ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Review on Security in Wireless Sensor Network

Apeksha Malik[#1], Archit Kumar[*2]

[#]M.Tech Scholar, Department of Computer Science, Banasthali University, Jaipur, India

[*]Assistant Professor, Department of Computer Science, CBS Group of Institutions, Jhajjar, India

***Abstract*— Wireless Sensor Networks (WSN) is an emerging and one of the dominant technology trends in the upcoming decades has posed many potential applications and numerous unique challenges to researches. These networks consist of hundreds or potentially thousands of small sized, low power, low cost and self-organizing sensor nodes which are highly distributed in hard accessible terrains. Due to their deployment in open environments, unattended nature, resource constraints, wireless and shared communication, un-trusted and broadband transmissions between them, WSNs are prone to different types of attacks. Thus, security is a crucial requirement in WSNs which is a very difficult task to implement. In this paper, we focus on some security issues and different types of attacks in sensor networks. This paper also discusses some security detection approaches and defensive mechanisms against these attacks efficiently.**

***Keywords*— Wireless Sensor Networks, Data Communication, Sensor nodes, Physical attacks, countermeasures.**

I. INTRODUCTION

A wireless sensor network (WSN) is a medium of interaction between user or computer and the surrounding environment. WSN can be described as network of spatially distributed nodes having general-purpose computing elements that cooperatively sense, monitor, and collect the data from the environment. These nodes are embedded with sensing devices called sensors, to track physical or environmental conditions such as temperature, humidity, pressure, sound, vibration, motion, direction, and pollution levels. Two other components of sensor nodes are: data processing and communication.

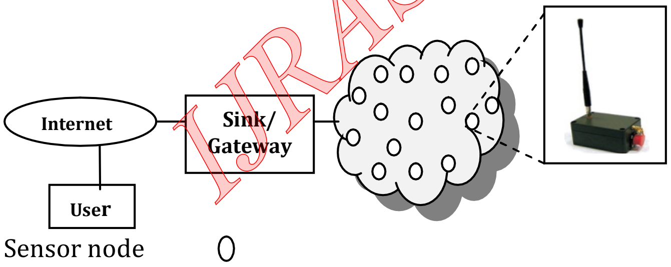

Fig. 1 Wireless Sensor Network

In WSN, sensor nodes collect data from the real world that can be concerning a physical object or the happening of a certain event in the environment and apply their processing abilities to locally perform simple calculations to convert them into digital signals. An aggregation point of WSN gathers this data from their neighbouring nodes, integrates the collected data and then transmits it to a computing system called base station for further processing. Base station acts as an interface between user and internet. In WSN, sensor nodes' location needs not to be preset. There can be random deployment of sensor nodes in hard accessible terrains. In this case, self-organizing capability of sensor network protocols and algorithms must be hold [1]. But due to the above random deployment, unattended nature of sensor nodes and communication between nodes and base station without human intervention, WSNs become susceptible to many types of attacks which can be malicious and harmful for WSNs. Due to deployment in unfriendly environments, automated nature, limited resource constraints, unprotected and insecure nature of communication channel, un-trusted and broadcast transmission media, most of the security techniques of traditional networks are impractical to implement in WSNs, therefore security is a crucial requirement for WSNs against harmful attacks. The main purpose of the paper is to present an overview of security in WSNs, different types of attacks and their defensive mechanisms.

IJRASET: ISSN: 2321-9653

IJRASET: ISSN: 2321-9653

II. Security in Wireless sensor network

WSN is an active research area at present. Security is a general concern for all networks, but security in WSN is very significant to make its applications successful. For instance, if sensor network is used for military or homeland security purpose, it is very important to keep the sensed information confidential and authentic. Providing security for WSN represents a rich field of research challenges as many existing security techniques for traditional networks are not appropriate for WSN. Security attack is a major concern for WSNs because of the following reasons [2]:

A. *Usage of limited resource constraints in the system*

1) *Limited memory and storage space*

2) *Limited power*

3) *Limited Bandwidth*

B. *Physical accessibility to sensor and unattended operation of sensor nodes*

1) *No central management point*

2) *Absence of Infrastructure*

3) *Managed remotely*

4) *Exposure to physical attacks*

C. *Wireless unreliable communication of the system devices*

1) *Latency*

2) *Unreliable transfer*

Because of the above reasons, sensor nodes should be equipped with security techniques to protect against many attacks such as eavesdropping, physical tempering, denial of service, node capture and replacement etc. The researchers in WSN security have purposed various security techniques which are optimized for these networks with resource constraints [3]. These techniques cover a large spectrum of security issues such as authentication, cryptography, integrity, key management etc., to detect, prevent or recover from various security attacks and result in protecting the sensitive information. A number of secure and efficient routing protocols, data aggregation protocols etc. has also been purposed by several researchers in WSN security. Even with these mechanisms, sensor nodes could be attacked or could be made non-operational by malicious attackers or physical break-down of the infrastructure. That's the reason that WSN requires a security mechanism which can minimize the overhead without affecting network performance.

III. Security requirements

As WSN shares the information among sensor nodes, it requires a secure protocol. An effective security protocol should services to meet several security requirements which are described as below [4] [5] [6]:

A. *Authentication*

Authentication is an assurance of communication nodes' (i.e. source node and destination node) identities. This ensures that the communication from one node to another node is valid or genuine i.e. a malicious node cannot pretend to be a trusted node in the network. Authentication can be achieved through the use of message authentication code (MAC), broadcast and multicast authentication, authenticating public key, signature, and challenge response etc.

B. *Confidentiality*

Confidentiality is an assurance of authorised access to sensitive information. It is the ability of the network to make the information confidential. This ensures that the sensitive information is protected and cannot be understood by unauthorised third parties. Confidentiality can be achieved through the use of data encryption with a secret key that only intended receivers possess.

C. *Integrity*

This is basic requirement of any communication network. Integrity is an assurance that the data packets are not manipulated in transmission. This ensures that the information sent from one node to another is not manipulated either by malicious intermediate nodes or by accident. Integrity can be achieved through the use of message integrity code in the network.

D. *Availability*

Availability is an assurance of the ability to provide expected services for which they are designed in advance such as minimize the energy consumption and extend the network life. In WSN, senor nodes may run out of battery power due to excess communication or computation and becomes unavailable. So, it ensures that the expected services are available even in the presence of denial-of-service attacks. Availability can be achieved through the use of key

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

management functions, multipath routing, selective forwarding etc. in the network.

E. *Flexibility*

Flexibility is an assurance that a network can work well with changing conditions. WSN are used in dynamic area scenarios where tasks and environmental conditions change frequently. Changing task means sensors may be eliminated from the network or introduced to the network. And a single network may be divided into two or more networks or two or more sensor networks may be combined into one. To achieve the flexibility in the network, key establishment protocols for all possible scenarios of sensor network must be flexible.

F. *Data freshness*

Data freshness is an assurance that the data is fresh and no old message is replayed by an adversary. All information represents a temporary status of an object or event and this information changes with time. Therefore, the data packets are valid only up to a limited time interval. After that time interval, it becomes useless. To achieve data freshness, a timestamp cab be attached to every packet. Recipient nodes compare the timestamp in the packet with its own time clock and decide whether the packet is legitimate or not.

G. *Self-Organization*

Self-Organisation capability is an assurance that every sensor node is independent and flexible enough to be self-organised or self-healed according to the circumstances. As the senor network is infrastructure less, self-organization becomes the important and challenging requirement to support multipath routing and public-key distribution in the network.

H. *Secure Localization*

Secure Localization is an assurance of ability of the sensor network to accurately and automatically locate each sensor in the network. In order to find the location of the fault in network, sensor network requires accurate location information of sensor nodes. This accurate location information can be calculated through various techniques such as Verifiable Multilateration (VM), Secure Positioning for Sensor Network (SPINE) algorithm, and Secure Range-Independent Localization (SeRLoc).

I. *Robustness and Survivability*

Robustness and survivability is an assurance that a sensor network's protection against the attacks and it can still work correctly even if any attack occurs. A Senor Network must be robust against various security attacks. It should have the capability to reduce the effect if any attack occurs.

J. *Time Synchronization*

Time synchronization capability of the sensor network is used to conserve energy of sensor nodes, to compute end-to-end delay of a packet, for tracking applications etc. An individual sensor node should be turned off for some time when it is not in use in order to save the power. This is a challenging task as a set of secure protocols is required for sender-receiver (pair wise), multihop sender-receiver (for use when the pair of nodes are not within single-hop range), and group synchronization.

IV. WSN SECURITY ATTACKS AND THEIR DEFENSIVE MECHANISMS

As WSNs are resource constraint networks. Due to this and above mentioned reasons, WSNs are prone to many attacks. The various WSN security attacks, their definitions, threats, effects on the network and their defensive mechanisms are defined below in table I [6] [10] [12] [14].

TABLE I
ATTACKS ON WIRELESS SENSOR NETWORK

Attacks	**Attack Definition**	**Attack Threat**	**Attack Effects**	**Defensive Mechanisms**
Eavesdropping	Attacker tries to capture the message from network traffic either by listening to the network	Confidentiality	Extracting sensitive WSN information, delete the privacy protection, reducing	Key protects DLPDU and session keys protect NPDU from

IJRASET : ISSN: 2321-9653

	traffic transmitted by the nodes, or directly compromising the nodes.		data confidentiality and launching other attacks.	Eavesdropper
Signal/ Radio Jamming	Attacker tries to transit radio signals emitted by the sensors to the receiving antenna at the same transmitter.	Availability, Integrity	Radio interference, resource exhaustion	Channel hopping and Blacklisting
Collision	When two nodes attempt to transmit on the same frequency	Integrity, Confidentiality	Change in data portion, delete the privacy protection	Error correcting code, CRC and Time diversity
Node capturing attack, Device tampering attack	Direct physical access, captured and replace nodes with malicious nodes.	Availability, Integrity, Confidentiality, Authenticity	Damage or modify physically stop/alter node's services, take complete control over the captured node, software vulnerabilities	Protection and Changing of key
Node Outage	Stopping the functionality of WSN's components	Availability, Integrity	Stop nodes services, impossibility reading gathered information, launching a variety of other attacks	Hiding components
Node Replication attack	An attacker adds node to an existing sensor network by copying the node ID of an existing sensor node	Integrity, Confidentiality, Authenticity	Misroutes packets, extracting sensitive WSN information, delete the privacy protection	Protection of Network ID and other information that is required to join device
General DOS attacks	Attacker injects malicious information or alters the routing setup messages which prevent the routing protocol from proper functioning.	Availability, Integrity, Confidentiality, Authenticity	Effects of physical layer, link layer, routing layer, transport layer and application layer attacks	Protection of network specific data like network ID etc. Physical protection and inspection of network
Path-based DOS attacks	Typical combinational attacks include jamming attacks	Availability, Authenticity	Nodes battery exhaustion, network disruption, reducing WSN's availability	Spread spectrum for radio communication, priority messages
Sybil attack	A malicious node influenced by an attacker creates fake identities to perform	Availability, Integrity	Damage routing algorithms, data aggregation, reduce the Integrity, Storage and	Physical protection of devices, regularly changing of key, Resetting of devices

IJRASET: ISSN: 2321-9653

	desired attacks on the network		Resource exhaustion	and changing of session keys
Blackhole attack	A malicious node influenced by the attacker advertises a short distance to all destinations and attracts all the traffic to make a blackhole.	Availability, Integrity	Cause traffic congestion, reduce the Integrity and Resource exhaustion	Authorization, monitoring, redundancy checking
Wormhole attack	An attacker records the packets at one location and then retransmits those packets to another location in the network.	Availability, Integrity	Exhaustion of energy resources, cause traffic congestion	Physical monitoring of field devices and regular monitoring of network using Source routing. Monitoring system may use Packet Leach techniques
Sinkhole attack	An attacker makes a malicious node attractive for surrounding nodes by forging routing information	Availability	Exhaustion of energy resources, decrease End-to-End Reliability	Authentication, monitoring, redundancy
Hello flood attack	An attacker sends HELLO packets to sensor nodes with high radio transmission range and processing power	Availability, Integrity	Wastage of energy, data loss	Authentication, bi-directional link verification, packet leashes by geographical and temporal info
Selective Forwarding attack	An attacker creates malicious nodes which selectively forward only certain messages and simply drop others.	Availability	Resource exhaustion, misdirection of traffic and disturbs quality of service	Regular network monitoring using Source Routing, using multiple paths to send data
Acknowledgement spoofing	An attacking node spoofs the acknowledgements of overhead packets destined for neighbouring nodes in order to provide false information to neighbouring nodes.	Availability, Authenticity	Unreliable communication, disturbs quality of service	Authentication, bi-directional link authentication verification, use different path for resending the message
Traffic Analysis attack	An attacker monitors the sender and receiver nodes, tracks the routing path, and	Integrity, Confidentiality, Authenticity	Extracting sensitive WSN information, delete the privacy protection, reducing	Sending of dummy packet in quite hours, and regularly monitoring WSN

IJRASET: ISSN: 2321-9653

	generates events.		data confidentiality and launching other attacks	network
Neglect and Greed attack	A malicious node influences multi-hopping in the network, either by dropping packets or by routing the packets towards a false node.	Availability, Authenticity	Resource exhaustion, unreliable communication	Redundancy, Probing

V. Conclusions

Security is an important requirement which is very challenging task to implement on sensor networks in different application areas. In this paper, we present a brief review on wireless sensor network. Then we discussed about the security in wireless sensor network and the reasons why it is required. And as the sensor networks share the information among sensor nodes, the security protocols must have security requirements. These various security requirements for creating secure protocols are also discussed in brief. The security attacks mainly targets the security dimensions such as availability, integrity, confidentiality, and authenticity. The different security attacks, their definitions, threats, effects and their defensive mechanisms are discussed as a comparative view in this paper.

References

[1] Aashima Singla and Ratika Sachdeva, "*Review on Security Issues and Attacks in Wireless Sensor Networks*", IJARCSSE, Vol. 3, Issue 4, ISSN: 2277-128X, April 2013.

[2] Rina Bhattacharya, "*A Comparative Study of Physical Attacks on Wireless Sensor Network*", IJRET, Vol. 2, Issue 1, ISSN: 2319-1163, Jan 2013.

[3] Amita Sharma, Yogita Wadhwa, and Ankit aggarwal, "*Routing and Computing in Wireless Sensor Networks*", IJARCSSE, Vol. 3, Issue 1, ISSN: 2277-128X, Jan. 2013.

[4] Shio Kumar Singh, M P Singh, and D K Singh, "*A Survey on Network Security and Attack Defense Mechanism for Wireless Sensor Networks*", International Journal of Computer Trends and Technology, May to June Issue , ISSN: 2231-2803, 2011.

[5] Rajeshwar Singh, Singh D.K. and Lalan Kumar, "*A Review on Security Issues in Wireless Sensor Network*", Journal of Information Systems and Communication, Vol.1, Issue 1, ISSN: 0976-8742, 2010.

[6] M. Yasir Malik, "*An Outline of Security in Wireless Senor Networks: Threats, Countermeasures and Implementations*", Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management, DOI: 10.4018/978-1-4666-0101-7.ch024, 2010.

[7] Hemanta Kumar Kalita and Avijit Kar, "*Wireless Sensor Network Security Analysis*", IJNGN, Vol. 1, No. 1, Dec 2009.

[8] Joseph Migga Kizza, "*Implementing Security in Wireless Sensor Networks*", Data Communication and Computer Networks, pp. 297-310, 2008.

[9] Jennifer Yick, Biswanath Mukherjee, and Dipak Ghosal, "*Wireless Sensor Network survey*", Computer Networks, pp. 2292-1330, 2008.

[10] Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti, "*A Survey on Wireless Sensor Networks Security*", 4th International Conference : Sciences of Electronic, Technologies of Information and Telecommunications (SETIT), March 25-29, 2007.

[11] Yong Wang, Garhan Attebury, and Byrav Ramamurthy, "*A Survey of Security Issues in Wireless Sensor Networks*", IEEE Communications Surveys, Vol. 8, No. 2, 2nd Quarter 2006.

[12] John Paul Walters, Zhengqiang Liang, Weising Shi, and Vipin Chaudhary, "*Wireless Sensor Network Security: A Survey*", Security in Distributed, Grid, and Pervasive Computing, 2006.

[13] Adrian Perrig, John Stankovic, and David Wagner, "*Security in Wireless Sensor Networks*", Communications of the ACM, Vol. 47, No. 6, June 2004.

[14] Chris Karlof and David Wagner, "*Secure Routing in Wireless Sensor Network: Attacks and Countermeasures*", In Proc. Of the 1st IEEE Int. Workshop on Sensor Network Protocols and Applications (SNPA' 03), pp. 113-127, May 2003.

IJRASET: ISSN: 2321-9653