Cognitive Sensor Techniques to Face Security Challenges in CWSN

Isra Sitan Mohammed Al-Qasrawi

Department of Information Technology, AL-BALQA APPLIED UNIVERSITY, AL-Huson University College, Irbid, Jordan

Abstract

Cognitive radio has emerged as the key technology to address efficient spectrum utilization challenge according to the increasing demand for wireless communication. Cognitive Wireless Sensor Networks (CWSNs) are introduced to use Dynamic spectrum access (DSA) to effectively face coexistence issues in overcrowded environments. Features existed in CWSNs make security really interesting and needs to be well-studied. In this paper, we introduce the main security challenges of CWSN and propose a new cognitive sensor system paradigm with many techniques which proved their efficiency separately to face the key challenges and threats on CWSN, especially the security aspects.

Keywords: *Cognitive Radio, Wireless Sensor Network, Efficient Spectrum Utilization, Primary User Emulation, Random Key Pre-distribution.*

1. Introduction

Over the recent years, wireless communications have become very popular with consumers all around the world. In addition, both the rapid adoption of wireless technology and its threats - that will not be easily mitigated- are amazing too. Overall mobile data traffic is expected to grow to 6.3 exabytes per month by 2015, a 26-fold increase over 2010 [1].

The development in wireless networks is very staggering, and one of most motivated wireless networks is wireless sensor networks (WSNs) which are used in many industrial and consumer applications, such as industrial process monitoring and control. A WSN usually consists of tens to thousands of nodes that communicate through wireless channels for information sharing and cooperative processing. 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 [2]. There are huge variations in usage of licensed frequency bands ranging from 15% to 85% in bands below 3 GHz. at the same time, the unlicensed spectrum bands are becoming overcrowded so that the problem of coexistence of heterogeneous systems is becoming increasingly important.

This led to emergence of an important and significant challenge which is the efficient utilization of the radio spectrum. To efficiently utilize spectrum there are two primary goals: first, in licensed bands, achieve reliable and trusted communication by using adaptive communications without affecting licensed users. Secondly, in unlicensed bands, provide efficient coexistence with heterogeneous environments. Attention is turned toward cognitive radio (CR) as the key technology to achieve these goals.

Cognitive radio systems offer the opportunity to improve spectrum utilization by detecting unoccupied spectrum bands and adapting the transmission or reception to those bands while avoiding the interference to high priority users. CR is aware of its surrounding environment, tracks changes and reacts upon what it found. Based on that, nodes in cognitive wireless sensor network (CWSN) change their transmission parameters according to the radio environment, to communicate efficiently, and coexist well with others. This is the main difference between WSN and new CWSN.

The capabilities of cognitive radio will provide many benefits to the existing WSNs, such as: improving reliability, power consumption, and network life. WSN is one of the most networks with the increasing demand for cognitive networking. This way, CWSN is a new concept proposed in literature [3] 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.

As [4] says, a WSN comprised of sensor nodes equipped with cognitive radio may benefit from the potential advantages of the salient features of dynamic spectrum access such as:

- Opportunistic channel usage for bursty traffic
- Dynamic spectrum access (DSA)
- Using adaptability to reduce power consumption
- Overlaid deployment of multiple concurrent WSN
- Access to multiple channels to conform to different spectrum regulations

CWSN is still vastly unexplored field despite the extensive volume of research results on WSN [5] and cognitive radio networks [6]. In this paper, we introduce the main challenges and principles of CWSN and propose some mechanisms which proved their efficiency separately to be gained together in a specific CWSN to face the key challenges and threats on CWSN, especially the security aspects.

The remainder of the paper is organized as follows. In Section 2, previous works on CWSN challenges are reviewed. In section 3, the main security challenges in CWSNs are introduced. A new cognitive sensor system is proposed in section 4. In section 5, analysis of a proposed system is discussed; conclusions are offered in section 6.

2. Related works

Relatively, a number very limited of works was done in the sector of cognitive wireless sensors networks. Most of them concentrate upon one side of CWSN challenges. Some of them try to introduce the attacks which threaten CWSN. Just handful research works presented integrated mechanisms to face most challenges.

In [7], an energy-efficient and adaptive modulation technique is introduced for CWSN in order to achieve high power efficiency to maximize the lifetime of sensor networks. Previous works about security in CR presented to analyze the effects emerged by cognitive features and how they could be used to reduce the negative effects. In the article [8] each characteristic of CR - the three main characteristics are: environment awareness, learning and acting capacity - and the attacks that could take advantage of it are analyzed. [9] Provides threats that affect the ability to learn of cognitive networks and the dynamic spectrum access. The article [10], present a new secure spectrum sensing protocol, it bases its functionality on the generation and transmission of specific keys to each node. Jamming attacks have special characteristics in cognitive networks, article [11] shows a countermeasure based on frequency hopping to avoid this kind of attacks. The definition of the primary user emulation (PUE) attacks was introduced by Chen and Park in [12], and they focused in [13] on countermeasures against PUE. Securing CR networks is well-introduced in many articles such as [14, 15] without taking into account the special characteristics of WSN. Also, much more articles discuss security in WSNs [16, 17, and 18] but do not use cognitive capabilities. In these days, very little works focus on security in CWSN. For this reason, we have to concentrate more in this topic.

3. Security challenges in CWSN

In this section, security challenges of CWSN will be shown. First of all, the difference between WSN node and CWSN node must be illustrated to understand the additional threats which face CWSN.

CWSN node structure is composed of: sensing unit, processor unit, memory unit, power unit, and cognitive radio transceiver unit as shown in Fig. 1 [4]. The main difference between the structure of classical sensor nodes [5] and CWSN nodes is the cognitive radio transceiver of CWSN nodes.

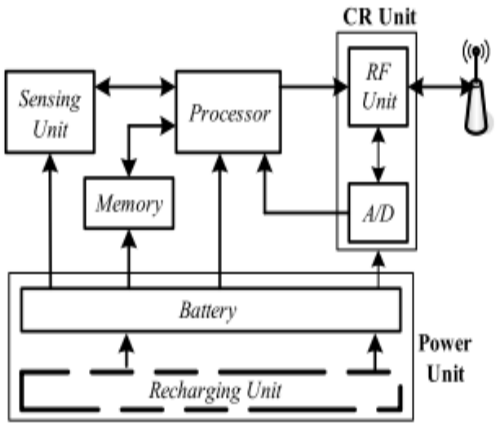

Fig.1 Hardware structure of a cognitive radio sensor node.

As we mentioned above in section 1, cognitive radio unit enables the nodes to dynamically adapt their transmission parameters according to the radio environment such as modulation, and carrier frequency. CWSN nodes also inherit the limitations of traditional WSN nodes including power, processing and memory resources limitations.

These limitations will impact on the cognitive radio characteristics too.

Most of security challenges which face CWSN caused by CR features. CR network constructs its environment depending on sensed information, which will change the nodes behavior. As we said previously one of the main characteristics of CR is the ability of learning, for that reason, having a wrong perceived environment will propagate the error to the new decisions. As a result, the malicious attacker will get the opportunity for long-term impact on behavior. Add to that the behavior itself will be propagated through the different networks.

As [8] illustrates, threats associated with CR network features can be detected. For example, it is a big opportunity to change the behavior depending on the feature of adaptation to its environment to meet requirements and goals. Another example is a potential opportunity for long-lasting impact due to an erroneous prediction, depending on the feature of anticipating events in support of future decisions. A reliable CR network must guarantee authentication, access control, and data integrity to face these threats. These features are existed in CWSNs as well with other special features that make security really interesting and needs to be well-studied. There is not a deep study of security in CWSNs, but some classifications of attacks in CR exist [19]. We will provide the security challenges with potential attacks on CWSNs and propose some mechanisms to face them.

Data reliability, lower energy consumption, and low delays will make CWSNs even better against attacks. In the other hand, low computation power, battery life and other nodes resources' constrains will endanger security of CWSNs. The new proposed cognitive sensor system must take into account the computation power and battery life of the nodes, as we will show later.

A kind of attacks that the attacker affects data transmissions between nodes is Sybil attack. Sybil attack is defined as [2] a malicious device illegitimately takes many identities. Sybil attack is proved its efficiency against routing algorithms, reputation systems and foiling misbehavior detection. For example, Sybil attack might utilize many identities to change the sensing spectrum information. If the network policy is very generous to re-maintain nodes that recently damaged by no requiring them to prove there are maintaining their quota, a malicious device may exploit this attack by claiming repeatedly to have been damaged. As a result, wrong spectrum information can be sent to the network to change the communications, knowing that CWSN could be affected more than a traditional WSN because nodes share information about the environment. This kind of attack called excuse attack.

CWSNs allow sharing resources to be aware of environment. Attackers could exploit this access to take some of node information. The attacker could easily discover the communication contents by eavesdropping. Also, the attacker can join to the network and impersonate the original victim sensor node to receive packets and access node's information, this called Impersonating attack.
The cryptographic attacks try to find the weaknesses in system analyzing the information transmitted [2]. The objectives of most cryptographic attacks are the same: to identify weakness in the algorithms or in the node software, and/or to acquire the cryptographic key. CWSN nodes do not have enough resources to implement powerful cryptographic algorithms.

Some kinds of attacks were meant to increase power consumption. The attacker can inflict sleep mode on a power constrained node by engaging in it unnecessary work to quickly drain its power and shorten its battery life time.

4. The Cognitive Sensor System

As we see, CWSN faces many dangerous threats in security. A lot of WSNs and CR networks attacks could be adapted to the CWSN. In this section, we propose a new cognitive sensor paradigm according to the specific characteristics of CWSN, with some mechanisms that separately proved efficacy in facing security attacks we discussed above in section 3.

First of all, Sybil attacks and excuse attacks each kind of them has different goals in attacking the network but a specific mechanism can be effective to face both of them. To defend against these attacks we should identify node's authentication. Some articles propose to use neighboring node relation to verify the node identities, and use schemes in which the node identities are verified simply by analyzing the neighboring node information of each node [20]. We should validate that each node identity is the only identity presented by the corresponding physical node. There are two ways to validate an identity: direct and indirect validation.

We propose to use Random Key Predistribution in our paradigm, In random key predistribution, a random set of keys or key-related information will be assigned to each

node, so that in the key set-up phase, each node can compute the common keys it shares with its neighbors; the common keys will be used as a shared secret session key to ensure node-to-node secrecy. The idea here is: to associate the node identity with the keys assigned to the node, and to help the network to verify part or all of the keys that an identity claims to have, rendering the attack more difficult. More Clarity of this technique will be shown in [21].

Secondly, to counter measurement against eavesdropping attacks we propose to use the jamming technique presented in [22] which use cognitive capabilities. This technique can operate independently of the higher layers to complete security demands. Cooperative jamming strategies are highly effective for increasing the secrecy in CWSNs.

The essential problem in WSN is the difficulty to obtain a full Channel State Information (CSI). Cognitive paradigm provides this information to the network by allowing the spectrum monitoring. CWSN avoid one of the main constraints to use jamming techniques, the knowledge of the CSI. In this technique the network composed of four terminals: a legitimate source node (S), a legitimate destination node (D), one or more relay nodes (R) and an eavesdropper node (E). All these nodes have cognitive capabilities and different radio interfaces. The inactive nodes in the relay network can be used as jamming sources to confuse the eavesdropper nodes and provide better security [22].

In this cooperative jamming technique any available jamming power will only be allocation to information transmitters, while D and S remain inactive. If the network detects eavesdropper node E, nodes can use the location information to increase jamming over the E node zone. Relay pool replay the message to the D and produce a jamming with the same communication features over the E node zone. Closer nodes to E node manage the jamming. As a result, E node cannot listen the transmitted information. This defines the "attacker location known" scenario. Additionally, two other scenarios "attacker location unknown, and attacker and relay co-located" are illustrated in [22].

Thirdly, to face cryptographic attacks, one of most efficient methods is the Elliptic curve cryptography (ECC). ECC is an approach to doing asymmetric cryptography. The critical feature of asymmetric cryptography is this key pair which provides the fact that one of the keys cannot be obtained from the other. By giving each sensor node public and private keys, we can ensure that the communication between the sensors will be very secret, and no one can view the message, or the forwarding nodes neither the attacker nodes. In section 5 we will analyze the reasons of choosing ECC.

Finally, all of these techniques mentioned above will slightly cause higher power consumption. And as we illustrated too, one of the attacks faces CWSN is power consumption attack. For that reason, we propose our cognitive sensor paradigm to be built according to a new energy efficient architecture in which spectrum sensing network is decoupled from data gathering network to increase network life time.

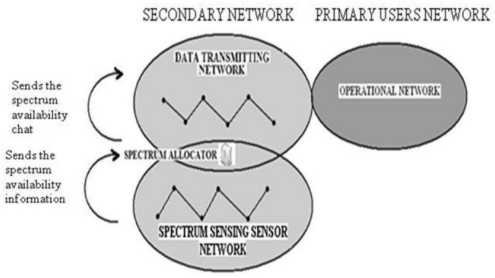

Fig.2 Proposed network architecture of cognitive sensor system.

This architecture is proposed and illustrated well in [23] where distributed to internal sub-networks. "Sensing sensor network" is the initial sensing network which consists of sensor nodes arranged in a particular manner to increase the life time of the network. "Data Transmitting/Data Gathering network" is the backbone network which responsible for data distribution to the "operational networks". This distinction will reduce the load on the sensors in the secondary network such as processing, analyzing and distributing the sensed data on the same front. This multitasking leads to battery drain and shortening network the life time. By distributing sub-networks, tasks have been divided and thus improve network spectrum efficiency. And by distinguishing the secondary network, the network life time will be increased as well. Sub-networks are shown in Fig. 2 [23].

The data transmitting network is associated with the operational network of unlicensed users. The sensors are placed in a grid paradigm for exploiting the characteristics of a sensor grid. The grid structure provides a seamless access to the network resources in a pervasive manner. One or more base stations collect the sensed spectrum data and forward it to the central head called spectrum allocator. In spectrum allocator the spectrum vacancy chart is dynamically formed based on the collected data and distributed to the operational networks in the secondary network. This forwarded

information shows the availability of the spectrum. And thus, unlicensed users (SU) will use it to avoid the licensed users (PU).

Embedding these techniques together will improve many features that make CWSNs better against attacks: lower power consumption, reliability of data, high transmission rate, and low delays.

5. Analysis of proposed cognitive sensor system

In section 4, we presented four techniques to be used together in our proposed system. Each one of them proved high efficacy to face specific attacks in CWSNs. For Random Key Predistribution technique, a randomly generated identity has only probability p of being usable. An adversary has to try 1/p times on average to obtain a usable Sybil identity, thus p has to be very small to make the sensor network immune to the Sybil attack.

Single-space pair wise key distribution, is intrinsically resistant to the Sybil attack as long as the attacker does not capture more nodes. Multi-space pair wise key distribution is superior to the single-space case in that the attacker has to compromise far more nodes. We can say that the multi-space pair wise approach to be the best among these approaches.

Random key predistribution is a promising method which associates a node's keys with its identity. It is easier to analyze than other methods of identity authentication because it relies on well understood cryptographic principles.

The security using jamming technique mentioned in section 4 was compared with current system metrics by defining secrecy rate and secrecy outage probability for this purpose. The secrecy rate is a reliable transmission rate on the main channel, which remains undecodable at the eavesdropper. The Secrecy Outage Probability (SOP) is a performance metric suitable for non-ergodic channels which describes the probability that a target secrecy rate is not achieved. The SOP characterizes the likelihood of simultaneously reliable and secure data transmission.

In order to simulate the attack and the counter measurements, a simulator has been developed over the well known Castalia simulator with cognitive features modifications. The simulation results show that the SOP decreases with a standard number of relay nodes in the network. Additionally, attacker location is not a problem for this kind of strategies. Cooperative jamming strategies with assistance from inactive neighboring nodes are seen to be highly effective for increasing the secrecy of the transmitted data [22].

Again, ECC is said to be one of the most efficient methods of cryptography. It is Asymmetric cryptography, which is a powerful and essential technology. The ability to widely distribute public keys and communicate securely over an open network is truly revolutionary.
ECC offers considerably greater security for a given key size. The smaller key size also makes possible much more compact implementations for a given level of security, which means faster cryptographic operations, running on smaller chips or more compact software. This means less heat production and less power consumption.

Its inverse operation gets harder, faster, against increasing key length than do the inverse operations in Diffie Hellman and RSA. This keeps ECC implementations smaller and more efficient than other implementations. ECC can use a considerably shorter key and offer the same level of security as other asymmetric algorithms using much larger ones. Moreover, the gulf between ECC and its competitors in terms of key size required for a given level of security becomes dramatically more pronounced, at higher levels of security [24]. Table 1 shows the differences between the public key sizes; we can conclude that ECC key is the shortest one.

Table 1: NIST Recommended Key Sizes

Symmetric Key Size (bits)	*RSA and Diffie-Hellman Key Size (bits)*	*Elliptic Curve Key Size (bits)*
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	521

This means, in turn, less heat, less power consumption, and software applications that run more rapidly and make lower memory demands such as what we need in CWSN.

6. Conclusions

In this paper, security challenges of CWSNs have been discussed and cognitive sensor system has been proposed; which is a new paradigm of CWSN with specific effective techniques formed by adopting cognitive radio capabilities in wireless sensor networks. We hope that this paper will

provide better understanding of the security challenges for CWSN and motivate research community to further explore this promising paradigm and make a deep studying to analyze its efficiency and suggest drawbacks or other attacks to avoid them.

References

[1] Cisco Systems Inc, Cisco Visual Networking Index: "Global Mobile Data Traffic Forecast Update", 2010-2015. (2011) White Paper

[2] Araujo et al., "Security in Cognitive Wireless Sensor Networks. Challenges and open problems", in EURASIP Journal on Wireless Communications and Networking 2012 (2012:48)

[3] 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, (August 2008) pp. 1–6

[4] B. Akan, B. Karli, O. Ergul, "Cognitive Radio Sensor Networks".

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazine, Vol. 40, No. 2, (Aug. 2002), pp. 102-114

[6] I. F. Akyildiz, W. Lee, M. C. Vuran, S. Mohanty, "NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: a Survey", Computer Networks Journal (Elsevier), Vol. 50, No. 13, (Sept. 2006), pp. 2127-2159

[7] S. Gao, L. Qian, D. R. Vaman and Q. Qu, "Energy Efficient Adaptive Modulation in Wireless Cognitive Radio SensorNetworks", in Proc.IEEE ICC 2007(June 2007), pp. 3980-3986

[8] 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, (May 2008), pp. 1–7. 15-17

[9] 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, (September 2008), pp. 1036–1041

[10] G Jakimoski, KP Subbalakshmi," Towards secure spectrum decision", in Proceedings of IEEE Intl. Conference on Communications. (ICC), vol. 1. Piscataway, NJ, USA, (June 2009), pp. 2759–2763

[11] 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, (June 2009), pp. 1–5

[12] 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, (September 2006), pp. 110–119

[13] R Chen, JM Park, JH Reed, "Defense against primary user emulation attacks in cognitive radio networks". IEEE J Sel Areas Commun. 26(1), (2008), pp.25–37

[14] 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, (2011), 1–25

[15] 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, (September 2008), pp. 565–570

[16] 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)

[17] Y Zhou, Y Fang, Y Zhang, "Securing wireless sensor networks: a survey". IEEE Commun Surv Tutor. 10(3), (2008), pp.6–28

[18] D Martins, H Guyennet, "Wireless sensor network attacks and security mechanisms: a short survey", in 13th International Conference on NetworkBased Information Systems (NBiS), vol. 1. Takayama, Gifu, Japan, (September 2010), pp. 313–320

[19] 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, (2009), pp. 309–313

[20] Ssu K.-F., Wang W.-T., Chang W.-C. "Detecting Sybil attacks in Wireless Sensor Networks using neighboring information", in Computer Networks, 53 (18), (2009), pp. 3042-3056

[21] Newsome J., E. Shi, D. Song, and A. Perrig," The Sybil Attack in Sensor Networks: Analysis and Defenses", Proc. IEEE Information Processing on Sensor Networks (IPSN), Berkeley, CA, (Apr. 2004)

[22] A Araujo, J Blesa, E Romero, O Nieto-Taladriz, "Cooperative jam Technique to Increase Physical-layer Security in CWSN", in Proceedings of the Second International Conference on Advances in Cognitive Radio (COCORA), 2012 .

[23] S Thaskani, "Energy Efficient Architecture and Protocols for Cognitive Radio based Sensor Networks", in Communication Research Center, International Institute of Information Technology Hyderabad - 500 032, INDIA (January 2011)

[24] Burton S. Kaliski, "A standard for RSA, Diffie-Hellman, and Elliptic Curve Cryptography", in IEEE P1363 Vol. 1189/1997, (1997), pp. 117-118

Author Isra Sitan Mohammed Al-Qasrawi received the B.S. degree in Computer Science from Al-Balqa' Applied University, Jordan in 2004, the MSc in Computer Science from Yarmouk University, Jordan in 2009, Working as instructor in Al-Balqa' Applied University / Al-Huson University College- Department of Information Technology.