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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

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

R.Sindhuja[1], Dr.K.A.Dattatreya[2]

PG Scholar, Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

Professor, Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India

ABSTRACT: Industrial networks are increasingly based on open protocols and platforms that are also employed in the IT industry and Internet background.Most of the industries use wireless networks for communicating information and data,due to high cable cost. Since,the wireless networks are insecure,it is essential to secure the critical information and data during transmission. The data that transmitted is intercepted by eavesdropper can be predicted by secrecy capacity. The secrecy capacity is the difference between channel capacity and main link of wireless transmission.When the secrecy capacity gets fades, then it is known that transmitted data is intercepted. In the event, of applying optimal sensor scheduling scheme a sensor with highest secrecy capacity is chosen and data is transmitted. It is followed with cooperative localization algorithm to enhance nodes, predict and maintain power of each sensor nodes. Through localization algorithm best sensor nodes are get predicted for transmission. Moreover, RC4 encryption and decryption algorithm is enhanced for data while transmission. This will enable protection to data to an extent. Also, an asymptotic intercept probability analysis is performed to provide an imminent into the impact of the sensor scheduling on the wireless security.

KEYWORDS: secrecy capacity, intercepted, sensor scheduling, channel capacity.

I.INTRODUCTION

Wireless sensor networks were initially motivated by the military for battlefield surveillance, and now are further developed for the military for battlefield surveillance,and now are further developed for various industrial applications such as the assembly line monitoring and manufacturing automation for the sake of improving the factory efficiency, reliability, and productivity which are referred to as, the industrial WSNs. In industrial applications, the real-time communications among the spatially distributed sensors should satisfy strict security and reliability requirements. The failure of ensuring the security and reliability of the sensed information transmissions may cause 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 hostile to the radio propagation and certainly adversely affect the performance of wireless transmissions.

The cryptographic tech-niques were exploited to protect the wireless communication 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(knouwn as the brute-force attack).

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

II. EXISTING SYSTEM

In conventional round robin algorithm, we only reduce the average waiting time and increase the throughput. But in round robin algorithm we will increase the CPU utilization, turnaround time, response time, waiting time.Round robin is a pre-emptive algorithm as the scheduler forces the process out of the CPUonce the time quota expires. If the time slot is 100 milliseconds, and job takes a total time of 250ms to complete, the round robin scheduler will suspend the job after 100ms and give other jobs their time on the CPU. Once the other jobs have had their equal share(100ms each), job 1 will get another allocation of CPU time and the cycle will repeat.This process continuous until the job finishes and needs no more time on the CPU. As the term generally used, time slices are assigned to each process in equal portions and in circular order and it process without priority.It is mainly for time sharing.

The N sensors may be used to detect and monitor different aspects of an industrial plant environment, including the machine motion, temperature, moisture, and pressure. The sensor data may also be obtained by exploiting the collaboration between multiple sensors for distributed state estimation.

III. PROPOSED SYSTEM

The industrial WSNs of N sensors communicate with the sink using an orthogonal multiple access method suchas the time division multiple access (TDMA) and orthogonal frequency division multiple access (OFDMA).Here the conventional roundrobin scheduling as a benchmark, where N sensor state turns in accessing a given channel and thus each sensor has an equal chance to transmit its sensed data to the sink, then 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. RC4is symmetric key ciper and bite-oriented algorithm that encrypt PC and laptop files and disks as well as protects confidential data message sent to and from secure websites. Output bytes require eight to 16 operations per byte.It is a stream cipher.Co-operative localization algorithms is based on realistic UWB ranging models developed through an extensive measurement campaign using FCC-complaint USB radios.

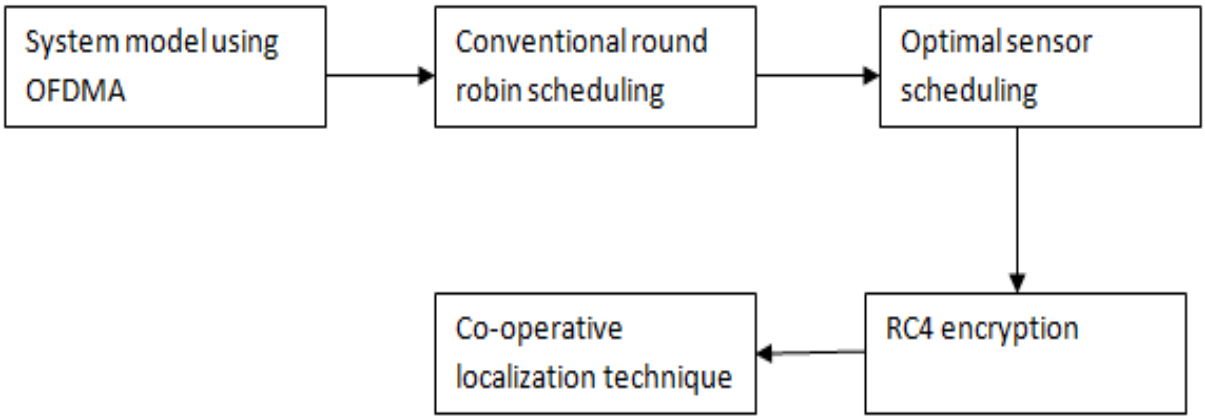

Fig 1: Functional Block Diagram Of Industrial WSNs

A. SYSTEM MODEL USING OFDMA

The industrial WSN of N sensors communicate with the sink using an orthogonal multiple access method such as the time division multiple access and orthogonal frequency division multiple access. When a sensor is scheduled to transmit its data to the sink over a channel the eavesdropper attempts to intercept the information to be transmitted. Traditionally,given an orthogonal channel, a node with the highest data throughput is typically

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

selected among 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.

B. ROUND ROBIN ALGORITHM

Round Robin is one of the algorithm employed by process and network schedulers for computing. Round-robin scheduling is simple, easy to implement, and starvation free. Round-robin scheduling can also be applied to other scheduling problems, such as data packet scheduling in computer networks.It is an operating system concept. The round robin function is mainly employed for network scheduling and processing in network process. In thisalgorithm theiris no priority based function. All the nodes receives equal share and in circular order. It is mainly responsible for time sharing.

Round-robin scheduling as a benchmark, where N sensors state turns in accessing a given channel and thus each sensor has an equal state turns in accessing a given channel and thus each sensor has an equal chance to transmit its sensed data to the sink. Round-robin is a pre-emptive algorithm as the scheduler forces the process out of the CPU once the time quota expires.

C. 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 sensor scheduling scheme is the sum of Nakagami shaping factors of the main links from N sensors to sink. Thus, as the number of N sensors increases, the diversity order of proposed sensor scheduling scheme increases accordingly. Inother words, increasing the number of sensors can significantly decreases the intercept probability of the proposed scheduling scheme. Byncontrast, the number of sensors even has a negative impact on the security performance of tne conventional round-robin scheduling.

An optimal sensor scheduling scheme is proposed for protecting the industrial wireless transmission against the eavesdropping attack, where a sensor with the highest secrecy capacity is selected to transmit its sensed information to the sink. The conventional round-robin scheduling is also considered as a benchmark. Closed form expressions of the intercept probability for the conventional round robin scheduling and the proposed optimal sensor scheduling schemes are derived in N akagami fading environments.As asymptotic intercept probability analysis is conduct and the diversity order of the proposed scheduling scheme is shown as the sum of Nakagami shaping factors of the main links from the sensor to the sink.

D. RC4 ENCRYPTION

RC4 is symmetric key cipher and bite-oriented algorithm that encryptes PC and laptop files and disks as well as protects confidential data message sent to and from secure websites.Output bytes require 8 to 16 operations per byte. It is a stream cipher. RC4 is perceived as the most requlary used stream figure in the realm of cryptography. RC4 has an utilization in both encryption and unscrambling while the information stream experiences XOR together with a progression of created keys. It takes in keys of irregular lengths and this is known as a maker of pseudo subjective numbers. It is additionaly 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.

E. CO-OPERATIVE LOCALIZATION

The need of highly accurate position information is of great importance in many commercial, public safty, and military applications.Localization aware technologies will revolutionize many aspects and are expected to spawn numerous unforeseen applications. Co-operative localization algorithms is based on realistic UWB ranging models developed through an ententive measurement campaign using FCC-complaint UWB radios. Reliable localization in such conditions is a key enabler for a wide varity of applications including logistics, security tracking, medical applications, search and rescue, control of home applications, automotive safty, and military systems, as well as in the large set of emerging wireless sensor network applications.

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

IV. RESULT AND DISCUSSION

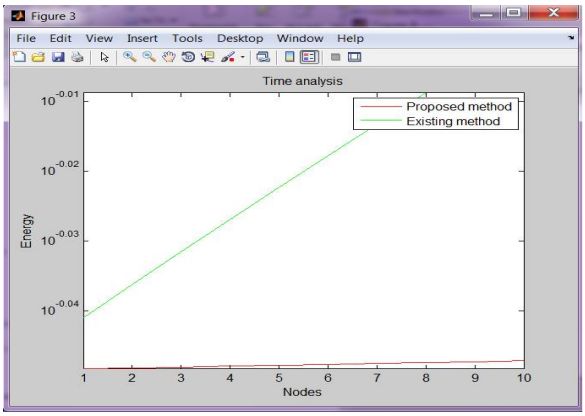

Fig:2 Time analysis of nodes

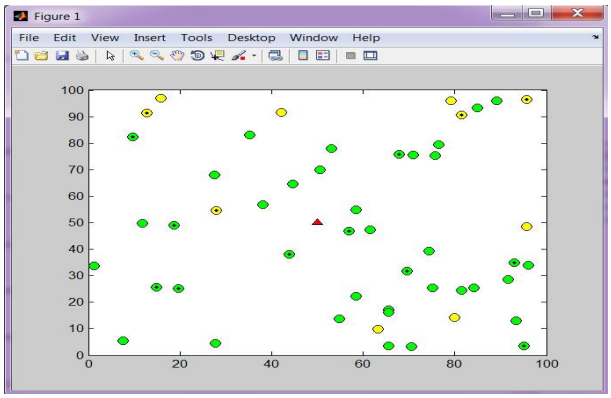

Fig:3Representation of nodes

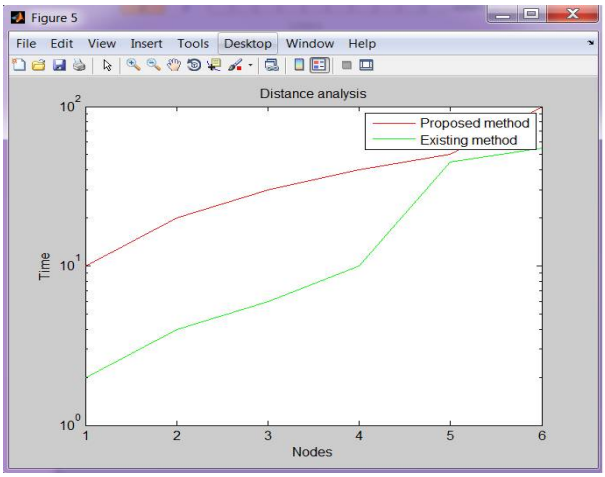

Fig:4 Distance analysis of nodes

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

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 6, Special Issue 3, March 2017

5th National Conference on Frontiers in Communication and Signal Processing Systems (NCFCSPS '17)

13th-14th March 2017

Organized by

Department of ECE, Adhiyamaan College of Engineering, Hosur, Tamilnadu, India.

Fig:5 sample output

V. CONCLUSION

In this paper, we proposed thatthe industrial wireless sensor networks in the presence of eavesdropping attack which had improved with USB utilization, around time, waiting time, response time, and inrease in throughput. Here we had improved the physical layer security of industrial WSNs against eavesdropping attack and proposed an optimal sensor scheduling scheme, aiming at maximizing the secrecy capacity of wireless transmissions from sensor to the sink. We also considered the conventional round-robin scheduling as a benchmark. Then we had improved the detection speed of the proposed system. Then we had equipped with multiple antennas for each network node.

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 homeautomation," 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,"IEEETrans.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 controltechnique 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 gradi-ent 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 IoTenvironment,"IEEETrans.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,"IEEENetw.,vol. 29, no. 1, pp. 42–48, Jan. 2015.

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