EURASIP Journal on
Wireless Communications and Networking
a SpringerOpen Journal

REVIEW Open Access

Security in cognitive wireless sensor networks. Challenges and open problems

Alvaro Araujo*, Javier Blesa, Elena Romero and Daniel Villanueva

Abstract

A cognitive wireless sensor network (CWSN) is an emerging technology with great potential to avoid traditional wireless problems such as reliability. One of the major challenges CWSNs face today is security. A CWSN is a special network which has many constraints compared to a traditional wireless network and many different features compared to a traditional wireless sensor network. While security challenges have been widely tackled in traditional networks, this is a novel area in CWSNs. This article discusses a wide variety of attacks on CWSNs, their taxonomy and different security measures available to handle the attacks. Also, future challenges to be faced are proposed.

Keywords: cognitive, security, wireless sensor networks

1. Introduction

Global data traffic in telecommunications has an annual growth rate of over 50%. While the growth in traffic is stunning, both the rapid adoption of wireless technology over the globe and its penetration through all layers of society are even more amazing. Over the span of 20 years, wireless subscription has risen to 40% of the world population, and is expected to grow to 70% by 2015. Overall mobile data traffic is expected to grow to 6.3 exabytes per month by 2015, a 26-fold increase over 2010 [1]. Over the recent years, wireless and mobile communications have increasingly become popular with consumers.

In regards to wireless networks, one of the fastest growing sectors in recent years was undoubtedly that of wireless sensor networks (WSNs). WSN consists of spatially distributed autonomous sensors that monitor a wide range of ambient conditions and cooperate to share data across the network. WSNs are introduced increasingly into our daily lives. Potential fields of applications can be found, ranging from the military to home control through commercial or industrial, to name a few. The emergence of new wireless technologies such as Zigbee and IEEE 802.15.4 has allowed for the development of interoperability of commercial products, which is important for ensuring scalability and low cost.

Most WSN solutions operate in unlicensed frequency bands. In general, they use ISM bands, like, the worldwide available 2.4 GHz band. This band is also used by a large number of popular wireless applications, for example, those that work over Wi-Fi or Bluetooth. For this reason, the unlicensed spectrum bands are becoming overcrowded with the increasing use of WSN-based systems. As a result, coexistence issues in unlicensed bands have been subject of extensive research [2,3], and in particular, it has been shown that IEEE 802.11 networks [4] can significantly degrade the performance of Zigbee/802.15.4 networks when operating in overlapping frequency bands [3].

The increasing demand for wireless communication presents an efficient spectrum utilization challenge. To address this challenge, cognitive radio (CR) has emerged as the key technology, which enables opportunistic access to the spectrum. 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 [5].

The main different between traditional WSN and new cognitive wireless sensor network (CWSN) paradigm is that 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

* Correspondence: araujo@die.upm.es
Electronic Engineering Department, Universidad Politécnica de Madrid, Avda/Complutense 30, 28040 Madrid, Spain

(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.

However, the cognitive technology will not only provide access to new spectrum but also provides better propagation characteristics. By adaptively changing system parameters like modulation schemes, transmit power, carrier frequency and constellation size, a wide variety of data rates can be achieved. This will certainly improve power consumption, network life and reliability in a WSN. Adding cognition to a WSN provides many advantages.

This way, CWSN is a new concept proposed in literature [6] 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.

Despite the research interest in CWSN, security aspects have not yet been fully explored even though security will likely play a key role in the long-term commercial viability of the technology. The security paradigms are often inherited from WSN and do not fit with the specifications of CR networks. Looking at the literature related to CR, security researchers have seen that CR has special characteristics. This make CR security an interesting research field, since more chances are given to attackers by CR technology compared to general wireless networks. However, at present there are no specific secure protocols which integrate WSN and CR needs.

At this, still immature, point of CR, it is important to understand some fundamental issues such as potential threats, potential attacks and the consequences of these attacks.

As [7] says, the CR nature of the system introduces an entire new suite of threats and tactics that are not easily mitigated. The three main characteristics of CR are environment awareness, learning and acting capacity. At first, these characteristics should be an advantage against attacks but they can become in weaknesses. For example, CR nodes collaborate to make better decisions but these communications are ways to propagate the attack in the network.

Considering these characteristics since the attacker point of view, the fundamental differences between a traditional WSN and the CWSN network are

- The potential far reach and long-lasting nature of an attack.
- The ability to have a profound effect on network performance and behaviour through simple spectral manipulation.

The information sensed in a CRN is used to construct a perceived environment that will impact in a certain way in current and future behaviour s of all the nodes in the network. The induction of an incorrectly perceived environment will cause the wrong adaptation of the CRN, which could affect short-term behaviour but also because of their ability to learn, it will propagate the error to the new decisions. Thus, the malicious attacker has the opportunity for long-term impact on behaviour. Furthermore, CR collaborates with its fellow radios sharing information. Consequently, this provides an opportunity to propagate behaviour through the different networks.

Threats associated with each CRN features can be detected [7], such as

- Maintains awareness of surrounding environment and internal state. It could be an opportunity for spoofing that will send malicious data to the environment to provoke an erroneously perception.
- Adapts to its environment to meet requirements and goals. It is an opportunity to force desired changes in behaviour in the victim.
- Reasons on observations to adjust adaptation goals. It could be an opportunity to influence fundamental behaviour of CRN.
- Learns from previous experiences to recognize conditions and enables faster reaction times. This could an opportunity to affect long-lasting impact on CR behaviour.
- Anticipates events in support of future decisions. It could be an opportunity for long-lasting impact due to an erroneous prediction.
- Collaborates with other devices to make decisions based on collective observations and knowledge. This is an opportunity to propagate an attack through network.
- Wireless communication. Data might be eavesdropped and altered without notice; and the channel might be jammed and overused by adversary. Access control, confidentiality, authentication and integrity must be guaranteed.

On the other hand, CRN features also help to mitigate malicious manipulation using:

- The ability to collaborate for authentication of local observations that are used to form perceived environments.
- The ability to learn from previous attacks.
- The ability to anticipate behaviours to prevent attacks.
- The ability to perform self-behaviour analysis.

Despite the extensive volume of research results on WSN [8], the considerable amount of ongoing research efforts on CR networks [9], and the new interest in CWSN [10], security in CWSN is vastly unexplored field. This is a new paradigm that offers many research opportunities.

The organization of this article is as follows. In Section 2, works in security are reviewed. In Section 3, a new taxonomy of attacks is proposed. In Section 4, countermeasures for CWSN attacks are analysed. Challenges and open works are shown in Section 5. Conclusions are offered in Section 6.

2. 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 [11]. 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 [12] 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 [13], two specific attacks against cognitive networks are analysed: primary user emulation (PUE), and sensing data falsification. It also provides some countermeasures well adapted to static scenarios such as TV system. In [14], 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 [15] 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 [16] for the first time in 2006. Since then, research of the same authors [17] 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 or jamming attack. These attacks have special characteristics in cognitive networks, for example, article [19] studies these features for DoS, and [20] shows a countermeasure based on frequency hopping (technically possible in CR) to avoid jamming attacks.

Although previous articles help to understand the importance of securing CRNs [21-23] they do not take into account the specific characteristics of WSN.

On the other side, there are several articles related with security in WSNs, a topic very studied [8,24-27], but without using cognitive capabilities.

Summarizing the state of the art, there is still much to investigate in the area of security for CWSNs, because nowadays there is not any work focus on this topic.

3. Taxonomy of attacks in CWSNs

As we shown in Section 1, CWSNs have special features that make security really interesting. However, security in CWSNs needs to be more studied by scientific community.

In this section, a complete taxonomy of attacks for CWSNs is shown. We are going to compare the differences in the scope between these attacks in a traditional WSN and in a cognitive one.

A taxonomy of attacks on CWSNs is very useful to design optimistic security mechanisms. There are several taxonomies of attacks on wireless networks [10] and focus on WSNs [6]. Moreover, some classifications of attacks in CR exist [3,9,11]. However, there is not a deep classification of attacks in CWSNs and study of attacks against cognitive WSNs does not exist.

We have analysed special network features that make CWSNs better against attacks: high transmission range, lower energy consumption, low delays and reliability of data. Their security is obviously endangered by the medium used, radio waves, but also by specific vulnerabilities of CWSNs like battery life or low computational resources.

Considering theses features, we propose a taxonomy which contains various attacks with different purposes, behaviours and targets. This will help researchers to better understand the principles of attacks in CWSNs, and further design more optimistic countermeasures for sensor networks. Figure 1 shows an outline of this CWSN taxonomy of attacks. CWSN attacks are divided into communications, against privacy, node-targeted, power consumption, policy and cryptographic attacks.

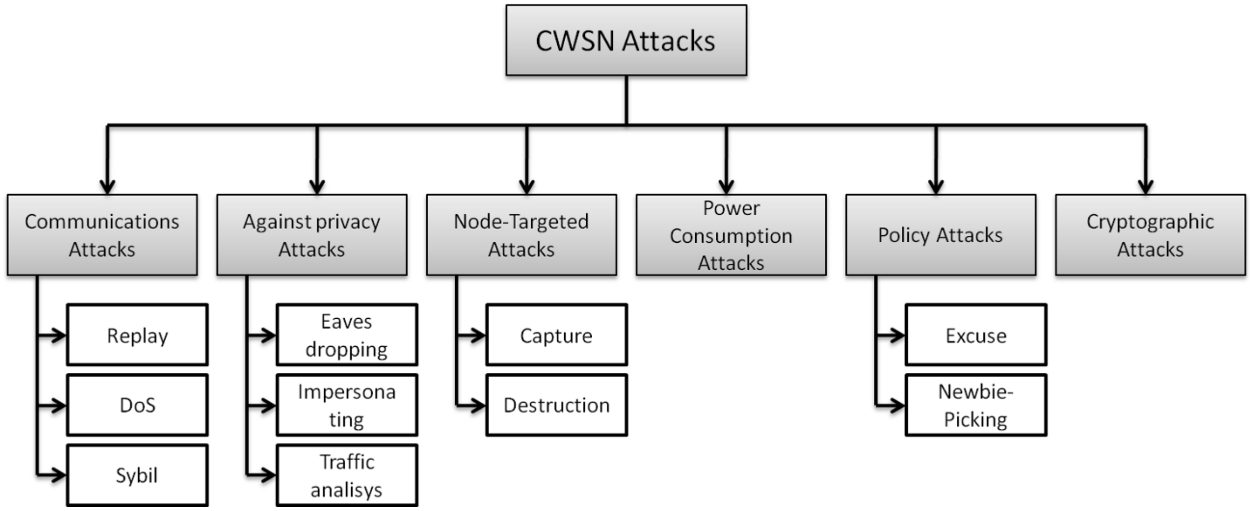

Figure 1 Taxonomy of attacks.

3.1. Communication attacks

First group is communication attacks. In this kind 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 behaviour of whole network.

Communication attacks can be classified into three different types according to the attack behaviour: replay attack, DoS attack and Sybil attack. Replay attack [28] consists on the replay of messages from inside or outside the current run of communication. 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.). CWSN could be affected in more degree that a regular WSN because nodes share information about the environment. If a node receives wrong information and also repeated, network behaviour could be affected deeply. If the PU packets are repeated, SU could have a wrong perspective of the spectrum too, avoiding the communications in frequencies or protocols used by the attacker.

DoS attack is characterized by an explicit attempt to present the legitimate use of a service. In this case, services are the spectrum or a special node. Different kinds of DoS attacks are

- Jamming attack, 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 [29]. 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.
- Collision attack [30] consist of the intention of violate the communication protocol. 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. For example, the secondary users (SUs) have to share the spectrum. Therefore, the use of this type of attack is very efficient in order to disrupt the SU communication. Nodes, detecting collisions, will relay the information, making communication very difficult.
- 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.
- In flooding attack, a malicious node sends many connection request to a susceptible node, rendering the node or the resource useless. For instance, a joint network request to the coordinator node.

Sybil attack is defined as a malicious device illegitimately taking multiple identities. Sybil attack is effective against routing algorithms, voting, reputation systems and foiling misbehaviour detection. For instance, Sybil attack might utilize multiple identities to generate additional reputation to malicious nodes or to change the sensing spectrum information. The most studied attack against CR is the PUE.

3.2. Against privacy attacks

The other 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 [31] 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.

3.3. 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 [32,33] 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 co-operational behaviour 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.

3.4. Power consumption attacks

Battery life in WSN is a crucial factor. Small size of nodes and batteries makes CWSN very vulnerable to power consumption attacks. The attacker can inflict sleep 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.

3.5. Policy attacks

The security and privacy policies are imperative since the policy basically influences the setup principles of a CWSN. Policy attacks can be classified as:

- Excuse attack, if the network policy is overly generous to recovering nodes that recently crashed or damaged by no requiring them to prove there are maintaining their quota, a malicious node may exploit this attack by repeatedly claiming to have been crashed/damaged. In this way, for instance, wrong spectrum information can be sent to the network very often to change the communications.
- Newbie-picking attack, if a CWSN requires that new nodes pay their dues by requiring them to give information to the net for some period of the time before they can consume any shared resource, therefore a veteran node could move from one newbie node to another, leeching their information without being required to give any information back.

3.6. Cryptographic attacks

Concluding the taxonomy, the cryptographic attacks try to find the weaknesses in system analysing the information transmitted. Several cryptographic attacks exist but their objectives are the same: to acquire the cryptographic key, to identify weakness in the algorithms or in the node software. CWSN nodes do not have enough resources to implement a powerful cryptographic code and they are vulnerable to these attacks.

Apart from the above listed attacks that may hinder the key management of CWSNs, the following actions will also danger the key management within CWSNs: brute forces, dictionary attack and monitoring attack. One example of this kind of attack is Differential Power Analysis (DPA) attack. The DPA attack can be used to target an unsuspecting victim either by using special equipment that measures electromagnetic signals emitted by chips inside the device or by attaching a sensor to the device's power supply.

4. Countermeasures in CWSN

According to Section 3 is very clear that CWSN face a dangerous problem in security. Several attacks could be adapted from WSN to the new paradigm of cognitive networks. In the last 10 years, some researches related with security on CRN have appeared. They related specific attacks against these networks but a few countermeasures are proposed. In this section, we show three different groups of countermeasures according to the specific characteristics of CWSN.

4.1. Based on geolocation

CR has it's origin in United States where an important problem with the spectrum occupancy becomes real. The main reason is that the access to the radio spectrum is ruled by a restrictive regulatory regime that emerged when the Radio Act of 1927 declared the "ether" to be a publicly owned resource. The goal of CR was to use the radio spectrum when base stations did not transmit.

According to that, first real and simulated scenarios were static, with base stations making the role of PU and different devices like SU. If an attacker tries to emulate a PU the geolocation is an efficient method [18,34]. For example, in [34] the authors assume that the attacker is close to the victim and the real PU is much far from the SU and the attacker. Moreover, the position of each node, including the attacker, is fixed. Assuming that, SU can learn about the characteristics of the spectrum according to the received power.

Geolocation countermeasure does not work for most of cases in CWSN scenarios, almost with the same approach that previous mentioned papers. In a regular WSN, nodes can change their location, even attackers can change it. In fact, attackers have in the movement a great advantage to not be detected.

Another disadvantage of node mobility related to security is that if we would like to monitor PU we need to sense continuously the spectrum to detect new locations. The continuous sensing reduces node batteries. Moreover, if the PU could be in any spatial point, its location is irrelevant for security. For example, a mobile phone with Wi-Fi could be a PU and this device could stay in any location. Others parameters should be observed to differentiate between PU and an attacker.

To conclude, if we want to use a countermeasure based on geolocation, some restriction should be defined. For example, restricted areas for attackers or fixed number of PU in the scenario.

4.2. Based on behaviour

In the same way that geolocation countermeasures, defences based on behaviour tries to modelling the PU [35]. The model is used to look for differences between a PU and attackers.

For example, in [17] authors use some radio parameters to decide if the transmitter is an incumbent transmitter or an attacker. These parameters are: signal characteristics, transmitted power and location. For a typical TV scenario on CR the PU model could be very precise. However as in geolocation countermeasures, the previous studies do not work for CWSN. Unfortunately it does not exist any model for PU in CWSN yet. PU usually are more unpredictable that in previous scenarios.

However, if we focus our CWSN in limited scenarios, for example intelligence ambient in a home or a building, the PU is defined specifically. Parameters like power transmission, time occupancy of spectrum and frequency used could be detected.

Genetic or Self-Organizing Maps algorithms could be used to detect the PUs behaviour and to difference them against attackers. These algorithms can detect patterns and behaviour changes, so they are a good solution for this problem. However, computational cost and batteries life should be taking in account.

4.3. Based on reputation and trust of the CR nodes

Two different groups of countermeasures related with the location and behaviour are proposed. Third group is a complement for the previous solutions that could improve the detection of attacks.

Reputation systems are very common in WSN [36]. Reputation takes advantage from the own characteristics of WSN: redundancy and adaptation. Usually several sensors form the networks and information is replied. Redundancy can be used to detect and isolate faulty or compromised nodes.

In CWSN where information is essential for the cognitive behaviour and sharing information is almost compulsory, reputation system can describe if the primary and SUs act like we expect. The big amount of information supplies the reputation system adjusting the reputation and trust of any node.

The best advantage of reputation systems is their versatility. The countermeasures could be implemented in any device, even small sensors with low resources, and could be used, in combination with others attacks, against most of attacks of Section 3.

5. Challenges and open problems

The nature of large, dynamic, adaptive, cognitive WSNs presents significant challenges in designing security schemes. A cognitive WSN is a special network which has many constraints compared to a traditional wireless network and many different features compared with a traditional WSN. While security challenges have been widely tackled in traditional networks, is a novel area in CWSN. In this section, most important challenges are discussed.

The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Cognitive features allow a dynamic reconfiguration to avoid these attacks. However, malicious nodes can use the dynamic reconfiguration to create new attacks such us PUE. CWSNs have to adapt traditional wireless problems to cognitive networks and provide solutions to new problems.

The dynamic nature of sensor networks means no structure can be statically defined. Cognitive approach includes new dynamic issues: communication protocol, modulation, frequency, sensibility or emitted power. The attacker can use these powerful characteristics to affect the data transmissions between nodes with a concrete purpose. The goal could be from isolate a node to try to change the behaviour of entire network. Security schemes must be able to operate within this dynamic environment.

The next challenging factor is the hostile environment in which cognitive sensor nodes function. Nodes face the possibility of destruction or capture by attackers. Since nodes may be in a hostile environment, attackers can easily gain physical access to the devices. Attackers may capture a node, physically disassemble it, and extract from it valuable information (e.g. cryptographic keys). Because of the capacity of change the communication protocol, a capture node can affect to the whole network. For example, a malicious node can order to the network use a specific modulation or cryptographic algorithm and capture all the data. Also node can provide wrong information to the network causing a bad configuration. The ability to have a profound effect on network performance and behaviour through simple spectral manipulation is very dangerous. The highly hostile environment represents a serious challenge for security researchers.

The extreme resource limitations of CWSN devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity and memory. This is no trivial task. Energy is the most precious resource for these networks. Communication and cognitive algorithms are especially expensive in terms of power. Cognitive networks usually reduce power emission to save batteries. Attacker can isolate a node easily. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient.

The proposed scale of cognitive WSNs poses a significant challenge for security mechanisms. Cognitive networks are not only hundreds of sensors; they can also include different wireless interfaces and integrate a myriad of nodes in the same network. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks with different radio interfaces while maintaining high computation and communication efficiency.

One of the main goals of CWSNs is to allow a reliable communication. Certainly, unreliable communication is another threat to nodes security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. Even if the channel is reliable, the communication may still be unreliable. The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes to change the communication scheme.

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are two main cautions to unattended sensor nodes: exposure to physical attacks and managed remotely. Remote management of a sensor network makes it virtually impossible to detect physical tampering or DPA attack. Perhaps most importantly, the longer that a sensor is left unattended the more likely that an adversary has compromised the node.

CWSNs have a special feature for security mechanism: dynamic reconfiguration network scheme. Level security can adapts to a specific application, network topology, power and other constraints. Security level reconfiguration biased by different constraints has to be considered in order to improve network security.

6. Conclusions

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.

Acknowledgements

This study was funded by the Spanish Ministry of Science and Innovation, under Research Grant AMILCAR TEC2009-14595-C02-01, and the P8/08 within the National Plan for Scientific Research, Development and Technological Innovation 2008-2011.

Competing interests

The authors declare that they have no competing interests.

Received: 20 May 2011 Accepted: 15 February 2012
Published: 15 February 2012

References

1. Cisco Systems Inc, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015. (2011) White Paper
2. I Howitt, J Gutierrez, IEEE 802.15.4 low rate–wireless personal area network coexistence issues, in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 3. New Orleans, Louisiana, USA, pp. 1481–1486 (March 2003)
3. D Cavalcanti, R Schmitt, A Soomro, Achieving energy efficiency and QoS for low-rate applications with 802.11e, in *IEEE Wireless Communications and Networking Conference (WCNC)*, vol. 1. Hong Kong, pp. 2143–2148 (March 2007)
4. IEEE 802.11 Standard, Wireless LAN medium access control (MAC) and physical layer (PHY) specifications, (Reaff 2003) Edition (1999)
5. J Mitola, Cognitive radio: an integrated agent architecture for software defined RADIO, Ph.D. dissertation, (Royal Institute of Technology, Stockholm, Sweden, 2000)
6. D Cavalcanti, S Das, J Wang, K Challapali, Cognitive radio based wireless sensor networks, in *Proceedings of 17th International Conference on Computer Communications and Networks*, vol. 1. St. Thomas, U.S. Virgin Islands, pp. 1–6 (August 2008)
7. JL Burbank, Security in cognitive radio networks: the required evolution in approaches to wireless network security, in *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, (CrownCom)*, vol. 1. Singapore, pp. 1–7. 15-17 (May 2008)

8. D Xiaojiang, C Hsiao-Hwa, Security in wireless sensor networks. IEEE Wirel Commun. **15**(4), 60–66 (2008)
9. TC Clancy, N Goergen, Security in cognitive radio networks: threats and mitigation, in *3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, (CrownCom)*, vol. 1. Singapore, pp. 1–8 (May 2008)
10. AS Zahmati, S Hussain, X Fernando, A Grami, Cognitive wireless sensor networks: emerging topics and recent challenges, in *IEEE International Conference Science and Technology for Humanity (TIC-STH)*, vol. 1. Toronto, Canada, pp. 593–596 (September 2009)
11. X Zhang, C Li, The security in cognitive radio networks: a survey, in *Proceedings of the International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly (IWCMC)*, ACM, New York, NY **1**, pp. 309–313 (2009)
12. Y Zhang, G Xu, X Geng, Security threats in cognitive radio networks, in *Proceedings of the 10th IEEE international Conference on High Performance Computing and Communications (HPCC)*, vol. 1. Dalian, China, pp. 1036–1041 (September 2008)
13. C Ruiliang, P Jung-Min, YT Hou, JH Reed, Toward secure distributed spectrum sensing in cognitive radio networks. IEEE Commun Mag. **46**, 50–55 (2008)
14. G Jakimoski, KP Subbalakshmi, Towards secure spectrum decision, in *Proceedings of IEEE Intl. Conference on Communications. (ICC)*, vol. 1. Piscataway, NJ, USA, pp. 2759–2763 (June 2009)
15. T Zhao, Y Zhao, A new cooperative detection technique with malicious user suppression, in *Proceedings of IEEE Intl. Conference on Communications (ICC)*, vol. 1. Dresden, Germany, pp. 14–18 (June 2009)
16. R Chen, JM Park, Ensuring trustworthy spectrum sensing in cognitive radio networks, in *1st IEEE Workshop on Networking Technologies for Software Defined Radio Networks, (SDR)*, vol. 1. Orlando, Florida, USA, pp. 110–119 (September 2006)
17. R Chen, JM Park, JH Reed, Defense against primary user emulation attacks in cognitive radio networks. IEEE J Sel Areas Commun. **26**(1), 25–37 (2008)
18. Z Jin, S Anand, KP Subbalakshmi, Detecting primary user emulation attacks in dynamic spectrum access networks, in *IEEE International Conference on Communications, (ICC)*, vol. 1. Dresden, Germany, pp. 14–18 (June 2009)
19. TX Brown, A Sethi, Potential cognitive radio denial-of-service vulnerailities and protection countermeasures: a multi-dimensional analysis and assessment, in *2nd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, (CrownCom)*, vol. 1. Orlando, Florida, USA, pp. 456–464 (July 2007)
20. L Zhang, J Ren, T Li, Spectrally efficient anti-jamming system design using message-driven frequency hopping, in *IEEE International Conference on Communications (ICC)*, vol. 1. Dresden, Germany, pp. 1–5 (June 2009)
21. G Baldini, T Sturman, A Biswas, R Leschhorn, G Godor, M Street, Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead. IEEE Commun Surv Tutor. **99**, 1–25 (2011)
22. A Sethi, TX Brown, Hammer model threat assessment of cognitive radio denial of service attacks, in *3rd IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks, (DySPAN)*, vol. 1. Chicago, USA, pp. 1–12 (October 2008)
23. S Arkoulis, L Kazatzopoulos, C Delakouridis, GF Marias, Cognitive spectrum and its security issues, in *Proceedings of The Second International Conference on Next Generation Mobile Applications, Services, and Technologies (NGMAST)*, vol. 1. Cardiff, Wales, UK, pp. 565–570 (September 2008)
24. P Walters, Z Liang, W Shi, V Chaudhary, Wireless sensor network security: a survey, (Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press, New York, USA, 2006)
25. W Yong, G Attebury, B Ramamurthy, A survey of security issues in wireless sensor networks. IEEE Commun Surv Tutor. **8**(2), 2–23 (2006)
26. Y Zhou, Y Fang, Y Zhang, Securing wireless sensor networks: a survey. IEEE Commun Surv Tutor. **10**(3), 6–28 (2008)
27. D Martins, H Guyennet, Wireless sensor network attacks and security mechanisms: a short survey, in *13th International Conference on Network-Based Information Systems (NBiS)*, vol. 1. Takayama, Gifu, Japan, pp. 313–320 (September 2010)
28. DR Raymond, RC Marchany, SF Midkiff, Scalable, Cluster-Based Anti-Replay Protection for Wireless Sensor Networks, in *IEEE Information Assurance and Security Workshop (IAW)*, vol. 1. West Point, NY, USA, pp. 127–134 (June 2007)
29. H Sun, S Hsu, C Chen, Mobile jamming attack and its countermeasure in wireless sensor networks, in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW)*, vol. 1. Washington, DC, USA, pp. 457–462 (May 2007)
30. P Reindl, K Nygard, D Xiaojiang, Defending malicious collision attacks in wireless sensor networks, in *IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC)*, pp. 771–776 (2010)
31. X Luo, X Ji, MS Park, Location privacy against traffic analysis attacks in wireless sensor networks, in *International Conference on Information Science and Applications (ICISA)*, vol. 1. Seoul, Korea, pp. 1–6 (April 2010)
32. T Bonaci, L Bushnell, R Poovendran, Node capture attacks in wireless sensor networks: a system theoretic approach, in *49th IEEE Conference on Decision and Control (CDC)*, vol. 1. Atlanta, Georgia, USA, pp. 6765–6772 (December 2010)
33. P Tague, R Poovendran, Modeling node capture attacks in wireless sensor networks. in *46th Annual Allerton Conference on Communication, Control, and Computing* 1221–1224 (2008)
34. Z Chen, T Cooklev, C Chen, C Pomalaza-Raez, Modeling primary user emulation attacks and defenses in cognitive radio networks, in *IEEE 28th International Performance Computing and Communications Conference (IPCCC)*, vol. 1. Phoenix, Arizona, USA, pp. 208–215 (December 2009)
35. TW Wu, YE Lin, HY Hsieh, Modeling and comparison of primary user detection techniques in cognitive radio networks, in *IEEE Global Telecommunications Conference (GLOBECOM)*, vol. 1. New Orleans, LA, USA, pp. 1–5 (December 2008)
36. S Ganeriwal, MB Srivastava, Reputation-based framework for high integrity sensor networks, in *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (SASN)*, vol. 1. ACM, New York, NY, pp. 66–77 (2004)

doi:10.1186/1687-1499-2012-48
Cite this article as: Araujo *et al.*: Security in cognitive wireless sensor networks. Challenges and open problems. *EURASIP Journal on Wireless Communications and Networking* 2012 **2012**:48.