Different Approaches to Mitigate Selective Forwarding Attacks in WSN

Jaspreet Singh
Department of Computer Science Engineering,
RIMT IET, Punjab, India

Anuj Gupta
Head, Department of Computer Science Engineering,
RIMT IET, Punjab, India

Abstract: Wireless Sensor Networks (WSN) are being increasingly used due to their wide range of applications in military and civilian domains. These networks are prone to security attacks. Some of the inherent features like limited battery and low memory make sensor networks infeasible to use conventional solutions of security, which needs complex calculations and more memory. There are many types of attacks on these networks that can be classified as routing attacks and data traffic attacks. In sensor nodes some of the data attacks are black hole, wormhole and selective forwarding attack. Black hole attack is that in which compromised node usually drops all the packets being forwarded through it. A special type of black hole attack is selective forwarding attack, in which compromised node drops packets selectively, which may decrease the network efficiency. In this paper, we will discuss about selective forwarding attack and some of the mitigation techniques to defend this attack. Selective forwarding attacks can corrupt some very critical applications. In these types of attacks, malicious nodes behave like normal nodes in most time but selectively drop sensitive packets.

Keywords: Wireless Sensor Network, Security, Selective Forwarding Attack, Sensor Network.

I. INTRODUCTION

WSN is being emerged as a promising and interesting area. It is designed for real-time data collection and analysis of data in hostile environments so they used mainly in monitoring and surveillance based applications. Most widely used applications of WSN are military appliance, area monitoring, environmental monitoring, industrial monitoring, machine health monitoring, water/waste water monitoring, fleet monitoring. Since, WSNs are mostly used in a hostile environment security is mainly concerned. The conventional security measures are not suitable to the wireless sensor networks due to resource constraints of both memory and energy. In WSN, sensor nodes use wireless communication to send packets. A sensor node uses multi-hop transmission to deliver the packet to the base station, due to its limited transmission range. so a packet is forwarded through too many hops/nodes to reach the destination. As, we discussed sensor networks are usually deployed in hostile environments, an adversary can launch attacks. Attacks can be classified into two types, inside attacks and outside attacks. The latter one can be easily detected and security solutions are provided. In former one, adversary compromises some internal nodes and launches attacks which will be difficult to detect. One kind of such attack is Selective Forwarding.

In Selective Forwarding Attack, internal nodes that are compromised selectively drops/forwards some of the packets passing through them. If any node drops all the packets, then it becomes black hole attack. Therefore, selective forwarding attack is sometimes called as a special case of black hole attack.

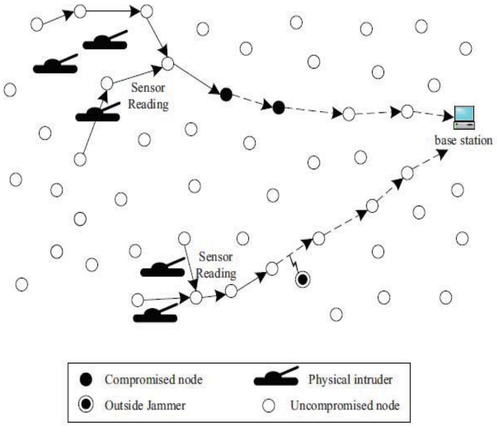

Figure 1. An example sensor network under selective forwarding attacks.

Selective forwarding attack is hard to detect, since the wireless communications are unreliable because there is a loss of data packets due to noise also. In some cases, sensor nodes go into sleep state (mode) to save power and they are not able to send and receive data in this period. So, we have to be examine carefully whether the packet drop is due to selective forwarding or any other reason.

In this paper, we have discussed about selective forwarding attacks, their types and some countermeasure techniques.

II. ATTACKS AND THEIR CLASSIFICATION

To secure wireless sensor networks, it has to satisfy all the security properties like integrity, confidentiality, availability and authenticity. Let us briefly discuss some of the security attacks.

A. Selective Forwarding

In selective forwarding attacks malicious nodes behaves like black hole and refuse to forward some messages and simply drop them and ensure that they are not propagate further. Such an attacker runs the risks that neighbouring nodes will conclude that they have failed and decide to seek another route. A more refined form of this attack is when an adversary selectively forwards some packets. An adversary interested in suppressing or modifying packets originating from a few selected nodes can constantly forward the remaining traffic and limit suspicion of its wrongdoing.

B. Wormhole

In the wormhole attacks, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. An adversarial node situated close to the base station can completely disrupt routing by creating a wormhole. An adversarial node can convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a node like sinkhole since the adversarial node on the other side of the wormhole can artificially provide a high-quality route to the base station. Thus potentially all the traffic in the surrounding area will be drawn through it if alternate routes are significantly less attractive.

C. Acknowledgement Spoofing

Many sensor network routing algorithms rely on implicit or explicit link layer acknowledgements or acceptance messages. Because of the inherent broadcast medium, sometimes an adversary can spoof link layer acknowledgments for “overheard” packets that are addressed to neighbouring nodes. Its goal is to convince the sender node that a weak link is strong or that a disabled or dead node is alive.

D. Impersonation

Node Replication is also called Multiple Identity or Impersonation. An attacker node seeks to add a node to an existing sensor network by replicating or copying the node ID of an existing node. These types of attacks can occur if an adversary can copy the network node's ID. In this way packets could be corrupted, deleted or misrouted and if this attacker could perform its replication it is possible that cryptographic keys could be disclosed.

E. Eavesdropping or monitoring.

The attacker could easily discover the communication contents by listening to the data. Network traffic is also susceptible to eavesdropping and monitoring. This can be avoided if there is a robust security protocol, but monitoring could lead to similar type of attacks that are previously described. It could also lead to black hole or wormhole attacks.

F. Traffic Analysis

Traffic analysis attacks are mostly forged where the base station is determinable by observation that the majority of packets are being routed to one particular node. If an attacker node can compromise the base station network then it can leave the network useless.

III. CLASSIFICATION OF SCHEMES AGAINST SELECTIVE FORWARDING DETECTION

The schemes for defending against selective forwarding attack can be classified according to two types of criteria i.e. defence of scheme and nature of scheme. Defence of scheme can again be classified into two classes, detection based and prevention based. The nature of scheme can be classified into two classes i.e. centralized and distributed.

A. Distributed and Centralized

In Distributed based schemes, both sensor node and base stations are responsible for prevention and detection of malicious nodes and selective forwarding attack. While in centralized based schemes only cluster head or base station are responsible for countering the selective forwarding attack.

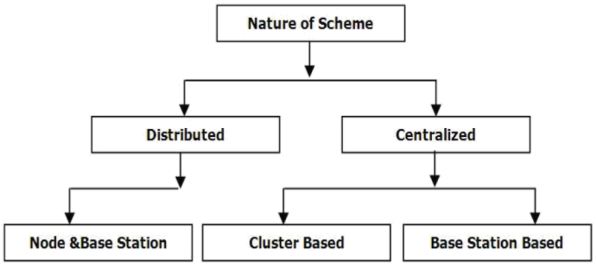

Figure 2. Classification by nature of schemes

B. Detection and Preventions:

Detection based schemes detect malicious node or the attack or both. On other hand the prevention based schemes only ignores or by pass the malicious node and are not capable of detecting the malicious nodes and attack.

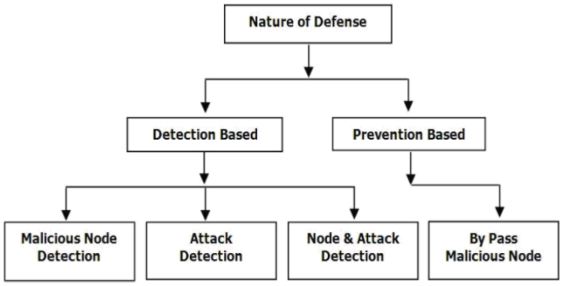

Figure 3. Classification by defense of schemes

IV. SCHEMES AGAINST SELECTIVE FORWARDING DETECTION AND COUNTERMEASURES

A broad overview of the existing techniques and schemes in opposition to selective forwarding attack is described below.

A . Secure routing in wireless sensor networks:

Karlof et al. [1] first time discuss the selective forwarding attack and to counter these types of attacks he suggest that Multi-path routing can be used. Messages routed over n paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most n compromised nodes and still offer some probabilistic protection when over n nodes are compromised. The use of multiple braided paths may provide probabilistic protection against selective forwarding and only localized information is used. It Allows nodes to dynamically choose a packet's next hop by using probability from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow.

Draw Backs of Scheme:

1. Poor Security Resilience if there exists at least one node in the path.

2. No detection of malicious node and no notification about attack to neighbours.

3. Increase in energy consumption when the number of paths increases.

4. Increase in Network flow and communication overheads.

5. No implementation of specific method for detection of attack and attacker.

B. Using multi hop acknowledgements from intermediate nodes:

Yu and Xiao [2] have proposed a distributed detection scheme that uses multi hop acknowledgements from intermediate nodes to raise alarms in the network. This scheme focuses on selective forwarding attack in which detection occurs in both the base station and source nodes.

In this scheme, each intermediate node along the forwarding path is in charge of detecting malicious nodes. If an intermediate node detects the misbehavior of its downstream (upstream) nodes, it will generate an alarm packet and deliver it to the source node (the base station) through multiple hops. The base station and the source node can then use more complicated IDS (Intrusion Detection System) algorithms to make decisions and responses.

Draw Backs of Scheme:

1. The nodes may involve more multi-hop response acknowledgements to detect selective forwarding attack, and choose another path to retransmit the packet successfully resulting in certain delay and communication overhead.
2. Lack of efficiency. Sensor nodes in this scheme take much effort to detect the selective forwarding attack.

3. Security problem. This scheme cannot detect the attack successfully in some particular condition.

4. Lack of scalability. This scheme only considers the selective forwarding attack. Hence, WSN needs other countermeasures if suffering other kinds of attacks.

5. The members of a checkpoint list (acknowledge node) are predictable, thus making part of the intermediate nodes the target of compromising.

C . Checkpoint-based multi-hop acknowledgement:

Xiao, Yu and Gao [3] have proposed a technique for identifying suspect nodes in selective forwarding attack. They have actually improved their previous technique for detection of selective forwarding attack i.e. checkpoint-based multi-hop acknowledgement scheme. In this scheme they randomly select part of intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgements for each packet received. In addition to this, for ensuring the authenticity of packets each node needs a one-way hash key chain. To send current one-way hash key Delay mechanisms are also developed. Each intermediate node in a forwarding path has the potential to detect abnormal packet loss and identify suspect nodes if it does not receive enough acknowledgements from the downstream checkpoint nodes.

Draw Backs of scheme:

1. By using one-way hash key chains for authentication for each packet requires storage space.

2. Alert packets include one-way hash key, therefore more energy is consumed by sending acknowledgement.

3. No guarantee for reliable transmission of packet in case of packet dropping.

4. It requires nodes to be loosely time synchronized

D. multi-dataflow topologies (MDT) method:

Hung-Min Sun et al [4] have proposed a multi-dataflow topologies (MDT) method to countermeasure the selective forwarding attacks. In this scheme, the authors divided the sensor nodes into two-dataflow topologies, both dataflow topologies can cover the area to be monitored. Therefore the base station only requires one report from either topology for the entire network to be controlled. Using two topologies the base station can defend against the selective forwarding attack. If in one topology a malicious node exists the base station can still receive packets from other topology. The authors deployed the sensor nodes region by region during the deployment phase for locating a malicious node. Sensor nodes may locate in a range of some regions. Base station will mark all possible regions that the malicious sensor nodes may be deployed in, if it loses some packets. After that, the base station can gather and analyze the information about all possible lost regions; hence the base station can utilize the information to locate the malicious sensor nodes.

Draw Backs of scheme:

1. When there is a malicious node in each path, the attacker can completely destroy data transmission. Thus communication overhead is also not improved. This scheme’s ability to resist the attacks is very limited.

2. Scheme cannot identify compromised nodes efficiently and there is an increased communication overhead since it sends duplicate packets.

E . Using Two-hop Neighbour Knowledge:

Tran Hoang et al [5] have proposed a centralized cluster based lightweight detection technique to detect selective forwarding attack and its different types in Wireless Sensor Networks. His scheme is based on two-hop neighbourhood information only and over-hearing technique. In this scheme, each sensor node is equipped with a detection module that works on application layer. Detection module passively detects the selective forwarding attack in its neighbouring node. This detection method relies on the sensor communication’s broadcast nature and takes advantage of high density of sensors deployed in the sensed environment. . The sensor nodes activate the detection module called monitor nodes module. This also uses two-hop neighbour knowledge as a part of its detection technique and two-hop neighbour list is stores by each node. Each neighbour node is associated with a malicious counter that can be defined as the threshold of abnormal activity of a sensor node which cannot exceed by some assumed value. When malicious counter crosses the threshold value, the malicious node is detached from its direct neighbour list.

Draw Backs of Scheme:

1. No way out is proposed if the monitoring node or cluster head is compromised.

2. In case of change in topology, the scheme does not work because the topology is assumed to be static.

3. No countermeasures are taken for selective forwarding attack and reliable data retransmission is not assured.

F . Lightweight Defence Scheme

Wang Xin-sheng et al [7] have presented a distributed lightweight defence scheme against selective forwarding attacks. This scheme is based on a hexagonal Wireless Sensor Networks mesh topology. This scheme utilizes the neighbour nodes to monitor the transmissions of the event packet and detect the selective forwarding attack by monitoring packet forwarding of the two nodes in the transmission path. It resend these packets dropped by the attackers to the destination node. To send an event packet from source to destination, the route is calculated by The routing algorithm (OPA_uvwts). The intermediate node is responsible for forwarding the event packet. The node that is assigned as monitor node is responsible for the detection of selective forwarding attack and if selective forwarding attack is identified, the event packet is retransmitted to the destination node by monitor node and finally when selective forwarding attack is detected, it sends an alarming message to its neighbour nodes thus notify the location of attacker thus avoiding the attacker node in forwarding the incoming packets.

Draw Backs of Scheme:

1. If there is any change in topology, performance of scheme as will be affected as it is assumed that nodes will not change their location.

2. No countermeasure is proposed if in case the monitoring node is compromised**.**

G. A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks

Guorui Li et al [9] have proposed the sequential mesh test based selective forwarding attack detection scheme in WSN. This scheme's nature is centralized and it works for cluster based sensor networks. The sensor node sends the packet drop report message through another path to the cluster head if it doesn't observe the forwarding data message from the next hop sensor node in a fixed interval. The cluster head runs the sequential mesh test based detection scheme against the suspicious node after receiving the packet drop reports. Instead of regulating the total times of test in advance, the sequential mesh test extracts a small quantity of samples to run the test. This is how it is decided whether to continue the test or not based on the test result until it obtains the final conclusion.

Draw Backs of Scheme:

1. Although the detection of selective forwarding attack depends upon the ratio of packet drop but this detection is not accurate (not satisfy able) because when the attack package drop rate is lower than the normal package drop rate. This is because the normal package drop events have severe influence on the selective forwarding attack detection.

2. The scheme also suffers when the cluster head is comprised as there is no countermeasure given for this. The scheme also suffers from single node failure problem.

H. Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks

Suk-bok et al [10] have proposed a resilient packet-forwarding scheme. This scheme uses Neighbour Watch System (NWS) against maliciously packet-dropping nodes in sensor networks. This scheme consumes less power than multi-path schemes because it employs single-path data forwarding. The packet is forwarded along the single-path towards the base station. The scheme uses multi-path data forwarding at the location where Neighbour Watch System detects relaying node's misbehaviour. In this, the watch node around a malicious node can find that the malicious node do not transmit the received packet to other nodes or transmit to a node that does not exist in its neighbour list and then the watch node must retransmit the package. This scheme is based on LEAP protocols.

Draw Backs of Scheme:

1. As, it is necessary that each node broadcasts its neighbour's table and then stores the neighbour's table of its neighbour's, which consumes more space for storage. Moreover, the watch nodes need to store more packets around them for potential retransmit, which requires large buffer and more energy consumption.

V. Conclusion

Secure and on time transmission of packets is the basic need in wireless sensor network. One of the attacks, that violates this need is Selective Forwarding attack. In this attack, a malicious node is dropping packets which make information unavailable. Here we have discussed some of the mitigation schemes to defend this attack and had given analysis on every scheme. This analysis will help us to know the drawbacks in the previous schemes and may helpful to overcome the drawbacks in the future

ACKNOWLEDGEMENTS

We wish to thank the editors and reviewers for their valuable suggestions and expert comments that help improve the quality as well as quantity of the paper.

REFERENCES

[1] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: attacks and countermeasures,” in Ad Hoc Networks, Vol. 1, No. 2, 2003, pp. 293-315.

[2] B. Yu and B. Xiao, “Detecting selective forwarding attacks in wireless sensor networks,” in *Proc. of the 2nd International Workshop on Security in Systems and Networks*, April 2006, pp. 1-8.

[3] B. Yu and B. Xiao, “CHEMAS: identify suspect nodes in selective forwarding attacks,” in *Journal of Parallel and Distributed Computing*, *Vol.* 67, *No.* 11, 2007, pp. 1218-1230.

[4] H. Sun, C. Chen and Y. Hsiao, “An efficient countermeasure to the selective forwarding attack in wireless sensor networks,” in *Proc. Of IEEE TENCON 2007*, Oct. 2007, pp. 1-4.

[5] Tran Hoang Hai, Eui-Nam Huh, “Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbour Knowledge” Seventh IEEE International Symposium on Network Computing and Applications, 2008, pp.325-331.

[6] G.Padmavathi, D.Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks” international Journal of Computer Security, Vol. 4, No. 1 & 2, pp. 117-125, 2009

[7] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, Wang Liang-min, “Lightweight Defence Scheme against Selective Forwarding Attacks in Wireless Sensor Networks‟ pp.226-232, IEEE, 2009.

[8] Yenumula B Reddy, S. Srivathsan ,“Game Theory Model for Selective Forward Attacks in Wireless Sensor Networks” 17th Mediterranean Conference on Control & Automation Makedonia Palace, Thessaloniki, Greece June 24 - 26, 2009, pp. 458-463

[9] Guorui Li, Xiangdong Liu, and Cuirong Wang, “A Sequential Mesh Test based Selective Forwarding Attack Detection Scheme in Wireless Sensor Networks”, pp.554-558, 2010.

[10] S.-B. Lee and Y.-H. Choi, A Resilient Packet-Forwarding Scheme against Maliciously Packet-Dropping Nodes in Sensor Networks, In Proceedings of the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks(SASN‟06), pp. 59-70, 2006.