Threats and Security in Wireless Sensor Network

Manish Kumar

Research Scholar, JJT University, Jhunjhunu, Rajasthan, India. manishnit4u@gmail.com

Abstract - With an increasing amount of people getting connecting to the networks, the security that cause massive harm are also increasing. So; network security is major part of the network that need to be maintained because the information is being passed between the computers and are more vulnerable to attacks. As far as security of the network is concerned; security plays a vital role to protect both wired and wireless networks. Although, the wired and the wireless networks tends to achieve same goals but they differ at the technical level. In case of wireless networks different security mechanism are used depending upon the nature of wireless communication. The wired networks are more secure as they are connected through the Ethernet. Whereas, the wireless networks are less secured as in case of wireless network the connection is formed over optical fibers. Due to the security constraints in wireless network it becomes essential to configure the security in the wireless communication so as to avoid malicious action such as hacking [S. Xiao et.al, 2010].WSN is a part of wireless networks. WSN is a highly distributed network that can to work autonomously in a harsh environment. Many sensors nodes are very important and which are deployed in WSN in order to monitor some specific phenomena. Security is essential as during communication and data collection, low cost sensor nodes need to transfer the correct and meaningful data to the sink. In order to develop the security mechanism for WSNs, it is essential to know the threats, security requirements, challenges as well as the types of attacks that are involved in WSNs. The present paper is an attempt to explain in detail about the threats and security in wireless sensor network.

Key Terms: - Wireless Sensor Network; Security Requirements; Layer-based Attacks; Countermeasures.

I. INTRODUCTION

A wireless sensor network (WSN) is a mesh network. It consists of a set of compact and automated devices which are known as sensing nodes. It has its own resources and computational competence and fitness. These nodes and knots are spreaded transversely which is and it an ad hoc network is being represented by this well-defined area. This area is having the capacity and ability to communicate among themselves. There are some o classes of certain special nodes in a wireless sensor network and these nodes have the ability and capability to process and store the information which is being collected over the network. When the researchers compare these nodes with sink nodes; they always find that sink nodes are popularly known as good as these nodes. It is observed that the communication between two nodes is over multiple hops whether these two nodes are not within each other's transmitting and receiving range [Berkeley MICA, 2003].

The network architecture is crucial for WSNs so as to enable them to be scalable and reliable. Moreover, the architectural design of WSNs enables the network to be active and workable. Wireless sensor network are used to gather essential data from the installed environment where they are embedded. The data collected is processed by the sensor nodes and then forwarded over non-secure channels to sink node for further processing. The sensor networks have vast application in the areas of environment, infrastructure, public safety, medical, security and transportation. Wireless sensor network are used to gather essential data from the installed environment where they are embedded. The data collected is processed by the sensor nodes and then forwarded over non-secure channels to sink node for further processing. The sensor networks have vast application in the areas of environment, infrastructure, public safety, medical, security and transportation. The main purpose of Wireless sensor network is used to collect necessary data from the fitted atmosphere where they are fixed. This collected data which is being processed by the sensor nodes and then forwarded over non-secure channels to sink node for further processing. It is having vast application in the areas of environment, infrastructure, public safety, medical, security and transportation.

Energy efficient: Energy in WSNs is used for different purpose some to mention are computation, communication and storage. Most of the energy is consumed by sensor nodes during the communication. When these nodes run out of the power they often become inevitable as if it does not have any possibility to recharge.

DOI : 10.18231/2454-9150.2019.0116

Objectives:

To provide security services in order to protect the information and resources from attacks is the sole purpose of the WSN.

Following are the standard security requirements in WSN [R. Di Pietro et.al, 2003]:

II. THREATS IN WIRELESS SENSOR NETWORK

Owing to the broadcast nature of the wireless network transmission medium, it has become more susceptible to security attacks. The targeted WSNs is being easily attacked by an attacker due to sensor nodes which are being deployed randomly in the environment in wireless sensor networks [S. K. Singh et.al, 2011].

Different perspectives can be studied regarding the security of WSNs. This work presents a threat model that can distinguishes between two major types of attacking classes [D. G. Padmavathi et.al, 2009.]- [T.G. Lupu et.al, 2009] which are based on attacker's location and attacker's strength.

Attacks are of two kinds i.e. internal and external. These attacks have been classified on the basis of privileges and the knowledge of the attacker. These are popularly known as internal and external attack. This depends upon, whether the attacker is a trusted node of the network or not [S. Mohammadi et.al, 2011].

Internal attacks:

Internal attack occurs when a trusted node of the network acts abnormally or illicitly. In case of internal attacks the compromised nodes are used to attack the network, in order to destroy or disrupt the network. As the legitimate keys are present with the attacker, an attacker has the ability to perform various attacks on the network and that too without being easily detected. The internal attacks constitute the main security challenge in WSN.

External attacks:

The external attack can be defined as the attack that is performed by a node that lies outside the network. In this way; the attacker nodes have no internal information of network. Attacks can be categorized as passive and active attacks:

Passive attacks:

The passive attack does not effect on the network directly as it lies outside the network. Passive attacks comprise of eavesdropping and monitoring of packets exchanged within a WSNs. Such attack does not interruption the communication process. In this an attacker only inject the useless packets in order to physically destroy the nodes, or drain the receiver's battery. For preventing such type of attacks encryption and authentication techniques are used.

Active attacks:

In active attacks, the normal activity of the network is disrupted. In such attacks information interruption, modification, traffic analysis, and traffic monitoring can be performed [P. Goyal et.al, 2010]. Active attacks include impersonating, jamming, and denial of servicing and message replay presented by C. Karlof et.al, 2003 which includes laptop-class and mote-class attackers.

Attack based on attacker's strength:

An attackers uses different types of devices so as to attack the targeted network. Devices that are used by the attacker can have different radio antenna, computation power and other capabilities. The following two categories:

Laptop class:

As far as **Laptop type of class attack is concerned;** powerful devices to attack the network can be used by the attackers. These powerful devices possess faster CPU, larger battery power, bigger memory space and high-power radio Trans receiver.

Mote-class:

As far as **Mote-class** type of **attack is concerned;** one or more sensor nodes with the same or similar capabilities in order to perform attacks can be used and recycled by an attacker.

III. SECURITY REQUIREMENTS

Authentication: Authentication is one of the main issues for security in WSN. It is also used to determine the authenticated node and check whether the data received was send from the authorized node or not.

Confidentiality: It ensures that a transmitted message is understandable by the recipient only and nobody else can understand the message.

Integrity: It ensures that a no modification in message is performed while sending message from one node to another.

Freshness: It ensures that the data is fresh and unused in order to save the network from packet replay.

Secure management: It ensure the management of the cryptographic keying material in the network.

Availability: It ensures the availability of desired network even when there is presence of denial- of-service attacks.

Internal Attacks in WSN:

As sensor nodes are cheap and are deployed in open environment where they can be easily be compromised. Therefore from such a compromised node an attacker can

DOI : 10.18231/2454-9150.2019.0116

easily extract all the sensitive information. Some of the characteristics of the compromised are as follows [M. Ahmed et.al, 2012] [E. Shi et.al, 2010].Compromised nodes are reprogrammed by injecting malicious code by an attacker. So, the compromised node steals the information from the network and can disrupt the normal functionality of the network.

Compromised node appears to communicate with normal sensor nodes as these compromised nodes have the same radio frequency as that of other sensor nodes. It is easy for an attacker feels an easy to entree cryptographic information through the compromised nodes, owing to which the compromised node can easily increase the confidence of other sensor knots. Although such type of attacks are difficult to stop or seize. Due to this, security in WSN from internal attacks has become a challenging task.

In several applications, the data collected from the sensing nodes are required to be confidential and authenticated. When the security factor is not present in the network then a malicious node can easily intercept the private information and could even send false messages to other nodes.

Some of the major attacks are illustrated below:

Denial-of-Service (DOS) attack:

These types of attacks are produced by a malicious action or by an unintentional failure. The simplest method of this attack involves exhaustion of available resources of the targeted node. Exhaustion of available resources can be done by sending multiple request to the targeted node, so that the targeted node is unable to respond to the normal traffic. This results in making the service or node unavailable for the others.

Wormhole attack:

In wormhole attack, a malicious attacker firstly receives packets from preceding node, forwards those packets through the tunnel and then finally releases those packets to another location. This enables the attacker to send packets, routing information etc., through a tunnel to the outside network to another node although the network is same.

The malicious node usually achieves the faith of the neighbour node as an authorized node [A.-S.K. Pathan et.al, 2007]. An attacker uses a wormhole for the purpose of a base for eavesdropping, not promoting packets in DoS like manner, and altering information packets before forwarding them.

Sinkhole attack:

In sinkhole attack a mischievous node attracts all the traffic in the sensor network towards it, by forging the routing information [J. Jeong et.al, 2007, R. Mulligan et.al, 2010]. At the end all the nodes surrounding the malicious node chooses it as a next node to route their packets (data). In such type of attacks all the traffic within the network flows through the malicious node.

Sybil attack:

In Sybil attack, a single node possesses multiple identities so as to disrupt the accordance among the entities. Sybil attack tends to degrade the integrity of data, resource utilization. Douceur proposed the concept of Sybil attack in P2P networks [J. R. Douceur, 2002]. In this a malicious node forges multiple identities in order to mislead the network and let the neighbouring nodes believe that they have multiple trusted neighbours [Ssu et.al, 2009]. In this attack, determination of position of malicious node is considered to be hard task as a malicious node may appear at different place at same time.

Selective forwarding attack:

Selective forwarding attacks is also known as gray hole attack. In this an attacker creates a malicious nodes that will selectively forward only certain set of messages and will drop others [C. Karlof et.al, 2003]. This type of attack is difficult to detect as the node behaviour changes from malicious to non-malicious with respect to time.

Black hole attack:

The black hole assault in remote sensor organize makes to bargain course foundation in a system. A malignant hub that communicates a directing message with an additional normal high power can misdirect countless. These hubs endeavor to utilize the malevolent hub as their next jump in their course to the sink. Be that as it may, the hubs those are at a distant separation would just send their messages in the condition of ignorance. A comparable situation, black hole opening assault going about as a vindictive hub can persuade every neighboring hub those are ordinarily different jumps from the sink hub that they are really one bounce far from the goal hub. These hubs accordingly attempt to send their bundles straightforwardly to the sink hub, which is unfit to hear them. In black hole assault the assault hub retains or drop every one of the parcels end-course to the goal.

IV. SUMMING UP

To conclude; the research scholar, at last comes to the point that it is quite impossible to provide security in a wireless sensor network because it a very difficult and tough task. Although; in the present paper; the researcher has discussed the several security threats present at different layer of wireless sensor network. To distribute key among sensor nodes is also a challenging task. At present; security in a wireless sensor network in all levels is not possible but it can be predicted that the security scheme will be well established for individual layer in the days and years to come. The researcher further tells that to give security in a remote sensor organize is a testing task. In the

DOI : 10.18231/2454-9150.2019.0116

present paper, the researcher has also attempted to examine the different security dangers present at various layer of WSN convention stack. Identification and countermeasures of certain dangers in WSN isn't at all simple. Key dispersion among sensor hubs is additionally a testing task. In present time, a large portion of the security plans depend on explicit system models and complete security show for all layers isn't at all present in spite of the fact that, in future, the security plan may turn out to be settled for individual layer. In this paper; the research scholar tries to discuss in detail about the threats and security in wireless sensor network.

REFERENCES

[1] Ali Tufail, Ki-Hyung Kim, "A Backbone Assisted Hybrid Key Management Scheme for WSN", IEEE 978-0-9564263-8/3 (2011).

[2] Marcos A. Simplício Jr., Cintia B. Margi, Paulo S.L.M. Barreto, Tereza C.M.B. Carvalho, " A survey on key management mechanisms for distributed wireless sensor networks", Computer Networks 54 2591 - 2612 (2010).

[3] Yang Xiao, Venkata Krishna Rayi , Bo Sun , Xiaojiang Du , Fei Hu ,Michael Galloway, "A survey of key management schemes in wireless sensor networks", Computer Communications 30 (2007) 2314– 2341.

[4] Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh, "Overview of Security Issues in Wireless Sensor Networks", 2011 Third International Conference on Computational Intelligence, Modelling & Simulation.

[5] Johnson C. Lee And Victor C. M. Leung, University Of British Columbia Kirk H. Wong, Jiannong Cao, And Henry C. B. Chan, "Key Management Issues In Wireless Sensor Networks: Current Proposals And Future Developments", IEEE wireless communications (2007).

[6] Hiren Kumar, Avijit Kar, Deva Sarma, "Security Threats in Wireless Sensor Networks", IEEE 1-424401 74-7 (2006).

[7] Syed Muhammad Khaliq-ur-Rahman Raazi, Zeeshan Pervez and Sungyoung Lee, "Key Management Schemes of Wireless Sensor Networks: A Survey".

[8] H.-J. Kim, et al., "A method to support multiple interfaces mobile nodes in PMIPv6 Domain," Presented at the proceedings of 2nd International Conference on Interaction Sciences, (Seoul) Korea (2009).

[9] W. Xu, et al., "The feasibility of launching and detecting jamming attacks in wireless networks", pp. 4657 (2005).

[10] H. K. Kalita and A. Kar, "Wireless sensor network security analysis", (IJNGN), vol. 1, pp. 1–10 (2009). [11] Y. C. Hu, et al., "Packet leashes: a defense against wormhole attacks in wireless networks", pp. 19761986 vol. 3 (2003).

[12] H. Deng, et al., "Routing security in wireless ad hoc networks", Communications Magazine, vol. 40, pp. 70-75 (2002).

[13] B. Awerbuch, et al., "An on-demand secure routing protocol resilient to byzantine failures", pp. 21-30 (2002).

[14] W. Enck, et al., "Exploiting open functionality in SMS-capable cellular networks", pp. 393-404 (2005).

[15] Y. C. Hu, et al., "Rushing attacks and defense in wireless ad hoc network routing protocols", pp. 30-40 (2003).

[16] Huan-Chung Lin and Yuh-Min Tseng, "A Scalable ID-Based Pair wise Key Establishment Protocol for Wireless Sensor Networks" , Journal of Computers (2008).

[17] J. Elson, K. Römer, Wireless sensor networks: a new regime for time synchronization, SIGCOMM Computers and Communication Reviews 33 (1) (2003) 149–154.

[18] P. Santi, Topology control in wireless ad hoc and sensor networks, ACM Computers and Survey 37 (2) (2005) 164–194.

[19] J. Yick, D. Ghosal , B. Mukherjee, "Wireless sensor network survey", computer networks 52 (12) 2292–2330 (2008).

[20] Y. C. Hu, et al., "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks", ad hoc networks, vol. 1,pp. 175-192 (2003).

[21] Barua Poonam, Indora Sanjeev, Overview of Security Threats in WSN, International Journal of Computer Science and Mobile Computing.

ACKNOWLEDGEMENTS

I consider it is my moral duty to pay honour, regards and thanks to the authors, Learned Researchers, Research Scholars, librarians and publishers of all the books, Research papers and all other sources which I have consulted during the preparation of the present paper.

DOI : 10.18231/2454-9150.2019.0116