American Journal of Networks and Communications
2013; 2(2) : 28-39
Published online April 2, 2013 (http://www.sciencepublishinggroup.com/j/ajnc)
doi: 10.11648/j.ajnc.20130202.12

SciencePG
Science Publishing Group

Defending WSNs against jamming attacks

Abdulaziz Rashid Alazemi

Computer Engineering Department, Kuwait University, Kuwait

Email address:
fortinbras222@hotmail.com (A. R. Alazemi)

To cite this article:
Abdulaziz Rashid Alazemi. Defending WSNs Against Jamming Attacks, *American Journal of Networks and Communications.* Vol. 2, No. 2, 2013, pp. 28-39. doi: 10.11648/j.ajnc.20130202.12

Abstract: Wireless sensor networks WSNs consist of a group of distributed monitor nodes working autonomously together cooperatively to achieve a common goal. Generally they face many threats, threatening the security and integrity of such networks. Jamming attacks are one of the most common attacks used against WSNs. In this paper we discuss the jamming attack and defense mechanisms proposed by two papers and suggest improvements on those four approaches.

Keywords: Jamming Attacks, Network Security, Wireless Sensor Networks

1. Introduction

WSNs are generally heterogeneous distributed wireless radio networks, with little to no manual operation. Sensors or nodes use low power frequencies to conserve energy and prolong battery life. Thus, their transmission range is often low and relay on other sensors to route their messages. For this reason, multi-hop communications [1] are used as an alternative for single hop communications as they consume less power. The word node and sensor are used interchangeable in the text, but they reference the same thing. Signal propagation problems stem from long-distance wireless communication were the signal might be jammed, lost, blocked, due to physical objects, or its power level drops before reaching its destination. That said WSN usually operate in an autonomous fashion, with minimal intervention. They are usually scalable networks with high fault tolerance aspects, as the sensors, gateway sensors, or even the links making the network may fail at any time during operation.

WSNs consist of inexpensive sensors or nodes, geographically scattered to cover an area in which the WSN is deployed for monitoring. Communications are done solely by radio frequency, which is inherently insecure. The sensors are cheap component off the shelf units built using the prevalent Micro Electro Mechanical Systems MEMS technologies. They consist of very simple designs; they consist of a battery, a small flash memory ROM (using a primitive OS like TinyOS), a microcontroller, a radio transceiver with an antenna and a transducer to acquire readings. The transducer is a device that converts energy from one domain to another [2]. these sensors is their low power consumption necessary to insure long battery life, as battery power is usually not replenshable. Another characteristic is the robustness of these sensors as they are placed in industrial, military, and hazardous zones. Other importance characteristic is their long life expectancy as they monitor areas for a long time with minimal intervention and maintenance, see Fig.1.

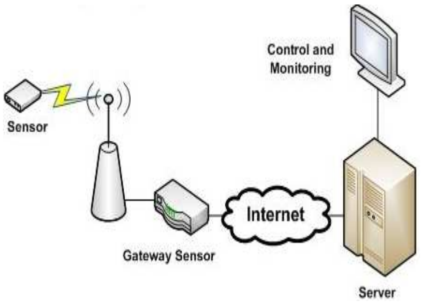

Figure 1. *WSN Architecture.*

The development of WSNs can be traced back to the Cold War, were the SOund Surveillance System (SOSUS) was developed and deployed in the United States as a surveillance system. SOSUS consisted of sensors deployed at the bottom of the sea to monitor Soviet submarines and possible attacks. late 1990’s that WSNs got huge commercial breakthrough. The huge advancements in digital consumer electronics have made low-cost, low power, multifunctional radio sensors -the elements that make up the WSN- became a commodity [3]. Protocols especially designed for WSN were developed like ZigBee/IEEE 802.15.4 and ISA 100 [4]. Protocols were specified to address the heterogeneity and diversity of sensors and other components that make up the WSN and intercommunications between these components.

Counteracting this issue, the Institute of Electrical and Electronics Engineers IEEE and the National Institute of Standards and Technology NIST in 1993 worked on IEEE 1451, the Standard for Smart Sensor Networks.

1.1. Applications of WSNs

WSN applications are varied, due to the advent of radio networks [5]. Monitoring is an application for WSNs, surveillance of secure or territorial areas were motion sensors are deployed to locate any source of motion. Pollution control, were sensors monitor air, water pollution, greenhouse effects, and waste control systems, used in heavily populated cities. Disaster alert systems, like forest fire, earthquakes, and tornados, were many weather and geological sensors are used to forecast natural disasters. Major applications of WSNs are in industrial monitoring, to monitor mechanical ware of large industrial machines, give day-to-day status checks.

Structural monitoring is an application were WSNs dominate, were sensors measure the exact structural integrity of large structures like bridges, dams and skyscrapers, these sensors measure pressure, bending, heat and wind speeds, readings that are vital to control and safety engineers. WSNs are also used in planetary and space exploration, were satellites are in practice the sensors. As more satellites are deployed and together, they form a WSN that monitors interplanetary movements and anti-matter presence [6]. Medical monitoring is another new field that WSNs are used in, were a micro sensor is attached to a device that is implanted inside an organ, thus providing real time monitoring of the device and the organ.

2. Related Work

WSN are used in many applications and in some applications, security compromises may lead to threat to national security, commercial lose or even environmental damage [4]. WSNs use radio frequency for communication between its different parts, this is by default a shared medium, security becomes a serious issue [7]. There are many attacks against WSN, but jamming attacks are the most common and widely used attacks that threaten WSNs. Jamming attacks are relatively cheap and easy to implement than other attack types, for example synch flooding. Usually we can defend against jamming attacks using two main methods, spread spectrum techniques and authentications as in [8].

In [9] the authors represented SPREAD (Second-generation Protocol Resiliency Enabled by Adaptive Diversification), a technique to resist smart jammers. By smart jammers, we mean jammers that act more like reactive jammers, discussed later. These jammers only jam the payload of the delivered packet, knowing exactly what protocol is in use. This serious attack will have a high rate of corrupting the data carried by the packets and can effectively reduce throughput to zero. Furthermore, these smart jammers utilize cross-layer attacks, they jam certain layers. Smart jammers reduce the power needed to jam the entire channel but they should carefully time their attacks to target protocol specific information.

The authors also mention other attempts to defend against jamming; the spectrum spread techs, and how it is not practical for WSNs as it was developed for voice communications. They mention that there are jam attack patterns that target specific layer protocols, the Wolfpack program [10]. This ultimately leads to SPREAD, a technique that avoids smart jammers that target specific protocols, by using a parallel collection of network protocol stacks and switching between them.

In [11] the authors represented a novel mapping service to detect jamming attacks. JAM (Jamming Area Mapping) is a service that provides quick and accurate jamming attack response, which alerts the WSN for a possible jamming attack in effect. As geographic information is important for most WSNs, knowing where exactly the jamming is and what sensors does it effect, certainly will help in mitigating and leveraging its effects. As jammers often, attack specific areas like the gateway sensor area or critical proxy areas. Finding where the jamming are coming from and what sensors are currently cut-off, is very essential in the next step which is avoiding or challenging the jammer. The authors suggested that cost of other solutions like spread spectrum techniques [12] is high, and only practical in military WSN, were security compromise is not an option.

3. Security Issues

Security of WSNs is an important research area, as it plays a major role defending from malicious hackers and possibly terrorists. WSN are used in many applications and some applications security compromise may lead to threat to national security, commercial lose or even environmental damage, making security breaches not an option. Security issues include confidentiality, meaning that authorized personnel shall not access the data; this is hard due to the use of radio waves. In addition, another issue is data integrity that means that the data is not tampered with when received by the other side. Service availability is another security issue, availability means that authorized access of data and other WSN resources is made ready when requested or demanded. Attackers range from the hackers, for blackmailing and monetary gain, or industry spies, gathering confidential business insight, or espionage spies, for confidential and top secret information.

Since WSNs use radio frequency for communication between its different parts, this is by default a shared medium, security becomes a serious issue. In addition, the constraints such as limited processing and limited memory capabilities of the sensors and their dependency on battery power alone make it more difficult to keep these networks secure and safe. WSNs are especially venerable to Denial of Service Attacks DoS, since we have limited processing capabilities and the dependency on battery power for the scattered sensors and the inability to secure the shared medium used for communications.

3.1. Types Attackers

Attacks on WSNs come from two groups, insiders, or outsiders. Outsiders usually sniff the packets sent over the channels; they can tamper with the data or jam the signals all together. Insiders are capable of damage that is more malicious. As they have certain keys the nodes use for their communications. Insiders with keys can take hold of one of the sensors, inject their own programming to harm the whole WSN or even take parts out like in a blackout only to insert their own nodes in order to take hold of the entire WSN.

Aside from this categorization of attackers, we will classify attackers into four kinds as found in [15]. First kind is the Passerby; they are not determined, very little knowledge about the WSN but with common tools that disturb the flow of the WSN work. More malicious are the Vandals, they intend to damage the WSN on purpose, with significantly more resources and inside knowledge. Even more malicious are Hacker, extremely determined and fueled by curiosity or financial interests. Hackers are skilled network intruders, they tend to cause damage spontaneously and to show off or just for self-recognition. Another kind is the Raiders, motivated by personal, economical, or political gains. They are determined, usually very well knowledgeable with lots of insiders' information and backed up by organizations or governments. Finally, we have the Terrorist or Foreign Powers; they cause international security damage by breaking in or hindering of critical military or civil systems. Politically motivated, in most cases will die for their cause, highly knowledgeable. Terrorists are usually well funded with money and work force; this in effect allows them to cause the most harm among all the kinds of attacks. Security policies were mainly driven by the amount of damage possible from the kind of attacks that may attack the WSN.

Usually attackers with high computational powers as PCs or laptops do much harm than malicious attackers using injected sensors. These attacks usually have virtually unlimited processing powers and can easily out number or use brute force to enter the WSN. Furthermore, they can send their own programming into the entire network through fake packets in effect overriding the original programming of the sensors. In addition, when the attacker is a group of computers, they can launch what it is called a sandwich attack. Sandwich attacks are attacks that try to take control of more than a single node in the network at different time. Allowing attackers to acquire authentication keys and group keys used for exchanging secure messages around, in effect taking control of the entire WSN. In addition, attackers can cause target localization intrusions, when WSNs are used for intruder detection and motion, attackers can mislead the sensors by faking, or misinterpreting their signals thus giving wrong readings making it possible to go under the radar under the area WSN is covering.

3.2. Layers of Threats

Let us dissect the security threats facing WSNs by the network layers [2]. First the physical layer, we have the jamming and tampering, were the sending and receiving frequencies are jammed or distorted. Then link layer, we have exhausting floods, were attackers flood links, and make packets drop. We also have collision attacks, it is a technique to make packet drop and get reordered more frequently thus disturbing the data transmission in the WSNs. Another attack unique to WSNs is the denial of sleep attacks [14], in these attacks external intruders keeps the sensors busy with fake communications or even sending fake or empty packets in order to let the sensor in the on mode as much as possible. Preventing sensors to go to sleep mode will ultimately drain the battery, once the battery is drained the sensor goes down, thus making the network go into a partitioning process and blacking out parts of it.

In the network layer, we have the malicious sinkhole and wormhole attacks were packets are drawn out of the network to different destinations the attacker wants, usually their own databases. The wormhole attack may also include selective forwarding attacks, were packets are forwarded by the wormhole to different locations maliciously. Transport layer, we have the synchronization flooding attacks we channels are flooded with fake packets that require a full TCP communication. Finally in the application layer, we have the clone attack were a node is taken over by a clone node with the same key and identity. In addition, a popular attack is the DoS attacks, since WSNs are inherently weak to it, an attacker can easily deny the service by sending fake empty messages continuously on the same receiving frequency of the sensors. Other application layer attacks are Deluge or reprogramming attacks [9]. These attacks often done by professional insiders were they send their own programming using authenticated messages to certain sensors, the program is like a virus it replicate itself through the network resulting in complete take over by the attackers. A summary of the attacks is shown in table 1, which is illustrated using the Open Systems Interface standard network layers OSI.

Table 1. *OSI Layers with the corresponding threat and defense mechanism.*

Network Layer	**Attack**	**Defense**
Physical	Jamming, Tampering	Spectrum spread, Authentication
Link	Collision, Exhausting flood, Denial-of-sleep	Authentication, Error Correction Codes, Anti-Replaying
Network	Sinkhole, Wormhole, Selective Forwarding	Authentication, Keying Techniques
Transport	Synchronization flooding	Authentication, Synchronization Cookies
Application	Clone, Deluge, DoS	Authentication, Anti-Replay

4. Jamming Attacks

Jamming in the physical layer [13] is usually done by distorting the sending and receiving frequencies using heavy noise levels. They are easily accomplished by either bypassing link layer protocols or emitting a signal targeted that jams a certain channel. Most WSNs are made of commodity sensors and components, thus these technologies are easily targeted by attackers. That means attackers are can easily gain access to communications channels used between sensors since they already know technology and accompanied protocol. Jamming attacks target the shared medium and even with the technological advancements in security of this shared medium, it is still difficult to defend against jamming attacks. Attacker usually prevent legitimate data from reaching its target, or even make packet collide thus no legitimate packets can be delivered over the channels [14].

4.1. Types of Jamming Attacks

We have four types of jamming attacks. The first one is constant jamming, were attackers emits a radio signal, this is done using waveform generators that continuously send radio signals or sends random bits to channels' link layer protocols, in effect jamming the channels. The link layer protocols allow sensors to send data when only if the channel is idle, when jammed constantly, sensors can't get any data through effectively. Major back draw of constant jamming is the nearly unlimited resources the attacker must have. The second type of jamming is deceptive jamming; the attackers won't send random data but will send a stream of real packets of data. This stream will be continuous so that receiving sensors will never go to sleep or ever be able to send its legitimate packets, because the stream of fake packets has no gap between those packets. Requiring again near unlimited resources, also attackers must sniff packets streams in order to replicate them.

Third type is random jamming; this can be constant jamming attack or deceptive jamming attack with power conservation taken into account. Attackers jam the signal for a set period, later they go to sleep, to conserve power. Usually attackers attack at certain send patterns for the sensors, then go to sleep when sensors aren't sending. Requiring far less power and processing resources, but careful timings are required to get effective jamming results. The last type of jamming is reactive jamming attacks. This is the hardest jamming attack to detect and hardest to implement. Unlike all previous jamming types, which are active, this type is reactive, meaning that jamming only start with legitimate sensor sending data out into channels. Blocking channels only when data is about to be sent. This type of jamming however requires precise sniffing and complex pattern recognition in order to occupy the whole channels effectively. In addition, this type of jamming attacks strikes a balance between power consumption and effectiveness, making it an efficient choice for attackers. Check Fig 2.

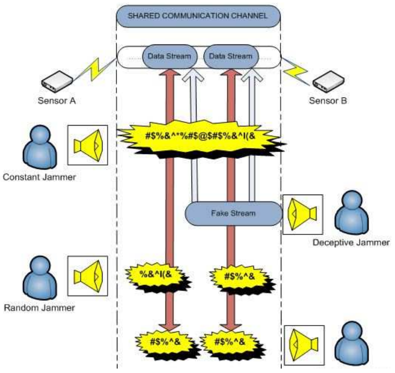

Figure 2. Types of Jamming Attacks.

4.2. Defense Mechanisms Against Jamming

First of all we must be able to detect the jamming signals from the legitimate. It is both difficult and imperative to distinguish between the legitimate signals and jamming signals. The first method to detect jamming is signal strength, whenever jamming is present; the signal levels are usually high when compared with signal levels without jamming. The other way to detect jamming is use the packet delivery ratio, in the presence of jamming packet delivery ratios is below average or even drops to zero if the jammer is completely blocking the signal. Thus, we can determine that the channel is being jammed and that the sensors should switch to another channel.

After detecting the presence of jamming, now we take action. Many security techniques were developed for protection against jamming. Mainly they fall into two main categories, evasion strategies, and competition strategies. In evasion strategies, sensors under attack from a jamming signal will evade the jammer by changing their broadcast channels or by physically moving away from the jamming. First evasive technique is called Channel Surfing; a technique that allows sensors to change their broadcast frequencies in presence of jamming. Change in frequency is on demand and done after the sensing of jamming on certain channels. In other evasive techniques, sensors physically move out of range from jamming thus allowing the jamming signals to be very weak and die out before affecting the WSN. The other strategy is the competition strategy; here sensors compete against the jamming attack. Sensors after detecting the jamming signal; will try to compete with the jamming. While competing, the sensors will use stricter ECCs that effectively lowers the data rates in each packet, but more successfully decoded packets will be received.

5. Selected Papers

5.1. Combined Approach for Distinguishing Different Types of Jamming Attacks Against Wireless Networks

The authors have described a novel method not just only to detect jamming attacks but distinguish which type of jamming attacks [16]. The work discusses how jamming attacks are one of the most prevalent attacks launched against WSNs. Main reason is that jamming attacks are one of the most effective Denial of Service DoS attack [17], as it completely deny any communications done between sensors in a jammed area. Another reason is that jamming, as the authors presumed, from an attacker perspective, is easy to implement and launch, using commodity Radio Frequency RF devices. The authors stated that detection of the jamming attack isn't always easy, as many attributes must be considered. Attributes hinder clear detection of jamming include low signal to noise ratios SNR, this is where outside interference with the channel can reduce its quality. Low SNR ratio however, isn't deliberate as opposed to jamming attacks. Other attributes hindering jamming detection is caused by low battery power that can give off low signal transmission strengths. In addition, sensors mobility can have the same effect on the signal strength. State of the art mechanism to detect jamming is Signal Strength Consistency Checks [18], as stated by the authors. This method can effectively distinguish jamming signals from other interference and noise. The authors proposed approach uses this technique to detect jamming. The authors presented a novel method that uses the Packet Delivery Ratio PDR, and Packet Sent Ration PSR, in their statistical method to detect and distinguish the jamming attack. Method described in there paper works upon the MAC layer, as this layer is responsible for the delivery of data frames in the shared medium, which are radio channels.

The basic protocol applied in the MAC layer is the Carrier Sense Multiple Access CSMA. The authors stated that CSMA/CD, which is with Collision Detection is not suitable for WSN [19], as multiple transmissions are possible but what matter is the receiver ready to receive the transmission or not. For two situations, hidden station problem and exposed station problem. In hidden station problem, it is a situation where three sensors in the same vicinity try to communicate with each other. For example, if sensors A, B, and C, are in the same vicinity, if A is communicating with B, then if C tries to communicate with B, its transmission is using a different channel, which is between C and B. Under CSMA/CD, channel between C and B is idle, so C starts to send its packet stream over the channel. However since channel is part of the shared medium, and sensors are in the same vicinity, the stream from C corrupts the stream sent from A. Other problem is exposed channel problem, in the same settings as before, if A is communicating with B again and C is wishing to transmit to a nearby sensor D. D is out of range from A and B, but C is in there transmission range still. C will sense that the channel is busy and will never transmit to D until A finishes. However, C will be idly waiting for A to finish while in fact the channel from C to D is idle. For these reasons, CSMA/CD is not suitable and CSMA/CA, which is CSMA over Collision Avoidance, is used instead. In this protocol, the sender before sending the sending sensor sends a handshake message, Request to Send RTS, and then waits for an acknowledgment, which is Clear To Send CTS message from the receiving sensor, and then communication is established. Even with CSMA/CA protocol in use, jamming can corrupt the handshake or even send fake packets to occupy the channels.

To distinguish jamming attacks, authors used the fact that jamming can both corrupt the protocol messages or handshaking or jammers send fake useless packets to fill channels. Jamming signals usually ignores the protocol messaging to get ACKs and just send junk messages over medium. The authors for their approach used three parameters the Signal Strength SS, PSR and PDR. SS parameter is used to detect jamming, it is used with threshold parameters for distinguishing whether jamming is disturbing channels or not. PSR determines how idle channels are, as if more packets were sent from total packets; it indicates that no constant or deceptive jamming is occurring in channels. Other parameter, PDR, indicates that jamming occurred actually, as all types exemplify extremely low rates, low successful transmissions. The case of zero PDR is when reactive jamming is done against the WSN, as almost no packets can go through the channel without being distorted halfway, this means that when the receiver will run its cycle redundancy checks CRCs, it finds that packets are corrupted, and won't acknowledge it back. In addition, when PSR drops to nearly zero value, with PDR nearing zero, it indicates constant jamming. Differences in PSR and the huge drop in PDR will result in detection of jamming.

For distinguishing four types of jamming, the authors used two main thresholds. Two thresholds are experimental threshold statistically set. Threshold1 is for the signal strength value, and the PDR, used to detect jamming. Threshold2 is about PSR, when it falls to a certain level, it is used to distinguish which jamming attack is the channel is under. Approach has two phases, in the first phase checks if PDR is below threshold1, if yes; it checks the signal strength, if it is above this threshold, threshold1. If no then no jamming had occurred, just interference or noise. If yes then jamming is detected, and the channel is under one of the four type of jamming. Second phase is to check the PSR with threshold2; if PSR is above threshold2 then it is either reactive jamming or random jamming. If PSR is below threshold2 then it's either deceptive jamming or constant jamming. The authors used statistical models to distinguish between four types; usually they proclaimed that with reactive jamming PSR is very high, above 60% for random jamming, which saves power for the jammer, PSR is below 60% but above threshold2. If PSR is, zero then its deceptive jamming. Finally, it is under threshold2 but not zero then its constant jamming. After detection of jamming, the authors suggest that the sensors communicate in another secure channel with different frequency, already set up in advance. The final stage of the method then, after detecting the jamming and its type, is to utilize the secret channel, on the different secret frequency not under attack. This means that the sensors under the jamming will negotiate what to do next. This technique is similar to channel surfing [20] for avoiding the jamming attack. The method does not specify what methods to use, but since the sensors under attack know exactly which type of jamming. They are freely communicating in this secret channel to initiate a solution. Fig.4 illustrates how the method can both detect the jamming attack and distinguish its type.

For the experiment the authors used the Network Simulator NS2, simulating all four jamming types. The results from the simulation runs showed that effectively all jamming types would drop the PDR value to nearly under 10%. This is expected, as one of the main aims of jamming is to corrupt packets in transmits. However, the PSR value shows huge differences as random and reactive will keep it above 70%, while deceptive and constant drop it under 10%. The method used to detect SS, the signal strength consistency checks, a well know and widely used technique for signal strength measurement. The SS is especially useful in the first phase, as it will help distinguish jamming from other factors contributing to low PDR and PSR. These other factors are low batteries, as they will drop the signal power, and moving out of range in case of mobile sensors, they will affect PDR value and drop it. In this case, the SS is measured, if it is lower than the threshold1, then this interference is not due to jamming, as usually jamming have high signal strengths, even higher than normal. This is called interference or noise distortions, and not considered jamming. As only, as the authored assumed in the experiments, if the SS is above threshold1, then the drop of PDR is deliberate and it is the result of jamming attacks.

The thresholds used in the experiments were based on statistical models of average signal strengths, PSR, and PDR rates in normal situations. Threshold2 and PSR are used to determine the type of jamming. The authors divided their method into two main algorithms, the PDR detection, and the PSR differentiation. The differentiation that occurs after detection does not really specifies a special avoidance plan. The method after detection and differentiation of the jamming, sensors just send jamming detection messages with the type of jamming, then use a suitable method to counteract this jamming type efficiently. The authors have not specified or suggested any jamming countermeasure to be used in their experiments though.

5.1.1. Outcomes, Limitations and Improvements

The authors came up with a novel method based on experimental and statistical results. Detection process doesn't need extra hardware; it utilizes SS and PDR only. PDR and PSR can be collected locally in the WSN. Distinguishing process between the different types helps in counter measurements selection. As in defense strategies, competition strategies specifically are more effective if the jamming mode is known. The method is simple, does not require any further modification to the sensors hardware. Even protocol modifications are not needed. Statistical data for the PDR and PSR needed however. The experiment showed clear and consistent results. The algorithm based on the approach, used simple switching statements can lead to identifying the jamming type. Authors showed how CSMA/CA is vulnerable against jamming as the jammer can still bypass the protocol, or utilize the protocol to occupy the channel with fake packets. The jamming attacks will leave the sensors in constant waiting or receiving modes according to the protocol CSMA/CA.

The method also distinguishes between interference disturbances in the signal and jamming. Interference comes from moving out of range or low batteries giving low signal strengths. This hinders PDR but isn't necessarily from jamming attacks. This allows multiple defensive techniques to be used depending on the type of jamming attack. The method also helps in protecting against multiple jamming attacks against multiple parts of the WSN. The method detection of the type of jamming helps against jammers that switch their modes after detection are caught, and suitable counter measurements are taking against them accordingly.

The assumption that was used is that jammers will constantly use a single model of jamming is an oversimplification. This is not entirely true, as jammers tend frequently to avoid detection by continually switching their modes. Switching the jamming mode is found in [21]. The statistical model applied is not entirely true, not for all WSNs, as the thresholds are approximation values from the experiment only. The approach is evasive in nature, as once the jamming is detected; the authors suggest using a secret channel to send messages to confirm the jamming attack and its type. This means that sensors avoid the jamming by using predefined secret channels to conform only of the jamming attack. Without proper usage of an effective method, the jamming problem will still affect the WSN. In addition, other defensive technique leaves the distinguishing of the jamming type rather useless as once jamming is detected no need really to know the type, in some defensive techniques. This leads to the truncation of the second phase of the approach as sensors are now using a different channel with different frequency.

Possible hopping to another channel to convey jamming attack conformation may not be possible either. As most jammers jam entire spectrums, at high costs though. On the other hand, attackers will try to retune their frequencies to that new channel. Therefore, the retune will reduce the possibility of using those secret channels. Furthermore, threshold calculations, PSR, and PDR, is not easily managed in large WSNs with scattered sensors. As larger areas are jammed and more sensors involved, the harder it is to get reasonable PSR and PDR readings indicating the average values. The authors did not specify any means to acquire PSR or PDR, other than theoretically, but not physically between the sensors under the jamming attack. Compared to SPREAD, this method tries to differentiate the jamming type, while this method the authors after detection, try to differentiate the type of the jamming but this means that more damage is done before it distinguishing. In SPREAD, immediate actions are taken to hop to another protocol or to change the protocol settings. This method of detection and differentiation is very slow in effectively taking action against the jamming. As only, after the damage is quite apparent can the sensors counter act. The sensors only send messages acknowledging that a jamming attack is affecting the WSN and its type only, as the authors have not specified any defense counter measurement.

Improvements to this method include the use of PDR and PSR values that are predefined depending on the size of WSN and the average message exchanged between the sensors. This eliminates the stochastic values overhead taken during operation. Furthermore, the use of channel surfing techniques after the detection and identification of the jamming attack. This will be used instead of just exchanging messages regarding that the jamming over the secret channels. Finally, if the defensive technique used to defend against the jamming attack is not for a specific type, we can simply skip the second phase and apply the technique after the detection phase. Another improvement is to use a mapping protocol like in [11], to map an area of the jamming attack, or possibly locate the jammer, as the method was developed under the assumption that the sensors are mobile.

5.2. A Defense Technique for Jamming Attacks in Wireless Sensor Networks Based on SI

In this paper [22], the authors have presented a novel jamming detection and evasion method based on Swarm Intelligence SI inspired by biological systems. Their technique utilizes autonomous agents to detect possible jamming attacks, and further mitigate its effects. Authors stated that other techniques detected jamming attacks through modifying used protocol or by using new MAC layer protocols; this is not always a practical solution to the jamming attacks problem. The authors mentioned the work in [21], and also how it employs a variant or alternative MAC layer protocol to defend against stealthy jammers. These techniques are all evasive techniques, similar to the SI method proposed. The jamming attack model used is the pulse jamming attack. This type of jamming attack is done through sending discrete pulses that destroy parts of the frames making up the packets, in affect corrupting them.

The proposed detection and evasion method is based on SI techniques. SI [23] is based on biological behaviors of social insects. SI is an Artificial Intelligence AI technique, used in cellular robotics for coordination, team work, and monitoring. SI consists of simple agents that try to solve complex problems together, like bees and ants. The authors stated that the agents they employ act much like ants, which get useful information from following trails of chemicals, and certain body movements. In the sense that the work done by ants is not supervised by any other ant, instead their combination of exchanging information, knowledge and work partitioning, achieves their ultimate goal without the need of any supervision. The ants in the colony do all their work in this manner, communication without supervision. In the same manner, the authors have proposed a similar technique called Swarm Based Defense Technique SBDT.

The technique utilizes AI, namely the Swarm Intelligence, a type of biological inspired algorithms. The method is based on intelligent agents, like ants in an ant colony, working together to achieve a common goal. The authors claimed that such a method is adaptable, as the intelligent agents gather enough information about WSN status dynamically. Agents gather both topology and traffic information that help in generating an overall view of the current status of WSN's channels. Agents collect non-local information that helps other sensor to be updated about the current channels availability. Agent use stochastic components, they act like pheromone table for the swarm agents, and they are autonomous. The gathered information helps in finding the best routes in which the packets will face less congested traffic, or avoid deliberate jamming attacks. The pheromone P, borrowed from the ant metaphor, will act as the information or probability provided to guide the agents in choosing which channels are safe to use.

SBDT, is based on four main principles, these principles organize autonomous work of agents. First principle is positive feedback, this feedback is the information regarding that the channels aren't under any jamming and still running without deliberate interference. Second principle is negative feedback, this feedback is alert information, resulting that jamming and its interferences are found on the travelled path, these channels are under heavy interference from jamming pulses, thus this path should be avoided. Third principle is randomness, the authors haven't stated what this principle is exactly, but it's a factor that help agents in selecting next hops, this factor helps reduce overhead of maintaining channels, and reduces updating data of channels very quickly. Randomness, is used when channels information of the next possible hop is available, thus agents depending on factor choose a channel. Last principle is multiple interactions; this is how agents communicative together. Multiple interactions between agents, means that agents traversed WSN will effectually transmit their gathered information to the other agents that traverse WSN right after them. This leads to acquiring prior knowledge about the channel status for other agents. agents use channel hopping, similar to what is found in [20] but not exactly the same, the hopping is used to evade the jammer. The hopping is based on a pair-wise key shared key K, this secret key will generate an encryption sequence factor E, and this is used to create a pseudorandom channel sequence, in the following equation (1):

$$\text{Chnext} = E(i) \bmod \text{Chcurrent},\ i \geq 0 \qquad (1)$$

Furthermore, the MAC layer will provide the packet fragmentation over the channels. The sending sensor will transmit its fragments on a certain channel after filling its transmit FIFO queue then it issues the transmission command. The authors listed an equation that calculates the time to fragment and issue the sending of such packet fragment. As each fragment will be send on its channel, and using the secret sequence, the sender will hop from channel to channel for each packet. The authors used Pulse jammers as the used model for jamming. Pulse jammers, are jammers that use a single channel and send random pulse to destroy such fragments, as whole packets cannot be detected quickly as fragments are scattered over many channels on a secret sequence. The method has two main agents, the forward ants FA, and the backward ants BA. The FA agents are the agents that start from a starting point; the author did not state exactly where, and traverses the whole WSN's channels collecting any information about possible jammers. When they reach the end of the network, they are transformed into new BA agents and their information is inherited and carried over. Finally, the BA agents will retrace back the same path their FA counterparts have travelled and update the current information inherited from the FA agents.

When the BA agents reach the source of which the FA agents started from, all of their information is verified and the current status of the channels is detected, then BA agents turn again to FA agents and inherit the information and redo the process in a new iteration. The agents will unicast or broadcast depending on the availability of the channels. Agents try to go through channels that we do not have any previous information about, newly created channels. As sensor, mobility is considered in the experiments, and sensor random movements create and destroy dynamically these channels. Channels which we have already recent information are not likely chosen, this as the authored said would lessen the overhead of maintaining channel information. When the agents face channels were all information is recently acquired, then the agents apply the randomness principle, this means randomly choosing their next channel. For choosing the channels randomly, much like in the biological system where the pheromones are used by ants to guide their way, the author used a channel probability equation. This equation depends on the available information about channel from the sender and the receiver. Also in the channel, probability equations are two relative weight values. Also in the equation is a variable called λ, this variable's value depends on the jamming pulses generated in each channel by some jammers. The variable λ value change depends on its previous value, if the change is positive; this means a negative feedback is sensed by the FA. If the change is negative, this leads to positive to the FA, which means that the jamming is lessened for some reason on that channel. Each channel neighbor or end points have also a probability equation that the feedback will update. Since the sensors are mobile, this means that channels are dynamic and are not fixed, and the sensors movements are random and not predefined or limited. Fig. 5 shows how the agents spread from a starting point sensor A, until they reach sensors F and G, which are situated at the end of the WSN. The FA agents will turn to BA agents upon reaching the end point of the WSN. The BA agents will traverse back the same path taken by the FA agents. Likewise, the BA agents turn to FA when reaching sensor A again, to start a new iteration. Channel information is always updated with each iteration.

The authored did their experiment using the Network Simulator NS2 tool. The MAC layer used is the IEEE 802.15.4; supporting the direct sequence spectrum spread DSSS, implemented in the hardware. The authored have compared their method SBDT with DEEJAM. The main attributes are the aggregated throughput, packet drop rate PDR, and the packet dropped during transmission. The results showed that SBDT usually have higher PDR than DEEJAM, much lower packet dropped rate, and higher aggregate throughput. The main reasons for these improvements are due to the positive and negative feedbacks and the lessened maintenance overhead. The feedbacks can give a message to the routing of the packets quickly to avoid channels with bad quality, for some reasons. Therefore, channel status can quickly be acquired and used to avoid channels under jamming attacks and reduce the traffic through them by omitted the jammed channels. The other contributing factor is the channel maintenance criteria. The agents, FA and the BA, will always choose the channels that they do not have recent information about their status. In case all channels information is known, they choose randomly using a probabilistic equation. This behavior will reduce the overhead of channel maintenance. In addition, it will also speed up the convergence process of having a clear view of the channels status quickly. Using he channel status the WSN can detect the quality of each channel faster, checking if any channel is under jamming or not.

These factors helped SBDT also achieve a much faster detection and convergence. In affect lessening the damage caused by jamming attacks much faster. The authored also used mobile sensors were topology is not fixed. The mobility of the sensors in the experiment is random. This in affect made channel creation and destruction completely dynamic. The other also used in their experiment, two different attackers. The attackers were placed randomly in the path of the channels in range. This random model of jamming however is not entirely true. As most deliberate jamming attacks usually target pivotal channels, those that link several parts of the WSN.

5.2.1. Outcomes, Limitations and Improvements

The authors proposed method based on swarm intelligence, to our knowledge, this utilization of agent-based method is novel. The probability equations used help reduce the overhead of maintaining or updating the channel values to soon or very quickly that will not be relevant as the channels are dynamic in nature. The agents work independently and try to listen in each channel to the traffic, thus if multiple jamming at multiple channels is present, such agents will detect each jammer individually. Randomness and the stochastic model also give the agents freedom and allow the method to adapt to changes in the WSN. The method uses channel hopping, by default, to spread the fragments over the channels using a pair-wise keying method. However, when jamming affects certain channels, they are omitted and skipped, meaning not used. This helps fragments escape the jamming on such channels. Finally, the brilliant aspect of this method is the fast convergence speed of the method, as the FA agents with the BA agents in a single iteration can give a very accurate view of the current status of the channels and how much traffic on each, every iteration updates theses values.

The authors did not take into consideration that limited resources available for each sensor. Nowhere in the paper is ever mentioned that the mobile sensors have limited memory or power constraints. As the SBDT's agents are continuously traversing the WSN, power is drained and memory is used. In addition, the authors used sensors that are DSSS capable; this is of most used hardware technique to avoid jamming [24]. This means that channel-hopping technique avoids the jamming, but the SBDT is used further to detect where the jamming attacks are and what channels to be avoided. The paper did not specify how or where the agents start, or what is the end point where the FA agents are turned to BA agents. Taking into consideration this is a mobile WSN, and the channels are not fixed. How will the autonomous agents know which channels exist and which that does not anymore? In addition, FA agents al go through different paths depending on the current topology, then the BA must retrace those route that may not exist anymore. The method also has no coordination regarding how the information will be used, when a FA or BA agent dismiss its information for each sensor, how will each sensor get the information relevant to its use? Sensors in this mobile setup will eventually need information regarding the whole WSN.

The paper used for jamming, the pulse jamming model, this model specifically jams only a single frequency of the whole frequency band allowed for the sensors. Under this model alone, the SBDT will detect affected frequencies and omit them. Other jamming models like constant jamming, where the jamming affects an entire frequency band. In addition, deceptive jamming model is not considered, when the jammer sends valid but empty packet fragments, how can the FA agents, and the BA agents detect such a jamming attack? The λ variable is a heuristic value dependent on the number of pulses sent on that channel. This means that deceptive jammers will not be easily detected as they append fake packet fragments into the channel. The injected packet fragments are continuous; therefore, it does not appear as a pulse but as a stream filling the channel. Also in the experiment, the authors considered the jamming attacks to be done randomly; this meant that the jamming attacks do not target certain channels. The agents FA and BA agents eventually gather information after at least the first iteration. The question is will this information be relevant, in case of a random jammer, jamming can be done randomly at random times and channels. Will information gathered by the agents be relevant to this random pattern? Also the computational and memory overhead is not considered in this method. In addition, the authors suggested that jamming attacks are mitigated by routing the traffic to other channels not under jamming attacks. The only defense mechanism in the SBDT method is when certain channels are found to be under jamming attacks is to switch their traffic to other unaffected channels. This is not entirely true all the time, as in the case where the jammed channels are the only path to certain parts of the WSN. Alternatively, maybe the jammers have jammed certain bridging channels, which resulted in partitioning the WSN. Furthermore, how can we, in these cases then routing the traffic to other unaffected channels? Routing to other unaffected channels will not certainly help all the time.

Improvements to the SBDT are to use better jamming detection. Jamming or random and deceptive jamming can be caught by using pattern tables like in [16], by using the localizing approach found in [25] to locate the jamming and try to avoid it. For further reducing the agents overhead, sensor may have their individual agents. Each sensor has a FA and its BA counterpart. The heuristic model should be replaced with a stochastic model based on routes this sensor use, and the patterns known for jamming attacks. Comparing the SBDT with DEEJAM, it seems apparent that SBDT is much more costly, in terms of agents' maintenance and coordination. When compared with SPREAD, we think that SBDT reaction to jamming is not as fast. For example, SPREAD, when jamming is detected, immediately the jamming is mitigated by using a new protocol or changes its settings. SBDT, on the other hand, must wait for the agents to traverse the entire WSN, and then verify the information, and then jammed channels are not used or omitted. When compared with JAM, this method gathers information about dynamic channels, which are quickly destroyed and created. Whereas JAM, maps an area where the jammer is launching attacks against WSN. Mapping the area of jamming is more helpful than information about the channels themselves.

5.3. SPREAD: Foiling Smart Jammers Using Multi-layer Agility

The authors represented SPREAD (Second-generation Protocol Resiliency Enabled by Adaptive Diversification) [9], a technique to resist smart jammers. By smart jammers, the authors mean jammers that act more like reactive jammers. To be more precise, these jammers only jam the payload of the delivered packet, meaning they know exactly what protocol is in use. This serious attack will have a high rate of corrupting the data carried by the packets and can effectively reduce the throughput to zero. Furthermore, these smart jammers utilize cross-layer attacks, meaning they jam certain layers to hinder the other layers from communicating with this layer. Smart jammers reduce the power needed to jam the entire channel but they should carefully time their attacks to target protocol specific information.

The authors also mention another attempt to defend against jamming attacks, the spectrum spread, and how it is not practical for WSNs as it was developed for voice communications. They mention that there are jam attack patterns that target specific layer protocols, the Wolfpack program [10]. This ultimately leads to SPREAD, a technique that avoids smart jammers that target specific protocols, by using a parallel collection of network protocol stacks and switching between them.

The technique has two major parts, the core, and the layers. The core is the central control part of the protocol; it uses the data collected from the layers to analyze when and how to hop to another protocol sequence in case of jamming on the current protocol. The layers are physical layer, Medium Access Control MAC layer, Data Link layer, and the Transport layer. The layers use certain set of protocols, and report to the core the variables readings, variables like network congestion, channel status, PDR and the energy levels used.

The core, depending on these reading will decide to initiate the hopping sequence to other protocols in case of a smart jamming found targeting the used protocols. Two technique of hopping are used, the Inter-protocol hopping and the Intra-protocol hopping. The inter-protocol hopping means that several instances of interleaved protocols are used and the network uses them redundantly, taking into consideration that a smart jammer cannot possibly target all of the protocols at once. The other type, intra-protocol hopping, means that a single protocol is running but the core cryptographically and dynamically changes the packet size, coding rates, and the transmission rates.

The authors applied their technique against Extended Inter-frame Space EIFS attacks, were the jammers jams the period the channel is supposedly idle. This attack will reduce the throughput to zero as sensors will always check for the channel to be idle and simply find it busy. Then for fine-tuning SPREAD, the authors used game theory [26], to demonstrate how SPREAD can be tuned to fend off the jamming attacks more effectively.

5.3.1. Outcomes, Limitations and Improvements

The authors have presented a novel method to defend against smart jammers. SPREAD helps to mitigate and leverage the damage cause by jammers that target protocol critical information. The authors assume that it is more efficient that other methods like spectrum spread or using more than a single channel for communications. SPREAD framework utilizes the same hardware, only needs fundamental protocol changes and implementations. They also presented their work in a game theoretical framework, which illustrates how SPREAD is tuned to lower the effects of the jamming.

The authors suggested that most jammers are smart jammers. This is not typically the case, as most jammers use nearly unlimited power supplies to effectively cutoff the channels. Most jammers target many protocols simultaneously, in case the WSN used different protocols. Another effective defense against jamming is channel surfing that dynamically change the frequency instead of the protocol. It is less complex and more effective, as most WSN employ ZigBee and IEEE 802.15.4 compatible. These protocols complaint sensors support multi-channel frequencies. The authors suggest that the jammer only use different jamming rates also. This is not entirely true as jammers can be deceptive, that mean sending jamming signals right after the packet payload to trick the receiver into continuously receiving junk data. In addition, reactive jammers target the payloads, even if the WSN used multiple protocols and used redundancy in sending the packets, these jammers will corrupt most of the data payloads leaving the protocol data unaffected.

5.4. JAM: A Jammed-Area Mapping Service for Sensor Networks

In [11] the authors represented a novel mapping service to detect jamming attacks. JAM (Jamming Area Mapping) is a service that provides quick and accurate jamming attack response, which alerts the WSN for a possible jamming attack in effect. As geographic information is important for most WSNs, knowing where exactly the jamming is and what sensors does it effect, certainly will help in mitigating and leveraging its effects. As jammers often, attack specific areas like the gateway sensor area or critical proxy areas. Finding where the jamming are coming from and what sensors are currently cut-off, is very essential in the next step which is avoiding or challenging the jammer. The authors suggested that cost of other solutions like spread spectrum techniques is high, and only practical in military WSN, were security compromise is not an option.

The authors described JAM, as a service that provides feedback to the routing directories, thus warning the WSN of the jammer current activities. It also provides preemptive warnings to entry of individuals or sensors or even vehicles to this area as the enemy or jammer is currently active in. Finally, the mapped area aids the WSN in deploying its strategies against the jammer effectively. For example, the WSN can switch off the sensors in the jammed area, reallocate the sensors, if they are mobile or capable of moving, or reroute all packets to avoid that area. Power management strategies can also be used to foil the jammer possible damage. The authors clearly claim that JAM provides a much cheaper and convenient solution to jamming attacks, as it aids the WSN to take critical actions and imply simple solutions to jamming.

JAM is a protocol applied by all the sensors in the WSN. The protocol works as follows; the jammed sensors inside the jamming area send 'Jammed' messages to sensors outside of the jammed area. Then the sensors outside will cooperatively map an area of the possible jamming attack. The JAM paradigm utilize a loose group semantics were sensors do not wait for acknowledgment ACKs messages and eager eavesdropping were only needed sensors must be notified. Many assumptions are presumed in the sensors and in the jamming attack itself. JAM works in two main modules, the jam detection module, and the mapping module that follows. In the jamming detection, the authors assumed that the sensors could override the MAC layer carrier sense multiple access CSMA policies in relaying the 'Jammed' message. This is critical, as the channels are most likely to be filled all the time by the jammer. This overriding with sent 'Jammed' messages blindly to the jammed sensor's nearest neighbor. Many factors will lead the sensor to detect it is under jamming, some of the main factors are, low signal-to-noise ratio SNR, repeated collisions, and protocol violations. The jammed sensors will send 'Jammed' messages to their nearest neighbors to instantiate the next phase. In addition, when the jamming affects wares off, they send an 'UnJammed message to their previous neighbors to update the status.

The next phase is the mapping phase, here an edge sensor, the sensor that receives the actual 'Jammed' message, starts this phase upon receiving the message. When an edge sensor receives this message, the edge sensor instantiates a random group ID, in case it knows no other group. This group ID, with it assigns a normalized direction vector pointing to its jammed neighbor. It also includes its ID, along with the group ID and the normalized vector in a message called BUILD. Finally, this edge sensor now becomes a mapping sensor or node, and sends the BUILD message to its neighbors. Neighbors receiving this message will do the same but will no further propagate the message to their neighbors. These messages contain also a sequence number to prevent duplicates from being processed. When receiving more than one BUILD message, sensors check the group IDs, and check their direction vectors for coalescing compatible groups together.

Edge sensors are those that did not receive any BUILD message from their neighbors, thus they send Probe messages to detect other possible groups nearby. A bridge sensor or node is the sensor that upon checking the normalized vectors between two different groups, it appears they are very much pointing to the same area, and then there are coalesced. When coalescing, the group ID that is higher is used for the new group. Ideally, we want to get a mapping with a single group containing all the sensors surrounding the jammed area. The convergence of the protocol is, as the authors assume, achieved within seconds of the jamming detection. The use of loose group semantics and eager eavesdropping assure quick knowledge diffusion. In addition, the one-hop back flooding helps in reducing redundant information being exchanged. Probing and coalescing help in gathering compatible groups together to quick build a map of the current jammed area. The authors used extensive simulation to demonstrate JAM, using GloMoSim simulator [27].

5.4.1. Outcomes, Limitations and Improvements

The authors presented a protocol to leverage and mitigate the effects of jamming in a novel and descriptive way. The approach does not require extra hardware added to the sensors, thus implementing JAM is cost effective. The approach uses many heuristics to determine whether the channel is jammed or not. The convergence of the protocol is very high; this means that at the end we get a single map or group surrounding the jammed area. The normalized vectors used, not only help in pointing where the jammed area boundaries is, but also help in reducing the sent Probe messages to the neighbors that are on the edges of this jammed area, left and right only. Furthermore, during the protocol no messages are acknowledged, this reduce the complexity, timeouts are used instead with reception events. The use of probabilistic uniqueness in randomly selecting group IDs prevent any synchronization needed among the sensors. The simulation was very extensive and considered many parameters in different situations.

The authors assumed that most sensors are not capably of spread spectrum techniques, as most ZigBee and IEEE 802.15.4 compatible sensors are capable of Frequency Hopping Spread Spectrum FHSS and Direct Sequence Spread Spectrum DSSS. The authors assumed that not all or huge parts of the WSN are jammed, this allows JAM to detect the area and maps it. In addition, they do not allow multiple jammers to jam nearby areas or even merging their areas together in an ad hoc fashion. The critical assumption that the authors assume is that the MAC layer, CSMA is overridden in the protocol 'Jammed' message to start the second phase. The authors suggested modification if necessary. This is not always possible with hardware implementations of the MAC layer CSMA in some sensors, thus no override is possible. Also high sensor counts create message explosions from the excessive back-flooding messages. The overall protocol complexity is also noticeable, as in some cases, no single group, or map is achieved. The protocol assumes that all sensors know their location, IDs of their neighbors. They assume that also the network only use a single channel for all communications. The protocol is only compatible with static WSN, as mobile sensors may never reach any convergence in computational times.

6. Conclusion

WSNs are a rapidly growing field, with many opportunities and challenges. Strict architectural, economical, and technological aspects of such networks give it its unique characteristics' and traits. As more dependent we grow on WSNs, we cannot afford to compromise the availability and security of such networks. Since WSN hardware and software have many limitations, it allowed security issues to rise to the surface. In this paper, we have discussed the jamming attacks and sinkhole attacks. We discussed their main aspects and types, and how attackers utilize such techniques to launch their attacks.

We have discussed through two major papers that proposed techniques to defend against jamming attacks. We discussed and criticized the papers in terms of their positive contributions and limitations. Furthermore, we suggested improvements to such shortcomings. The improvements we suggested stemmed from other papers who suggested other defense mechanisms. The future work lies in further studying more techniques that try to generally improve the overall security levels and standards of WSN. Finally, we hope that WSN of the future, are designed and realized with security in mind as WSNs today lack such focus on security. As more secure WSN will be in the future, more possibilities and applications are sure to use WSNs.

Acknowledgements

The author would like to thank Dr. Abraham Al-Rashid, Computer Engineering Dept. Kuwait University for his support and careful follow up with this project.

References

[1] Kai Xing, Fang Liu, Xiuzhen Cheng, David H.C. Du

"Real-time Detection of Clone Attacks in Wireless Sensor Networks" The 28th International Conference on Distributed Computing Systems ICDCS, IEEE 2008.

[2] Lewis, Frank L; "Wireless Sensor Networks," Smart Environments: Technologies, Protocols, and Applications, pp. 11-46, © 2005 John Wiley & Sons, Inc.

[3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey", Computer Networks, Volume 38, Issue 4, pp. 393-422, 15 March 200.

[4] Lewis, Frank L; "Wireless Sensor Networks," Smart Environments: Technologies, Protocols, and Applications, pp. 11-46, © 2005 John Wiley & Sons, Inc.

[5] Sukumar Ghosh, Distributed Systems: An Algorithmic Approach, 2006 CRC Press.

[6] Pottie, G.J.; "Wireless sensor networks," Information Theory Workshop, pp.139-140, 22-26 June 1998.

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

[8] Alzaid, Hani; Park, Dong Gook; Nieto, Juan Gonzalez; Boyd, Colin; Foo, Ernest; "A Forward and Backward Secure Key Management in Wireless Sensor Networks for PCS/SCADA," Sensor Systems and Software, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 66-82, Vol.24, © 2010, Springer Berlin Heidelberg.

[9] Xin Liu, Guevara Noubir, Ravi Sundaram, San Tan, "SPREAD: Foiling Smart Jammers using Multi-layer Agility" IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2007 proceedings, IEEE 2007.

[10] DARPA, http://ww.darpa.mil/ato/programs/WolfPack/index.htm.

[11] Anthony D.Wood, John A. Stankovic, and Sang H. Son "JAM: A Jammed-Area Mapping Service for Sensor Networks" Proceedings of the 24th IEEE International Real-Time Systems Symposium (RTSS'03), IEEE, 2003.

[12] R. L. Pickholtz, D. L. Schilling, and L. B.Milstein "Theory of spread spectrum communications, a tutorial" IEEE Transactions on Communications, IEEE, May 1982.

[13] Onel, Tolga; Onur, Ertan; Ersoy, Cem; Delic, Hakan; Byrnes, Jim; "Wireless Sensor Networks For Security: Issues and Challenges," Advances in Sensing with Security Applications, NATO Security through Science Series, pp. 95-119, Vol. 2, © 2006 Springer Netherlands.

[14] AusCERT, "AA-2004.02 — Denial of Service Vulnerability in IEEE 802.11 Wireless Devices," http://www.auscert.org

[15] W. Xu, Timothy Wood, Wade Trappe, Yanyong Zhang "Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service," In the Proceedings of Wireless Security Workshop, ACM, pp. 80–89, 2004

[16] Wang, Le; Wyglinski, Alexander M.; , "A Combined Approach for Distinguishing Different Types of Jamming Attacks against Wireless Networks," In the Proceedings of the Conference on Communications, Computers and Signal Processing Pacific Rim, pp.809-814, 23-26 IEEE, Aug. 2011.

[17] Wood A. D., Stankovic J. A., "A Taxonomy for denial-of service attacks in wireless sensor networks," in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, edited by Mohammad Ilyas and Imad Mahgoub, CRC Press LLC, 2005.

[18] 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, JATIT & LLS, 15th August 2011.

[19] Y. Hu, A. Perrig, and D. Johnson "Ariadne: A secure on demand routing protocol for ad hoc networks". In 8th ACM International Conference on Mobile Computing and Networking, pages 12-23, September 2002.

[20] Wenyuan Xu, Wade Trappe, Yanyong Zhang "Channel Surfing: Defending Wireless Sensor Networks from Interference" In Proceedings of the 6th international conference on Information processing in sensor networks IPSN'07, April 25-27, Massachusetts, USA. ACM, 2007.

[21] Wood, A.D.; Stankovic, J.A.; Gang Zhou; "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15.4-based Wireless Networks," fourth Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks SECON '07. PP.60-69, 18-21 June 2007.

[22] Periyanayagi, S.; Sumathy, V.; Kulandaivel, R.; "A Defense Technique for Jamming Attacks in Wireless Sensor Networks Based on SI," International Conference on Process Automation, Control and Computing PACC, pp.1-5, 20-22 July 2011.

[23] Swarm Intelligence, http://www.sce.carleton.ca/netmanage/tony/swarm.html

[24] Aristides Mpitziopoulos, Damianos Gavalas, Grammati Pantziou, and Charalampos Konstantopoulos "Defending Wireless Sensor Networks From Jamming Attacks" The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07), IEEE, 2007.

[25] Zhenhua Liu, Hongbo Liu, Wenyuan Xu, and Yingying Che, "Exploiting Jamming-Caused Neighbor Changes for Jammer Lcalization", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 3, March 2012.

[26] Hai-Yan Shi, Wan-Liang Wang, Ngai-Ming Kwok and Sheng-Yong Chen "Game Theory for Wireless Sensor Networks: A Survey", Sensors 2012, doi:10.3390/s120709055, July 2012.

[27] X. Zeng, R. Bagrodia, and M. Gerla "GloMoSim: A library for parallel simulation of large-scale wireless networks" Workshop on Parallel and Distributed Simulation, pages 154–161, 1998.