International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 11, November - 2013

Security in Wireless Sensor Network: A Survey

Jeevan kumar
Computer science & Engg
RVSCET, Jamshedpur

Yogendra Kumar
Computer science & Engg
RVSCET, Jamshedpur

Sushanta mahanty
Electronics & Communication Engg
RVSCET, Jamshedpur

Abstract--- This paper present, detail discussion on Security in Wireless Sensor Network (WSN). Wireless sensor networks are generally set up for storing records from insecure environment. In the last decade, many advances in field of electronics and wireless communication technologies, have enabled the development of wireless sensor networks on large scale that consist of many thing as like that, low-power, low-cost, and small-size sensor nodes. Sensor networks hold the facilitating, large-scale and real-time data processing in complex environments. Current applications of wireless sensor networks are in the fields of medical, battlefield monitoring, environment monitoring, surveillance and disaster prevention. To provide security and privacy to small sensor nodes is challenging issues, due to the limited capabilities of sensor nodes in terms of computation, communication, memory or storage, & energy supply. In this paper, Also focus on the security in different situation in wireless sensor network.

Keywords- Wireless Sensor Network, Node, Security, Attack, Communication, Attacker, Layering-Based Attacks, Synchronization, Self-Organization.

1. Introduction

Wireless sensor networks have applications in many important areas, such as the military, home security, health care, the environment, agriculture, and manufacturing. In the future the deployment of large scale sensor networks where hundreds, thousands and many more of small sensor nodes from self-organizing wireless networks. It is not an easy task to providing security in sensor network. Compared to conventional desktop computers, several constraints exist since sensor nodes have limited storage, processing, energy capability and wireless links have limited bandwidth. Several recent contributions to the literature have addressed Security and privacy issues in sensor networks. Here, discuss current and past research activities carried out on sensor network security. The rest of the paper is outlined as follows. Summarize architecture of sensor and Wireless Sensor Network, Overview of security issues in sensor networks, Security Requirements, Attacks on Wireless sensor Networks, layering-based attacks and Cryptography. Due to page limits, we do not extensively discuss other sensor network security issues, such as broadcast authentication and detection of compromised sensor nodes.

2. Sensor Node and WSN Architecture

Wireless sensor networks are composed of hundreds and thousands of sensor nodes responsible for sensing, processing, and communication. The application scenarios impose different requirements for designing sensor nodes and network protocols. Application specific is a fundamental characteristic of WSNs, like most other embedded systems. It is impossible for general purpose sensor nodes and network protocols to address all application specific requirements. Wireless sensor nodes are basic elements to construct WSNs. Many efforts have been paid to research and develop appropriate architectures of sensor nodes. The Mote architecture, invented by researchers from Berkeley, is the most popular platform used by researchers around the world. This architecture is dividing in four parts, which is as like a sensing unit, a processing unit, a transceiver unit, and a power unit, as illustrated in Figure 1. The processing unit is typically a low power microcontroller. In this architecture, microcontroller is responsible for all jobs, such as scheduling, sampling, computing, communication and many more. In the process of development and deployment, many problems about the mote architecture are exposed. First, sampling, computing, and communication conflicts with each other if not carefully scheduled. Second, some jobs are very difficult even impossible to be implemented in the microcontroller. Third, low power, one of the most fundamental design principles in wireless sensor

network, is sometimes violated with all jobs implemented in the microcontroller [1].

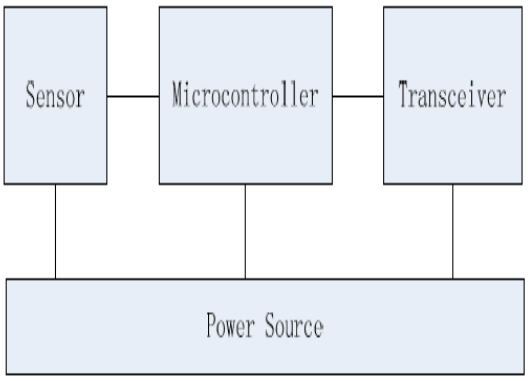

Figure1: the mote architecture

Software optimization is attempted to solve these problems. However, the effect is very limited. In order to implement these applications efficiently, more concrete sensor node architecture is necessary.

In current sensor node architectures, microcontroller is responsible for almost all jobs, which is an oppressive burden for it. To solve these problems, new sensor node architecture is needed. At the same time, design principles about how to design sensor nodes with particular application requirements are also needed. With our experiences from field deployments, new sensor node architecture is proposed [1], as shown in Figure 2. In this architecture, the sensor node is divided into core part and application specific part. The core part is only composed of an ultralow power microcontroller and a low power transceiver, which is different from all other architectures. The sensor subsystem and storage subsystem are all application specific, so they belong to the application specific part. For some applications, more powerful computing resources are needed. A new sensor node architecture putting only a microcontroller and a transceiver in the core part is from the fact that all sensor nodes need them. The design principle for the ultralow power microcontroller is as follows: it should not execute complicated sampling and computing tasks, only scheduling, communication, and simple sampling tasks belong to it. Power consumption should be as low as possible. Enough inner data memory should be provided for network protocol. In our architecture, sensor subsystem can be divided into direct and indirect parts using the following criterion: direct sensor subsystem will only introduce tasks that the microcontroller can handle efficiently, while the tasks in indirect sensor subsystem are not applicable on microcontroller. If low sampling rate is needed for the monitoring phenomenon, it can be processed by microcontroller directly. Temperature and humidity are examples of this form; because they are changing vary very slowly. On the other hand, vibration, which needs sampling rate higher than 100Hz, cannot be processed by microcontroller directly; hence vibration sensor belongs to the indirect sensor subsystem.

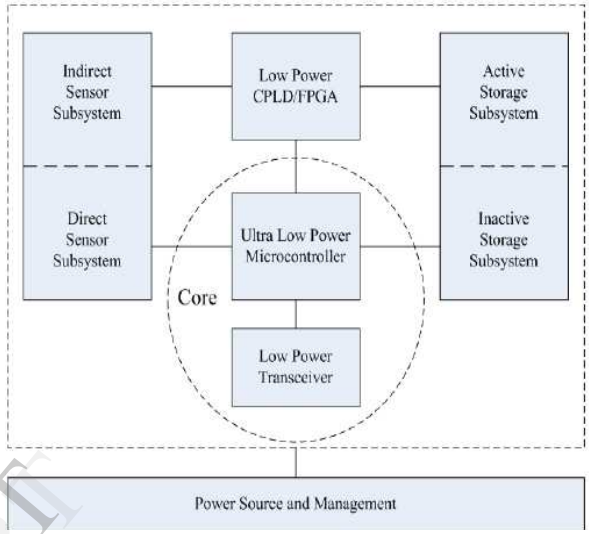

Figure 2: New sensor node architecture

Storage subsystem is also divided into two forms: active and inactive. The criterion is similar: according to the work load if it is applied to the microcontroller for memory access. One straightforward case is similar to the sensor subsystem: temperature/humidity monitoring with low memory access rate and vibration monitoring with high memory access rate.

In Figure 3, shows a typical WSN Architecture [2]. Also we see following network components –

• Sensor motes (Field devices) – Field devices are mounted in the process. Which must be capable of routing packets on behalf of other devices. Many cases, they characterize or control the process or process equipment. A router is a special type of field device which, does not have process sensor or control equipment and as such does not interface with the process itself.
• Gateway (or Access points) – The responsibility of a gateway is enables communication between Host application and field devices.
• Network manager – The network manager is responsible for configuration of the network, scheduling communication between devices,

management of the routing tables and monitoring and reporting the current status of the network.

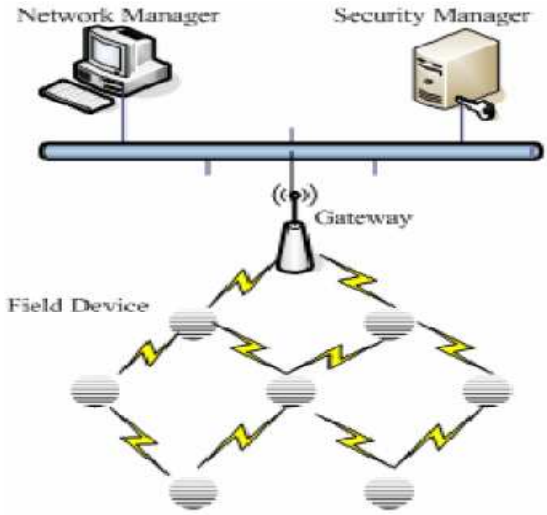

Figure 3: WSN Architecture

• Security manager – The Security Manager is responsible for the generation, management of keys and storage.

3. Overview of security issues

A wireless sensor network is an important network which has many constraints compared to a traditional computer network. For these constraints it is difficult to directly employ the existing security approaches to the area of wireless sensor networks. So, develop useful security mechanisms while borrowing the ideas from the current security techniques, it is very essential to know and understand these constraints first.

3.1 Limited Resources

All security methods require a certain amount of resources for the implementation, including data memory, code space, and energy to provide power of the sensor. Currently these resources are very limited in a small or tiny wireless sensor, which are as like that:
• Limited Memory and Storage Space
• Power Limitation Energy is the biggest constraint to wireless sensor capabilities.

3.2 Unreliable Communication

Another threat of sensor security is unreliable communication. The security of the network relies heavily on a defined protocol, which are depends on communication.
• Unreliable Transfer: The packet-based routing of the sensor network is connectionless and it is inherently unreliable.
• Conflicts: The channel is reliable; the communication may still be unreliable, due to the broadcast nature of the wireless sensor network.
• Latency: The greater latency in the network requires, multi-hop routing, network congestion and node processing. That is way, making it difficult to achieve synchronization among sensor nodes.

3.3 Unattended Operation

Depending on the various function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. Unattended sensor nodes have many problems:

• Physical Attacks: The sensor may be deployed in an environment, open to adversaries, bad weather, thundering and so on.
• Managed Remotely: Remote management of a sensor network that is, virtually impossible to detect physical tampering.
• No Central Management Concept: The sensor network must follow concept of distributed network without a central management point. The vitality of the sensor network will increase.

3.4 Attack and Attacker

An attack can be provide to get illegal access to a service, information, or the assay to conciliation integrity, confidentiality, or availability of a system. Attacks are originated by intruders or attackers [3, 4]. Adversaries of the WSN are:
• Passive: A person or entity that only monitors the communication channel, which threatens the confidentiality of data.
• Active: Effort to add, delete or alter the transmission on the channel, which threatens to confidentiality, authentication and data integrity.
• Insider: Steal key material and run malicious code by compromise some authorized nodes of the network.
• Outsider: The attacker has no particular access to the network.
• Mote-Class Attacker: It access to the minority nodes with similar capabilities.
• Laptop-Class Attackers: they have access to powerful devices such as laptop which has advantages greater than legal nodes, for instance more capable processor, greater battery power and high power antenna.

3.5 Security Principles

The requirements [5] of security in wireless sensor network can be classified as follows:
• Data Authentication: This make secure the data is started from the original source.
• Data Confidentiality: This secure only authorized sensor nodes can share or get the content of the messages.
• Data Integrity: This secure any received message has not been changed which is send by unauthorized parties.
• Availability: This secure the services offered by WSN or by a single node must be available.
• Data Freshness: This make secure that no old data have been replayed.

4. Security Requirements

A sensor network is a special type of network [6, 7]. It shares with a few typical computer networks. Therefore, here discuss requirements of a wireless sensor network. Also, encompassing both the typical network requirements and the unique requirements in the field of wireless sensor networks.

4.1 Data Confidentiality

The most important issue in network security is data confidentiality. In sensor networks, the confidentiality relates to the following:
• A sensor network should not passes or leak sensor readings to its neighbors node. For example, the data stored in the sensor node may be highly sensitive in a military application.
• In many applications nodes communicate highly sensitive data, e.g., key distribution, so that, it is extremely important to build a secure channel in a wireless sensor network.

4.2 Data Integrity

Data integrity ensures that any received data has not been altered in transit or changed while on the network. In a WSN the issue of integrity must refer the following requirements:
• Only the nodes in the network should have access to the keys and only an assigned base station should have the right to change the keys.
• It protects against an active and intelligent attacker who might attempt to disguise his attack as noise.

4.3 Data Freshness

This makes sure that, the confidentiality and data integrity. Here, also need to ensure the freshness of each message. Informally, data freshness suggests that the data is updated regularly and it sure that no previous messages have been replayed. In this case, it is easy for the adversary to use a replay attack. As well as, it is easy to disrupt the normal work of the sensor.

4.4 Availability

Availability makes sure that, the services of resources offered by the network or by a single sensor node should be available whenever required. In a WSN the issue of availability must refer the followings:
• A single point of failure must be avoided.
• Central access control system is used to make sure, the successful delivery of every message to its recipient node.
• Additional computation required more energy. If no more energy exists, the data will no longer be available.

4.5 Self-Organization

A typical WSN may have combination of thousand nodes fulfilling various operations, installed at different locations. Sensor networks are also ad hoc networks. Having the same flexibility and extensibility. In this context of applying public-key cryptography techniques in sensor networks. An efficient mechanism for public-key distribution is necessary as well. In this way, distributed sensor networks must self-organize to support multihop routing, they must also self-organize to conduct key management and building reliable relation among sensors. If self-organization is lacking in a sensor network the damage resulting from an attack.

4.6 Time Synchronization

Time synchronization is most important factor in the field of sensor network, many application depend on it. In order to save power, an individual sensor's radio may be turned off for some time. Moreover the sensors may wish to calculate the end-to-end delay of a packet. As it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications etc.

4.7 Secure Localization

The sensor network will rely on its ability to accurately and automatically locate each sensor in the network field. The sensor network designed to locate faults will need accurate location information in order to find out the location of a fault point. But, an

attacker can easily manipulate non- secured location information by reporting false signal strengths, replaying signals, etc. So, the secure localization an important feature that must be satisfied during our implementation of security protocol

4.8 Authentication

The attacker is not just limited to modifying the data packet. It can change the complete packet stream by injecting additional packets or other information. So the receiver cannot ensure that, the data used in any decision-making process originates from the correct source. On the other hand when constructing the sensor network. The authentication is necessary for many administrative tasks. From the above discussion, here analyze that, message authentication is important for many applications in sensor networks.

4.9 Flexibility

Sensor networks will be used in scenarios, related to environmental circumstances, hazards and mission may change frequently. Changing mission required sensors to be eliminated from or injected to a settled sensor node. Therefore, two or more sensor networks may be merged into one or a single network may be divided in two parts. Key establishment protocols must be ductile enough to render keying for all potential scenarios a sensor network may encounter.

5. Attacks on Wireless sensor Networks

Sensor networks have several key types of attacks [9]. Attacks can be performed in a different ways, most notably as denial of service attacks and many more as like traffic analysis, privacy violation, physical attacks. Here, summarize typical attacks on sensor networks and possible defense techniques as follow:

1 Jamming (physical layer) is one of the basic type destructive attacks, which attempt to interrupt in physical layer of the WSN structure. Jamming mostly of two types- constant jamming and intermittent jamming. Constant jamming affects the complete obstruct of the whole network. But, intermittent jamming nodes are capable of communicating data periodically not continuously. Possible defense of jamming are: spread - spectrum, lower duty cycle

2 Tampering (physical layer): tamper-proofing, effective key management schemes.

3 Collision (link layer) is a type of link layer jamming that occurs when two nodes try to transfer data at the same time with the same frequency. An attacker may cause collisions in particular packets such as ACK control messages. The effected packets are transmitted again, this cause increasing the energy and time cost for transmission. Such an attack reduces the network perfection. Possible defense of collision: error correcting code.

4 Exhaustion (link layer) occurs at the link layer. This attack dominates, the power resources of the nodes by causing them to retransmit the message. Either, there is no collision or late collision. Possible defense of exhaustion: rate limitation.

5 Manipulating routing information (network layer): authentication, encryption.

6 Selective forwarding attack (network layer): redundancy, probing.

7 Sybil attack (network layer) it was originally described as an attack able to defeat the redundancy mechanisms of distributed data storage systems in peer-to-peer networks. The Sybil attack is efficient enough to stroke other fault tolerant schemes as like dispersity, multi path routing, routing algorithms, data aggregation, voting, fair resource allocation, topology maintenance and misbehaviour detection. Possible defense of Sybil attack: authentication.

8 Sinkhole (blackhole) attack (network layer) it builds a node that seems to be very attractive in the sense that it promotes zero-cost routes to neighbouring nodes with respect to the routing algorithm, this makes results maximum traffic. Nodes adjoining to these harmful nodes collide for immense bandwidth, thus resulting into resource contention and message destruction. Possible defense of Sinkhole: authentication, monitoring, redundancy.

9 Wormhole attack (network layer) is a low-latency junction between two sections of a network. The malicious node receives packets in one section of the network and sends to another section of the network. This may cause congestion and retransmission of packets. Possible defense of Wormhole attack: monitoring, flexible route selection.

10 Hello flood attack (network layer): two-way authentication, three-way handshake.

11 Flooding (transport layer): limiting connection numbers, client puzzles.

12 Clone attack (application layer): unique pairwise keys Because of the page limit, we do not explicitly explain these attacks.

6. Layering-Based Attacks

6.1 Physical Layer

Jamming is a common attack on physical layer of wireless network. Jamming connecting with the radio frequencies being used by the nodes of a network. Jamming can interrupt the network impressive if a single frequency is used throughout the network. In this way, jamming can cause excessive energy consumption at a node by injecting impertinent packets. The receiver's nodes will as well consume energy by getting those packets. Physical layer also suffering from another attack which is tampering. In this attack, nodes are vulnerable to tampering or physical harm. In Table 1, describes Physical Layer Threats and Countermeasures in WSN [10].

Table 1

Interference	Channel hopping and Blacklisting
Jamming	Channel hopping and Blacklisting
Sybil	Physical Protection of devices
Tampering	Protection and Changing of Key

Table 2 Data-link layer threats and countermeasures

Threat	Countermeasure
Collision	CRC and Time Diversity
Exhaustion	Protection of Network ID and other Information that is required to joining device
Spoofing	Use different path for re-sending the message
Sybil	Regularly changing of key
De-synchronization	Using different neighbors for time synchronization
Traffic analysis	Sending of dummy packet in quite hours: and regular monitoring WSN network
Eavesdropping	Key protects DLPDU from Eavesdropper

6.2 Data Link Layer

The data link layer is suffering from many attacks. An attacker may change the communication protocol, and frequently send messages in an attempt to cause collisions. This type of collisions would need the retransmission of any packet influenced by the collision. In Table 2, describes Data Link Layer Threats and Countermeasures in WSN.

6.3 Network Layer

The network layer is very important for transferring packet from one to another layer. Generally, network layer attack can be grouped into two categories: passive and active attacks. It is very difficult to detect passive attack in view of the fact that a passive attack does not influence the functioning of the network. An active attack drops or modifies message thereby interfering the functioning of the network where both data packets and routing control packets kept by Messages. In Table 3, describes Network Layer Threats and Countermeasures in WSN.

Table 3 Network layer threats and countermeasures

Threat	Countermeasure
Eavesdropping	Session Keys protect NPDU from Eavesdropper.
DoS	Protection of network specific data link network ID etc. Physical protection and inspection of network.
Selective forwarding	Regular network monitoring using Source Routing
Sybil	Resetting of device and changing of session keys.
Traffic Analysis	Sending of dummy packet in quite hours: and regular monitoring WSN network.
Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use packet leach techniques.

6.4 Transport Layer

The transport layer is not safe layer from attack, as in the case of flooding. Flooding can be something simple as like sending many connection requests to a vulnerable node [10]. In this case, sender must be allocated to manage the connection request. Thus node's resources will be exhausted, then rendering the node useless.

Conclusion

In this paper, present details study on the security of wireless sensor network. Firstly, introducing hardware architecture of the sensor node and its network component. After this, discussed about the security in sensor networks and its related issues. Security is an important requirement and complicates enough to set up in different field of wireless sensor network. Also discussing Attacks and layered based attacks on wireless sensor networks and its possible countermeasure. Many security issues and its countermeasure in wireless sensor networks remain open. In the future, we expect to see more research activities on these exciting topics.

References

[1] Wei Liu, Xiaotian Fei, Tao Tang, Pengjun Wang, Hong Luo, Beixing Deng, Huazhong Yang "Application Specific Sensor Node Architecture Optimization-Experiences from Field Deployments", IEEE, 2012.

[2] Hemanta Kumar Kalita1 and Avijit Kar, "Wireless Sensor Network Security Analysis", International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009.

[3] Al-Sakib Khan Pathan, Hyung-Woo Lee, and Choong Seon Hong "Security in Wireless Sensor Networks: Issues and Challenges," International Conference on Advanced Communications Technology (ICACT), 2006.

[4] Hasan Tahir, Syed Asim Ali Shah "Wireless Sensor Networks – A Security Perspective," IEEE, 2008.

[5] Jaydip Sen, "A Survey on Wireless Sensor Network Security," International Journal of Communication Networks and Information Security Vol. 1, No. 2, August 2009.

[6] Shuai Yang, Jie Liu, Chunxiao Fan, Xiaoying Zhang , Junwei Zou, "A New design of security wireless sensor network using efficient key management scheme," IEEE, 2010.

[7] Yan-Xiao Li, Lian-Qin, Qian-Liang, "Research On Wireless Sensor Network Security," International Conference on Computational Intelligence and Security, IEEE, 2010.

[8] Yilin Wang and Maosheng Qin, "Security for Wireless Sensor Networks," International Conference on Control, Automation and Systems, Oct. 27-30, 2010, Korea

[9] Aashima Singla, Ratika Sachdeva, "Review on Security Issues and Attacks in Wireless Sensor Networks" International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013.

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

[11] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", ICACT, 2006

[12] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "Wireless sensor network survey", Computer Networks, Elsevier, 2008

[13] Chaudhari H.C. and Kadam L.U, "Wireless Sensor Networks: Security, Attacks and Challenges", International Journal of Networking, Volume 1, 2011.