Deployment of Sensor Scheduling in Wireless Sensor Networks for Shielding the data Against the Attack of Eavesdroppers

[1]Hebziba Jeba Rani S, [2]Kirthika KM, [3]Meenachi VR, [4]Revathi S, [5]Dr. Sumithra A

Assistant Professor
Department of Computer Science & Engineering
Sri Ramakrishna Institute of Technology, Coimbatore,Tamil Nadu, India.

***Abstract*—Wireless sensor networks are mainly used to monitor the environmental conditions like temperature, pressure, vibration, etc... The sensed data is then transmitted to the intended receiver. The sensed data on its path, may suffer from the interruption of the attacks due to the broadcast nature of the wireless environment and due to the fading effect. The sensitive information may get caught by the intruder and false data may be forwarded to the receiver. Sending the false data or dropping of the packets are tolerate to some less important data. But sensors are mainly fixed to monitor the important factors like forest fire detection, earthquake monitoring, productivity monitoring. These critical and time sensitive data need to be transmitted without suffering from any delay and attacks. Thus security measures are to be taken in sensor environment to prevent unnecessary activities in the network. In industrial wireless sensor network, the signal carrying the sensed data may suffer from fading effect due to the machineries, engine vibrations. This fading effect may pay way for the eavesdroppers to overhear the sensed data. Thus to avoid this problem, the secured channel is need to be selected to transmit the sensed data. The channel state information can be gathered and based on the channel information, scheduling scheme can be used to schedule the sensors based on the secrecy capacity of the channel. Thus the sensors sending the data in the secured channel will be less prone to the attackers.**

***IndexTerms*—Sensor scheduling, channel selection, security, eavesdropping attack, link information, channel state information.**

I. INTRODUCTION

The Wireless sensor network is a network consisting of sensors and other nodes. The sensors in the sensor network is mainly deployed to monitor the surroundings for its heat level, pressure level, moisture content level, vibration, movement detection, etc. Especially in today smart cities development projects the wireless sensors plays a very major role for making the city a smart city. For example consider one of the tasks under the smart city development project is preservation of the nature. To preserve the nature weather sensors and soil moisture indicator sensor can be placed along the roadside trees to monitor the temperature of the environment and the respective soil moisture content level. This information can be monitored periodically and sent to respective department to save the natural resources and also the air pollution level can also be monitored and updated periodically to limit the harmful emissions polluting the nature. Then during heavy rain conditions the sensors fixed along the shores of the ocean or the river can be used to monitor the water level in that particular water bodies. If water level crosses that limit the information can be sent immediately to take remedial actions. Then by using the sensors, the accident in the roads can be detected and updated instantly to the nearby hospitals and the traffic updates can also be made to the drivers through the GPS system and based on the severity of traffic the traffic signals can be automatically adjustable. Like the above mentioned smart projects, in future the smartness will be more improving through the deployment of wireless sensor network. In the recently emerging wireless sensor networks, the challenging task comes in the area of Security [19]. Since the wireless sensor networks are mainly deployed to monitor the sensitive information like accident monitoring, flood indication, fire accident alarm, the sensed data need to be transmitted without any delay or drop. The dropping of the packets may happen due to the changes in the network like over load in the network. Apart from the network related issues the main reason for the dropping of packets is the intentionally dropping of packets by the attackers. The unauthorized illegal attackers in the network may sometimes drop the sensitive information leading to the problems related to even the loss of life in case of critical applications like machine explosion in industry due to overheating of the machine. Thus the security against the attackers in the network has to be improved to avoid unnecessary dropping or misuse of the packets by the attackers. Although several security mechanisms are available to detect, prevent and protect the data against the hackers, the hackers are utilizing new tactics and tricks to steal the authorized user's content. Hence there is a strong need to improve the security in the wireless sensor networks. Especially in industrial wireless sensor networks [20], due to presence of machinery obstacles fading effect increases which leads to the sensor network becoming more vulnerable to the attackers.

There are several types of attacks that may happen in the network. Not all the attackers present themselves as the same way other show their identity [15]. For example some attackers show their identity as a trusted user by stealing the identity of the authorized users. Thus the other nodes which transmit the data via the hacker node assume the hacker as a trusted party due to its identity and share their data for transmission. But however some attackers hide their identity and secretly overhear the transmitted

data. Thus their presence will be most often hidden to the other nodes transmitting packets. One of the crucial and very dangerous attack is the attack which is done is secretly. It is because the nodes participating in the communication will be unaware of such attacks which may lead to their secret data overheard secretly by the hacker node. If the presence of the intruder is predictable or detectable timely measures can be taken to avoid the data misuse by the intruders. But if the attacking is done secretly, it is really very difficult to overcome that. In secret overhearing concept, even though the data is unmodified by the intruders but simply performing the overhearing of the data may lead several other critical attacks like stealing the passwords to fake their identity and their identity to perform illegal activities. Thus the overhearing attacks need to be concentrated more. This paper mainly focuses on the Eavesdropping attack which a passive attack in which it performs the overhearing of the data without the knowledge of the trusted parties.

Eavesdropping Attack

Eavesdropping attack is a type of passive attack where the malicious node silently over hears the secret information. These attackers got the name eavesdroppers due to the following. “Eaves” is the section of the roof that meets the walls of the buildings. “Eavesdrop” refers to the dripping of water from the eaves of the house to the ground. Thus “Eavesdropper” is the person who is standing near the eaves of the house to secretly overhear the conversation which is going inside the house. Similarly a malicious node which overhears the secret information is said to be eavesdropper node. Fig. 1 shows the eavesdropper in the network. Thus the passive attacking node which secretly overhears the conversation in the network is called eavesdropper and this type of attack is called eavesdropping attack [16].

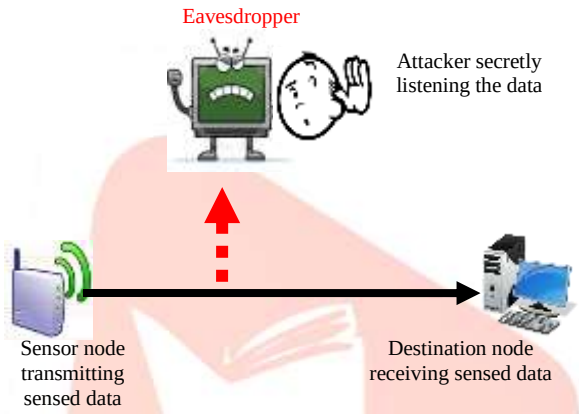

Fig. 1. Eavesdropper overhearing the data

The eavesdroppers achieve their target of gathering the secret data if the encryption is weak. If no encryption is used or if the encryption technique used is very weak the attacker finds no difficulty in understanding the original data. But if the encryption technique used is very strong, the attackers receive only the data with no meaning in it due to encryption.

II. Existing Techniques on Security

Several authors proposed various algorithms and techniques to improve the security in the wireless sensor networks.

There are several cryptographic techniques that are available to encrypt the data. An encryption technique helps to secure the data from the unauthorized users. Even though cryptographic techniques are available, the attacker having the unlimited computing capability can break the passwords and keys used by the cryptographic methods. But cryptographic techniques for limited computing capability attackers works well [7]. In this traditional way of improving the security, symmetric and asymmetric methods are made use of. In symmetric method same keys is used by the sender and receiver to encrypt and decrypt the message. Thus if an attacker steals the secret key, then they can have full access to data. They can both read and modify the data. But in case of asymmetric method, different keys are used which strengths the security than the symmetric method. But still attacker with unlimited capability can even have access to these data. Thus security needs to be improved more especially in wireless sensor network monitoring the sensitive and critical data.

In [16], the author proposed the concept of transmission power Control in mutihop wireless networks to minimize the risk of Eavesdropping attack. By minimizing the transmission power, the eavesdropping attack is minimized due to the minimal coverage area of the transmitting nodes. The attackers hiding in the farther area will never receive the data and also the network throughput, QoS, energy conservation improves. But this fails to work well in high-order eavesdropping attack. In [17] author addressed the problem of securing distributed storage systems against eavesdropping and adversarial attacks. In this paper author provides upper bounds on the secrecy and resiliency capacity and showed the security achievability in the bandwidth-limited regime. In [8] reviewed the attack detection schemes on the active attacks. The active attack is detected using the channel estimation.

Eavesdropping based Gossip Algorithm is used to improve the convergence rate with the convergence value around the average value. In this algorithm, the state or value of a particular node is unicasted to the randomly selected neighbour. While unicasting the state or a value, the neighbour of the receiving node may overhear (eavesdrop) the data. The nodes on reception of

the values, update the state values leading to faster rate of convergence with average value [18]. Using this technique the data aggregation in Wireless Sensor network can be done at the faster rate.

In [2] author concentrated on improving the security in wireless network environments against the use of Amplify and Forward (AF), Decode and Forward (DF) based multiple relay selections. In this relay selection method, only single source and single destination in concentrated. In [1], the security against the eavesdropping attack in the cognitive radio networks is focused. To achieve the security with QoS requirement, the cognitive user is scheduled to transmit the data only if the specific QoS parameters are achieved with the maximized secrecy capacity.

In artificial Noise Generation method, the intentionally produced noises are allowed to spread in the network with the motive of degrading the attacker channel. The attackers welcome the unnecessary noises imaging that it was a secret message from trusted users. In this way the channel capacity of the attackers can be made weak thereby which helps to detect the presence of attackers in the network. But the major drawback in implementing this method for improving security is that this method utilizes more resources for the production of unwanted noises in the network. The complexity of the network increases with this artificial noise method [4].

III. PROPOSED SCHEME TO IMPROVE SECURITY

To overcome the problems of additional utilization of resources in the noise generation and relay nodes, this paper deals with the use of the sensor scheduling which does not require more cost and power to install the additional resources in the sensor network. To perform the sensor scheduling, the channel state information is gathered from the available channels and based on the channel information, the sensor which is having the better channel capacity is allowed to transmit the data.

Collection of channel state information (CSI)

The nakagami fading model is used to determine the channel state information (CSI) of the sensor nodes. Every node collects its channel state information (CSI) and sends the collected channel information to the sink node. The sink node on receiving the channel information of all the channels performs the optimal sensor scheduling. The Fig. 2 shows the sensors in the presence of eavesdropping attack and the sink node.

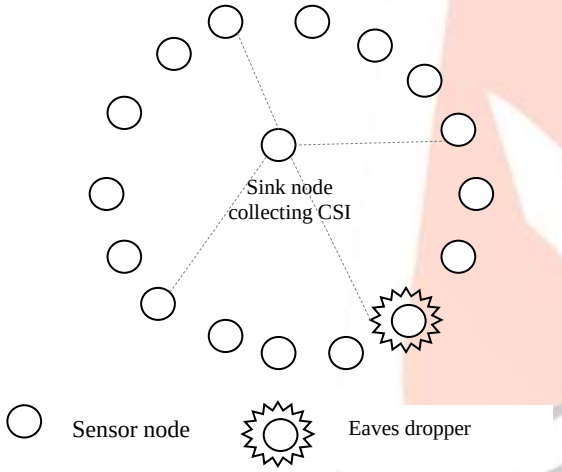

Fig. 2. Sink node and sensors nodes in the presence of Eavesdropper

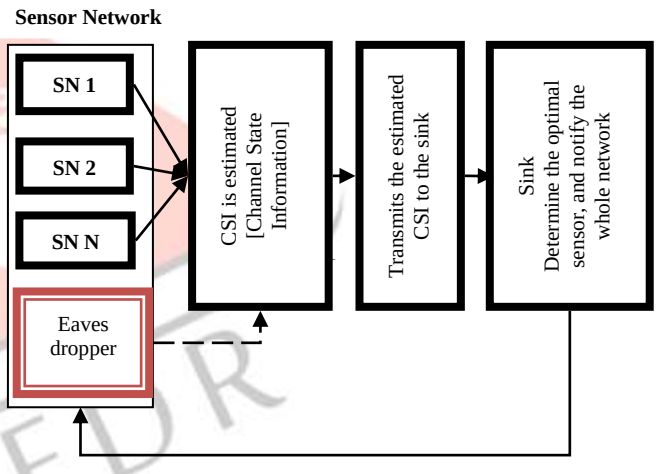

Fig. 3. CSI collection and Sensor Scheduling by sink

Sensor scheduling

This module proposes a Sensor Scheduling scheme to maximize the secrecy capacity of the legitimate transmission. The sink node after receiving the channel information from the available channels chooses the sensor which is having the highest secrecy capacity channel and schedules that sensor to transmit its data. Fig. 3 shows the scheduling of sensors concept through basic block diagram. The sensor scheduling is done in the following ways:

Step 1: Calculate the channel state information and send to the sink node

Step 2: Sink node scheduling the sensors to transmit the data based on its channel information. That is channel with more secrecy capacity is scheduled to transmit the data first.

Fading Model

In wireless environment, the transmitted signal from the sender has no single direct path to the destination. Due to the presence of obstacles the signal suffers from reflection in various paths leading to multipath propagation. The multiple reflective paths in the wireless environment lead to the fading of the signals. Fading refers to the fluctuations in the amplitude, phase and angle of the received signal. Thus the receiver suffers from multiple reflections from different obstacles. If the received multipath signals are all of same amplitude, then the envelope of the received signal is said to be Rayleigh distributed. When all of the reflected are not equal in its strength due to a dominant signal that is a signal having the direct line of sight, such signal has more strength than the other reflected signals. Thus if there is a dominant signal among the weak reflected signals, then the distribution is said to be rician. When that dominant signal fades away then the rician degenerates to the Rayleigh distribution. So when one dominant signal adds up to the Rayleigh distribution, it leads to the formation of rician distribution. If there is more than one dominant signal among the multiple reflected signals then such distribution is said to be nakagami fading model. . For characterizing the channel of the

wireless sensor environment rather than using the simple Rayleigh fading model, a complex fading model called the nakagami fading model is used. The need to focus on the complex nakagami fading model is due to the presence of obstacles in the wireless environment leading to complications in the wireless channel.

The proposed system mainly focuses on improving the security in the wireless sensor environment through the deployment of sensor scheduling. To protect the data against the eavesdropping attack, the sensors in the wireless sensor network can be scheduled based on the channel state information from the available channels. Through the sensor scheduling, the eavesdropping attack can be considerably reduced.

Nakagami Fading Channel

To the existing radio propagation models as an addition the nakagami fading model is developed and added in this patch. Nakagami fading model is the general mathematical modelling of a radio channel with the fading. Comparing to the existing models like shadowing and two-ray ground, the nakagami RF model has more configurable parameters to allow for the closer representation of the wireless communication channel. It is able to model from a perfect simple free space channel to a moderate fading channel on a highway or even to a drastically fading channel in urban communities.

Nakagami distribution is define by the following probability density function:

$$f(x) = \frac{2m^m x^{2m-1}}{\Gamma(m)\Omega^m} exp\left[-\frac{mx^2}{\Omega}\right], x \geq 0, \Omega > 0, m \geq 1/2 \quad (1)$$

The corresponding pdf of the power (square of the signal amplitude) at the given distance can be determined by a change of variables and is given by the gamma distribution of the following form:

$$p(x) = \left(\frac{m}{\Omega}\right)^m \frac{x^{m-1}}{\Gamma(m)} exp\left[-\frac{mx}{\Omega}\right], x \geq 0 \quad (2)$$

'(ohm)' is the expected value of the distribution and can be interpreted as the average of the received power. 'm' is the shape or fading parameter. The values of '(ohm)'and 'm' parameters are functions of distance. So the nakagami fading model is defined by the two functions. Those two functions are 'ohm (d)' and 'm (d)'.

Rayleigh distribution model is a other case of nakagami fading model distribution where m(d)=1 (for every d). Larger the values of m less severe the fading will be.

IV. Results and Discussion

Simulation

The simulation is done with the help of network simulator 2 in the linux operating system with ubuntu as the interfacing tool. The mobility model utilizes the random way point model. There are 50 nodes defined in the simulation area of size 1000m x 1000m. The mobility of the nodes is limited to about 5ms. The constant bit rate (CBR) connections with the packet sizeof 1000 bytes are the traffic model chosen to emulate the traffic over the network. Each packet starts from the random location to a random destination with a randomly chosen speed. Once the destination is reached, another random destination is targeted after a pause time. The pause time which affects the relative speed of the mobiles is varied.

Two sets of experiments are conducted. The simulation parameters for the sensor network are as follows: a)Sensor nodes are randomly deployed in the given area. b) The energy of the senor node is 2 joules initially. c) Each experiment is conducted for 2 simulation scenarios and the average is used. d) The sink node is placed at the centre of the sensor network in the simulation. The simulation parameters are given in the following Table I.

TABLE I. SIMULATION PARAMETERS

Parameter name	**Parameter value**
Simulation tool	NS2
Antenna	Omni directional antenna
Channel	Wireless
Number of mobile nodes	50
Topography size	1000 x 1000
Number of sinks	1
Initial energy	2J
Communication agent	TCP
MAC type	802.11

In the network construction, all the nodes are assumed with the single antenna. The eavesdropper node could be either an illegitimate user or a legitimate user who is trying to overhear other's data information without their knowledge.

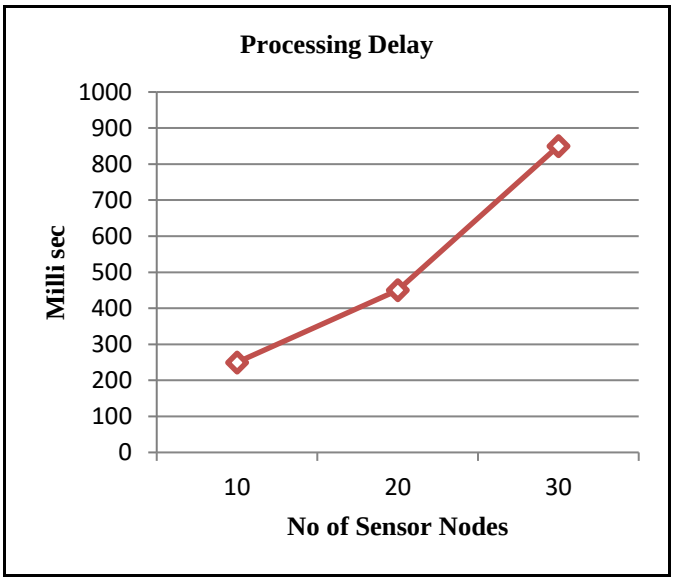

Fig. 4. Graph showing the packet delay in sensor scheduling

In the Fig. 4 graph is shown which represents the delay for sending the packets to the destination when using the method of sensor scheduling. The graph is constructed by implementing the sensor scheduling concept in the network simulator.

The delay occurred in the method, can be reduced by improving the QoS parameter 'delay'. In this paper, security is mainly focused and thus the achievement of QoS is not highly concentrated. Thus in future security along with the QoS achievement can be focused.

IV Conclusion and Future work

In this paper we investigated the utilization of scheduling the sensors in the network to improve the security in the wireless sensor environment. The improvement in security is achieved by utilizing the concept of sensor scheduling based on the gathered channel state information. Based on the channel information, the optimal channel is selected for transmitting the data. In the conventional round robin method of sensor scheduling, the intercept probability increases with the increase in the number of sensors. But in case of sensor scheduling based on the channel information, the intercept probability increases with the increase in the number of sensors. Thus the security is improved with the investigated sensor scheduling based on channel state information.

Sensors are now-a-days mainly deployed to monitor the sensitive information like data related to fire accidents, earthquakes. Thus such data should not experience any delay or dropping. With the application of scheduling the sensors based on its channel, some sensitive data in the unsecured channel may get dropped or delayed which could even lead to the loss of life. Thus such data irrespective of its channel information must be delivered fast without any delay. Hence based in the type of data, the scheduling should be made. As a future work Quality of Service requirements can be considered.

REFERENCES

[1] Y. Zou, X. Wang, and W. Shen, "Physical-layer security with multiuser scheduling in cognitive radio networks," IEEE Trans. Communications, vol. 61, no. 12, pp. 5103-5113, Dec. 2013.

[2] Y. Zou, X. Wang, and W. Shen, "Optimal relay selection for physical layer security in cooperative wireless networks," IEEE Journal on Selected Areas in Communications, vol. 31, no. 10, pp. 2099-2111, Oct.2013.

[3] 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.

[4] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," IEEE Trans. Vehicular Technology, vol. 59, no. 8, pp. 3831-3842, Aug. 2010.

[5] 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.

[6] Yilin Mo, Garone, E. ; Casavola, A. ; Sinopoli, B., "Stochastic sensor scheduling in Wireless Sensor Networks with general graph topology", IEEE Conference on American Control Conference (ACC), pp. 2048-2053, June 2012.

[7] Saini, N.; Pandey, N.; Singh, A.P., "Enhancement of security using Cryptographic Techniques", IEEE International Conference on Reliability, Infocom Technologies and Optimization (ICRITO), 2015.

[8] Kapetanovic, D. ; Gan Zheng ; Rusek, F., "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks", IEEE Journal on Communications Magazine, vol. 53, Issue. 6, pp. 21-27, June 2015.

[9] Yulong Zou, Nanjing, China Champagne, B. ; Wei-Ping Zhu ; Hanzo, L., "Relay-Selection Improves the Security-Reliability Trade-Off in Cognitive Radio Systems", IEEE Transactions on Communications, vol. 63, Issue. 1, pp. 215-228, Jan 2015.

[10] Zhang, Q.T., "A generic correlated Nakagami fading model for wireless communications", IEEE Transactions on Communications, vol. 51, Issue. 11, pp. 1745-1748, Nov 2003.

[11] Young-chai Ko ;Alouini, M.-S., "Estimation of Nakagami-m fading channel parameters with application to optimized transmitter diversity systems", IEEE Transactions on wireless Communications, vol. 2, Issue. 2, pp.250-259, March 2003.
[12] Jaafar, W. ; Ohtsuki, T. ; Ajib, W. ; Haccoun, D ., "Impact of the CSI on the Performance of Cognitive Relay Networks With Partial Relay Selection", IEEE Transactions on Vehicular Technology, vol. 65, Issue. 2, pp. 673-684, February 2016.
[13] Taricco, G., "Joint Channel and Data Estimation for Wireless Sensor Networks", IEEE Transactions on Wireless Communication Letters, vol. 1, Issue. 5, pp. 532-535, October 2012.
[14] Chamam, A. ; Pierre, Samuel "Optimal Scheduling of Sensors States to Maximize Network Lifetime in Wireless Sensor Networks", IEEE International Conference on Mobile Adhoc and Sensor Systems, pp. 1-6, October 2007.
[15] David Martinsa and Herve Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", IEEE International Conference on Network-Based Information Systems (NBiS), pp. 313 – 320, September 2010.
[16] Jung Chun Kao and Radu Marculescu, "Minimizing Eavesdropping Risk by Transmission Power Control in Multihop Wireless Networks", IEEE Transactions on Computers, Issue. 99, June 2008.
[17] Sameer Pawar, Salim El Rouayheb and Kannan Ramchandran, "Securing Dynamic Distributed Storage Systems Against Eavesdropping and Adversarial Attacks", IEEE Transactions on Information Theory, Vol. 57, Issue. 10, pp. 6734 – 6753, October 2011.
[18] Shaochuan Wu, Bo Liu, Xu Bai and Yuguan Hou, "Eavesdropping-Based Gossip Algorithms for Distributed Consensus in Wireless Sensor Networks", IEEE Signal Processing Letters, Vol. 22, Issue. 9, pp.1388 – 1391, September 2015.
[19] Tian Jing, Yi Shengwei, Yu Bing and Ma Shilong, "Study on Wireless Sensor Networks", IEEE International Conference on Intelligent System Design and Engineering Application (ISDEA), vol. 2, pp. 510-521, October 2010.
[20] Cheminod M, Durante L, and Valenzano A, "Review of security issues in industrial networks," IEEE Transactions on Industrial Informatics, vol. 9, no.1, pp. 277-293, Feb. 2013.