Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

An Efficient Security Mechanisms for Different Sort of Attacks in CWSN

K.Katyayini[1] and S.V. Ramanamurthy[2]

[1] Pragati Engineering College, Surampalem - JNTU Kakinada

Received: 15 December 2012 Accepted: 3 January 2013 Published: 15 January 2013

Abstract

One of the major important aspects of wireless sensor networks (WSNs) is their capability to collect and process huge amounts of information in parallel with the help of small, power limited devices enabling their use in observation, target detection and various other monitoring applications. Recently, new ideas have been proposed to develop cognitive WSNs (CWSNs) to enhance awareness about the network and environment, and make adaptive decisions based on the application goals. A CWSN is a special network, which has many constraints compared to traditional wireless network. But the major problem is security. In this paper discovering various security threats in these networks and various defense mechanisms to counter these vulnerabilities. Various types of attacks on CWSNs are categorized under different classes based on their natures and targets, and corresponding to each attack class, appropriate security mechanisms are discussed.

Index terms— WSN, WSN attacks, cognitive WSN.

1 Introduction

ver the last decade, wireless sensor networks (WSNs) have attracted a lot of interest in the research community due to their wide range of potential applications. A WSN consists of hundreds or even thousands of small devices each with sensing, processing, and communication capabilities to monitor a real-world environment. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring and building security monitoring **??**Akyildiz et al., 2002). Most of the WSN deployments operate in the unlicensed ISM bands **??**2.4GHz). Several other small range wireless protocols like Wi-Fi, Bluetooth etc. also use the same band. This has led to overcrowding in this band with the increasing deployment of WSN-based applications. As a result, coexistence issues in the ISM bands have attracted extensive research attention (Cavalcanti et al., 2007).

The increasing demand for spectrum in wireless communication has made efficient spectrum utilization a big challenge. To address this important requirement, cognitive radio (CR) has emerged as the key technology. A CR is an intelligent wireless communication system that is aware of its surrounding environment, and adapts its internal parameters to achieve reliable and efficient communication and optimum utilization of the resources (Mitola, 2000).With the advent of CR technology, we have a different perspective of the traditional WSNs. In the current cognitive wireless sensor networks (CWSNs), the nodes change their transmission and reception parameters according to the radio environment. Cognitive capabilities are based on four activities: (i) monitoring of spectrum sensing, (ii) analysis and characterization of the environment, (iii) optimization of the best communication strategy based on different constraints such as reliability, power, security and privacy issues etc., and (iv) adaptation and collaboration strategy. The cognitive technology will not only enable access to new spectrum but it will provide better propagation characteristics leading to reduction in power consumption, network life-time and reliability in a WSN. With cognitive capabilities, WSN will be capable of finding a free channel in the unlicensed band to transmit or could find a free channel in the licensed band for communication.

A CWSN, therefore, will be able to provide access not only to new spectrum bands in addition to the available 2.4 GHz band, but also to the spectrum band that has better propagation characteristics. If a channel in a lower frequency band is accessed, it will certainly allow communications with higher transmission range in a CWSN, and hence fewer sensor nodes will be required to provide coverage in a specific area with a higher network lifetime due to lower energy consumption in the nodes. CWNs will also provide better propagation characteristics by adaptively changing systems parameters like modulation schemes, transmit power, carrier frequency and constellation size. The result will be a more reliable communication with reduced power consumption, increased network lifetime and higher reliability and enhanced quality of service (QoS) guarantee to applications.

There is some basic difference between WSN and CWSN. In CWSN nodes change their transmission and reception parameters according to the radio environment. Cognitive capabilities are based in four technical components: sensing spectrum monitoring, analysis and environment characterization, optimization for the best communication strategy based on different constrains (reliability, power consumption, security, etc.) and adaptation and collaboration strategy. Adding those cognition capabilities to the existing WSN infrastructure will bring about many benefits. In fact, WSN is one of the areas with the highest demand for cognitive networking. In WSN, node resources are constrained mainly in terms of battery and computation power but also in terms of spectrum availability.

Hence with cognitive capabilities, WSN could find a free channel in the unlicensed band to transmit or could find a free channel in the licensed band to communicate. CWSN could provide access not only to new spectrum (rather than the worldwide available 2.4 GHz band), but also to the spectrum with better propagation characteristics. A channel decision of lower frequency leads more advantages in a CWSN such us higher transmission range, fewer sensor nodes required to cover a specific area and lower energy consumption.

This way, CWSN is a new concept proposed in literature [4] with the following advantages:

? Higher transmission range.

? Fewer sensor nodes required to cover a specific area. ? Better use of the spectrum.

? Lower energy consumption.

? Better communication quality.

? Lower delays.

? Better data reliability.

2 II.

3 Motivation

The ultimate goal is to design WSNs which are more aware of the concurrent conditions of the network, can make decisions based on the information, and take actions. Based on definition of cognitive WSN in [5], a cognitive WSN should be aware of the amount of sensory data being communicated and know when and where to forward it. It can allow the network to avoid communicating sensed data when it is not necessary. The energy available to each node is fed back to determine a maximum average power. This in turn dictates a maximum duty cycle for the node and a constraint on the maximum sleep time [6]. In addition, because cognitive sensor networks should have such high level of knowledge about the environment and the types of information exchanged, they must be application specific. The main aspects of the cognitive network are behavior-oriented architecture with agents that have a sensor-based robust behavior with slow rate of processing, distributed control, small size, and inexpensive low power consumption hardware [6]. We believe that cognition, when incorporated in sensor networks will enable achieving the following objectives: (i) Make the network aware of, and dynamically adapt to, application requirements and the environment in which it is deployed. (ii) Provide a holistic approach to enable the sensor network to achieve its end-to-end goals, i.e. gather information about the network status from network and MAC layers, application requirements from the application layer and achieve the objectives of the network.

Since WSN is comprised of low power consumption devices with limited processor capabilities, cognition should be implemented in such an infrastructure. To avoid imposing high load of processing or forcing a costly upgrade on all devices of a WSN, this work proposes implementing new devices called cognitive nodes. By using cognitive nodes in the network, the performance of the network would be improved and the cost as well, so the cost must justify the performance [9]. Cognitive nodes are designed such that they use the same infrastructure as sensor nodes but are able to handle cognition processes and manage decisions and actions by commanding other nodes. This way the cost added due to cognition will be as low as possible and can benefit from previous developments in the design of sensor nodes. Since WSN employs nodes with limited batteries which need to last for a long time one of the challenges is how to maximize lifetime. Transmission is one of the most power consuming processes in sensor nodes and nonefficient transmissions of data can lead to a shorter lifetime. So this work tries to schedule nodes' transmission rate by the means of cognition to maximize lifetime. In addition, since in a WSN, there are redundant sensor nodes deployed, efficient scheduling of the redundant nodes can lead to an improved lifetime.

The Main Characteristics of a CWSN can be divided in to three parts:? Awareness ? Decision making ? Taking appropriate action III.

4 Related Work

First works about security in CR were developed specifically to analyse the effects produced by cognitive features and how they could be used to mitigate the negative effects. So, as we have said, in the article [7] each characteristic and the attacks that could take advantage of it are analysed. A different point of view is shown in the article of Zhang and Li [1]. They make a survey about the weaknesses introduced by the nature of CR. They base the security of the system in two tasks: protection and detection, and divide the attacks and countermeasures depending on which layer of the protocol stack affects. The article [2] studies threats that affect the ability to learn of cognitive networks and the dynamic spectrum access. To conclude the general references about security, it should be noted the article of Goergen and Clancy [9] where an attack classification in cognitive networks is done: DSA attacks, objective function attacks and malicious behaviour attacks.

In [3], two specific attacks against cognitive networks are analysed: primary user emulation (PUE), Year and sensing data falsification. It also provides some countermeasures well adapted to static scenarios such as TV system. In [4], a secure protocol spectrum sensing is presented. It bases its functionality on the generation and transmission of specific keys to each node. As a third example of safety sensing investigation, the research [5] proposes a collaborative algorithm based on energy detection and weighted combining (similar to a reputation system) to prevent malicious users.

Related to specifics attacks, the most studied against CR is the PUE, which was defined by Chen and Park [6] for the first time in 2006. Since then, research of the same authors [7] has focused on countermeasures against PUE. Also, in [18] a way to detect the PUs through an analytical model that does not require location information is shown. As well as the PUE attack, the community of researchers in CR has been studying other kind of attacks originate from different wireless networks, such as denial of service (DoS) attack jamming attack. These attacks have special characteristics in cognitive networks, for example, article [9] studies these features for DoS, and [2] shows a countermeasure based on frequency hopping (technically possible in CR) to avoid jamming attacks.

5 IV.

6 Attacks in CWSN a) Communication Attacks

This types of attacks the attacker affects data transmissions between nodes with a concrete purpose. The goal could be from isolate a node to try to change the behavior of whole network.

7 b) Replay Attack

It consists on the replay of messages from inside or outside the current run of communication [6]. For example, message is directed to other than the intended node. This receiver node replays the message to the intended principal and this receives the delayed message. This delay is fundamental to calculate network characteristics (channel, topology, routing, etc.).

8 c) Jamming Attack

In this attacks, the transmission of a radio signal that interferes with the radio frequencies used by nodes. Jamming attack is one of the most studied attacks against WSN [7]. However, CWSN has great advantages to solve jamming but also can produce negative effects like energy consumption or communication failures. A typical jamming attack is a high power transmission using the PU frequency.

9 d) Collision Attack

It consist of the intention of violate the communication protocol [8]. This attack does not consume much energy of the attacker but can cause a lot of disruptions to the network operation. Due to the wireless broadcast nature, it is not trivial to identify the attacker.

10 e) Routing ill-directing attack

In this attack, a malicious node simply refuses to route messages. Examples of this kind of attacks are the grey hole and black hole ones. In these attacks, the nodes refuse all packets that arrive or a percentage thereof. Because of this misinformation, the network can change the routes, the topology or leaving isolated nodes.

11 f) Sybil Attack

It is defined as a malicious device illegitimately taking multiple identities. Sybil attack is effective against routing algorithms, voting, reputation systems and foiling misbehavior detection.

12 g) Against privacy attacks

It is also important attack class is attacks against privacy. CWSNs allow sharing resources to establish a communication and to be aware of environment. Attackers could use this access to take some of node information. The attacks against node privacy include eavesdropping, through taping the information; the attacker could easily

discover the communication contents. Impersonating attack, where the attacker joins to the network and it can impersonate the original victim sensor node to receive packet, and traffic analysis, using wireless and cognitive features to listen in the entire spectrum. Traffic analysis attacks **??**19] try to deduce the context information of nodes analysing the traffic pattern from eavesdropping on wireless communication. Acquired information could be used to prepare a most harmful attack. For example, spectrum information can be used to know what the weakest spectrum zone is or where the PUs are emitting. h) Node-targeted attacks Node-targeted attacks need more attention that in a normal WSN because of the propagation of information is more important for the correct working of CWSN. A node can be captured and attackers use reverse engineered and become an instrument for mounting counterattacks. Other possibility is to destroy the nodes. This destruction not only affects to node functionality, but also affects whole network. Usually, node-targeted attacks ought to be less important for WSN. However, distributed information and cooperational behavior in CWSN make a captured node a powerful weapon for attackers. Extracting a cryptographic key and modifying the internal device code are examples of node targeted attacks.

13 i) Power consumption attacks

CWSNs are susceptible to attack, because they are cheap small devices. Small size of nodes and batteries makes CWSN very vulnerable to power consumption attacks. The attacker can inflict sleep(D D D D D D D D)

Year torture on an energy constrained node by engaging in it unnecessary communication work to quickly drain its battery power. Depriving the power of a few crucial nodes (e.g. Access Point) may lead communication breakdown of the entire network. Attacker node can request a channel change every time, increasing power consumption.

V.

14 Proposed System

A robust authentication mechanism is a prime requirement in collaborative spectrum sensing. The authentication scheme may have different perspectives to different categories of nodes in a CWSN. The authentication of the primary users is a critical issue since an attacker may transmit signals with high power that has close resemblance with the signals of a primary user and launch a primary user emulation (PUE) attack **??**Chen et al., 2008c; **??**iu et al., 2010). To prevent such an attack, the secondary users should have a robust verification scheme for verifying the authenticity of the received signals. Similarly, when the secondary users receive the sensing reports from other users, they should be able to verify the authenticity of the other secondary users; otherwise, a potential adversary may be able to spoof the identity of a secondary user. The authentication of sensing reports distributed across the network is also a very important issue. Even if the authentications of the secondary users are done during the sensing report aggregation process, it is still possible for a malicious secondary user to send false sensing reports and launch spectrum sensing data falsification (SSDF) attack **??**Wang et al., 2009b). Hence, each sensing report in the aggregation process should be authenticated.

A popular approach for defending against unauthorized spectrum access is to deploy a spectrum monitoring system in the CR network. The spectrum monitoring system acts as a spectrum ”watch guard” for detecting spectrum misuse and carries out the following functions: (i) monitoring of the spectrum usage in a specific spatial region and over a range of frequencies, (ii) identifying wireless services and the nodes providing such services. However, design of an effective spectrum monitoring system is a challenging task since natural or man-made obstacles can change the features of the radio signal, and identification of wireless services may be difficult if an attacker can successfully emulate a specific wireless service being provided in the network. To address these problems, spectrum monitoring systems can be distributed across the nodes. Information on the wireless services in an area can be transmitted to a central monitoring location, which can, then, correlate the various inputs and check the received information against other data like the known position of the wireless services in the area and their source.

The cognitive pilot channel (CPC) of a CR network is responsible for distributing the cognitive control messages. The CPC is vulnerable to numerous attacks including the DoS attacks and the saturation attacks on the control channels. A popular protection mechanism against the jamming attack in a specific spectrum band of a CR network is to use frequency hopping. The CPC could use more than one spectrum band and ”hop” around the spectrum bands to avoid a possible jamming attack. The trade-off is an increased complexity of the CR network as the CR nodes should be notified about the change in the frequency band of the CPC. If an attacker effectively monitors the CPC, it could ”chase” the CPC band for every change and eventually cause continual adaptation and outage of service to the CR network.

Yue et al. present two coding schemes for recovering lost packets transmitted through parallel channels coding technique (Yue & Wang, 2009). The two coding schemes, known as rateless coding and piecewise coding, can be adapted to CWSNs for protecting the CPC and CCC. Meucci et al. present a lightweight mechanism for achieving security in the PHY layer in a CR network using orthogonal frequency division multiplexing (OFDM) (Meucci et al., 2009). In the proposed scheme, the user’s data symbols are mapped over the physical sub-carriers using a permutation strategy. The security in the PHY layer is achieved using a random and dynamic sub-carrier permutation which is based on a single pre-shared information.

15 VI.

16 Conclusion

CWSNs are increasingly being used in military, environmental, health and commercial applications. These networks are inherently different from traditional wireless networks as well as WSNs. Security is a mandatory feature for the deployment of CWSNs. This article summarizes the attacks and their taxonomy and also an attempt has been made to explore the security mechanisms widely used to handle those attacks. The challenges of WSNs are also briefly discussed. Security issues are a novel research area. This survey will hopefully motivate future researchers to design smarter and more robust security mechanisms and make their networks safer.

.1 Global Journals Inc. (US) Guidelines Handbook

www.GlobalJournals.org

[Thomas and Virgin Islands ()] , U S Thomas , Virgin Islands . 2008. 1 p. .

[Cavalcanti et al. ()] 'Achieving energy efficiency and QoS for low-rate applications with 802.11e. IEEE Wireless Communications and An Efficient Security Mechanisms for Different Sort of Attacks'. D Cavalcanti , Schmitt , Soomro . *CWSN Networking Conference (WCNC)*, (Hong Kong) 2007. p. .

[Burbank ()] Burbank . *Security in cognitive radio networks: the required evolution in approaches to wireless network security. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, (Singapore) 2008. CrownCom. p. .

[Cavalcanti et al.] 'Cognitive radio based wireless sensor networks'. D Cavalcanti , Das , Wang , Challapali . *Proceedings of 17th International Conference on Computer Communications and Networks*, (17th International Conference on Computer Communications and Networks) St.

[Mitola ()] *Cognitive radio: an integrated agent architecture for software defined RADIO*, J Mitola . 2000. Stockholm, Sweden. Royal Institute of Technology (Ph.D. dissertation)

[As Zahmati et al. ()] 'Cognitive wireless sensor networks: emerging topics and recent challenges'. As Zahmati , Hussain , Fernando , Grami . *IEEE International Conference Science and Technology for Humanity (TIC-STH)*, (Toronto, Canada) 2009. p. .

[Howitt and Gutierrez ()] 'low rate–wireless personal area network coexistence issues'. Howitt , Gutierrez . IEEE 802.15.4. *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, (IEEE Wireless Communications and Networking Conference (WCNC)New Orleans, Louisiana, USA) 2003. 3 p. .

[Xiaojiang and Hsiao-Hwa ()] 'Security in wireless sensor networks'. D Xiaojiang , Hsiao-Hwa . *IEEE Wirel Commun* 2008. 15 (4) p. .

[Zhang et al. ()] 'Security threats in cognitive radio networks'. Y Zhang , X Xu , Geng . *Proceedings of the 10th IEEE international Conference on High Performance Computing and Communications (HPCC)*, (the 10th IEEE international Conference on High Performance Computing and Communications (HPCC)Dalian, China) 2008. p. .

[Tc Clancy and Goergen ()] Tc Clancy , Goergen . *Security in cognitive radio networks: threats and mitigation. 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications*, (Singapore) 2008. CrownCom. p. .

[Zhang and Li ()] 'The security in cognitive radio networks: a survey'. X Zhang , Li . *Proceedings of the International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC)*, (the International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC)New York, NY) 2009. ACM. p. .