iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** II **Month of publication:** February 2017

DOI: http://doi.org/10.22214/ijraset.2017.2078

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue II, February 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Study of Various Algorithms Used for Analyzing Eavesdropping Attack in Industrial Wireless Sensor Network

Dr. K. A. Dattatreya[1], R. Sindhuja[2]
[1]Professor,[2] PG Scholar, Department of ECE, Adhiyamaan College of Engineering, Hosur

Abstract: ***In industrial applications, the real time communications among the spatially distributed sensors should satisfy reliability requirements and strict security. 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. 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 choosen and the data is transmitted. In this paper various types of scheduling are studied.***

Keywords-Real- Time scheduling, optimal sensor scheduling, secrecy capacity, Intercepted

I. INTRODUCTION

Wireless sensor networks were initially motivated by 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 WSN's. In industrial applications, the real-time communications among the spatially distributed sensors should satisfy strict security and reliability requirements.

Moreover, in industrial environments, metallic frictions, engine vibrations, the machinery obstacles and certainly adversely affect the wireless transmissions performance. In industrial WSNs the broadcast nature of radio propagation,both authorized and unauthorized users access the wireless medium, leading WSNs to be more vulnerable to the eavesdropping attack than wired sensor networks, where communicating nodes are physically connected using wire cables and a nodes without connection is unable to access for illegal activities. To be specific, as long as an eavesdropper hides in the industrial WSNs, the legal wireless transmissions among the sensors can be r overheard by the eavesdropper readily, which may decode its tapped transmissions and violate the confidentiality of the sensors information communication. Therefore, it is importance to investigate the protection of industrial WSNs against the eavesdropping attack. To overcome this by the use of sensor scheduling to improve the physical-layer security of industrial WSNs against the eavesdropping attack and proposed an optimal sensor scheduling scheme, aiming at maximizing the secrecy capacity of wireless transmissions from sensors to the sink.

II. RIOUS TYPES OF SCHEDULING

A. *Conventional Round-Robin scheduling*

Round robin is one of the algorithms employed by process and network schedulers in computing. Round-robin scheduling is very simple, much 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.

B. Conventional Round -robin description

The Round –robin function is mainly employed for network scheduling and processing in network process.
In this function there is no priority based function. All the nodes receive equal share and in circular order.
It is mainly responsible for time sharing.

1) *Description:* The scheduler maintains a queue of ready processes and a list of blocked and swapped out processes. The Process Control Block of newly created process is added to end of ready queue. The Process Control Block of terminating process is removed from the data structures scheduling.

The scheduler should select the Process Control Block from the head of the ready queue. Here all processes are basically given the

©IJRASET: All Rights are Reserved

same priority that is a main disadvantage. Round robin also favours the process with short CPU burst and penalizes long ones.
When a running process finishes its time slice, it is moved to end of ready queue. A time slice is an amount of time requires for each process that spends on the processor per iteration of the Round Robin algorithm. All processes are executed in a FCFS manner but are preempted after a time slice. The process will either finish in the given time slice.
he event handler performs some actions such as:
When a process makes an input-output request or swapped out, its Process Control Block is removed from ready queue to blocked/swapped out list.
When input-output operation is awaited by a process finishes or process is swapped in its Process Control Block is removed from blocked/swapped list to end of ready queue.
According to proposed algorithm

2) *Priority based Round-Robin CPU scheduling consists of two rounds:* Round 1: Process with the highest priority is executed first for the time equal to time quantum given i.e.5 ms. Similarly other processes are executed according to their priorities for single time quantum. Round 2: This round includes the changing of processes priorities according to the remaining CPU Burst Time. The process with least remaining CPU Burst Time. The process with least remaining CPU Burst Time is assigned highest priority.

B. Optimal Sensor Scheduling

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.
It is observed from that the CSI of each sensor is required for determining the optimal sensor, which can be obtained by using classic channel estimation methods. 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 read-ily determine the optimal sensor and notify the whole network.
An optimal sensor scheduling scheme is proposed mainly for protecting the industrial wireless sensor 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 schemes are derived in Nakagami fading environments.

C .*Real –Time Scheduling*

The Real-time computing includes the analysis and testing of the scheduler system and the algorithms used in Real-time applications. A real-time scheduling system is consists of the scheduler, clock and the processing hardware elements. In a real-time system, a process or task has scheduled; tasks are accepted by a real-time system should be completed as specified by the task deadline depending on the scheduling algorithm characteristics. Modeling and evaluation of a real-time scheduling system concern is on the analysis to meet a process deadline of the algorithm capability. A deadline is also defined as the task to be processed in a given time.
For example, in a real-time scheduling algorithm a deadline could be set to five nano-seconds. In a critical operation the task must be proposed in the real-time specified by the deadline(i.e.five nano-seconds).A task can be classified as either a periodic or aperiodic process.
The criteria of a real-time can be classified as hard, firm or soft. The scheduler set the algorithm for executing tasks according to a specified order. To represent a scheduling system, most implementations of real-time scheduling algorithm there are multiple mathematical models which are modeled for the implementation of uniprocessors or multiprocessors configurations. A real-time scheduling algorithm can also be classified as static or dynamic. Tasks are accepted by the hardware elements in a real-time scheduling system from the computing environment and processed in real-time.

D. Priority Scheduling

Priority scheduling is a method of scheduling processes based on priority. In this method, the scheduler chooses the tasks to work as per the priority. Priority scheduling involves priority assignments to every process, and processes with higher priorities are carried out first, whereas tasks with equal priorities are carried out on a round robin basis or First-come-first-out (FCFC) . An example of a

©IJRASET: All Rights are Reserved

general-priority-scheduling algorithm is the shortest-job-first (SJF) algorithm.

Priority scheduling can be either classified into Preemptive and Non-preemptive,

Preemptive: This type of scheduling may preempt the central processing unit(CPU)in the case the priority of the freshly arrived process being greater than those of the existing processes.

Non-preemptive: This type of scheduling algorithm simply places the new process at the top of ready queue.

III.CONCLUSION

In this Wireless Physical-layer security with a aid of sensor scheduling is secured. In order to effectively defend against the eavesdropping attack, a sensor scheduling is employed to improve 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 sensors to the sink. We also considered the benchmark as a conventional round-robin scheduling. An asymptotic intercept probability analysis was also presented to characterize the diversity gains of the optimal sensor scheduling and the round-robin scheduling schemes. Numerical results demonstrated that the proposed optimal scheduling scheme performs better than the conventional round-robin scheduling in terms of intercept probability.

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,”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 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 IoT environment,”IEEE Trans.Ind. Informat., vol. 10, no. 2, pp. 1417–1425, May 2014.

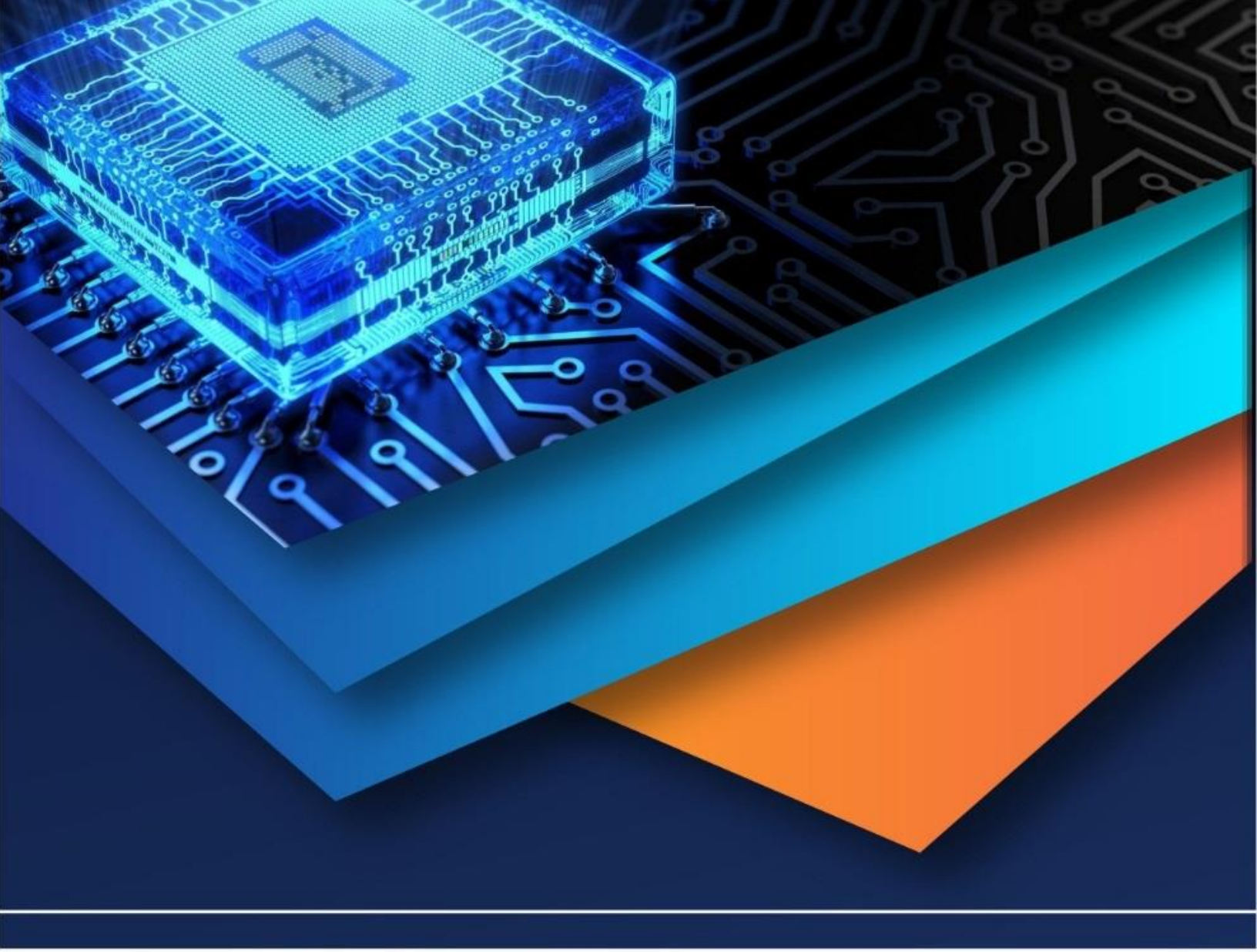
[9] F. Gandino, B. Montrucchio, and M. Rebaudengo, “Key management for static wireless sensor networks with node adding,”IEEE Trans. Ind. Informat., vol. 10, no. 2, pp. 1133–1143, May 2014.

[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.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)