# Analysis of Selective Forwarding Attacks In Wireless Sensor Networks

Preeti Sharma
Department of Computer Engineering
SBS College of Engineering & Technology, Ferozpur INDIA

Monika Saluja
Department of Computer Engineering
SBS College of Engineering & Technology, Ferozpur INDIA

Krishan Kumar Saluja
Department of Computer Engineering
PIT Kapurthala,INDIA

## ABSTRACT

Wireless sensor network has been grown as hottest research area for past few years. They have extensive applications; there are various areas in wireless sensor networks on which researchers are working. The area which have gain attention of almost every researcher is security, security of wireless sensor network has become very important since once deployed these networks are unattended and unprotected. . As security playing very important role in it, to provide better security algorithms nature of attack should be known and the type of parameter on which it affects most should be considered. Sensor networks are vulnerable to various attacks like sink hole attacks, black hole attacks, wormhole attacks and selective forwarding attacks .in this paper we are going to concentrate on selective forwarding attacks .In selective forwarding attack, malicious nodes may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any more. In this research paper we are going to analyze the selective forwarding attacks in wireless sensor networks on the basis of some parameters like network throughput, end to end delay and energy consumption, dropped packets by simulating it using OPNET MODELER 14.5

## General Terms

Analysis ,attacks .

## Keywords

Analysis, selective forwarding attacks

## 1. INTRODUCTION

Wireless Sensor Network (WSN) is conceived as a network of small devices called sensors distributed over an area of interest where some specific phenomena must be monitored. Wireless sensor networks are vulnerable to many routing attacks for example Selective forward attack , HELLO flood attack , sinkhole attack, Wormhole attack ,etc because of broadcast nature of transmission medium( as it using wireless medium for communication ), resource limitation on sensor nodes and uncontrolled environments where they are left unattended. The existing security mechanisms are inadequate and new approaches are required for each routing attack since each attack has its own nature and characteristics. In this paper we are going to concentrate on selective forwarding attacks. In selective forwarding attack compromised node act as a normal node but refuses to forward certain selected packets and simply drop them. So, due to this nature, the selective forwarding attack is very harmful for mission critical applications and can damage the whole network communication, making the network useless. The selective forwarding Attack was first described by Karlof and Wagner [1]. This attack is sometimes called Gray Hole attack. In a simple form of selective forwarding attack, malicious nodes try to stop the packets in the network by refusing to forward or drop the messages passing through them. There are different forms of selective forwarding attack. In one form of the selective forwarding attack, the malicious node can selectively drops the packets coming from a particular node or a group of nodes. This behavior causes a DoS attack for that particular node or a group of node. Another form of selective forwarding attack is called Neglect and Greed. In this form, the subverted node arbitrarily neglecting to route some messages [2]. It can still participate in lower level protocols and may even acknowledge reception of data to the sender but it drops messages randomly. Such a node is neglectful. When it also gives excessive priority to its own messages it is also greedy. Moreover, another variance of selective forwarding attack is to delay packets passing through them, creating the confused routing information between sensor nodes [3].

This paper is the effort towards the systematic analyses of the Selective Forwarding attack by simulating the network in opnet modeler 14.5. The main objective of this research paper is to give an overview for all those researchers and developers who used to propose different techniques to counter Selective Forwarding attack Is that how selective forwarding attacks impacts on Wireless Sensor Networks with some basic parameters such network throughput, end to end delay and energy consumption as It is very difficult to distinguish between selective forwarding attacks and normal packet drops due to some network errors in wireless sensor networks. So the analysis is important for collecting information about the impact of that packet dropping which would help us to decide how badly that packet dropping will affect the Wireless Sensor Network, for that purpose I created and simulated the network using opnet modeler.

## 2. SIMULATION MODEL

Open-ZB [4] is an open source implementation of IEEE 802.15.4/ZigBee [5]. The simulation models are available for OPNET and TinyOS. Version 2.0 of the accurate simulation model of the slotted IEEE 802.15.4 is programmed for the OPNET simulator. The model structure is shown in Figure 1 [4]. This model implements PHY and MAC and APP layers. PHY is includes a transmitter and a receiver working at 2.4 GHz frequency, 2 MHz bandwidth and QPSK modulation. The MAC layer contains slotted CSMA/CA, generates beacon frames and synchronizes nodes with a PAN Coordinator. The battery module calculates consumed and remaining energy levels. The APP layer includes a sensory data generator using unacknowledged frames and a MAC command frame generator creating acknowledged frames. The sink module performs statistics of

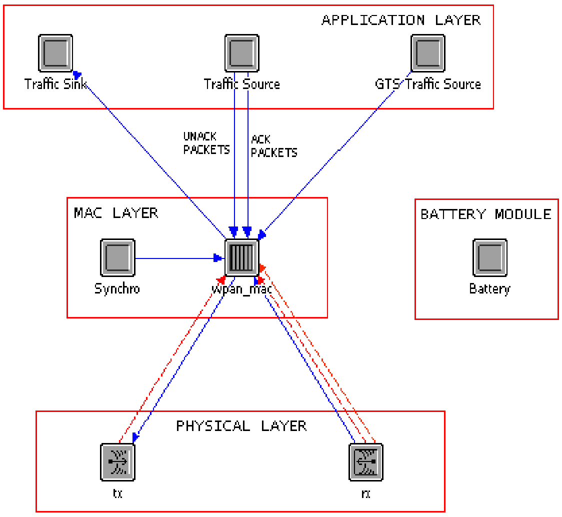

**Fig. 1 Structure of the IEEE 802.15.4 Simulation Model**

## 3. TYPESET TEXT

The received frames. The radio model contains the standard OPNET wireless modules, which emulate the radio channel with such elements as interference, noise, BER, propagation delay, etc.

The supported features of the Open-ZB are:

– Beacon-enabled mode (Generation of beacon frames)
– Slotted CSMA/CA MAC protocol
– Beacon, data, ACK packet frame formats
– IEEE 802.15.4 PHY characteristics
– Calculation of power consumption (MICAz model)
– GTS Mechanism (v2.0)

## 3 Experimental Results & Analysis

The given figure showing the arrangement of nodes in the wireless sensor network, in total there are 30 nodes out of which 15 nodes are GTS nodes that means their GTS parameters are active and priority will be given to the packet sent by them rest 15 nodes are CAP nodes .

### 3.1 Network Throughput

A network throughput is the average rate at which message is successfully delivered between a receiver (destination node) and its sender (source node). It is also referred to as the ratio of the amount of data received from its sender to the time the last packet reaches its destination [6]. Throughput can be measured as bits per second (bps), packets per second or packet per time slot and OPNET Modeler expresses it using bits per second. For a network, it is required that the throughput is at high-level. Some factors that affect WSN's throughput are: unreliable communication, changes in topology, limited energy and bandwidth.

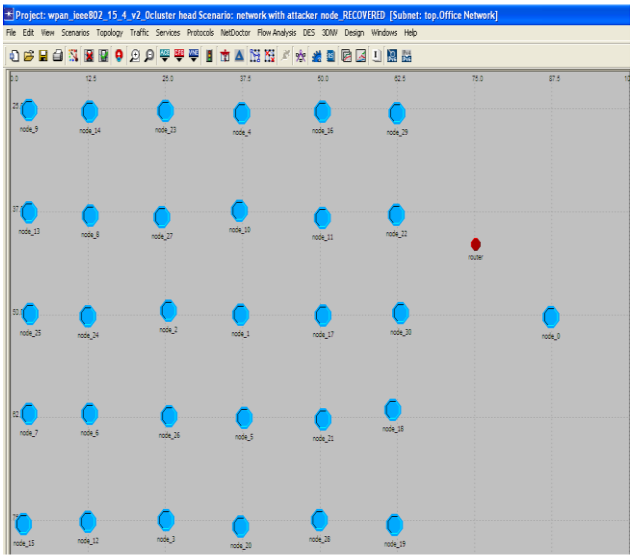
Project: wpan_ieee802_15_4_v2_0cluster head Scenario: network with attacker node_RECOVERED [Subnet: top.Office Network]
File Edit View Scenarios Topology Traffic Services Protocols NetDoctor Flow Analysis DES 3DNV Design Windows Help
router

**Fig. 2 Simulation workspace with 30 nodes**

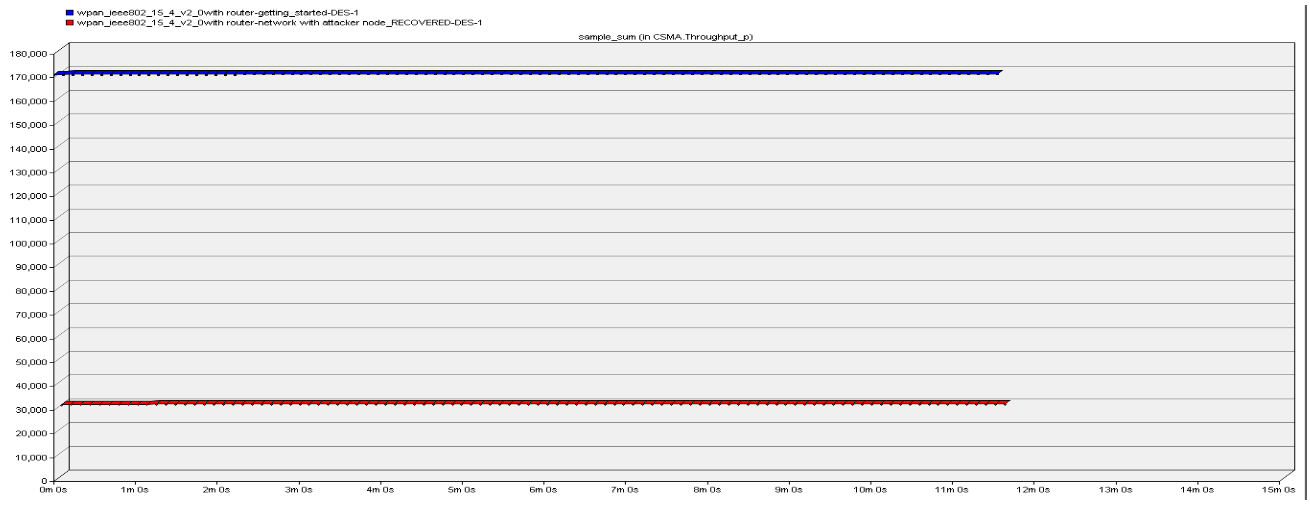

**Fig 3: Throughput of 30 nodes**

## 3.2 Energy consumption

The energy consumed by nodes can be defined as amount of energy nodes need to consume while communicating.

## 3.3 End to End Delay

Packet end-to-end delay is the time delay it takes a network source to deliver a packet to its destination. Thus, the end-to-end delay of packets is the total amount of delays encountered in the whole network at every hop going to its destination. In WSNs, this kind of delay is usually caused by certain connection tearing or/and the signal strength among nodes

been low or because of attacks like selective forwarding attacks. The reliability of a routing protocol can be determined by its end-to-end delay on a network, thus a steadfast WSN routing gives less packet end-to-end delay

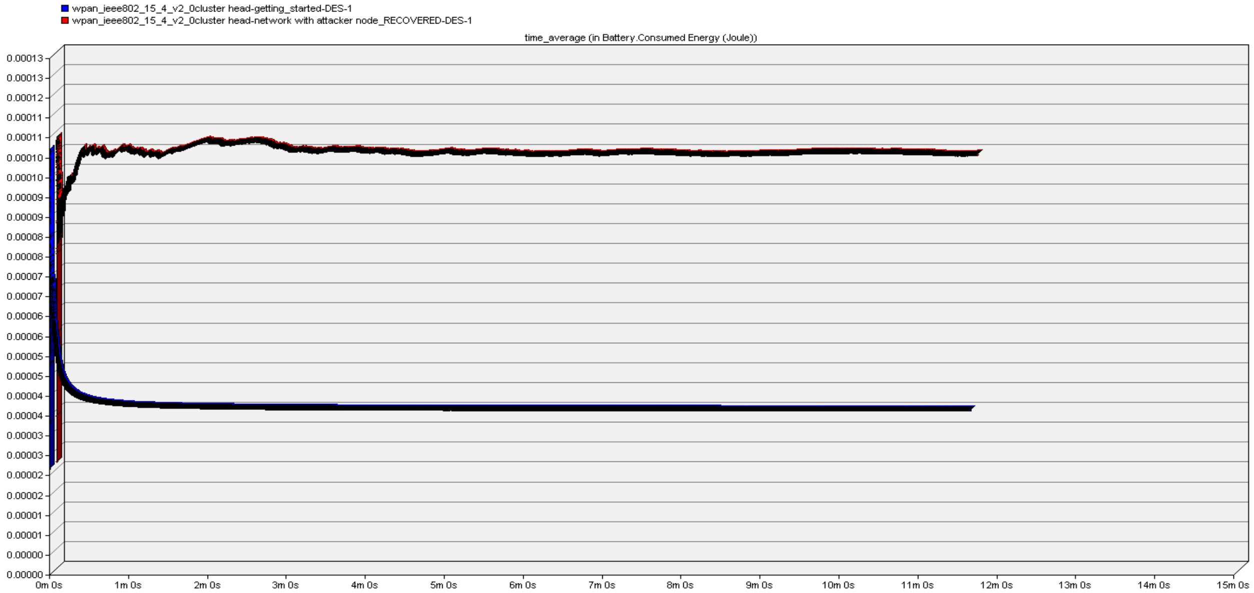

**Fig: 4 Energy Consumed**

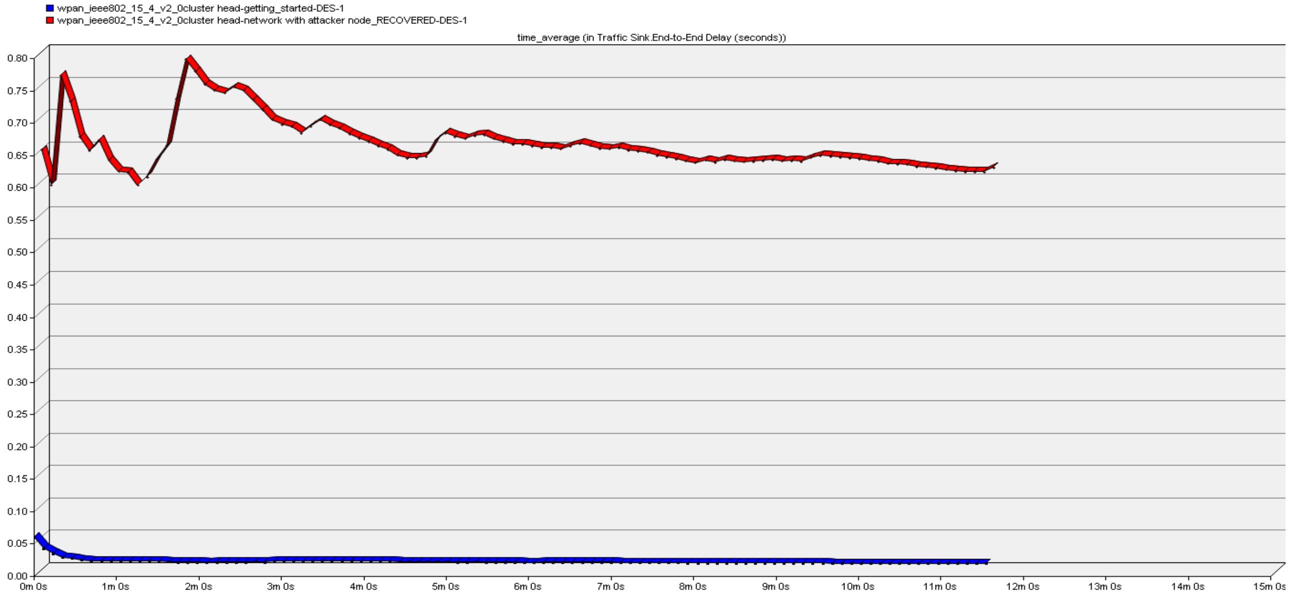

**Fig: 5 End to End delay**

## 3.4 Dropped Packets

It defines number of packets dropped due to attacks or some network issues

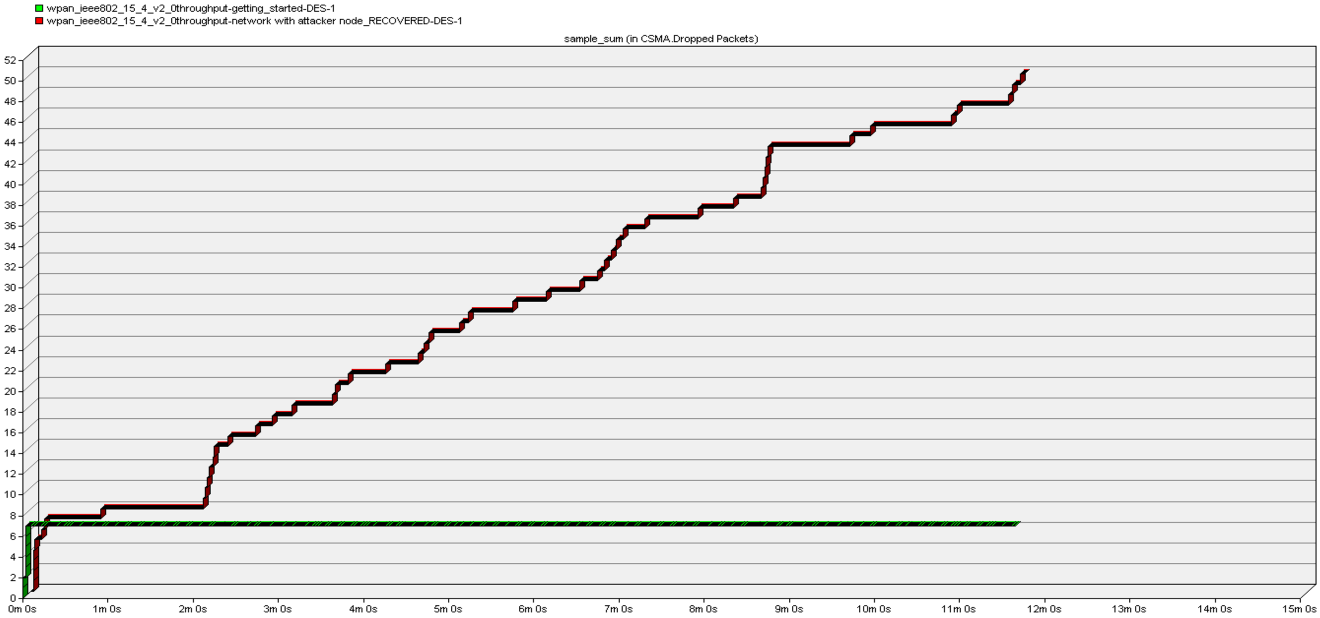

**Fig: 6 Dropped packets**

**Table 1 analysis of performance metric**

| **Performance metrics** | **Value** | **Sim 1without attack** | **Sim 2 with attack** |
|---|---|---|---|
| Throughput | Initial | 171,242.975 | 29,781.386 |
| (bps) | Final | 171,574.295 | 30,099.203 |
| | Minimum | 171,242.975 | 29,781.386 |
| | Maximum | 171,574.295 | 30,099.203 |
| Energy consumption | Initial | 66.571428 | 66.57142 |
| (joules) | Final | 70.515714 | 70.35428 |
| | Minimum | 59.857142 | 56.71428 |
| | Maximum | 75.389610 | 72.42857 |
| End to end delay | Initial | 0.0600252 | 0.647820 |
| (ms) | Final | 0.0194139 | 0.620626 |
| | Minimum | 0.0194139 | 0.593053 |
| | Maximum | 0.0600252 | 0.787957 |
| Dropped packets | Initial | 0.00000 | 0.00000 |
| (packets) | Final | 7.00000 | 50.0000 |
| | Minimum | 0.00000 | 0.00000 |
| | Maximum | 7.00000 | 50.0000 |

## 4. ANALYSIS

The scenario was completed using two different simulations to easy the presentation and analyses of results. These two simulations shows the throughput performance metrics of simulations 1 and 2, which are based on WSN's regular operation compared with when under selective forwarding attack, respectively. We observe that without selective forwarding attack, the WSN has a high throughput varying from 0.0000 to 700.00 packets per sec. On the other hand, with attack, its throughput dropped and ranged from 0.0000 to 10.0000 packets per second. Similarly in case of energy consumption more energy was consumed in case when there was attack in network it varies from 66.57142 to 72.42857 and in case when there is no attack in network it varies from 66.571428 to 72.42857. in case of end to end delay more end to end delay in case when there was attack it varies from 0.647820 to 0.787957 and with no attack it varies from 0.0600252 to 0.0600252 similar results was there with dropped packets more packets dropped with attack scenario and less in case when there was no attack. This analysis help us to study the nature and effects of selective forwarding attacks we can see that in case of normal scenario that is without any attacks packet dropping exists due to network issues but still that much packet drop is bearable but the selective forwarding attacks effecting the network more badly.

## 5. CONCLUSION

This paper presented a simulation study of a Wireless Sensor Network to analyze the effects of selective forwarding attacks. The scenarios considered are no attack and attacks on nodes. The simulation tool OPNET 14.5 is used effectively for detailed analysis. The scenarios considered are mainly taken from the literature. The simulation results show that the impact of selective forwarding attacks on performance of WSN can become quite significant. In case there is an attack the performance degradation is more severe. From this analysis we can conclude that packet dropping due to some network errors and selective forwarding attacks are affecting the network to different extent.

## 6. 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] Anthony Wood, John A. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer, 35(10):54-62, October 2002.

[3] Wazir zada khan et. al "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks" I.J. Computer Network and Information Security, 2011, 1, 1-10 Published Online February 2011 in MECS.

[4] "Open-ZB, " http://www.open-zb.net".

[5] IEEE, *IEEE* Standard 802.15.4, http://standards.ieee.org/getieee802/download/802.15.4-2003.pdf.

[6] N.V Trang and X.Xing "Rate –adaptive Multicast in MANETS" WiMob'2005, Vol.3, Pages: 352-360.