INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

A SURVEY PAPER ON SECURITY MECHANISM OF WIRELESS SENSOR NETWORK

Mehul Joshi[1], Megha Joshi[2], Pooja Awasthi[3], Kakelli Anil Kumar[4]

[1]BE (Computer Science), Indore Institute of Science & Technology-II, Indore, Madhya Pradesh, India, mehul.joshi898@gmail.com
[2]BE (Computer Science), Indore Institute of Science & Technology-II, Indore, Madhya Pradesh, India, m.joshics@gmail.com
[3]BE (Computer Science), Indore Institute of Science & Technology-II, Indore, Madhya Pradesh, India, awasthipuja123@gmail.com
[4]Associate Professor, Department of CSE, Indore Institute of Science & Technology-II, Indore, Madhya Pradesh, India, anilsekumar@gmail.com
Mehul Joshi: 52,Ashok Vihar Colony Rau 453331, Indore M.P., Mobile No : +918982613685, mehul.joshi898@gmail.com

Abstract: - In this paper, a survey on Wireless Sensor Network (WSN) and their technology, standards, prototype and applications was carried out. A wireless sensor network consists of thousands of inexpensive miniature devices capable of computation, communication and sensing. It provides a bridge between both the real and virtual worlds. Allow the ability to observe the previously non-observable at a fine resolution over large spatio-temporal scales. Have a wide range of potential applications to agriculture, health, transport system, disaster detection, and defence. This paper supports the difficulties of operating such sensor network in the most hostile environments. Although the measurements and analysis demonstrated that control deployment was possible to some extent.

Keyword: Wireless Sensor Network, Personal computers, Personal Digital Assistants, Denial of Service attack, Offset codebook.

1. Introduction

A **wireless sensor network (WSN)** are structurally distributed self-directed sensors to monitor environmental or physical conditions such as sound, temperature, pressure, military work etc. and to cooperatively transfer their data through the network to a main location. Its simplest form makes it a network of (possibly low-size and low-complex) devices denoted as nodes that can sense the atmosphere and communicate the information collected from the monitored field through wireless links; the data is forwarded, possibly by multiple hops transmitting, to a sink that can use it locally, or is connected to other networks (e.g. Internet) through a gateway [10].

A **sensor node** or **mote** is a node in a sensor network that is proficient of performing some processing [3], collecting sensory information and communicating with other associated nodes in the network.

Gateways allow the scientists/system executives to interface Motes to personal computers (PCs), personal digital assistants (PDAs), Internet and surviving networks and protocols. In a shell, gateways act as a proxy for the sensor network on the Internet [2].

Application Manager connects to the gateways via some media like Internet or satellite link. Task Managers consist of data service and client data browsing and processing [2].

Sink interconnects the user through internet or satellite communication. It is positioned near the sensor field or well-equipped nodes of the sensor network. Collected data from the sensor field routed back to the sink by a multi-hop arrangement less architecture through the sink

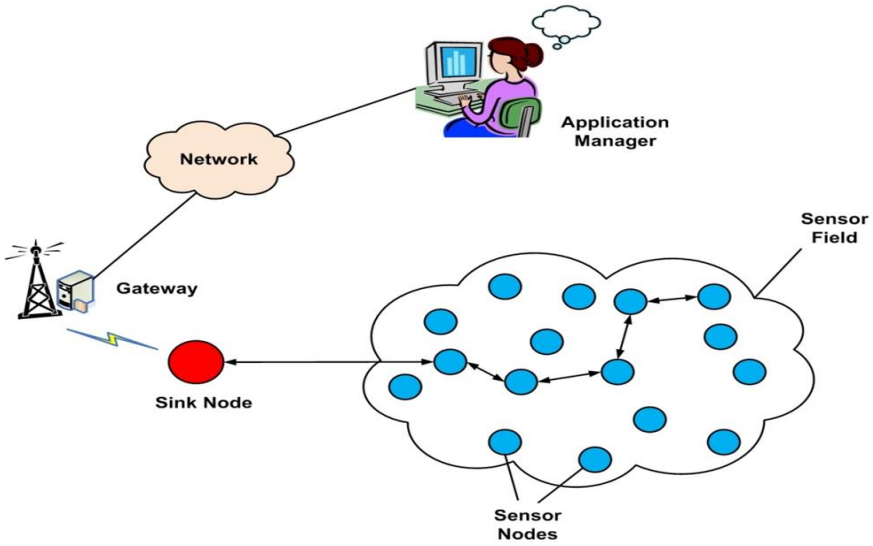

Figure 1: Architecture of Wireless Sensor Network

2. Characteristics of Wireless Sensor Network

- Dynamic nature
- Scalability
- Wide range of densities
- Re-programmability
- Maintainability
- Ability to face node failures
- Mobility of nodes
- Dynamic network topology
- Heterogeneity of nodes

3. Applications of Wireless Sensor Network

The WSN applications can be classified into three groups [5][6][7]:

1. Environmental sensing
2. Condition monitoring

3. Process automation

Figure 2: Different Application of Wireless Sensor Network

4. Research Challenges to Wireless Sensor Network[5]

- We have the opportunity to architect security solutions into these systems from the outset [1].
- Many applications are likely to involve the deployment of sensor networks under a single administrative domain, simplifying the threat model.
- It may be possible to exploit redundancy, scale, and the physical characteristics of the atmosphere in the solutions. If we form sensor networks so they continue operating even if some fraction of their sensors is negotiated, we have an opportunity to use redundant sensors to resist further attack.
- How to secure wireless communication links against snooping, tampering, traffic analysis, and denial of service.
- Others involve resource constraints, current guidelines include asymmetric protocols where most of the computational burden falls on the base station and on public-key cryptosystems well-organized on low-end devices.
- Finding ways to tolerate the lack of physical security.

5. Security issues in WSN

5.1 ***Data Integrity*****:** It ensures that data packets received by destination is exactly the same with transmitted by the sender and any one in between cannot alter that packet i.e. Reliability [4][11].

5.2 ***Data Confidentiality*****:** Confidentiality is to shield data during communication in a network to be understood other than intended recipient. Cryptography methods are used to make available confidentiality [4][11].

5.3 ***Data Availability*****:** Availability ensures that the services are always presented in the network even under the attack such as Denial of Service attack (Dos). Availability ensures that sensor nodes are active in the network to accomplish the functionality of the network [4][7][11].

5.4 ***Data Authentication*****:** Authentication of a sensor node safeguards the receiver that the data has not been modified during the transmission. Data authentication is attained through symmetric or asymmetric mechanisms where sending and receiving nodes share secret keys [4][11].

5.5 ***Data Freshness:*** It ensures that the data received by the receiver is recent and fresh and no adversary can replay the old data. It is achieved by using mechanisms like nonce or timestamp should add to each data packet [3][4][11].

6. Deployment Models

6.1 Random Node Deployment**:** In this, the nodes are scattered on those locations which are uncertain.

6.2 Grid Deployment**:** A grid deployment is deliberated as a good deployment in WSN, especially for the coverage. There are three popular grid arrangements namely, unit square, an equilateral triangle, a hexagon, etc. Among them, we explore a square grid because of its natural placement approach over a unit square.

6.3 Deterministic Node Deployment**:** In this, the locations of nodes are predefined i.e. positions of the sensors are calculated before deployment and then the sensors are placed on their respective positions.

7. Attacks in Wireless Sensor Network

7.1 Power consumption related attacks**:** One of the most valuable assets in wireless network is the power source. In power consumption related attacks an attacker tries to exhaust the wireless device's power source and it may degrade the lifetime of the network. A worst case scenario may even collapse the network communication [10].

- ***Denial of Sleep Attack:*** In a wireless network when there is no radio transmission, the MAC layer protocol reduces the node's power consumption by adaptable the node's radio communications. An attacker may use this scenario and try to drain a wireless device's limited power source (especially sensor devices) so that the node's lifetime is significantly shortened. Thus, the attacker tries to attacks the MAC layer protocol to shorten or disable the sleep period [10].
- ***Collision Attack*****:** In collision attack, attacker tries to impure the octet of transmitted packets. If attacker succeeds in doing so; then, at the receiving end; the packets will be rejected due to checksum mismatch. The retransmission of packets could cause exhaustion of essential resources i.e. energy of the sensor nodes [10].
- ***De-Synchronisation Attack:*** In de-Synchronization Attacks, attacker forges messages between sender and receiver. Modification in control flags or sequence numbers are usually made. If the attacker is lucky and get the control at right time, then he might prevent the endpoints from ever exchanging messages as they will be, by continuously requesting for retransmission of lost message [10]

7.2 Routing related attacks**:** These attack performs its act at the network layer and attempt to change routing information, and to manipulate and benefit from such a change in different ways by altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel traffic on network, extend or shorten source routes, generate false error notification, partition the complete network and also it increases end-to-end latency, etc. [10].

- ***Unauthorized routing update attack*****:** An attacker tries to modify routing information maintained by routing hosts, such as base stations, access points to exploit the routing protocols**.** [10]
- ***Wormhole attack:*** In a this attack, an attacker gains a packets at any one point within a network, "tunnels" them to another point in the network, and then replays that packet into the network from the packet attaining point . An attacker intrudes propagates originated by the sender, duplicates a portion or a whole packet, and speeds up sending the duplicated packet through a specific wormhole tunnel in such a way that the copied or error packets reaches at the destination before the original packet which traverses through the usual routes [10].

- ***Spoofing Attack:*** In this, attacker complicates the network by creating routing loop, attracting or replaying the routing information [10].
- ***Sinkhole attack:*** It is particularly severe attack that prevents the base station from obtaining complete and correct sensing data, thus forming a major threat to higher-layer applications. In this, a compromised node tries to draw all or as much traffic as conceivable from a particular area, by making it looks attractive to the neighbouring nodes with respect to the routing metric. As a result, the affected node manages to attract all traffic that is to be sending to the base station by advertising as having a higher level of trust and also as a node in the shortest distance [10].

***7.3 Privacy related attacks*:** This type of attack uncovers the privacy of communications and in the worst case; it can cause false assertions casualty.

- ***Traffic analysis attack*:** An attacker attempts to gain knowledge of the network, traffic, and node behaviour. The traffic analysis may include examining the message length, message pattern or coding, and duration of the message stayed in the router. In addition, the attacker can correlate all incoming and outgoing packets at any router or member of the system. Such an attack violates privacy and can harm members for being linked with messages

8. Secured Protocols in Wireless Sensor Networks[10]

There are following 8 Secured Protocols in Wireless Sensor Network-

8.1 SPINS: Security Protocols for Sensor Networks: "SPINS" is proposed by Adrian Perrig. SPINS has two secure building blocks: SNEP and µTESLA. **SNEP** constitute: - confidentiality of data, two-party data authentication, integrity and evidence of freshness of data. **µTESLA** provides authenticated broadcast for severely resource-constrained environments [10].

***8.2 TINYSEC*:** Karlof designed the replacement for the unfinished SNEP, known as TinySec. Inherently it provides similar services that are provided by snep wich includes authentication of data, message integrity, data confidentiality and replay protection. The big difference between TinySec and SNEP is that there are no counters used in TinySec that are used in SNEP. For encryption, it uses CBC mode with cipher text stealing, and for authentication, CBC-MAC is used. TinySec is a link layer security protocols for WSN. Link layer security provides an effective way to support passive communication among local nodes so as to remove overlapping communication of the local nodes with the base station [10].

***8.3 MINISEC*:** Minisec is a secure network layer protocol that claims to have lower energy consumption than TinySec while achieving a level of security which matches that of Zigbee. An important feature of MiniSec is that it uses offset codebook (OCB) mode for operation of its block cipher mode, which offers authenticated encryption with only one pass over the message data whereas normally two passes are required for both secrecy and authentication.

***8.4 LEAP: Localized Encryption and Authentication Protocol*:** Sencun Zhu proposed LEAP Protocol. It is a key management protocol for sensor networks. LEAP is designed in such a way that it supports secure communications in sensor networks; that is why it provides the basic security services such as data confidentiality and data authentication in wireless sensor network.

***8.5 ZIGBEE*:** Zigbee plays the three roles as follows [6] :

i. Trust manager: authentication of devices requesting to join the network.
ii. Network manager: maintaining and distributing network keys.
iii. Configuration manager: enabling end-to-end security between devices.

8.6 LiSP: Llightweight security mechanism is based on efficient rekeying technique. It can be used for key management of small and large networks as well. The main features of LiSP includes efficient key broadcast without retransmission/ACK, ability to detect and recover lost keys, key refreshment without disrupting ongoing data encryption/decryption [10].

***8.7 LEDS*:** It provides end-to-end authentication, security and enroots filtering. It provides location aware key management. LEDS can be used in both small and large networks [10]. However, number of keys increases with cell size. In addition, LEDS does not support dynamic

topology. It divides the network in cell regions. If an event happens within a region, the event should be sensed by T nodes.

8.8 Energy Efficient Link-Layer security Protocol (LLSP): It ensures message authentication, access control, message confidentiality, and replay protection. It follows the same idea follows in Tinysec. However, it uses different packet format and crypto structure. LLSP supports early rejection capability. However, it has low scalability as maintaining large networks are difficult within the node counter.

9. Conclusion

Our Review paper presents various key security mechanisms for wireless sensor networks. These security mechanisms are highly essential mechanism for wireless sensor network because wireless sensor network is a sensitive network and easily attack with various security attacks. Our research work is proceeding further to introduce a new security mechanism for WSN to improve its security feature with low computational resources.

REFERENCES

[1] **Bhaskar Krishnamachari,** January 2005 "An Introduction to Wireless Sensor Networks" Presented at the Second International Conference on Intelligent Sensing and Information Processing (ICISIP), pp 3.
[2] **Sangeeta , Mr. Rajesh Parihar**, May-2015 "A comprehensive study of Medium Access Control Protocols in Wireless Sensor Network " International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463 Vol. 4 Issue 5, pp 82.
[3] **Akkaya, K. and Younis,** 2005 "A survey of Routing Protocols in Wireless Sensor Networks", Elsevier Ad Hoc Network Journal , pp 4
[4] **Dr. G. Padmavathi**, **Mrs. D. Shanmugapriya**, 2009 "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, pp 1-2
[5] **D. Puccinelli and M. Haenggi,** Aug. 2005 "Wireless Sensor Networks-Applications and Challenges of Ubiquitous Sensing," IEEE Circuits and Systems Magazine, pp 19-31.
[6] **Marco Zennaro**, ICTP Trieste-Italy, "Introduction to Wireless Sensor Networks", February 2012, pp 3, 7,14,20,24.
[7] **Kazem sohraby, daniel minoli, taieb znati**, 2007"Wireless Sensor Networks Technology, Protocols, and Applications",pp 10-11.
[8] ***Wikipedia*** https://en.wikipedia.org/wiki/**Wireless_sensor_network**
[9] **Mokhtar Aboelaze, Fadi Aloul**, IEEE-2005 "Current and Future Trends in Sensor Networks: A Survey", pp 4.
[10] **Abu Shohel Ahmed,** 27 April 2009 "An Evaluation of Security Protocols on Wireless Sensor Network ", pp 2-5
[11] **Himani Chawla**, July 2014 "Some issues and challenges of Wireless Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering Volume 4, Issue 7, pp-237-238

A Brief Author Biography

1st Mehul Joshi: Mehul Joshi is pursuing B.E. (Computer Science and Engineering) from Indore Institute of Science and Technology, Indore. He is 4th Year student. His Research interest are Artificial Intelligence includes and security mechanism in Wireless sensor network and Object Oriented Technology. He is continuing research work in WSN, heterogeneous deployment.

2st Megha Joshi: Megha Joshi is pursuing B.E. (Computer Science and Engineering) from Indore Institute of Science and Technology, Indore. She is 4th Year student. Her Research interest is security mechanism in Wireless sensor network and Architecture of Wireless Sensor Network. She is continuing research work in security algorithms in WSN.

3rd Pooja Awasthi: Pooja Awasthi is pursuing B.E. (Computer Science and Engineering) from Indore Institute of Science and Technology, Indore. He is 4th Year student. Her research interest is Different Attacks on Wireless Sensor Network. She is continuing research work on Different attacks on Wireless Sensor Network.

4th Kakelli Anil Kumar: Kakelli Anil Kumar is working as Associate Professor in Dept. of CSE at Indore Institute of Science and Technology. He is having 12 Years of Teaching Experience at UG and PG engineering level. His Research interest includes protocols design and development in Wireless sensor network for quality Data Transmission. He is continuing research work in WSN, heterogeneous deployment and secures algorithms.