International Journal of Pure and Applied Mathematics
Volume 119 No. 14 2018, 1641-1646
ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

A SURVEY ON ATTACKS AND SECURITY GOALS IN WSN

N. Poongavanam[1], P. Lathaparthiban[2], K. Vadivelu[3], H. Sathiyamoorthi[4] and N. Balaji[5]
[1]Research Scholar, [2]Assistant Professor, Department of CS, School of Engineering Pondicherry University, India.
[3]M.Tech, Department of ECE, Prist University, India.
[4,5]Assistant Professor, Department of CSE, SVCET, Pondicherry University, India.

ABSTRACT— The largest innovation in telecommunications is the Wireless Sensor Networks. Wireless Sensor Networks (WSN) are currently being used in a wide range Eg. Battle field monitoring, Residential monitoring, disaster Maintenance, health monitoring or industrial control.Taking advantage of WSN in today's world has become a research area due to the huge number of applications.This paper gives idea about the fundamentals, challenges and security goal in WSN and also the different types of attacks like Sinkhole Wormhole Attacks in WSN.Finally concluded that it will help readers to have good feedback on wireless sensor networks.

Keywords: WSN, Sinkhole and Wormhole Attacks.

INTRODUCTION

We perform all manifestation algorithms to create an example of differential digestion as well as small receptors, including an accelerated variation plan. The rapid development of the technology of technologies of electronic components of microprocessors has been made possible to develop devices with size and weight gain, with lower cost and low power. WSNs typically have a large number of (hundreds or thousands) wide resources and sensor nodes containing one or more base stations (BSs) or sink (Figure 1), specifically the gateway to the user or another network. Nodes can collect and transmit ecological data (temperature, pressure, humidity, noise levels, etc.) in an automated manner (with wireless links). Node plays in WSN: Collect data and data back to base station.Taking advantage of WSN [17-23] in today's world has become a research area due to the huge number of applications. WSN's application involves disaster control, residential monitoring, safety monitoring, and home entry system.

I. SECURITY GOALS IN SENSOR NETWORKS

Specific alarm websites system are temporarily organized, security goals protect these types of security by traditional websites and are ideal for temporary alert system networks for primary interruptions. Primary and other key objectives are often called standard security protection targets in terms of energy, privacy, adaptance and proof, while security targets are sorted. Additional goals information flavors, time synchronization, self-organization and shielded localization.

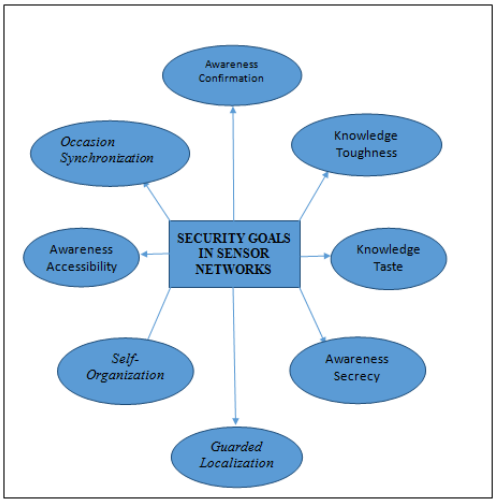

Fig.1. Security Goals in Sensor Networks

A. Awareness Secrecy

In fact, there is an ability to pay equipment through strongly-illiterate advocate to make sure that any kind of home security system is confidential. One of the most serious injuries in the security process is serious. Strict warning node should not show their understanding to neighbours.

B. Awareness Confirmation

Challenges contracts in full burger alarm web sites only require customization; Opponents may give additional simulation agreements [14]. Receiver receives an

understanding of the identity of the sender along with the receiver. In reality, an awareness can be achieved through disproportionate and unequal forms, in which the key obtained by the nodes shows crucial keys. Because the clipboard is challenging for some specific authentication individually, without the person and immediate treatment associated with alarm websites.

C. Knowledge Toughness

The dependence on the knowledge of the thieves alarm websites identifies the ability to discern that it is not necessarily unchanged, altered, in addition to the convenience of having data.

Although the procedure involves the secretive processes, there is a possibility, even if the data depend on the dependencies

D. Awareness Accessibility

It chooses which features have the ability to use these solutions with the ability to solve, and the process can be traced to the peripheral devices. However, the failure of the part under the head, might as well team leader, will slowly alert the full burger alarm. Hence there is a major emphasis on getting comfortable performance with strong performance.

E. KnowledgeTaste

Although confidential and data-dependency is generally confident, there can be a desire to assure every message grade. Unauthorized, awareness ensures high quality [2] data is complete, but warranties are actually repetitive to existing devices. This particular challenge can be helpful to end any challenge, as well as once again the relevant dining table, to have some awareness freshness for the deal.

F. Self-Organization

Instant housing security systems is often an frequent activity process, which corresponds to each requirement that each burglar alarm node often has plenty of self-management and self-management before different conditions. Warning You will find the entire mounting structure targeting process operations within the network. The healthy operation of this instantly gives the home security system a great deal of security. The self-organism can actually be very well secured with loss as a result of strong hit together formally secured, secure without the need for a warning process.

G. Occasion Synchronization

Most home securityapplication systems are based on a few forms of moment synchronization. Most often, the receivers need to recognize this end because it provides and supplying techniques between a pair of pairing sensor sensors. Call for synchronization [4] to monitor more cooperative housing security systems.

H. Guarded Localization

In general, the activity related to a warning process may be based on their ability, possibly identifying each burglar alarm from network. A strict warning process derived to identify errors should be a way to identify the correct location files. However, an opponent can easily identify the advantages implicated by extracting the files in the non-preserved area and rewrite the signals.

II. ATTACKS IN SENSOR NETWORKS

WSNs suffer various attacks (Fig 2). Throughout WSNs, this kind of problems is often:

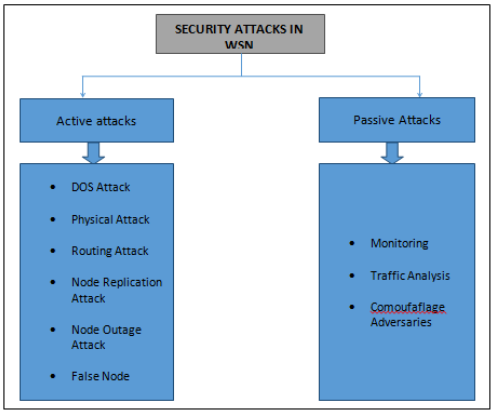

Fig.2. Security Attacks in WSN

The passive attack is limited to listening and analyses exchanged traffic. This type of attacks is easier to realize, and it is difficult to detect. Since, the attacker does not make any modification on exchanged information. The intention of the attacker can be the knowledge of confidential information or the knowledge of the significant nodes in the network, by analysing routing information, to prepare an active attack.

In the active attacks, an attacker tries to remove or modify the messages transmitted on the network. He can also inject his own traffic or replay of old messages

to disturb the operation of the network or to cause a denial of service. Among the most known active attacks.

III. ROUTING ATTACKS

WSNs are designed in layered form; this layered architecture makes these networks susceptible and lead to damage against many kinds of attacks. For each layer, there are some attacks and defensive mechanisms. Thus, WSNs are vulnerable against different routing attacks, such as DoS attacks, traffic analysis, privacy violation, sinkhole and other attacks to routing protocols (Fig.3); since in the WSNs, sensor nodes collaborate to each other for routing; the collaboration between sensors is susceptible to routing attacks.

Attackers can gain access to routing paths and redirect the traffic, or propagate or broadcast false routing information into the WSNs

In the descriptions below, note the difference betweenattacks that try to manipulate user datadirectly and attacks that try to affect the underlyingrouting topology.

We start with some general discussion of thesetypes of attacks; we show how theseattacks may be applied to compromise routingprotocols

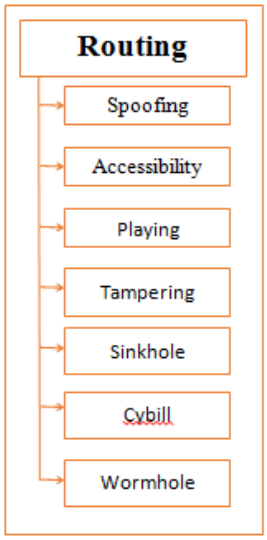

Fig.3.Routing Attacks

A. Spoofing

Virtual cryptography procedures can communicate realistic mystery and legitimacy, communicating with outreach stations, outbreaks of plus customization, box replay problems might as well as spoofing with a packets.

B. Accessibility

Attack on Community Access: Problems with access are also known as rejection-service attacks. DoS Problems Maybe any strategy of your index network is the strategy.

C. Playing

It is a term of invasion, which interferes with wavelengths, which apply to the network's nodes [3,5]. Refers to blocking anything, is consistent with embarrassing the entire community and being less powerful and difficult to address the reduced area of the network. For example, if the compact seriously sacrificed portion from the network's index nodes provides you with the possibilities to prevent the entire community from choosing the options you are blocking on the network. In addition to the scattering rule, such as regulatory rights volume jumping beside volumes with spread-spectrum transmission [4]. Frequency-Hopping Projection Option (FHSS) is a process commonly used to change the induction. It uses a duplicate arbitrarily modeled algorithm along with a receiver for transmitter through several volume programs by rapidly moving your bag. Since an abuser is unable to regularly examine the procurement procurement system, an assailant can not be employed at the appointed time during the delivery period. However, since the dominance of the diolable wavelengths is limited, one alternative can be quickly replaced by a huge area of an volume band. However, the more important style and design of this approach requires glitter and so it makes it easier to use in WSNs. Generally, in order to lower the cost of minimum electricity demand demands, index machines are linked to the use of a single-frequency and are therefore phenomenal in preventing attacks.

D. Tampering

Another physical layer was damaged. Given the physical access to a node, the attackers may collect sensitive information such as cryptographic keys or other data in the node. The node can be changed or replaced to create a compromised node that controls the

attack. A defence for this attack is to damage the node's physical package. However, the sensor nodes are thought to be inappropriate in WSN due to additional cost. This suggests that a security scheme should be considered as a situation where the sensor nodes are compromised. Nevertheless, in many cases, the sensor nodes are generally believed to be no more cost-effective within WSNs. The following points must also be taken into account by a thief program that the sensing unit nodes are compromised.

E. Sinkhole

In a sinkhole strike, the nodes that make a rival's sacrifice appear to be the edge of the nodes by duplicating the new information and facts [5]. Particularly the border nodes are going to choose the next node sacrifice node for you by way of its facts. The choice of this type of attack is quite simple, because the network passes through the node of all traffic adversary from a large area.

F. Cybill

A node or device may have several identities that are not legally valid. It does not cheat any node, but it is faster, it identifies only one of several nodes, which can cause redundancies in routing protocols. Cybill attacks have reduced data integrity, security and resource utilization. It can also maintain storage, routing techniques, gas resource allocation and misconduct identity. Hundreds of sensor nodes communication network can be created on a sensor network. These sensor passes through wireless communication center between nodes. These nodes are the specified communications of the nodes of a specified number. There are many encryption methods available to avoid external attack on nodes, but can also mount the attack on the nodes in the communication network. One of these insider attacks is called Sybil attack, which is the node spoofing the other node is called the Sybil node and the other is the normal node. Nodes must communicate with just one person in the correct information system. But here, the node comes in as an internal node in its other forms and launches the attack on the network. Cybill Node seeks to communicate with neighbour nodes using the identification of a general node, and a node in this process gives many nodes in the area to other nodes in the network. Hence, it is considered an additional organization of a misconduct node. This causes confusion in the network and it will collapse. A wrong node that enters the network with different ID.

G. Wormhole

Wormhole attack is one of the most serious attacks to detect and protect the wireless sensor network.

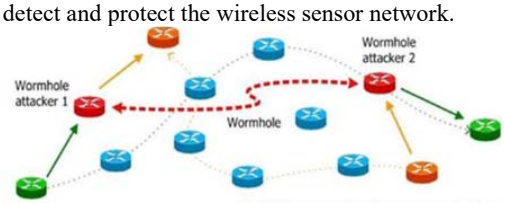

Fig .4. Shows Wormhole Attack

In this attack, malicious attackers receive packets from one area of the network, tunnelling them through the tunnel and releasing them to another location. An example of the Wormhole attack on wireless sensor networks as shown in Fig 4. Wormhole link will be arranged by various means, eg, using Ethernet cable, distant wireless transmission or optical link. Once the Wormhole link is established, the hostile broadcasts are captured at one end and send them via the Wormhole link and replay them at the other end.

IV. CONCLUSION

This paper provides security basics, challenges, and security goals in the wireless sensor network. In challenges, WSN defines regulation of security, some restrictions on lack of central control, remote location and erroneous opportunities. This article includes security attacks on wireless sensor networks. The reader helps to see the sheet's basics, challenges, security targets and attacks on wireless sensor networks.

V. REFERENCES

[1] Fei Hu and Neeraj K. Sharma, “Security considerations in ad hoc sensor networks”, Ad Hoc Networks, Published by Elsevier Science, 2005, pp. 69–89.

[2] Rajeev Shorey, Akkihebbal L. Ananda, MunChoon Chan, and Wei Tsang Ooi, “Mobile, Wireless, and Sensor Networks: Technology, Applications, and Future Directions”,John Wiley & Sons, Inc, 2006.

[3] David Boyle, Thomas Newe. “Securing Wireless Sensor Networks: Security Architectures”, Journal of networks, Volume 3, No. 1, 2008.

[4] Daniel Cvrcek, PetrSvenda, “Smart Dust Security – Key Infection Revisited”, Electronic Notes in Theoretical Computer Science 157, Elsevier, 2006, pp. 11–25.

[5] John Paul Walters, Zhengqiang Liang, Weisong Shi, and VipinChaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid, and Pervasive Computing, Auerbach Publications, CRC Press 2006.

[6] Song, Ning, LijunQian, and Xiangfang Li. "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach." Parallel and distributed processing symposium, 2005.Proceedings.19th IEEE international.IEEE, 2005.

[7] Azer, Marianne A., Sherif M. El-Kassas, and Magdy S. El-Soudani. "An innovative approach for the wormhole attack detection and prevention in wireless ad hoc networks." Networking, Sensing and Control (ICNSC), 2010 International Conference on. IEEE, 2010.

[8] Win, KhinSandar. "Analysis of detecting wormhole attack in wireless networks." World Academy of Science, Engineering and Technology. 2008.

[9] Khalil, Issa, SaurabhBagchi, and Ness B. Shroff. "Liteworp: Detection and isolation of the wormhole attack in static multihop wireless networks." Computer networks 51.13 (2007): 3750-3772.

[10] Thalor, Jyoti, and Ms Monika. "Wormhole Attack Detection and Prevention Technique in Mobile Ad Hoc Networks: A Review." International Journal of Advanced Research in Computer Science and Software Engineering 3.2 (2013).

[11] Qian, Lijun, Ning Song, and Xiangfang Li. "Detecting and locating wormhole attacks in wireless ad hoc networks through statistical analysis of multi-path." Wireless Communications and Networking Conference, 2005 IEEE. Vol. 4. IEEE, 2005.

[12] Nait-Abdesselam, Farid, BrahimBensaou, and TarikTaleb. "Detecting and avoiding wormhole attacks in wireless ad hoc networks." IEEE Communications Magazine 46.4 (2008): 127-133.

[13] Chiu, Hon Sun, and King-Shan Lui. "DelPHI: wormhole detection mechanism for ad hoc wireless networks." Wireless pervasive computing, 2006 1st international symposium on. IEEE, 2006.

[14] Poovendran, Radha, and LoukasLazos. "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks." Wireless Networks 13.1 (2007): 27-59.

[15] Kannhavong, Bounpadith, et al. "A survey of routing attacks in mobile ad hoc networks." IEEE Wireless communications 14.5 (2007).

[16] Ji, Shiyu, Tingting Chen, and Sheng Zhong. "Wormhole attack detection algorithms in wireless network coding systems." IEEE trasaction on mobile computing 14.3 (2015): 660-674.

[17] Ganesan, M., PremKumar, A., KumaraKrishnan, S., Lalitha, E., Manjula, B., "A novel based algorithm for the prediction of abnormal heart rate using Bayesian algorithm in the wireless sensor network", (2015) ACM International Conference Proceeding Series, 06-07-March-2015, art. no. 2743118,

[18] Pradeepa, D., Halima Begam, T., Rajaguru, D., Jaiganesh, S., Vengattaraman, T., "A contemporary research analysis on discrete wireless sensor networks routing algorithms", (2015) International Journal of Applied Engineering Research, 10 (3), pp. 2039-2042.

[19] Satyanarayana, K.V.V., Kathavate, P., Reddy, L.S.S., "Energy aware routing protocol with QoS constraint in wireless multimedia sensor networks", (2017) Journal of Advanced Research in Dynamical and Control Systems, 9 (Special Issue 12), pp. 1449-1457.

[20] Buvanesvari, M., Uthayakumar, J., "Fuzzy based clustering to maximize network lifetime in wireless mobile sensor networks", (2017) Journal of Advanced Research in Dynamical and Control Systems, 9 (Special Issue 12), pp. 2133-2143.

[21] Rajakumar, R., Dhavachelvan, P., Vengattaraman, T., "GWO-LPWSN: Grey Wolf Optimization Algorithm for Node Localization Problem in Wireless Sensor Networks", (2017) Journal of Computer Networks and Communications, 2017, art. no. 7348141, .

[22] Uthayakumar, J., Vengattaraman, T., "A simple data compression algorithm for anomaly detection in Wireless Sensor Networks", (2017) International Journal of Pure and Applied Mathematics, 117 (19 Special Issue), pp. 403-409.

[23] Uthayakumar, J., Vengattaraman, T., "Data compression algorithm to maximize network lifetime in wireless sensor networks", (2017) Journal of Advanced Research in Dynamical and Control Systems, 9 (Special Issue 12), pp. 2156-2167.