International Journal of Management, IT & Engineering
Vol. 9 Issue 7, July 2019,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

WSNS PRONE TO SWAP ATTACKING AND EAVESDROPPING

Shafiqul Abidin[*]

Abstract

This paper evaluates the nature and impact of Swap Attack and Eavesdropping in Wireless Sensor Network (WSNs). This shows the phenomenon of how it works at the industrial site which consists of a sink node and also contains multiple sensors, and are used in broadcasting of propagation of radio waves, the transmission from the sensor to the sink and from the sensor to the eavesdropper and the difference between these two is the secrecy capacity of the transmission through wireless mode. The transmitted data will be easily intercepted by an eavesdropper if the result or the secrecy capacity will be low or under positive or non negative resulting in the sense due to wireless fading effects as such as obstacles in machinery parts or vibrations through engines. Earlier, cryptographic techniques were used to save or prevent the coded information from eavesdropper having low computing capability but now the information can be decoded easily by the eavesdropper with having high computational capability. As such in Wireless Sensor Networks, the swap attack against Directed Diffusion, in this there are basically two nodes to be considered namely called as source node and sink node. The source node to be

Keywords:
Wireless Sensor Netorks (WSNs);
Swap Attack;
Eavesdropping in WSN;
Cryptography Techniques.

[*] **HMRITM (Affiliated with GGSI P University), Delhi, India**

known from where the data are to be sent to other node and other node called as sink node where data are received. The Swap Attack works under the bad route for routing the messages. There are two modes called Norm mode and Halt mode through which swap attack is being performed whereas, in Norm mode the attacker node gets alternated between the bad and good routes in the on and off cycles whereas, in Halt mode, the attacker node can hide its Presence by putting itself in the sleep mode.

1. Introduction

The main application of Wireless Sensor Networks(WSNs) is that it is used in the army lines mainly in the surveillance [1] of battlefield and also the of this is major contributed to the industrial applications that is used in the factory efficiency from where the productivity [2] can be increased and hence results in the profit of the industry. For the purpose of use of industrial purpose it is often known as the industrial WSNs [3] and the distributed sensors in the industry results in the increment of the security purposes in the industry. The vibrations through machinery parts and engines are not good for the propagation of radio waves and causes severe damage to the work of transmission through wireless medium, which results in failure of security and machinery parts in turn will not work accordingly or properly and may in turn can cause harm to the lives of the workers working on the machines and can even result in disablement [4]. Working for WSNs at the industrial site, if it would be Wired Sensor Network not the wireless network, then there would be very less chance for the eavesdropper or for the eavesdropping attack in wired network than in comparison to the wireless network for the eavesdropper because of its broadcast nature of radio waves for its propagation as such this is used in wireless network as this is not used in wired network so less chance for intercept by the eaves- dropper. It is important to make protection of the industrial WSNs as the eavesdropper can overheard the transmission through the transmission medium that is wireless medium from the sensors' information communication [5]. By the use of cryptography, the eavesdropper can decode the information and to reduce this the new technology called as physical layer security for the security purpose from eavesdropper are to be introduced.

For the swap attack, Directed Diffusion is used in which there are basically two nodes called source node and the sink node. In the source node, the data or the query is sent to the other nodes and the node that receives the information are said to be the sink node, which takes the information. The interest is created by the sink by using naming in this protocol. The messages are being sent to the all nodes according to the interest through the broadcasting periodically from the network. The interest cache is being created by receiving interest to the nodes from which stores all the interests and gradient values which determines the data rate and tells about the direction about the data flow. Interest caches are being checked by the source node to verify that more data is to be required or not. If the interest exists in the interest cache then data message are sent through gradient list from the sink at the highest possible data rate. The messages are being dropped if no match was found, by the source node. If the match was found and hence there will be no data in the data Cache then update of cache will be done through the source node otherwise the message will be drop by the source node. Gradient paths are established in the network by the messages which are sent from the sink node. The messages sent from the sink nodes directly proportional to the data rate which results in the data can be negative or positive.

2. Background Study

Earlier cryptography techniques were used to protect the communications through wireless medium from the eavesdropper. But, as the hacking is increasing day by day and with the aid of attack known as brute force attack[6],[7] and with high computing power, the eavesdropper can be able to easily crack or decode the encrypted data. To work for security purpose or for securing communications, physical layer security [8] was introduced. The difference between the main link from the source to end point of the channel capacity and to that of wiretap link from the source point to the eavesdropper is called secrecy capacity [9]. If this would be increased then it would be difficult for the eavesdropper to intercepts the message. This would be the great limitation of the Wireless Network. By the use of artificial noise, it helps in improving the secrecy capacity and the receiver gets not affected. [10] this results in the increase of Secrecy

capacity, without having any effect of the channel capacity. For the link to be not effected, the number of antennas should be more at the legitimate transmitter then that at the receiver [11].
As artificial noise increase secrecy capacity, but for this it also requires additional power cost. For this purpose, a multiuser scheduling scheme was introduced for Wireless security improvements of the networks, without any power cost[12]. For saving power resource and also for reducing complexity of the system, sensor scheduling is introduced. For security enhancement, the relay node has the highest secrecy in against of the eavesdroppers; in relay nodes the additional network nodes are introduced [13]. Also in the addition to this, artificially noise methods ,a great strategy was made in order to improve the security through wireless medium for distracting the mind of eavesdropper without affecting the destination source. The main topics covered or summarize of the contributions in this paper are the sensor scheduling scheme was introduced for securing data from eavesdropper through wireless medium. The closed form expressions and scheme of optimal sensor were derived.

3. Eavesdrp and Sensors

In Eavesdrop different data are meant for different sensors, the sensors in the industrial site are used for industrial aspects such as motion of machines, waves generated, pressure generated by the machines, efficiency etc. For the broadcasting of the waves the sensors are used This describes about the phenomenon that consists of a sink node and also contains multiple sensors, and are used in broadcasting of propagation of radio waves, the transmission from the sensor to the sink and from the sensor to the eavesdropper and the difference between these two is the secrecy capacity of the transmission through wireless mode [14]. The main focus of this paper is on the improving the physical layer security by using sensors and the medium is wireless. The transmitted data will be easily intercepted by an eavesdropper if the result or the secrecy capacity will be low or under positive or non negative resulting in the sense due to wireless fading effects as such as obstacles in machinery parts or vibrations through engines.

Cryptographic techniques were used to save or prevent the coded information from eavesdropper having low computing capability but now the information can be decoded easily by the eavesdropper with having high computational capability[14]. The use of distributed sensors in the industry results in the increment of the security purposes in the industry. The vibrations through machinery parts and engines are not good for the propagation of radio waves and causes severe damage to the work of transmission through wireless medium, which results in failure of security and machinery parts which in turn will not work accordingly or properly. By the use of artificial noise, it helps in improving the secrecy capacity and the receiver gets not affected. For the link to be not effected, the number of antennas should be more at the legitimate transmitter then that at the receiver. As artificial noise increase secrecy capacity, but for this it also requires additional power cost. For this purpose, a multiuser scheduling scheme was introduced for Wireless security improvements of the networks, without any power cost.

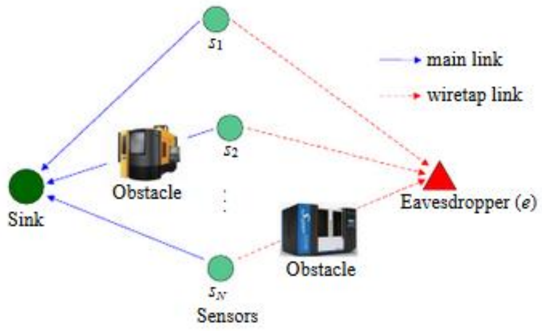

Figure 1. Industrial WSN Setup

Above figure of Industrial WSN in the presence of eavesdropper consists of a sink and N sensors [15]. In this diagram of industrial WSN, it consists of sink; eavesdropper and the lines represent the figure are wiretap link and the main link. N sensors are considered which are represented by S1, S2… Sn. In this N sensors communicate with the sink and eavesdropper intercepts the information passed from sensors to sink and the transmitted medium is wireless transmitted medium. This concept is used in Nakagami model and hence This model is used mainly in literature.

4. Swap Attack

For the swap attack, we consider the security reasons for preventing the attack. Directed diffusion and leach is some sensor routing protocols. Security in sensor network is different than traditional network because of computing power. For security purpose encryption techniques are used and also the use of antennas is there. In this paper the topics which are covered or highlighted issues represents the routing should be safe and also represents how to extend the directed diffusion and directed diffusion should be safe. The security should be the main reason for this as to prevent them from the attacks. For routing, good path should be selected so as to reduce energy[16].

The delivery of data should be secure by doing secure Diffusion which reduces traffic in the networking or sending of the data and also provides good quality for the delivery of the data. If the network ability is reduced or transmission of data will be `low then the transmission of message will be suspicious. The main focus of the protocol of routing diffusion is to be the energy efficiency of the network by using hop- to-hop not end-to-end communication protocol.

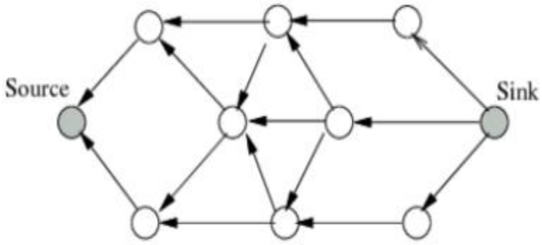

Figure 2. Interest Propagation

Interest is a type of message which describes what the user wants.

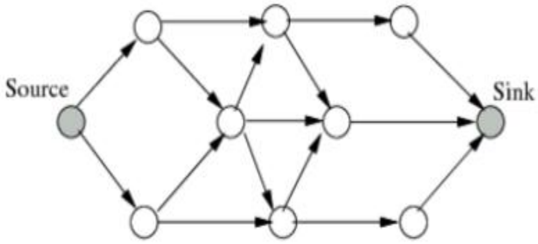

Figure 3A. Initial Gradient Setup

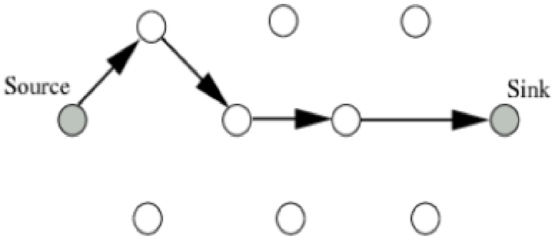

Figure 3B. Send Data & Path Reinforcement

Aforementioed figures describe about the flow of direction of data and also the data rate and the interest is received from the adjacent nodes . When there will be the activation of the attack then there will be more nodes are included in the route or path and hence this results in the performance of network degradation.

5. Conclusion

A Wireless Sensor Network (WSN) sometimes called a Wireless sensor and actuator network) (WSAN). The WSN is build of "nodes" –from few to several hundred or thousand, where each node is connected to one or more sensors. The main application of this are used in industry monitoring and also in military purpose .the focus of this paper is mainly on the betterment of the physical layer security through wireless medium with the help of the sensor scheduling[17]. This is done to increase the security from the eavesdropper. The eavesdropping attack is considered in this paper in which sensors communicate with the sink and eavesdropper intercepts the information passed from sensors to sink and the transmitted medium is wireless transmitted medium and the swap attack was being discovered only the bad routes for routing not the good one path.We can say in swap attack that countermeasure should be used and using the on-off timer, the time gets divides according to different time divisions. By the use of artificial noise, it helps in improving the secrecy capacity and the receiver gets not affected, this results in the increase of Secrecy capacity, without having any effect of the channel capacity.

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. Industrial Informatics, 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 home automation,”IEEE Trans. Industrial Informatics, vol.1, no. 1, pp.803-812, feb.2014.

[3] 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.

[4] T.M. Chi ewe 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.

[5] 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.

[6] 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.

[7] 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.

[8] Shafiqul Abidin “WSN – An Emerging Technology and its Security Measures” International Journal of Computer Science and Engineering, Vol 5, Issue 9, pp 260-264, September 2018.

[9] S.K. Leung-Yan-Cheong and M.E. Hellman, “The Gaussian wiretap channel,” IEEE Trans. Information theory, vol.24, pp.451-456, Jul. 1978.

[10] S. Goel and R.Negi,”Guaranteeing secrecy using artificial noise,” IEEE trans. Wireless Communications, vol. 7, no.6, pp. 2180-2189, Jul. 2008.

[11] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] F.Akyildiz and I.H. Kasimoglu, "Wireless Sensor and Actor Networks: Research Challenges," Ad Hoc Networks, vol. 2, no.4 pp. 351-367, Oct. 2004.

[17] Shafiqul Abidin and Mohd Izhar "Attacks on Wireless and its Limitations" International Journal of Computer Science and Engineering, Vol 5, Issue 11, pp 157-160, November 2017.