Attacks and Countermeasures on Routing Protocols in Wireless Sensor Networks: A Survey

E. Jyothi Kiranmayi[1], N.V. Rao[2], K.S. Nayanathara[3]

[1] CVR College of Engineering, IT Department, Hyderabad, India
Email: jyothikiran_2121@yahoo.com
[2]CVR College of Engineering, CSE Department, Hyderabad, India
Email: nvr@ieee.org
[3]CVR College of Engineering, ECE Department, Hyderabad, India
Email: ksattiirajunayanathara@gmail.com

Abstract - **Security in Wireless Sensor Networks has become one of the most relevant research topics. Designing a secure routing protocol in a wireless sensor network is a challenging task because of the limitations on memory, computational and communication capabilities, bandwidth and energy of the sensor nodes. Most of the routing protocols that were proposed were designed by keeping efficiency of energy in view but not security. Routing protocols in wireless sensor networks are susceptible to various types of attacks such as hello flood attack, Sybil attack, sink hole attack, worm hole attack, selective forwarding attack, eavesdropping, acknowledgment spoofing, routing table overflow and so on. In this paper we discuss different types of attacks on routing protocols in detail and also some of the defensive techniques proposed in literature to counter the attacks.**

Index Terms - **Wireless sensor network, Routing protocols, attacks, countermeasures**

I. INTRODUCTION

A Wireless Sensor Network (WSN) is a spatially distributed heterogeneous system consisting of one or more base stations and low-powered, low-cost tiny sensor nodes(SNs) capable of sensing, detecting, and monitoring the physical attributes of the environment like pressure, temperature, sound, vibration, acceleration, velocity, humidity, stress, strain and so on. WSNs were initially introduced for military applications, over time the range of applications has been increasingly diversified ranging from defense to general security.

The main task of a sensor node is to sense the data from the environment and communicate it to the base station. The components and the functionality of a sensor node are shown in Table I.

Table I Components of a sensor node

Component	Functionality
Micro-controller	Controls the functionality of other components and processes the data
Transceiver	Transmits and receives signals
External Memory	Stores application related data
Battery	Source of energy

Wireless Sensor Network uses wireless communication for data transmission. As its transmission range is limited, a sensor node cannot transmit the sensed data directly to the base station. Hence sensor node transmits the data through multiple intermediate nodes in which routing protocols play a significant role.

Routing protocols in WSNs are broadly classified into two types based on network structure and protocol operation. Figure 1 shows further classification of network structure and protocol operation based routing protocols [1]. The routing protocols that were designed for WSNs were developed by keeping energy constraints in mind in order to prolong WSN lifetime, but security did not get its due share of consideration.

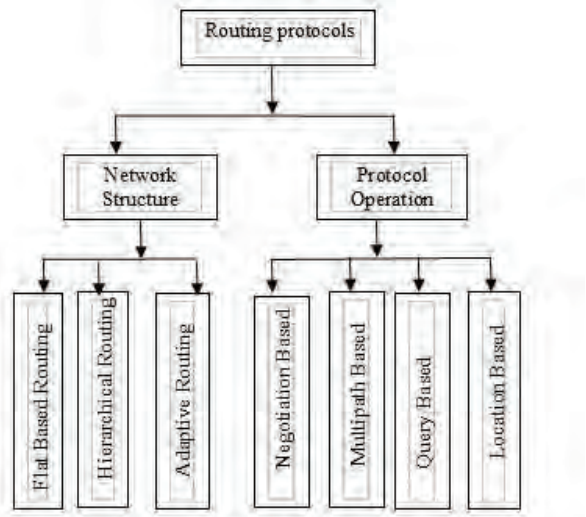

Figure 1. Classification of Routing Protocols in Wireless Sensor Networks

Routing protocols in Wireless Sensor Networks are exposed to various types of attacks. This paper discusses attacks and some of the defensive techniques reported in literature.

The paper is organized as follows: Various types of attacks on routing protocols are presented in detail in Section II. Defensive techniques for some of the attacks are discussed in Section III.

The paper is organized as follows: Various types of attacks on routing protocols are presented in detail in

DOI: 10.32377/cvrjst1018

Section II. Defensive techniques for some of the attacks are discussed in Section III.

II. Attacks on Routing Protocols

Nodes in WSN are vulnerable to physical attacks as the environment in which they are deployed is open, never or rarely attended and harsh and makes them susceptible to various types of attacks. Attacks in general can be external or internal. External attack on routing protocols aims at the following: introduce wrong routing information, replay old routing information, misinterpret the information resulting in partition or overload the network with increasing frequency of retransmission and also using inefficient routing. Internal attacks are highly detrimental and also not easily detectable. The following are different types of attacks on routing protocols in Wireless Sensor Networks:

- Spoofed/alter, replay routing information[8]
- Eavesdropping
- Hello Flood Attack[9]
- Selective Forwarding Attack[10]
- Sink Hole Attack[2]
- Worm Hole Attack[12]
- Sybil Attack[13]
- Acknowledgment Spoofing[14]
- Node Capture Attack

A. *Spoofed/alter/replay routing information*

In this attack an adversary passively captures the routing information that is being transmitted, spoofs/alters or replays the routing information which may create routing loops, convey false routing information, partition the network and so on.

B. *Eavesdropping*

This is an attack on the confidentiality of the data that is being transmitted. In this attack an adversary monitors the data without interrupting the normal operation of the network. An adversary can even launch traffic analysis by observing the traffic in the network.

C. *Hello Flood Attack*

In this attack, during the neighbor discovery phase an adversary transmits a "Hello" message with strong transmission power. The malicious node convinces the other nodes that the attacker is its neighbor, so all the nodes mark the attacker as its parent node. When the nodes in the network send data to the adversary, data is actually transmitted to the oblivion because the adversary is far away.

D. *Selective Forwarding Attack*

In selective forwarding a malicious node acts like a normal node, rejects to forward all the packets and selectively drops the packets carrying sensitive information.

Sensor node -

Malicious Node -

Base Station -

Packet -

Routing Path -

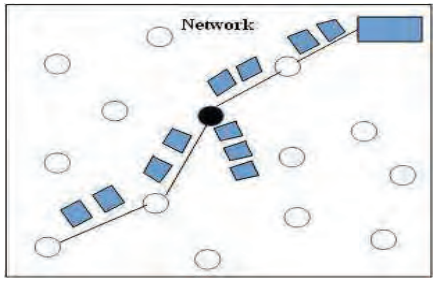

Figure 2. Illustration of Selective Forwarding Attack

E. *Sink Hole Attack*

With respect to routing metrics, a malicious node attracts its neighboring nodes and draws as much traffic as possible, and then the attacker may drop or modify the received packets or sometimes severe attacks like selective forwarding may be launched.

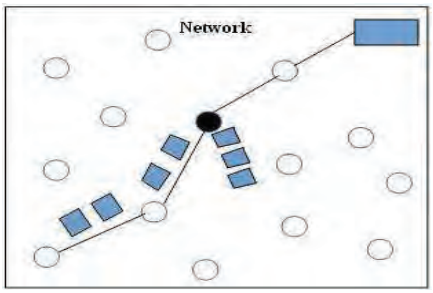

Figure 3. Illustration of Sink Hole Attack

F. *Worm Hole Attack*

In this attack two adversaries cooperate with each other, collect information at one location and replay from another location of the network.

G. *Sybil Attack*

In Sybil attack, a malicious node illegitimately claims multiple identities to represent multiple nodes in the network. In Figure 4 below, a malicious node claims different identities (A, B, C) with its neighbors.

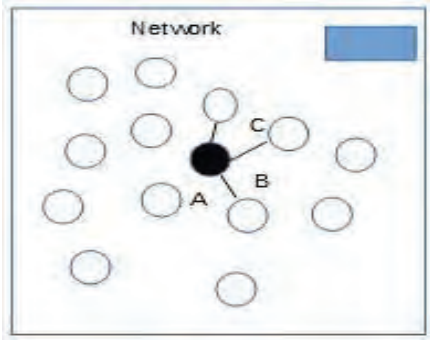

Figure 4. Illustration of Sybil attack

H. Acknowledgment Spoofing

In this attack, an adversary spoofs/forges the ACK packet. As a result, a weak link is assumed to be strong and a dead node as alive. Packets transmitted through these links may be lost or corrupted.

I. Node Capture Attack

As sensor networks are deployed in harsh and unattended environment, sensor nodes lack physical security. Hence an adversary may capture the sensor node and compromise not only sensitive data but also the key material used for security.

III. DEFENSIVE TECHNIQUES

This section discusses some of the defensive techniques proposed in literature to address the above mentioned attacks.

A. Selective Forwarding Attack

Selective Forwarding is an active and internal attack. In selective forwarding attack malicious nodes behaves like normal nodes but selectively drop data packets carrying sensitive data which destroy the entire monitoring system. Black hole is a special type of selective forwarding attack in which adversary rejects to forward all the packets. The defensive techniques proposed in literature for addressing selective forwarding attack are:

Multi Data flow Topologies

Multi Data Flow topologies (MDT) is one of the defensive techniques proposed in [3] to address selective forwarding attack. In the proposed MDT scheme before deployment the entire network is divided into different groups with overlapping regions. Each group belongs to one data flow topology. After deployment multi data flow topologies are built. Each node belongs to one data flow topologies and can communicate only with the nodes belonging to the same topology. If a malicious node belonging to one topology drops the packet, the base station still receives the dropped packets from other data flow topology because the monitoring area is overlapped. MDT scheme is simple and efficient, besides addressing selective forwarding attack it is also resistant to jamming attacks and there is no need to resend the dropped packets as the base station receives the dropped packets.

Yu and Xia [4] proposed a defensive scheme based on ACK packets. On the path of data transmission selected, intermediate nodes transmit ACK packets. With the ACK packets source node can easily identify the malicious nodes. The scheme is simple but the major drawback is the additional overhead associated with each node. Besides sensing and forwarding, the nodes must transmit ACK packets and are also responsible for identifying malicious nodes. The lost packets must be resent by the source node.

B. Worm Hole Attack

In worm hole attack two adversaries cooperate with each other, collect information at one location and replay from another location of the network. The defensive techniques proposed in the literature are:

Directional Antennas

Hu and Evas [5] proposed use of directional antennas to counter worm hole attack. In the proposed scheme every node is equipped with a directional antenna which examines the direction of received signal from the neighbor nodes with a shared witness. The relationship with the neighbors is confirmed only when the directions match. The main drawback in this scheme is that every node must be equipped with a special hardware component called directional antenna, which may not be a promising approach.

Packet Leashes

Hu et al. [6] proposed Packet Leashes for detecting and protecting the network from wormhole attack. Two types of packet leashes were proposed: geographic and temporal leashes. In case of geographic leashes geographic location of each node or a fixed clock synchronization between nodes is required. Geographic leash ensures that the packet travels up to a certain distance from the sender. In temporal leash every packet has a life time which strictly controls the maximum distance traveled by the packet. The drawbacks are either fixed clock synchronization between nodes and that information about the location of each node is required.

In [16] authors have presented an attack specific secure routing protocol specially designed to address worm hole attack. Neighbor discovery, initial route discovery, worm hole detection during data dissemination phase and finally discover a secure route against a worm hole attack are the four phases of this protocol.

C. Sybil Attack

In Sybil attack malicious node illegitimately claims multiple identities by stealing or fabricating identities of legitimate nodes. In [7] various defensive techniques to address Sybil attack are proposed.

Random Key Pre-Distribution

In literature researchers have proposed many random key pre-distribution schemes to establish secure links between the nodes. By using key distribution schemes Sybil attack can be addressed.

Position Verification

Another defensive technique to prevent Sybil attack is position verification. In this approach the network identifies the physical location of each node, with which malicious nodes claiming multiple identities can be identified. But automatic location detection is still an open research problem. This solution suits static networks rather than dynamic networks or networks with mobile nodes.

Code Attestation

The code running on a malicious node must be different from that of the code running on legitimate node.

DOI: 10.32377/cvrjst1018

By verifying the memory content i.e. the code, malicious nodes can be easily identified. But this approach is expensive.

Registration

By registering the identities of the sensor nodes in the network to the trusted central authority (i.e the base station) sensor networks can prevent Sybil nodes. But the drawback is that the list of registered nodes and the deployment information must be securely maintained and protected from being maliciously modified.

D. Sink Hole

Sink hole is an internal attack in which a malicious node convinces the neighboring nodes by advertising single-hop, high quality path to the destination and attracts the traffic as much as possible, and the packets destined to the base station are dropped or modified by the sink hole node.

In [12] authors have proposed an attack-specific secure routing protocol. The proposed protocol uses redundancy based mechanism to address sink hole attack. In this protocol the messages are sent to the suspicious nodes through multiple paths, the attacked nodes are confirmed by evaluating the replies comprehensively.

E. Eavesdropping

Eavesdropping is a passive attack in which the adversary just monitors the data being transmitted between the source and destination without disturbing the normal operation. The countermeasure is encryption. But choosing a light weight and strong encryption algorithm is a challenging task in Wireless Sensor Networks because of the limited resources. Many secure routing protocols are proposed in literature [13, 14, 15]. The protocols provide confidentiality for the data that is being transmitted and protect the data from eavesdropping.

F. Replay

Replay is an active attack in which the adversary passively captures data or the routing information and subsequently replays it to create an unauthorized effect. The counter measure is to include a field in the packet so that the packet can be uniquely identified, like sequence number or time stamp or a nonce.

TABLE II

Summary of Attacks and Countermeasures

ATTACKS	COUNTERMEASURES
Eavesdropping	Encryption
Selective Forwarding	Multi Data flow Topologies, Acknowledgment
Worm Hole Attack	Directional Antennas, Packet Leashes, Authentication
Sybil Attack	Authentication, Random Pre-key distribution, Position verification, Code attestation, Registration
Sink Hole Attack	Authentication, Redundancy based mechanism
Hello Flood Attack	Authentication

IV. CONCLUSIONS

In this paper security issues relating to the routing protocols in Wireless Sensor Networks have been discussed in detail. Defensive techniques proposed in literature have been presented. Based on the survey it is found that there is a need to design a secure routing protocol which can provide basic security services like confidentiality, authentication, integrity and availability, addressing all the known types of attacks.

REFERENCES

[1] Carlos De Morais Cordeiro, Dharma Prakash Agrawal," Ad Hoc and Sensor Networks: Theory and Applications", 2nd Edition, World Scientific, 2006.

[2] C. Karlof and D. Wanger, "Secure Routing in wireless Sensor Networks: Attacks and countermeasures," Ad Hoc Networks, 1(2-3), Vol. 1, pp. 293-315, Sep. 2003.

[3] Hung-Min Sun, Chien-Ming Chen and Ying-chu Hsiao, "An efficient counter measure to the selective forwarding attack in wireless sensor networks," in IEEE TECON 2007, pp. 1-4.

[4] B. Yu and B. Xia, "Detecting selective forwarding attack in wireless sensor networks," in Proceedings of the 20th IEEE International Symposium on parallel and distributed processing, April 2006.

[5] L.Hu, D. Evas, "Using Directional Antennas To prevent Wormhole Attacks", in Proceedings of the IEEE Symposium on Network and Distributed System Security (NDSS) 2004.

[6] Yih-chun Hu, Adrian perrig, David B Johnson, "Packet Leashes: A Defensive Against Wormhole Attack in Wireless Sensor Networks and Ad Hoc Networks, in proceedings of the twenty second Annual Joint Conference of the IEEE Computer and Communication Societies (INFOCOM 2003), *IEEE San Fransisco*, CA, 2003.

[7] James Newsome, Elaine Shi, Dawn Song, Adrian Perrig, "The Sybil Attack in Sensor Networks: Analysis and Defenses", in IPSN' 04 proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, pp. 259- 268 , ACM, 2004.

[8] C. Gupta, K. Gupta, and V. Gupta, "Security threats in sensor network and their possible solutions," in Proceedings of the International Symposium on Instrumentation and Measurement, Sensor Networks, and Automation (IMSNA '12), pp. 25–28, Sanya, China, August 2012.

[9] W. Z. Khan, Y. Xiang, and M. Y. Aalsalem, "Comprehensive study of selective forwarding attack in wireless sensor networks," International Journal on Computer Network and Information Security, vol.1, pp.1–10, 2011.

[10] Y. C. Hu and A. Perrig, "Wormhole attacks in wireless networks," IEEE Journal on Selected Areas in Communications, vol. 24, no.2, pp.370–380, Feb. 2006.

[11] M. Healy, T. Newe, and E. Lewis, "Security for wireless sensor networks: a review," in Proceedings of IEEE Sensors Applications Symposium (SAS '09), pp. 80–85, New Orleans, La, USA, February 2009.

[12] Fang-Jiao Zhang, Li-Dong Zhai, Jin-Cui Yang, Xiang Cui, "Sinkhole attack detection based on redundancy mechanism in wireless sensor networks", in 2nd International Conference of Information Technology and Quantitative Management, ITQM 2014, Vol. 13, pp. 711-720, Elseiver 2014.

[13] D.P.S.Edvine Christins, R. Jothi Chitra, "Energy Efficient Secure routing in Wireless Sensor Networks", in IEEE ICETECT 2011, pp. 982-986.

[14] Li Wei, Chen Ming, Li Minming, "Information Security Routing Protocol in the WSN", in IEEE IAS'09 ,Vol. 2, pp. 651-666, 2009.

[15] Suraj Kumar, Sanjay jane "SCRMP: Secure Cluster Based Multipath Routing Protocol for Wireless sensor Networks", Sixth International Conference on Wireless Sensor Networks(WCSN), pp. 1-6, IEEE , Dec. 2010.

[16] Sanjay Madria, Jian Yin, "SERWA: A Secure Routing Protocol against wormhole attacks in Sensor Networks", Elsevier, Ad Hoc Networks, Vol.7, pp.1051-1063, August 2009.

 DOI: 10.32377/cvrjst1018