Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack

T.Abilasha[1] , V.Jyothi Lakshmi[2]
[1](PG Student, Electronics and Communication Engineering, Anna University, Dharmapuri, India
2(Asst Professor, Electronics and Communication Engineering, Anna University, Dharmapuri, India

ABSTRACT

This proposed technique introduces a concept of Intercept performance Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack. In this paper it scholarships the intercept action of an industrial wireless sensor network, it includes sink node and multiple sensor. Gradually depending upon the exposed protocols and platforms, the industrial networks are engaged in the IT industry and internet background. By using wireless channel, sensor transmitting the sensed report to the sink node via wireless channels. Radio wave propagation has transmission essence hence wireless transmission from the sensor to the sensor can be eagerly heard by the eavesdropper for interception functions. Maximum industries utilize wireless networks for interacting the information and data, because of huge cable cost. Most of the industries use wireless networks for communicating information and data, due to high cable cost. By seeing this, the wireless networks are insecure, which is important to protect the detracting the instruction and data at the time of transmission. The difference among the main link and wiretap link of the wireless transmission is called secrecy capacity, and this secrecy capacity is used to anticipated the eavesdropper at the time of transmitting the data, if it is intercepted. When the secrecy capacity have etiolate then it considered as a transmitted data is intercepted. Anyhow in all industrial area the existence of machinery obstacles, metallic frictions, and engine vibrations causes the wireless fading variation immensely. This shows the decline of the secrecy capacity. So, to overcome this we are going to introduce a method called optimal sensor scheduling scheme. In this scheme applying optimal sensor scheduling scheme a sensor with highest secrecy capacity is chosen and data is transmitted. Moreover, RC4 encryption and decryption algorithm is enhanced for data while transmission, it protects the data to long time. Also, the examination of asymptotic intercept probability is operated in order to give an inevitable into the impression of the sensor scheduling on the wireless security. Numerical results demonstrate that the proposed sensor scheduling scheme outperforms the conventional round-robin scheduling in terms of the intercept probability. By using this technique we can calculate average distance and time delay of data while transmitting. The advantage of this proposed paper is it provides security password. From this, it is not possible to see the data and also not possible to copy the data from any third person. Hence out data is protected to long extent.

Keywords *– Intercept performance analysis, Eavesdropping Attack, round-robin algorithm, RC5 encryption algorithm, wireless sensor network.*

I. INTRODUCTION

Wireless sensor networks were originally excited by the military for battlefield surveillance[1], and now are further improved for different industrial applications like assembly line monitoring and manufacturing automation for the sake of improving the factory efficiency, reliability, and productivity [2], [3], which are referred to as the industrial WSNs [4]–[6]. In case of industrial applications, the real-time communications between the spatially distributed sensors should satisfy strict security and reliability requirements [7]. The decline of protecting the security and dependability of the sensed information transmissions can affect an outage of the production line, a damage of the factory machine, or even the loss of workers' lives. Moreover, in industrial environments, the machinery obstacles, metallic frictions, engine vibrations, and equipment noise are opposite to the radio propagation and certainly adversely affect the performance of wireless transmissions. In industrial Wireless sensor network WSNs, due to the broadcast nature of radio propagation, the wireless medium is open to be accessed by both authorized and unauthorized users, leading WSNs to be more vulnerable to the eavesdropping attack than wired sensor networks, where communicating nodes are physically connected with wire cables and a node without being connected is unable to access for illegal activities. To be specific, as long as an eavesdropper hides in the industrial WSNs, the legitimate wireless transmissions among the sensors can be readily overheard by the eavesdropper, which may decode its tapped transmissions and violate the confidentiality of the sensors' information

communications [8]. Therefore, it is of importance to investigate the protection of industrial WSNs against the eavesdropping attack. Traditionally, the cryptographic techniques were exploited to protect the wireless communications against eavesdropping, which typically rely on secret keys and can prevent an eavesdropper with limited computational capability from intercepting the data transmission between wireless sensors. However, an eavesdropper with unlimited computing power is still able to crack the encrypted data communications with the aid of exhaustive key search (known as the brute force attack) [9], [10]. Moreover, the secret key distribution and agreement between the wireless sensors exhibit numerous vulnerabilities and further increase the security risk. To this end, physical-layer security is emerging as a promising paradigm for secure communications by exploiting the physical characteristics of wireless channels, which can effectively protect the confidentiality of communication against the eavesdropping attack, even with unlimited computational power

The main improvements of this paper are given as follows. 1) An optimal sensor scheduling method is projected in order to protect the industrial wireless transmission against the eavesdropping attack, where a chosen of greatest secrecy capacity with sensor in order to transmit its sensed information to the sink. The conventional round-robin scheduling is also considered as a benchmark. 2) Closed-form expressions of the intercept probability for the conventional round-robin scheduling and the proposed optimal sensor scheduling schemes are derived in Nakagami fading environments. 3) An asymptotic intercept probability analysis is conducted and the diversity order of the proposed scheduling scheme is shown as the sum of Nakagami shaping factors of the main links from the sensors to the sink. 4) Numerical results show the advantage of the proposed sensor scheduling scheme gives security password and protection from unauthorized person.5) This proposed system helps in the reduction of time and delay at the time of data transmission. By using Round robin algorithm we can calculate the average distance and time delay.

II. BLOCK DIAGRAM

In the industrial WSN, by using orthogonal multiple access method N sensors communicate with the sink, such as the time division multiple access (TDMA) and orthogonal frequency division multiple access (OFDMA). When a sensor (e.g., si) is scheduled to transmit its data to the sink over a channel (e.g., a time slot in TDMA or an OFDM subcarrier in OFDMA), the eavesdropper attempts to intercept the information transmitted from si.

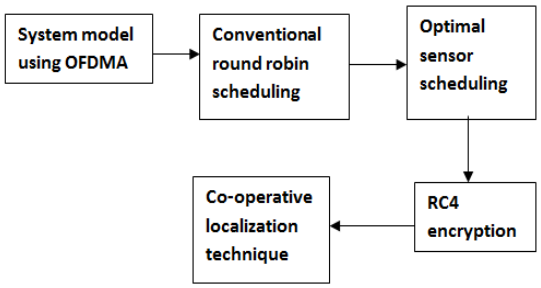

Fig 1, Block diagram of industrial wireless sensor network

Normally, providing an orthogonal channel, chosen of highest data throughput node is done between N sensors to access the given channel and to communicate with the sink, which aims at maximizing the transmission capacity without considering the eavesdropping attack. By modification, concentration of this paper is to developing the wireless physical-layer security with the utility of sensor scheduling. To get meritoriously shield in contradiction of the eavesdropping occurrence, the sensor forecast must take into account the channel state information (CSI) of both the main channel and wiretap channel, differing from the traditional scheduling method, where only the CSI of main channel is considered for the throughput maximization. Assume that the CSIs of both the main channel and wiretap channel are available, which is an assumption commonly used in the physical-layer security.

III SENSOR SCHEDULING USING ROUND ROBIN

In this proposed technique we are using single antena, where each network node is assembled with the single antenna. It is of high interest to extend the results of this paper to a general scenario with multiple antennas for each network node. Also, we don't treated the requirement of QoS in the sensor scheduling, where all the sensors are assumed with the same priority and scheduled for data transmissions solely based on their CSI without considering specific QoS requirements for different sensor data. In practice, some sensors may have

time-critical data with a strict real-time requirement, which should be assigned with a higher priority than the others in accessing the wireless channel. Hence, it is highly necessary to explore the QoS guaranteed sensor scheduling, attempting to improve the wireless security while guaranteeing each sensor's specific QoS requirement. Additionally, due to the channel estimation errors, it is impossible to obtain the perfect CSI knowledge for the sensor scheduling. It is of thus interest to investigate the impact of CSI estimation errors on the intercept performance of sensor scheduling.

IV SYSTEM MODEL USING OFDMA

Industrial wireless sensor network includes a sink node and N sensors in the presence of an eavesdropper, in which all nodes are expected with single antenna and the solid line indicates the main link and dash lines represent wiretap link, respectively. The eavesdropper may be aillegitimate user or a legitimate user who is interested in tapping other users' data information. For notational convenience, N sensors are denoted by S = {si |i = 1, 2, · · · , N}.

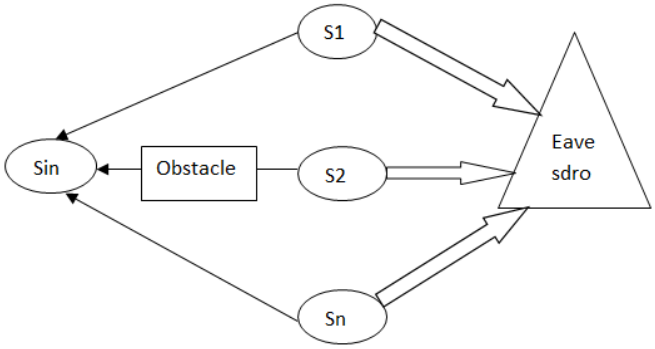

Fig 2 System model using OFDMA

Main link

Wiretap link

The occurrence of machinery obstacles, metallic frictions and engine vibrations in industrial environments is intimidating to the radio propagation, it causes the wireless fading variations severely. Hence we use the Nakagami fading model for describing both the main channel and wiretap channel. It shows that the Nakagami model is more completed compare to other fading models (e.g., Rayleigh fading, etc.).

V OPTIMAL SENSOR SCHEDULING

An optimal sensor scheduling scheme to maximize the secrecy capacity of the legitimate transmission. Naturally, a sensor with the highest secrecy capacity should be chosen and scheduled to transmit its data to the sink.

Optimal user = arg $max_{i\epsilon s} C_{secrecy}$(i)

$$= \arg max_{i\epsilon s} \frac{1+\frac{|h_{is}|^2 Pi}{No}}{1+\frac{|h_{ic}|^2 Pi}{No}}$$

Where, S represents the set of N sensors. It is observed from that the channel state information (CSI) (i.e., $|his|^2$ and $|hie|^2$) of each sensor is required for determining the optimal sensor, which can be obtained by using classic channel estimation methods.

1. More specifically, each sensor may first estimate its own CSI through channel estimation and then transmits the estimated CSI to the sink. After collecting all the sensors' CSI, the sink can readily determine the optimal sensor and notify the whole network.

2. Thus, in the presence of an eavesdropper, the secrecy capacity of legitimate transmissions relying on the proposed sensor scheduling scheme can be obtained using,

$$\text{poroposed secrecy} = max_{i\epsilon s} log_2 \left(\frac{1+\frac{|h_{is}|^2 Pi}{No}}{1+\frac{|h_{ic}|^2 Pi}{No}} \right)$$

By using Round robin algorithm we can calculate the average distance and time delay.

Round robin algorithm steps as follows:

Step 1: Assign number of nodes

Step2: Assign initial energy

Step3: Find distance between the nodes

D0=sqrt (Efs/Emp)

Where Efs and Emp are transmit amplifier types

Step4: Generate random sensor nodes by using

xd=rand(1,1)*x

yd=rand(1,1)*y

xd= x-axis value for generating sensor nodes

Rand=Random generation of nodes

x=x co-ordinate of the sink

Yd= y-axis value for generating sensor nodes

y=y co-ordinate of the sink

Step 5: According to this equation the position of the sensor nodes are change based on number of sensor nodes

Step 6: Calculate distance between the nodes by using the below formula,

Distance=sqrt(IE.xd-ET.xd)^2-(IE.yd-ER.yd)^2

Where,

IE-Initial Energy

ET-Transmitter Energy

ER-Transmitter Energy

Step7: Calculate time between transmitter and receiver node

Time delay= (ETX+EDA)*4000+EMP*4000*(distance)^4

Step8: Initialize the routing time and waiting time as zero.A

Step9: Initialize number of time as 2 and denote as q.

Step10:Now assign routing time as time delay Assign i= number of nodes

Step11: If routing time greater than or equal to q means routingtime=routing time-q; else i==j means waiting time= waiting time+q;

Step12: Next condition routing time greater than zero and i==j means routing time=0 Else waiting time= waiting time + routing time

VI RC4 ENCRYPTION

RC4 is symmetric key and bite-oriented algorithm that encryptes the data and protects classified data message sent to and from secure websites. RC4 is used in both encryption and unscrambling at the time of information stream practises XOR composed with a evolution of produced secrets. It is a stream cipher. RC4 is supposed as the utmost traditionally used stream figure in the realm of cryptography. It takes in keys of irregular lengths and this is known as a maker of pseudo subjective numbers. And it is recognized with two different names, for example, the ARC4 and ARCFOUR, which means Alleged RC4. The striking characteristics which made RC4 popular among the many web enthusiasts are its rate in the software as well as its simplicity. However, RC4 also has its own weak points just like any other entities in this kind of technology.

VII Results

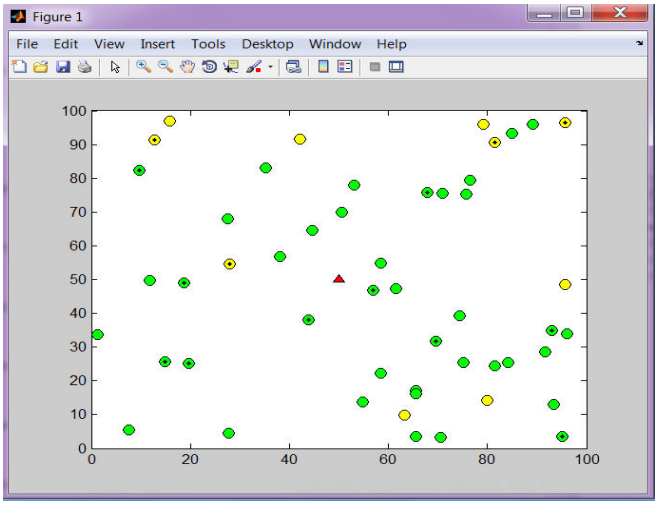

Fig.3 Sender and Receiver nodes

The above image1, green nodes represents the sender, and yellow nodes represent the receiver, and red nodes represent the base station. In this data is transmitted by sender to receiver. The data is transmitted through base

station, in this system, at the time of receiving, the data is protected and any other persons can't steal the data and also it takes very less time for sending. This is the advantage of this proposed system.

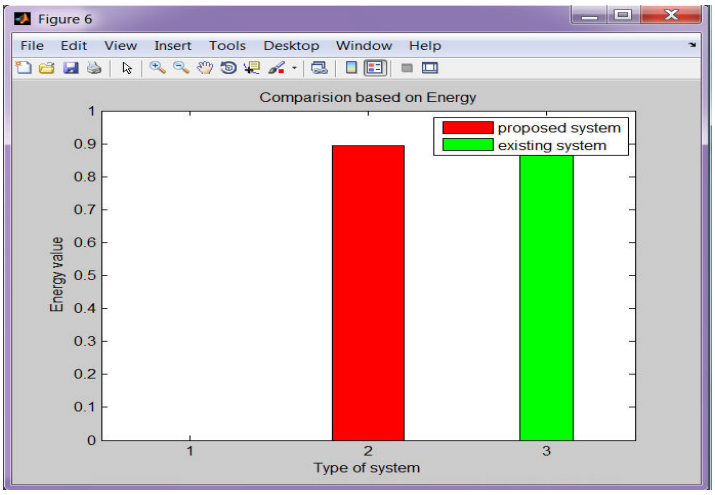

Fig.4 Comparison of energy needed for conventional and proposed system

The above image2 shows the graphical representation of value of energy versus type of system. This shows the comparison based on the energy. In this image compared to existing system, proposed system energy level is less as shown in the above image

.

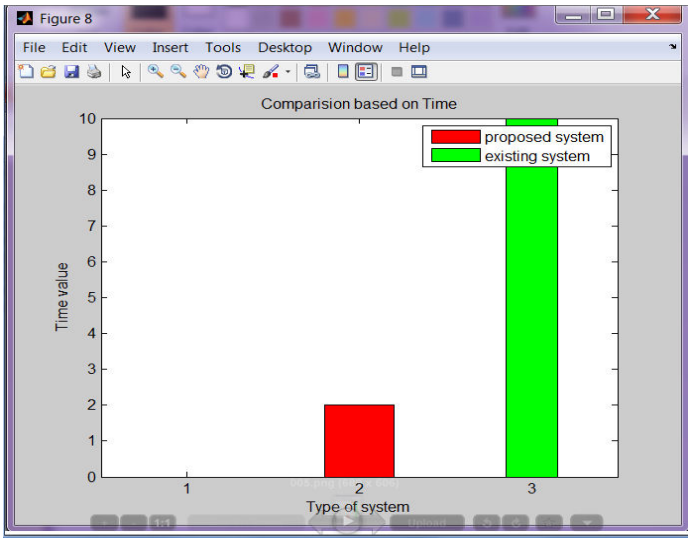

Fig.4 Comparison of time needed for conventional and proposed system

The above image3 shows the comparison based on time between existing system and proposed system. This image shows the graphical representation of value of time and type of system. In this proposed system it takes less time for sending data compared to existing system, this is the advantage of this proposed system.

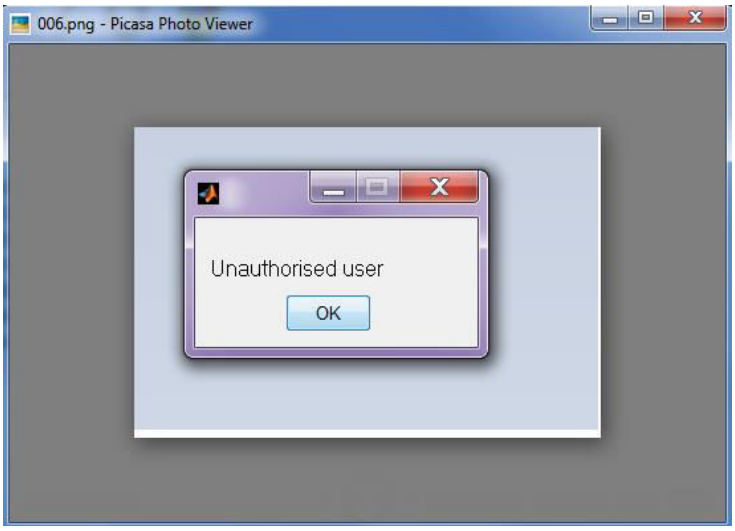

Fig 5 Response for access any unauthorized person

The above image shows the output result of this proposed system, it acts as a security. At the time of sending data if any unauthorised person try to steal the data or try to see the means it shows unauthorised users, so from this our data is protected.

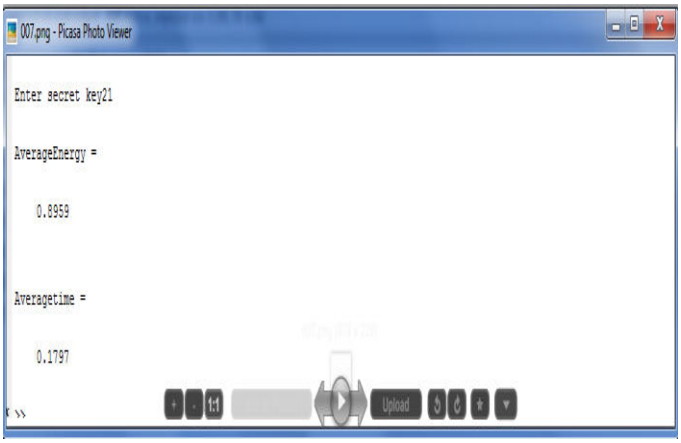

Fig 6 Energy usage with time

In the above image 5, it shows the calculation of average energy and average time by using the formula. The procedure for the calculation of this average time and average energy as explained in the above section.

VIII CONCLUSION

In this proposed paper we explored the consumption of sensor scheduling in order to develop the physical-layer security of industrial WSNs against the eavesdropping

attack and suggested an optimal sensor programming method in order to improve the secrecy capacity of wireless transmission from sensors to the link. In this, we also use round-robin scheduling as a benchmark. In order to describe the miscellany gains of the Round robin scheduling and optimal sensor scheduling scheme, a asymptotic intercept probability analysis also offered. . Arithmetical outcomes established that the suggested optimal scheduling system executes well than the previous attempts in intercept probability. Along with this, by increasing the number of sensors, the intercept probability of the proposed optimal sensor scheduling scheme meaningfully decreases, it shows the improvement in the physical-layer security of industrial wireless sensor network.

In the proposed paper, we only inspected the single-antenna circumstance, where all network node is equipped with the single antenna. It is of high interest to extend the results of this paper to a general scenario with multiple antennas for each network node. In this proposed paper by using Round robin scheme we can calculate the average time delay and average distance, when the data is transferring from sender to receiver. And it gives security protection from this nobody can steal the data.

REFERENCES

[1] W. Shen, T. Zhang, F. Barac, and M. Gidlund, "PriorityMAC: A priority-enhanced MAC protocol for critical traffic in industrial wireless sensor and actuator networks," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 824–835, Feb. 2014.

[2] 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. Ind. Informat*., vol. 10, no. 1, pp. 803–812,Feb. 2014.

[3] R. C. Luo and O. Chen, "Mobile sensor node deployment and asynchronous power management for wireless sensor networks," *IEEE Trans. Ind. Electron*., vol. 59, no. 5, pp. 2377–2385, May 2012.

[4] 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. Ind. Informat*., vol. 10, no. 3, pp. 1806–1816, Aug. 2014.

[5] O. Kreibich, J. Neuzil, and R. Smid, "Quality-based multiple-sensor fusion in an industrial wireless sensor network for MCM," *IEEE Trans. Ind. Electron.*, vol. 61, no. 9, pp. 4903–4911, Sep. 2014.

[6] T. M. Chiwewe and G. P. Hancke, "A distributed topology control technique for low interference and energy efficiency in wireless sensor networks," *IEEE Trans. Ind. Informat*, vol. 8, no. 1, pp. 11–19, Feb. 2012.

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

[8] Q. Chi, H. Yan, C. Zhang, Z. Pang, and L. Xu, "A reconfigurable smart sensor interface for industrial WSN in IoT environment," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1417–1425, May 2014.

[9] F. Gandino, B. Montrucchio, and M. Rebaudengo, "Key management for static wireless sensor networks with node adding," *IEEE Trans. Ind. Informat.*, vol. 10, no. 2, pp. 1133–1143, May 2014.

[10] M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 277– 293, Feb. 2013.

[11] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Netw.*, vol. 29, no. 1, pp. 42–48, Jan. 2015.

[12] C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol. 28, pp. 656–715, 1949.

[13] A. D. Wyner, "The wire-tap channel", *Bell Syst. Tech. J.,* vol. 54, no. 8,pp. 1355–1387, Aug. 1975.

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

[15] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," *IEEE J. Sel. Areas Commun*., vol. 31, no. 10, pp. 2099–2111, Oct. 2013.