International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 07 | Oct-2015 www.irjet.net p-ISSN: 2395-0072

AN EFFECTIVE SYSTEM OF DETECTING THE SPYING ASSAULT IN WIRELESS SENSOR NETWORKS

S.Monica[1], R.Prabha[2], R.Alwin[3]

[1]PG Scholar, Dept. of ECE, SNS College of Technology, Tamil Nadu, India.
[2]Asst. professor, Dept. of ECE, SNS College of Technology, Tamil Nadu, India.
[3]Asst. professor, Dept. of ECE, Coimbatore Institute of Engineering and Technology, Tamil Nadu, India.

Abstract-*Security and energy efficiency are the basic concerns in wireless sensor network (WSN) design. This paper aims to develop an energy-efficient secure scheme for industrial wireless sensor network; it consists of a sink node and multiple sensors. In the presence of a spying assault(eavesdropper) the sensors transmit their sensed information to the sink node through wireless links , the secrecy capacity of the wireless transmission measured by taking the difference between the channel capacity of main link (from sensor to sink) and the wiretap link (from sensor to eavesdropper). If the secrecy capacity becomes non-positive because of the wireless fading effect, the sensor's data transmission could be successfully intercepted by the spying assault and an intercept event occurs in this case. A sensor with the highest secrecy capacity is used to transmit its detected information to the sink. An optimal sensor scheduling scheme is proposed in this paper to protect the legal wireless transmission against the spying assault.*

Key Words:*Wireless Sensor Networks, spying assault (eavesdropping), optimal sensor scheduling.*

1. INTRODUCTION

Wireless sensor network is arising technology of great interest to many academic units and research centres on the world. Thespying assault is intense security threat towards wireless sensor network because this attack is a precondition for other attacks.In industrial WSNs, due to the broadcast nature of radio propagation, the wireless medium is open to access hence it is accessed by both authorized and unauthorized users, leading WSNs is more vulnerable to the spying assault than wired sensor networks, here the communicating nodes are physically connected with wire links and a node without being connected is not able to access for illegal activities.

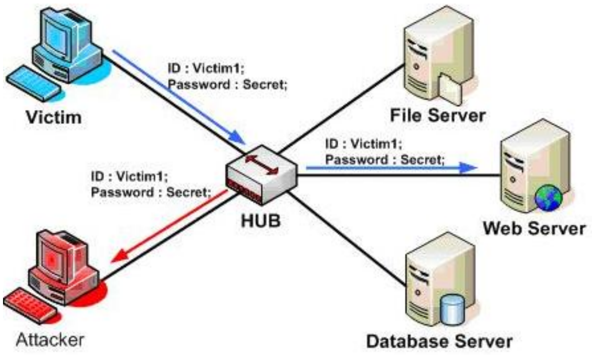

Fig.1. Spying assault in wireless sensor networks

Fig 1, described about the spying assault in WSN, here the attacker may steal all the information of network. Spying assault is the process of gathering data from a network by snooping on transmitted information and secretly listen a private conversation over a confidential communication in an unauthorized way. The data remains the same but affects its privacy. An attacker may listen secretly between any two nodes and may gather the important data regarding connection such as MAC address and cryptographic data. An attacker may also take the User Id and password. In WSNs unidirectional antennas transmit radio signals in all directions and are subsequently inclined to the spying attack. But directional antennas give out radio signals on required directions and possibly diminish the chance of the spying assault. The spying assault has two common types active and passive.

Passive attack is used to watch over an unlimited wireless session. The main condition to be satisfied here is that the attacker has the access to the area of emission. With a decrypted session the attacker has a capacity to read the data during its transmission and accumulate them indirectly by surveying the packets. This sort of attack is not based on violation of privacy, but information gathered in this way can be utilized for more dangerous sorts of assaults.

Active attack with partially known plaintext, this type of attacker watches over a wireless session and effectively infuses his own messages in order to reveal the content of the messages in the session. Precondition for this sort of assault is to access communication area and some information with respect to the message, such as IP address. The attacker has the capacity to alter the content of the packet so that the integrity of the message stays protected. Generally the aggressor changes the final IP or TCP address.

Active attack with known plaintext, this kindof attackerinfuses the known messages into the traffic in order to create conditions for decryption of the packets which are received by different wireless users. These conditions are created by creating IV sequence and message for each single message that is sent. After some time, when a packet with the same IV as in the database appears, the attacker has the capacity to decrypt the message. The best way to prevent this sort of assaults is to change WEP key frequently. Three methods can disregard the activity's trustworthinessthat are unauthorized access, high jacking attack and replay attack. In order to effectively implement these methods, it is important to apply assault strategies for protection.

The security requirements in WSN consist of Confidentiality, Authentication, Integrity, and Availability. Confidentiality is hiding the information from unauthorized access. In many applications, nodes communicate highly sensitive data. A sensor network should not leak sensor reading to neighbouring networks. Authentication ensures the reliability of the message by identifying its origin.In a WSN,the issue ofauthentication should address the following requirements: communicating node is the one that it claims tobe and the receiver should verify that the received packets have undeniably come from the actual sensor node.Data authentication can provide data integrity also.Availability ensures that services and information can be accessed at the time they are required. In sensor networks there are many risks that could result in loss of availability such as sensor node capturing and denial of service attacks.

2. RELATED WORK

2.1Cryptographic technique:

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. The cryptographic techniques is categorized into two types that are symmetric and asymmetric cryptographic. In symmetric cryptographic techniques, a single shared key is used between the two communicating nodes both for encryption and decryption. This key has to be kept secret in the network, which can be quite hard in the exposed environment where WSNs are used. Most security schemes for WSN use only symmetric cryptography, due to its ease of implementation on limited hardware and small energy demands, especially ifthe implementation is done in hardware to minimize performance loss.In asymmetric cryptography, a private key can be used to decrypt and sign data while a public key can be used to encrypt and verify data. The private key needs to be kept confidential while the public key can be published freely. Asymmetric cryptography is also known as Public key cryptography. Public key cryptography tends to be resource intensive, as most systems are based on large integer arithmetic. For a number of years many researchers discarded public key cryptography as infeasible in the limited hardware used in WSN.

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). Moreover, the secret key distribution and agreement between the wireless sensors exhibit numerous vulnerabilities and further increase the security risk. Moreover, the secret key distribution and agreement between the wireless sensors exhibit numerous vulnerabilities and further increase the security risk.

2.2Physical layer security using diversity techniques:

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. Diversity techniques are exploited to increase the transmission reliability, which also have great potential to enhance the wireless security. This technique explained the physical-layer security improvement through the use of MIMO, multiuser diversity, and cooperative diversity, respectively.

As shown in Fig. 2, all the network nodes are equipped with multiple antennas, where M, Nd and Ne represent the number of antennas at source, destination and eavesdropper, respectively. MIMO has been shown as an effective means to combat wireless fading and increase the capacity of wireless channel.

Diversity techniques is to improve the physical layer security, differing from the conventional artificial noise generation and beam forming techniques which typically consume additional power for generating artificial noise and exhibit high implementation complexity for beam former design. That increasing the secrecy capacity can effectively decrease the probability that the eavesdropper successfully intercepts the source message. However, the secrecy capacity of wireless transmission is severely limited due to the wireless fading effect.

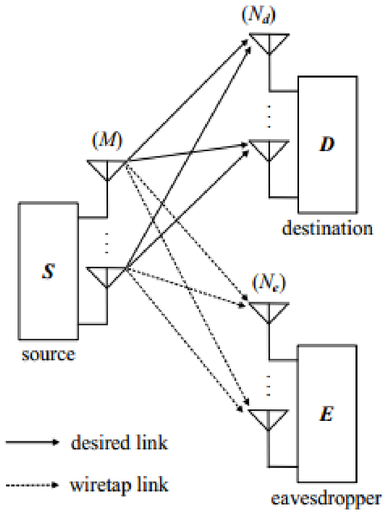

Fig.2.A multiple-input multiple-output (MIMO) wireless system consisting of one source and one destination in the presence of an eavesdropping attack

2.3Physical Layer Security via Cooperating Relays:

Cooperating Relays addresses secure communications of one source-destination pair with the help of multiple cooperating relays in the presence of one or more eavesdroppers. Three cooperative schemes are considered: decode-and-forward (DF), amplify-and-forward (AF), and cooperative jamming (CJ). For these schemes, the relays transmit a weighted version of a re-encoded noise-free message signal (for DF), a received noisy source signal (for AF), or a common jamming signal (for CJ). The determination of relay weights and the allocation of transmit power, that maximize the achievable secrecy rate subject to a transmit power constraint, or, minimize the transmit power subject to a secrecy rate constraint. For DF in the presence of one eavesdropper, closed-form optimal solutions are derived for the relay weights. For other problems, since the optimal relay weights are difficult to obtain, several criteria are considered leading to suboptimal but simple solutions, i.e., the complete nulling of the message signals at all eavesdroppers (for DF and AF), or the complete nulling of jamming signal at the destination (for CJ). Based on the designed relay weights, for DF in the presence of multiple eavesdroppers, and for CJ in the presence of one eavesdropper, the optimal power allocation is obtained in closed-form; in all other cases the optimal power allocation is obtained via iterative algorithms. The main drawback is the number of relays is no greater than the number of Eavesdroppers.

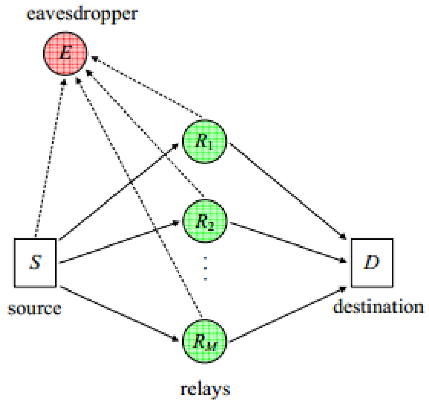

Fig.3A cooperative diversity system consisting of one source, M relays, and one destination in the presence of an eavesdropper.

Fig. 3 shows a cooperative wireless network including one source, M relays, and one destination in the presence of an eavesdropper, where M relays are exploited to assist the signal transmission from source to destination. To be specific, the source node first transmits its signal to M relays that then forward their received source signals to destination.

3. PROPOSED WORK:

In wireless networks, the transmission between legitimate users can be easily overheard by an eavesdropper for interception due to the broadcast nature of wireless medium, making the wireless transmission highly vulnerable to spying assaults. In order to achieve the confidential transmission, existing communications systems typically adopt the cryptographic techniques to prevent an eavesdropper from tapping the data transmission between legitimate users [1], [2]. But an eavesdropper with unlimited computing power is able to crack the encrypted data communications. In industrial applications, the real-time communications among the spatially distributed sensors should satisfy strict security and reliability requirements [3].

In proposed method an optimal sensor scheduling scheme is proposed for protecting the industrial wireless transmission against the spying assault, where a sensor with the highest secrecy capacity is selected to transmit its sensed information to the sink and the conventional round-robin scheduling is considered as a benchmark. The Conventional round robin scheduling and optimal sensor scheduling schemes are derived in Nakagami fading environments. Throughput efficiency increases without degrading the performance using Round robin algorithm.

3.1 System Model

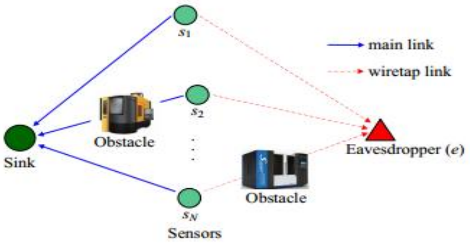

Fig.4. An industrial WSN consisting of a sink and *N* sensors in the presence of an eavesdropper (e).

As shown in Fig. 4, we consider an industrial WSN consisting of a sink node and *N* sensors in the presence of an eavesdropper, where all nodes are assumed with single antenna and the solid and dash lines represent the main link and wiretap link, respectively. Notice that the eavesdropper of Fig. 1 could be either an illegitimate user or a legitimate user who is interested in tapping other users' data information. For notational convenience, *N* sensors are denoted by $\mathcal{S} = \{si|i = 1, 2, \cdots, N\}$. As illustrated in Fig. 1, the presence of machinery obstacles, metallic frictions and engine vibrations in industrial environments is hostile to the radio propagation, which makes the wireless fading fluctuate drastically. We thus consider the use of Nakagami fading model for characterizing both the main channel and wiretap channel. It is pointed out that the Nakagami model is more complex than other fading models (e.g., Rayleigh fading, etc.), which is widely used in literature [4], [5].

In the industrial WSN of Fig. 4, *N* sensors communicate with the sink using an orthogonal multiple access method 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, the eavesdropper attempts to intercept the information transmitted from sensor. In orthogonal channel nodes are selected with highest data throughput which is selected among N sensors to access the given channel and to communicate with the sink, which will increases the transmission capacity without any attack.By contrast, this paper is focused on improving the wireless physical-layer security with the aid of sensor scheduling. In order to effectively defend against the eavesdropping attack, the sensor scheduling should 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.The presence of eavesdropping attack, the secrecy capacity of wireless transmission from *si* to sink can be obtained as

$$C\text{secrecy}\ (i) = \text{Cs}(i) - Ce(i)$$

where $Cs(i)$ and $Ce(i)$ are given by (6) and (7), respectively

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. Hence, the optimal sensor scheduling criterion is given by

$$\text{Optimal User} = \arg\max C_{\text{secrecy}}(i)$$

$i \in \mathcal{S}$

where $\mathcal{S}$ represents the set of *N* sensors

According Round-Robin Schedulingwhen the secrecy capacity becomes non-positive, the eavesdropper will succeed in decoding and intercepting the source message and an intercept event is considered to occur in this case. Hence, given that *si*is scheduled to transmit to the sink, the intercept probability of *si*-to-sink transmission is obtained as

$$P^{i}_{\text{int}} = \Pr\,[C\text{secrecy}(i) > 0]$$

4. SIMULATION AND RESULTS

In this section, we present the simulation result of throughput efficiency for various methods using different algorithm.

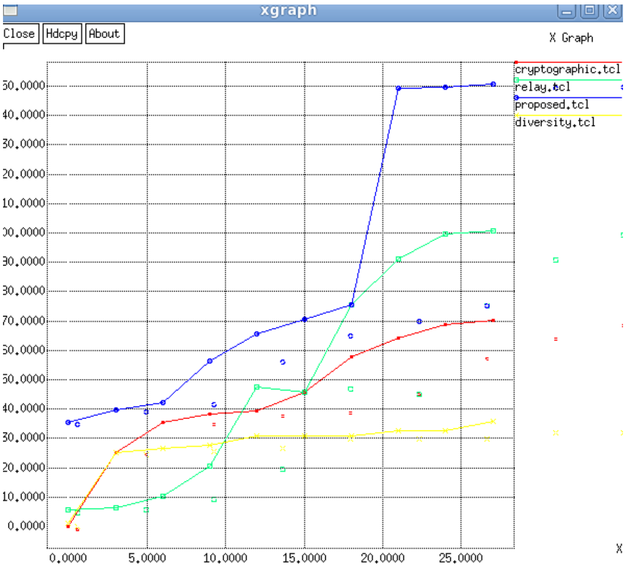

Fig.5. Number of nodes versus throughput efficiency of cryptographic, Cooperating Relays, diversity techniques and proposed work optimal sensor method.

In Fig.5, we show the throughput efficiency for various methods such as cryptographic, Cooperating Relays, diversity techniques and proposed work optimal sensor method. Here the result is obtained using NS2 simulator.

5. CONCLUSION

This paper gives overview of wireless sensor networks security issues and generic solutions for spying assault. Some applications of wireless Sensor network need a secure communication (like battlefield environment).The sensor scheduling is used 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. We also considered the conventional round-robin scheduling as a benchmark. By using these scheduling algorithms security and throughput efficiency has been increased.

REFERENCES

[1] M. E. Hellman, “An overview of public key cryptography,” IEEE Commun. Mag., vol. 16, no. 6, pp. 42-49, May 2002.

[2] S. V. Kartalopoulos, ”A primer on cryptography in communications,” IEEE Commun. Mag., vol. 20, no. 4, pp. 146-151, Apr. 2006.

[3] 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.

[4] D. Lee and B. J. Jeong, “Performance analysis of combining space-time block coding and scheduling over arbitrary Nakagami fading channels,” IEEE Trans. Wireless Communications, vol. 13, no. 5, pp. 2540-2551, May 2014.

[5] S. Hussain and X. N. Fernando, “Closed-form analysis of relay-based cognitive radio networks over Nakagami-m fading channels,” IEEE Trans. Vehicular Technology, vol. 63, no. 3, pp. 1193-1203, Mar. 2014.

[6]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.

[7] 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.

[8] Davis, R., “The Data Encryption Standard in Perspective,” Proceeding of Communication Society magazine, IEEE, Volume 16 No 6, pp. 5-6, Nov. 1978.

S[9] Daemen, J., and Rijmen, V. "Rijndael: The Advanced Encryption Standard." Dr. Dobb's Journal, March 2001.

[10] Pratap Chnadra Mandal “Superiority of Blowfish Algorithm,” International Journal Of Advanced Research in Computers Science and Software Engineering Vol 2 Issue 9, September 2012.

[11] R.L.Rivest, A.Shamir, and L.Adleman, “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” Communication of the ACM, Volume 21 No. 2, Feb. 1978.

[12]Jin Qi1 , Xiaoxuan Hu2 , Yun Ma1 , And Yanfei Sun2 “A Hybrid Security and Compressive Sensing-Based Sensor Data Gathering Scheme” Special Section On Industrial Sensor Networks With Advanced Data Management: Design And Security, Vol 3, June2015 , pp. 718- 724

[13]Nithya.S , Sivaraja.S & Sindhu.S “An Efficient SRECRP Protocol for Secure Energy Constraint Routing in MANET” International Journal of Computer Science Engineering and Technology(IJCSET) | March 2015 | Vol 5, Issue 3,51-56

[14]Saravanan,T.ArokiaArun,M.Krishnakumar,C.Karthik, S.Ponnusamy “A Protocol to Increase the Lifetime for Wireless Sensor Network” International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-5, April 2013

[15] Keita Emura, Akira Kanaoka, and Satoshi Ohta, and Kazumasa Omote, and Takeshi Takahashi “Secure and Anonymous Communication Technique: Formal Model and its Prototype Implementation” Ieee Transactions On Emerging Topics In Computing, September 2015.

[16] Bhaskar Bhuyan, Hiren Kumar Deva Sarma, Nityananda Sarma, Avijit Kar, Rajib Mall4 “Quality of Service (QoS) Provisions in Wireless Sensor Networks and Related Challenges” Wireless Sensor Network, 2, 861-868, October 19, 2010