J. Sustain. Wireless Syst., vol. 03, no. 2, pp. 59-67
https://doi.org/10.36548/jsws.2021.2.001

Physical Layer Protection Against Sensor Eavesdropper Channels in Wireless Sensor Networks

Dr. Abul Bashar,
Department of Computer Engineering,
Prince Mohammad Bin Fahd University,
Kingdom of Saudi Arabia.
Email: abashar@pmu.edu.sa

Dr. S. Smys,
Professor,
Department of Computer Science and Engineering,
RVS Technical Campus,
Coimbatore, India.
Email: smys375@gmail.com

Abstract: This paper presents an analysis of Wireless Sensor Network (WSN) security issues that take place due to eavesdropping. The sensor-eavesdropper channels and the sensor sinks are exposed to generalized K-fading. Based on the physical layer security framework we use cumulative distribution, optimal sensors and round robin scheduling scheme to decrease the probability of interception and to equip secure connection between the nodes. For identifying the interception probability, a novel analytical methodology is present with simple analytical expressions. Moreover, diversity orders of scheduling schemes and asymptotic closed-form expressions are evaluated. Numerical results show the crucial result of shadowing and fading parameters of wiretap and main links, selected schemes on WSN security and network size. We have analyzed the output using Monte Carlo simulation and conclusions show the validation of the proposed work.

Keywords: Wireless Sensor Network; Scheduling Schemes; Physical layer security; Intercept probability

ISSN: 2582-3167
Submitted: 20.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 3.06.2021

1. Introduction

Over the years, there are a number of military applications in which the wireless sensor networks are incorporated. Moreover, because of the scalability, flexibility, low operating costs and installation costs, the WSNs [1] are also used in a number of new techniques such as Industry 4.0, Smart Grid and Internet of Things, etc. When communication takes place by means of an open radio channel, using spatially distributed sensors, it becomes vulnerable to attacks by third-party users by means of eavesdropping. The battery life of the sensor nodes is limited which makes it not practical to use cryptographic techniques [2] which consumes a large amount of energy to protect the sensor node from attacks. The traditional cryptographic techniques are based on the assumption that takes into consideration of the eavesdropper's ability [3]. Brute-force attack [4] was later on used to determine the strength of the cryptographic method. Hence along with typical data encryption, we also propose the use of physical layer security. This layer shows a simple methodology that can be used as an additional layer of protection by using the characteristics of mediums like noise, shadowing and fading [5]. In a number of published papers that have been observed so far wiretap model that describes relationship between destination source and eavesdropper based on fading channels were analysed in [6]. Similarly Alice Bob Eve model that uses fading channels off α-μ is also investigated in [7].

Similarly the authors in [8] study the performance of Wyner's system model. The secure outage probability and secrecy capacity of wiretap channels the take into to consideration and excess disturbance such as shadowing effect was analysed in [9]. Analysis is completed based on the assumption of gamma distribution and their distribution. This methodology is also used to investigate security issues in fading channels of k distribution. Different diversity techniques, conventional relay selection, cooperative relaying an artificial noise approach have been implemented resulting in improved privacy of downlink wiretap networks in an effective manner [10]. However the major disadvantages of these methodologies are higher system complexity as well as excessive energy resources requirement. Based on the characteristics of the sensors with respect to power constrained transmission the proposed physical layer security [11] is incorporated and is deemed to be inflexible when used for WSN.

ISSN: 2582-3167
Submitted: 20.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 3.06.2021

Based on the review of literature work on PLS in WSN there are not many solutions that point to less consumption of energy. In [12], an optimal sensor scheduling is executed wherein the probability of interception of the messages is reduced significantly when compared with other benchmark methods such as round Robin scheduling scheme. In this methodology a scenario of m fading environment is built to obtain the asymptotic and exact expressions in the form of integrals. This methodology involved an estimation of rate of sensor sink channel to determine the best choice of transmitting the message in a secure manner while eliminating the sensor sink links that are affected during the process. However this methodology had a downfall in terms of energy consumption in a wireless sensor network. In order to overcome this disadvantage we have incorporated a cumulated distribution function that is used to schedule secure transmission of message using an optimal scheduling framework. This methodology is mainly used in [13] to choose the apt active downlink users. It is preferred because of its qualitative fairness when compared with other similar scheduling methodologies. Based on this detailed study we propose to analyse PLS in WSN using multiple sensors attack [14] through eavesdropping and the observed results are also recorded. This paper is organised such that the following section gives a detailed outline of the proposed PLS methodology problem formulation. Section 3 outlines evaluation of probability of intersection and the results obtained via simulation using Monte Carlo is shown in section 4. Based on the observed results, a conclusion is drawn in section 5.

2. Problem Formulation

A WSN that holds N sensors (each built with a single antenna) and one sink is represented in Fig.1 where the dashed lines represent wiretap channels and the solid lines represent main channels. The main sensor is the sink and the other sensors use orthogonal multiple access to communicate with the sink. In general the sensor which holds maximum data throughput is given access to communicate with the sink, respective of the effect of attacks, such that the channel capacity is maximized. In this methodology we have incorporated PLS in WSN using several scheduling methods. Based on the availability of wiretap and main channels with their channel state information analysis can be made. As the eavesdropper could be a WSN user who has restricted access to private data, this assumption is quite reasonable. However, we should take into consideration, the different data types are sensed by the sensors and their respective data streams should hold a higher priority during

ISSN: 2582-3167
Submitted: 20.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 3.06.2021

transmitting the data. While operating, certain service requirements hold a higher priority when compared to others. However, due to constraint of execution, this factor is not considered in this paper and is left for further research work. The signal to noise ratio SNR is observed such that

$$\gamma_{si} = \frac{|h_{si}|^2 P_a}{\sigma_{si}^2}, a = 1, \ldots, N$$

Where P_a denotes the power transmission and σ_{si}^2 denotes variance value with white Gaussian noise as an additive. h_{si} is a fading coefficient between the sink and the a[th] sensor. Based on Shannon capacity formula, we can determine the channel capacity of the a[th] main link using the expression:

$$R_{si} = log_2(1 + \gamma_{si})$$

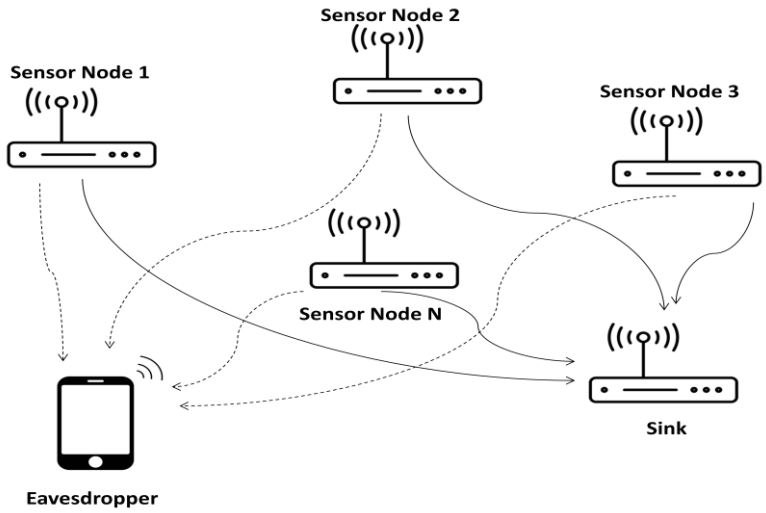

Fig.1. System Model with Eavesdropper to Intercept the Transmission

For an eavesdropper, the SNR can be expressed as

$$\gamma_{ei} = \frac{|h_{ei}|^2 P_a}{\sigma_{ei}^2}, a = 1, \ldots, N$$

ISSN: 2582-3167
Submitted: 20.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 3.06.2021

With the fading coefficient, power transmission and variance denoting that of the eavesdropper while the channel capacity can be represented as

$$R_{ei} = log_2(1 + \gamma_{ei})$$

3. Determining the Intercept Probability

In this paper, we consider the a[th] sensor to transmit signal with a maximum achievable rate R_{si}. Accordingly, one can calculate the probability of interception using the formula given below:

$$P_{int}^{i} = \Pr\left[C_{secrecy}^{i} < 0\right] = \Pr\left[R_{si} < R_{ei}\right]$$

On substituting the values of the previous expressions,

$$P_{int}^{i} = \Pr[\gamma_{si} < \gamma_{ei}]$$

$$= \int_0^{\infty} \int_0^{\gamma_{ei}} P_{\gamma_{si}}(\gamma_{si}) P_{\gamma_{ei}}(\gamma_{ei}) d\gamma_{si} d\gamma_{ei}$$

Every node present in the WSN are exposed to GK fading and the corresponding probability density function can be expressed as follows:

$$P_{\gamma_{ei}}(x) = 2 \frac{x^{\frac{m_a + k_j - 2}{2}}}{\Gamma(m_a)\Gamma(k_a)} \left(\frac{m_a k_a}{\gamma_a}\right) K_{m_a - k_a}[2(\frac{m_a + k_j - 2}{\gamma_a})]^{1/2}$$

Secrecy capacity is defined as the difference between wiretap channel capacity and legitimate main channel capacity. In case of a non-positive secrecy, it is possible for the eavesdropper to intercept the transmitted message successfully. For a high average metric value, asymptotic probability is used such that when compared with the other methodologies, it gives a practical and quick insight to the various risks faced by the system.

ISSN: 2582-3167
Submitted: 20.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 3.06.2021

4. Results and Discussion

Analytical results are carried out using Matlab simulation and the value of P_a is estimated with a total of 10^8 sample set such that Fig.2 shows the environment of identically distributed shadowing/ fading environment and the intercept probability of the different schemes used.

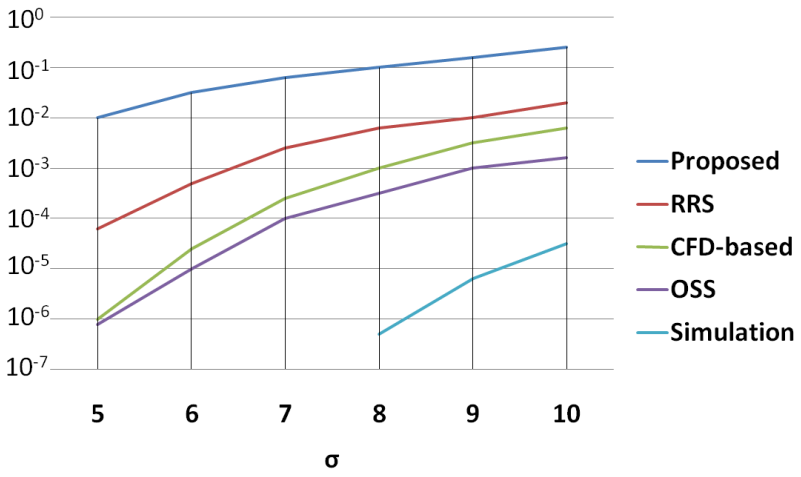

Fig.2. Intercept probability Vs. Fading and Shadowing shaping parameters in identically distributed links

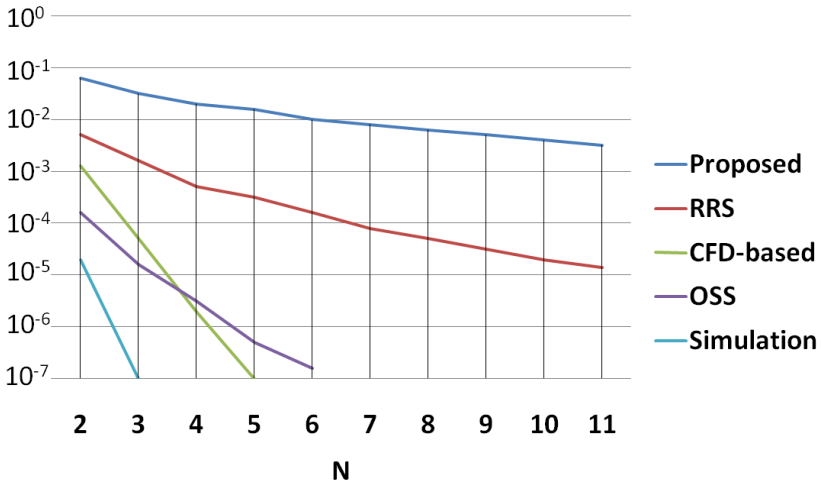

Fig.3. Intercept probability with respect to various wiretap links based shadowing methods

ISSN: 2582-3167
Submitted: 20.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 3.06.2021

Fig.3 shows the output of the intercept probability with respect to the different methods of shadowing condition with respect to presence of wiretap links. It indicates that the intercept probability of RSS is found to be independent of the dimension of the network

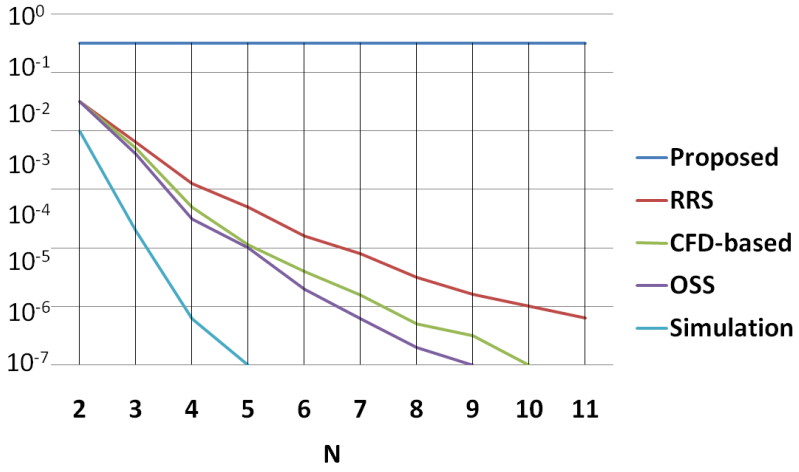

Fig.4. Intercept probability with respect to the different dimensions of the proposed methodology

Fig.4 shows the intercept probability of the WSN network when there are different dimensions involved.

5. Conclusion

In this paper, we have introduced a physical layer in the WSN that operates using different scheduling schemes. On analysis of these schemes and its implementation, we have obtained the intercept probability express that is general and can be used with various shadowing/fading scenarios. The simulation results indicate that the asymptotic results are well matched with the outputs obtained for WSNs that are of smaller dimensions. Similarly, the scheduling policy for diversity order is also determined. Experimental analysis indicates that favorable wiretap/main channel conditions will tend to decrement the interception probability. Of the four schemes developed, the OSS scheduling policy shows the most optimal output. However, since the battery life of the sensor was restricted in the WSN, the CDF-based scheduling methodology is preferred over the OSS scheduling resulting in a tradeoff between fairness and reasonable intercept probability in the nodes of the network.

ISSN: 2582-3167
Submitted: 20.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 3.06.2021

Moreover, under the conditions of distributed fading channels, it was observed that both the OSS scheduling as well as CDF scheduling resulted in the same order of diversity. The later was found to be sensitive on wiretap channel in comparison with the former scheduling methodology. However, the OSS scheduling framework was found to be very sensitive to the size of the network.

References

[1] López, J., & Zhou, J. (Eds.). (2008). *Wireless sensor network security* (Vol. 1). Ios Press.

[2] Viani, F., Oliveri, G., Donelli, M., Lizzi, L., Rocca, P., & Massa, A. (2010, September). WSN-based solutions for security and surveillance. In *The 40th European Microwave Conference* (pp. 1762-1765). IEEE.

[3] Deng, Y., Wang, L., Elkashlan, M., Nallanathan, A., & Mallik, R. K. (2016). Physical layer security in three-tier wireless sensor networks: A stochastic geometry approach. *IEEE Transactions on Information Forensics and Security*, *11*(6), 1128-1138.

[4] Yılmaz, M. H., & Arslan, H. (2015, October). A survey: Spoofing attacks in physical layer security. In *2015 IEEE 40th Local Computer Networks Conference Workshops (LCN Workshops)* (pp. 812-817). IEEE.

[5] Rohokale, V. M., Prasad, N. R., & Prasad, R. (2012, September). Cooperative jamming for physical layer security in wireless sensor networks. In *The 15th International Symposium on Wireless Personal Multimedia Communications* (pp. 458-462). IEEE.

[6] Senthilkumar, M., Kavitha, V. R., Kumar, M. S., Raj, P. A. C., & Shirley, D. R. A. (2021, March). Routing in a Wireless Sensor Network using a Hybrid Algorithm to Improve the Lifetime of the Nodes. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1084, No. 1, p. 012051). IOP Publishing.

[7] Chopra, R., Murthy, C. R., & Annavajjala, R. (2019). Physical layer security in wireless sensor networks using distributed co-phasing. *IEEE Transactions on Information Forensics and Security*, *14*(10), 2662-2675.

ISSN: 2582-3167
Submitted: 20.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 3.06.2021

[8] Gupta, M., Singh, P., & Rani, S. (2015). Optimizing physical layer energy consumption for reliable communication in multi-hop wireless sensor networks. *Indian Journal of Science and Technology*, *8*(13), 1-7.

[9] Chen, J. I. Z., & Smys, S. (2020). Social Multimedia Security and Suspicious Activity Detection in SDN using Hybrid Deep Learning Technique. *Journal of Information Technology*, *2*(02), 108-115.

[10] Barua, M. P., & Indora, M. S. (2013). Overview of security threats in WSN. *vol*, *2*, 422-426.

[11] Tayebi, A., Berber, S., & Swain, A. (2018). Security enhancement of fix chaotic-DSSS in WSNs. *IEEE Communications Letters*, *22*(4), 816-819.

[12] Wen, H. (2013). *Physical layer approaches for securing wireless communication systems*. Springer Science & Business Media.

[13] Bashar, A. (2020). Sensor cloud based architecture with efficient data computation and security implantation for Internet of Things application. *Journal of ISMAC*, *2*(02), 96-105.

[14] Jacob, I. J., & Darney, P. E. (2021). Artificial Bee Colony Optimization Algorithm for Enhancing Routing in Wireless Networks. *Journal of Artificial Intelligence*, *3*(01), 62-71.

ISSN: 2582-3167
Submitted: 20.04.2021
Revised: 12.05.2021
Accepted: 28.05.2021
Published: 3.06.2021