Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
REVIEW PAPER
Available Online at www.ijarcs.info

Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks

Rajat Malik
Department of Computer Science and Engineering
U.I.E.T.,M.D.U
Rohtak,India

Harkesh Sehrawat
Department of Computer Science and Engineering
U.I.E.T.,M.D.U.
Rohtak,India

Dr Yudhvir Singh
Department of Computer Science and Engineering
U.I.E.T.,M.D.U.

Abstract: In present scenario, the fastest and cheapest way of communicating worldwide is via networks. Wireless Sensor Networks (WSNs) have become extensive part of many areas like traffic surveillance, defense, asset tracking, healthcares, structural monitoring of building and bridges and environmental monitoring of air, water and soil. The emergence of WSNs in today's technological world has lead to the need of secured and safeguarded transmission of data over networks. WSNs have issues like low memory and limited battery availability, so conventional security establishments are not effective here. A number of attacks are possible over WSNs like black hole, wormhole and selective forwarding attack. Selective forwarding attack is a special case of black hole attack where compromised nodes drop packets selectively. This leads to degradation of network performance. In this paper we will review some important attacks over WSNs with possible ways to detect and defend selective forwarding attack.

Keywords: WSN, selective forwarding attack, topology, sensor node, classification, defense.

1. INTRODUCTION

Wireless Sensor Network (WSN) is a wireless network of geographically dispersed self-determined devices called nodes that have inbuilt sensors to capture environmental and physical situations [1]. WSN is incorporated with gateways that do the work of acting as a medium of interaction between distributed wireless nodes and wired world. These WSNs follow a number of protocols based on requirements of the user and applications. Some of the standards usually found are 2.4 GHz radios based on either IEEE 802.15.4 or IEEE 802.11 (Wi-Fi) standards or proprietary radios, which are usually 900 MHz [1].

A. Sensor Nodes: Sensor nodes are major constituent component of WSN. These nodes include: -

- A Radio
- Microcontroller
- Analog circuit
- Battery
- Sensor interface

Radio is used for transmission of signal among nodes or to gateways. The data rate of these radios depends on battery capacity, so preferably a battery with long life, relative high capacity (in terms of power), low weight and easy availability is considered. Microcontroller, analog circuit and sensor interface contribute to the processing of collected data and its forwarding within network. Figure 1 given below shows architecture of WSNs.

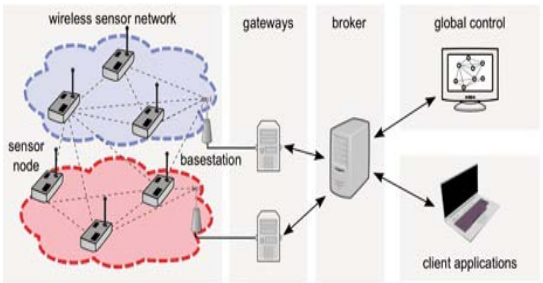

Figure1. Architecture of WSN

B. Topology of WSN: Three types of topologies are found in WSNs as described below:-

- Star topology: - Here each sensor node is connected directly to the gateway.
- Cluster tree topology: - In this, each node is connected to another node at higher degree in the tree and gateway act as root of the tree. Data routes from leaf nodes to gateway.
- Mesh topology: - In mesh, nodes are interconnected to each other and to the gateway. This topology is most reliable of all.

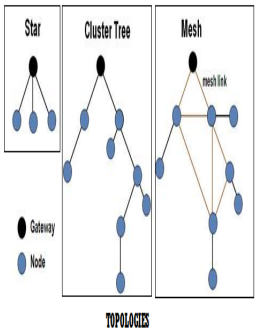

Figure2. Topology in WSN

C. Attacks on WSN: A real world WSN may be made up of thousands of sensor nodes and these nodes have low security capabilities due to their limited resources. These nodes are vulnerable to much kind of attacks. Some of the possible attacks, classified on the bases of OSI reference model's layers, are listed in table given below with their defense strategies.

Table1. Attacks on WSN [2], [3]

OSI Reference layer	Attacks	Defense strategy
Application layer	• Attacks on reliability • Data aggregation distortion	• Cryptography • Encoding • Watermarking
Transport layer	• Adding false messages • Sync flood • De-synchronization	• Authentication • Verification
Network layer	• Packet removal • Selective forwarding • Hello flood • Black hole • Worm hole	• Authentication
Data link layer	• Collusion • Jamming • Disruption MAC	• Spread spectrum • Error correction techniques
Physical layer	• Jamming • Tampering	• Spread spectrum strategy • MAC layer admission control

2. SELECTIVE FORWARDING ATTACK

Selective forwarding attack is an attack of network layer found in WSNs. Usually in WSNs, sensor nodes forward data packets to next or neighboring sensor node keeping a trust factor that packets will reach their destinations at the end. In this attack, malicious nodes are setup by intruders which act as sensor node of the network. These malicious nodes drop out data packets passing through them and forward only selective packets to the next sensor node. When all the packets are dropped out, in that instance, this attack can be called as black hole attack solely.

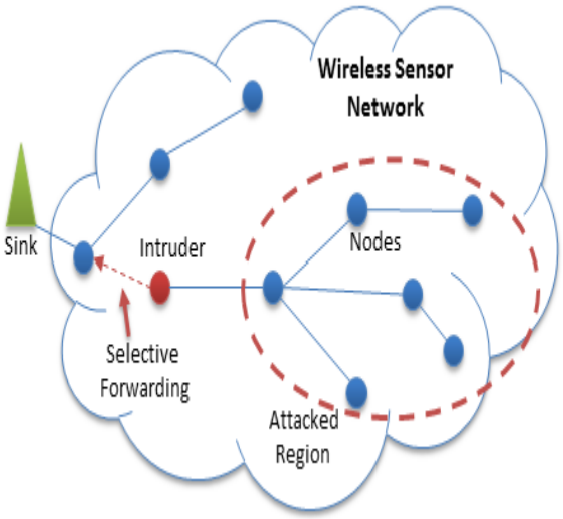

Figure3. Selective forwarding attack

Black hole attack is easy to detect as it drops all the incoming packets which gives clear indication of being a malicious node. But in selective forwarding, it is hard to detect this attack as losing of few data packets is a normal phenomenon in network transmission.

A. Classification of Selective Forwarding Attack

A.1. On the bases of malicious node*:* Selective forwarding attack can be categorized based on the arrangement of malicious nodes within the network. Figure 4 given ahead illustrated it.

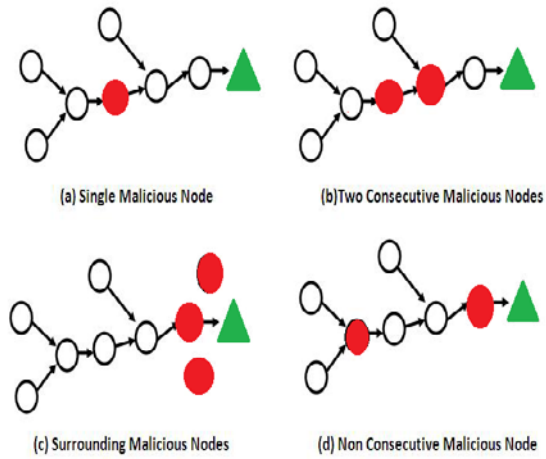

Figure4. Categorization of selective forwarding attack [4]

A.2. On the bases of dropped packets*:* On the basis of packets dropped by the malicious nodes, this attack can be classified into two types [4]: -

(a) Packets dropped of a specific node of the network.

(b) Packets dropped of a specific type.

B. Detection and avoidance techniques of Selective Forwarding Attack

In this segment, we talk about different measures to detect and avoid selective forwarding attack. In light of the past research, we can arrange prevention plans in these types: -

(a) Techniques that detects malicious nodes and eliminate them from network routing.

- Detection using acknowledgement

- Detection with the help of neighboring node's information

(b) Techniques of using multiple data flow paths that eliminates attack's effects.

These techniques are explained further in the paper.

B.1. Acknowledgement based detection

This technique was proposed by Yu and Xiao in [5]. In this technique, every sensor node in the WSN helps to detect malicious nodes. If any intermediate node detects any node as malicious then it sends alarm message to the base node/ source node depending on the packet flow direction (Upstream/Downstream) using multi-hops instead of single hopping. Direction of packets towards base node is denoted by upstream whereas direction of packet flow towards source node is called downstream. A group of three packets is sent in this scheme which is report, ACK and alarm packets. They together do the work of data transmission and attack detection. Every event packet in this scheme further contains three values which are set by every node of the WSN. These three values are ACK_Cnt that represent a counter value, ACK_span and ACK_TTL which are already set initially.

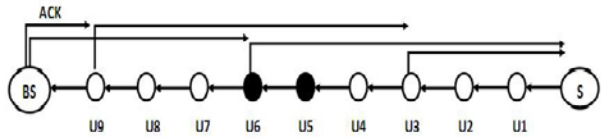

Figure5. Acknowledgment based scheme [5]

In above figure 5, ACK_span is taken 3, ACK_TTl is taken 6 and U5, U6 are malicious nodes. "BS" is base station and "S" is source node.

B.1.1. Detection process: Initially ACK_Cnt within report packet is set equal to ACK_Span generated from a predefined matrix. This report packet is forwarded upstream. When any node gets this report packet it decreases the ACK_Cnt by 1, saves information in its cache memory and forwards the packet to next node. If ACK_Cnt value is already reached to 0 then it sends the packet to downstream by generating ACK packet and setting its TTL value using predefined matrix. As the ACK packet travels downstream, the TTL value is also decreased by 1 till it reaches 0. Now all intermediate nodes matches their report packets ACK_Cnt, stored in cache, with ACK_TTL. If they do not match then an alarm packet is sent to source node informing about existence of malicious node.

In this way, the selective forwarding attack can be detected.

B.2. Neighborhood monitoring scheme

Paper presented by Xin et al. [6] describes this scheme where the neighbor sensor nodes act as monitor nodes while defending against selective forwarding attack. Here, the monitor nodes detect the dropping of packets and resend those packets making attack to fail. Hexagonal mesh topology is followed in this scheme.

Following stages are adopted in this scheme: -

B.2.1. Constructing topology: In this stage, all the nodes with their neighbors within the network are discovered using GPS. Then they send secure *Hello* packets to share their identities with neighbor nodes within a specified distance. After this, every node decides to which RC it would belong by knowing nearest RC to its location. At last, an active node for each RC is selected that communicate with other RCs.

B.2.2. Constructing secure architecture: Here, a secure architecture is created for safe transmission of data packets. Each active node sends request packet to its neighboring RCs. These neighboring RCs in return checks validity of request packet's sender and if found true then adds it to the neighboring RC's table.

B.2.3. Discovering routes and selection: It has two steps incorporated:

- Finding possible routes
- Selecting route and transmitting data applying defense mechanism

In this stage, selection of route is done by counting the minimum number of hops required and data is transmitted in a secure manner.

B.2.4. Transmitting data incorporating defense: In this stage, packets are transmitted over the selected route while monitoring nodes in action. If any monitoring node detects dropping of packets by some other node then it broadcasts an alarm message declaring dropping node as malicious. After this, any other monitoring node selects alternate path to destination and sends packets through this new path.

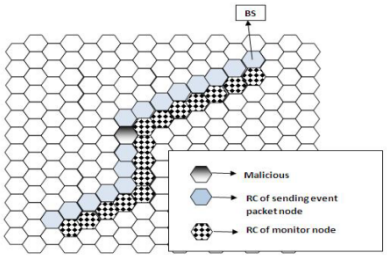

Figure6. Detection of malicious node and changing of path by RC [4]

B.3. Multipath data flow scheme

Hung Min-Sun, Chen and Ying-Chu [7] have stated a scheme to defend this attack. This scheme uses multiple data flow paths to undo the effect of selective forwarding attack. Here, the network is divided into many topologies keeping the fact in consideration that each topology must cover the whole network. After it, sensor nodes are assigned among these topologies so that these nodes can forward data only to those nodes that belong to same topology. This work is done usually at deployment time. Now the data packets are replicated according to number of topologies and forwarded to the destination through sensor nodes within each topology.

Suppose if malicious node is present in any one topology and it drops packets, in that case other topologies assures transmission of packets to the destination. This gives a reliable scheme of data transmission in case of selective forwarding attack.

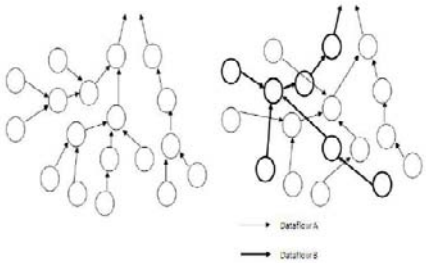

Figure7. Multi path scheme

B.4. Advantages and Disadvantages of techniques

Table2. Pros and cons of techniques

Technique	Advantages	Disadvantages
Acknowledgement based detection	Easy to implement No special hardware required	Packet overhead is increased Ifacknowledgement packets gets lost than this scheme would fail
Neighborhood monitoring scheme	Secret key is not needed anymore here Traffic overheads for detection of malicious nodes will be reduced	Responsibilities will increase for monitor nodes and it would deviate focus from data transmission Monitor nodes are not fully trustworthy GPS will be required to locate nodes
Multipath dataflow scheme	No extra hardware/software required No packet loss or delay which leads to high packet delivery ratio	Network cost will be high If all paths have malicious node than this scheme will fail

3. CONCLUSION

The foremost need of any WSN is transmission of data securely to pre-defined destination with time constraint followed. Selective forwarding is one of many attacks that degrade network's performance. Malicious node drops out packets selectively harming overall authenticity of WSN. In this paper we reviewed basic introduction to wireless sensor networks with different attacks focused over it. We also discussed selective forwarding attack with its classification, detection and avoidance schemes. This investigation will emphasis the downsides within the past plans and will accommodate to mitigate the disadvantages later on.

4. REFERENCES

[1]. "http://www.ni.com/white-paper/7142/en/", [online].

[2]. Geethu PC and Rameez Mohammed A, "Defense Mechanism against Selective Forwarding Attack in Wireless Sensor network", IEEE-31661, 4th ICCNT-2013, July 4-6, Triruchengode.

[3]. Naser M. Alajmi and Khaled M. Elleithy, "Comparative Analysis of Selective Forwarding Attacks over Wireless Sensor Networks", International Journal of Computer Applications, ISSN: 0975-8887, Volume 111, No. 14, February 2015.

[4]. Leela Krishna Bysani and Ashok Kumar Turuk, "A Survey on Selective Forwarding Attack in Wireless Sensor Networks", 978-1-4244-9190-2/11/$26.00 ©2011 IEEE.

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

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

[7]. 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.