www.ioirp.com

International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 2, Issue – 1. January 2016

Averting Eavesdrop Intrusion in Industrial Wireless Sensor Networks

ARUL SELVAN M
M.E Student/IT DEPT
Kongunadu College of Engineering & Technology,
Trichy, India.
[1]arul2591@gmail.com

Mr. D.FELIX XAVIER DHAS
Assistant Professor/IT DEPT
Kongunadu College of Engineering & Technology,
Trichy, India.
femi5304@gmail.com

Mr.S. KALAIVANAN
Assistant Professor/IT DEPT
Kongunadu College of Engineering & Technology,
Trichy, India.
kalaivanan3@gmail.com

***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 of main link and wiretap 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.**

***Index Terms*—Intercept behavior, industrial wireless sensor networks, sensor scheduling, intercept probability, Nakagami fading RC4, Localization.**

I. INTRODUCTION

WIRELESS sensor networks (WSNs) were initially provoked by the military for battlefield surveillance, and now are further developed for various industrial employments such as assembly line monitoring and manufacturing automation for the sake of civilizing the factory efficiency, reliability, and productivity, which are enhanced to the industrial WSNs. In industrial applications, real-time communications among spatially distributed sensors should gratify strict security and reliability requirements. The failure of ensuring the security and reliability of sensed information transmissions may cause an outage of the production line, a spoil of the factory machine, or even the loss of workers' lives.

Moreover, in industrial environments, the machinery obstacle, metallic frictions, engine ambiance and equipment noise are aggressive to the radio propagation and certainly badly affect the performance of wireless transmissions.

In industrial WSNs, due to the broadcast character of radio propagation, the wireless medium is open to be accessed by both authoritative and illegal users, leading WSNs to be more in danger to the eavesdropping attack than wired sensor networks, where communicating nodes are actually connected with wire cables and a node without being connected is unable to access for prohibited activities. To be specific, as long as an eavesdropper hides in the industrial WSNs, the genuine wireless transmissions among the sensor's data can be readily overheard by the eavesdropper, which may crack its tapped transmissions and breach the confidentiality of the sensors' information communications. Therefore, it is important to examine the protection of industrial WSNs in opposition to the eavesdropping attack.

Traditionally, the cryptographic technique is demoralized to defend the wireless communications against eavesdropping, which usually rely on secret keys and can avoid an eavesdropper with limited computational ability from intercepting the data broadcast between wireless sensors. However, an eavesdropper with unlimited computing influence is still able to crack the encrypted data

communications with the aid of extensive key search (such as the brute-force attack). Moreover, the secret key allocation and contract between the wireless sensors display numerous vulnerabilities and advance increase the security risk. As a consequence, physical layer security is rising as a promising pattern for secure communications by exploiting the physical individuality of wireless channels, which can effectively defend the confidentiality of communication against the eavesdropping attack, even with boundless computational power.

The physical layer security work was pro worked by Shannon and extended by Wyner, where an information-theoretic structure was established by developing feasible secrecy rates for a traditional wiretap channel model comprising of one source, one destination and an eavesdropper. The *secrecy capacity* was found to be difference between the channel capacity of the main link as of source to destination and that of the wiretap link from source to eavesdropper. If the secrecy capacity becomes negative(i.e., the channel capacity of the main link becomes less than that of the wiretap link), the eavesdropper will be successful in intercepting the source message and an intercept event is well thought-out to occur in this case. This suggests that increasing the secrecy capacity can successfully decrease the probability that the eavesdropper effectively intercepts the source message. However, the secrecy capacity of wireless transmission is rigorously limited due to the wireless fading effect. Moreover, the occurrence of machinery obstacle, metallic frictions and engine ambiance in industrial environments makes the wireless fading varies drastically, ensuing in a further humiliation of the secrecy capacity.

To surmount this limitation, extensive research efforts have been committed to civilizing the secrecy capacity of the wireless transmission in the course of the artificial noise generation. The artificial noise aided security approaches permit the valid transmitters to produce a specifically designed intrusive signal (called artificial noise) such that only the eavesdropper is favorably affected by the artificial noise, while the deliberate receiver remains unaffected. This leads to a humiliation of the wiretap link in provision of the channel capacity without disturbing the channel capacity of the main link, resulting in an augmented secrecy capacity. The employment of multiple antennas for generating the artificial noise and displayed that the number of antennas at the legal transmitter should be more than that at the reliable receiver for the sake of proving that the main link is unaltered by the artificial noise. Furthermore, Goeckel investigated the service of cooperative relays for the artificial noise generation and established a significant security improvement in provision of the secrecy capacity.

It is pointed out that even though the artificial noise approaches can efficiently enhance the wireless secrecy capacity, supplementary power resources are devoted for generating the artificial noise to mystify the eavesdropper. The multiuser scheduling scheme for humanizing the wireless physical layer security devoid of any additional power cost and showed the security enhancement of cognitive radio networks in provision of the secrecy capacity and intercept probability. In this paper, we scrutinize the sensor scheduling in an industrial WSN consisting of a sink node and numerous sensors in the existence of an eavesdropper, conflicting from the multiuser scheduling for cognitive radio networks. More exclusively, in industrial WSNs, the wireless channel is intricate due to the machinery obstacle, metallic frictions and engine ambiance. This motivates us to deem the use of a complex fading model (i.e., Nakagami model) for characterize the industrial wireless channel, as a substitute of a Simpler Rayleigh fading model.

The sensor scheduling deliberated in this paper exhibits some reward over the conventional relay selection and the artificial noise methods in provision of sinking the system implementation complication and cutback the power resource. Exclusively, supplementary network nodes were introduced and engaged for relaying the transmissions among the source and destination, which are referred to as relay nodes. There by multiple relay nodes existing, the relay selection for wireless security augmentation, where the relay node that can attain the highest secrecy in opposition to eavesdropping is selected as the “best” relay to assist the source-destination transmissions. Even though the relay selection improves the wireless physical-layer protection, it relies on supplementary relay nodes and requires intricate synchronization among spatially distributed relays, follow-on in extra system complexity. In accumulation, the artificial noise methods advance wireless security by generating a in a classy manner designed artificial noise for confusing the eavesdropper only without disturbing the genuine destination. However, this costs extra energy resources for the artificial noise production, compared to the sensor scheduling, where a sensor with the highest secrecy in opposition to eavesdropping is scheduled for data transmission devoid of consuming any additional energy assets. Since wireless sensors are habitually motorized with limited batteries, the energy becomes one of the most valued resources in industrial WSNs, which makes the sensor scheduling further attractive than the conventional artificial noise methods commencing the energy saving perspective.

The main support of this paper is summarized as follows. An optimal sensor scheduling scheme is projected for protecting the industrial wireless transmission adjacent to the eavesdropping attack, where a sensor with the highest secrecy capacity is chosen to transmit its sensed information to the sink. While data is been transmitted it is encrypted and decrypted using RC4 algorithm. The conventional round-robin scheduling is too considered as a benchmark. Closed form expressions of the intercept probability in support to conventional round-robin scheduling and the optimal sensor scheduling schemes are derived in Nakagami fading circumstance. Finally, numerical results show the advantage of the proposed sensor scheduling scheme against the conventional round-robin scheduling in condition of the intercept probability.

Through which we are able to avoid eavesdropping to an extent. As a sequence by implementing cooperative localization we

are able to interconnect entire sensor nodes and there by predicting its power level. The interconnection allows Round Robin scheduling to be more dynamic in nature. With this we are able prioritize and schedule data transmissions without depending upon CSI solely. Numerical results demonstrate that the proposed sensor scheduling scheme outperforms the conventional round-robin scheduling in terms of the intercept probability. The numerical intercept probability comparison among the conventional and proposed sensor scheduling schemes are presented.

II. SENSOR SCHEDULING IN INDUSTRIAL WSNS

A. System Model

As shown in Fig. 1, we deem an industrial WSN con-sisting of a sink node and sensors in the existence of an eavesdropper, where all nodes are implicit with single antenna and the solid and dash lines represent the main link and wiretap link, respectively. As illustrated in Fig. 1, the presence of machinery obstacle, metallic frictions and engine ambiance in industrial environments is unfriendly to the radio propagation, which makes the wireless fading vary drastically. We thus think of using Nakagami fading model for predicting both the main channel and wiretap channel. It is critical out that the Nakagami model is more difficult than other fading models (e.g., Rayleigh fading, etc.), which is widely used in literature.

In the industrial WSN of Fig. 1, sensors correspond with the sink using an orthogonal multiple access technique such as the time division multiple access (TDMA) and orthogonal frequency division multiple access (OFDMA). When a sensor is programmed to transmit its data to the sink over a channel (e.g., a time slot in TDMA or an OFDM sub-carrier in an OFDMA), the eavesdropper tries to intercept the information transmitted.

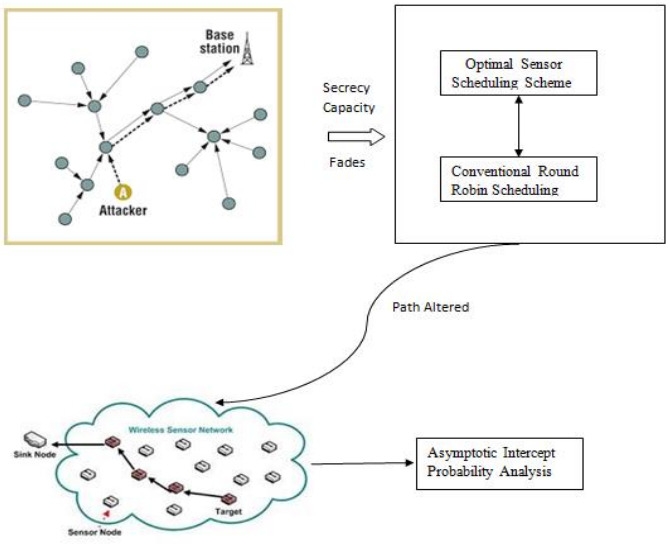


Fig. 1. An industrial WSN consisting of a sink and sensors in the presence of an eavesdropper (*e*).

Habitually, provided an orthogonal channel, a node with the highest data throughput is normally selected among sensors to access the given channel and to correspond with the sink, which aims at improvising the transmission capacity without taking into account the eavesdropping attack. By dissimilarity, this paper is paying attention on improving the wireless physical-layer security with aid of sensor scheduling. In order to effectively protect against the eavesdropping attack, the sensor scheduling consider channel state information (CSI) of both main channel and wiretap channel, differing from the conventional scheduling method, where only the CSI of main channel is considered for the throughput improvement. Here, we imagine that the CSIs of both the main channel and wiretap channel are existing, which is an theory commonly used in the physical-layer security literature.

International Journal of Innovative Research in Computer Science and Engineering (IJIRCSE)
ISSN: 2394-6364, Volume – 2, Issue – 1. January 2016

B. Conventional Round-Robin Scheduling

Conventional round robin scheduling as a benchmark, where N sensors take turns in accessing a given channel and thus each sensor has an equal possibility to transmit its sensed data to the sink. Without any loss of generality, we consider that (sensors) S_i is scheduled to transmit its signal x_i with power P_i and rate R_i, where R_i is specified to the maximum achievable rate from S_i to sink, which guarantees that ergodic capacity is achieved by the legitimate transmission.

Thus, we can express received signal at sink as

$$y_s=\sqrt{P_i}h_{is}x_i + n_s \qquad \text{----------(1)}$$

where h_{is} is a fading coefficient of the main channel from S_i to the sink and n_s represents zero-mean additive white Gaussian noise (AWGN) with variance N_0.

The channel capacity of main link from S_i to sink as

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

The signal overheard at eavesdropper e is given by

$$y_e=\sqrt{P_i}h_{ie}x_i + n_e \qquad \text{----------(3)}$$

Where h_{ie} is a fading coefficient of the wiretap channel from S_i to the eavesdropper and n_e represents zero-mean AWGN with variance N_0. We can similarly obtain channel capacity of wiretap link from S_i to eavesdropper e as,

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

Therefore, in presence of eavesdropping attack, secrecy capacity of wireless transmission from S_i to sink can be obtained as

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

C. Optimal Sensor Scheduling

The optimal sensor scheduling scheme is to maximize the secrecy capacity of the legitimate transmission. Naturally, a sensor with highest secrecy capacity should be chosen and scheduled to transmit its data to the sink. Each sensor may first estimate its own CSI through channel estimation and then transmits the estimated CSI to the sink. Once collecting all the sensors' CSI, the sink can readily determine the optimal sensor and notify the whole network.

D. RC4 Algorithm

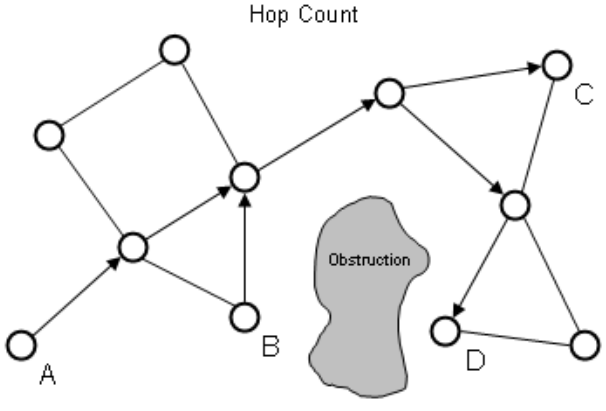
The RC4 algorithm is a stream cipher. It is remarkable for its simplicity and speed in software. Initially data that need to be encrypted is obtained and the key is selected. It follows with two string arrays. Commence one array with numbers from 0 to 255. Then employ the selected key for other array. Sequentially randomize first array depending on the array of key. Further, the final key stream is obtained by generated within the first array itself. Finally, XOR final key stream with the data to be encrypted to give cipher text.

E. Cooperative Localization Technique

The localization handles two major issues. The first is to define a coordinative system. The second is to calculate distance between the sensors. The major goal of localization is to predict physical coordinates of sensor nodes in group. Beacon nodes or anchor nodes are helpful in localizing a network. Beacon nodes are too ordinary nodes that they know their global coordinates a priori. Thus with radio hop count and Received Signal Strength Indication (RSSI), we are able analyze the location of sensor nodes available in a group.

The distance covered by one hop count can be given by,

$$d_{hop} = R(1+ e^{-nlocal} - \int e^{-nlocal/(pi)(arccost\ t - t\sqrt{1-t2}\ dt)}$$



Distance measurements are always integral multiples of d_{hop}. The time difference of arrival retrieves the factor of lateness,

$$d = (S_{radio} - S_{sound}) * (t_{sound} - t_{radio} - t_{delay})$$

The other predictive measures can be of Angle of Arrival (AoA). The localization algorithm is somehow sensitive to node density. It suffers with problem of positioning nodes near the edges of sensor field.

III. Conclusion

We analyzed the use of sensor scheduling to improve the physical-layer security of industrial WSNs against eavesdropping attack and projected an optimal sensor scheduling scheme, aiming at maximizing the secrecy capacity of wireless transmissions from conventional round-robin scheduling as a benchmark. An asymptotic intercept probability analysis was also presented to describe the diversity gains of the round robin scheduling and the optimal sensor scheduling scheme. Increasing the number of sensors, the intercept probability of the optimal sensor scheduling scheme significantly decreases, showing the physical-layer security development of industrial WSNs. To maintain secrecy over transmission of data, we come ahead with RC4 algorithm. This algorithm takes consumes only little amount of power with higher efficiency. It is followed with cooperative localization algorithm to determine distance between each node. It also helps in reduction of power usage to an extent and predicts power range at each node. Moreover we are able to predict exact location of various nodes through which we can be able to sense the active nodes and avoid obstacles. There by reducing delay and other issues in delivery of data to sensor nodes.

References

[1] Yulong Zou, *Senior Member, IEEE*, and Gongpu Wang (2015); 'Intercept Behavior Analysis of Industrial Wireless Sensor Networks in the Presence of Eavesdropping Attack' ; *IEEE transactions on industrial informatics (accepted to appear).*

[2] priority-enhanced 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.

[3] 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.
[4] 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.
[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] 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.
[7] 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.
[8] P. T. A. Quang and D.-S. Kim, "Enhancing real-time delivery of gradient routing for industrial wireless sensor networks," *IEEE Trans. Industrial Informatics*, vol. 8, no. 1, pp. 61-68, Feb. 2012.
[9] 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.
[10] 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. 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.
[11] Y. Zou, J. Zhu, X. Wang, and V. Leung, "Improving physical-layer security in wireless communications using diversity techniques," *IEEE Network*, vol. 29, no. 1, pp. 42-48, Jan. 2015.
[12] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656-715, 1949.
[13] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, 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. Information Theory*, vol. 24, 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 Journal on Selected Areas in Communications*, vol. 31, no. 10, pp. 2099-2111, Oct. 2013.
[16] 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.
[17] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Communications*, vol. 7, no. 6, pp. 2180-2189, Jul. 2008.
[18] 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.
[19] D. Goeckel, *et al.*, "Artificial noise generation from cooperative relays for everlasting secrecy in two-hop wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 10, pp. 2067-2076, Oct. 2011.
[20] 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.