International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-2, Issue-4)

Research Article | **April 2013**

Reviewing Strategies to Deal with Jamming in WSNs

Ms. Sunita
CSE,SES,BPSMV
Haryana, India.

Jyoti Malik
CSE,SES,BPSMV
Haryana, India.

Abstract:

Wireless sensor network (WSNs) have emerged as an important application area resulting from the advancement of efficient short-range radio communication and miniaturization of computing devices. As these networks are built upon a shared medium that makes it easy for adversaries to conduct radio interference, or jamming, attacks that effectively cause a denial of service of either transmission or reception functionalities. In this paper, we survey on the possible jamming attack scenarios that a WSN may encounter as well as different types of security schemes in order to cope with the problem of jamming attacks.

Keywords— WSN, Jamming ,Jamming models, Security schemes against jamming, JAM, DEEJAM, Mobile Agent Based Solution.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) [1] are used in many applications which often include the monitoring and recording of sensitive information (e.g. battlefield awareness, secure area monitoring and target detection). Recently the high drop in the prices of CMOS cameras and microphones has given rise to the development of a special class of WSNs, that of Wireless Multimedia Sensor Networks (WMSNs) [2-4].WMSNs allow the retrieval of video and audio streams, still images, and scalar sensor data from deployed nodes [4]. Hence, they can be efficiently used in various security applications such as surveillance systems for monitoring of secure areas, patients, children, etc. In these applications, QoS requirements rise, since in such systems even a temporal disruption of the proper data streaming may lead to disastrous results. It is therefore evident that the critical importance of WSNs raises major security concerns.

II. JAMMING

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it. Jamming represents a type of electronic warfare which interferes with the radio frequencies utilized by network nodes and may be viewed as a special case of denial of service (DoS) attacks. Wood and Stankovic define DoS attacks as 'any event that diminishes or eliminates a network's capacity to perform its expected function' [5]. Typically, DoS prevents or inhibits the normal use or management of communications through flooding a network with 'useless' information. In a jamming attack [6] the radio frequency (RF) signal emitted by the jammer corresponds to the 'useless' information received by all sensor nodes. This signal can be white noise or any signal that resembles network traffic. In jamming, there are some jammer attacks. A jammer is a device which can partially or entirely disrupt a node's signal, by increasing its power spectral density (PSD). Jammer can never re-produce a signal nor can it pretend like a receiver node. The parameters such as signal strength of a jammer, the location and the type influence the performance of the network and each jammer has different effect on the node. The application of spread spectrum (SS) techniques developed by the end of World War II. Using SS technique the data is spread across the frequency spectrum making the signal resilient to jamming, noise and eavesdropping. There are different types of SS such as Direct Sequence (DS), Frequency hopping (FH), Time hopping (TH) and hybrid. There are both advantages and disadvantages associated with using SS in sensor networks.

The advantages are:

- Ability to alleviate multi-path interference
- Jamming attacks reduced, and
- Less power spectral density.

The disadvantages are:

- Bandwidth inefficiency
- Compels implementation, and
- Computational cost.

Bluetooth [7] uses FHSS, which consumes more power as frequency hops needs to be synchronized. Whereas, Zigbee [8] uses IEEE802.15.4 standard where DSSS with CSMA-CA is used. Of late Zigbee is being considered as a wireless technology for wireless sensor networks as it consumes less power. Study of different characteristics of an attack keeps the attack attempts minimal as knowledge of the types of jammer helps in taking the appropriate countermeasure. There are four different types of jammer [9], namely: single-tone jammer, multiple tone jammer, pulsed-noise jammer and ELINT.

A. Different Types Of Jammer

1) Single Tone Jammer[10]: A. single-tone jammer's frequency lies within the specified bandwidth of the signal being jammed. It targets any narrowband communication. Since traditional wireless sensor network use narrowband technology [11]. This kind of jammer tries to continuously jam the node within specified bandwidth, which might result in a dead link and diminishes the node's coverage.

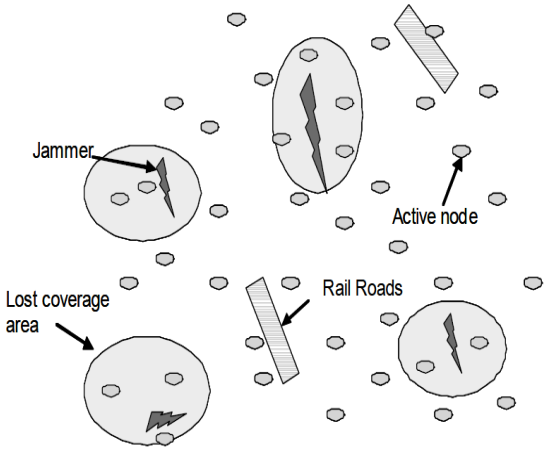

Fig. 1 Jammer Attack on Sensor Network

2) Multiple-Tone Jammer: A jammer that can disrupt the signal of some or entire channel of a multiple channel receiver. This type of jamming leads to a complete node failure, if the entire channel is compromised. The only time the node can recover is when the jammer is turned off. Typically, an intruder plays it safe while jamming a node by occasionally turning off its radio. Thus, make the neighboring node assume the node is not under attack but rather lost its energy and needs recuperation. Hence, detections of a jammed node is very important.

3) Pulsed –Noise Jammer[10]: A pulsed-noise jammer is a wideband jamming, which behaves like a pulsed signal by turning on and off periodically. The primary goal of this jammer is to disrupt the spread spectrum communication by spreading the peak jamming power during the "on" time. Two types of pulsed-noise jammers are considered, namely, slowly switching and fast switching jammers.

4) ELINT: ELINT is typically a passive system that tries to break down or analyze radar or communication TCF signals. They may be integrated.

B. Comparison of Jamming Models

In [12] and [13], Xu et al. introduce four common types of jammers: constant, random, reactive and deceptive. Constant jammers continually emit a jamming signal and achieve the highest censorship of packets corrupted to total packets transmitted. The constant jammer, however, is not energy-efficient and can be easily detected and localized. The random jammer is similar to the constant jammer but operates at a lower duty cycle with intervals of sleep. A random jammer transmits a jamming signal at instances derived from a uniform distribution with a known minimum and maximum interval.

The censorship ratio of the random jammer is constant and invariant to channel utilization. At low duty cycles, the random jammer is difficult to detect and avoid. A reactive jammer keeps its receiver always on and listens for channel activity. If a known preamble pattern is detected, the reactive jammer quickly emits a jamming signal to corrupt the current transmission. Reactive jammers, while effective in corrupting a large proportion of legitimate packets, are not energy efficient as the receiver is always on. Another type of reactive jammer uses a simple physical layer energy detector as sensing and wake-up radios. These agile jammers wait until channel activity is detected and then jam. Although energy to 'listen' is lower, this behavior is also energy inefficient since any kind of channel activity triggers a transmission of a jamming pulse. Due to physical layer delays these jammers are effective in jamming the fraction of packets that are greater than a certain threshold length. A deceptive or protocol-aware jammer is one that has knowledge of the link protocol being used and the dependencies between packet types. Such a jammer exploits temporal and sequential patterns of the protocol and is very effective.

In [14], a statistical jamming model is described where the jammer first observes temporal patterns in channel activity, extracts a histogram of inter-arrival times between transmissions and schedules jamming pulses based on the observed distribution. This results in a very effective jammer that is not protocol-aware and is also difficult to detect. A statistical jammer chooses its transmission interval to coincide with the peak inter-arrival times and is thus able to maximize its censorship ratio with relatively little effort.

III. SECURITY SCHEMES AGAINST JAMMING IN WSNS

The security scheme in the WSN to address jamming issue can be categorized in

- Detection Techniques,

- Proactive Countermeasures,
- Reactive Countermeasures, and
- Mobile agent (MA)-based countermeasures.

A. Detection Techniques

The purpose of detection techniques is to instantly detect jamming attacks. The approaches of this category cannot cope with jamming alone; they can significantly enhance jamming protection only when used in conjunction with other countermeasures by providing valuable data (e.g., the initiation and type of jamming attack).

1) *Radio interference detection in wireless sensor network:* Radio interference relations among the nodes of a wireless sensor network (WSN) and the design of a radio interference detection protocol (RID) are discussed in Reference [15]. However, jamming from external sources is not investigated; hence RID remains highly vulnerable from jamming attacks.
2) *The feasibility of launching and detecting jamming attacks in WSNs:* In Reference [16] Xu et al. claim that understanding the nature of jamming attacks is critical to assuring the operation of wireless networks, so their focus is on the analysis and detection of jamming signals and they do not deal with effective countermeasures against jamming.

B. Proactive Countermeasures: Proactive countermeasures are performed in the background, even in jamming-free environments; typically, they cannot be initiated, stopped or resumed on demand. Hence, they enable instant response against jamming at the expense of increased computational and energy cost upon the resource-constrained sensor nodes. As a result, they defend more efficiently against stealth jamming attacks, which may pass undetected for a significant period of time from a reactive countermeasure.

1) *DEEJAM:* Wood et al. in Reference [17] proposed DEEJAM, a new MAC-layer protocol for defending against stealthy jammers using IEEE 802.15.4-based hardware. The general design approach of this protocol is to hide messages from a jammer, evade its search and reduce the impact of messages that have been someway corrupted. The main advantage is that it is compatible with existing nodes' hardware (no hardware modification is needed); the authors have also provided evidence of its effectiveness via simulations on Micaz [18] nodes. However as the authors already noted against a powerful and more sophisticated jammer DEEJAM cannot effectively defend the WSN and the most probable scenario is that an adversary will use more advanced hardware compared to that of the nodes'. Another drawback is the overhead that DEEJAM requires to operate and the increased computational and energy cost in the already resource constrained nodes of a WSN.
2) *Energy-efficient link-layer jamming attacks against WSNs' MAC protocols:* Law et al. [19] examine link-layer jamming algorithms and conclude that in typical contemporary WSN systems no effective measures against link-layer jamming are possible. They recommend: (a) encrypting link-layer packets to ensure a high entry barrier for jammers, (b) the use of spread spectrum hardware, and (c) the use of a TDMA protocol.

C. Reactive countermeasures: The main characteristic of reactive countermeasures is that they enable reaction only upon the incident of a jamming attack sensed by the WSN nodes. Thus they need reduced computational and energy cost compared to proactive countermeasures but in the case of stealth or deceptive jamming there is a great possibility for delayed sensing of jamming.

1) *JAM*: Wood and Stankovic propose the detection and mapping of jammed regions [20] to increase network efficiency. However, this method presents several drawbacks: first, it cannot practically defend in the scenario that the attacker jams the entire WSN or a significant percentage of nodes; second, in the case that the attacker targets some specific nodes (e.g., those that guard a security entrance) to obstruct their data transmission, again this technique fails to protect nodes under attack.
2) *Channel surfing and spatial retreat:* Xu et al. in Reference [21] proposed two evasion strategies against constant jammers: channel surfing and spartial retreat. Channel surfing is essentially an adaptive form of FHSS. Instead of hopping continuously from one channel to another, a node switches to a different channel only when it discovers that the current channel is being jammed. Spatial retreat is an algorithm according to which two nodes move in Manhattan distances to escape from a jammed region. The main shortcoming of the two Abovementioned strategies is that they are effective only against constant jammers and they have no results against more intelligent or follow-on jammers.
3) *Wormhole-based anti-jamming techniques in sensor networks*: Cagalj et al. proposed a reactive anti-jamming scheme for WSNs using wormholes [22]. The basic idea is that jammed nodes use channel diversity in order to establish a communication with another node outside the jammed area. The authors propose three types of wormholes: (a) wired pair of sensors (b) frequency hopping pairs, and (c) uncoordinated channel-hopping. In summary, wormholes may be an interesting idea to defend against jamming attacks but many problems still remain, as increased cost, the need for a large amount of time for the deployment of the sensor nodes in large scale WSNs and the fact that FHSS alone is not an effective countermeasure against fast-follower jammers [23].

D. Mobile agent (MA)-based countermeasures. This class of anti-jamming approaches enables MAs to enhance the survivability of WSNs. The term MA [24] refers to an autonomous program with the ability to move from host to host and act on behalf of users toward the completion of an assigned task. MA-based solutions do not require the use of specialized hardware. However, in conjunction with spread spectrum hardware their anti-jamming properties can be significantly improved.

1) Jamming attack detection and countermeasures in WSNs using ant system: Muraleedharan and Osadciw propose the use of ant system algorithm as an effective countermeasure against jamming attacks in a WSN [25]. In effect, ants may be viewed as a type of MAs. An initial set of ants traverse through the nodes in a random manner and once they reach their destinations, they deposit pheromone on trails as a means of communication indirectly with the other ants. The amount of pheromone left by the previous ant agents increases the probability that the same route is taken during the current iteration. Parameters such as hops, energy, distance, packet loss, signal-to-noise ratio (SNR), bit error rate (BER), and packet delivery affect the probability of selecting a specific path or solution. Also pheromone evaporation over time prevents suboptimal solutions from dominating in the beginning. Unfortunately, this system has not been tested in large-scale simulated WSNs(simulations have been conducted in topologies comprising 16 nodes), hence its scalability is questionable. Also the extra computational and energy cost required by ants is not evaluated. Notably, the authors omitted information on how quickly the 'pheromone' trails are able to react to nimble attackers. Finally, in the case that a considerable proportion of WSN nodes are jammed then ants will probably fail to guarantee the uninterrupted network's operation.

IV. CONCLUSIONS

Jamming is defined as the act of intentionally directing electromagnetic energy towards a communication system to disrupt or prevent signal transmission. In the context of wireless sensor networks (WSNs), jamming is the type of attack which interferes with the radio frequencies used by sensor nodes and may be viewed as a special case of denial of service (DoS) attacks. Herein, we outline the possible jamming attacks and security schemes.

ACKNOWLEDGMENT

I would like to give our sincere gratitude to our guide Ms. Sunita who encouraged and guided us throughout this paper. Apart from her support as a professor and a researcher, we were fortunate to have her support as a friend.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankara subramaniam, E. Cayirci,"A survey on sensor networks", IEEE Commun. Mag., pp. 102-114, August 2002.
[2] E. Gurses and O.B. Akan, "Multimedia communication in wireless sensor networks", Annals of Telecommunications, vol. 60, no. 7-8, , pp. 799-827, 2005.
[3] S. Misra, M. Reisslein, G. Xue, "A survey of multimedia streaming in wireless sensor networks", IEEE Commun. Surveys Tutorials, in print, 2008.
[4] I. F. Akyildiz, T. Melodia and K. R. Chowdhury, "A survey on wireless multimedia sensor networks", Computer Networks, vol. 51, no. 4, pp. 921-960, 2007.
[5] Wood A D, Stankovic JA. Denial of service in sensor networks. Computer 2002; **35**(10): 54–62.
[6] Schleher DC. Electronic Warfare in the Information Age. Artech House, Boston, MA, USA, 1999.
[7] Technical Information of Bluetooth: Official website www.bluetooth.com.
[8] Technical Information of Zigbee: official website www.zigbee.org
[9] Poisel Richard, "Modern communications jamming principles and techniques".
[10] F.C.M. Lau and C.K. Tse, " Study of Anti-Jamming Capabilities of Chaotic Digital Communication Systems,"Proceedings, 2002 International Symposium on Nonlinear Theory and Its Applications, (NOLTA'2002), October 2002, Xian, China, pp.65-68.
[11] K.D.Wong, "Physical Layer considerations for Wireless Sensor Networks", IEEE Int'l Conference Net, Sensing and Control, Mar 2004, pp 1201-1206.
[12] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In ACM MobiHoc, 2005.
[13] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service. In ACM WiSe, pages 80–89, 2004.
[14] Y. W. Law et al. Energy-efficient link-layer jamming attacks. In ACM SASN, 2005.
[15] Zhou G, He T, Stankovic JA, Abdelzaher TF. RID: radio interference detection in wireless sensor networks. In Proceedings of the IEEE INFOCOM'2005, 2005.
[16] Xu W, Trappe W, Zhang Y, Wood T. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of the 6th ACMInternational Symposium on Mobile Ad Hoc Networking and Computing, Urbana-Champaign, IL, USA, ISBN:1-59593-004-3, 2005, 46–57

[17] Wood AD, Stankovic JA, Zhou G. DEEJAM: defeating energyefficient jamming in IEEE 802.15.4-based wireless networks.In The 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks(SECON), San Diego, CA, June 2007.
[18] Crossbow Technology Inc. http://www.xbow.com/
[19] Law Y, van Hoesel L, Doumen J, Hartel PH, Havinga PJM. Energy-efficient link-layer jamming attacks against wirelesssensor network MAC protocols. Proceedings of SASN'2005, 2005, 76–88.
[20] Wood AD, Stankovic JA, Son SH. JAM: a jammed-area mapping service for sensor networks. 24th IEEE Real-Time Systems Symposium (RTSS'2003), 2003, 286–297.
[21] XuW,Wood T, TrappeW, Zhang Y. Channel surfing and spatial retreats: defenses against wireless denial of service. InWiSe'04: Proceedings of the 2004 ACM Workshop on Wireless Security, New York, USA, 2004, 80–89.
[22] Cagalj M, Capkun S, Hubaux J-P. Wormhole-based antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing, May, 2006.
[23] Schleher DC. ElectronicWarfare in the Information Age. Artech House, Boston, MA, USA, 1999.
[24] Pham V, Karmouch A. Mobile software agents: an overview.IEEE Communications Magazine 1998; **36**(7): 26–37.
[25] Muraleedharan R, Osadciw L. Jamming attack detection andcountermeasures in wireless sensor network using ant system.2006 SPIE Symposium on Defense and Security, Orlando, FL,April 20