www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11289-11296

Survey Of Electronic Countermeasures Attacks And Techniques In Wireless Detector Networks

Sundar R*
*Final Year Student [M.C.A,], Vel Tech Dr.Rr & Dr.Sr University, Avadi.
Sundar.Ayan007@Gmail.Com

Abstract:

As wireless detector networks still grow, therefore will the necessity for effective security mechanisms. Because sensor networks might move with sensitive information and/or operate in hostile unattended environments, it is imperative that these security considerations be addressed from the start of the system style. However, thanks to inherent resource and computing constraints, security in detector networks poses totally different challenges than ancient network/ computer security. There's presently huge analysis potential within the field of wireless detector network security. Thus, familiarity with this analysis during this field can profit researchers greatly. With this in mind, we have a tendency to survey the key topics in wireless detector network ECM and attacks, and gift the obstacles and also the necessities within the detector security, classify many of this attacks and list their corresponding defensive measures/related work, and at last open challenges for the same.

Keywords: network, wireless, security, detector, attacks.

1. Introduction:

Securing sensing element networks may be a difficult task attributable to the limited resources related to affordable sensing element hardware. the mixture of the artifact nature of wireless technologies associate degreed an progressively refined user base implies that adversaries area unit ready to simply gain access to communications between sensing element devices by getting their own device and running it in an exceedingly monitor mode. Standard science security mechanisms area unit being translated to the sensing element domain so as to defend against attacks like packet injection and spoofing network level management info. However, in spite of the progress being created to use network security within the sensing element realm, sensing element networks can stay liable to at- tacks that focus on their use of the wireless medium.

The wireless medium permits for radio interference attacks that focus on communications. Not like ancient denial of service at- tacks, that area unit involved with filling user domain and kernel domain buffers,

jam attacks exploit the shared nature of the wireless medium so as to forestall devices from human activity or receiving. Such attacks on the physical (PHY) layer are renowned by the communications and radar community for a few times, and there is a unit various texts, which debate the problems related to these attacks. Typically, within the context of ancient communication systems, the target of the transmitter is to deny the reception of communications at the receiver mistreatment as very little power as attainable. In these systems jam is sometimes self-addressed through spreading techniques, whereby resilience to interference is achieved by transmittal info employing a band- dimension abundant larger than its needed minimum information measure. Often, this spreading is additionally accustomed attain multiple access, as in code-division multiple access (CDMA) cellular systems.

With the exception of some military systems, most commodity sensing element and wireless networks don\'t use sufficiently sturdy spreading techniques to survive jam or to attain multiple accesses. Instead, for reasons of value, systems just like the Berkeley MICA2, the Zigbee (e.g., MICAZ), and even 802.11 area unit supported a carrier sensing approach to multiple access. Thanks to their use of carrier sensing for medium access management (MAC), these systems area unit susceptible to a straightforward associate degreed severe jam problem: an adversary will merely disregard the medium access protocol and frequently transmit on a wireless channel. By doing thus, he or she either prevents users from having the ability to begin with legitimate raincoat operations, or introduces packet collisions that force continual backoffs, or maybe jams transmissions. Such raincoat and PHY layer security threats for wire- less networks are revisited recently by the Australian sure thing , and can be a essential vulnerability for wireless sensor networks.

Finally our paper is organizes as, in section two we have a tendency to describe the safety attacks and jam attacks in section three. In section four we have a tendency to describe the comparison of various physical layer security techniques and connected works with careful survey in section five. Section half dozen describes the open challenges and new analysis direction in security space of WSN and eventually conclusion.

2. Jamming Attacks:

There square measure many alternative attack methods associate degree person will use to jam wireless communications , such constant jammer, Deceptive transmitter, Random transmitter, Reactive transmitter.

Constant transmitter: The constant jammer frequently emits a radio emission, and might be enforced victimisation either a wave- type generator that unendingly sends a radio emission or a standard wireless device that unendingly sends out random bits to the channel while not following any MAC-layer rule. In general, the macintosh protocol permits legitimate to send information packet if channel is detected idle.

Therefore a relentless transmitter holds the channel by causation perpetually dumpy packets.

Deceptive jammer: rather than causation out random bits, the deceptive transmitter perpetually injects regular packets to the channel with none gap between sequent packet transmissions. As a result, a standard someone are deceived into believing there\'s a legitimate packet and be duped to stay within the receive state. As an example, in Tiny OS, if a preamble is detected, a node remains within the receive mode, in spite of whether or not that node contains a packet to send or not. Even if a node has packets to send, it cannot switch to the send state as a result of a relentless stream of incoming packets are detected.

Random jammer: Rather than unendingly causation out a radio emission, a random transmitter alternates between sleeping and ECM. Specifically, when ECM for a jiffy, it turns off its radio and enters a "sleeping" mode. It will resume ECM when sleeping for a few times. Throughout its ECM part, it will behave like either a relentless transmitter or a deceptive transmitter. This transmitter model tries to require energy conservation into thought, that is particularly necessary for those jammers that don\'t have unlimited power offer.

Reactive jammer: The 3 models mentioned on top of square measure active jammers within the sense that they struggle to dam the channel regardless of the route on the channel. Active jammers square measure typically effective as a result of they keep the channel busy all the time. As we have a tendency to shall see within the following section, these ways square measure comparatively straightforward to discover. An alternate approach to ECM wireless communication is to use a reactive strategy. The reactive transmitter stays quiet once the channel is idle, however starts transmittal a radio emission as presently because it senses activity on the channel. One advantage of a reactive transmitter is that it\'s tougher to discover.

3. Security attacks:

In this section we have a tendency to summarize most ordinarily seen attacks in wireless networks. Most attacks may be classified into 2 categories: passive and active. Passive attacks don\'t disrupt network operation, and therefore the adversary's objective is to steal transmitted data from wireless channels. 2 styles of passive attacks area unit usually used, eaves- dropping intrusion and traffic analysis.

On the opposite hand, active attacks will considerably interfere with traditional network operations as a result of a person usually tries to change the network knowledge. The foremost common kinds of active attacks embrace denial-of-service (DoS) attacks, masquerade and replay attacks, and knowledge speech act and message modification attacks.

DoS attacks: A DoS attack is AN adversary's decide to exhaust the resources accessible to its legitimate users. ECM is additionally wide wont to launch DoS attacks at the physical layer. oftenness ECM may be utilized to invade the

transmitted signal band. A person will utilize ECM signals (thereby disrupting the communications) to create the attacked nodes suffer from DoS during a specific region.

Masquerade attacks: During a masquerade attack, a trespasser pretends to be a legitimate user and deceives the authentication system therefore on usurp the system resource. A masquerade attack sometimes involves another style of active attack. As an example, the authentication sequences may be captured, and so an invalid user will acquire privileges to access data lawlessly.

Information speech act and message modification: A compromised node will act as a data source by deliberate speech act of direction to unauthorized nodes. Data like the quantity and cyclicity of the traffic between a particular try of nodes and therefore the ever-changing traffic patterns may be valuable to the adversaries in several military applications. Message modification refers to AN attack during which AN aggressor performs additions or deletions to the network communication content. As an example, a message that claims "Allow adventurer to browse" could also be changed as "Allow Fred Brown to read."

Eavesdropping intruders and traffic analysis: Eavesdropping could be a manner for an uncaused receiver to intercept a message referred to as a listener. A mobile communication session could contain confidential knowledge. Thus, we have to forestall the eavesdroppers from learning the contents. Coding is that the most ordinarily used technique for masking the vital contents. Eve could be ready to intercept the transmitted signal however cannot acquire any important data from it as a result of the coding.

On the opposite hand, traffic analysis also can be wont to determine the locations and identities of the human activity parties by intercepting and examining the transmitted messages. The traffic data could also be helpful for following the communication patterns of any 2 parties. Eavesdropping may be performed though the messages area unit encrypted; therefore, the malicious users will use the knowledge gleaned from this kind of attack for different kinds of attack.

4. Comparisons of testing scheme:

Table a pair of provides a short outline for many standard physical layer security schemes in terms of their resistance against attacks and their security needs. Of these schemes, some create use of the inherent characteristics of the channels, and that they work counting on a range of assumptions to confirm security. The assumptions embody that Associate in Nursing unauthorized user incorporates a abundant worse channel than that of Associate in Nursing supposed user, or has no plan regarding the spreading codes or channel characteristics. Secrecy will be achieved whereas these assumptions are valid; otherwise, secrecy might not be obtained.

A comparison among completely different approaches with relevance the machine quality of resisting brute force attacks (decryption

victimisation the complete key search). a bigger key size makes it harder for Associate in Nursing snoop to decipher the message, however the computational quality can become a significant challenge to receivers since they need to decipher all messages (even if those incoming messages are modified by jam or tampered with by illegitimate users). Alternately, anti- jam and error correction codes will be used to preserve knowledge integrity.

5. Related work and motivation:

We target the countermeasures that are analyzed and evaluated extensively (general-purposed and unregistered counter- measures, e.g. the utilization of unfold spectrum hardware, don\'t seem to be listed). what is more we have a tendency to assume associate degree economical range of constant jammers with unlimited power provide that perform electronic jamming attacks upon large-scale WSNs. we have a tendency to assume that not all WSN nodes area unit packed at a same time. within the 'defense effectiveness' column we have a tendency to measure the extent of defense every measure provides against the above-named ECM state of affairs whereas in 'compatibility with existing hardware' column we have a tendency to report if the planned countermeasures area unit compatible with existing hardware or would like a specialised hardware platform. Finally in 'expected implementation/ preparation value' column we have a tendency to measure the implementation and preparation cost of every measure.

Paper work physical layer to provided security mistreatment OFDM signal that provided high security. During this pro- expose methodology is quick and channel freelance that uses cooperative ECM technique however it\'s not appropriate for WSN since it energy consumption and power for computation is a lot of conjointly system is complicated. Paper planned a theory of games resolution for physical layer security work on un-trusted trust friendly transmitter. Advantage of will be none zero secrecy rate can be doable however is troublesome to implement conjointly system complexness is a lot of thus it\'s conjointly not appropriate for WSN. Paper uses artificial chemist vector methodology for channel estimation to provide security at physical layer however enclosed estimation that needed applied mathematics knowledge improvement that needed high energy consumption.

Paper cooperative transmitter power allocation methodology that power management nice however measurability is massive issue to implement it on WSN. Paper work on link layer attack security mistreatment bottom protocol data demand, this offer energy potency and improve measurability of system but during this planned methodology supported TDM that needed high degree of synchronization.

From the discussion it's clear that we have a tendency to cannot, adopt associate degree {jamming|electronic ECM|jam|electronic countermeasures|ECM} and security technique

over wireless detector network thus we would like to develop a replacement to theme to tackle a jamming an attack problems in WSN this is often the key motivation of our research work.

6. Open Research Issues:

OPEN analysis problems: The constraints of up to date detector nodes resources (e.g. restricted energy, computation and communication capabilities) and also the undeniable fact that they\'re typically deployed in insecure or maybe hostile terrains underline their condition to ECM attacks. Therefore, the matter of ECM on the physical and circuit layers of WSNs has been a theme of intense analysis throughout the previous few years. However, there is a unit still several open analysis problems, made public below:

UWB transceivers: Despite the proposal of many unfold spectrum schemes for defense against ECM attacks, the usage of UWB radio units has not extensively examined, all though UWB exhibits several blessings against ECM

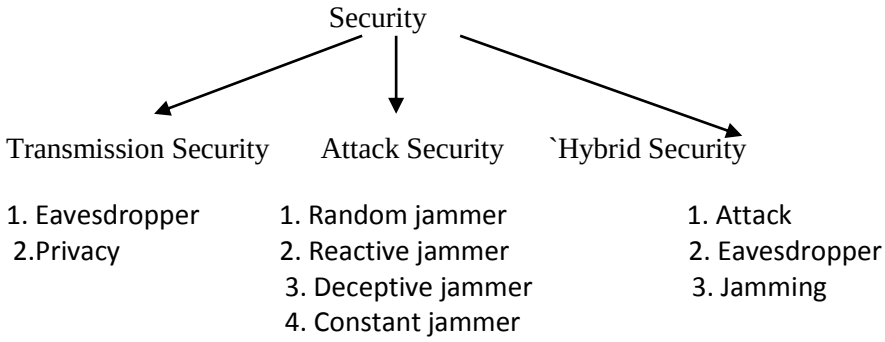
Mobile agents: The utilization of MAs for defensive against jam- dynasty attacks could be a partly undiscovered and promising methodology. Presently solely 2 works address ECM in WSNs with the utilization of MAs. The distinctive characteristics of MAs may be explored to accentuate their profit upon WSNs beneath jam-dynasty attacks (e.g. the very fact that traveling agents will temporary stay on their current position and come to the alphabetic character with their collected knowledge once they sense clear terrain).

A new communication protocol that uses the five gigacycle belief band, that suffers less interference compared to the heavily used a pair of.4 GHz band, must be planned and designed. Conjointly the five gigacycle belief band (5.15-5.35GHz and five.725-5.825 GHz) offers a lot of information measure for unfold spectrum techniques compared to the two.4 gigacycle belief band (2.4 - 2.4835 GHz).

The antennas that detector nodes presently use area unit omni-directional. The planning necessities and also the implementation of other, interference and jamming-resistant antennas got to be devised.

The proposal of recent modulation techniques and adjustive macintosh protocols along side new power management schemes that enhance LPD/LPI properties of WSNs and build them concealment to the potential attackers.

Broadly we are able to classes' security and ECM in 3 categories: Transmission security, Attack Security and Hybrid Security. Transmission security includes eavesdropping and privacy threats. In Attack security, the most objective of a node is to concentrate the continued communication and attack on the network Hybrid Security includes the characteristic of each transmission and attack security problems. During this paper our main objective is to tackle with the hybrid security issue. Fig[1] a pair of shows temporary classification of of these 3 classes of security



We would wish to propose a completely unique approach, wherever we would use a frequency hopping unfold spectrum (FHSS) based mostly anti-jamming methodology for secure communication in wireless detector network. Our main objective with the analysis is to tack with the hybrid security issue.

7. CONCLUSION:

As wireless detector networks still grow and become a lot of common, we have a tendency to expect that more expectations of security are needed of those wireless detector network applications. Specially, the addition of opposing ECM capability, as delineated in previous sections, can doubtless build robust security a lot of realistic expectation within the future. We have a tendency to conjointly expect that the present and future add ECM and attacks can build wireless detector networks a lot of enticing choice in a very style of new arenas.

In this paper we\'ve delineated differing types of attacks and ECM techniques in wireless detector network security: obstacles, necessities, attacks, and defenses. Our aim is to produce each a general summary of the rather broad space of wireless detector network security, and provides the most citations such more review of the relevant literature is completed by the interested investigator.

REFERENCES:

[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 |