ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Secrecy Concept in Wireless Sensor Networks For AF-CS

B.Saranya[1], P.RajKumar[2]

M.E Applied Electronics, Varuvan Vadivelan Institute of Technology, Dharmapuri, India

Assistant Professor, Dept of ECE, Varuvan Vadivelan Institute of Technology, Dharmapuri, India

ABSTRACT: WSNs are severely energy-constrained because they consist of many small, cheap and power limited nodes whose batteries cannot be recharged in most cases. Hence, the application of energy-efficient algorithms turns out to be crucial. *Compressed Sensing* (CS) appears to be a good candidate in order to exploit signal correlations in the time domain. The goal is twofold. First, to take advantage of the time correlation in order to produce sparse versions of the signal vector, which collects the transmitted signals of all the sensors? Second, to benefit from the nature of the multiple access channels in order to perform random measurements of the signal vector. This model is then used to select the number of active nodes and relays based on a cost function that controls the tradeoff between reconstruction error and energy consumption. In this Paper we propose a system physical layer secrecy performance for the case when malicious eavesdropping under the assumption that they have corrupted channel state information. A metod with channel estimation technique based on random pilots. Simulation results evaluvate the corruption of data packets providing secured results in channels.

I. INTRODUCTION

Wireless communications have been extended to virtually all the possible scenarios and applications. Unfortunately, security risks are inherent in any wireless transmission. This is mainly because the communication channel is open to any intruder. Therefore, unauthorized entities may exploit this sce-nario in order to obtain confidential information, to corrupt the transmitted data, to degrade the network performance, etc.
For our convenience, we differentiate these attacks in two groups [Sri08]:

• Physical layer attacks. They benefit from the wireless connection na-ture. Mainly, there exist two kind of attacks at physical layer: i) the eavesdropping that refers to the existence of one/many unauthorized receiver/s trying to extract information from the signal present in the wireless channel, and ii) the jamming [Kas04,Sha05], that refers to the existence of a malicious transmitter (or a group of them) that intentionally degrades the intended communication by introducing additional interference. Although both approaches are extremely in-teresting, we focus our study on the robustness of the AF-CS scheme against eavesdropping attacks.

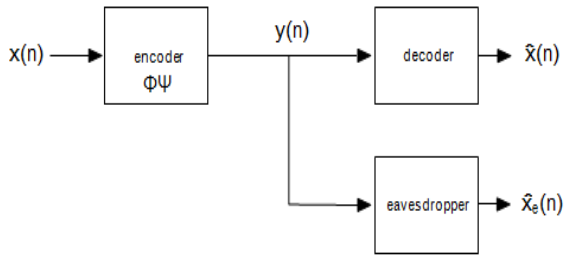


Figure 5.1: Block diagram of PHY-Layer secrecy scenario

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

the paper studies how difficult it is for the eavesdropper to re-cover x(n) from the measurements y(n) without the knowledge of the key ΦΨ. Actually, it has been proved (see Lemma 1 in [Rac08]) that compressed sensing encryption does not achieve perfect secrecy, i.e., $\mathbf{I}(x(n); y(n)) > 0$. The mutual information $\mathbf{I}(x(n); y(n)) = 0$ would be zero if and only if x(n) and y(n) are independent. However, since ΦΨ is lineal, $x(n) = 0$ implies that $y(n) = 0$, and hence $P(y(n) = 0|x(n) = 0) = P(y(n) = 0)$, meaning statistical dependence.

II. SYSTEM MODEL AND ASSUMPTIONS

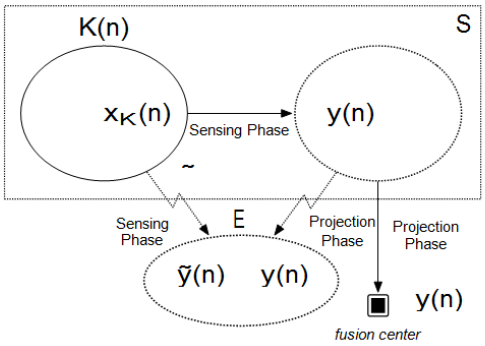
We consider a WSN configured in star-topology that monitors a given phys-ical scalar magnitude (e.g., temperature, humidity) or detects a physical event (e.g., wildfire). In particular we assume the scheme in Fig. 5.3, that is:

- A set S of S sensing nodes connected (wirelessly) to one fusion center, that acts as the intended receiver. Their measurements at discrete time n are represented by x(n).

- A subset $K(n) \subseteq S$ (of cardinality K) of active sensors that are transmitting at a given time n. The transmitted vector is $x_K(n)$ where only K positions are different to zero. The remaining sensors in $Q(n) = S \setminus K(n)$ (of cardinality Q) remain silent.

- A subset $R \subseteq S$ (of cardinality R) acts as relay nodes in Amplify-and-Forward (AF) mode.

- A set E (of cardinality E) of malicious and passive eavesdropping nodes.



Amplify-and-Forward Compressed Sensing Scheme

During this phase, all the sensors in K(n) broadcast their readings, and hence the relay sensors receive linear combinations due to the nature of the MAC, namely,

$$y(n) = \Phi x_K(n) + w(n), \tag{5.16}$$

where the vector $y(n) \in R^R$ stacks all the received signals of the nodes in R, the sensing matrix Φ models the channel between S and R as a random

matrix with i.i.d. Gaussian entries with zero mean and variance $\sigma_\Phi^2 = R^{-1}$. Finally, w(n) denotes white Gaussian noise with zero mean and variance

σ_w^2.

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

Similarly to (5.16), the received signal at the eavesdroppers is:

$$y(n) = \Phi x_K(n) + w(n). \quad (5.17)$$

where $y(n) \in R^E$ stacks the signals received by the nodes in E, and Φ mod-els the channel between S and E as a random matrix with i.i.d. Gaussian entries with zero mean and variance $\sigma_\Phi = E^{-1}$ and w(n) denotes white Gaussian noise with zero mean and variance σ_w.

For the sake of simplicity and without loss of generality, we focus on the noiseless problem. Moreover, we will address two different cases: i) PHY-Layer secrecy with perfect CSI at the eavesdroppers, and ii) PHY-Layer secrecy with imperfect CSI.

III. CHANNEL ESTIMATION BASED ON RANDOM PILOTS

The without decreasing their own estimation. In particular we propose a training phase where each sensing node sends N random pilots with amplitude A + s(n), where A is a known and constant value and s(n) is a (pseudo)random sequence distributed as

$$s(n) \sim N(0, \sigma_s),$$

which has been previously agreed. The pilot signal from sth sensing node at the rth relay is:

$$p_{r,s}(n) = (A + s(n))[\Phi]_{r,s} + [w(n)]_r. \quad (5.36)$$

On the other hand, the eth eavesdropper will receive the pilot signal from the sth sensing node as

$$p_{e,s}(n) = (A + s(n))[\Phi]_{e,s} + [w(n)]_e. \quad (5.37)$$

We assume the general scheme that the eavesdroppers do not have com-plete information of the pilot amplitudes. Instead, they only know partial information of the pilot sequence. The part that they know is A, while it is assumed that the eavesdroppers do not have access to s(n).

IV.RELATIVE WIRETAP DISTORTION AS A FUNCTION OF THE ESTIMATION CHANNEL DISTORTION

Here we study the performance of the relative wiretap distortion as a func-tion of the channel estimation distortion. This study actually extends the one in [Her10] and confirm some of their results. Mainly, we show (as in [Her10]) that the distortion at the receiver grows linearly with the power of the channel estimation distortion for values D < 0dB. This is true (up to some error floor) not only for the case D < 0dB but also when D > 0dB, as we can graphically.

We also show that the relative wiretap distortion decreases for lower values of D up to some error floor, which depends on the number of eaves-droppers. It means that even for the ideal case of $D = -\infty$dB, the relative wiretap distortion cannot be decreased further than the error floor.

However, probably the most relevant result of this subsection is the fol-lowing: for values of D = 0dB all the configurations achieve a similar relative wiretap distortion of 1. It means that the distortion of the reconstruction phase performed at the eavesdroppers is equal to the actual variance of the signal.

V.CONCLUSIONS

The AF-CS as a physical-layer secrecy solution for WSNs. In particular, the presence of a eavesdropper set of nodes

ISSN(Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Special Issue 6, May 2015

has been considered. The secrecy level for each of the cases according to the number of eavesdroppers have been separately studied. It has been demonstrated that AF-CS achieves perfect secrecy for the cases when the number of eavesdroppers is less than the sparsity of the signal. For larger number of eavesdroppers, a random pilot technique has been proposed as a training phase in order to contam-inate the channel estimation of the eavesdroppers and therefore decrease their performance. Simulation results have supported the theoretical results and they have validated the random pilot technique as a good candidate to increase the protection of AF-CS against a large number of eavesdropping nodes.