Proc. of Int. Conf. on Emerging Trends in Engineering & Technology, IETET

Security in Wireless Sensor Networks using Key Management

Ruchi Gupta[1] and Ravi Kumar[2]
Geeta Institute of Management and Technology, Kurukshetra, India
Email: guptaruchi2292@gmail.com
Geeta Institute of Management and Technology, Kurukshetra, India
Email: ravi.kawatra@gmail.com

***Abstract*—Key management is basically one of the aspect in regard to the security in wireless sensor Networks. The goal is to reduce the time complexity as number of nodes increases as well as to execute the tasks with the help of minimum key exchanges for further performance enhancements. This paper is used to review the security in wireless sensor networks, their applications, issues & challenges. Wireless sensor networks (WSNs) consisting of low power, low-cost intelligent devices have limited IT resources. With an overall growth of WSN applications, security mechanisms are also a big problem on the rise. Many Real world applications have already been deployed and many of them will be based on wireless sensor networks. Examples of these applications include surveillance, health care, manufacturing, transportation, military operations, environmental monitoring, industrial machine monitoring and surveillance.**

***Index Terms*— Wireless Sensor Networks, Security in wireless sensor Networks, Types of security.**

I. INTRODUCTION

Wireless Sensor Networks are heterogeneous systems containing many small devices called sensor nodes and actuators with general-purpose computing elements. These networks will consist of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed either inside the system or very close to it. These nodes consist of three main components-sensing, data processing and communication. Two other components are also there called, aggregation and base station[1]. Aggregation point's gathers data from their neighboring nodes, integrates the collected data and then forwards it to the base station for further processing.

Advances in wireless communication and electronics have enabled the development of low-cost, low power, multifunctional sensor nodes. These tiny sensor nodes consisting of sensing, data processing, and communication components make it possible to deploy Wireless Sensor Networks (WSNs), which represent a significant improvement over traditional wired sensor networks.

These sensors are deployed in harsh environments to collect different types of data such as temperature, pressure, humidity, soil makeup, vehicular movement, noise levels, lighting conditions, the presence or absence of certain kinds of objects or substances, mechanical stress levels on attached objects and other

Grenze ID: 02.IETET.2016.5.49

properties. The collected data is then sent to a special node called the base station (BS) either directly or via other sensor nodes. BS is a more powerful device that usually behaves as an interface between the services provided by the sensor nodes (the "data acquisition network") and the users of the network. It can issue control orders to the sensor nodes in order to change their behavior.

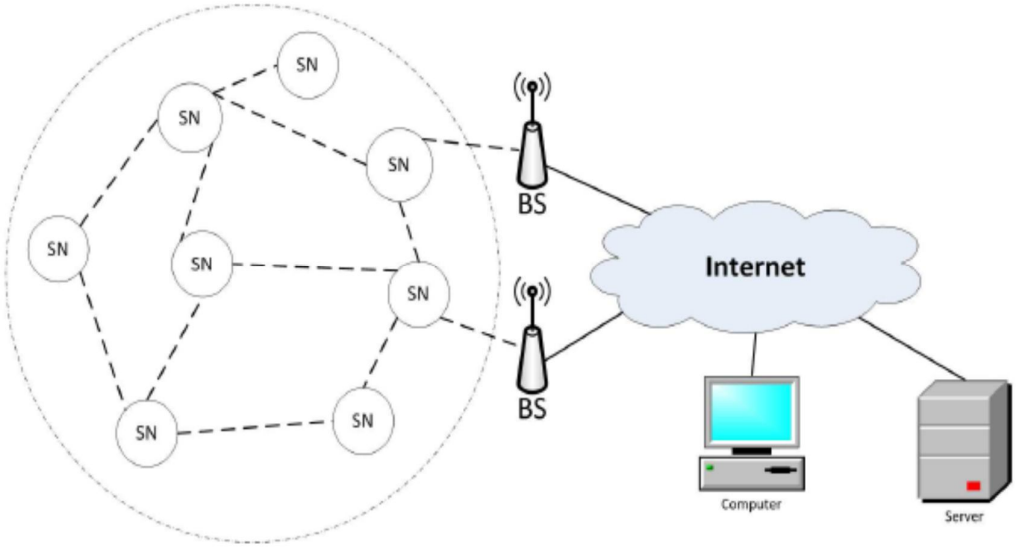

Figure 1.1 Structure of Wireless Sensor Network

A. Applications

There are many applications of WSNs ranging from simple habitat monitoring in a forest to highly secure military applications. According to the areas of deployment, applications of WSNs can be categorized as follows:

(1) Habitat Monitoring
(2) Manufacturing & Logistics
(3) Environmental observation & Forecast systems
(4) Military Applications
(5) Health related Applications
(6) Home & office Application
(7) A variety of intelligent & Smart systems

B. Issues/Challenges

Limited Resources

All security approaches require a certain amount of resources[2] 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.

Limited Memory and Storage Space

A sensor is a tiny device with only a small amount of memory and storage space[2] for the code. In order to build an effective security mechanism, it is necessary to limit the code size of the security algorithm.

Power Limitation

Energy is the biggest constraint to wireless sensor capabilities. We assume that once sensor nodes are deployed in a sensor network, they cannot be easily replaced (high operating cost) or recharged (high cost of sensors).

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.

Conflicts

Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts[2] will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem.

II. Security in Wireless Sensor Network

Security is one of the major aspects of any system. Traditional WSNs are affected by various types of attacks. These attacks can be categorized as:

1. Attacks on secrecy and authentication
2. Silent attacks on service integrity
3. Attacks on network availability

Cryptographic techniques can be used to prevent against the secrecy and authentication attacks. In silent attacks, the attacker compromises a sensor node and feeds wrong data. Attacks on network availability are also known as denial of service (DoS) attacks. If DoS attacks are promoted successfully, it can badly degrade the functioning of WSNs.

A. Data Confidentiality

Confidentiality is an acceptance of authorized access to information communicated from a certified sender to a certified receiver. A sensor network must not reveal sensor readings to its neighbours. Highly sensitive data is sometimes routed through many nodes before reaching the final node. For secure communication, encryption is used. Data is encrypted with a secret key that only authorized users have [7]. Public sensor information should also be encrypted to some degree to protect against traffic analysis attacks.

B. Data Integrity

Provision of data confidentiality stops the outflow of information [2], but it is not helpful against adding of data in the original message by attacker. Integrity of data needs to be assured in sensor networks, which strengthens that the received data has not been tampered with and that new data has not been added to the original contents of the packet. Data integrity can be provided by Message Authentication Code (MAC).

C. Data Authentication

An adversary is not only limited to modify the data packet but it can change the complete packet stream by adding extra packets. So the receiver needs to confirm that the data used in any decision-making process comes from the authorized source [8]. Data authenticity is an assurance of the identities of communicating nodes. Nodes taking part in the communication must be capable of recognizing and rejecting the information from illegal nodes. Authentication is required for many administrative tasks.

D. Data Freshness

Data freshness ensures that the data communicated is recent and no previous messages have been replayed by an adversary. Data freshness is classified into two types based on the message ordering [9]; weak and strong freshness. Weak freshness provides only partial message ordering but gives no information related to the delay and latency of the message. Strong freshness on the other hand, gives complete request-response pair and allows the delay estimation. Sensor measurements require weak freshness, while strong freshness is needed for time synchronization within the network. For ensuring the freshness of a packet, a timestamp can be attached to it. Destination node can compare the timestamp with its own time clock and checks whether the packet is valid or not

E. Availability

Availability is an insurance of the endowment to indulge expected services as they are designed earlier. It guarantees that the network services are feasible even in the subsistence of denial of service attacks. For making data available, security protocol should obsess less energy and storage, which can be targeted by the reuse of code and making sure that there is slight increase in communication due to the functioning of

security protocols. Central point scheme should also be avoided as single point failure will be introduced due to this in a network that threatens the availability.

F. Self Organization

A typical WSN may have thousands of nodes fulfilling various operations, installed at different locations. Sensor networks are also ad hoc networks, having the same flexibility and extensibility. Sensor networks crave every sensor node to be independent and ductile enough to be self-organizing and self-healing according to different situations.

III. Literature Review

Aashima Singla & Ritika Sachdeva[1] has presented a paper on " Review on Security Issues & Attacks in Wireless Sensor Networks ". WSN consists of hundreds or thousands of low cost, low power and self-organizing nodes which are highly distributed. Due to the reason that the sensor nodes are highly distributed, there is a need of security in the network. This paper discusses some of the issues and the denial of service attacks of security.

Chidambaram , Edwin Prem Kumar[5] has presented a paper on "A Review on different resource efficient key management schemes for Wireless Sensor Networks". The wireless sensor networks needs security for transferring the sensed data to the base station. There are many possible ways to attack the transferred data, for reducing the attacks security is mostly needed for the network.

Ali Bagherinia, Akbar Bemana [3] has presented a paper on "A Key Management approach for Wireless Sensor Networks " which facilitates an efficient scalable post-distribution key establishment that provides different security services.We have developed and tested this approach under TinyOs.

Snehal R Mankar, Prof.A.B.Raut[8] has presented a paper on "A Review on Certificate less Key Management Policy in Wireless Sensor Network" which proposed that a certificate less-effective key management (CL-EKM) protocol for secure communication in dynamic WSNs characterized by node mobility. The CL-EKM supports efficient key updates when a node leaves or joins a cluster and ensures forward and backward key secrecy.

Avinash Chaurasia, Utkarsh Dubey, R. K. Ghosh [4] has presented a paper on "A robust key management scheme with strong connectivity for wireless sensor network". In a wireless sensor network (WSN), creating pairwise secure links between resource constrained sensor nodes is a major challenge. In this paper we point out three serious weaknesses, namely, lack of scalability, high memory requirements and vulnerability to node capture attacks in an earlier scheme for designing pair-wise key agreement between any pair of sensor nodes in a WSN

Abdoulaye Diop, Yue Qi, Qin Wang, and Shariq Hussain[2] has presented a paper on "An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks". Key management in wireless sensor network is a complex task due to its nature of environment. Wireless sensornetwork comprise of large number of sensor nodes with different hardware abilities and functions. Due to the limited memory resources and energy constraints, complex securityalgorithms cannot be used in sensor networks. Therefore, an energy efficient key management scheme is necessary to mitigate the security risks.

Murat Al1, Kenji Yoshigoe[6] has presented a paper on "A Secure and Energy-Efficient Key Generation Mechanism for Wireless Sensor Networks". It enhances the data confidentiality and energy saving of an existing solution. Our approach utilizes encrypted message as a key generator (KG) for the next message. Thus, a KG that used to be exposed is now encrypted. A masking policy is incorporated to an encryption technique to further improve the data confidentiality. Furthermore, the proposed method no longer requires a transmission of extra information in a form of KGs reducing energy consumption incurred by data transmission.

Sneha Ghormare, Vaishali Saharel, Anil Jaiswal[7] has presented a paper on " A survey on data confidentiality for providing high security in Wireless Sensor network" .In Wireless Sensor Network, the security of data and confidentiality of data is an important aspect. Hence the data cannot be interrupted by the intruder. For updating configuration parameters and distributing management commands, data discovery and dissemination protocol for wireless sensor network is responsible. But, it has drawback is that, some protocols were not designed with security.

IV. CONCLUSIONS

In this paper we have surveyed about the Wireless Sensor Networks, its applications and challenges. Also we study about the Security in WSN and their types in reference to DOS attacks. As from the survey we can see that it is a very vast scheme and we furthermore can do a lot of enhancements in numerous fields as per the need accordingly.

REFERENCES

[1] Aashima Singla & Ritika Sachdeva“ Review on Security Issues & Attacks in Wireless Sensor Networks ”, ijarcsse, Volume 3, Issue 4, April 2013**.**

[2] Abdoulaye Diop, Yue Qi, Qin Wang, and Shariq Hussain “An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks”.

[3] Ali Bagherinia, Akbar Bemana “A Key Management approach for Wireless Sensor Networks ”, International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.3, August 2014

[4] Avinash Chaurasia, Utkarsh Dubey, R. K. Ghosh“A robust key management scheme with strong connectivity for wireless sensor network”.

[5] Chidambaram , Edwin Prem Kumar “A Review on different resource efficient key management schemes for Wireless Sensor Networks”, ijirset, K.L.N. College of Engineering and Technology, Madurai, Tamil Nadu, India , Volume 3, Special Issue 3, March 2014

[6] Murat Al1, Kenji Yoshigoe “A Secure and Energy-Efficient Key Generation Mechanism for Wireless Sensor Networks”.

[7] Sneha Ghormare, Vaishali Saharel, Anil Jaiswal“ A survey on data confidentiality for providing high security in Wireless Sensor network“, ijarcsse, Volume 5, Issue 1, January 2015

[8] Snehal R Mankar, Prof.A.B.Raut “A Review on Certificate less Key Management Policy in Wireless Sensor Network”, ijirc, International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.3, August 2014