International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 21 Issue 1 – APRIL 2016.

SECURITY AGAINST EAVESDROPPING ATTACK IN INDUSTRIAL WIRELESS SENSOR NETWORK

A.GIRIJA
PG Scholar
Arunai Engineering College
Tiruvannamalai
girijaramya55@gmail.com

Mrs.K.YOGITHA,M.E.,
Asst.Professor
Arunai Engineering College
Tiruvannamalai

***Abstract*- The broadcast natural world of the wireless medium creates the communication over this medium susceptible to eavesdropping. This project studies the intercept behavior of an industrial wireless sensor network (IWSN) comprising of a sink node and several sensors in the occurrence of an eavesdropping attacker, where the sensors convey their sensed data to the sink node over wireless links. Due to the broadcast nature of radio wave propagation, the wireless transmission from the sensors to the sink can be eagerly overheard by the eavesdropper for interception purposes. In an information-theoretic sense, the privacy capacity of the wireless transmission is the difference between the channel capacity of the main link (from sensor to sink) to the wiretap link (from sensor to eavesdropper). The conventional round robin scheduling and optimal sensor scheduling scheme is used for protected data broadcast process. Here multiple antennas are used for secure data transmission.**

***Index Terms*- Intercept behavior, industrial wireless sensor networks, sensor scheduling, intercept probability.**

I.INTRODUCTION

Wireless networks have gained much popularity because of the broadcast nature of the wireless medium, which makes it effortlessly accessible. However, this ease of accessibility also makes it simple to overhear communication above this medium, thus raise privacy concern. Privacy problems involve three nodes; transmitter, receiver and an eavesdropper. We believe the problem of secret communication from the transmitter to the receiver, over a wireless medium, where a eavesdropper may be present.

Wireless communications have enabled the development of low-cost and low-power WSNs. WSNs have many potential application and unique challenges. They usually are heterogeneous systems contain many small plans, called sensor nodes, that monitor different environments in cooperative; i.e. sensors cooperate to each additional and arrange their local data to arrive at a global view of the environment; sensor nodes also can operate autonomously.

WSNs are vulnerable to several types of attacks and due to dangerous and unconfident nature of communication channel, un-trusted and broadcast communication media, deployment in aggressive environments, automatic nature and restricted possessions, most of security technique of traditional networks are impracticable in WSNs; therefore, security is a very important and difficult requirement for this network. It is essential to design a suitable security mechanism for these networks.

A wireless sensor network (WSN) in its simplest structure can be defined as a network of plans denoted as nodes to sense the atmosphere and communicate the information gather from the monitor field through wireless links, the information is forwarded, probably via several hops relaying to a sink that can use it locally or is connected to additional networks (e.g.., the internet) through a gateway.

Multifunctional wireless sensor nodes are a development brought about by latest advancement in wireless communications and electronics [1]. These sensor nodes are small in size and communicate unrestrictedly over small distances. They have sensing, information processing and communication capability and their features have enabled, as well as provide, impetus to the design of Wireless Sensor Networks (WSNs). WSNs are authoritative in that they are satisfying to carry a lot of real world applications that differ significantly in terms of their necessities and individuality.

Networks of sensors exist in lots of industrial applications provide the capability to monitor and control the environment in real-time. The majorities of these networks, however, is wired and as a outcomes are expensive to fix and maintain. To lower the system and infrastructure costs wireless solutions can be use [2]. Wireless solution have additional benefits in manufacturing applications such as improved physical mobility, reduced hazard of breaking cables, less hassle with connectors and simplicity of upgrading [3].

The troubles of cryptography and privacy systems supply an attractive application of communication theory. In this paper a theory of privacy systems is developed. The approach is on a hypothetical level and is planned to complement the treatment found in typical mechanism on cryptography [4].

More basic to the plan of sensor networks, however, is to sensor nodes have a severely inhibited energy allocation due to the restricted power supply from batteries and as a result energy-efficiency is the mainly important figure of merit in WSNs [5]. Internal power source help to remove the need for wires to the nodes and authorize bigger mobility. Part of the present vision for WSNs is to have sensor nodes to final forever with no external power sources or having to change their batteries.

The authors of [6] and [7] investigate the relay selection for wireless security enhancement, where the relay node that can realize the maximum privacy against eavesdropping is selected as the “greatest” relay to support the source-destination transmissions. Although the relay selection studied in [6] and [7] improve the wireless physical-layer security, it relies on extra relay nodes and requires difficult synchronization among spatially spread relays, resulting in additional system complexity.

The artificial noise method be devise in [8]-[9] to increase wireless security by generate a sophisticatedly-designed artificial noise for confuse the eavesdropper only without affecting the rightful destination. This, however, costs other energy resources for the artificial noise generation, compare to the sensor scheduling, where a sensor with the highest secrecy against eavesdropping is scheduled for data transmission without consuming any other energy resources. Since wireless sensors are generally powered with restricted batteries, the energy becomes one of the most valuable resources in industrial WSNs, which makes the sensor scheduling smarter than the conventional artificial noise method from the energy saving perspective.

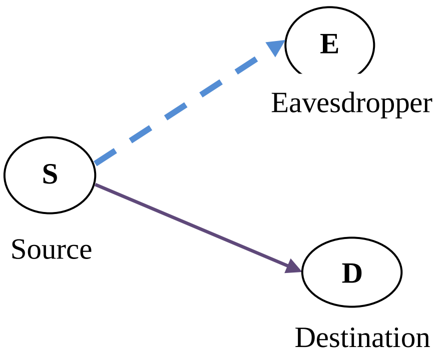

Fig.1. A wireless network consists of source (S) and destination (D) in the presence of an eavesdropper (E).

The remainder of this article is ready as follows. Section II describes sensor scheduling while in Section III we propose a optimal sensor scheduling with multiple antenna system. In Section IV, we provide simulation results and show that the performance of multiple antenna system is better than the single antenna due to the throughput, delay and energy loss. At last, Section V presents our concluding remarks.

II. SENSOR SCHEDULING

Conventional Round-Robin Scheduling

For comparison purposes, let us first examine the conventional round-robin scheduling as a benchmark, where N sensors get turns in accessing a known channel and thus every sensor has an equal chance to transmit its sensed data to the sink. Without any loss of generality, we consider that iss_i scheduled to transmit its signal x_i((|x_i|2) = 1) with power $P_i$and rateR_i, whereR_i is specified to the maximum achievable rate (also known as the channel capacity) from $s_i$to the sink, which guarantees that the ergodic ability is achieve by the rightful transmission.

It needs to be pointed out that the sensed information xi could be various types of data for various sensors. For example, the Nsensors of Fig. 2 may be used to sense and monitor various aspects of an industrial plant environment, including the machine motion, temperature, moisture, pressure, and so on. The sensor data might be obtained by exploiting the collaboration between multiple sensors for distributed state estimation [10]-[11].

Thus, we can express the received signal at sink as

$$y_s = \sqrt{p_i}\, h_{is}\, x_i + n_s, \qquad (1)$$

Where $h_{is}$is a fading coefficient of the main channel from $s_i$to the sink andn_s. We can obtain the channel capacity of main link from $s_i$to sink as

$$C_s\ (i) = \log_2\left(1 + \frac{|h_{is}|^2 P_i}{N_0}\right), \qquad (2)$$

The signal overheard at eavesdropper $e$is given by

$$y_e = \sqrt{p_i}\, h_{is}\, x_i + n_e\ , \qquad (3)$$

Where h_{ie} a fading coefficient of the wiretap is channel from s_i to the eavesdropper and $n_e$represents the zero-mean AWGN with varianceN_0. Using (3), we can similarly obtain the channel capacity of wiretap link from si to eavesdropper e as

$$C_e(i) = \log_2\left(1 + \frac{|h_{ie}|^2 P_i}{N_0}\right). \qquad (4)$$

The secrecy capacity is the difference between the channel capacity of main link to the wiretap link. Therefore, in the presence of eavesdropping attack, the secrecy capacity of wireless transmission from $si$to sink can be obtained as

$$C_{secrecy}(i) = C_s\ (i) - C_e(i) \qquad (5)$$

Where $C_S(i)$and $C_e(i)$ are given by (2) and (4), respectively.

III. SYSTEM MODEL

Let us now present our system model. Consider the wireless scenario of Fig. 1 consisting of a S, D and E, where the solid and dashed lines represent the S-D main link and SE respectively. Observe that the system model of Fig.1 is appropriate to diverse suitable wireless systems, as well as the family of wireless local area networks (WLAN), wireless sensor networks (WSN), cellular networks, mobile ad-hoc networks (MANETs) and so on.

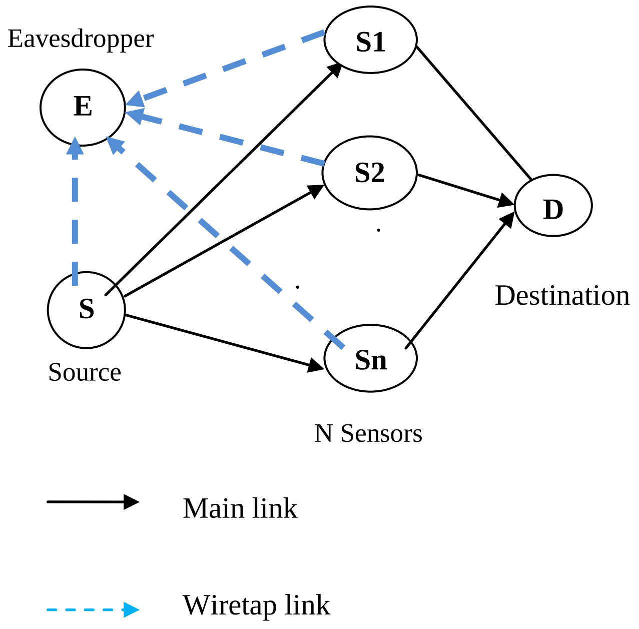

Fig.2. A wireless network consists of one source (S), one destination (D) and N sensors in the presence of an eavesdropper (E).

As shown in Fig. 2, we consider an industrial WSN consisting of a sink node and Nsensors in the presence of an eavesdropper, where all nodes are assumed by means of single antenna and the solid and dash lines stand for the main link and wiretap link, correspondingly. Note that the eavesdropper of Fig. 1 can be either an illegitimate user or a legitimate user who is interest in tapping additional users' data information. Notational convenience, Nsensors are denoted by S= $\{s_i|i= 1, 2, \cdots,\}$. As illustrated in Fig. 2, the presence of machinery obstacle, metallic frictions and engine sensations in industrial environments is aggressive to the radio propagation, which makes the wireless fading vary drastically.

A. Proposed Optimal Sensor Scheduling

This subsection presents an optimal sensor scheduling scheme to increase the secrecy capability of the rightful transmission. Naturally, a sensor with the maximum secrecy capability should be chosen and scheduled to transmit its information to the sink. Hence, from (5), the optimal sensor scheduling principle is given by

$$\text{Optimal User} = \arg\max_{i\in S} C_{secrecy}(i)$$

$$= \arg\max_{i\in S} \frac{1+\frac{|h_{is}|^2 P_i}{N_0}}{1+\frac{|h_{ie}|^2 P_i}{N_0}}, \qquad (6)$$

Where S represents the set of N sensors. It is observed from (6) to the channel state information (CSI) (i.e., $|h_{is}|^2$and$|h_{ie}|^2$) of each sensor is required for determining the optimal sensor, which can be obtain by using classic channel estimation methods [12]-[13]. More specifically, every sensor may first calculate approximately its own CSI through channel estimation and then transmits the predictable CSI to the sink. After collect all the sensors' CSI, the sink can willingly find out the optimal sensor and inform the entire network. Thus, in the occurrence of an eavesdropper, the secrecy capacity of rightful transmissions relying on the proposed sensor scheduling system can be obtained from (6) as

$$C_{secrecy}^{proposed} = \max_{i\in S} \log_2\left(\frac{1+\frac{|h_{is}|^2 P_i}{N_0}}{1+\frac{|h_{ie}|^2 P_i}{N_0}}\right). \qquad (7)$$

B. Multiple Antennas System

The multiple antennas offer a receiver more than a few observations of the same signal. Each antenna wills knowledge a various interfering environment. Thus, if one antenna is experience a deep fade, it is likely that one additional has a adequate signal. Collectively such a system can offer a robust link. While this is primarily seen in receiving systems, the analog has also verified valuable for transmitting systems as well. Typically, however, signal dependability is paramount and using multiple antennas is an well-organized way to reduce the number of drop-outs and lost connections. The multipath transmission is used for secure data transmission.

IV. RESULT AND DISCUSSIONS

In this section, the proposed multiple antennas system outperforms the single antenna.

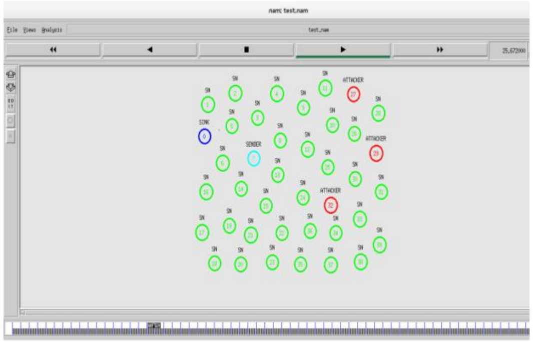

Fig.3. Identification of Attacker Node

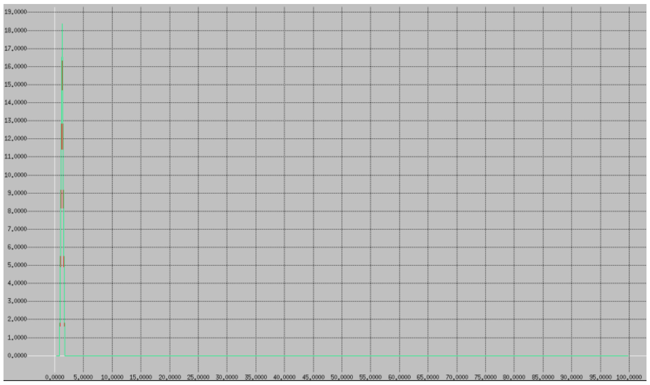

Fig.4. Throughput versus Time

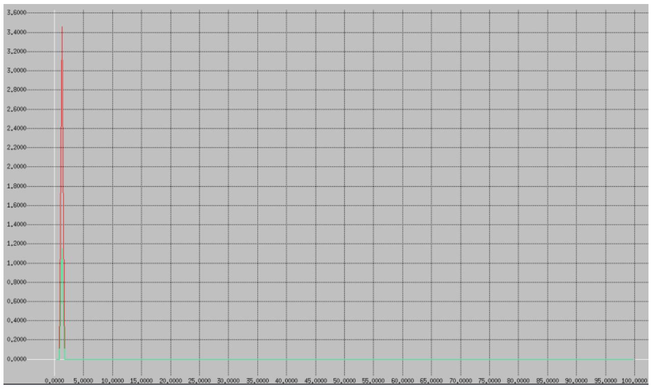

Fig.5. Delay versus Time

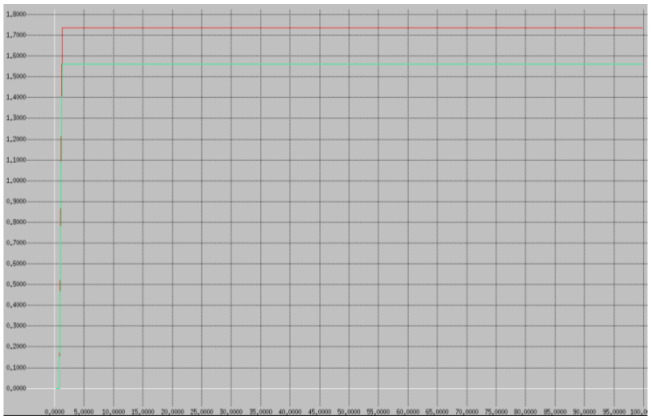

Fig.6. Energy versus Time

In the above figures shows, red line represents the single antenna and green line represents the multiple antenna. In multiple antennas system throughput, delay and power are less compare to single antenna.

V. CONCLUSION

In this paper, we investigated the proposed an optimal sensor scheduling scheme, aiming at maximize the secrecy capability of wireless transmissions from sensors to the sink and the use of sensor scheduling to improve the physical-layer safety of industrial WSNs against the eavesdropping attack. In the present paper, we examined the multiple-antenna case, where each network node is equipped with the multiple antennas and the performance of the multiple antenna system is higher than the single antenna due its throughput, delay and energy. In future we will extend the results of this paper to use Markov chain of real-world processes.

REFERENCES

[1] Norton Corporation, “The 2012 Norton cybercrime report,” Sept. 2012, available on-line at http://www.norton.com/2012cybercrimereport.

[2] M. E. Hellman, “An overview of public key cryptography,” *IEEE Commun. Mag.*, vol. 16, no. 6, pp. 42-49, May 2002.

[3] S. V. Kartalopoulos, ”A primer on cryptography in communications,” *IEEE Commun. Mag.*, vol. 20, no. 4, pp. 146-151, Apr. 2006.

[4] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[5] Q. Chi, H. Yan, C. Zhang, Z. Pang, and L. Xu, “A reconfigurable smart sensor interface for industrial WSN in IoT environment ,” *IEEE Trans.Industrial Informatics*, vol. 10, no. 2, pp. 1417-1425 , May 2014.

[6] W. Shen, T. Zhang, F. Barac, and M. Gidlund, “PriorityMAC: A priorityenhanced MAC protocol for critical traffic in industrial wireless sensor and actuator networks,” *IEEE Trans. Industrial Informatics*, vol. 10, no. 1, pp. 824-835, Feb. 2014.

[7] J.-C. Wang, C.-H.Lin, E. Siahaan, B.-W.Chen, and H.-L. Chuang, “Mixed sound event verification on wireless sensor network for home automation,” *IEEE Trans. Industrial Informatics*, vol. 10, no. 1, pp. 803-812, Feb. 2014.

[8] R. C. Luo and O. Chen, “Mobile sensor node deployment and asynchronous power management for wireless sensor networks,” *IEEE Trans.Industrial Electronics*, vol. 59, no. 5, pp. 2377-2385, May 2012.

[9] N. Marchenko, T. Andre, G. Brandner, W. Masood, and C. Bettstetter, “An experimental study of selective cooperative relaying in industrial wireless sensor networks,” *IEEE Trans. Industrial Informatics*, vol. 10,no. 3, pp. 1806-1816, Aug. 2014.

[10] O. Kreibich, J. Neuzil, and R. Smid, “Quality-based multiple-sensor fusion in an industrial wireless sensor network for MCM,” *IEEE Trans.Industrial Electronics*, vol. 61, no. 9, pp. 4903-4911, Sept. 2014.

[11] T. M. Chiwewe and G. P. Hancke, “A distributed topology control technique for low interference and energy efficiency in wireless sensor networks,” *IEEE Trans. Industrial Informatics*, vol. 8, no. 1, pp. 11-19, Feb. 2012.

[12] P. T. A. Quang and D.-S.Kim, “Enhancing real-time delivery of gradient routing for industrial wireless sensor networks,” *IEEE Trans. IndustrialInformatics*, vol. 8, no. 1, pp. 61-68, Feb. 2012.

[13] F. Gandino, B. Montrucchio, and M. Rebaudengo, “Key management for static wireless sensor networks with node adding,” *IEEE Trans.Industrial Informatics*, vol. 10, no. 2, pp. 1133-1143, May 2014.

[14] M. Cheminod, L. Durante, and A. Valenzano, “Review of security issues in industrial networks,” *IEEE Trans. Industrial Informatics*, vol. 9, no. 1, pp. 277-293, Feb. 2013.

[15] Y. Zou, J. Zhu, X. Wang, and V. Leung, “Improving physical-layer security in wireless communications using diversity techniques,” *IEEENetwork*, vol. 29, no. 1, pp. 42-48, Jan. 2015.

[16] C. E. Shannon, “Communication theory of secrecy systems,” *Bell System Technical Journal*, vol. 28, pp. 656-715, 1949.

[17] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355-1387, Aug. 1975.

[18] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wiretap channel,” *IEEE Trans. Information Theory*, vol. 24, pp. 451-456, Jul. 1978.

[19] Y. Zou, X. Wang, and W. Shen, “Optimal relay selection for physicallayer security in cooperative wireless networks,” *IEEE Journal onSelected Areas in Communications*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.

[20] Y. Zou, X. Wang, W. Shen, and L. Hanzo, “Security versus reliability analysis of opportunistic relaying,” *IEEE Trans. Vehicular Technology*, vol. 63, no. 6, pp. 2653-2661, Jun. 2014.