ISSN No. 0976-5697

Volume 5, No. 2, March 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Combat Approach to Overcome Attacks in Different Layers of Wireless Sensor Networks

Balaji Tedla, Ch.Rajesh,
Asst.Prof Department of CSE in Vasavi College of Engineering, Hyderabad, India

B.Kiran Kumar
Asst.Prof Department of CSE in Shri Vishnu Engineering College Engineering for Women, Hyderabad, India

Abstract: The new era of computing is now done through wireless sensor networks. The sensor nodes though small are very powerful. A WSN consists of many distributed autonomous sensors cooperatively pass their data through the network to a main location. Each sensor network node has typically several parts-a transceiver, a microcontroller and a power source usually a battery. As it is used in most of the real time applications, the threat to data confidentiality and integrity also increases over the internet/network. Attacks at all the layers of network protocol can be expected. This paper deals with security aspects in the wireless sensor networks and probably giving the counter measures for the same.

Keywords- WSN, combatmodel, Denial of service, confidentiality and integrity.

I. INTRODUCTION

The advances on miniature techniques and wireless communications have made possible the creation and subsequent development of Wireless Sensor Networks (WSN) paradigm. The main purpose of WSN is to serve as an interface to real world, providing physical information such as temperature, light, radiation etc. to a computer system. A WSN is a heterogeneous system consisting of hundreds or thousands of low-cost and low-power tiny sensors to monitor and gather information from environment and real time applications. The sensor network security is generally characterized by the same properties as traditional network security but WSNs are vulnerable to new methods of exploitation due to their unique characteristics. The major difference between this type of networks and wired networks is their decentralized and specialized nature. In WSN, all its members collaborate towards the common goal of obtaining or deducing certain physical information from their environment. Moreover WSN is capable of Self-organization, thus it can be deployed in a certain context without requiring the existence of a supporting infrastructure. As in all the computing environments, it is essential to assure the proper functionality of WSN in order to allow the correct provisioning of services.

The sensor nodes gather and transmit the information by observing the physical environment to one or more sink, which is a high end node that collects information from these sensors and processes further. Normally, the radio transmission range of the sensor nodes are in the orders of magnitude which are smaller than the geographical extent of the entire network. Thus, data needs to be forwarded towards the sink node in hop-by-hop manner. If the amount of data which needs to transmitted are reduced, then the energy consumption of the network is also minimized. WSNs are susceptible to many types of link layer attacks [1] and most of traditional networks security techniques are unusable on WSNs due to wireless and shared nature of communication channel, untrusted transmissions, deployment in open environments, unattended nature and limited resources [1]. Such network should comply with certain security requirements, such as confidentiality, integrity, authentication and others derived from application context. However achieving this goal is not an easy task for WSN.

The reason is the WSN consists of nodes with very limited resources whereas the attacker may have very powerful attacking (malicious) resources such as laptops with wireless LAN capability, long range wireless communication capability etc. Therefore security in WSN is a major issue. The security techniques of the normal computer networks cannot be implemented in WSN because of limited resources. A holistic approach aims at improving the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach could be the best option. The holistic approach has some basic principles like, in a given network; security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not surpass the assessed security risk at a specific time, if there is no physical security ensured for the sensors, the security measures must be able to exhibit a graceful degradation if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measures should be developed to work in a decentralized fashion. If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building security layers as in the holistic approach, protection could be established for the overall network.

Basically the major challenge for employing any efficient security scheme in wireless sensor networks is created by the size of sensors, consequently the processing power, memory and type of tasks expected from the sensors. We discuss these issues and challenges in this paper.

II. MODES OF OPERATION & SECURITY REQUIRMENTS

Most of the research on this topic is revolved around security solutions using a layered approach. The layered approach is shown in Figure. 1. In layered approach the protocol stacks consists of the physical layer, data link layer, network layer, transport layer and application layer. These five layers and the three planes, i.e., power management plane, mobility management plane and the task management plane jointly forms the wireless layered architecture.

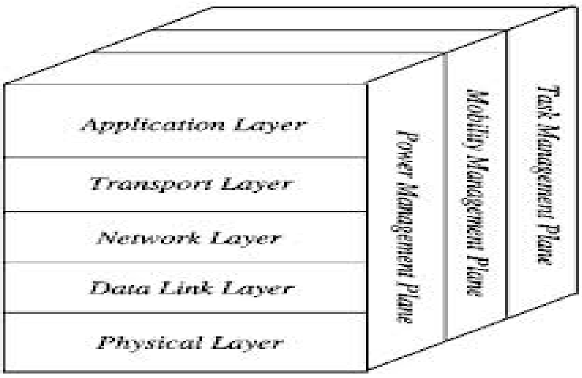

Figure. 1: Sensor Networks Protocol Stack

The major elements of WSN are the sensor nodes and the base stations. In fact, they can be abstracted as the "sensing cells" and the "brain" of the network, respectively. Usually, sensor nodes are deployed in a designated area by an authority and then automatically form a network through wireless communications. Sensor nodes are static most of the time, whereas mobile nodes can be deployed according to application requirements. One or several, static or mobile base stations (BSs) are deployed together with the network. Sensor nodes keep monitoring the network area after being deployed. After an event of interest occurs, one of the surrounding sensor nodes can detect it, generate a report, and transmit the report to a BS through multi hop wireless links. Collaboration can be carried out if multiple surrounding nodes detect the same event. In this case, one of them generates a final report after collaborating with other nodes. The BS can process the report and then forward it through either high quality wireless or wired links to the external world for further processing .The WSN authority can send commands or queries to a BS, which spreads those commands or queries into the network. Hence, a BS acts as a gateway between the WSN and the external world. An example is shown in Figure 2.

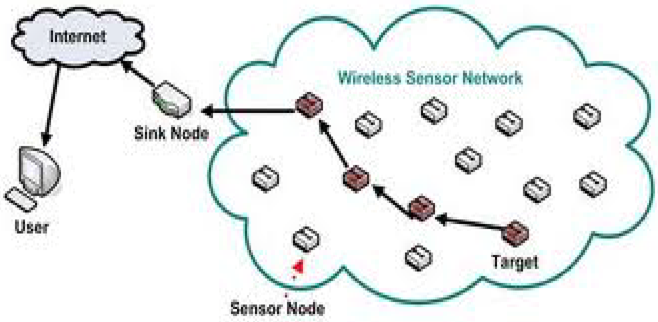

Figure. 2: Wireless sensor network

WSN though being a special type of network, shares some commonalities with a typical computer network. It also exhibits many distinctive characteristics. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehaviour of nodes. The most important security requirements in WSN are [3] [4]:

A. *Data confidentiality:*

There is a clear need to protect sensitive transmitted data from passive attacks such as eavesdropping. Hence, cryptography based solutions are typically employed to alleviate this shortcoming. However, the sensor's power can be used quickly by the complicated encryption and decryption methods like multiplications of large numbers in public key based cryptosystems[5].The issue of confidentiality should address the following requirements [6] [7]: (i) a sensor node should not allow its readings to be accessed by its neighbours unless they are authorized to do so, (ii) key distribution mechanism should be extremely robust, (iii) public information such as sensor identities, and public keys of the nodes should also be encrypted in certain cases to protect against traffic analysis attacks. Many applications like information surveillance, industrial management, key distribution etc. need to rely on confidentiality as the sensitivity of the data becomes an issue of concern.

B. *Data integrity:*

It is very imperative that the data in transit should not be changed by the adversaries. Since sensor nodes lack expensive tampering resistant hardware, they can easily be compromised [8]. Data integrity is to ensure that information is not changed in transit in any case which may be due to malicious intent or accidently .The mechanism used for data integrity should ensure that no message could be altered by an entity as it traverses from the sender to the recipient.

C. *Availability:*

Unavailability of sensor nodes may occur in case of hardware failure when the sensor runs out of battery power due to excess computation or communication. In other cases, it may happen that an attacker may jam communication to make sensor unavailable. The requirement of security not only affects the operation of the network, but also is highly important in maintaining the availability of the network. This requirement ensures that the services of a WSN should be available always even in presence of an internal or external attacks such as a denial of service (DoS) attack.

Attacks on wireless network can be broadly classified as interruption, interception, modification and fabrication.

Interception is an attack on confidentiality. The sensor network can be compromised by an adversary to gain unauthorized access to sensor node or data stored within it.

Modification is an attack on integrity. Modification means an unauthorized party not only accesses the data but tampers it, for example by modifying the data packets being transmitted.

Fabrication is an attack on authentication. In fabrication, an adversary injects false data and compromises the trustworthiness of the information relayed.

D. *Different types of threats in Network model:*

Different threats at each layer in OSI model can be summarized as in table I.

Table 1.

Layers	**Attacks**
Physical Layer	Jamming, Tampering
Data Link Layer	Jamming, Collision
Network Layer	Spoofing or Replaying Information, Selective Forwarding Or Black Holes, Sink Holes, Sybil Attacks, Node Replication Attacks, Wormholes Flooding, Attacks Against Privacy
Transport Layer	Injects False Messages , Energy Drain Attacks
Application Layer	Attacks On Reliability

III. COMBAT MODEL

Based on the characteristics and goals of the attacks and attackers, threat model of WSN can be presented by comparing them on the most important classes. This model of WSNs is presented by attributes such as the damage level caused, location, network functionality and attacker's strength [1]. In this section each of these is explained with respect to the function and effect of the attacks. Figure 3 shows the threat model that has been used in this paper to evaluate various attacks and effects of these attacks on the network.

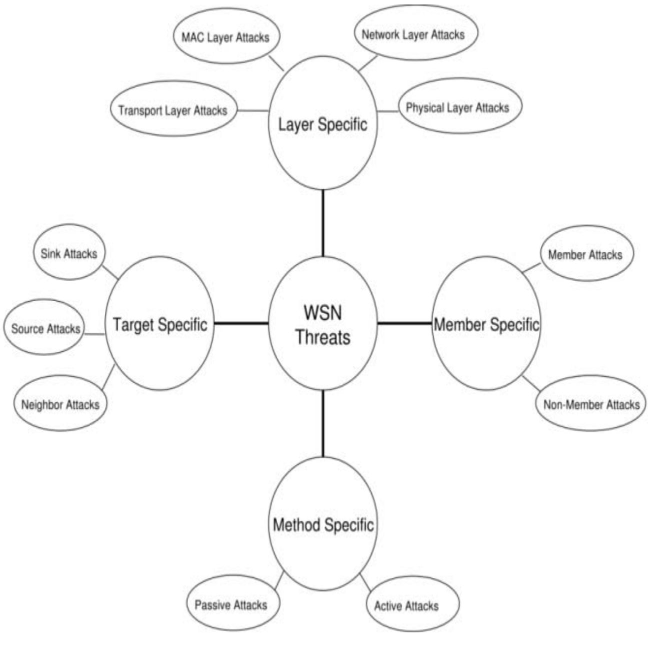

Figure 3.WSN Threats

a. In WSN, the nodes are vulnerable to security threats due to the unique characteristics of their underlying networking protocols and their limited resources. Attacks can occur in different layers such as physical, link (MAC), network, transportation, and application layer. The vulnerability increases as most of the routing protocols used in these layers are not designed having security threats in mind and hence leave open the chances of attacks. Hence the probability of attacks in such scenarios becomes very strong and the attacker doesn’t need much effort to launch any attack. Though there is no such standard layered architecture of the communication protocol for wireless sensor network.

b. The attackers can be classified as active attackers and passive attackers depending on the kind of threat and the effect on the WSN. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack, such as attacks against privacy [10] [11]. Passive attacks have to do with eavesdropping on, or monitoring, transmissions. Such an attack results in disclosure of information to attackers. Whereas, in the active attack, the unauthorized attackers monitor, listens to and modifies the data stream in the communication channel. Active attacks are used to break protection features; this may result into dissemination or loss of data, denial of service or abruption of important services.

c. Based on the location of attackers, the network attacks in WSN can be categorized as outsider or insider i.e. external or internal respectively. It is based on whether the attacker is a legitimate node of the network or is not a part of the network. If the intruding node is not an authorized participant of the sensor network it can be used to launch passive attacks. In such cases, the attacker has no special access to the sensor network. Whereas an inside attacker or internal threat is an authorized participant in the sensor network which has gone hostile [4]. Insider attacks may be mounted from either compromised sensor nodes running malicious code or adversaries who have stolen the key material, code, and data from legitimate nodes, and who then use one or more laptop-class devices to attack the network. Threats that are external may cause passive eavesdropping on data transmissions. They may also extend to injecting bogus data into the network so that network resources are consumed and then raise Denial of Service (DoS) attack. To prevent such attacks the best methods are the authentication and encryption techniques that shall prevent such attackers from gaining any special access to the network.

d. Based on the resources like computation power, transmission range and power, and other such capabilities, the attackers can use different types of devices to attack the targeted network. Based on these parameters attackers can be classified in two categories [12] i.e. laptop-class and mote-class attackers. Laptop-class attackers may possess powerful hardware such as faster CPU, larger battery, and high-power radio transmitter. Using such specialized hardware allows more broad range of attacks which are difficult to control. Such attacks may be used to run some malicious code and seek to extract secret keys and information from the sensor network and hence disrupt its normal functions. On the other hand, mote-class attackers are constrained to the CPU, power, bandwidth, and range limitations of the used mote platform. In such cases, they have access to a few sensor nodes with similar capabilities, but not much more than this. They may try to jam a radio link, but only in the sensor node's immediate vicinity. However, these attacks are more limited since the attackers try to exploit the network's vulnerabilities using only the sensor's node capabilities.

IV. DEFENCIVE MECHANISIM FOR VULNERABILITIES IN DIFFERENT LAYERS OF THE WSN NETWORK

A holistic approach [13] improves the performance of wireless sensor networks with respect to security, longevity and connectivity under changing environmental conditions. The holistic approach of security concerns about involving all the layers for ensuring overall security in a network. For such a network, a single security solution for a single layer might not be an efficient solution rather employing a holistic approach could be the best option. In holistic approach security is to be ensured for all the layers of the protocol stack, the cost for ensuring security should not exceed the assessed security risk at a specific time, the security measures must be able to exhibit a graceful degradation if there is no physical security ensured for the sensors and if some of the sensors in the network are compromised, out of order or captured by the enemy and the security measure should be developed to work in a decentralized fashion. If security is not considered for all of the security layers, for example; if a sensor is somehow captured or jammed in the physical layer, the security for the overall network breaks despite the fact that, there are some efficient security mechanisms working in other layers. By building security layers as in the holistic approach, we can improve the security for the whole network.

V. CONCLUSION

In this paper, we have discussed various security threats expected at different layer of WSN protocol stack. Possible solution against each threat is also outlined. Detection and countermeasures of some threats in WSN is not at all easy. Key distribution among sensor nodes is also a challenging task. Most of the attacks against security in wireless sensor networks are caused by the insertion of false information by the compromised nodes within the network. For defending the inclusion of false reports by compromised nodes, a means is required for detecting false reports. In present time, most of the security schemes are based on specific network models and complete security model for all layers is not at all present although, in future, the security scheme might become well established for individual layer. Again, ensuring holistic security in wireless sensor network is a major research issue. Many of today's proposed security schemes are based on specific network models.

VI. REFERENCES

[1]. I.F.Akyildiz et al.,"A Survey on Sensor Networks", IEEE Commun.Mag., vol.40, no.8, Aug.2002, pp.102-114.

[2]. Mohammadi Shahriar, Hossein J. , "A Comparison Of Link Layer Attacks On Wireless Sensor Networks", International Journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC), Vol.3, No. 1. March 2011

[3]. Asif Habib "Sensor Network Security Issues at Network Layer" 2nd International Conference on Advaificances in Space Technologies, Pp. 58 – 63 National Engineering and Scientific Commission, Islamabad, Pakistan..

[4]. Shahnaz Saleem, Sana Ullah, Hyeong Seon Yoo" on the Security Issues in Wireless Body Area Networks "International Journal of Digital Content Technology and its Applications Volume 3, number 3, September 2009.

[5]. Asif Habib "Sensor Network Security Issues at Network Layer", 2nd International Conference on Advaificances in Space Technologies,Pp.58-63 National Engineering and Scientific Commission Islamabad, Pakistan.

[6]. Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and challenges", International Conference on Advaificances in Space Technologies.

[7]. C.Karlof and D.Wagner,"Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Proc. First IEEE Int'l Wksp. Sensor Network Protocols and Applications, May 2003, pp.113-27.

[8]. Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Adhoc Networks (Elsevier), Page: 299-302, year 2003.

[9]. Haowen Chan, and Adrian Perrig,"Security and Privacy in Sensor Networks", Carnegie Mellon University pp.99-101.

[10]. J.Newsome et al., "The Sybil Attack in Sensor Networks: Analysis and Defenses", IPSN'04: Proc. IEEE Int'l. Conf. Info. Processing in Sensor Networks, Apr.2004.

[11]. Y.C.Hu, A.Perrig, and D.B.Johnson,"Packet Leashes: A defense Against Wormhole Attacks in Wireless Networks", Proc.IEEE INFOCOM 2003, Apr.2003.

[12]. Wang Yong, Garhan Attebury, Byrav Ramamurthy, "A Survey of Security Issues In Wireless Sensor Networks", CSE, Journal Articles, paper 84, 2006.

[13]. Giannetsos Athanasios, "Security Threats in Wireless Sensor Networks: Implementation of Attacks & Defense Mechanisms", Ph.D Dissertation Submitted to the Department of Electronic Systems and the Committee on Graduate Studies of Aalborg University in Wireless Communications, 2011.

Short Bio Data for the Authors

Mr.Balaji Tedla working as an Asst.Prof in the Department of CSE in Vasavi College of Engineering, Hyderabad, India. He has a good teaching experience of 4 years.

Mr.Ch Rajesh working as an Asst.Prof in the Department of CSE in Vasavi College of Engineering, Hyderabad, India. He has a good teaching experience of 6 years.

Mr.B.Kiran Kumar working as an Asst.Prof in the Department of CSE in Shri Vishnu Engineering College Engineering for Women, Hyderabad, India. He has a good teaching experience of 4 years.