Original Research Paper Computer Science

WIRELESS SENSOR NETWORKS: SECURITY ATTACKS AND CHALLENGES

Viralkumar B. Polishwala Research scholar, Calorx Teachers' University

P. H. Bhathawala Professor, Calorx Teachers' University

Kamljit Lakhtaria Asso.Professor, Dept. of Computer Science, Gujarat University

ABSTRACT The Wireless Sensor Network built of nodes from very few to several hundred or even thousands and each node connects with one or more sensors. During transmitting the date among these nodes and sensors, security is the main concern for the WSNs. A Sensor responds and detects some type of input from both the physical or environmental conditions, such as pressure, heat, light, etc. To protect from such kind of situations Cryptography is one option. Cryptography can applied with symmetric key techniques, asymmetric keytechniques and hash function. Selection of appropriate lightweight cryptographic technique is much important due to the constraint like computing, communication and battery power over the WSNs.

KEYWORDS : Wireless Sensor Network, Sensor, Node, WSNS, Cryptography techniques.

I. INTRODUCTION

Currently, wireless sensor network is the most standard services employed in commercial and industrial applications, because of its technical development in a processor, communication, and low-power usage of embedded computing devices. WSNscan be defined as a network of devices that can communicate the information gathered from a monitored field through wireless links. The data is forwarded through multiple nodes, and with a gateway, the data is connected to other networks like wireless Ethernet.

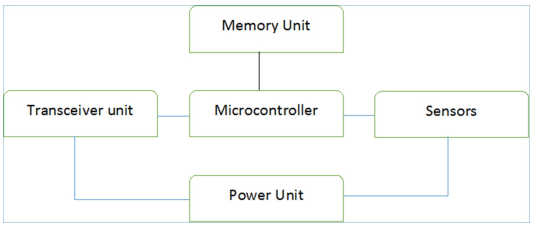

Figure I: Components of WSN

The WSNs are composed of five basic components: microcontroller unit (works as in charge of tasks like data processing and controlling of other components), a transceiver unit (do the data communication with other components of WSNS), a memory unit (stores the sensed data on temporary basis), a power unit (supplies the energy to the nodes through batteries) and a sensor unit(responsible for receiving information like temperature, humidity, light, heat etc). (See Figure I)

I. NEED OF SECURITY FOR WSN

The basic reasons behind the security needs for WSN are as follows:[1]

Integrity

It is necessary for the message that is travelling over the network; it must not be altered or changed maliciously by the attacker. To ensure this it is required that the node of the network should only able to use and upgrade the keys to access the information and ability to protect it against the active and intelligent attacker.

Availability

When anyresource is required by any node of WSN it should be easily available for operational access. The security techniques should always be available to avoid single failure. Sensor identities and public key of nodes should encrypted to prevent the attacks.

Confidentiality

The message should remain confidential from the passive attacker over the WSN. To achieve this the receiving node should not allow accessing the message to their neighbor nodes without authentication

Authentication

Authentication of the message with its origin node as well as other nodes, base station, cluster heads before granting the resource or revealing the message is required. The node which receive the message should also authenticate the message received from the original sender.

II. SECURITY ATTACKS ON WSNs

The attacker targets the communication channel to modify the data stream over WSN is identified as active attacks.[3]

a) Routing attacks in WSNs
b) Denial of Service
c) Node Subversion
d) Node Malfunction
e) Node Outage
f) Physical Attacks
g) Message Corruption
h) False Node
I) Node Replacement Attacks
j) Passive Information Gathering

a) Routing attacks in WSNs-

The network layer based attacks are considered as routing attacks, which occurs during routing of messages over network.

(I) Spoofing, altering and replaying the routing information

It causes routing loops, extension or shorten the service routes, generation of fake messages, growth in the end to end seek time.[3]

(ii) Selective Forwarding

Certain malicious node drops selective packets of information instead of forwarding. In such case neighbor node starts using another route.[3]

(iii) Sinkhole Attack

Capturing the traffic on a specific node is known as sinkhole attack. The attacker targets the nearby traffic through the compromised node.[3]

(iv) Sybil Attack

Self-duplication of the node causes the multiple identities for other nodes. It targets the fault tolerance schemes like multipath routing, distributed storage and topology maintenance.[3]

(v) Warmholes Attack
The warmhole attack causes the retransmission of the data packets through the network via recorded data packets from other locations of network.[3]

(vi) HELLO Flood Attack
In this attack, the attacker sends the HELLO packets to no of sensor nodes to generate the traffic over the WSN. By this act the nodes influenced with adversary as their neighbor. Where actually the attacker spoofs their neighbor nodes.[3]

b) Denial of Service
The DoS cause by whether the unwanted failure of node or malicious action. In many cases it is not due to adversary's attempt to subvert, disrupt or destroying a network but also due to disturb the network capability to provide a service. It can prevented by providing the strong authentication or identification of traffic. This attack make the unavailability of the resources over the network for fix or indefinite time like disturbing the provision of internet to the connected hosts for a while or for indefinite time.[4]

c) Node subversion
When any node is capture by the adversary the node information as well as the encryption keys may get disclosed as well as whole sensor network may get affected.[4]

d) Node malfunction
A malfunctioned node may cause inaccurate data over the network, due to which integrity concept may effected badly. If the affected node is cluster node or around the base station area whole network may get disturbed.[4]

e) Node Outage
The situation arises when any node of network stops functioning. If the cluster leader node stops functioning then the sensor network protocol should design in such way that the alternate routing should be provided to mitigate the node outage effect.[4]

f) Physical attacks
These attacks are irreversible which means unlike above attacks in this situation the sensors may get permanently destroyed. Whole control of the sensor network may in hand of the attacker. The attacker will be able to change the sensors with the malicious ones, extract the encryption keys, tamper with the network routing, alter the programs of sensor.[4]

g) Message Corruption
Integrity of the network may get affected when the attacker changes the details of the transmitted message.[5]

h) False Node
It is the most dangerous attack for WSN when it happens. In this attack an adversary adds a malicious node with wrong message. It prevents the original data to be transmitted over the network among other nodes of the network. It may potentially disturb the whole network.[5]

I) Node Replacement Attack
In this attack the adversary simply gives the nodeID of existing network sensor node to the new malicious node and enters the node in the network. This can totally disrupt the network. The attacker is also able to manipulate the whole segment of network or disconnect the segment.[6]

j) Passive Information Gathering
Un-encrypted information over the sensor network may get collected by the adversary through powerful resource. When such messages are containing the location of sensor nodes over the network the attacker is able to find the node and destroy them from the network. The prevent such attacks there should be a strong encryption technique should be implemented for transmitted message.[7]

III. CHALLENGES OF SENSOR NETWORKS

Comparing to the traditional network the WSNs may face no of constraints

a) Wireless Medium
Wireless medium is less secure due to its broadcasting nature which eavesdropping simple. The wireless medium allows the attacker to intercept and alter the valid nodes of the network. There must be some effective solution for securing the wireless medium for WSNs.[8]

b) Ad-Hoc Deployment
It is not possible to define static structure for the WSN due to its ad-hoc nature. The network topology is subject to change according to the node failure, addition of new node or mobility of nodes. Security scheme must be applied in such a way that it can adapt the dynamic environment.[9]

c) Hostile Environment
Hostile Environment is another challenge for functioning sensor nodes. Attackers can easily get the physical access of the resources of the network.

d) Resource Scarcity
The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. Security mechanism must be effective enough to communication efficient in order to energy efficient.[10]

e) Immense Scale
Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency.

f) Unreliable Communication
The security of the network is purely relying on the used protocol, which depends on the communication.[10]

(I) Due to connectionless network, packet routing is unreliable. (ii) Due to broadcast nature of WSN, communication may get conflict. (iii) Due to multi-hop routing, network congestion and node processing seek time may exceed in the network, which make hard to synchronize among the nodes.

g) Unattended Operation
In certain scenarios some of some node may unattended for long time due to functions of sensor network. There are three cautions to unattended nodes:[10]

Exposure to Physical Attacks: Sensors are deployed in an open environment where the attacker can get easy access to the node. Even if the node is located at secure place, the attack happened from the network itself.

Remote Management: The sensor network is managed from the remote locations. So it is hardly possible to detect physical tampering or maintenance issues.

No Central Management Point: the sensor network should be a distribute network by nature without any central point. If it is designed incorrectly, it will make the network organized fragile and inefficient.

IV. CONCLUSION

Networks become vulnerable due to deployment of sensor nodes in an unattended environment. WSNs implemented in applications like military, environmental, health and commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks. Security is an important feature for the deployment of Wireless Sensor Networks. In this paper, we have tried to narrate the attacks over the WSNs and

challenges to recover from them. This paper may motivate future researchers to come up with smarter and more robust security mechanisms and make their network safer.

REFERENCES:

1. Sharma, G., Bala, S., &Verma, A. K. (2012). Security frameworks for wireless sensor networks-review. Procedia Technology, 6, 978-987.
2. Padmavathi, D. G., &Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.
3. Karlof, C., &Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), 293-315.
4. Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006, February). Security in wireless sensor networks: issues and challenges. In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Vol. 2, pp. 6-pp). IEEE.
5. Zia, T., & Zomaya, A. (2006, October). Security issues in wireless sensor networks. In Systems and Networks Communications, 2006. ICSNC'06. International Conference on (pp. 40-40). IEEE.
6. Perrig, A., Stankovic, J., & Wagner, D. (2004). Security in wireless sensor networks. Communications of the ACM, 47(6), 53-57.
7. Undercoffer, J., Avancha, S., Joshi, A., & Pinkston, J. (2002, October). Security for sensor networks. In CADIP Research Symposium (pp. 25-26)
8. Naeem, T., & Loo, K. K. (2009). Common security issues and challenges in wireless sensor networks and IEEE 802.11 wireless mesh networks. 3; 1.
9. Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), 293-315.
10. Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2007). Wireless sensor network security: A survey. Security in distributed, grid, mobile, and pervasive computing, 1, 367.