A Survey On Selective Forwarding Attack in Wireless Sensor Networks

Leela Krishna Bysani
Dept. of Computer Science and Engg.
National Institute of Technology Rourkela
Rourkela India-769008
Email: leelakrishnabysani@gmail.com

Ashok Kumar Turuk
Dept. of Computer Science and Engg.
National Institute of Technology Rourkela
Rourkela India-769008
Email: akturuk@nitrkl.ac.in

***Abstract*—Wireless Sensor Network(WSN) is being emerged as a prevailing technology in future due to its wide range of applications in military and civilian domains. These networks are easily prone to security attacks, since once deployed these networks are unattended and unprotected. Some of the inherent features like limited battery and low memory makes sensor networks infeasible to use conventional security solutions, which needs complex computations and high memory. There are lot of attacks on these networks which can be classified as routing attacks and data traffic attacks. Some of the data attacks in sensor nodes are wormhole, black hole and selective forwarding attack. In a black hole attack, compromised node drops all the packets forwarding through it. A special case of black hole attack is selective forwarding attack, where compromised node drops packets selectively, which may deteriorate the network efficiency. In this paper, we discussed about selective forwarding attack and some of the mitigation schemes to defend this attack.**

***Index Terms*—Wireless Sensor Network, Selective Forwarding, Downstream.**

I. Introduction

In recent days, WSN is emerging as a promising and interesting area. WSN is mostly designed for real-time data collection and analysis of data in hostile environments which makes them to be used mainly in monitoring and surveillance applications. Most popular applications are military appliance, area monitoring, environmental monitoring(example: bush fire monitoring), industrial monitoring, machine health monitoring, water/waste water monitoring, fleet monitoring. Since, WSNs are mostly deployed in a hostile environment security is mainly concerned. The conventional security measures are not suitable to this wireless sensor networks due to resource constraints of both energy and memory. In WSN, sensor nodes use wireless communication to send packets. Due to limited transmission range, a sensor node uses multi-hop transmission to deliver the packet to a base station. Hence a packet is forwarded through so 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, the compromised internal nodes selectively drops/forwards some of the packets passing through them. If node drops all the packets, then it becomes black hole attack. So, selective forwarding attack can be called as a special case of black hole attack. The selective forwarding attack is difficult to detect, since the wireless communications are unreliable, where there is a loss of data packets due to noise. In some cases, sensor nodes goes into sleep state to save power and they cant send and receive data in this period. So, we have to be careful whether the packet drop is due to selective forwarding or any other reason.

In this paper, we have discussed about selective forwarding attack, its types and some countermeasure schemes. The rest of the paper is organized as follows. In section 2, we discussed some of the attacks in sensor networks. In section 3, we discussed about selective forwarding attack and classified it.Section 4 goes through some of the detection schemes and how they defend this attack. Section 5 concludes it.

II. Attacks and their Classification

To secure wireless sensor network, it has to satisfy all the security properties like integrity, confidentiality, availability and authenticity. Before discussing selective forwarding attack, let us discuss some of the security attacks[2]

A. Selective Forwarding

In a selective forwarding attack[3], [4], malicious nodes behaves like black hole and may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. However, such an attacker runs the risks that neighboring nodes will conclude that she has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a few selected nodes can reliably forward the remaining traffic and limit suspicion of her wrongdoing.

B. Wormhole

In the wormhole attack[1], an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. An adversary situated close to a base station may be able to completely disrupt

978-1-4244-9190-2/11/$26.00 ©2011 IEEE

routing by creating a well-placed wormhole. An adversary could 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 sinkhole: since the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive.

C. Sybil

Sybil attack[8] is defined as a ”malicious device illegitimately taking on multiple identities”. Using the Sybil attack, an adversary can ”be in more than one place at once” as a single node presents multiple identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage, dispersity and multi path. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of neighboring nodes uses a unique key to initialize frequency hopping or spread spectrum communication. Sybil attacks also pose a significant threat to geographic routing protocols.

D. Acknowledgement Spoofing

Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements[8]. Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for ”overheard” packets addressed to neighboring nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive.

E. Impersonation

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

F. Eavesdropping

Monitor and eavesdropping. Also called confidentiality. By listening to the data, the adversary could easily discover the communication contents. Network traffic is also susceptible to monitoring and eavesdropping. This should be no cause for concern given a robust security protocol, but monitoring could lead to attacks similar to those previously described. It could also lead to wormhole or black hole attacks.

G. Traffic Analysis

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

III. Selective Forwarding and its classification

Selective Forwarding Attack is one of the network layer attack described in [8]. In multi-hop wsn, the nodes send packets to the neighbouring nodes thinking that they forward messages to destination faithfully. In Selective Forwarding attack, malicious nodes legitimately refuses some packets and drops them. A simple form of this attack is when a malicious node acts like a black hole and drops all the packets passing through it. However in such an attack, the nodes can detect the attack and can exclude attacker from routing. A more refined of this attack is when a malicious node selectively drops/forwards packets. This makes detection of the attack more complicated.

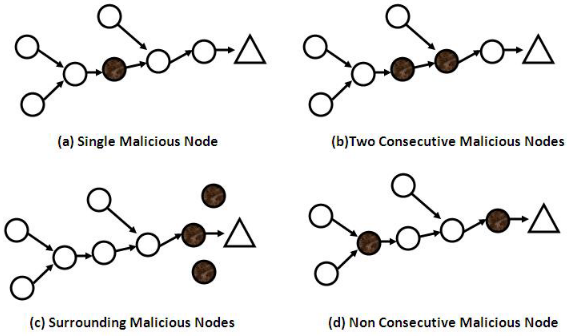
(a) Single Malicious Node
(b)Two Consecutive Malicious Nodes
(c) Surrounding Malicious Nodes
(d) Non Consecutive Malicious Node

Fig. 1. [9]Categorization Of Selective Forwarding based on node count in WSN

Selective forwarding attacks are typically most effective when the attacker is explicitly included on the path of a data flow. However, it is conceivable an adversary overhearing a flow passing through neighboring nodes might be able to emulate selective forwarding by jamming or causing a collision on each forwarded packet of interest. In the fig:3 (referred from [9]), we shown how many ways an adversary can deploy malicious nodes in transmission path to BS.

Based on the packets it drops, selective forwarding can be classified into two types:

- Drops packets of some specified nodes
- Drops packets of some specified type

IV. Countermeasures and Detection Schemes

In this section, we discuss some countermeasures for selective forwarding attack. Based on the previous research, we can classify mitigation schemes into following ways

1) Schemes that detect malicious nodes and remove them from routing information.
    - Acknowledgment based detection.
    - Detection using neighbourhood information.
2) Schemes that uses multi-data flow to mitigate attack.

In latter case, we are not focusing on detecting the attack and malicious nodes, but just avoiding packet loss using multi data flow. In every detection scheme, there will be some prior requirements. Before we go through mitigation schemes, let have a look at some of the requirements and assumptions needed in every detection process. They are

- There must be a secure communication among nodes in the network.
- In deployment phase, nodes cant be compromised.
- To differentiate an attack from normal dropping of packets due to unreliable transmission of sensor networks, the drop ratio has to be more than normal.

A. *Detection using acknowledgments*

Yu and Xiao in [5], proposed a scheme which uses a multi-hop acknowledgment scheme to launch alarms by obtaining responses from intermediate nodes. Each node in the forwarding path is incharge of detecting malicious nodes. If an intermediate node detects a node as malicious in its downstream/upstream, then it will send an alarm packet to the source node/base station through multi-hops. Downstream denotes direction towards base station and upstream denotes direction towards source node. The detection process consists of upstream detection and downstream detection. The scheme uses three types of packets in transmission of an event packet and detection of the attack. They are report packet, ACK packet and alarm packet. There are three different values to be set when a node is transmitting an event packet. They are ACK_Cnt which is a counter value, ACK_Span and ACK_TTL which are predefined values.

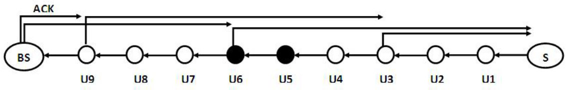

Fig. 2. [5]An example with ACK Span=3 and ACK TTL=6 and u5 as malicious node.

1) Upstream Detection Process: When a node detects an event it forwards a report packet to base station through multi hops. Initially, the field ACK_Cnt is set to ACK_Span which is a predefined metric. When each intermediate node receives the report packet, it first saves the report packet in its cache, decreases the ACK_Cnt by one, or resets ACK_Cnt to its initial value ACK_Span if ACK_Cnt equals to 0 already, and then forwards the report packet to the next downstream node. Meanwhile, if the node finds ACK_Cnt is equal to 0, it generates an ACK packet, where the TTL in the ACK packet is initially set to ACK_TTL, which is also a pre-defined metric. The node sends the ACK packet to the upstream node where the previous report packet comes from. The ACK packet will traverse multiple hops until TTL is decreased to 0, following the same path as traversed by the previous report packet but in the opposite direction.

The intermediate nodes after forwarding report packet waits for the ACK_packet and if an intermediate node receives less than *t*(which is precalculated from ACK_TTL and ACK_Span) packets, it sends an alarm packet to source node. Based on alarm packets recieved, source node identifies malicious node.

2) Downstream Detection Process: If an intermediate node receives a report packet which has a discontinuous Packet_ID for a specific source node, packet loss might have occurred. The node generates an alarm packet, in which, Lost_Packet_ID_Beg and Lost_Packet_ID_End describe the range of the lost Packet_IDs, and Suspicious_Node_ID is set to the upstream node where the report with the discontinuous Packet_ID came from. The alarm packet will be forwarded through multiple hops to the base station. The discontinuity of Packet_IDs might be caused by a malicious upstream node, a nearby outside jammer, or even by routing topology changes. Thus it is likely that the alarm packet is a false alarm. However, when the base station ultimately receive all the report packets, it is easy for the base station to remove false alarms

B. *Lightweight Defense scheme Using Neighbour Nodes as Monitor Nodes*

Xin, etal. proposed [3] a light weight defense scheme against selective forwarding attack which uses neighbor nodes as monitor nodes. The neighbor nodes(monitoring nodes) monitors the transmission of packet drops and resends the dropped packets. Here they used a hexagonal WSN mesh topology.

1) Topology Construction:

- *Node Initialization:* Here nodes of the network gets location of it and their neighbors through GPS. Then, they forward/broadcast a securely digest *Hello* packet at a distance of $2a$. Based on loaction information, node is initialized.
- *Cell Partition:* Each node has to determine which RC it belongs to. To find which RC they belongs to a node first calculates distances from it to midpoints of four adjacent RCs. Then the RC with minimum distance will be adopted as its RC by node.
- *Active Node Election:* Now we have to select an active node for each RC to have communication with other RCs. Active node is the node (x, y) which satisfies the condition $x \leq x_0 andy \leq y_0$ for all $x_0 \in G$ and $y_0 \in G$ where G is node coordinate set in RC

2) Secure Architecture Construction:: In this phase, we construct a secure architecture for secure commmunication between nodes. Each active node of RCs sends a request packet, the recipient active node chescks the coordinates of the sent node are right or wrong. If true adds to the neighbouring RC's table.

3) Routing Discovery and Selection:: There are two phases in attack defense scheme, they are finding route & selecting and data transmission with attack defense. Coming to routing discovery and selection process, it is designed in a way to defend selective forwarding attack. In discovery process, we find routes with number of hops in each direction by some probability schemes.

4) Data Transmission with Attack Defense:: When an event is generated, a packet is sent by a source node through the selected route which is generated from the above routing discovery process. During this transmission if any malicious node in the transmission path drops a packet, then the monitoring neighbour nodes detects the packet drop and broadcasts an alarm packet informing that node as malicious. Now one of the monitoring node choses another path to destination and sends packet without making any delay.

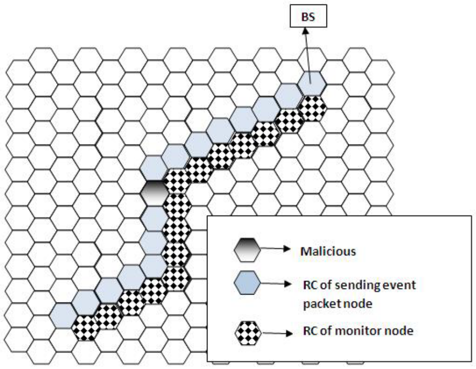

Fig. 3. [3]An example where monitor nodes detects an attack and then reroute the packet.

- *Advantages:*
  - The routing discover scheme is dynamically generating path which makes adversary difficult to launch attack.
  - There is no traffic overhead to detect malicious node.
  - Neighbour nodes are judging the malicious nature of a node, so no need of shared key between every two nodes in the network, which reduces storage required.
  - Efficient utilisation of energy since only one node is active at a time in each RC.
- *Drawbacks:*
  - How much trustworthy a monitor node is?
  - If a node is malicious, the scheme did not explain wheteher to remove complete RC or only that node from routing discovery process. If we are removing complete RC then not efficient resource utilisation.
  - Routing is a probability based one which is not an optimal one.
  - We require GPS to acquire the locations of nodes which makes network costly.

C. Multi Data Flow Scheme

Hung Min-Sun, Chen and Ying-Chu [9] have proposed a single scheme which defends against selective forwarding attack. Their scheme uses multiflow topologies to defend the attack. In multi-dataflow scheme, the whole network is divided into different data topologies that makes, a sensor node belonging to one toplogy can communicate and send information only through nodes of the same topology. This division can be done at different times. Generally division takes place at deployment time. If not then the nodes can randomly choose a topology number after deployment phase. The condition in this scheme is that every topology has to cover the sensing area completely. The scheme is well explained in the figure(2). Here the network is divided into two topologies A and B.

Suppose an event is raised, nodes in both topologies senses the event, raises an event packet and forwards to the base station.

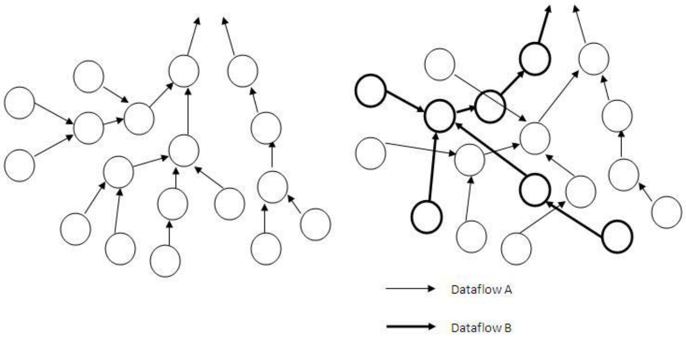

Fig. 4. [9]Dividing original network into two dataflows.

Suppose, a malicious node drops packet in toplogy A, still packet reaches base station through path in topology B. By this scheme, it proves that the scheme successfully defend the selective forwarding attack.

To find the malicious node in this scheme if we have deploye information of sensor nodes. By using their location information base station can detect malicious node.

1) Advantages Of this Scheme:

- In this scheme no need of any additional hardware/software is needed to mitigate the attack.
- There won't be any packet loss or delay due to attack due to which packet delivery ratio will be high.

2) Drawbacks::

- Network cost is high.
- Network lifetime will be low since due to multi data transmission.
- If attack occurs in all topologies then there wont be any defend from attack.

D. Detection Scheme in Hetrogeneous Networks

Brown and Xiaojiang [7] has proposed a scheme to detect selective forwarding using a Heterogeneous Sensor Network(HSN) model. The HSN consists of powerful high-end sensors(H-sensors) and large number of low-end sensors(L-sensors). After deploying sensors, a cluster formation takes place with H-sensor as cluster head.

1) Detection Process:: Whenever packet drops occur at a node, L-sensor nodes report the packet drop to a cluster head (an H-sensor). Based on the reports recived, H-sensor runs a test and determines whether a node is compromised or not.Due to its high memory and high computational capabilities H-sensor can easily run the test.

The scheme uses a Sequential Probability Ratio Test(SPRT) method. In this method, we use a random variable X is used to denote status of a packet forwarding. X only take values 0 or 1, where 0 denotes a successful packet forwarding and 1 denotes a packet drop. For each node, probability value 'p' is calculated which is equal to the percentage of dropped packets in all forwarded packets at a node. As shown in the figure, the scheme considers three threshold values $p_0, p_1 and p_2$. If the node has a value of p below than p_1, then it is considered as legitimate sensor node and greater than p_1 is considered as a compromised node. The other two thresholds are used to say the behaviour of node with more confidence.

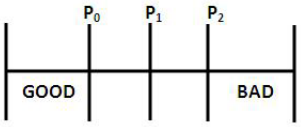

Fig. 5. [7]Threshold values for detection.

2) Reporting packet drops and forwarding them:: Here a secure authentic communication takes place to report the packet drops. The report packet format is $[data\|seq_u]_{K_{H_u}}$. Suppose a packet travels from nodes x,y,z to reach H-sensor then the format will be $[[[data\|seq_x]_{K_{H_x}}\|ID_x]_{K_{H_y}}\|ID_y]_{K_{H_z}}$. Here the encryption occurs at L-sensors and after report reaches H-sensor it does multiple decryption.

E. *Detection Using Twohop Neighbourhood Information:*

Hoang Hai and Eui-Nam Huh[6] proposed a lightweight detection sheme which uses only neighbourhood information.

1) Collecting Twohop Neighbourhood information: The scheme uses two hop neighborhood information to detect the attack. In deployment phase, each node constructs two-hop neighbor table. To achieve this, each node sends/broadcasts a hello packet which contains three important fields source node ID, intermediate node ID and hop counter value. Initially the source node and intermediate node ID fields are equal to node ID which broadcasts the packet and hop counter is initialized to 2. When a node receives hello packet, checks the hop count value if it is equal to 2 then stores source node ID as its immediate neighbor and changes intermediate node ID with its node ID, decrements the hop count by 1 and rebroadcasts it. Sensor node receiving this packet will store intermediate node as their immediate neighbor and source node as two-hop neighbor. Here we are assuming that in deployment phase all communications are secure.

2) Detection Scheme: Each sensor node associates each neighbor node with malicious counter. If malicious counter crosses the threshold then the node is set as malicious and revoked from its neighboring list. When a sensor node receives a packet it checks both source and destination of the packet. If both are in its direct neighbouring list then it activates monitoring/detection process.

- *Rule1* The monitor node waits to see if the destination node forwards the packet on the path to the sink. If not, it raises an alert packet with malicious factor α to the sender/source node.
- *Rule2* The monitor node waits and detects the packet which has been forwarded on the path to the sink. It checks it two-hop neighbour knwoledge to see if the destination node of the forwarded packet is on the right path to the sink. If not, it raises an alert packet with malicious factor β to the sender/source node.

α and β are the malicious factors with $0 < \alpha < 0.5 < \beta < 1$. When a sensor node recieves an alert packet from its neighbours it calculates the malicious value of the node and if it crosses threshold value then it revocates it from neighbouring list.

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 Selectice Forwarding attack. In this attack, a malicious node is dropping packets which makes 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.

References

[1] Y.C.Hu, A.Perrig, and D.B.Johnson. Packet leashes: a defense against wormhole attacks in wireless networks In *In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, 2003.

[2] Hemanta Kumar Kalita and Avijit Kar. Wireless sensor network security analysis. In *International Journal of Next-Generation Networks*, 2009.

[3] Wang Xin-sheng, Zhan Yong-zhao, Xiong Shu-ming, and Wang Liang-min. Lightweight defense scheme against selective forwarding attacks in wireless sensor networks. pages 226 –232, oct. 2009.

[4] S. Kaplantzis, A. Shilton, N. Mani, and Y.A. Sekercioglu. Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pages 335 –340, 2007.

[5] Bo Yu and Bin Xiao. Detecting selective forwarding attacks in wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*, page 8 pp., 2006.

[6] Tran Hoang Hai and Eui nam Huh. Detecting selective forwarding attacks in wireless sensor networks using two-hops neighbor knowledge. In *NCA*, pages 325–331, 2008.

[7] Jeremy Brown and Xiaojiang Du. Detection of selective forwarding attacks in heterogeneous sensor networks. In *ICC*, pages 1583–1587, 2008.

[8] Chris Karlof and David Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks*, 1(2-3):293–315, 2003.

[9] Hung-Min Sun, Chien-Ming Chen, and Ying-Chu Hsiao. An efficient countermeasure to the selective forwarding attack in wireless sensor networks. pages 1 –4, oct. 2007.

[10] Bin Xiao, Bo Yu, and Chuanshan Gao. Chemas: Identify suspect nodes in selective forwarding attacks. *J. Parallel Distrib. Comput.*, 67(11):1218–1230, 2007.