effectively defend in jamming environments. To avoid the problem of the synchronization of changing the antenna polarization, it is suggested to program the nodes when they sense interference [20].

Directional antenna

The directional antenna transmits and receives radio waves only from one particular direction unlike the Omni-directional antenna that transmits and receives radio waves from all directions in the same time. The use of directional antennas could dramatically improve jamming tolerance in WSN. It provides better protection against eavesdropping,

detection, and jamming than Omni-directional transmission [20].

III. Proposed Enhancements

A. Jamming detection enhancement

It is suggested to use PSR with carrier sense time to detect the disturber type at the sender side and also PDR with both carrier sense time and signal strength at the receiver side. The dependence on PSR and PDR specifies the presence of jamming in the communication channel while the use of carrier sense time and signal strength after PSR or PDR to specify the jamming type.

If the sender detected the presence of jamming in the communication channel by using PSR, then the state of the channel after the detection process, the end of transmission process, can specify the jamming type. The state of the channel is idle means that the jamming was caused by a reactive disturber and the busy channel means an active disturber stays in the communication channel. But, the sender cannot facilitate between the types of the active jamming. The receiver side can use PDR with both the signal strength and carrier sense time to facilitate between the reactive and active jamming and also between all types of the active jamming. PDR specifies the presence of the jamming in the communication channel while the carrier sense time and the signal strength of the received packets can facilities between the jamming types. The use of carrier sense time after PDR facilitate between the active jamming and the reactive jamming while the use of the signal strength metric after the carrier sense time metric facilitates between the types of active disturbers:

- Constant disturbers jam all the packets in the communication channel.
- Deceptive disturbers jam some bits and leave the others periodically.
- Random disturbers jam some packets and leave the others.

B. Proposed disturber localization method

The disturber target is the disruption of the exchanged data within the communication area which contains sensor nodes namely by victim nodes because of the impact of the jamming on them. The jamming center is the disturber position and it is determined by disturber localization methods. But, These methods cannot determine the disturber position exactly because the disturber transmitted power P_{txj} is unknown parameter in the Friis transmission equation [20] which shown in (6). So, it should find a solution to determine the disturber position from Friis transmission equation. Firstly, it should specify the known and unknown parameters in the Friis transmission equation with respect to the victim nodes. The known parameters are: received power P_{rx}, receiver antenna gain G_{rx}, and wavelength λ while the unknown parameters are: disturber transmitted power P_{txj}, disturber antenna gain G_{txj}, and system loss factor L. To solve this problem, it should rewrite the Friis transmission equation at the victim nodes as in (7) by considering all G_{rxi} are the same for all n-victim nodes and i=1,2,…,n. So, the Friis transmission equation becomes a proportional relationship between P_{rxi} and d_i where: d_i is the distance between the victim node-i and the disturber.

$$P_{rx} = P_{tx}\frac{G_{tx}G_{rx}\lambda^2}{16\pi^2 d^2 L} \quad (6)$$

$$P_{rx1}d_1^2 = P_{rx2}d_2^2 = \ldots = P_{rxn}d_n^2 = P_{tx\,j}\frac{G_{txj}G_{rxi}\lambda^2}{16\pi^2 L} \quad , \quad i=1,\ldots,n \quad (7)$$

Secondly, from the analytic geometry, the distance between two points in the xy-plane or between a victim node (x_i, y_i) and the disturber position (x_j, y_j) can be determined by using the distance formula as in (8) and as shown in Fig. 2.

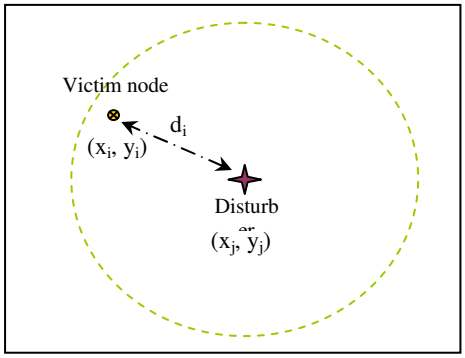

Figure 2. xy-plane for a victim node at (x_i, y_i) and a disturber at (x_j, y_j)

Finally, the disturber position at x_j and y_j can be determined from (7) and (8) in (9) and (10) respectively where its derivatives steps are shown in Appendix A.

$$d_i^2 = (x_j - x_i)^2 + (y_j - y_i)^2 \quad (8)$$

$$x_j = \frac{C_1 S_{y2} - C_2 S_{y1}}{S_{x1}S_{y2} - S_{x2}S_{y1}} \quad (9)$$

$$y_j = \frac{1}{S_{y1}}(C_1 - x_j S_{x1}) \quad (10)$$

Where:

- $C_1 = \left[\left(x_1^2 - x_3^2\right) + \left(y_1^2 - y_3^2\right)\right]\frac{P_{rx2}P_{rx3} - P_{rx1}P_{rx3}}{P_{rx2}P_{rx3} - P_{rx1}P_{rx2}} - \left[\left(x_1^2 - x_2^2\right) + \left(y_1^2 - y_2^2\right)\right]$
- $C_2 = \left[\left(x_2^2 - x_4^2\right) + \left(y_2^2 - y_4^2\right)\right]\frac{P_{rx3}P_{rx4} - P_{rx2}P_{rx4}}{P_{rx3}P_{rx4} - P_{rx2}P_{rx3}} - \left[\left(x_2^2 - x_3^2\right) + \left(y_2^2 - y_3^2\right)\right]$
- $S_{x1} = 2\left(x_2 - x_1\right) - 2\left(x_3 - x_1\right)\frac{P_{rx2}P_{rx3} - P_{rx1}P_{rx3}}{P_{rx2}P_{rx3} - P_{rx1}P_{rx2}}$
- $S_{x2} = 2\left(x_3 - x_2\right) - 2\left(x_4 - x_2\right)\frac{P_{rx3}P_{rx4} - P_{rx2}P_{rx4}}{P_{rx3}P_{rx4} - P_{rx2}P_{rx3}}$
- $S_{y1} = 2\left(y_2 - y_1\right) - 2\left(y_3 - y_1\right)\frac{P_{rx2}P_{rx3} - P_{rx1}P_{rx3}}{P_{rx2}P_{rx3} - P_{rx1}P_{rx2}}$
- $S_{y2} = 2\left(y_3 - y_2\right) - 2\left(y_4 - y_2\right)\frac{P_{rx3}P_{rx4} - P_{rx2}P_{rx4}}{P_{rx3}P_{rx4} - P_{rx2}P_{rx3}}$

C. Two proposed defensive techniques

C.1. Inhomogeneous Carriers Modulation Technique (ICMT)

The enhancement in the modulation techniques is one of the tools used to face the effectiveness of jamming. WSN has used O-QPSK shown in table (1) to face the effectiveness of jamming in the communication channel. We suggest an enhancement in O-QBSK to improve the performance of the WSN at the presence of Jamming in the communication channel. The proposed modulation technique is shown in Fig. 3 and is namely by Inhomogeneous Carriers Modulation Technique (ICMT). Both the modulator and demodulator have different carrier to transmit and reconstruct the Message, Ms, respectively. The modulator uses C1 while the receiver uses C_2 as in (11 and 12) respectively. The modulator generates the modulated signal, T_x, from the original message by multiplying it by C_1 to send it to the receiver as in (13) and Fig. 3.a. The receiver can reconstruct the original message by multiplying the received signal, R_x, by C_2 to get M_r which applied on Low Pass Filter (LPF) as in (14) and Fig. 3.b to get the reconstructed message, M'.

$$C_1 = \frac{1}{\sqrt{2}}\left[Cos\left(2\pi f_c t\right) - Sin\left(2\pi f_c t\right)\right] \quad (11)$$

$$C_2 = \frac{1}{\sqrt{2}}Cos\left(2\pi f_c t\right) \quad (12)$$

$$T_x = \frac{M_s}{\sqrt{2}}\left[Cos\left(2\pi f_c t\right) - Sin\left(2\pi f_c t\right)\right] \quad (13)$$

$$M_r = \frac{R_x}{\sqrt{2}}Cos\left(2\pi f_c t\right) \quad (14)$$

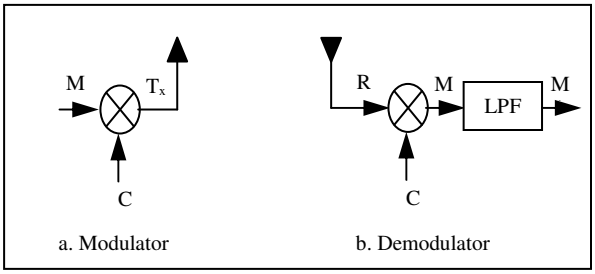

Figure 3. Inhomogeneous Carriers Modulation Technique (ICMT)

C.2. Hybrid Frequency Modulation and Amplitude Modulation (FM-AM)

Every disease has a weakness point causing the appearance of its medicine. The weakness point of the disturber is the inability to distort the frequency of the transmitted signal. Fig. 4 shows three signals: transmitted signal (the upper signal), jamming signal (the middle signal), and received signal (the last signal). The disturber adds his jamming signal to the transmitted signal to jam it. He successes to jam both amplitude and phase but he cannot jam the frequency. The incapability to jam the signal frequency is the condition of the jamming which is the disturber must use the same frequency of the transmitted signal to jam it.

So, it has been thought to use the Frequency Modulation (FM) at Low Frequency (LF) band with Amplitude Modulation (AM) at 2.4GHz band (ZigBee band) as shown in Fig. 5. FM is used to modulate the carrier frequency at LF by the amplitude of the original signal then, the Amplitude Modulation (AM) is used to modulate the carrier frequency at 2.4GHz band (ZigBee band) by FM modulated signal. Both FM and AM are analog modulation techniques. So, it should use the decimal value of every byte which will be in [0,255] range. And also, it is suggested to represent every byte, 8-bits, by a signal at LF band using FM in a duration time equal to one bit duration time, t_b. The reduction in duration time of the one byte will enhance the data rate. The proposed defensive technique (FM-AM) steps are shown as follows:

At the transmitter

Step 1: let the first byte of some packet be $(10110100)_2$.

Step 2: convert the byte to a decimal value: f_m=180.

Step 3: by using FM in LF band, the decimal value can be represented by a signal with a frequency equal to f_m as in (15) where A_m is the multitude of the FM modulating signal.

$$x(t) = A_m \sin\left(2\pi f_m t\right) \quad (15)$$

Step 4: use AM-modulator to modulate the carrier frequency by x(t) at ZigBee band, f_c=2.4GHz, as in (16) where A_c is the amplitude of the carrier signal.

$$y(t) = x(t)\left[A_c \sin(2\pi f_c t)\right] \quad (16)$$

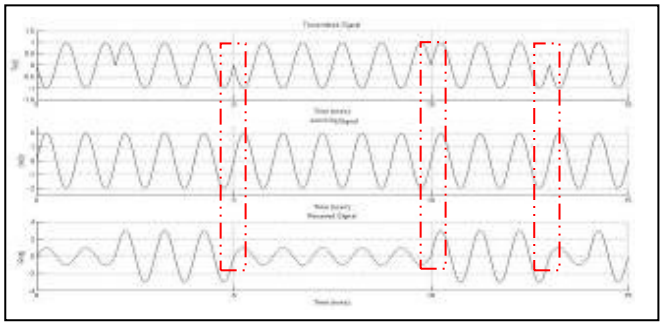

Figure 4. Effectiveness of jamming on the amplitude, phase, and the frequency of the transmitted signal

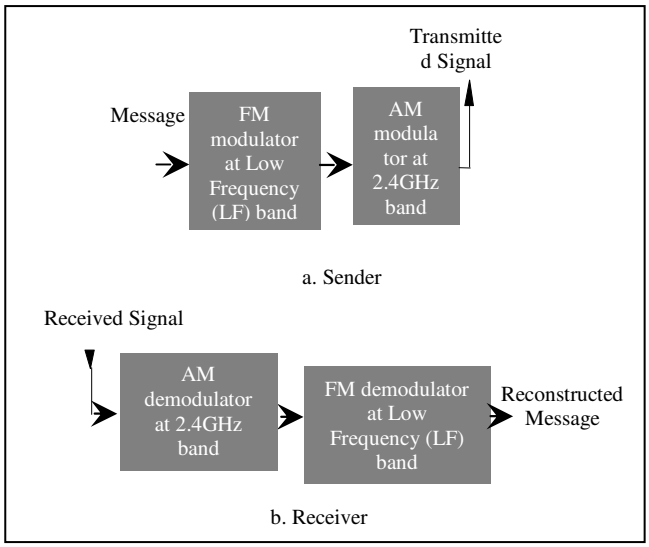

Figure 5. FM-AM modulation technique

At the receiver

Step 1: Use AM demodulator to multiply the received jammed signal, s(t) shown in (17), by $\sin(2\pi f_c t)$ where A_j and v(t) are the jammed and jamming signal respectively. Then, apply the results on Low Pass Filter (LPF) to get FM jammed signal, r(t), as shown in (18) where A_{jj} is the jammed amplitude of recovered FM signal.

Step 2: Use FM demodulator to reconstruct the original image.

Step 3: convert f_m to a binary to get $(10110100)_2$ as in step 1.

$$s(t) = A_j y(t) + v(t) \quad (17)$$

$$r(t) = A_{jj} \sin(2\pi f_m t) \quad (18)$$

FM demodulator can be replaced by three suggested ideas to reconstruct the original message:

First idea: Apply r(t) on a differentiator to get r'(t) as in (19). Then, we can get f_m by the relation shown in (20).

$$r'(t) = A_{jj}(2\pi f_m)\cos(2\pi f_m t) \quad (19)$$

$$f_m = \frac{\max(r'(t))}{2\pi \max(r(t))} \quad (20)$$

Second idea: Apply r(t) on a differentiator twice to get r''(t) as in (21). Then, we can get fm by the relation shown in (22).

$$r''(t) = -A_{jj}(2\pi f_m)^2 \sin(2\pi f_m t) \quad (21)$$

$$f_m = \frac{1}{2\pi}\sqrt{\frac{-r''(t)}{r(t)}} \quad (22)$$

Third idea: Apply r(t) on Fast Fourier Transform (FFT) with each period to get R(w). R(w) is a delta function at f_m. So, we can reconstruct f_m value from frequency domain.

IV. Results and Discussions

A. Jamming detection techniques

Although the benefit of use a periodic jamming detection to reduce the battery exhausting, it has some drawbacks:

First, the assumption of the disturber inability to analysis the communication channel traffic to specify the detection type, periodic or non-periodic from the transmitted packet size, and its periodic time. The disturber can deceive the sensor nodes. He can stop to jam the communication channel during the detection process to jam it during the transmission time only. This idea can exhaust the battery of the sensor nodes quickly.

Second, the drawback of the periodic detection is the inability to detect the jamming type because each type will be active during the transmission process and the detection techniques are used only to detect the presence or absence of the disturber.

Third, the dependence on the disturber removal by himself in the near time although he plans to stay for long time to exhaust the sensor nodes in his area; the detection techniques plans to detect the channel after some time if they detect jamming in the communication channel. So, no need to use a periodic jamming detection technique because the disturber has planned to stay for long time.

Forth, the time used to detect the presence of the jamming in the communication channel causes a delay time to send the sensed data quickly. This drawback gives a success to the disturber in his task without any efforts.

It has been proved the preference of use PSR than carrier sense time with MAC protocols at the sender side and also the preference of use PDR than signal strength at the receiver side [1]. As shown later, the dependence on PSR and PDR specifies the presence of jamming in the communication channel while the use of carrier sense time and signal strength after PSR or PDR to specify the jamming type. So, this enhancement solves the second and the forth drawbacks of periodic detection techniques while the first and the third drawbacks can be solved by a defensive technique.

B. Disturber localization methods

The main requirements of the disturber localization methods are:

1. A suitable node localization protocol to specify the exact node positions.
2. Suitable defensive mechanism to ensure the arrival of node information to the sink correctly.
3. All victim nodes positions should be known and also the boundary nodes positions should be known as in the case of VFIL method.

The disturber localization methods have some drawbacks:

- The drawback of both CL and DCL methods is the consideration of the disturber position inside the communication area of the victim nodes although the disturber can jam the victim nodes from outside their communication area. The disturber can jam the same victim nodes with the same boundary nodes from different positions as shown in Fig. 6.
- The drawback of WCL is the consideration of the distance, d_i, between the victim nodes and the disturber is known in its calculations. Three victim nodes only can specify the disturber position exactly if d_i is known. So, the assumption of d_i known in the estimation is not acceptable.
- The drawback of VFIL method is the consideration of the transmitted power, P_{txj}, of the disturber known although the disturber can jam an area wider than the communication area of the victim node with unknown P_{txj} as shown in Fig. 6. So, the weights determinations are undefined for unknown P_{txj}.

The proposed localization method considered only the known parameters which area easily to measure. These parameters are the received signal strength of the disturber and the positions of the victim nodes which announce the presence of jamming in its area. So, the disturber position can be specified correctly even if his position was outside the WSN. The localization methods requires only a defensive technique to carry these jamming information to the sink.

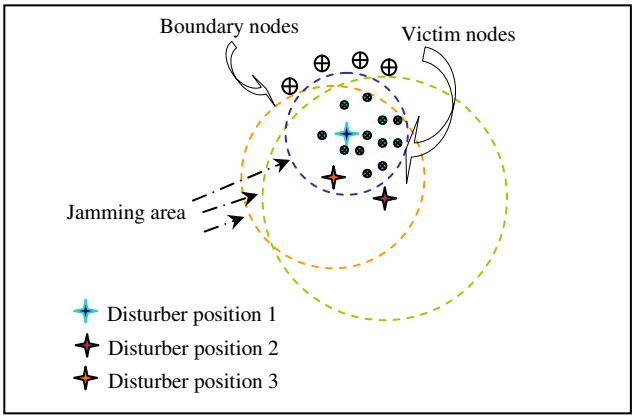

Figure 6. Three different positions for the disturber with different transmitted power or different jamming area

C. Defensive techniques

The survey on the defensive techniques showed their drawbacks as follows:

1. Avoid dealing with the victim nodes gives a success for the disturber in his task. The disturber plans to exhaust the victim nodes for long time. So, the disturber will accelerate the energy depletion of the victim nodes.
2. The spatial retreats [9] solution needs a vehicle or a creature to carry the sensor node to another position because the victim nodes cannot move by their selves. So, it should have enough space for motion without any obstacles. The motion by a vehicle needs enough energy to carry the sensor node to another space. So, we suggest to use the vehicle energy to send the data by high transmitted power instead of the motion to another position.
3. The use of trigger nodes as receivers [16] change the sensor node task to send the sensed data to the sink and no plan to send data from the sink to the sensor node. So, it gives the ability for the reactive disturber to end the life of the trigger nodes.
4. The problem of FHSS is the synchronization between the sender and the receiver or the both side must take this action together but, this is difficult in the presence of jamming. So, it was suggested to use FHSSS technique between the sender and the receiver as a communication technique. But, the disturbers can change from their natural to jam all available communication channels by a rate higher than FHSS.
5. Although both FHSS and DSSS spread the spectrum, they improve the performance by reducing the number of retransmission processes.
6. The use of O-QPSK as a modulation technique with FHSS and DSSS improves the performance of the transmission process in the face of effectiveness of jamming.
7. The disturber can jam all available communication channels even if secure the hop sequence or PN code as in Ares nodes because the disturber depends on disruption all the available channels by a rate higher than FHSS and also the secure of PN does not face the disturber but enhance the data encryption not more.

As a result, it should use a defensive technique to deal with the jamming rather than avoid dealing with it. And also, all suggested defensive mechanisms cannot remove the effectiveness of jamming from the communication channel because the probability of retransmission processes still exists due to channel jamming.

O-QPSK is tested by different jamming signals and compared with the two new defensive techniques: Inhomogeneous Carriers Modulation Technique (ICMT) and Hybrid Amplitude Modulation and Frequency Modulation

(FM-AM). The jamming signals shown in (23-27) where: A_j and f_c are the amplitude and frequency of the jamming signals. These modulation techniques are tested under effectiveness of jamming using an image of size 100x80 as shown in Fig. 7, A_j=±1, and f_c=2.4GHz. The quality of the reconstructed image is measured by Peak Signal-to-Noise Ratio (PSNR) and is written down in table (2). Fig. 8 shows the reconstructed image at the receiver according to the measured PSNR shown in table (2). In the end, the results show that:

1. O-QPSK is affected by all jamming signals except J_{a5} at A_j=±2.
2. ICMT is affected only by J_{a2} and J_{a3} as shown in table (2).
3. FM-AM is not affected by any jamming signals because of the dependence on the frequency which is the weakness point of the disturber.
4. FM-AM represents each one byte by one signal while both O-QPSK and ICMT represents each two bits by one signal in a time period equal to the two bits time. So, FM-AM enhances the data rate 8-times the data rate of O-QPSK.
5. No effectiveness of jamming means no need to the redundancy bits of the coding techniques. So, the data rate will be enhanced by removal these redundancy bits from the message.
6. No effectiveness of jamming prolongs the battery lifetime of the sensor node because no retransmission process and no delay time spent to detect the presence of jamming in the communication channel.
7. The attackers cannot change the contents of the transmitted data.
8. The disturber localization methods can use FM-AM to ensure the reception of jamming information to the sink correctly. And also, FM-AM solves the first the third drawbacks of the periodic detection techniques shown later.

`

Figure 7. Original image

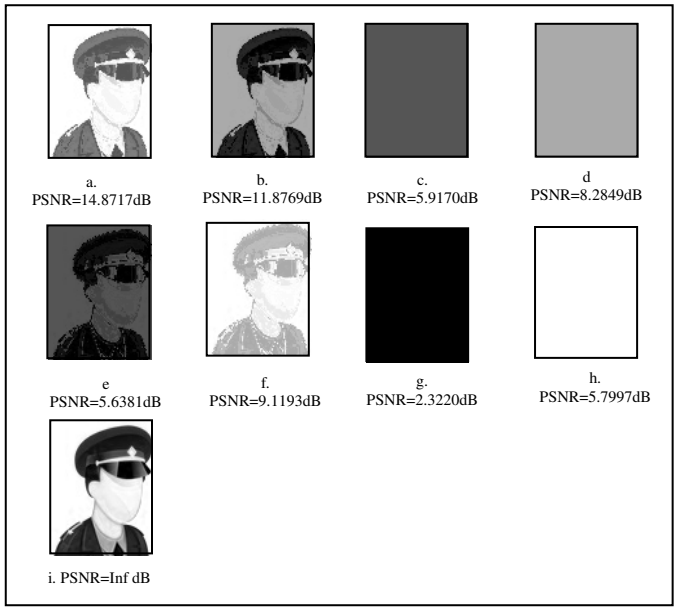

Figure 8. Reconstructed images

Table 2. Measured PSNR (in dB) of modulation techniques

	A_j	O-QPSK	ICMT	FM-AM
J_{a1}	-1	14.8717	Inf	Inf
	1	11.8769	Inf	Inf
J_{a2}	-1	5.6381	2.3220	Inf
	1	9.1193	5.7997	Inf
J_{a3}	-1	5.9170	2.3220	Inf
	1	8.2849	5.7997	Inf
J_{a4}	-1	14.8717	Inf	Inf
	1	11.8769	Inf	Inf
J_{a5}	-1	Inf	Inf	Inf
	1	Inf	Inf	Inf
	-2	14.8717	Inf	Inf
	2	11.8769	Inf	Inf

$$J_{a1}(t) = A_j \sin(2\pi f_c t) \quad (23)$$

$$J_{a2}(t) = A_j \cos(2\pi f_c t) \quad (24)$$

$$J_{a3}(t) = A_j\left[\sin(2\pi f_c t) + \cos(2\pi f_c t)\right] \quad (25)$$

$$J_{a4}(t) = A_j square(2\pi f_c t) \quad (26)$$

$$J_{a5}(t) = \frac{A_j}{2}\left[square\left(2\pi f_c t\right)+1\right]$$

(27)

V. Conclusions

Data transmission in WSN faces many threats. Jamming is one of these threats causing retransmission processes and exhaustion the battery energy of the sensor node. This threat is analyzed from three directions: detection techniques, and localization methods, and defensive techniques. The enhancements in these techniques came from their drawbacks. The enhancement in the detection techniques prolong the sensor node lifetime. The enhancement in the disturber localization methods specifies the disturber position correctly. And also, it guides us to deal with the threat without high efforts manually or automatically. The paper introduced two proposed techniques as defensive techniques, ICMT and FM-AM. ICMT is the enhancement of O-QPSK. FM-AM is the hybrid AM and FM. The quality of reconstructed image at the receiver showed the weakness point of the disturber in its inability to jam the signal frequency. This enhancement, FM-AM, guides us to remove the redundancy of the coding techniques from the transmitted packets and reducing the byte duration time to equal the bit duration time. FM-AM can face the other threats which change the contents of the transmitted data and helps the localization methods to do their task correctly. And also, it enhances the overall performance of WSN because of the improvement in the data rate without effectiveness of jamming which prolong the battery lifetime of the sensor node.

References

[1]. X. Wenyuan, T. Wade, Z. Yanyong, and W. Timothy, "The feasibility of launching and detecting jamming attacks in wireless networks", Mobihoc 2005, Urbana-Champaign, Illinois, USA, pp. 25-27, May 2005.

[2]. S. Periyanayagi and V. Sumathy, "A swarm based defense technique for jamming attacks in wireless sensor networks", International Journal of Computer Theory and Engineering, vol. 3, no. 6, pp. 816-821, Dec. 2011.

[3]. S. Uke, A. Mahajan, and R. Thool, "UML modeling of physical and data link layer security attacks in WSN", International Journal of Computer Applications, vol. 70, no. 11, pp. 25-28, May 2013.

[4]. R. Muraleedharan and L. Osadciw, "Jamming attack detection and countermeasures in wireless sensor network using ant system", Proc. Wireless Sensing and Processing, vol. 6248, pp. 62480G, 2006.

[5]. Sanchita Gupta and Pooja Saini, "Modified Pairwise Key Pre-distribution Scheme with Deployment Knowledge in Wireless Sensor Network", International Journal of Scientific Research in Network Security and Communication, Volume-01, Issue-02, Page No (21-23), May -Jun 2013.

[6]. L. Mingyan, K. Iordanis, and P. Radha, "Optimal jamming attacks and network defense policies in WSN," IEEE INFOCOM, 2007.

[7]. R. Shivanagu and C. Deepti, "An assessment of security mechanisms against reactive disturber attack In wireless sensor networks", International Journal in Foundations of Computer Science & Technology (IJFCST), vol. 3, no.3, pp. 31-40, May 2013.

[8]. M. Dawood, L. Ahila, S. Sadasivam, and G.Athisha, "Image compression in wireless sensor networks- A survey", International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS, New York, USA, vol.1, no. 9, pp. 11-15, Feb. 2012.

[9]. W. Xu, T. Wood, W. Trappe, Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service", In WiSe'04: Proceedings of the 2004 ACM Workshop on Wireless Security, pp. 80–89, New York, USA, 2004.

[10]. G. Zhou, T. He, J. Stankovic, and T. Abdelzaher, "RID: Radio Interference Detection in wireless sensor networks", In Proceedings of the IEEE INFOCOM'2005, 2005.

[11]. C. Murat, G. AKIRO, and A. Turan, "Design and evaluation of a query-based jamming detection algorithm for wireless sensor networks", Turk J Elec Eng & Comp Sci, vol. 19, no. 1, pp. 1-19, 2011.

[12]. K. Siddhabathula, Q. Dong, L. Donggang, and M. Wright, "Fast jamming detection in sensor networks", IEEE International Conference on Communications (ICC), 2012.

[13]. A. Wood, J. Stankovic, S. Son, "JAM: A jammed-area mapping service for sensor networks", 24th IEEE Real-Time Systems Symposium (RTSS'2003), pp. 286–297, 2003.

[14]. C. Tianzhen, L. Ping, and Z. Sencun, "An algorithm for disturber localization in wireless sensor networks", IEEE 26th International Conference on Advanced Information Networking and Applications (AINA), 2012.

[15]. A. Wood, J. Stankovic, and G. Zhou, "DEEJAM: Defeating Energy Efficient Jamming", In The 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), San Diego, CA, June 2007.

[16]. S. Incheol, S. Yilin, X. Ying, M. Thai, and T. Znati, "Reactive jamming attacks in multi-radio wireless sensor networks: An efficient mitigating measure by identifying trigger nodes", FOWANC'09, New Orleans, Louisiana, USA, pp. 87-96, May 2009.

[17]. N. Bulusu, J. Heidemann, and D. Estrin, "Gps-less low cost outdoor localization for very small devices," in IEEE Personal Communications Magazine, pp. 28-34, 2000.

[18]. J. Blumenthal, R. Grossmann, F. Golatowski, and D. Timmermann, "Weighted Centroid localization in ZigBee-based sensor networks", in WISP'07: Proceedings of the IEEE International Symposium on Intelligent Signal Processing, pp. 1-6, 2007.

[19]. H. Liu, W. Xu, Y. Chen, and Z. Liu, "Localizing disturbers in wireless networks," in PERCOM'09: Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications, pp. 1-6, 2009.

[20]. A. Mpitziopoulos and D. Gavalas, "An effective defensive node against jamming attacks in sensor networks", Security and Communication Networks Security Comm. Networks, Published online in Wiley InterScience, 2008.

[21]. M. Cagalj, S. Capkun, and J. Hubaux, "Wormhole-based antijamming techniques in sensor networks", IEEE Transactions on Mobile Computing, May 2006.

[22]. RFC 2898. PKCS #5: Password-based cryptography specification version 2.0: http://rfc.net/rfc2898.html

[23]. M. Matsumoto and T. Nishimura, "Mersenne twister: a 623-dimensionally equidistributed uniform pseudo-random number generator", ACM Transactions on Modeling and Computer Simulation, vol. 8, no. 1, Jan. 1998.

[24]. L. Rizzo, "Effective erasure codes for reliable computer communication protocols", ACM CCR, vol. 27, no. 2, pp. 24–36, 1997.

[25]. K. Siwiak, "Ultra-wide band radio: Introducing a new technology", Vehicular Technology Conference (VTC 2001) Spring, IEEE VTS 53rd, vol. 2, pp. 1088–1093, 2001.

Appendix A

Friis transmission equation [20] is defined by:

$$P_{rx} = P_{tx}\frac{G_{tx}G_{rx}\lambda^2}{16\pi^2 d^2 L} \quad \text{(A.1)}$$

Where: P_{rx} is the received power at the receiver side, P_{tx} is the transmitted power at the sender side, G_{tx} and G_{rx} are the antenna gain at the sender and the receiver side respectively, λ is the wavelength, d is the distance between the receiver and the transmitter, and L is the system loss factor. So, the received power at the victim node-1 can be determined by:

$$P_{rx1} = P_{tx\,j}\frac{G_{txj}G_{rx1}\lambda^2}{16\pi^2 d_1^2 L} \quad \text{(A.2)}$$

Then,

$$P_{rx1}d_1^2 = P_{tx\,j}\frac{G_{txj}G_{rx1}\lambda^2}{16\pi^2 L} \quad \text{(A.3)}$$

And also, for victim nodes 2, 3, and 4, we can get:

$$P_{rx2}d_2^2 = P_{tx\,j}\frac{G_{txj}G_{rx2}\lambda^2}{16\pi^2 L} \quad \text{(A.4)}$$

$$P_{rx3}d_3^2 = P_{tx\,j}\frac{G_{txj}G_{rx3}\lambda^2}{16\pi^2 L} \quad \text{(A.5)}$$

$$P_{rx4}d_4^2 = P_{tx\,j}\frac{G_{txj}G_{rx4}\lambda^2}{16\pi^2 L} \quad \text{(A.6)}$$

So, we can say that:

$$P_{rx1}d_1^2 = P_{rx2}d_1^2 = P_{rx3}d_1^2 = P_{rx4}d_4^2 = P_{tx\,j}\frac{G_{txj}G_{rx}\lambda^2}{16\pi^2 L} \quad \text{(A.7)}$$

By considering all G_{rxi} of the victim nodes are the same. From the analytic geometry, the distance between two points in the xy-plane or between a victim node (x_i, y_i) and the disturber position (x_j, y_j) can be determined by using the distance formula as follows:

$$d_1^2 = (x_j - x_1)^2 + (y_j - y_1)^2 \quad \text{(A.8)}$$

$$d_2^2 = (x_j - x_2)^2 + (y_j - y_2)^2 \quad \text{(A.9)}$$

$$d_3^2 = (x_j - x_3)^2 + (y_j - y_3)^2 \quad \text{(A.10)}$$

$$d_4^2 = (x_j - x_4)^2 + (y_j - y_4)^2 \quad \text{(A.11)}$$

Subtract: (A.8)-(A.9), we can get:

$$\begin{aligned} d_1^2 - d_2^2 &= \left(-2x_1x_j + x_1^2 - 2y_1y_j + y_1^2\right) \\ &-\left(-2x_2x_j + x_2^2 - 2y_2y_j + y_2^2\right) \\ &= x_j\left(2(x_2 - x_1)\right) + y_j\left(2(y_2 - y_1)\right) \\ &+\left(x_1^2 - x_2^2\right) + \left(y_1^2 - y_2^2\right) \end{aligned} \quad \text{(A.12)}$$

Subtract: (A.8)-(A.10), we can get:

$$\begin{aligned} d_1^2 - d_3^2 &= \left(-2x_1x_j + x_1^2 - 2y_1y_j + y_1^2\right) \\ &-\left(-2x_3x_j + x_3^2 - 2y_3y_j + y_3^2\right) \\ &= x_j\left(2(x_3 - x_1)\right) + y_j\left(2(y_3 - y_1)\right) \\ &+\left(x_1^2 - x_3^2\right) + \left(y_1^2 - y_3^2\right) \end{aligned} \quad \text{(A.13)}$$

By using (A.7), we can get:

$$\frac{d_1^2 - d_2^2}{d_1^2 - d_3^2} = \frac{1 - \frac{d_2^2}{d_1^2}}{1 - \frac{d_3^2}{d_1^2}} = \frac{1 - \frac{P_{rx1}}{P_{rx2}}}{1 - \frac{P_{rx1}}{P_{rx3}}} = \frac{P_{rx2}P_{rx3} - P_{rx1}P_{rx3}}{P_{rx2}P_{rx3} - P_{rx1}P_{rx2}} \quad \text{(A.14)}$$

Equal (A.14) by the division result of (A-12)÷(A.13), we will get:

$$\frac{P_{rx2}P_{rx3} - P_{rx1}P_{rx3}}{P_{rx2}P_{rx3} - P_{rx1}P_{rx2}} = \frac{x_j\left(2(x_2 - x_1)\right) + y_j\left(2(y_2 - y_1)\right) + \left(x_1^2 - x_2^2\right) + \left(y_1^2 - y_2^2\right)}{x_j\left(2(x_3 - x_1)\right) + y_j\left(2(y_3 - y_1)\right) + \left(x_1^2 - x_3^2\right) + \left(y_1^2 - y_3^2\right)}$$

Finally, we can get:

$$S_{x1}x_j + S_{y1}y_j = C_1 \quad \text{(A.15)}$$

Where:

- $S_{x1} = 2(x_2 - x_1) - 2(x_3 - x_1)\frac{P_{rx2}P_{rx3} - P_{rx1}P_{rx3}}{P_{rx2}P_{rx3} - P_{rx1}P_{rx2}}$
- $S_{y1} = 2(y_2 - y_1) - 2(y_3 - y_1)\frac{P_{rx2}P_{rx3} - P_{rx1}P_{rx3}}{P_{rx2}P_{rx3} - P_{rx1}P_{rx2}}$
- $C_1 = \left[\left(x_1^2 - x_3^2\right) + \left(y_1^2 - y_3^2\right)\right]\frac{P_{rx2}P_{rx3} - P_{rx1}P_{rx3}}{P_{rx2}P_{rx3} - P_{rx1}P_{rx2}} - \left[\left(x_1^2 - x_2^2\right) + \left(y_1^2 - y_2^2\right)\right]$

By the same way

Subtract: (A.9)-(A.10), we can get:

$$d_2^2 - d_3^2 = \left(-2x_2x_j + x_2^2 - 2y_2y_j + y_2^2\right) - \left(-2x_3x_j + x_3^2 - 2y_3y_j + y_3^2\right) = x_j\left(2(x_3 - x_2)\right) + y_j\left(2(y_3 - y_2)\right) + \left(x_2^2 - x_3^2\right) + \left(y_2^2 - y_3^2\right) \quad \text{(A.16)}$$

Subtract: (A.9)-(A.11), we can get:

$$d_2^2 - d_4^2 = \left(-2x_2x_j + x_2^2 - 2y_2y_j + y_2^2\right) - \left(-2x_4x_j + x_4^2 - 2y_4y_j + y_4^2\right) = x_j\left(2(x_4 - x_2)\right) + y_j\left(2(y_4 - y_2)\right) + \left(x_2^2 - x_4^2\right) + \left(y_2^2 - y_4^2\right) \quad \text{(A.17)}$$

By using (A.7), we can get:

$$\frac{d_2^2 - d_3^2}{d_2^2 - d_4^2} = \frac{1 - \frac{d_3^2}{d_2^2}}{1 - \frac{d_4^2}{d_2^2}} = \frac{1 - \frac{P_{rx2}}{P_{rx3}}}{1 - \frac{P_{rx2}}{P_{rx4}}} = \frac{P_{rx3}P_{rx4} - P_{rx2}P_{rx4}}{P_{rx3}P_{rx4} - P_{rx2}P_{rx3}} \quad \text{(A.18)}$$

Equal (A.18) by the division result of (A-16)÷(A.17), we will get:

$$\frac{P_{rx3}P_{rx4} - P_{rx2}P_{rx4}}{P_{rx3}P_{rx4} - P_{rx2}P_{rx3}} = \frac{x_j\left(2(x_3 - x_2)\right) + y_j\left(2(y_3 - y_2)\right) + \left(x_2^2 - x_3^2\right) + \left(y_2^2 - y_3^2\right)}{x_j\left(2(x_4 - x_2)\right) + y_j\left(2(y_4 - y_2)\right) + \left(x_2^2 - x_4^2\right) + \left(y_2^2 - y_4^2\right)}$$

Finally, we can get:

$$S_{x2}x_j + S_{y2}y_j = C_2 \quad \text{(A.19)}$$

Where:

- $S_{x2} = 2(x_3 - x_2) - 2(x_4 - x_2)\frac{P_{rx3}P_{rx4} - P_{rx2}P_{rx4}}{P_{rx3}P_{rx4} - P_{rx2}P_{rx3}}$
- $S_{y2} = 2(y_3 - y_2) - 2(y_4 - y_2)\frac{P_{rx3}P_{rx4} - P_{rx2}P_{rx4}}{P_{rx3}P_{rx4} - P_{rx2}P_{rx3}}$
- $C_2 = \left[\left(x_2^2 - x_4^2\right) + \left(y_2^2 - y_4^2\right)\right]\frac{P_{rx3}P_{rx4} - P_{rx2}P_{rx4}}{P_{rx3}P_{rx4} - P_{rx2}P_{rx3}} - \left[\left(x_2^2 - x_3^2\right) + \left(y_2^2 - y_3^2\right)\right]$

Divide: (A.15)÷S_{y1}, we will get:

$$\frac{S_{x1}}{S_{y1}}x_j + y_j = \frac{C_1}{S_{y1}} \quad \text{(A.20)}$$

Divide: (A.19)÷S_{y2}, we will get:

$$\frac{S_{x2}}{S_{y2}}x_j + y_j = \frac{C_2}{S_{y2}} \quad \text{(A.21)}$$

Subtract: (A.20)-(A.21), we will get:

$$\left(\frac{S_{x1}}{S_{y1}} - \frac{S_{x2}}{S_{y2}}\right)x_j = \left(\frac{C_1}{S_{y1}} - \frac{C_2}{S_{y2}}\right)$$

Then,

$$x_j = \frac{C_1S_{y2} - C_2S_{y1}}{S_{x1}S_{y2} - S_{x2}S_{y1}} \quad \text{(A.22)}$$

And y_j can be calculated from (A.20) as follows:

$$y_j = \frac{1}{S_{y1}}\left(C_1 - x_jS_{x1}\right) \quad \text{(A.23)}$$

Authors Profile

Nagy Wadie Messiha was born in Asiut Egypt, 1942. He received the B.S. in Electrical Engineering Telecommunication Department, Ein Shams University, Cairo, Egypt, June 1965, and M.S. in "Telecommunication Engineering", Helwan University, Cairo, Egypt, 1973, and the "dipl. Ing" and "Dr. Ing" in Communicationn engineering from University of Stuttgart,W.Germany, in 1978, and1981 respectively. Currently he is a Professor at the department of communication engineering, Menoufia University, Menouf, Egypt. His research interests are in traffic modelling and performance enhancement in wireless networks, Computer and

communication network Planning, cognitive networks, and network Security.

Nawal El-Fishawy She received the PhD degree in mobile communications the faculty of Electronic Eng., Menoufia University, Menouf , Egypt ,in collaboration with Southampton University in 1991 .Now she is professor at Computer Science and Engineering Dept., Faculty of Electronic Eng. Her research interest includes computer communication networks with emphasis on protocol design, traffic modeling and performance evaluation of broadband networks and multiple access control protocols for wireless communications systems and networks. Now she directed her research interests to the developments of security over wireless communications networks (mobile communications, WLAN, Bluetooth), VOIP, and encryption algorithms.

AbdelRahman A. Elkafas received the B.S. in Nuclear Engineering, Alexandria University, Alexandria, Egypt, June 1980, and M.S. in " Analysis of Residual Heat Removal Systems in PWR-NPPs ", Alexandria University, Alexandria, Egypt, June 1990, and Ph.D in " Safety Analysis of an Expert Reactor Protection System in PWR-NPPs", Alexandria University, Alexandria, Egypt, June 1996. He was an associate professor in 2002, Nuclear Research Centre, Egypt. Currently, he is a Professor in the Nuclear Research Centre, Egypt. He is interested in Safe Operation of Nuclear Reactors, Automatic Control of research reactors, and Physical protection systems (design and evaluation).

Ahmed H. Madian was born in 1975. He received the B.Sc. degree with honors, the M.Sc., and the Ph.D. degrees in electronics and communications from Cairo University, Cairo, Egypt, in 1997, 2001, and 2007, respectively. He is currently an Associate Professor in the Electronics Engineering Department, Micro-Electronics Design Center, Egyptian Atomic Energy Authority, and Cairo, Egypt. Dr. Madian served as Assistant Professor in the Electronics Engineering Department, Faculty of Information Engineering and Technology, German University in Cairo (GUC) from 2008 till now. Dr. Madian is the co-author of 20 research papers in different scientific journals and has served as program and publication chair for many conferences. He is a Senior member IEEE and co-founder for the IEEE Robotics Chapter- Egypt section (best chapter on Region 8 for 2013). His research interests are in circuit theory; low-voltage analog CMOS circuit design, current-mode analog signal processing, digital VLSI, system security and mixed/digital applications on field programmable gate arrays.

Amr M. Kishk was born in Ashmun city, Egypt, on July 11, 1981. He received the B.S. in Electronics and Electrical Communication Engineering, Menoufia University, Menouf, Egypt, 2003, and M.S. in "Data Security in Wireless Local Area Network", Menoufia University, Menouf, Egypt, 2010. Now, he works as a lecturer assistant in Egyptian Atomic Energy Authority (EAEA), Cairo, Egypt. His research interests to Wireless Sensor Network (WSN), Data Security in Wireless Network.

