ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

Encryption and Fusion of Target Decision Based On Channel Gain in Wireless Sensor Networks

R.S.Varshini dhevi, D.Vijendra Babu

PG Student, Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University, Chennai, India

Head, Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University, Chennai, India

Abstract: A wireless sensor network (WSN) is a collection of nodes organized into a cooperative network. Security and energy consumption have been considered as long-lasting technical challenges in WSNs, as sensors usually suffer from complexity and energy constraints. In particular, it has played an important role in such applications that require proactive actions responding to rapid changes of outside environments. In order to provide data confidentiality in a distributed detection scenario, a simple and efficient physical-layer security is studied. Specifically, to prevent passive eavesdropping on transmitting data from sensors to an ally fusion center (AFC), we propose a novel encryption scheme and decision fusion rules for a parallel access channel model. The proposed scheme takes advantage of a free natural resource, i.e., randomness of wireless channels, to encrypt the binary local decision of each sensor in such a way that the binary local decision is flipped according to instantaneous channel gain between the sensor and AFC. The location-specific and reciprocal properties of wireless channels enable the sensor and AFC to share the inherent randomness of wireless channels which are not available to an eavesdropper. Furthermore, it is shown that the scheme is well-suited to a low complexity and energy efficient modulation technique, non-coherent binary frequency shift keying. To evaluate performances of the proposed Scheme, log-likelihood-ratio-based decision fusion strategies at the AFC are analyzed, and comparisons of decision performances are carried out. In addition, we prove that the proposed scheme achieves perfect secrecy with a simple structure that is suited for sensors of limited complexity.

Index Terms—Decision fusion, distributed detection, eavesdropping, encryption, perfect secrecy, wireless sensor networks.

I. INTRODUCTION

In recent years, wireless sensor networks (WSNs) have gained worldwide attention for use in different applications. Sensor nodes are spatially distributed across a large area of interest to sense, measure, and gather information and transmit the data to the user. The nodes are typically equipped with radio transceivers, micro-controllers, and batteries. They are small in size, inexpensive, and could be deployed in large numbers. They can be used in applications such as military target tracking and surveillance, natural disaster relief, biomedical health monitoring, and industrial automation

The uses of WSN for industrial applications are expected to open large opportunities for collecting data, enabling remote control, and automation to improve the safety and productivity of facilities. Unlike wire-based systems, WSNs can be deployed in bearings of motors, oil pumps, whirring engines, or other inaccessible or hazardous environments. In general, wireless solutions are considered to be cheaper compared to wire-based systems. This is due to the cost associated in shielding wires to prevent severe conditions which are usually present in these harsh environments (high humidity, high temperature, strong vibration, etc.). Short-range wireless technologies such as IEEE 802.15.4 in mesh network configuration are widely considered to be cost effective solution for use in industrial settings.

In harsh industrial environments, noise is significant due to the wide operating temperatures,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

strong vibrations, excessive electromagnetic noise caused by large motors, etc.. Interferences from other wireless systems operating on the same frequency band might also be present. In addition, the signal might be subject to heavy multipath propagation effects caused by multiple reflections from mainly metallic structures in the surrounding environment. The random/periodic movement of people, robots, trucks, and other objects may also cause time varying channel conditions. Effects of the aforementioned propagation impairments to mission-critical signals in industrial settings can result in environmental monitoring, inventory management, and many others. In particular, it has played an important role in such applications that require proactive actions responding to rapid changes of outside environments. Early warning system such as intrusion detection and disaster alert, network control in the self-organized network, and spectrum sensing in the cognitive radio are the notable ones that the the binary distributed detection can be applied to prevent a potential conflict or crisis. Moreover, in practice, sensors for the distributed detection in WSNs are often incapable of employing traditional cryptographic techniques due to practical constraints of sensors such as limited energy resources, computing power, etc

To resolve the technical challenge of secure communications in WSNs, there have been several notable approaches, where the ability of the physical layer is explored as a solution to the data confidentiality for the distributed detection in WSNs. Assuming the presence of a passive eavesdropper called an enemy fusion center (EFC), sensors in a WSN individually or collaboratively transmit their local decisions on a target state to an ally fusion center (AFC), where final decision is made. In this case, the central issue is how to design a physical layer scheme at the sensors to achieve reliable transmission with the AFC while preventing information leakage to the EFC.

In, it is found that simultaneous transmission of local decisions using the type-based multiple access (TBMA) protocol over a multiple access channel (MAC) can be utilized for the data confidentiality in costly disasters in terms of money, manpower, time, and even human lives. Thus, knowledge of the propagation channel is needed to successfully design and evaluate robust WSNs for industrial applications.

II. SYSTEM MODEL AND WORKING PROCESS

From military to civilian applications, binary distributed detection problems in wireless sensor networks (WSNs) have been introduced in a wide range of areas such as military surveillance, disaster recovery, such a way that some sensors are deliberately selected to transmit interfering signals to make the EFC confused. Since all the transmitting data from sensors are naturally fused during transmission over MAC, the EFC is unable to remove the interfering signals, which thus hinders it from making a correct decision. In particular, the rule selecting the sensors generating interference is designed 1) to minimize the degradation of detection performance at the AFC and 2) to be autonomous and nondeterministic, which prevents the EFC from identifying the sensors generating interference. It is shown that, by taking advantage of the inherent randomness of wireless channels, the design goals can be achieved. The results in further show that the proposed scheme provides both reliability and *information-theoretic perfect secrecy* for distributed detection. Although the scheme reduces the complexity and power consumption required for the security goal at each individual sensor level, the power consumption across the entire sensor network may get even higher due to the wasted energy for generating the interference. In addition, the scheme assumes coherent communications from the sensors to the FCs, which requires full channel state information in the sensors, namely, amplitudes and phases of their channel gains, and thus may be too complicated to be implemented in some applications. On the other hand, the work is addressed the data confidentiality issue over a parallel access channel (PAC) where sensors individually access to the AFC through orthogonal channels.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

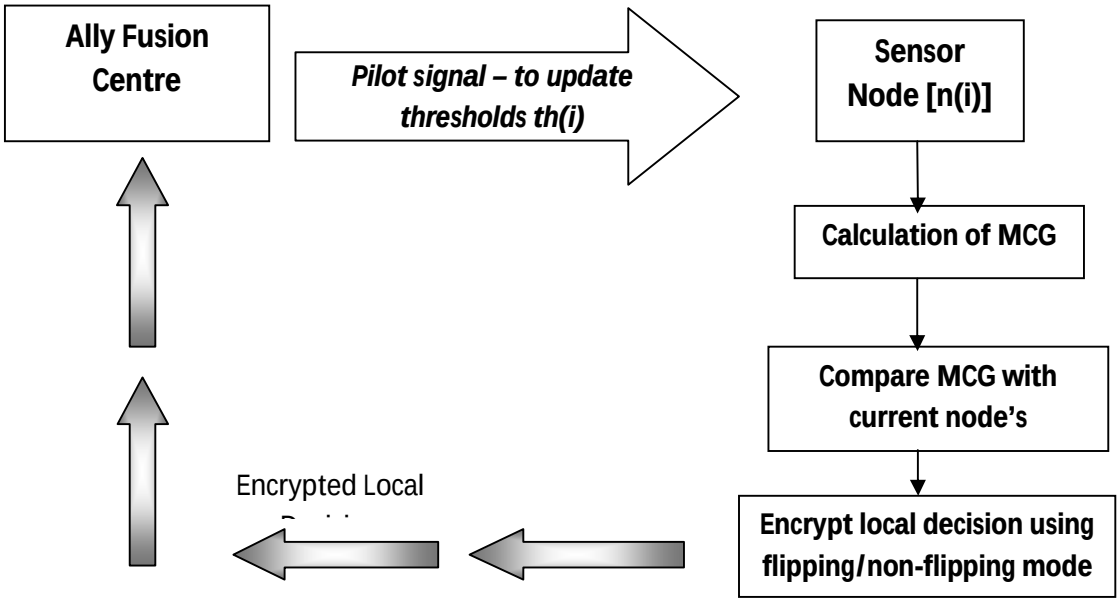

FIG:1 Block diagram

In this scheme, each sensor intentionally induces decision errors by randomly flipping its binary local decision before transmitting it. The rates of intentionally induced errors are assumed to be known at the AFC and sensors a priori except for the EFC. In it is shown that the scheme enables the AFC to detect the target state reliably while resulting in sufficiently high detection error rate at the EFC. This approach seems simple and efficient but basically does not eliminate the key distribution problem since the a priori shared error rates between the AFC and sensors can be understood as a pre shared key. In addition, the detection error rate is a relaxed measure of security that does not guarantee the information-theoretic perfect secrecy.

In this paper, we study a transmission scheme at the physical layer to secure the transmission from sensors to the AFC over a PAC without resorting to secret key sharing.

In addition, the proposed scheme aim at achieving the information-theoretic perfect secrecy, which is not possible with traditional cryptographic techniques. For this work to be more practical, we consider a simple and energy efficient modulation

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

technique, but not limited to, non coherent binary frequency shift keying (NC-BFSK). NC-BFSK known as *green modulation* is widely employed in WSNs as a realistic option (e.g., MICA2 Motes) thanks to its low cost and complexity in implementation.

A. System Model

In the proposed scheme, it is assumed that the AFC broadcasts a pilot signal to initiate distributed detection, and each sensor measures the strength of the received pilot signal, which is equivalent to measuring the magnitude of the channel gain (MCG) from the AFC to the sensor. Since a simple energy detector is enough to measure the pilot signal strength, the required additional complexity may be acceptable in many cases. Then, each sensor autonomously joins one of three groups, *dormant, flipping,* and *non flipping* groups, according to their MCG measurements whenever the AFC broadcasts the pilot signal. The sensors in the flipping and non ffipping groups are called *activated* sensors, and they report their local decisions over a PAC in the time-division duplexing (TDD) manner.

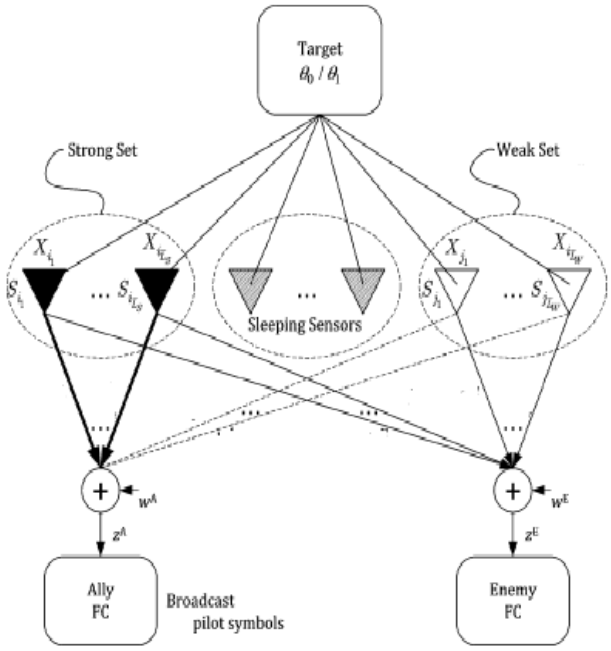

FIG 2: System model

That is, the transmission from the sensors are carried out in the same coherence time over the same wireless channel where the pilot signal is broadcasted. The main idea behind the proposed scheme is that the sensors in the flipping and nonflipping groups send their local decisions to the AFC in the completely opposite ways from each other to make the EFC confused. For example, when two activated sensors involved in the two different groups, i.e., flipping and nonffipping groups, make the same local decision on the target state, the transmitted data from the sensor in one group becomes a bit-flipping version of the other's. Note that the MCGs determining the group assignment of sensors can be seen as an encryption seed obtained from the nature on demand, and thus we need not the assumption i.e., the a priori shared error rates.

Meanwhile, at the AFC and EFC, the transmitting data from activated sensors in different groups should be fused in an appropriate way to make a

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

final decision on the target state. Since the activated sensors report their local decisions in the TDD manner in the same coherence time, the received signal strengths at the AFC provide estimates of the MCGs measured at the sensors, and thus the AFC can incorporate such estimates into the fusion. On the other hand, the EFC eavesdrops the signals from the sensors over a statistically independent PAC, and is totally ignorant of the MCGs when it is more than one half wavelength away from the AFC. It should be noted that when compared with the schemes where the signals from the interfering group are used only for confusing the EFC, in the proposed scheme, the signals of the activated sensors from both the flipping and nonffipping groups are combined at the AFC, and thus the energy consumed by sensors to transmit signals is not wasted, which leads to better energy efficiency.

Besides the general results of physical-layer security for wireless communications, the proposed scheme is closely related to existing works in three specific areas: 1) secret key extraction from wireless channel, 2) cooperative secrecy, and 3) secret communication using artificial noise. In references there in, wireless channel gains are considered as common randomness exclusively shared by transmitter and legitimate receiver using the TDD protocol. Various schemes to extract secret keys from different types of wireless channels have been extensively studied, e.g., wireless MIMO channels, Ultra-Wide Band channels and multi path fading channel. In WSNs, however, such schemes may be too expensive to be realized in sensor nodes in terms of complexity and/or power consumption. Nevertheless, motivated by the precursory works, we can find a simple but efficient scheme tailored to wireless sensor nodes with constraints of complexity and resources. Novelties of the proposed scheme also lie in judiciously designed cooperations among sensors each of which autonomously conducts different roles, i.e., reporting of their observations and generating interference to confuse possible EFCs. The collective behavior of self-organized sensors achieves the perfect secrecy against passive eavesdropping without requiring high intelligence in the sensors.

The works of cooperative secrecy and artificial interference techniques provide a great deal of insight into the techniques we utilize while they are considered in different communication scenarios such as relay networks and point-to-point and multiuser communications.

Our contributions in the work are summarized as follows: 1) we derive conditions for the EFC to be totally ignorant of target state, i.e., achieving perfect secrecy, and 2) two decision fusion rules for the AFC are proposed; i) a log-likelihood ratio (LLR) based decision fusion rule with channel statistics and ii) a suboptimal decision fusion obtained from a high signal-to-noise ratio (SNR) approximation, and their performances are evaluated. With both reliability and security ensured at the physical layer, our scheme is unique in that it includes an energy-efficient modulation and activation rule of sensors for longer lifetime of WSNs. The claim for security will be thoroughly proved and confirmed by carrying out numerical evaluations of the proposed scheme. In addition, comparisons will be performed, which shows that the proposed scheme outperforms over a broad range of SNR values without compromising the security goals, perfect secrecy.

III. SECURITY ANALYSIS

In the security analysis of our scheme, the main concern is how much information the EFC can obtain from eavesdropping on the sensors' transmission to the AFC

A. Perfect Secrecy

We begin with the likelihood function of the i-th sensor for given *O*, denoted by f ($\mathcal{Z}_i^E|\theta_l$). With the total probability theorem, $f(\mathcal{Z}_i^E|\theta_l)$ is given by

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

$$
\begin{aligned}
f\left(\mathbf{z}_i^E|\theta_\ell\right) &= \sum_{u_i}\sum_{\mathbf{x}_i} f\left(\mathbf{z}_i^E, \mathbf{x}_i, u_i|\theta_\ell\right) \\
&= \sum_{u_i} p\left(u_i|\theta_\ell\right) \sum_{\mathbf{x}_i} \int f\left(\mathbf{z}_i^E, h_i^S, \mathbf{x}_i|u_i, \theta_\ell\right) dh_i^S \\
&= \sum_{u_i} p\left(u_i|\theta_\ell\right) \sum_{\mathbf{x}_i} \int f\left(\mathbf{z}_i^E|h_i^S, \mathbf{x}_i, u_i, \theta_\ell\right) \\
&\quad \times f\left(h_i^S|u_i, \theta_\ell\right) p\left(\mathbf{x}_i|h_i^S, u_i, \theta_\ell\right) dh_i^S \\
&\overset{(a)}{=} \sum_{u_i} p\left(u_i|\theta_\ell\right) \sum_{\mathbf{x}_i} f\left(\mathbf{z}_i^E|\mathbf{x}_i\right) \\
&\quad \times \int f\left(h_i^S\right) p\left(\mathbf{x}_i|h_i^S, u_i\right) dh_i^S, \quad \ell \in \{0,1\},
\end{aligned}
$$

where (a) is valid as $\theta_l \rightarrow u_i \rightarrow X_i \rightarrow Z_i^E$ forms a Markov chain and h_i^S is independent of Z_i^E u_i, , and θ_l . Although the EFC is not aware of the MCGs of the main channel, h_i^S we could assume that she knows the encryption scheme performed in the sensors. Thus, $f(Z_i^E|\theta_l)$ is derived as follows:

$$
\begin{aligned}
f\left(\mathbf{z}_i^E|\theta_\ell\right) &= \sum_{u_i} p\left(u_i|\theta_\ell\right) \\
&\quad \times \left\{ f\left(\mathbf{z}_i^E|\mathbf{E}(u_i)\right) \int f\left(h_i^S\right) p\left(\mathbf{E}(u_i)|h_i^S, u_i\right) dh_i^S \right. \\
&\quad \left. + f\left(\mathbf{z}_i^E|\bar{\mathbf{E}}(u_i)\right) \int f\left(h_i^S\right) p\left(\bar{\mathbf{E}}(u_i)|h_i^S, u_i\right) dh_i^S \right\} \\
&\overset{(a)}{=} \sum_{u_i} p\left(u_i|\theta_\ell\right) f\left(\mathbf{z}_i^E|\mathbf{E}(u_i)\right) \lambda_1 \\
&\quad + p\left(u_i|\theta_\ell\right) f\left(\mathbf{z}_i^E|\bar{\mathbf{E}}(u_i)\right) \lambda_2, \quad \ell \in \{0,1\},
\end{aligned}
$$

By combining (1) with the condition for perfect secrecy, $f(Z_i^E|\theta_0) = f(Z_i^E|\theta_1)$ we can get

$$
\begin{aligned}
&(1 - P_{f_1})\left(f\left(\mathbf{z}_i^E|\mathbf{E}(0)\right)\lambda_1 + f\left(\mathbf{z}_i^E|\bar{\mathbf{E}}(0)\right)\lambda_2\right) \\
&\quad + P_{f_1}\left(f\left(\mathbf{z}_i^E|\mathbf{E}(1)\right)\lambda_1 + f\left(\mathbf{z}_i^E|\bar{\mathbf{E}}(1)\right)\lambda_2\right) \\
&= (1 - P_{d_1})\left(f\left(\mathbf{z}_i^E|\mathbf{E}(0)\right)\lambda_1 + f\left(\mathbf{z}_i^E|\bar{\mathbf{E}}(0)\right)\lambda_2\right) \\
&\quad + P_{d_1}\left(f\left(\mathbf{z}_i^E|\mathbf{E}(1)\right)\lambda_1 + f\left(\mathbf{z}_i^E|\bar{\mathbf{E}}(1)\right)\lambda_2\right).
\end{aligned}
$$

$$
f\left(\mathbf{z}_i^E|\mathbf{E}_i(u_i)\right) = f\left(\mathbf{z}_i^E|\bar{\mathbf{E}}(\bar{u}_i)\right)
$$

This means that we have to make the sizes of flipping and non flipping groups statistically equal, which is intuitive since equally likely contradicting reports must make the EFC totally confused, which provides perfect secrecy.

B. Security against Cryptographic Attacks

In addition to perfect secrecy against eavesdropping, we further analyze the strength of our proposed scheme against two well known attacks in cryptanalysis where the EFC can attempt to decrypt the captured signals without prior access to an encryption seed.

1) Known Plaintext Attack: In cryptanalysis, it is assumed that an attacker can take some pairs of the plaintext and its encrypted data, i.e., cipher text. In this case, the attacker can obtain secret information such as an encryption seed by analyzing correlation between them. This problem can happen in our scenario if the EFC has prior knowledge about the target state. Comparing the captured signals (cipher text) from the activated sensors with the known target state (plaintext), the EFC can immediately know the group assignment of sensors and their individual encryption seeds. However, such an attempt to attack becomes in vain in our scheme, because each sensor update its encryption seed in every reporting session based on its instantaneous MCG, which is purely random and independent in each session. Even if the EFC obtains all the encryption seeds for activated sensors in a certain time period, they are disposable ones that are useless in the next reporting session. Thus, it is impossible for the EFC to predict which sensors will be activated and how the sensors will encrypt their measurements in the next

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

reporting session.

2) Brute Force Attack: Assuming that *K* sensors are activated in a certain reporting session, there are no more than 2^K group assignments in our scheme. In this case, the EFC can try a brute force attack that checks all possible group assignments and figures out which one is highly likely. Then the Eve can deduce the target state. However, it can be easily showed that the two probabilities for the *i* -th sensor to be involved in flipping and nonffipping groups are the same under the condition, and 2^K group assignments are equally likely (see Appendix A). This is attributed by the following facts: a) the captured signals at the EFC are delivered through the eavesdropping channel that is independent of the main channel, and b) the activation probabilities are decided to be equal. Therefore, even though the EFC can consider all the possible group assignments for a small *K*, the Eve is unable to recognize which sensors are in the flipping or non flipping groups.

IV SIMULATION RESULTS

Using the above equation the packets, no. of nodes and SNR ratio are calculated and result are produced using ns-2 comparison with previous research gives void of good and efficient result

1. Packet Delivery Ratio: Gives the ratio of successfully delivered packets

$$PDR = \frac{No.of\ packets\ deliverd}{Time}$$

2. Packet loss Ratio: Gives the loss occurred in the data transmission inside the network.

$$PLR = \frac{No.of\ sent - No.of\ Recieved}{Time}$$

3. Delay: It is the delay occurred during a packet transmission

$$Delay = packet\ sent\ time - received\ time$$

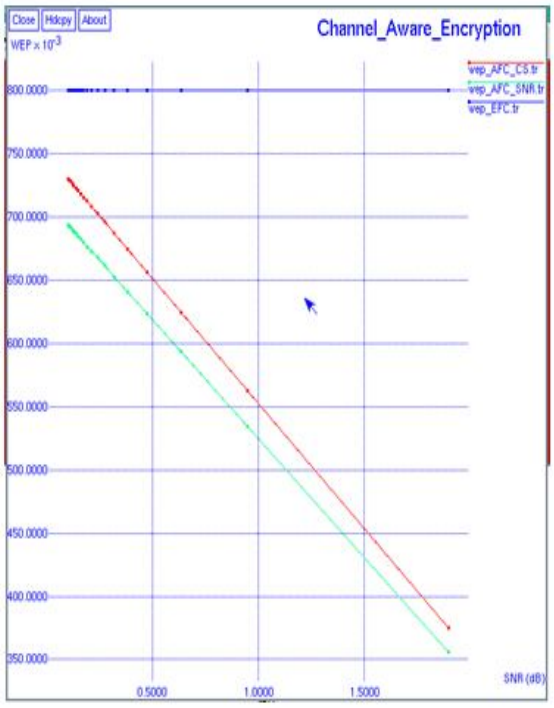

FIG 3: Packet Delivery Ratio

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

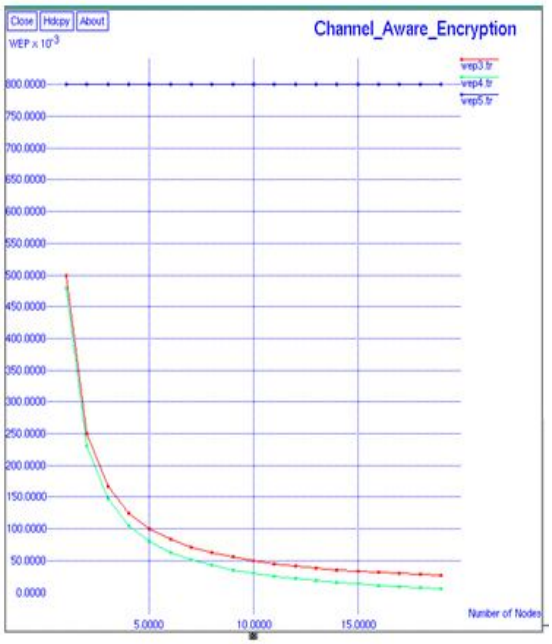

FIG 4: Packet loss Ratio

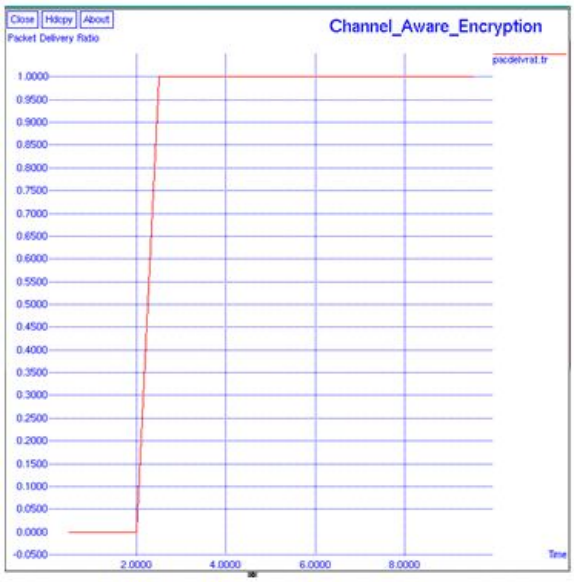

FIG 5: Delay

V. CONCLUSION

In this paper, we studied a physical layer security for data confidentiality which is tailored to wireless sensors suffering from limited resources in a distributed detection scenario. In particular, for a WSN where sensors report their binary local decisions over a PAC, we showed that by carefully utilizing a free natural resource, i.e., randomness of wireless channels, it is possible to make the EFC totally ignorant of the target state, i.e., perfect secrecy.

The claim was thoroughly proved by information-theoretic point of view and also confirmed by performing numerical evaluations. For the performance evaluations, we designed the proposed scheme with an energy efficient modulation technique, NC-BFSK and the fusion rules with channel statistics and the high SNR approximation at the AFC for which performances are evaluated in terms of WEP at various SNR values and sizes of WSN. The evaluation verified that the proposed scheme results in a WEP of 0.5 at the EFC for perfect secrecy.

In addition to the confidentiality, the reliability, i.e., WEPs at the AFC of the proposed scheme were evaluated and compared with those of a conventional scheme in which the data confidentiality is implemented by introducing intentional errors in the physical layer. The comparisons showed that the proposed scheme can achieve perfect secrecy while maintaining superior WEP performances across wide ranges of SNR values and sizes of WSN. We believe that this work paves a new dimension to develop an energy efficient security system by utilizing natural resources in WSNs.

REFERENCES

[1] X. Chen, K. Makki, K. Yen, and N. Pissinou, "Sensor network security: A survey," *Commun. Surveys Tuts., vol.* 11, no. 2, pp. 52-73, Second Quarter, 2009.

[2] H. Jeon, D. Hwang, J. Choi, H. Lee, and J. Ha, "Secure type-based multiple access," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 763-774, Sep. 2011.

[3] T. C. Aysal and K. E. Barner, "Sensor data cryptography in wireless sensor networks," *IEEE Trans. Inf. Forensics Security*, vol. 3, no.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

An ISO 3297: 2007 Certified Organization *Vol. 3, Special Issue 3, April 2014*

International Conference on Signal Processing, Embedded System and Communication Technologies and their applications for Sustainable and Renewable Energy (ICSECSRE '14)

Organized by

Department of ECE, Aarupadai Veedu Institute of Technology, Vinayaka Missions University,

Paiyanoor-603 104, Tamil Nadu, India

2, pp. 273-289, Jun. 2008.

[4] V. Nadendla, "Secure Distributed Detection in Wireless Sensor Networks via Encryption of Sensor Decision," M.S. thesis, Louisiana State University and Agricultural and Mechanical College, Baton Rouge, LA, USA, 2009.

[5] S. Marano, V. Matta, and P. K. Willett, "Distributed detection with censoring sensors under physical layer secrecy," *IEEE Trans. Signal Process., vol.* 57, no. 5, pp. 1976-1986, May 2009.

[6] J. Polastre, R. Szewczyk, C. Sharp, and D. Culler, The Mote Revolution: Low Power Wireless Sensor Network Devices Sep. 2004 [Online]. Available: http://webs.cs.berkeley.edu/papers/hotchips-2004-motes.ppt

[8] J. Abouei, K. N. Plataniotis, and S. Pasupathy, "Green modulation in dense wireless sensor networks," in *Proc. IEEE ICASSP 2010*, Dallas, TX, USA, Mar. 2010.

[9] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. I*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[10] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339-348, May 1978.

[11] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451-456, Jul. 1978.

[12] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687-4698, Oct. 2008.

[13] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2470-2492, Jun. 2008.

[14] M. Bloch, J. Bums, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515-2534, Jun. 2008.

[15] H. Jeon, N. Kim, J. Choi, H. Lee, and J. Ha, "Bounds on secrecy capacity over correlated ergodic fading channels at high SNR," *IEEE Trans. Inf. Theory*, vol. 59, no. 3, pp. 1975-1983, Mar. 2011.

[16] M. Bloch and J. Bums, *Physical-Layer Security: From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.

[17] Y. Liu, S. C. Draper, and A. M. Sayeed, "Exploiting channel diversity in secret key generation from multipath fading randomness," IEEE *Trans. Inf Forensics Security, vol.* 7, no. 5, pp. 1484-1497, Oct. 2012.

[18] J. Wallace and R. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf Forensics Security, vol.* 5, no. 3, pp. 381-392, Sep. 2010.

[19] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security, vol.* 5, no. 2, pp. 240-254, Jun. 2010.

[20] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Trans. Inf. Forensics Security*, vol. 2, no. 3, pp. 364-375, Sep. 2007.

[21] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776-3784, Nov. 2005.

[22] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52-55, Feb. 2000.

[23] L. Lai and H. E. Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf Theory*, vol. 54, no. 9, pp. 4005-4019, Sep. 2008.

[24] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," IEEE *Trans. Signal Process.*, vol. 58, no. 3, pp. 1875-1888, Mar. 2010.

[25] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf Theory*, vol. 54, no. 9, pp. 4005-4019, Aug. 2010.

[26] E. Ekrem and S. Ulukus, "Secrecy in cooperative relay broadcast channels," *IEEE Trans. Inf Theory, vol. 57*, no. 1, pp. 137-155, Jun. 2011.

[27] N. Chang, C. Chae, J. Ha, and J. Kang, "Secrecy rate for MISO Rayleigh fading channels with relative distance of eavesdropper," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1408-1411, Sep. 2012.

[28] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," IEEE *Commun. Lett.*, vol. 14, no. 10, pp. 885-887, Oct. 2010.