RESEARCH PAPER | Engineering | Volume : 3 | Issue : 8 | Aug 2013 | ISSN - 2249-555X

Survey of Jamming Attacks and Techniques in Wireless Sensor Networks

KEYWORDS Senor Networks, Jamming, Attacks, Counter Measure, Energy-Efficiency, frequency hopping

Prakash J. Parmar
Sinhgad Institute of Technology, Lonavala Pune University India

Sachin D. Babar
Sinhgad Institute of Technology, Lonavala Pune University India

ABSTRACT *As wireless sensor networks continue to grow, so does the need for effective security mechanisms. Because sensor networks may interact with sensitive data and/or operate in hostile unattended environments, it is imperative that these security concerns be addressed from the beginning of the system design. However, due to inherent resource and computing constraints, security in sensor networks poses different challenges than traditional network/ computer security. There is currently enormous research potential in the field of wireless sensor network security. Thus, familiarity with the current research in this field will benefit researchers greatly. With this in mind, we survey the major topics in wireless sensor network jamming and attacks, and present the obstacles and the requirements in the sensor security, classify many of the current attacks and list their corresponding defensive measures/related work, and finally open challenges for the same.*

INTRODUCTION

Securing sensor networks is a challenging task due to the limited resources associated with low-cost sensor hardware. The combination of the commodity nature of wireless technologies and an increasingly sophisticated user base means that adversaries are able to easily gain access to communications between sensor devices by purchasing their own device and running it in a monitor mode. Conventional cryptographic security mechanisms are being translated to the sensor domain in order to defend against attacks like packet injection and spoofing network level control information. However, in spite of the progress being made to apply network security in the sensor realm, sensor networks will remain vulnerable to attacks that target their use of the wireless medium.

The wireless medium allows for radio interference attacks that target communications. Unlike traditional denial of service attacks, which are concerned with filling user domain and kernel domain buffers, jamming attacks exploit the shared nature of the wireless medium in order to prevent devices from communicating or receiving. Such attacks on the physical (PHY) layer have been known by the communications and radar community for some time, and there are numerous texts, such as [1, 2], which discuss the issues associated with these attacks. Typically, in the context of traditional communication systems, the objective of the jammer is to deny the reception of communications at the receiver using as little power as possible. In these systems jamming is usually addressed through spreading techniques, whereby resilience to interference is achieved by transmitting information using a bandwidth much larger than its required minimum bandwidth. Often, this spreading is also used to achieve multiple access, as in code-division multiple access (CDMA) cellular systems.

With the exception of some military systems, most commodity sensor and wireless networks do not employ sufficiently strong spreading techniques to survive jamming or to achieve multiple accesses. Instead, for reasons of cost, systems like the Berkeley MICA2, the Zigbee (e.g., MICAZ), and even 802.11 are based on a carrier sensing approach to multiple access. Because of their use of carrier sensing for medium access control (MAC), these systems are susceptible to a simple and severe jamming problem: an adversary can simply disregard the medium access protocol and continually transmit on a wireless channel. By doing so, he or she either prevents users from being able to commence with legitimate MAC operations, or introduces packet collisions that force repeated backoffs, or even jams transmissions. Such MAC and PHY layer security threats for wireless networks have been revisited recently by the Australian CERT [3], and will be a critical vulnerability for wireless sensor networks.

Finally our paper is organizes as, in section 2 we describe the security attacks and jamming attacks in section 3. In section 4 we describe the comparison of different physical layer security techniques and related works with detailed survey in section 5. Section 6 describes the open challenges and new research direction in security area of WSN and finally conclusion in section 7.

SECURITY ATTACKS

In this section we summarize most commonly seen attacks in wireless networks, as listed in Table 2.1 Most attacks can be classified into two categories: passive and active [4]. Passive attacks do not disrupt network operation, and the adversary's objective is to steal transmitted information from wireless channels. Two types of passive attacks are often used, eavesdropping intrusion and traffic analysis.

On the other hand, active attacks can significantly interfere with normal network operations because an adversary often tries to alter the network data. The most common forms of active attacks include denial-of-service (DoS) attacks, masquerade and replay attacks, and information disclosure and message modification attacks.

DoS attacks: A DoS attack is an adversary's attempt to exhaust the resources available to its legitimate users. Jamming is also widely used to launch DoS attacks at the physical layer. Radio frequency jamming can be employed to invade the transmitted signal band. An adversary can utilize jamming signals (thereby disrupting the communications) to make the attacked nodes suffer from DoS in a specific region [5].

Masquerade attacks: In a masquerade attack, an intruder pretends to be a legitimate user and deceives the authentication system so as to usurp the system resource. A masquerade attack usually involves another form of active attack. For example, the authentication sequences can be captured, and therefore an invalid user can obtain privileges to access information illegally.

Information disclosure and message modification: A compromised node can act as an information leaker by deliberate disclosure of confidential information to unauthorized nodes. Information such as the amount and periodicity of the traffic between a selected pair of nodes and the changing traffic patterns can be valuable to the adversaries in many military applications. Message modification refers to an attack in which an aggressor performs additions or deletions to the network communication content. For example, a message that says "Allow John Smith to read" may be modified as "Allow Fred Brown to read."

Eavesdropping intruders and traffic analysis: Eavesdropping is a way for an unintended receiver to intercept a message called an eavesdropper. A mobile communication session may contain confidential data. Thus, we have to prevent the eavesdroppers from learning the contents. Encryption is the most commonly used technique for masking the important contents. Eve might be able to intercept the transmitted signal but cannot obtain any critical information from it due to the encryption.

On the other hand, traffic analysis can also be used to determine the locations and identities of the communicating parties by intercepting and examining the transmitted messages. The traffic information may be useful for tracking the communication patterns of any two parties. Eavesdropping can be performed even if the messages are encrypted; hence, the malicious users can use the information gleaned from this type of attack for other forms of attack.

Table -1 Classification of the commonly used security attacks in wireless communication

Security Attack	
Passive Attack	Active Attack
Traffic Analysis	Denial of Service Attack
	Resources consumption
	Masquerade Attack
Eavesdropping	Reply Attack
	Information Disclosure
	Message Modification

JAMMING ATTACKS

There are many different attack strategies an adversary can use to jam wireless communications [6-8], such constant jammer, Deceptive jammer, Random jammer, Reactive jammer.

Constant jammer: The constant jammer continually emits a radio signal, and can be implemented using either a waveform generator that continuously sends a radio signal or a normal wireless device that continuously sends out random bits to the channel without following any MAC-layer etiquette. In general, the MAC protocol allows legitimate to send data packet if channel is sensed idle. Thus a constant jammer holds the channel by sending constantly dumpy packets.

Deceptive jammer: Instead of sending out random bits, the deceptive jammer constantly injects regular packets to the channel without any gap between subsequent packet transmissions.

As a result, a normal communicator will be deceived into believing there is a legitimate packet and be duped to remain in the receive state. For example, in Tiny OS, if a preamble is detected, a node remains in the receive mode, regardless of whether that node has a packet to send or not. Even if a node has packets to send, it cannot switch to the send state because a constant stream of incoming packets will be detected.

Random jammer: Instead of continuously sending out a radio signal, a random jammer alternates between sleeping and jamming. Specifically, after jamming for a while, it turns off its radio and enters a "sleeping" mode. It will resume jamming after sleeping for some time. During its jamming phase, it can behave like either a constant jammer or a deceptive jammer. This jammer model tries to take energy conservation into consideration, which is especially important for those jammers that do not have unlimited power supply.

Reactive jammer: The three models discussed above are active jammers in the sense that they try to block the channel irrespective of the traffic pattern on the channel. Active jammers are usually effective because they keep the channel busy all the time. As we shall see in the following section, these methods are relatively easy to detect. An alternative approach to jamming wireless communication is to employ a reactive strategy. The reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel. One advantage of a reactive jammer is that it is harder to detect.

As given in [8], Figure 1 shows the different types of jammers in attack category.

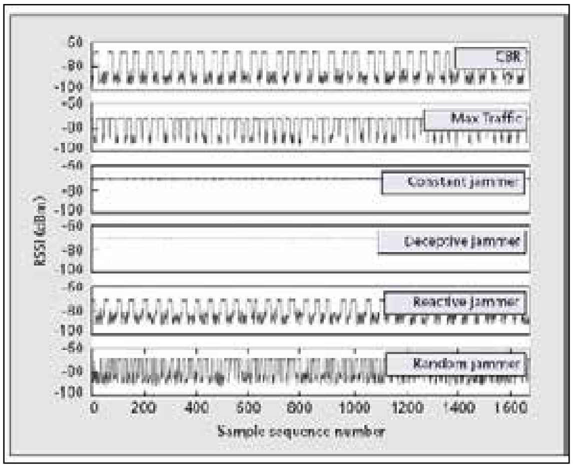

Figure 1: Jamming Type [10]

COMPARISON OF PHYSICAL LAYER SECURITY SCHEMES

Table 2 provides a brief summary for most popular physical layer security schemes in terms of their resistance against attacks and their security requirements. Of those schemes, some make use of the inherent characteristics of the channels, and they work depending on a variety of assumptions to ensure security. The assumptions include that an unauthorized user has a much worse channel than that of an intended user, or has no idea about the spreading codes or channel characteristics. Secrecy can be achieved while these assumptions are valid; otherwise, secrecy may not be obtained.

Table .3 makes a comparison among different approaches with respect to the computational complexity of resisting brute force attacks (decryption using the exhaustive key search). A larger key size makes it more difficult for an eavesdropper to decrypt the message, but the computational complexity will become a serious challenge to receivers since they have to decrypt all messages (even if those incoming messages have been changed by jamming or tampered with by illegitimate users). Alternately, anti-jamming and error correction codes can be employed to preserve data integrity.

Table 2: Comparison of different attack methods and their security schemes. [ref]

Security Scheme	Resisted Attacks	Achieved Security Requirement
RF fingerprint	Eavesdroping, resources consumption , masquerade	Authentication confidentiality
Rand MIMO	Eavesdropping	Confidentiality
AES CDMA	Eavesdropping	Confidentiality
ACDM	Eavesdropping	Confidentiality
FHSS	Jamming, eavesdropping, traffic analysis	Availability confidentiality
Pseudo- chaotic DS/SS	Eavesdropping, traffic analysis	Confidentiality
Artificial noise	Eavesdropping	Confidentiality

Table 3: Required decryption time comparison.

Approach	Method	Number of secret keys	Time required at 106 decryptionns/ ms
RF fingerprint	24-bit DES	1.7x108 keys	8.4 milliseconds
IS-95 CDMA	42-bit LFSR	4.4x1012 keys	2.2 seconds
AES CDMA	128-bit AES	3.4x1038 keys	5.4x1018 years
Rnad –MIMO	Random matrix	3.4x1038 x4 matrix	5.4x1018 years

RELATED WORKS / MOTIVATION

Table 4 lists all the works reviewed in this article. We focus on the countermeasures that have been analyzed and evaluated extensively (general-purposed and undocumented countermeasures, e.g. the use of spread spectrum hardware, are not listed). Furthermore we assume an efficient number of constant jammers with unlimited power supply that perform spot jamming attacks upon large-scale WSNs. We assume that not all WSN nodes are jammed at a same time. In the 'defense effectiveness' column we evaluate the level of defense each countermeasure provides against the above-mentioned jamming scenario while in 'compatibility with existing hardware' column we report if the proposed countermeasures are compatible with existing hardware or need a specialized hardware platform. Finally in 'expected implementation/ deployment cost' column we evaluate the implementation and deployment cost of each countermeasure. Also we have studded various jamming and security technique which we briefly summaries as shown in table 5.

Paper [10] work at physical layer to provided security using OFDM signal, which provided high security. In this [10] proposed method is fast and channel independent which uses cooperative jamming technique but it is not suitable for WSN since it energy consumption and power for computation is more also system is complex. Paper [11] proposed a game theory solution for physical layer security work on un-trusted rely friendly jammer. Advantage of this is non zero secrecy rate can be achievable but is is difficult to implement also system complexity is more so it is also not suitable for WSN. Paper [12] uses artificial Eigen vector method for channel estimation to provided security at physical layer but included estimation that required statistical data optimization which required high energy consumption.

Paper [13] cooperative jammer power allocation method which power management nice but scalability is big issue to implement it on WSN. Paper [14] work on link layer attack security using minimal protocol knowledge requirement, this provide energy efficiency and improve scalability of system but in this proposed method based on TDM which required high degree of synchronization.

From above discussion it is clear that we cannot adopt any jamming and security technique over wireless sensor network so we need to develop a new to scheme to tackle a jamming an attack issues in WSN this is the key motivation of our research work.

OPEN RESEARCH ISSUES

The constraints of contemporary sensor nodes resources (e.g. limited energy, computation and communication capabilities) and the fact that they are often deployed in insecure or even hostile terrains underline their susceptibility to jamming attacks. Therefore, the problem of jamming on the physical and data link layers of WSNs has been a subject of intense research during the last few years. However, there are still many open research issues, outlined below:

UWB transceivers: Despite the proposal of several spread spectrum schemes for defense against jamming attacks, the usage of UWB radio units has not extensively examined, although UWB exhibits many advantages against jamming.

Mobile agents: The use of MAs for defending against jamming attacks is a partially unexplored and promising method. Currently only two works address jamming in WSNs with the use of MAs [15] [16]. The unique characteristics of MAs could be explored to intensify their benefit upon WSNs under jamming attacks (e.g. the fact that traveling agents can temporary remain on their current position and return to the PE with their collected data when they sense clear terrain).

A new communication protocol that uses the 5 GHz ISM band, which suffers less interference compared to the heavily used 2.4 GHz band, needs to be proposed and designed. Also the 5 GHZ ISM band (5.15-5.35GHz and 5.725-5.825 GHz) offers more bandwidth for spread spectrum techniques compared to the 2.4 GHz ISM band (2.4 - 2.4835 GHz).

The antennas that sensor nodes currently use are omnidirectional. The design requirements and the implementation of alternative, interference and jamming-resistant antennas need to be devised.

The proposal of new modulation techniques and adaptive MAC protocols along with new power management schemes that enhance LPD/LPI properties of WSNs and make them stealth to the possible attackers.

Broadly we can categories security and jamming in three categories: Transmission security, Attack Security and Hybrid Security. Transmission security includes eavesdropping and privacy threats. In Attack security, the main objective of a node is to listen the ongoing communication and attack on the network Hybrid Security includes the characteristic of both transmission and attack security issues. In this paper our main objective is to tackle with the hybrid security issue. Fig 2 shows brief classification of all these three categories

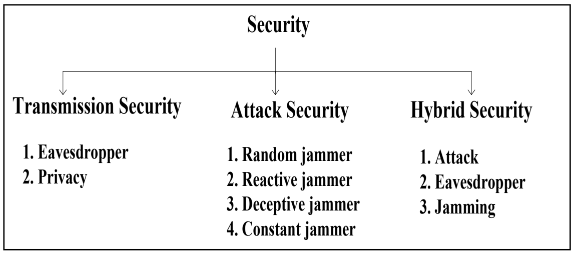

Figure 2: General classification of jamming and security

So based on our study we would like to propose a novel approach, where we would use a frequency hopping spread

–spectrum (FHSS) based anti-jamming method for secure communication in wireless sensor network. Our main objective with the research is to tack with the hybrid security issue as shown in figure 2.

CONCLUSIONS

As wireless sensor networks continue to grow and become more common, we expect that further expectations of security will be required of these wireless sensor network applications. In particular, the addition of anti jamming capability, as described in previous sections, will likely make strong security a more realistic expectation in the future. We also expect that the current and future work in jamming and attacks will make wireless sensor networks a more attractive option in a variety of new arenas.

In this paper we have described different types of attacks and jamming techniques in wireless sensor network security: obstacles, requirements, attacks, and defenses. Our aim is to provide both a general overview of the rather broad area of wireless sensor network security, and give the main citations such that further review of the relevant literature can be completed by the interested researcher.

Table-4: Characteristics and Features of proposed Anti-Jamming schemes

	Proposed countermeasures against jamming	Type of countermeasures	Defense effectiveness	Compatibility with existing hardware	Expected implementation/ deployment cost	Impact to energy efficiency
Feasibility of Lauanching and detecting jamming attacks in WSN	• Detection of jamming using signal strength • Detection of jamming using location information	Detection tech Detection tech	n/a n/a	Yes Yes	Low Low	Low Low
Radio interference detection protocol (RID)	• High normal packet detection • Information sharing • Interference calculation	Detection tech Detection tech Detection tech	n/a	Yes	Medium	High
Energy Efficient Link Layer jamming attacks against WSN MAC protocol	• S-MAC: High duty cycle • L-MAC : shorter data packet • Encryption of link layer packet • TDMA protocol • Transmission in randomized intervals	Proactive Software Proactive Software Proactive Software Proactive Software Proactive Software	Low	Yes	Low	Low
De-Jam: defecting energy –efficient jamming	• Frame masking • Frequency hopping • Packet fragmentation • Redundant encoding	Proactive Software	Medium	Yes	High	Medium
Hermes II node	• Hybrid FHSS-DSSS	Proactive Soft-Hard	High	No	High	Medium
How to secure a wireless sensor network by law and Having	• FHSS • L-MAC	Proactive Soft-Hard Proactive Software	Medium Low	Partial Yes	High Medium	Medium Low
JAM: a jammed area mapping service for sensor networks	• Detection of jamming • Mapping of jammed Area	Reactive Software	Medium	Yes	Medium	Low
Channel surfing and spatial retreat	• Channel surfing (Adaptive FHSS) • Spatial retreat	Reactive Soft-Hard	Medium Medium	Partial Partial	High High	Medium High
Wormhole-based anti jamming technique in sensor networks	• Wired pair of sensors • Frequency hopping pairs • Uncoordinated channel hopping	Reactive Soft-Hard	High Medium Medium	Partial Partial Partial	High High High	Low Medium Low
Jamming attack detection and countermeasures in WNS using ant system	• Ants (mobile agents)	Mobile Agent Based	Medium	Yes	Medium	Low
JAID	• Mobile agents	Mobile Agent Based	Medium	Yes	Medium	Low

Table 5: Comparisons between Different Proposed Security Method

Reference Number	[10]	[11]	[12]	[13]	[14]
Characteristics	Physical layer ,OFDM Signal	Un-trusted rely Friendly jammer, game theory solution	Physical layer, Channel estimation, Eigen vector, artificial intelligence	Physical layer, Cooperative jammer, power allocation method	Link layer, attack security, minimal protocol knowledge required
Advantage	High Security ,Channel Independent and non-cooperative Method	Non zero secrecy rate possible, cooperative method	Estimation error included, cooperative method, artificial method	Power management, suboptimal power allocation solution	Energy efficient , scalable, minimal protocol knowledge required, Simple algorithm,
Disadvantages	Need Statistical data, time synchronization,	Difficult solution, optimization	Statistical data required, optimization	scalability overhead	TDM based system, high degree of synchronization, suboptimal solution
Complexity	High	High	High	< low	low
Adoptable for sensor network	No [energy efficiency & Computation power]	No [energy efficiency & Computation power]	No [energy efficiency & Computation power, scalability]	Could be very difficult to adapt[energy efficient and scalability]	Adaptable but required s synchronization,

REFERENCE [1]. B. Sklar, Digital Communications: Fundamentals and Applications, Prentice Hall, 2nd ed., 2001. | [2]. J. G. Proakis, Digital Communications, McGraw-Hill, 4th ed., 2000. | [3]. AusCERT, “AA-2004.02 — Denial of Service Vulnerability in IEEE 802.11Wireless Devices,” http://www.auscert.org. | [4]. A D. Wyner, “The Wiretap Channel,” Bell System Tech. J., vol. 54, 1975, pp. 1355–87. | [5]. C. S. R. Murthy and B. S. Manoj, Ad Hoc Wireless Networks: Architectures and Protocols, Prentice Hall PTR, 2004 | [6]. W. Xu et al., “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks,” MobiHoc ’05: Proc. 6th ACM Int’l. Symp. Mobile Ad Hoc Net. and Comp., 2005, pp. 46–57. | [7]. Y. Law et al., “Link-Layer Jamming Attacks on S-Mac,” Proc. 2nd Euro. Wksp. Wireless Sensor Networks, 2005, pp. 217–25. | [8]. A Wood and J. Stankovic, “Denial of Service in Sensor Networks,” IEEE Comp., vol. 35, no. 10, Oct. 2002, pp. 54–62. | [9]. Wenyuan Xu, Ke Ma, Wade Trappe and Yanyoung Zhang “Jamming Sensor networks: Attack and Defense Strategies” , IEEE network, , vol,pp 41-47 , May/June 2006 | [10]. Gollakota, S.; Katabi, D.; , "Physical layer wireless security made fast and channel independent," INFOCOM, 2011 Proceedings IEEE , vol., no., pp.1125-1133, 10-15 April 2011 | [11]. Rongqing Zhang, Lingyang Song, Zhu Han and Bingli Jiao “Physical Layer Security for Two-Way Un trusted Relaying with Friendly Jammers” IEEE 2012 | [12]. James M. Taylor, Jr., Michael Hempel, Hamid Sharif, Yang “Impact of Channel Estimation Errors on Effectiveness of Eigenvector-Based Jamming for Physical Layer Security in Wireless Networks”, IEEE CAMAD 2011 | [13]. Lun Dong Homayoun Yousefi’zadeh Hamid Jafarkhani “Cooperative Jamming and Power Allocation for Wireless Relay Networks in Presence of Eavesdropper”,IEEE ICC 2011 | [14]. Yee Wei Law, Lodwijk van Hoesel, Jeroen Doumen, Pieter Hartel and Paul havinga “Energy Efficient Link Layer Jamming Attack against Wireless Sensor Network MAC Protocol” , ACM , SACN November 7, 2005 | [15]. Rajani Muraleedharan and Lisa Osadciw, “Jamming Attack Detection and Countermea-sures In Wireless Sensor Network Using Ant System”, 2006 SPIE Symposium on Defense and Security, Orlando, FL, April, 2006. | [16]. B. Krishnamachari, D. Estrin, S. Wicker, ‘‘Modelling Data-Centric Routing in Wireless Sensor Networks,’’ Proceedings of the 21st Annual Joint Conference of the IEEE Computer and Communications Societies (InfoCom’02), New York, June 2002 |