International Journal of Computer Science and Network (IJCSN)
Volume 1, Issue 4, August 2012 www.ijcsn.org ISSN 2277-5420

# Study of Network Layer Attacks and Countermeasures in Wireless Sensor Network



[1]Atul Yadav, [2]Mangesh Gosavi , [3]Parag Joshi

[1] Information Technology, Mumbai University, RMCET
Devrukh, Maharashtra, *India*

[2] Computer Engineering, Mumbai University, RMCET
Devrukh, Maharashtra, India

[3] Computer Engineering, Mumbai University, RMCET
Devrukh, Maharashtra, India

**Abstract**

Wireless platforms are less expensive and are more powerful, with usage in enabling the promise health science to military sensing operations. The wireless sensor networks are prone to more attacks than wired networks. However, the hardware simplicity of these devices makes defense mechanisms designed for traditional networks infeasible. This paper studies the security aspects of wireless sensor networks. A survey with attacks and countermeasures is carried out, in particularly network layer.

***Keywords:*** *WSN, Network layer attack, Countermeasure*

## 1. Introduction

A wireless sensor network (WSN) consists of distributed autonomous sensors to closely monitor physical or environmental conditions (such as temperature, sound, vibration, pressure, motion or pollutants). The applications supported by WSNs vary from monitoring, tracking to controlling. The Battlefield surveillance used in military operations is the idea behind WSN development. In a typical application, a WSN is scattered in a region where it collects data sensor nodes. In the era of interconnected world, security of both external and internal data exchange over network nodes is a primary concern. A sensor network constitutes of a wireless ad-hoc network, where each sensor supports a multi-hop routing algorithm (several nodes may forward data packets to the base station). In addition to one or more sensors, each node in a sensor network is typically equipped with a radio transceiver or other wireless communications device, a small microcontroller, and an energy source (battery). An attacker can easily intercept, inject or alter the data transmitted between the sensor nodes.

## 2. Layered Architecture of WSN

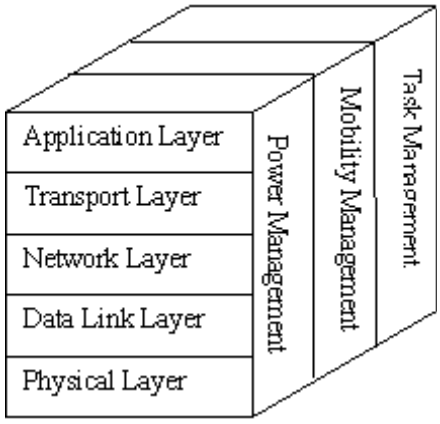


Fig.1 Sensor Network Protocol Stack

Wireless sensor networks use layered architecture like wired network architecture which shown in Fig.1.The protocol stack consists of the application layer, transport layer, network layer, data link layer, physical layer, power management plane, mobility management plane, and task management plane. Depending on the sensing tasks, different types of application software can be built and used on the application layer. The transport layer helps to maintain the flow of data if the sensor networks application requires it. The network layer takes care of routing the data supplied by the transport layer. The

physical layer addresses the needs of a simple but robust modulation, transmission and receiving techniques. In addition, the power, mobility, and task management planes monitor the power, movement, and task distribution among the sensor nodes. These planes help the sensor nodes coordinate the sensing task and lower the overall power consumption. The power management plane manages how a sensor node uses its power.

## 3. Network Layer Attacks

The objective of Network layer is to find best path for efficient routing mechanism. This layer is responsible for routing the data from node to node, node to sink, node to base station, node to cluster head and vice versa. To save the power of sensor so as to increase the life of sensor, network layer use SMECN (Small Minimum Energy Communication Network) and LEACH (Low Energy Adaptive Clustering Hierarchy) protocol.

### 3.1 Alter Routing Information Attack

The most direct attack against a routing protocol is to target the routing information in the network. An attacker may spoof, alter, or replay routing information to disrupt traffic in the network. These disruptions include creation of routing loops, attracting or repelling network traffic from selected nodes, extending or shortening source routes, generating fake error messages, causing network partitioning, and increasing end-to-end latency.

### 3.2 Selective Forwarding Attack

In a multi-hop network like a WSN, for message communication all the nodes need to forward messages accurately. An attacker may compromise a node in such a way that it selectively forwards some messages and drops others.

### 3.3 Sinkhole Attack

In a sinkhole attack, an attacker makes a compromised node look more attractive to its neighbors by forging the routing information. The result is that the neighbor nodes choose the compromised node as the next-hop node to route their data through. This type of attack makes selective forwarding very simple as all traffic from a large area in the network would flow through the compromised node.

### 3.4 Wormhole Attack

A wormhole is low latency link between two portions of a network over which an attacker replays network messages. The attacker receives packets at one location in the network, and tunnels them to another location in the network, where the packets are resent into the network. The tunnel between the two colluding attackers is known as the *wormhole*.



### 3.5 Sybil Attack

In Sybil attack, a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage, multipath routing, and topology maintenance. Replicas, storage partitions and routes believed to be used by disjoint nodes could in actuality be used by one single adversary presenting multiple identities.

### 3.6 Blackhole and Gayhole Attack

In this attack, a malicious node falsely advertises good paths (e.g. the shortest path or the most stable path) to the destination node during the path-finding process (in reactive routing protocols), or in the route updates messages (in proactive routing protocols). The intention of the malicious node could be to hinder the path-finding process or to intercept all data packets being sent to the destination node concerned. A more delicate form of this attack is known as the grayhole attack, where the malicious node intermittently drops the data packets thereby making its detection even more difficult.

### 3.7 Hello Flood Attack

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbor and begin exchanging information with the nodes.

### 3.8 Byzantine Attack

In this attack, a compromised node or a set of compromised nodes works in collusion and carries out

attacks such as creating routing loops, forwarding packets in non-optimal routes, and selectively dropping packets. Byzantine attacks are very difficult to detect, since under such attacks the networks usually do not exhibit any abnormal behavior.

### 3.9 Information Disclosure Attack

A compromised node may leak confidential or important information to unauthorized nodes in the network. Such information may include information regarding the network topology, geographic location of nodes, or optimal routes to authorized nodes in the network.

### 3.10 Resource Depletion Attack

In this type of attack, a malicious node tries to deplete resources of other nodes in the network. The typical resources that are targeted are: battery power, bandwidth, and computational power. The attacks could be in the form of unnecessary requests for routes, very frequent generation of beacon packets, or forwarding of stale packets to other nodes.

## 4. Countermeasure against Attack

We purposed some countermeasure to avoid or minimize such attack in network layer as follows.

### 4.1 Countermeasure against Selective forwarding Attack

*a. Using watchdog*

Watchdog technique is in fact a kind of supervising and observance over the network. For example, supervising whether a node has sent a received message or not?

*b. Listening to a channel*

Another resolution is to listen to a channel to make sure that each node sends the same message which its neighboring node has sent.

### 4.2 Countermeasure against Blackhole Attack

*a. Geographic forwarding*

Nodes are aware of their own and neighboring nodes' coordinates. Thus, each node can send messages according to the geographical position of the neighbors. So it is not absorbed easily towards the attacking node. In this method, nodes can send data from different routes regarding the coordinates of themselves or the neighboring nodes and avoid sending from a repeated and fixed route.

*b. Using resistive routing protocols*



Protocols resistant against different formations can also reduce the effect of this attack. These protocols do not confine themselves to the nodes' position in choosing a node as the next node to send data towards the sink and the nodes' remaining energy is efficient in algorithm selection. As soon as the network identifies a defect or detects incorrect data forwarding, it uses a systematic rerouting to avoid attacks. Those protocols which use serial number, when forwarding a package, can identify fake messages. Thus they are able to identify the messages sent by black hole node.

### 4.3 Countermeasure against Sybil Attack

Nodes' validation is one of the defensive methods against this attack. In this case, authentication and reliability of the node should be investigated before accepting it as a neighboring node. For validation, usually code identification of messages is used. In this method, the sink uses a valid key to validate nodes. Sometimes a periodical common key between the nodes is used to encode the communications.

### 4.4 Countermeasure against Hello Flood Attack

Such attacks can easily be avoided by verify bi-directionality of a link before taking action based on the information received over that link. If the base station limits the number of verified neighbors it can prevent this attack all together.

### 4.5 Countermeasure against Wormhole Attack

As it is described about black hole, geographical forwarding will be achieved through a routing protocol with resistant negotiations. Each message is forwarded singly. Selection of the next node is done by informing about the geographical position of the node. Such a design will not create a hole in the network, although sometimes it can be achieved randomly.

### 4.6 Countermeasure against Information Disclosure Attack

An effective method against this attack is to reevaluate the routing tables of the nodes when updating to avoid changing them by enemy nodes. Also the novelty mechanisms of the data can avoid the repeat of the data by investigating them. In this way, repeated messages are thrown away and this will preserve the network from repeated messages and node's memory filled. In wireless sensor networks which use hierarchical structure for routing, there are filters which test each message before forwarding. Messages with source addresses which are lawfully located in lower levels of hierarchy will be overthrown.

## 5. Conclusions

Attacks in Wireless Sensor Network are vital to the acceptance and use of sensor networks. In particular, Wireless Sensor Network product in industry will not get acceptance unless there is a fool proof against attack to the network. In this paper, we have made a attack analysis to the Wireless Sensor Network and suggested some counter measures particularly for Network layer of WSN.

## References

[1] A. K. Pathan, H. W. Lee, and C. S. Hong," Security in wireless sensor network: issues and challenges," In proceeding of the 8th ICACT 06,Volume 2, Phoenix Park, Korea, pp. 1043-1048,February, 2006.

[2] Abhishek Panday, R. C. Tripathi, "A Survey on Wireless Sensor Network Security" International Journal of Computer Application(0975-8887) Volume 3- No.2, June 2010

[3] James Newsome et al "The Sybil Attack in Sensor Networks: Analysis & Defenses" IPSN'04, April 26–27, 2004, Berkeley, California, USA.

[4] B. Yu, B. Xiao. "Detecting selective forwarding attacks in wireless sensor networks" in *Proceedings of the 20th International Parallel and Distributed Processing Symposium (SSN2006 workshop)*,. Rhodes, Greece, pp. 18, April 2006.

[5] Jaydip Sen "Routing Security Issues in Wireless Sensor Networks: Attacks and Defenses" *Innovation Lab, Tata Consultancy Services Ltd. India* Pages.280-306

[6] Y. W. Law and P. Havinga. How to secure a wireless sensor network. Pages 89–95, Dec. 2005.

[7] Y.-C. Hu and A. Perrig, "A Survey of Secure Wireless Ad Hoc Routing," *IEEE Security & Privacy Special Issue: Making Wireless Work*, vol. 2, no. 3, May/June 2004, pp. 28–39.

**Atul Yadav** I have done B.E. from Electronics & Telecommunication Department of RMCET Devrukh (Ambav) India in 2007. Presently I am pursuing M. E. from Shivaji University. I am working as Lecturer in Information Technology Department of RMCET Devrukh (Ambav).

**Mangesh Gosavi** I have done B.E. from Computer Deparment of Bharati Vidyapeeth Kolhapur India in 2009. I am working as Lecturer in Computer Department of RMCET Devrukh (Ambav).

**Parag Joshi** I have done B.E. from Electronics & Telecommunication Department of RMCET Devrukh (Ambav) India in 2007. Presently II am pursuing M. Tech. from COEP Pune.