ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

A Study on Security Threats and Their Countermeasures in Sensor Network Routing

Heena Singh[1], Monika Agrawal[2], Nidhi Gour[3], Prof. Dr. Naveen Hemrajani[4]

M.Tech Scholar, CSE, JECRC UNIVERSITY, Jaipur, India[1,2,3]

Head of Department, CSE, JECRC UNIVERSITY, Jaipur, India[4]

Abstract: In the present situation, Wireless Sensor systems have various provisions. WSN have an extensive number of compelled appended to them .WSN comprise of hundreds or many ease, low memory, low power, constrained vigour assets and sorting toward oneself out hubs that are profoundly circulated. As the sensor hubs are quite dispersed, there is a necessity of furnishing security in the system. The data in the system must be secured from the ambushers. These attackers may devise diverse kind of security dangers to make the WSN framework insecure. Exertion has been made to model the dangers scientifically so the answer for these dangers to be provided. This paper examines a portion of the security dangers and their countermeasures.

Keywords: Wireless Sensor networks, issues, security Concern, Security threats, Countermeasures**.**

I. INTRODUCTION

In current years, WSN has found a huge number of applications in the field of both research and academics. In WSN, the nodes are called as sensors, which sense the data like temperature, noise or sound, pressure, humidity, stress levels, soil variety, movements of objects, uncovering of objects around and other properties from the surroundings and then send this gathered information to the base station for the further analysis and decision making [4].WSN are deployed in natural environment where the sensor nodes remain unattended and are used for surveillance and monitoring [2]. WSN finds a large application in the fields like military, home automation, healthcare applications, traffic control and many civilian application areas [10]. In WSN, the data transmitted should be safeguarded from the unauthenticated and unauthorized nodes and attackers. The authenticity, integrity and confidentiality of the data that is transmitted between the nodes of the network should be maintained.

Table 1: Layer based attacks and possible security approaches [10]

Layers	Security Threats	Security Approach
Physical layer	Jamming and tampering	Uses MAC layer admission control mechanism & spread spectrum techniques.
Data Link Layer	Jamming and collision	Uses spread spectrum techniques and error correcting codes
Network Layer	Packet drop, bogus routing information and tunnel	Authentication
Transport Layer	Energy drain attacks and inject false messages	Authentication
Physical Layer	Attacks on reliability	Cryptographic Approach

II. SECURITY CHALLENGES

We have identified diverse challenges in providing safety measures to the wireless sensor networks. These challenges are [2, 7]:

- *First Challenge*: At the time of designing any of the security solution we should take care of the following resource constraints like limited energy, limited memory, limited computing power, limited communication bandwidth, and lastly the limited communication range.
- *Second Challenge*: The type of security mechanism that can be hosted on a sensor node is dependent on the capabilities and the constraints of the sensor node hardware.
- *Third Challenge*: The attacks on WSN can be introduced or come from all the directions and can target at any node lead to the leaking of secret information, interfering message, impersonating nodes, etc.
- *Fourth Challenge*: As the communication in WSN is through the wireless media i.e. primarily radio. This attribute of WSN makes wire-based security schemes impractical for WSNs.
- *Fifth Challenge*: The overall cost of WSN should be as low as possible.
- *Sixth Challenge*: The node failures may be permanent or intermittent, as this gives a higher level of system dynamics. The large number of nodes is expected in sensor network deployments and the nature of this is unpredictable.

III. FOR ACHIEVING SECURITY IN WIRELESS SENSOR NETWORKS

Four key issues have been recognized for furnishing security to the WSN [7]:

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

1. Prevention of Denial-of-Service: In denial-of –service attack, any event that diminishes a network's capacity to perform its expected function. The factors that can cause denial-of-service are resource exhaustion, hardware failures, software bugs, and environmental conditions.

2. Key Management in WSN: Key management is an important issue for the high security protection in WSN [5]. Providing key management service in WSN is extremely difficult due to various constraints in WSN environment, e.g. limited communication bandwidth, ad-hoc nature of the network, intermittent connectivity, resource limitation, etc.

3. Encryption and Decryption Mechanism: Since the WSN environment is resource-constrained, therefore this encryption and decryption mechanism has to be very simple and energy efficient [3, 9]. Due to the constraints like memory and energy, which are being used in the WSN environment, we can not use the asymmetric cryptography.

4. Secure Routing of WSN: The major threats that occur in the routing protocols of WSNs are [5]:

- External attackers- These attackers become successful in partitioning a network or introducing the excessive traffic load into the network. Various attacks include: replaying of old routing information, distorting routing information, etc. Cryptographic schemes can be used for defending against the external attacks.

- Internal attackers- There is a difficulty to put defence against such attacks. These nodes may send the malicious information to other nodes in the network.

IV. SECURITY CONCERNS

There are some security concerns which are as follows [3]:-

A. Availability

It guarantees that the network services are feasible even in the subsistence of denial of service attacks [3]. For the data availability, security protocol should possess less energy and storage, which can be reused by the code [4].

B. Data Confidentiality

Confidentiality is an acceptance of authorized access to information communicated from a verified sender to a verified receiver. For secure communication, encryption is used. The sensor information should also be encrypted to some extent to protect against the traffic analysis attacks [9, 4].

C. Data Integrity

In sensor networks, the integrity of data needs to be assured. In data integrity, the received data should not be tampered with and the new data has not been added to the original contents of the packet. Message Authentication Code (MAC) provides the data integrity [4, 3].

D. Data Authentication

Data authenticity is an assurance of the identities of communicating nodes. Nodes that are taking part in the communication must be capable of recognizing and rejecting the information from the authorized node [4].

E. Secure Localization

Attacker may probe the headers of the packets and protocol layer data for the secure localization. This feature must be satisfied during the implementation of security protocol [4].

F. Flexibility

Two or more sensor networks may be combined or merged into one or a single network may be divided into two or more networks [4].

V. SECURITY THREATS AT SENSOR NETWORK ROUTING

In sensor organizes, the system layer is planned as per the accompanying standards [9]:

1. The significant thought is the force effectiveness.
2. Most of the sensor systems are information driven.
3. Data conglomeration is advantageous just when it doesn't upset the community oriented exertions of the sensor hubs.
4. The attributes of a perfect sensor are area consciousness and characteristic based tending to.

Sensor hubs are spread either in close or inside wonder. Different tracking conventions are required between the sensor hubs and the sink hub for conveying the information all around the system [6]. A portion of the dangers of the system layer might be condensed as: Selective sending, Spoofed, modified, or replayed steering data, Sinkhole assaults, Wormholes ambushes, HELLO surge strike, and Acknowledgement assault.

Selective Forwarding:

In particular selective forwarding ambush, the malignant hub may say no to positive messages and basically can drop them by guaranteeing that further they are not proliferated. Typically it is accepted that in multi hop system, the hubs that are partaking will send the gained message steadfastly [1]. Yet sometimes it doesn't happen. This is really happens in particular sending ambush, as the pernicious hub may decline to certain messages and they drop these messages. An alternate manifestation of particular sending ambush is, a foe may be embedded in the smothering bundles that are beginning from few chose hubs and can dependably advance the remaining activity and can additionally restrict the suspicion of the wrong doing [7].

Spoofed, altered, or replayed routing information:

This is the most immediate attack or danger beside the routing protocol, since it focuses to the steering data that is traded around the nodes. By modifying, ridiculing, or replaying the tracking data, the adversaries could have the capacity to make the steering loops, pull in or repulse to the system movement, broaden or abbreviate the source routes, partition the system, create false blunder messages, builds the close to-end inactivity, and so on [1, 7, 5].

Sinkhole Attacks:

In a sinkhole attack, the objective of the adversary is to attract in all the traffic from a specific area through a

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 2, February 2014

compromising hub, making a sinkhole with the adversary at the inside of the network. For the explanation for why nodes on, or close to the way that the packet accompanies has numerous chances to mess around with the application information. Sinkhole ambushes works by making the bargaining node look uniquely striking to the encompassing nodes as for the tracking calculation [1, 7, 5].

Wormhole Attack:
Wormhole strike ought to be utilized as a part of grouping with the specific sending or listening in. In wormhole attack, the foes tunnel the accepted message in one some piece of the network in access to a low latency connection and are replayed in an alternate part [5]. Wormhole attacks are included in two far off malicious nodes that plot to minimize their separation from one another by handing-off the packets between an out-of-bond channels that is accessible just to the attacker [1, 7]

HELLO Flood Attack:
A novel attack is presented against the sensor systems i.e. the HELLO attack. There are numerous conventions that require the nodes to telecast the HELLO bundles for their proclamation to their neighbours, and a node which is getting such sort of packet can accept that it is in an ordinary radio extent of the sender [5]. This supposition may be false if there should be an occurrence of data with the huge transmission power which persuades each hub as the adversary is its neighbour [1].

Acknowledgement Attack:

A huge part is played by acknowledgements to ensuring the nature of administration and by making an alternate connection. This attack is presented on the routing calculations at the routing layer that needs the transmission of the affirmation messages. Attackers may eavesdrop packet transference from its connecting hubs and dupe the affirmations, in that way sends wrong data to the hubs [1].

VI. COUNTERMEASURES AT SENSOR NETWORK ROUTING

There is a problem in securing the network layer which reduces to the problem of route discovery security of a routing protocol [1, 7, 8].

Selective Forwarding Attack:
The countermeasure against this type of attack is that we can use multiple routing paths and send the redundant messages through which the probability of selecting a vulnerable route can be reduced. This forces the adversary to compromise more nodes to succeed.

Misdirection and Internet SMURF attack:
It can be easily handled as: If it is observed that a node's network link is flooded without any valuable information, then for sometime the victim node can be scheduled to sleep.

Black hole Attack:
For this attack, the unauthorized node may be easily identified by checking if any node is behaving abnormally. This attack is defended by accepting the routing replies from the authorized nodes.

Sybil Attack:
In the network layer, there is no effective defence mechanism against the Sybil attack. One important thing to note is that this attack may not survive only in the routing layer. In Sybil attack the attacker must attack the link layer and then gets the Sybil identities. The best mechanism available for the defence of Sybil attack is at the link layer. One solution is that every node shares a unique symmetric key with a trusted base station.

Wormhole Attack and HELLO flood attack:
In these attacks we check the bi-directional link while selecting a path. The location-based routing protocols avoid the wormhole attacks as in these protocols , each node may know that approximately how many hops it is from the sink. Wormholes cannot fool the nodes as they know their location.

Rushing Attack:
The technique that is used for the prevention of this attack is that while electing the route we have to detect a secure neighbour by checking the bidirectional link.

Alteration, Spoofed and Replay of information:
To assembly the base stations trustworthy, the adversaries are not able to spoof the broadcasted or flooded messages from any base station. Authentication and efficient techniques can be used to defend against the spoofing attacks. The encryption technique is applied to some of the fields at the header message, which saves some energy from computing and communicating some extra bits. Further for broadcasting the authenticated messages we make use of conventional techniques like packet overhead or the digital signatures. For the authenticated broadcast and flooding an efficient protocol is used i.e. TESLA and symmetric key cryptography is used.

VII. CONCLUSION

In this examination paper we have considered about distinctive key issues for the accomplishment of security identified angle in remote sensor systems. We examined or imparted the tests, dangers and countermeasures that are constantly confronted as for security. Conceivable results are characterized for the improvement of the security. This work is embraced by a portion of the creators which is in advancement for the planning of the security structure. For the further improvement the technocrats are basically being actualized so that there ought to be upgrade in the security.

REFERENCES

[1] C. Karlof and D Wanger, Secure Routing in Wireless Sensor Networks: Attacks and countermeasures, Sensor Network Protocols and Applications (SNPA 2003), May 2003
[2] L P. Akyildiz , W. Su , Y. Sankarasubramaniam and E. Cayiric, A survey on sensor networks, IEEE Communications Magazine.
[3] William Stallings, Cryptography and Network Security Principles and Practices, Third Edition, Pearson Education, ISBN 81-7808-902-5.

[4] SINGLA A. And SACHDEVA R., "Review on Security Issues and Attacks In Wireless Sensor Networks"3(4), 529-534, (2013)
[5] YONG WANG, GARHAN ATTEBURY, AND BYRAV RAMAMURTHY,"A Survey Of Security Issues In Wireless Sensor Networks", IEEE COMMUNICATION SURVEYS,8(2),2-23,(2006).
[6] CHEE-YEE and SRIKANTA P. KUMAR, "Sensor Networks: Evolution, Opportunities, and challenges", Proceeding of the IEEE, Vol.91, No.8, Aug 2003.
[7] KAR A. AND SARMA H.K.D ,"Security threats in wireless sensor networks" ,IEEE A&E SYSTEM MAGAZINE,39-45,(2008)
[8] Fei Hu, Jim Ziobro, Jason Tillett, Neeraj and K. Sharma, Secure Wireless Sensor Networks: Problems and Solutions, internet draft.
[9] Shio Kumar Singh, M P Singh, 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 2011, ISSN: 2231-2803.
[10] Kumari B., Shukla J., "Secure Routing In Wireless Sensor Network", Intenational Journal of Advanced Research in Computer Science and Software Engineering , 3(8),746-751,(2013)

BIOGRAPHIES

HEENA SINGH Born in 1990 in Rajsamand District (Rajasthan). She completed her B.Tech. (Information Technology) from Rajasthan Technical University and currently pursuing M.Tech (Computer Science) from JECRC University. Her major fields of study areas are Information Security, Wireless Sensor Networks.

MONIKA AGRAWAL Born in 1990 in Bharatpur District (Rajasthan). She completed her B.Tech. (Information Technology) from Rajasthan Technical University and currently pursuing M.Tech (Computer Science) from JECRC University. Her major fields of study areas are Information Security, Wireless Sensor Networks.

NIDHI GOUR Born in 1989 in Jaipur District (Rajasthan). She completed her B.Tech. (Computer Science) from Rajasthan Technical University and currently pursuing M.Tech (Computer Science) from JECRC University. Her major field of study areas are Information Security, Mobile Ad-Hoc Network.

NAVEEN HEMRAJANI Prof. (Dr.) Naveen Kumar Hemrajani has twenty years of research and teaching experience in Computer Engineering. He is currently a Professor and Head in Computer Science and Engineering Department, JECRC University. Presently he is chairman of computer Society of India, Jaipur Chapter. He is editorial member of various international journals of repute; more than 70 papers are credited to his credentials. Research Areas are Computer Networks and Software Engineering.