Cooperative jam Technique to Increase Physical-layer Security in CWSN

Alvaro Araujo, Javier Blesa, Elena Romero, Octavio Nieto-Taladriz
E.T.S.I. Telecomunicacion
Electronic Engineering Department
Universidad Politecnica de Madrid
Madrid, Spain
{araujo,jblesa,elena,nieto}@die.upm.es

***Abstract*— This paper considers the problem of secure communication in Wireless Sensor Networks in the presence of non-colluding passive eavesdroppers. Cognitive networks capabilities such as spectrum sensing, share information and collaboration to optimize the communications can be used to avoid attacks. A collaborative jamming technique is proposed to increase Cognitive Wireless Sensor Networks security and a counter measurement against eavesdropped attacks. Three types of scenarios are defined: attacker location known, attacker location unknown, and attacker and relay co-location. Each new scenario adds a difficulty to the countermeasure to the previous one. Simulations show as Secrecy Outage Probability decreases until 10% with a standard number of relay nodes in the network. As a result, cooperative jamming strategies are seen to be highly effective for increasing the secrecy in Wireless Sensors Networks.**

Keywords-WSN; cognitive; jamming; collaborative; security

I. INTRODUCTION

Wireless Sensor Networks (WSN) is one of the fastest growing sectors in recent years. The unlicensed Industrial, Scientific and Medical (ISM) spectrum bands, used by these networks, are becoming overcrowded. The cognitive paradigm has appeared to solve spectrum scarcity, interference and reliable connections problems.

Cognitive Wireless Sensor Networks (CWSN) are based on the cycle sensing spectrum monitoring, analyzing for environment characterization, reasoning to chose the best communication strategy, and sending to provide adaptation and collaboration. Cooperation between devices regarding information sharing and taking decisions allows better spectrum use, lower energy consumption and better data reliability. CWSN are used in systems with critical data (telecare monitoring, military scenarios) and critical applications (safety home system, infrastructure protection, etc.). Hence, security is a fundamental challenge to face. Cognitive nature of the system introduces an entire new suite of threats and attacks that are not easily mitigate.

The broadcast characteristic of the wireless medium makes difficult to shield transmitted signals form unintended recipients. Security in wireless data transmission has traditionally been developed using cryptographic techniques at the network layer. The main drawback of this approach when deployed to WSN consists in limited resources, which cannot support the execution of complicated encryption algorithms, resulting in shorter keys that are easier to discover. WSN nodes can also be captured and attackers use reverse-engineered and become an instrument for mounting counterattacks.

Physical-layer security becomes a very interesting approach in the past few years [1]. The main idea behind physical-layer security is to limit the amount of information that can be extracted at the 'bit' level by unauthorized receivers with the exploitation of all available Channel State Information (CSI). The fundamental problem in WSN is the difficulty to obtain a full CSI. Cognitive paradigm allows the spectrum monitoring and provides this information to the network.

In this paper, a selective jam technique to increase physical-layer security in CWSN using cognitive capabilities is presented. This technique can operate independently of the higher layers to complement security requirements.

The organization of this paper is as follows. In Section II, works in physical-layer security for WSN are reviewed. In Section III, we formulate the technique description. Section IV provides its evaluation. Finally, the collusions are drawn in Section V.

II. PHYSICAL-LAYER SECURITY APPROACHES

In this section, we introduce schemes that could be used to achieve physical layer security against different attacks in WSN.

In recent years, the main issues of secure channel capacity have drawn much attention in the information theory community. Most of the works are focused in schemes to obtain the secrecy capacity with different CSI approaches. Barros and Rodrigues in [2] developed a secure communication protocol to ensure wireless information-theoretic security based on: common randomness via opportunistic transmission, message reconciliation, common key generation via privacy amplification and, finally, message protection with a secret key. It was shown that the protocol is effective in secure key renewal even the presence of imperfect CSI.

Other methods have been proposed to avoid attacks based on exploitation of channel characteristics. The Radio Frequency (RF) fingerprinting system implemented by [3] consists of multiple sensor system that captures and extracts RF

 ISBN: 978-1-61208-197-7

features from each receiver signal. An intrusion detector processes the feature sets and generates a dynamic fingerprint for each internal source identifier derived from a few packets. This system monitors the temporal evolution and alerts when a strange fingerprint is detected. In [4], L. Xiaohua and E.P Ratazzi propose a precoding scheme, in which the transmitted code vectors are generated by singular value decomposition of the correlation matrix, which describes the channel characteristic features between the transmitter and the intended receiver. Because of the difference in the multipath structure of the transmitter-receiver channels, even intruders, which have

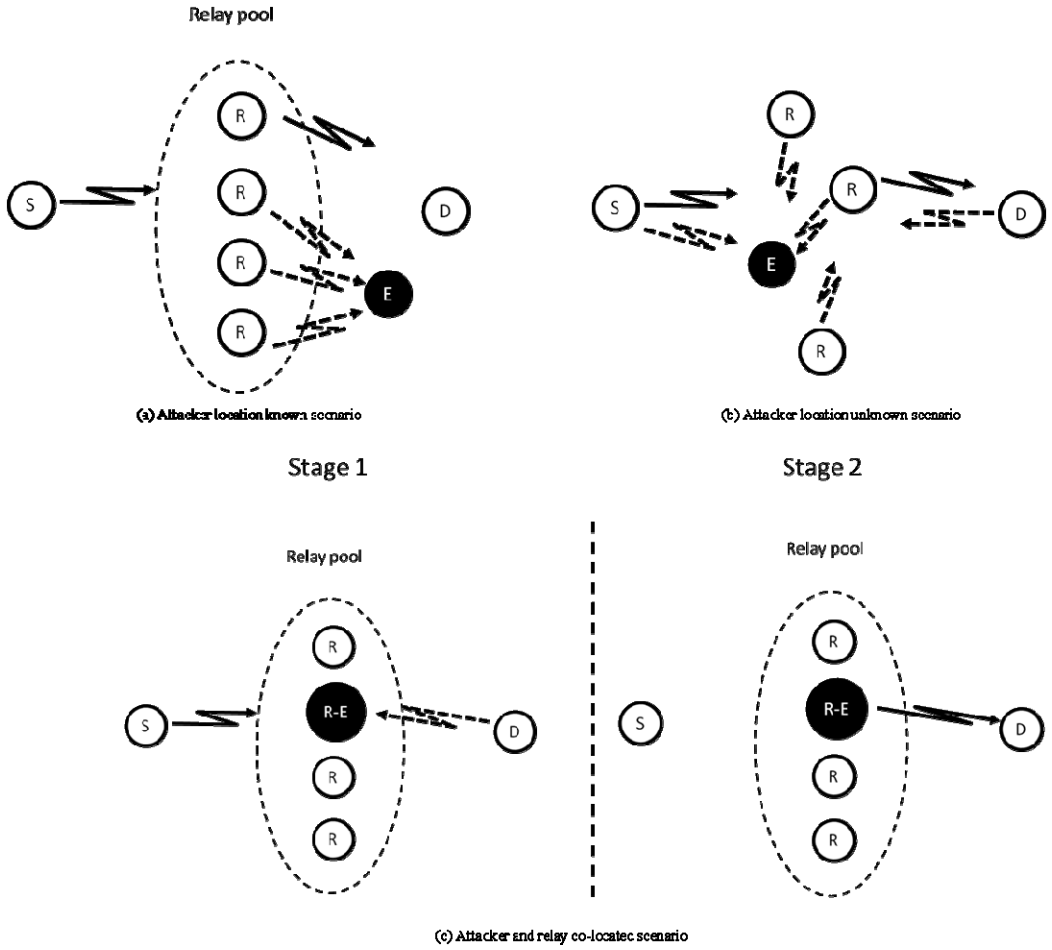

Figure 1. Cooperative Jamming Scenarios

a perfect knowledge of the transmission code, vectors, cannot achieve to acquire the true messages due the difference in the locations of the intruders and the legitimate users.

Code approaches improve resilience against jamming and eavesdropping. In [5], a combination of turbo coding and Advanced Encryption Standard (AES) cryptosystem is proposed. An error in the received ciphertext could cause a large number of errors in plaintext after coding. Depending of the channel condition, this method can be adopted to choose the number of redundant bits required to protect the information in order to achieve high efficiency. Another technique is Spread Spectrum Coding, which signal is spread by a pseudo-noise sequence over a wide frequency bandwidth much wider than that contained in the frequency ambit of the original information. The main difference between convention cryptographic systems and spread-spectrum systems lies in their key sizes. Traditional systems can have a very large key space. However, in a spread-spectrum system, the key space is limited by the range of carrier frequencies and the number of different sequences. In [6], a method is proposed to enhance the physical layer security of Code Division Multiple Access (CDMA) system by using AES operation to generate the scrambling sequences.

Data protection can also be facilitated using power approaches. The method proposed in [7] ensures perfectly secure communications. This method shows that perfect secrecy can be achieved when the intruder's channel is noisier than the receiver's channel. Artificial noise is generated using multiple antennas or the coordination of helping nodes, and is injected into the null-subspace of the intended receiver's channel.

According to the proposal in work [8], discriminatory channel estimation is performed by injecting artificial nose to

 ISBN: 978-1-61208-197-7

the left null space of the legitimate receiver's channel to degrade the estimation performance of the eavesdropper. By exploiting the channel feedback information from the legitimate receiver at the beginning of each communication stage, a multistage training-based channel estimation scheme is proposed [9] to minimize the normalized mean squared error of channel estimation at the legitimate receiver subject to a constraint on the estimation performance attainable by the non-legitimate receiver.

Most of these approaches can be improved using cognitive capabilities. Cognitive paradigm provide a new scenario because of the spectrum sensing, the protocols to share information and the collaboration to optimize the communications. In this paper a collaborative jamming technique is proposed to increase CWSN security and a counter measurement against eavesdropped attacks.

III. COOPERATIVE JAMMING SCENARIO

CWSN avoid one of the main constraints to use jamming techniques, the knowledge of the CSI. In a cooperative scenario there are several network entities. We consider a four-terminal system composed of a legitimate source (S), a legitimate destination (D), one or more relay nodes (R) and an eavesdropper (E). All these agents have cognitive capabilities and different radio interfaces. In this approach, the normally inactive nodes in the relay network can be used as cooperative jamming sources to confuse the eavesdropper and provide better performance in terms of security. Depends of the nodes nature three types of scenarios are defined (Fig. 1): attacker location known, attacker location unknown, and attacker and relay co-location. Each new scenario adds a difficulty to the countermeasure to the previous one.

A. Attacker location known

In the proposed cooperative jamming strategy any available jamming power will only be allocation to information transmitters, while D and S remain inactive. If E is detected by the network, nodes can use the location information to increase jamming over the attacker zone.

Relay pool replay the message to the D and produce a jamming with the same communication features over the E zone. Closer nodes to the attacker manage the coordinated jamming. Thus, E can not listen the transmitted information and the communications in the rest of the network is not affected.

B. Attacker location unknown

In this approach, both the source and the destination nodes act as temporary helpers to transmit jamming signals during transmission phase in which they are normally inactive. The transmitter and the temporary helpers can perform cooperative jamming in the jamming subspace, which will allow the legitimate receivers to us beamforming to reject interference from this subspace. Note that cooperative jamming requires the receiver to broadcast the jamming subspace so that the interference can be aligned at the desired receiver without a loss of information. Although E may also be aware of this subspace, it cannot remove the jamming signal since it sees different channels from the transmitters and jammers.

C. Attacker and relay co-located

A most complicated issue is when E is co-located with the helper node. A secure countermeasure in this case is to have the destination jam the relay while it is receiving data from the source in the first phase. This intentional interference can then be subtracted out by the destination from the signal it ultimately receives via the relay.

Protocol sequence is as follows. Directional jamming is produced by D while S sends data to the R-E node. R node detects an adding of real data and jamming signal. When replay data arrive D, a subtraction of jamming signal is done to recover the real sent data.

IV. RESULTS

In order to compare the security using this cooperative jamming technique with current system metrics are necessary. For this propose, secrecy rate and secrecy outage probability are defined. The secrecy rate is a reliable transmission rate on the main channel, which remains undecodable at the eavesdropper. In Gaussian channels, it is represented by the different of the mutual information of the source-to-receiver information and the source-to-eavesdropper channels, with the secrecy capacity being the maximal achievable secrecy rate. When larger networks with multiple transmitters/receivers/eavesdroppers, as well as additional nodes such as relays are considered, we can define the corresponding secrecy rate (capacity) regions, or the aggregate secrecy sum rate (capacity).

A performance metric suitable for non-ergodic channels is the Secrecy Outage Probability (SOP), which describes the probability that a target secrecy rate is not achieved. The SOP characterizes the likelihood of simultaneously reliable and secure data transmission.

The efficacy of this scheme for different example scenarios using these metrics is presented. In order to simulate the attack and the countermeasurements a new CWSN simulator has been used. This simulator has been developed over the well known Castalia simulator. Modifications improve Castalia and include new cognitive features. The CWSN simulator responsibilities are: the scenario definition, the simulation of spectrum state, the communications between nodes and the implementation of cognitive behaviors, attacks and countermeasures.

Several simulations have been executed in the simulators to extract results and to draw conclusions of the work. Attacker location known strategy has been selected for these simulations. The number of nodes in the simulation is 34 nodes, including one emitter user, one destination node, one attacker (eavesdropper) and a variable number of cooperative jammer relays for both scenarios. Both scenarios are 50x50 meters. In the first scenario the D-E distance is 30 meters while in the second scenario D-E distance is 45 meters. Jamming is better focalized in the second scenario because the penalty in the destination node is less that in the first one.

 ISBN: 978-1-61208-197-7

We have developed two graphics that summarize the results. In the Fig. 2, the percentage of received packets in the destination node and the eavesdropper is showed for the first scenario. Number of packets decrease with the number of collaborative jammer relay nodes. Using only ten nodes for the collaboration strategy, less than 50% of packets are received. However, destination node receives fewer packets because of the jamming, but this rate is enough for a good communication.

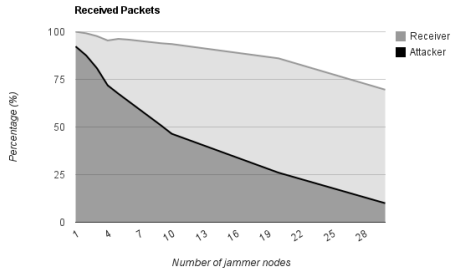

Figure 2. Received Packets in the receiver and the attacker

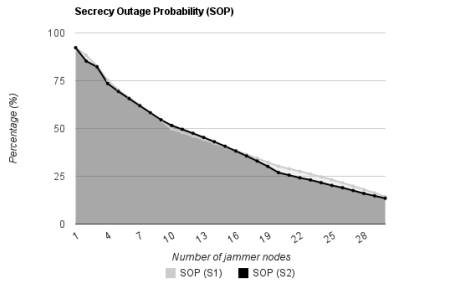

Figure 3. Secrecy Outage Probability for different scenarios

In Fig. 3, the SOP for the two different scenarios depending of number of nodes is showed. In both scenarios SOP is very similar. We can conclude that attacker location is not a real problem using this technique. Using 20 nodes for the collaborative jamming technique SOP is less than 25%, increasing system security in a significant way.

V. CONCLUSION AND FUTURE WORK

In this article, we presented a cooperative jamming strategy for physical-layer security in multi-user wireless sensor networks as a supplement to encryption at higher layers.

Depending on the nature of the nodes, three types of scenarios are defined: attacker location known, attacker location unknown, and attacker and relay co-location. A simulation framework has been used to simulate different scenarios. From the simulation results, we showed that the SOP decreases with a standard number of relay nodes in the network. Also, attacker location is not a problem for this kind of strategies.

Cooperative jamming strategies with assistance from external helpers or inactive neighboring nodes are seen to be highly effective for increasing the secrecy of the transmitted data.

ACKNOWLEDGMENT

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

REFERENCES

[1] Y. Shiu; et al., "Physical layer security in wireless networks: a tutorial," *Wireless Communications, IEEE*, vol. 18, no. 2, pp. 66-74, April 2011.

[2] J. Barros and M.R.D. Rodrigues, "Secrecy Capacity of Wireless Channels," *Information Theory, 2006 IEEE International Symposium on*, vol. 1, pp. 356-360, July 2006.

[3] C. Sperandio and P.G. Flikkema, "Wireless physical-layer security via transmit precoding over dispersive channels: optimum linear eavesdropping," *MILCOM 2002. Proceedings*, vol. 2, pp. 1113- 1117, Oct. 2002.

[4] L. Xiaohua and E.P Ratazzi, "MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks," *Military Communications Conference, 2005. MILCOM 2005. IEEE*, vol. 3, pp. 1353-1359, Oct. 2005.

[5] H. Yongsun Hwang and H.C. Papadopoulos, "Physical-layer secrecy in AWGN via a class of chaotic DS/SS systems: analysis and design," *Signal Processing, IEEE Transactions on*, vol. 52, no. 9, pp. 2637-2649, Sept. 2004.

[6] G. Noubir, "On Connectivity in Ad Hoc Network Under Jamming Using Directional Antennas and Mobility," *2nd International Conference in Wired and Wireless Internet Communications*, vol. 1, pp. 54-62, 2004.

[7] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," *Military Communications Conference, 2005. MILCOM 2005. IEEE*, vol. 3, pp. 1501-1506, Oct. 2005.

[8] T.H. Chang, Y.-W.P Hong and C.-Y. Chi; "Training Signal Design for Discriminatory Channel Estimation," *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, vol. 1, pp. 1-6, Dec. 2009.

[9] I. Csiszar and J.Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339-348, May 1978.

 ISBN: 978-1-61208-197-7