AN UPDATE OVERVIEW ON SECURITY ISSUES OF WIRELESS SENSOR NETWORKS

Rupam Sharma[1], Nidhi Tripathi[2]

[1,2]*Department of Computer Sciences, Gwalior Institute of Technical Studies, Gwalior (India)*

ABSTRACT

It is well understood that Wireless Sensor Networks (WSNs) is an emerging technology and have great potential to be employed in critical situations like battlefield and commercial applications including geographical monitoring, medical care, manufacturing, transportation, military operations, environmental monitoring, industrial machine monitoring, and surveillance systems. Due to broad range of WSNs applications, there is need to concern about their security and its related issues. The article provides update information on security issues of the sensor networks.

Key Words: Wireless Sensor Networks, Architecture, Applications, Security Requirements, Obstacles of Sensor Security, Security Attacks, Data Security Schemes

I. INTRODUCTION

Wireless Sensor network (WSN) is an emerging technology and is used to collect information from physical world. Therefore the sensor networks have great potential to be employed in critical situations including industrial purposes. Wireless sensor network is widely considered as one of the most important technology in the past decades. It has received tremendous attention from all over the world [1]. A WSN typically consists of a large number of low-cost, low-power, and multifunctional wireless sensor nodes, with sensing, wireless communications and computational capabilities. Wireless Sensor networks (WSN) are highly distributed networks of small, lightweight wireless nodes, deployed in large numbers to monitor the environment or system by the measurement of physical parameters such as temperature, pressure, and/or relative humidity. Basically sensor networks are application dependent. These are generally designed for real time analysis of low level data in hostile environments. Because of this reason they are well suited to a substantial amount of monitoring and surveillance applications.

A major benefit of these systems is that they perform in network processing to reduce large streams of raw data into useful aggregated information. Because sensor networks pose unique challenges, traditional security techniques used in traditional Networks cannot be applied directly. *First,* to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. *Second,* unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack. And *third,* sensor networks interact closely with their physical environments and with people, posing new security problems. Security is a broadly used term encompassing the characteristics of authentication, integrity, privacy, non-repudiation, and anti-playback. The more the dependency on the information provided by the networks has been increased, the more the risk of secure transmission of information over the networks has increased. For the secure transmission of various types of information over networks, several cryptographic, steganographic and other techniques are used which are well known [2]. In

continuation of the above, there is need to update knowledge on security issues of WSN's. Therefore existing security mechanisms are inadequate and more efficient tools could be generating to resolve their future issues.

II. ARCHITECTURE OF WIRELESS SENSOR NETWORK

We are presenting here basic architecture of WSN and it consists of four network components [2]. First, field device is also known as Sensor motes and the devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment. A router is a special type of field device that does not have process sensor or control equipment and as such does not interface with the process itself. Second, gateway enables communication between Host application and field devices. Therefore it is called as Access points. Third, network manager is responsible for configuration of the network, scheduling communication between devices (i.e., configuring super frames), management of the routing tables and monitoring and reporting the health of the network and fourth, security manager is responsible for the generation, storage, and management of keys.

III. APPLICATIONS OF WIRELESS SENSOR NETWORK

Wireless Sensor Networks (WSN) has off late, found applications in wide-ranging areas. Therefore, we discuss here WSN applications related to some prominent areas related to useful tools in military, medical, environmental and different industries [3]. These applications have major concern about need and safety of individual such as military applications, medical application, environmental monitoring, industrial applications, monitoring application in infrastructure protection and other applications related to smart sensor nodes can be built into appliances at home with remote – controlled i.e. ovens, refrigerators, and vacuum cleaners.

IV. SECURITY REQUIREMENTS IN WIRELESS SENSOR NETWORK

A sensor network is a special type of network. It shares some commonalities with a typical computer network, but also poses unique requirements of its own. Therefore, we can think of the requirements of a wireless sensor network as encompassing both the typical network requirements and the unique requirements suited solely to wireless sensor networks [4].

Here we are included common requirements on the basis of its applications -

4.1 Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault. Unfortunately, an attacker can easily manipulate non secured location information by reporting false signal strengths, replaying signals. This Section has discussed about the security goals that are widely available for wireless sensor networks and the next section explains about the attacks that commonly occur on wireless sensor networks.

4.2 Availability

Adjusting the traditional encryption algorithms to fit within the wireless sensor network is not free, and will introduce some extra costs. Some approaches choose to modify the code to reuse as much code as possible. Some approaches try to make use of additional communication to achieve the same goal. What's more, some

approaches force strict limitations on the data access, or propose an unsuitable scheme (such as a central point scheme) in order to simplify the algorithm. But all these approaches weaken the availability of sensor and sensor network for these reasons. First, a single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network. Second, additional computation consumes additional energy. If no more energy exists, the data will no longer be available and third, additional communication also consumes more energy. What's more, as communication increases so too does the chance of incurring a communication conflict.

4.3 Data Freshness

Data freshness implies that the data is recent, and it ensures that an adversary has not replayed old messages. Even if confidentiality and data integrity are assured, we also need to ensure the freshness of each message. Informally, data freshness suggests that the data is recent, and it ensures that no old messages have been replayed. This requirement is especially important when there are shared-key strategies employed in the design. A common defense is to include a monotonically increasing counter with every message and reject messages with old counter values. With this policy, every recipient must maintain a table of the last value from every sender it receives. Assuming nodes devote only a small fraction of their RAM for this neighbor table, an adversary replaying broadcast messages from many different senders can fill up the table. At this point, the recipient has one of two options: ignore any messages from senders not in its neighbor table, or purge entries from the table. Neither is acceptable; the first creates a DoS attack and the second permits replay attack. In the authors contend that protection against the replay of data packets should be provided at the application layer and not by a secure routing protocol as only the application can fully and accurately detect the replay of data packets.

4.4 Data Authentication

An adversary is not just limited to modifying the data packet. It can change the whole packet stream by injecting additional packets. So the receiver needs to ensure that the data used in any decision-making process originates from the correct source. On the other hand, when constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycles). From the above, we can see that message authentication is important for many applications in sensor networks. Informally, data authentication allows a receiver to verify that the data really is sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share secret key to compute the message authentication code (MAC) of all communicated data.

4.5 Data Confidentiality

Data confidentiality is the most important issue in network security. Confidentiality means keeping information secret from unauthorized parties. The confidentiality relates to the sensor network should not leak sensor readings to its neighbors especially in a military applications (the data stored in the sensor node may be highly sensitive.), Public sensor information, such as sensor identities and public keys, should also be encrypted to some extent to protect against traffic analysis attacks and many applications nodes communicate highly sensitive data, e.g., key distribution; therefore it is extremely important to build a secure channel in a wireless sensor network.

4.6 Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. Data integrity ensures the receiver that the received data is not altered in transit by an adversary. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. For example, a malicious node may add some fragments or manipulate the data within a packet. This new packet can then be sent to the original receiver. Data loss or damage can even occur without the presence of a malicious node due to the harsh communication environment. Thus, data integrity ensures that any received data has not been altered in transit.

V. OBSTACLES OF THE SENSOR SECURITY

A wireless sensor network is a special network which has many constraints compared to a traditional computer network. Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack [3]. And third, sensor networks interact closely with their physical environments and with people, posing new security problems. Due to these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. Therefore, to develop useful security mechanisms while borrowing the ideas from the current security techniques, it is necessary to know and understand these constraints first [4].

5.1 Very Limited Resources

All security approaches require a certain amount of resources for the implementation, including data memory, code space, and energy to power the sensor. However, currently these resources are very limited in a tiny wireless sensor. The major parameters are limited memory & storage space and power limitation.

5.2 Unreliable Communication

Certainly, unreliable communication is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. The major parameters are unreliable transfer, conflicts and latency.

5.3 Unattended Operations

Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. There are three main caveats to unattended sensor nodes; exposure to physical attacks, managed remotely and no central management point.

VI. SECURING ATTACKS ON WIRELESS SENSOR NETWORK

First of all Wireless networks are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically safe. Deployment of many nodes of WSN in open and harsh environment poses them another major threat. This compromises their physical security, and if the nodes are not temper-resistant, they can be mishandled and tempered with. Attacks on the physical

security of the nodes can cause the node to give away the data stored on it, which may enable the attacker to gain access to critical information such as source code, key and other data which may be crucial for security protocol of the entire wireless network [3]. Making these nodes temper resistant may be able to reduce the effects of side-channel attacks and to enhance the physical security of the network devices, but this may not be the feasible solution as the cost per node increases dramatically if we consider such defenses.

WSN are continuously being used in many critical and sensitive applications. WSN are popular because of their ability to incorporate in numerous applications in diverse fields. Health care, security, logistics and military applications are some of the areas of deployment of these wireless networks. It is evident that if the capabilities or functionalities of the sensor network are reduced or endangered, it may cause huge losses in terms of money, resources and may even result in human injuries or fatalities. Many sensors network routing protocols are quite simple and massages are recorded in form of data. The data obtained by the sensing nodes needs to be kept confidential and it has to be authentic [5]. In the absence of security a false or malicious node could intercept private information, or could send false messages to nodes in the network.

There are huge literatures on WSNs attacks and some major attacks of WSN are discussing here as given below

6.1 Denial of Service (DoS)

This type of attack results into making unavailable the resources to their intended users. As an example node 'A' sends request to node 'B' for communication and node 'B' sends acknowledge to node 'A' but 'A' keeps on sending request to 'B' continuously. As a result 'B' is not able to communicate with any other nodes and thus becomes unavailable to all of them. Denial of service attack may also occur at physical layer by jamming (by broadcasting mechanism) and/or tampering (modification or fabrication) of the packet. In Link Layer it is by producing collision data, exhaustion of resources and unfairness in use of networks. In network layer, it occurs by way of neglecting and the greediness of packets resulting into path failure. In transport layer, DOS attack occurs due to flooding and de-synchronization. Most of denial of service attacks may be prevented by powerful authentication and identification mechanisms [6].

6.2 The wormhole Attack

One node in the network (sender) sends a message to another node in the network (receiver node) [3].Then the receiving node attempts to send the message to its neighbors. The neighboring nodes think the message was sent from the sender node (which is usually out of range), so they attempt to send the message to the originating node, but it never arrives since it is too far away. Wormhole attack is a significant threat to wireless sensor networks, because, this sort of attack does not require compromising a sensor in the network rather, it could be performed even at the initial phase when the sensors start to discover neighboring information. Wormhole attacks are difficult to counter because routing information supplied by a node is difficult to verify.

6.3 The Sybil Attack

In this attack, a single node i.e. a malicious node will appear to be a set of nodes and will send incorrect information to a node in the network. The incorrect information can be a variety of things, including position of nodes, signal strengths, making up nodes that do not exist. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network. However, an insider cannot be prevented from participating in the network, but he should only be able to do so using the identities of the nodes he has

compromised. Public key cryptography can prevent such an insider attack, but it is too expensive to be used in the resource constrained sensor networks.

6.4 Sinkhole attacks

In a sinkhole attack, the adversary's aim is to attract nearly all the traffic from a particular area through a compromised node. Sinkhole attacks typically work by making a compromised node look especially attractive with high capability resources like high processing power and high bandwidth to surrounding nodes by which it always creates shortest path with respect to the routing algorithm. Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. As an example, a laptop class adversary has a strong power radio transmitter that allows it to provide a high quality route by transmitting with enough power to reach a wide area of the network.

6.5 Passive information gathering

An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques should be used.

6.6 Hello flood attacks

The Hello flood attacks in wireless sensor network can be caused by a node which broadcasts a Hello packet with very high transmission power to sender or receiver. The nodes receiving the messages assume that the sender node is nearest to them and sends packets by this node. By this attack congestion occurs in the network. Blocking techniques are used to prevent Hello Flood attacks.

6.7 Malicious Node

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. Insertion of malicious node is one of the most dangerous attacks that can occur and could spread malicious code to all nodes which potentially destroy the whole network or even worse.

6.8 Node capturing

A particular sensor might be captured, and information stored on it might be obtained by an adversary.

VII. DATA SECURITY SCHEMES FOR WIRELESS SENSOR NETWORKS

Studies revealed how to design secure distributed sensor networks with multiple supply voltages to reduce the energy consumption on computation and therefore to extend the network's lifetime. It aim sat increasing energy efficiency for key management in wireless sensor networks and uses [3]. Wood et al. (2002) studies DoS attacks against different layers of sensor protocols tack [7]. JAM presents a mapping protocol which ejects a jammed region in the sensor network and helps to avoid the faulty region to continue routing within the network, thus handles DoS attacks caused by jamming.

In another study, the authors show that worm holes those are so far considered harmful for WSN could effectively be used as a reactive defense mechanism for preventing jamming DoS attacks [7]. In another paper, a probabilistic secret sharing Protocol has been defined to defend Hello flood attacks. The scheme uses a bidirectional verification technique and also introduces multi-path multi-base station routing if bidirectional verification is not sufficient to defend the attack. 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. We should be concentrating more on sensor node themselves, because nearly all attacks on WSN starts from compromising a node. Since physical tampering cannot be avoided. Care must be taken to prevent software based tempering. There are enough chances that applications/ operating system running in sensor node are vulnerable to popular exploits such as buffer overflow. Here, the problem is with composing the components of the overall system. A secure system can be realized only by building security in to the system architecture and this requires:-

1. Security analysis of the architecture.
2. Security testing of the realized system for implementation bugs.
3. Removal/scrutiny of "undocumented features" that can be potentially exploited to violate the system security.

VIII. CONCLUSION

Wireless Sensor Networks, are self organizing, self healing networks of small "nodes" have huge potential across industrial, military and many other sectors. In present scenario, there is need to investigate the solution of emerging issues directly and indirectly concern about the WSN. Therefore the article serves as a text for researchers especially the beginners, and enables them to get an update on security issues related to wireless sensor networks.

REFERENCES

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, A survey on sensor networks. IEEE Communications Magazine, 40 (8), 2002, 102–114.

[2] R. Sharma, and N. Tripathi, Comprehensive Review on Wireless Sensor Networks. Orient. J. Comp. Sci. and Technol, 8 (1), 2015, 59 - 64.

[3] R. Sharma, and N. Tripathi, Wireless Sensor Network: Application, Service Attacks, and Security Schemes, Intern. J. Inno. Tren. Engineer; 04 (01), 2015, 51-54.

[4] G. Murugaboopathi, V. Geta, V. Sujathabai, T. K. S. Rathish babu, and S. Hariharasitaraman, An Analysis of Threat's in Wireless Sensor Networks, IJARCSSE, 2 (10), 2012.

[5] P. Kumar, S. Cho, D. S. Lee, Y. D. Lee, and H. J. Lee, TriSec: A secure data framework for wireless sensors networks using authenticated encryption. Int. J. Marit. Inf. Commun. Sci., 2010, 129-135.

[6] R. David, R. Scott, and F. Midkiff, Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses. IEEE Pervasive Computing, 7 (1), 2008, 74-81.

[7] H. Karl, and A. Willig, Protocols and Architectures for Wireless Sensor Networks, ISBN 0-470-09511-3, 2006,1 – 526.