A Security Solution Approach for Cognitive Wireless Sensor Networks

Murat DENER
Graduate School Of Natural And Applied Sciences
Gazi University
Ankara, 06500, Turkey
muratdener@gazi.edu.tr

***Abstract*--- In recent years, the resulting of "cognitive" concept, a new field called "Cognitive Wireless Sensor Networks" is gained to literature. The traditional Wireless Sensor networks are already complicated and complex security, adding cognitive turned into more complicated and more complex. The purpose of the paper to investigate security vulnerabilities in cognitive sensor networks, and propose methods of defense against these vulnerabilities to maximize the security of sensitive information circulating in a network.**

***Index Terms*— Cognitive Wireless Sensor Networks, Security**

I. INTRODUCTION

Recent advances in wireless communications and electronics have enabled the development of lowcost, low-power, multifunctional sensor nodes that are small in size and communicate untethered in short distances [1]. Wireless sensor networks (WSNs) consist of large populations of wirelessly connected nodes, capable of computation, communication, and sensing [2]. These nodes are randomly distributed to the observation environment, moreover they recognizes each other, and they can perform task of measuring in the a wide area [3]. Since they can work individually without additional maintenance and can be deployed in diverse applications such as military, healty, home security, detect of forest fires.

The WSN is facing a wide variety of security vulnerabilities due to the hardware limitations of the sensor nodes, wireless communication environment, real time processing needs, heterogenic structure, large number of nodes, need for measurability, mobility, the weight of the application environmental conditions as well as cost. Confidentiality which is the basic goal of security provides one of the most important obstacles to overcome in order to ensure the integrity and availability as well as the achievement of time-critical and vital goals [4]. When compared to the classical computer networks which are made up of personal or laptop computers that contain strong hardware and software nodes, the WSN displays many special characteristics [5]. These unique characteristics make many security problems that much harder to overcome. During sensitive WSN applications such as the surveillance of enemy or border lines, the security protocols which enable the sensors to transfer secret data to the base station must be used. However, the low processor and radio capacities of the sensors prevent traditional security protocols to be used in WSN applications [6]. Data confidentiality, integrity, freshness, identity verification and availability are considered as security requirements in the WSN [7,8].

The proliferation of wireless devices such as laptops, notebooks, cellular phones, smart phones, and tablets has caused the frequency spectrum used for transfer of information to become crowded [9].

So, the problem of spectrum shortage is occurred. Cognitive Radio (CR) is a novel technology that promises to solve the spectrum shortage problem by allowing secondary users to coexist with primary users without causing interference to their communication [10]. The resulting of "cognitive" concept, a new field called "Cognitive Wireless Sensor Networks" is gained to literature.

This way, CWSN is a new concept proposed in literature [11] 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.

Also a WSN comprised of sensor nodes equipped with cognitive radio may benefit from the potential advantages of the salient features of dynamic spectrum access [12] 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

However, the traditional Wireless Sensor networks are already complicated and complex security, adding cognitive turned into more complicated and more complex. In this paper, a security solution approach is presented for CWSNs. While Attacks and Defense Methods are given in Section 2, security solution is reported in Section 3.

II. ATTACKS AND DEFENSE METHODS

DOI : 01.IJNC.2014.1.12

Security and Privacy is extremely important in many Wireless Sensor Network applications. Some of these applications are target tracking and tracing systems used in the fields of war, law enforcement applications, automotive telemetry applications, monitoring offices-rooms, the temperature and pressure measurements in gas stations and forest fire detection systems. All of this applications has a large number of benefits and their development potential is high. However, if the sensor information is not maintained properly, the destruction of the information is likely to lead to false conclusions. Sensor Network works manifested in military applications as quickly as possible. The importance of security in this area are known to all. Information on the battle field, should be collected without risking someone's life. If Networks are no protect in this way, they can be used as a powerful weapon in the hands of the enemy. Robust security measures should be taken for this type of application. In commercial applications of sensor networks "Protection of privacy" issue is important as the network runs stable. Physiological or psychological information about people should be protected. Regardless of how widespread, and complex sensor network applications, these systems will increase the importance of protecting against unauthorized users. Because a wide range of sensor network applications are running under the physical conditions and restrictions. While Attacks and Defense Methods in WSNs is given in Table I, Attacks and Defense Methods in CWSNs is given in Table II [13].

TABLE I
Attacks and Defense Methods in WSNs

Layer	**Attacks**	**Security Mechanisms**
Physical	Jamming	Spread-spectrum, mode change
MAC	Collision	Error-correction code
	Exhaustion	Rate limitation
	Unfairness	Small frames
Network	Selective forwarding	Authentication
	Sybil	Authentication
	Wormhole	Authentication
	Hello Flood	Authentication
	Ack. Flooding	Authentication

TABLE II
Attacks and Defense Methods in CWSNs

Category	**Attacks**	**Security Mechanisms**
Attacks on Communication Protocols	Replay attack	Robust authentication scheme
	DoS attack	Frequency hopping in the cognitive control channel
	Malicious alteration of cognitive Messages	Data Integrity
	Sybil attack	Authentication
	Saturation of cognitive control channel	Robust system design
	Eavesdropping of cognitive radio messages	Data Confidentiality
	Disruption of MAC, network and cognitive engine	Data Integrity
Masquerading Attacks	Primary user emulation attack	Authentication
	Masquerading of a secondary CR node	
Unauthorized Access to Spectrum	Unauthorized use of spectrum band for selfish use by an attacker	A robust and secure framework to enforce spectrum policies
	Unauthorized use of spectrum band for DoS attack on primary users	
Power Exhaustion Attacks on Sensor Nodes	Frequent channel change request to drain energy	Robust authentication scheme

III. SECURITY SOLUTION

Security vulnerabilities for the WSN and CWSN are listed in Section 2. Security solution is divided into five stages considering layers and the formats of these attacks occurred. It is given that security mechanisms need to be developed for each group in this section.

A. First Stage

At this stage, the data confidentiality and data freshness will be provided.

1) Data confidentiality in WSN prevents access of unauthorized people to collected data which is one of the most important requirements in sensitive WSN applications. A sensor node should not relay the data obtained from the environment to its neighbors. Especially in military applications, the data collected on the nodes can be very sensitive. Moreover, in many applications, nodes have to transmit very sensitive data (key distribution for example) to other sensor nodes through wireless transmission environment. In addition, routing data should also be kept secret against malignant nodes as these nodes can make use of these data and decrease the performance of the network. Because of these issues, it is very crucial to construct a safe communication channel for data transmission in WSNs. The standard approach for maintaining data confidentiality is the encryption of the data with a secret key. Due to their low energy consumption, encryption algorithms based on secret key substructure are used in WSNs. These cryptographic algorithms (XXTEA, RC5, Skipjack, AES, SEA etc.)and modes (OCB, CBC) should be implemented on the sensor nodes in the developed security solution. The most efficient method should be used in terms of security and energy. During the coding of the system can be made positive contributions to the chosen algorithm. If this method is provided, the following attack / attacks will be prevented.

- Eavesdropping of cognitive radio messages

2) In WSN structures, sensors send measurement data about the environment they are presently in with specific time intervals and the delivery of the measurement times then matter. It is possible that copy of old measurement values are retransmitted by an attacker. Therefore, it is important to check that the data is new. Data freshness

can be maintained by adding a counter to the message packet or by using a random number during encryption. These methods should be implemented on the sensor nodes. The most efficient method should be selected in terms of security and energy.If this method is provided, the following attack / attacks will be prevented.

- Replay attack

B. Second Stage

Data confidentiality can prevent capturing of data by malicious nodes yet it cannot stop data from being changed by unauthorized people. Data integrity assures that the message will not be changed during communication. A malicious node can make the network work improperly by disrupting the message. What is more, without actual presence of a malicious node, the messages might get disrupted during transmission. Therefore, it is a must to use message authentication codes or cyclic codes for data integrity. These methods should be implemented on the sensor nodes. The most efficient method should be selected in terms of security and energy. During the coding of the system can be made positive contributions to the chosen method. If this method is provided, the following attack / attacks will be prevented.

- Malicious alteration of cognitive messages
-Disruption of MAC, network and cognitive engine

C. Third Stage

As WSNs use public wireless environment, they need authentication mechanisms to detect messages and deception packets coming from malicious nodes. Authentication mechanisms help a node with verifying the identity of a node it is in contact with. Without authentication, a malicious node can pretend to be a different node and might obtain some sensitive data and also prevent proper functioning of other nodes. If only two nodes are in contact, authentication can be accomplished by symmetric key cryptography. Transmitter and receiver can calculate the verification code of all the messages sent by a common hidden key. These methods should be implemented on the sensor nodes. The most efficient method should be selected in terms of security and energy.If this method is provided, the following attack / attacks will be prevented.

- Selective forwarding
- Sybil
- Wormhole
- Hello Flood
- Ack. Flooding
- Primary user emulation attack
- Masquerading of a secondary CR node

D. Fourth Stage

Availability refers to WSN's ability in maintaining its service continuity even during denial-of-service-DoS attacks. DoS type of attack is a method for hindering service. It is a type of attack that aims at making the target system incapable of harming any one and also consuming of all the sources of that system by regular or successive attacks. There is no takeover, capture or 'hacking' by technical terms. What is done is forcing of the victim system to use its sources and make system incapable of serving. DoS attacks can occur at any protocol layer of WSN and the selected victim might render the nodes inoperative. In addition to DoS attacks, excessive communication or computation load might finish the battery of the node quicker than expected. Not providing availability to WSN might lead to very serious consequences. For example, in a military based application, if a few of the nodes do not function properly, than the enemy alliances might leak in from these nonfunctional parts of WSN. To provide availability, it is necessary to develop a detection and defense unit. To ensure the data availability of a strong detection and defense unit should be developed. If this method is provided, the following attack / attacks will be prevented.

- Jamming
- Collision
- Exhaustion
- Unfairness
- Saturation of cognitive control channel
- Unauthorized use of spectrum band for DoS attack on primary users

E. Fifth Stage

Wireless Sensor Networks consists of small sensor nodes. These nodes by entering cooperation in a physical environment, carry informations into the virtual world what they have learned. The development of wireless communication technologies and due to high demand to wireless services of users, frequency scarcity problem emerged. Also, the increasing demand for spectrum in wireless communication has made efficient spectrum utilization a big challenge. To address this important requirement, cognitive radio has emerged as the key technology. Cognitive Wireless Sensor Networks have emerged addition to Wireless Sensor Networks. With cognitive approach, some attacks occur such as unauthorized use of spectrum band for selfish use by an attacker, frequent channel change request to drain energy. A strong and safe structure should be designed to access spectrum. During the design, some operations must be considered that providing efficient allocation of the spectrum and the spectrum monitoring operations. Process of spectrum management is strengthened with supervision and monitoring procedures. If this method is provided, the following attack / attacks will be prevented.

- Unauthorized use of spectrum band for selfish use by an attacker
- Frequent channel change request to drain energy

IV. CONCLUSION

Technological advances in wireless communication technologies, are likely to observe it would be a new landmark. With the spread of wireless communication has emerged the necessity of using the spectrum efficiently. Some frequency bands are used by many applications spectrum is underutilized. Therefore, to prevent intensive and inefficient use of spectrum, Dynamic Spectrum Access concept has been developed that allows the use of spectrum. In this way, the wireless technology that uses different methods will work together more efficiently.

The aim is through software changes instead of hardware differences, devices will be used more efficiently. This point of view was emerged to Cognitive Wireless Sensor Networks. Primarily Cognitive Wireless Sensor Networks security vulnerabilities will be grouped and categorized. Then, the appropriate security solution developed in each category. This paper will be helpful for security workers in CWSNs. Also, we will implement to sensors our security solution in our future work.

REFERENCES

[1] Akyıldız, I.F., Su, W., Sankarasubramaniam, Y., Çayırcı, E., "A survey on sensor networks", IEEE Communications Magazine, 40(8), 102-114, 2002.

[2] Elson,J., Römer, K., "Wireless sensor networks: a new regime for time synchronization", ACM SIGCOMM Computer Communication Review, Volume 33 Issue 1 Pages 149 - 154, January 2003.

[3] Dener, M., Bay, Ö.F., "Medium Access Control Protocols For Wireless Sensor Networks: Literature Survey", Gazi University Journal of Science, 25(2):455-464, 2012.

[4] Chong, C-Y., Kumar, S.P., “Sensor Networks: Evolution, opportunities, and challenges”, Proc IEEE, Vol 91, No 8, 1247-1256, 2003.

[5] Yong Wang, Garhan Attebury, And Byrav Ramamurthy, “A Survey Of Security Issues In Wireless Sensor Networks”, IEEE Communications Surveys & Tutorials, Volume 8, No. 2, 2nd Quarter, 2006.

[6] Cam, H., Ozdemir, S., Nair, P., Muthuavinashiappan, D., Sanli, H.O., “Energy-Efficient and secure pattern based data aggregation for wireless sensor Networks”, Special Issue of Computer Communications on Sensor Networks, 446-455, 2006.

[7] Hiren Kumar Deva Sarma, Avijit Kar, “Security Threats in Wireless Sensor Networks”, IEEE, 2006.

[8] Raymond D.R. Midkiff.S.F, “Denial of Service in Wireless Sensor Network: Attacks and Defenses”, IEEE Pervasive Computing, Vol:7, Issue 1, PP: 74 – 81, 2008.

[9] Sarah Purewal. Wireless devices out number us population, survey says, October 2011.

[10] El-Hajj, W., Safa, H., Guizani, M., "Survey of Security Issues in Cognitive Radio Networks", Journal of Internet Technology, Vol. 12 No. 2, P.181-198, 2011.

[11] D Cavalcanti, S Das, J Wang, K Challapali, Cognitive radio based wireless sensor networks.Proceedings of 17th International Conference on Computer Communications and Networks, 1, pp. 1–6, 2008.

[12] O. B. Akan, O. B. Karli, O. Ergul, "Cognitive Radio Sensor Networks," IEEE Network, vol. 23, no.4, pp. 34-40, July 2009.

[13] Jaydip Sen, “Security and Privacy Challenges in Cognitive Wireless Sensor Networks”, Book Chapter in Cognitive Radio Technology Applications for Wireless and Mobile Ad hoc Networks, Natarajan Meghanathan and Y. B. Reddy (Eds.), IGI-Global, USA. Published in July 2013.

Murat DENER received her M.Sc. and Ph.D. degrees in Electronic and Computer Education Department from Gazi University, Turkey, in 2008 and 2012, respectively. His doctorate thesis entitled by Design and Implementation of a Secure Data Link Layer Protocol for Wireless Sensor Networks. He worked in Georgia Tech E-Stadium Team in 2011. From 2005 to 2012, he was a Research Assistant in the Graduate School of Natural and Applied Sciences. Since 2012, he is Doctor in Gazi University. His research interest includes the Next-Generation Wireless Networks, Wireless Ad Hoc and Sensor Networks, Cognitive Radio Networks.

DOI : 01.IJNC.2014.1.12