A Survey Paper on Security Protocols of Wireless Sensor Networks

Aditya Sharma[1], Garima Tripathi[2], Md Sohail Khan[3], Kakelli Anil Kumar[4]

[1]BE (Computer Science), Indore Institute of Science & Technology-II, Indore, Madhya Pradesh, India
[2]BE (Computer Science), Indore Institute of Science & Technology-II, Indore, Madhya Pradesh, India
[3]BE (Computer Science), Indore Institute of Science & Technology-II, Indore, Madhya Pradesh, India
[4]Associate Professor, Department of CSE, Indore Institute of Science & Technology-II, Indore, Madhya Pradesh, India

---***---

Abstract - ***Wireless Sensor Network stands as one of the most emerging technologies combining together sensing, computational capability and communication into minute devices proceeding towards whole new world of simplicity. In this modern era we find intellectuals all over the world discussing on two major growing trends "Internet of things (IoT)" and "Cloud computing". Now emergence of them may directly or indirectly depend on WSN too .When we talk about IoT it includes smart devices which are collecting data through sensors and sharing this data through wired and wireless communication networks. Many of cloud computing applications like that in health sector includes collection of data by sensors and then sending it wirelessly to cloud. It is difficult to deny that we are moving towards a world where Wireless Sensor Network will impact our day to day lives. So it is becoming even more important to work towards development of wireless sensor network. It will not only give a push to these emerging technologies but also with its own applications help human kind towards a simpler and better world. A wireless sensor network is composed of large number of dispersed autonomous devices which uses sensors to monitor physical or environmental changes in a geographical area, process this data and report the changes to a centralized point through a wireless communication network. WSN acts as a mediator between the real physical world and the virtual world. In this paper, we report some of the current trends, challenges and security issues with wireless sensor network.***

Key Words: *Wireless Sensor Network; Personal computers; Personal Digital Assistants; Denial of Service attack; offset codebook*

1. INTRODUCTION [1]

A wireless sensor network (WSN) is a collection of spatially distributed autonomous sensors to examine present atmospheric and physical such as temperature, pressure, etc. and to cooperatively pass the data gathered through the network to a main centralized point. A WSN in its simplest form can be defined as a collection of sensing devices (nodes) that can sense the environment, process data and communicate the information gathered from the monitored field wirelessly to a centralized point (sink) that can use it locally, or it is connected to other networks through a gateway.

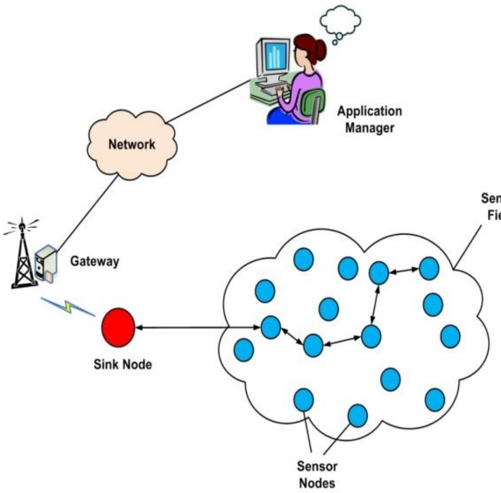

Fig -1: Architecture of WSM

A sensor node or a mote is a node which gathers information from fields performs some processing on that information and propagates this information with other connected nodes in the network. Gateways are the mediators that interface Motes with computers, personal digital assistants (PDAs), Internet and existing networks and protocols. Gateways may be considered as a proxy for the sensor network on the Internet. Application Manager is the software that connects to the gateways via some communication media like Internet or satellite link. Sink can be accessed by the user via communication link such as internet or satellite communication. Location of sink is mainly near the sensor field or well-equipped nodes of the sensor network.

2. CHARACTERISTICS OF WIRELESS SENSOR NETWORK

I. Dynamic network topology
II. Scalability to large scale of deployment
III. Wide range of densities
IV. Re-programmability
V. Maintainability
VI. Power consumption constrains for nodes using batteries or energy harvesting
VII. Ability to cope with node failures
VIII. Mobility of nodes
IX. Heterogeneity of nodes
X. Ability to withstand harsh environmental conditions
XI. Ease of use

3. DEPLOYMENT MODEL

I. Random Node Deployment: In this deployment nodes are deployed in random order i.e. they are scattered on uncertain locations. Critical inaccessible areas are deployed with this model.

II. Grid Deployment: Grid deployment is one of the most attractive approaches for moderate to large scale coverage-oriented deployment it is quite simple and scalable. Grid deployment is conducted by dropping sensors row-by row using a moving carrier.

III. Deterministic Node Deployment: In this deployment model the positions of nodes are predefined i.e. precise calculations are done for the positions of the sensors before deployment and then the sensors are placed on the respective positions according to these calculations.

4. APPLICATIONS OF WIRELESS SENSOR NETWORK [5]

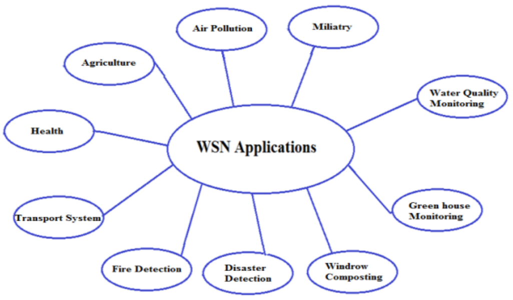

Fig -2: Application of WSM

Wireless sensor networks are currently being employed in a variety of applications ranging from smart homes to industry monitoring, and from medical investigation to military tracking. Military applications includes surveillance and target tracking. In industrial applications, sensor networks are used in monitoring hazardous chemicals. They are also used to monitor the environment and in early fire warnings in forests as well as seismic data collections. The WSN applications can be classified into three groups:

I. Environmental sensing
II. Condition monitoring
III. Process automation

5. RESEARCH CHALLENGES TO WIRELESS SENSOR NETWORK

I. Architect security solutions into systems from the start.

II. Current sensor network system lacks novel defences in conventional networks. Securing wireless communication links against attacks like eavesdropping, tampering, traffic analysis, and denial of service is a challenge.

III. Many applications are likely to engage the deployment of sensor networks under a single administrative domain in order to simplify the threat model.

IV. Possibilities to exploit redundancy, scale, and the physical characteristics of the environment in the solutions. Building sensor networks which continue to operate even if some fraction of their sensors is compromised, we have an opportunity to use superfluous sensors to resist further attack.

V. Resource constraints involving ongoing flow directions with asymmetric protocols where most of the computational burden falls on the base station and on public-key cryptosystems efficient on low-end devices.

VI. Challenges are to find ways to with-stand the lack of physical security through redundancy or knowledge about the physical environment.

6. SECURITY ISSUES IN WSN [7]

I. Data Integrity: It is very crucial in sensor network to ensure the reliability of the data. It ensures that data packets that are received by the destination are exactly the ones sent by the sender and any one cannot alter that packet in between.

II. Data Confidentiality: Confidentiality means to protect data during communication in a network to be understood other than intended recipient. Cryptography techniques are used to provide confidentiality. It is the one of the most important issue in network security.

III. Data Availability: It ensures that the services are always available in the network even under the attack such as Denial of Service attack (Dos). Availability is of primary importance to maintain an operational network. Availability ensures that a sensor node remains always active in the network to fulfil the functionality of the network.

IV. Data Authentication: It ensures that the data received by receiver has not been modified during the transmission. It is achieved through symmetric or asymmetric mechanisms where sender and receiver nodes share secret keys.

V. Data Freshness: It ensures that the data received by the receiver is most recent and fresh data and no adversary can replay the old data. It is achieved by using mechanisms like nonce or adding timestamp to each data packet.

7. VARIOUS WSN ATTACKS

I. Data integrity and confidential related attacks: In this type of attack, attempts to reveal or compromise the reliability and privacy of data contained in the transmitted packets.

i. denial of Service (DoS) Attack: Denial of Service attack attempts to make a network unavailable to its legitimate users. An attacker tampers the data before it is read by sensor nodes, thereby resulting in inaccurate readings and eventually leading to a wrong decision. This generally targets physical layer applications where sensor nodes are located.

ii. Node Capture Attack: Here, an attacker physically captures some of the sensor nodes and compromises them in a way that the sensor readings sensed by compromised nodes are inaccurate. The attacker may also attempt to extract important cryptographic keys like a group key from wireless nodes which are used to protect communications in most wireless networks.

iii. Eavesdropping attack: In Eavesdropping, the attacker gathers information from a network by snooping on transmitted data .To eavesdrop is to clandestinely overhear a personal conversation over a confidential communication in an unauthorized way. In eavesdropping information is not affected but its privacy is compromised.

iv. Service availability and bandwidth consumption attacks:

These attacks mainly aim to devastate the forwarding capability of forwarding nodes or consume inadequately available bandwidth; they are more likely related to availability of service and bandwidth consumption.

i. Flooding Attack: An attacker using this kind of attack normally sends a large number of packets to the victim or to an access point to avoid the victim or the entire network from establishing or continuing communications.

ii. Jamming (Radio Interference) Attack: In the simplest form of jamming, the attacker corrupts the transmitted messages by causing electromagnetic intervention in the network's operational frequencies, and in proximity to the targeted receivers. An attacker can commendably cut off the link among nodes by communicating continuous radio signals so that other authorized users are not allowed to access a particular frequency channel.

iii. Replay Attack: In replay attack, a valid data transmission is fraudulently repeated or delayed either by the originator or by an attacker, as a part of masquerade attack by an IP packet substitution. An attacker copies a forwarded packet and sends out the copies continuously to the victim in order to exhaust the buffers of the victim or power supplies and access points in order to disgrace network performance.

iv. Selective forwarding attack: This attack is sometimes called Gray Hole attack. In a simple form of selective forwarding, malicious nodes try to end the packets in the network by refusing to forward or drop the messages passing through them. There are various forms of selective forwarding attack. In one form of the selective forwarding, the malicious node can selectively drops the packets that are coming from a particular node or a group of nodes.

v. Identity related attacks: In general, these attacks cooperate with eavesdropping attacks or other network-sniffing software to achieve vulnerable MAC and network addresses. They target the authentication entity.

vi. Impersonate attack: An attacker imitate another node's identity (either MAC or IP address) to establish a connection with or launch other attacks on a sufferer; the attacker may also use the victim's identity to establish a connection with other nodes or launch other attacks on behalf of the victim.

vii. Sybil attack: A single node presents itself to other nodes with various fake identifications (either MAC or network addresses). The attacker can imitate other nodes identities or plainly create numerous random identities in the MAC and/or network layer.

8. SECURED PROTOCOLS IN WIRELESS SENSOR NETWORKS [14]

There are 8 Secured Protocols in Wireless Sensor Network:

I. SPINS: Security Protocols For Sensor Networks: It consists of two secure building blocks: SNEP and µTESLA. SNEP includes data privacy, two-party data validation, and proof of data freshness. µTESLA provides authenticated broadcast for severely resource-constrained environments.

II. TINYSEC: TinySec provides services similar to Snep, including authentication, integrity of messages, privacy and replay safeguard. A major difference between SNEP and TinySec is absence of counters that were used in TinySec. It uses CBC mode with cipher text stealing, for encryption and for authentication, CBC-MAC is used. TinySec is a link layer security protocols for WSN. Link layer security provides an effective way to prop up inactive communication (in network processing) among limited nodes to remove overlapping communication with the base station.

III. MINISEC: MiniSec is a safe and sound network layer protocol that requires lower energy consumption than TinySec while achieving a Security level which is similar with Zigbee. MiniSec uses offset codebook (OCB) mode as its block cipher mode of operation, which offers valid encryption with only one surpass over the message data. Normally two passes are required for both secrecy and authentication.

IV. LEAP: Localized Encryption And Authentication Protocol: LEAP Protocol is a key executive protocol for WSNs. LEAP is intended to support secure communications in sensor networks; therefore, it provides the fundamental protection services such as privacy and authentication.

V. ZIGBEE: Zigbee Coordinator acts as "Faith Manager", which allows other devices to link the network and also distributes the keys. It plays the three roles as follows:

i. Trust manager: Authentication of devices requesting to join the network is done.

ii. Network manager: Maintaining and distributing network keys.

iii. Configuration manager: Enabling end-to-end security between devices. It operates in both Residential Mode and Commercial Mode.

VI. LiSP: A lightweight Security Protocol: LiSP is a lightweight protection mechanism, which drives on efficient rekeying technique. LiSP can be used for key management of large as well as small networks. The main features of LiSP includes efficient key broadcast without retransmission/ACK, authentication of key discovery without incurring extra cost, facility to detect and recover lost keys, key refreshment without disrupting ongoing data encryption/decryption.

VII. LEDS: LEDS provides location aware end-to-end security. LEDS also provides end-to-end authentication and en-route filtering. It provides location aware key management. LEDS can be used in small as well as large networks. However, number of keys increment with cell size. In addition, LEDS does not prop up dynamic topology. LEDS divides the network in cell regions. If there is occurrence of an event within a region, the event should be sensed by T nodes.

VIII. Energy Efficient Link-Layer security Protocol (LLSP): LLSP stands for link layer security protocol which ensures message authentication, access control, message confidentiality, and replay protection. The idea of LLSP is based on TinySec. However, it uses dissimilar packet format and crypto structure. LLSP supports early rejection capability. It has also low performance overhead. However, it has low scalability as maintaining a large network is difficult with in node counter.

9. CONCLUSION

Our review paper has introduced various security protocols in Wireless Sensor Network Environment. These security protocols can function efficiently to provide security to WSN. In present generation WSN services are extending for mini applications like agriculture, military application and medical and health care. Security of WSN is one the most demanding and prominent key feature in today's world. So our research work is continuing to develop a new security protocol which can improve the security level of WSN.

ACKNOWLEDGEMENT

We would like to express our special thanks of gratitude to our mentor Mr. Kakelli Anil Kumar *for their guidance, our Head of Department (CSE) Mr. Virendra Singh for his encouragement and our Director Dr. Joy Banerjee for providing us opportunity to embark on this paper. We would like to thank all the faculty and staff members of the Computer Science Department who rendered their help towards completion of our paper. Finally we would like to thank our parents and friends for their support.*

REFERENCES

Dr. G. Padmavathi, Mrs. D. Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks”, International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009

Bhaskar Krishnamachari, *“An Introduction to Wireless Sensor Networks”,* Presentation at the Second International Conference on Intelligent Sensing and Information Processing (ICISIP), Chennai, India, 1 January 2005

Daniele Puccinelli, “The Basics of Wireless Sensor Networking and its Applications”

Marco Zennaro, ICTP Trieste-Italy, “Introduction to Wireless Sensor Networks”, February 2012

M.A. Matin and M.M. Islam , “Overview of Wireless Sensor Network”

Mark A. Perillo and Wendi B. Heinzelman, “Wireless Sensor Network Protocol”

Madhur Gupta, Monika Bansal, “Security Issues in Wireless Sensor Networks”, MIT International Journal of Computer Science & Information Technology Vol. 3, No. 1, Jan. 2013

Jason Lester Hill, “System Architecture for Wireless Sensor Networks”, Spring 2003

Kazem sohraby, daniel minoli, taieb znati, “Wireless Sensor Networks Technology, Protocols, and Applications”

Wikipedia https://en.wikipedia.org/wiki/Wireless_sensor_network

“Information processing and routing in wireless sensor networks”, http://www.worldscibooks.com/compsci/6288.html

Mokhtar Aboelaze, Fadi Aloul, “Current and Future Trends in Sensor Networks: A Survey”,IEEE-2005

Miguel Angel Erazo Villegas, Seok Yee Tang, Yi Qian, “Wireless Sensor Network Communication Architecture for Wide-Area Large Scale Soil Moisture Estimation and Wetlands Monitoring”

Sangeeta, Mr. Rajesh Parihar, “A comprehensive study of Medium Access Control Protocols in Wireless Sensor Network”, Vol. 4 Issue 5, May-2015

Himani Chawla, “Some issues and challenges of Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 7,July 2014

BIOGRAPHIES

Aditya Sharma is currently pursuing Computer Science & Engineering (CSE) from Indore Institute of Science & Technology II, Indore, Madhya Pradesh, India.

Garima Tripathi is currently pursuing Computer Science & Engineering (CSE) from Indore Institute of Science & Technology II, Indore, Madhya Pradesh, India.

Md Sohail Khan is currently pursuing Computer Science & Engineering (CSE) from Indore Institute of Science & Technology II, Indore, Madhya Pradesh, India.

Kakelli Anil Kumar is working as Associate Professor, Department of Computer Science and Engineering, Indore Institute of Science and Technology, Indore, Madhya Pradesh, India. He is having 12 years of teaching experience at UG and PG engineering level. His current research interests include protocol design, security, high quality data transmissions and cross layer design in wireless sensor networks, Mobile ad_hoc Networks, wireless communications and mobile computing.