Analyzing the Impact of Wormhole Attack on Routing Protocol in Wireless Sensor Network on Behalf of packet tunnel, dropped and intercepted

Er. Gurjot Singh
Department of Computer Science and Engineering
BBSBEC, Fatehgarh Sahib, Punjab, India

Er. Gurpreet Kaur
Department of Computer Science and Engineering
BBSBEC, Fatehgarh Sahib,Punjab, India

Abstract— *A Wireless Sensor Network can be defined as a group of independent nodes, communicating wirelessly over limited frequency and bandwidth. The novelty of WSNs in comparison to traditional sensor networks is that they depend on dense deployment and coordination to execute their tasks successfully. Wireless sensor network has limited resources like less storage space, low energy and computation power. In this paper, we introduce the wormhole attack, a severe attack in wireless sensor network that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many routing protocols like AODV and DSR. In this paper the impact of wormhole attack on these routing protocols are analyzed with different parameter like frame tunnel, frame dropped and intercepted.*

Index Terms— Wireless sensor network, AODV, DSR, wormhole attack.

I. Introduction

Advances in wireless communication and electronics have enabled the development of low-cost, low-power, multifunctional sensor nodes. These tiny sensor nodes, consisting of sensing, data processing, and communication components, make it possible to deploy Wireless Sensor Networks (WSNs), which represent a significant improvement over traditional wired sensor networks. WSNs can greatly simplify system design and operation, as the environment being monitored does not require the communication or energy infrastructure associated with wired networks[1]. WSNs are expected to be solutions to many applications, such as detecting and tracking the passage of troops and tanks on a battlefield, monitoring environmental pollutants, measuring traffic flows on roads, and tracking the location of personnel in a building. Many sensor networks have mission-critical tasks and thus require that security be considered [2, 3]. Improper use of information or using forged information may cause unwanted information leakage and provide inaccurate results. The use of radio transmission, along with the constraints of small size, low cost, and limited energy, make WSNs more susceptible to denial-of-service and wormhole attacks.

II. Attacks in Wireless Sensor Networks

Attacks against wireless sensor networks could be broadly considered from two different levels of views. One is the attack against the security mechanisms and another is against the basic mechanisms (like routing mechanisms). Here we point out the major attacks in wireless sensor networks.

A. *Denial of Service*

Denial of Service (DoS) [4], [5] is produced by the unintentional failure of nodes or malicious action. The simplest DoS attack tries to exhaust the resources available to the victim node, by sending extra unnecessary packets and thus prevents legitimate network users from accessing services Or resources to which they are entitled. DoS attack is meant not only for the adversary's attempt to subvert, disrupt, or destroy a network, but also for any event that diminishes a network's capability to provide a service. In wireless sensor networks, several types of DoS attacks in different layers might be performed. At physical layer the DoS attacks could be jamming and tampering, at link layer, collision, exhaustion, unfairness, at network layer, neglect and greed, homing,misdirection, black holes and at transport layer this attack could be performed by malicious flooding and desynchronization. The mechanisms to prevent DoS attacks include payment for network resources, pushback, strong authentication and identification of traffic.

B. *Sybil Attack*

In many cases, the sensors in a wireless sensor network might need to work together to accomplish a task, hence they can use distribution of subtasks and redundancy of information. In such a situation, a node can pretend to be more than one node using the identities of other legitimate nodes. This type of attack where a node forges the identities of more than one node is the Sybil attack [6], [7]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. Sybil attack can be performed for attacking the distributed storage, routing mechanism, data aggregation, voting, fair resource allocation and misbehavior detection [7]. Basically, any peer-to-peer network (especially wireless ad hoc networks) is vulnerable to sybil attack. However, as WSNs can have some sort of base stations or gateways, this attack could be prevented using efficient protocols. Douceur [6] showed that, without a logically centralized authority,sybil attacks are always possible except under extreme and unrealistic assumptions of resource parity and coordination among entities. However, detection of sybil nodes in a network is not so easy.

C. Blackhole/Sinkhole Attack

In this attack, a malicious node acts as a blackhole [9] to attract all the traffic in the sensor network. Especially in a flooding based protocol, the attacker listens to requests for routes then replies to the target nodes that it contains the high quality or shortest path to the base station. Once the malicious device has been able to insert itself between the communicating nodes (for example, sink and sensor node), it is able to do anything with the packets passing between them. In fact, this attack can affect even the nodes those are considerably far from the base stations.

D. Wormhole Attack

Wormhole attack is one of the Denial-of-Service attacks effective on the network layer, that can affect network routing, data aggregation and location based wireless security. [9] The wormhole attack may be launched by a single or a pair of collaborating nodes. In commonly found two ended wormhole, one end overhears the packets and forwards them through the tunnel to the other end, where the packets are replayed to local area. In case when they only forward all the packets without altering the content, they are helping the network to accomplish transmission faster. But in majority of the cases, it either drops or selectively forwards the packets, leading to 86 the network disruption. Wormhole attack does not require MAC protocol information as well as it is immune to cryptographic techniques. [10] This makes it very difficult to detect.

A number of approaches have been proposed for handling wormhole attack. Some approaches
only detect the presence of wormhole in the network, while some approaches also focus on
avoiding or preventing the wormhole attack. Majority of the techniques presented require
additional hardware support, tight time synchronization, localization information or may be
confined to specific routing algorithm.

1) Types of wormhole attack

Number of nodes involved in establishing wormhole and the way to establish it classifies Wormhole into the following types.

a. Wormhole using Out-of-Band Channel

In this two-ended wormhole, a dedicated out-of-band high bandwidth channel is placed between end points to create a wormhole link.

b. Wormhole using Packet Encapsulation

Each packet is routed via the legitimate path only, when received by the wormhole end, gets Encapsulated to prevent nodes on way from incrementing hop counts. The packet is brought into original form by the second end point.

c. Wormhole using High Power Transmission

This kind of wormhole approach has only one malicious node with much high transmission Capability that attracts the packets to follow path passing from it.

d. Wormhole using Packet Relay

Like the previous approach, only one malicious node is required that replays packets between two far nodes and this way fake neighbors are created.

e. Wormhole using Protocol Deviation

The malicious node creates wormhole by forwarding packets without backing off unlike a legitimate node and thus, increases the possibility of wormhole path getting selected.

2) Models of Wormhole Attacks

Packet forwarding behavior of wormhole end points as well as their tendency to hide or show the identities, leads to the following three kinds of models. Here, S and D are the source and destination respectively. Nodes M1 and M2 are malicious nodes.

a. Open Wormhole

Source and destination nodes and wormhole ends M1 and M2 are visible. Identities of nodes A and B, on the traversed path are kept hidden.

b. Half-Open Wormhole

Malicious node M1 near the source is visible, while second end M2 is set hidden. This leads to path S-M1-D for the packets sent by S for D.

c. Close Wormhole

Identities of all the intermediate nodes on path from S to D are kept hidden. This leads to a scenario where both source and destination feel themselves only one-hop away from each other. Thus fake neighbors are created.

III. ROUTING PROTOCOLS

Due to the difference of wireless networks from other contemporary communication and wireless ad hoc networks routing is a very challenging task in WSNs. For the deployed sheer number of sensor nodes it is impractical to build a global scheme for them. IP-based protocols cannot be applied to these networks. All applications of sensor networks have the requirement of sending the sensed data from multiple points to a common destination called sink. Resource management is required in sensor nodes regarding transmission power, storage, on-board energy and processing capacity.

IV. There are various routing protocols that have been proposed for routing data in wireless sensor networks due to such problems. The proposed mechanisms of routing consider the architecture and application requirements along with the characteristics of sensor nodes.

A. AODV ROUTING PROTOCOL

There are two types of routing protocols which are reactive and proactive. In reactive routing protocols the routes are created only when source wants to send data to destination whereas proactive routing protocols are table driven. Being a reactive routing protocol AODV uses traditional routing tables, one entry per destination and sequence numbers are used to determine whether routing information is up-to-date and to prevent routing loops.

The maintenance of time-based states is an important feature of AODV which means that a routing entry which is not recently used is expired. The neighbors are notified in case of route breakage. The discovery of the route from source to destination is based on query and reply cycles and intermediate nodes store the route information in the form of route table entries along the route[12]. Control messages used for the discovery and breakage of route are as follows:

- Route Request Message (RREQ)
- □Route Reply Message (RREP)
- Route Error Message (RERR)
- □HELLO Messages.

B. DSR ROUTING PROTOCOL

Dynamic Source Routing (DSR) protocol is specifically designed for multi-hop ad hoc networks. DSR allows the network to be completely self organizing and self configuring without the need for any other existing network. It is the reactive protocol. It has two major parts:

- ➢ Route Discovery
- ➢ Route Maintenance

In route discovery route reply would only be generated if message is reached to intended node. To return from route reply destination node must have a route to source node. The route may be destination node route cache. In route maintenance is initiated where by route error packets are generated at the node. The initiator (source) and target (destination) of the route discovery is identified by each route request packet. The source node also provides a unique request identification number in its route request packet. However, if no suitable route is found, target will execute its own route discovery mechanism in order to reach toward the initiator [11].

DSR is designed to restrict the bandwidth which is consumed by control packets in wireless adhoc networks by eliminating periodic table update message requires in table driven approach

IV. IMPLEMENTATION DETAILS

C. Network Design

The Qualnet network simulator is used for the performance evaluation. Th scenario is shown in fig. 1.The simulation is done for 8 nodes in a wireless sensor network scenario.

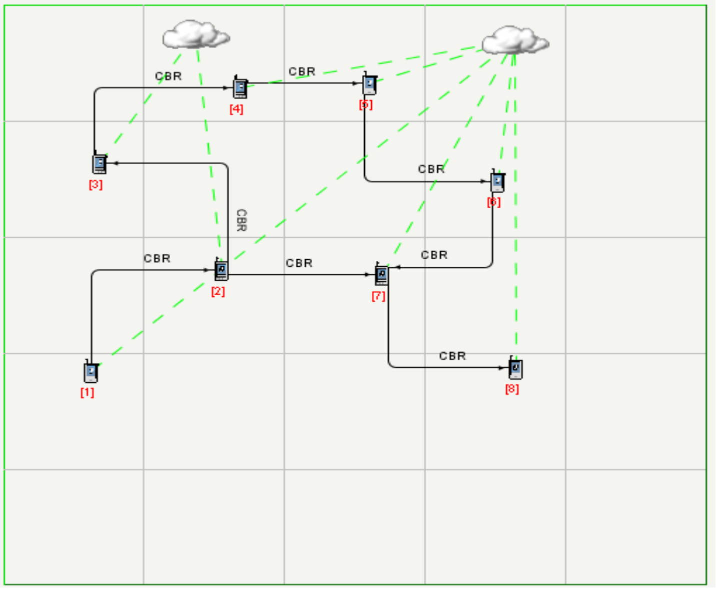

Figure1- Scenario Setup

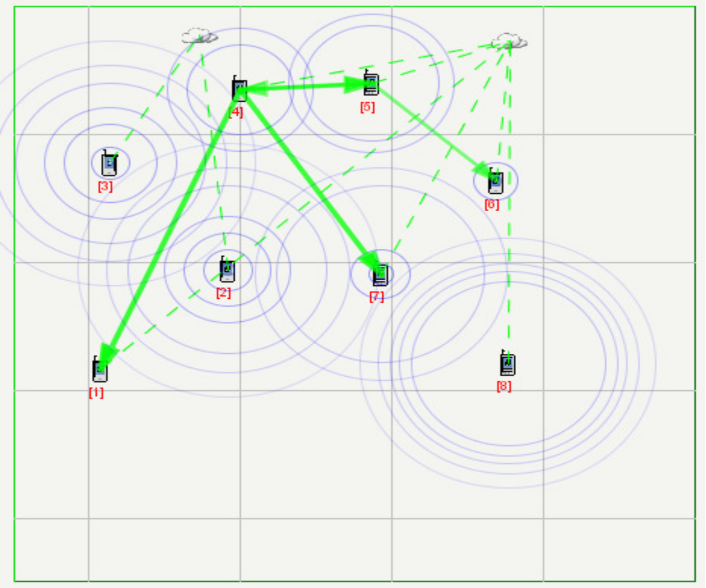

Figure2- Working Scenario

D. Simulation Setup

Parameters	Value
Simulation Time	300 sec
Terrain Dimensions	1500m,1500m
Channel Frequency	2.4 Ghz
Path Loss Model	Two Ray Model
Antenna Type	Omni- directional
Mobility Model	Random- Way Point
Traffic Type	CBR
Data Packets	512 Bytes/Packet
Data rate	2 Mbps
Number of Nodes	8
Type Of Attack	Wormhole
Radio/physical layer	802.15.4

E. Performance metrics

The following performance metrics are considered in analyzing the performance evaluations of routing protocols.

1. *Frames intercepted all-* Number of frames intercepted by the wormhole node.
2. *Frames dropped by wormhole-* Number of frames dropped by the wormhole link (since the frames are classified as data packets, for example, with packet size greater than a threshold).
3. *Frames tunneled-* Number of frames tunneled by the wormhole node. (Frames intercepted multiple times due to repetitive replay will not be tunneled.)

F. RESULT and DISCUSSION

In this the effect of wormhole attack on wireless sensor network can be analyzed on behalf of parameter frame tunneled, frame dropped and frame intercepted.

For AODV routing protocol, the frame that is being dropped by wormhole attack is less as compared to DSR routing protocol. The frame tunneled by wormhole attack is also more in DSR protocol as compare to AODV protocol and is same in case with frame intercepted by attack. The frame intercepted is more in DSR protocol. This shows that the data send by DSR routing protocol is lost.

1. Effect of wormhole attack on AODV routing protocol

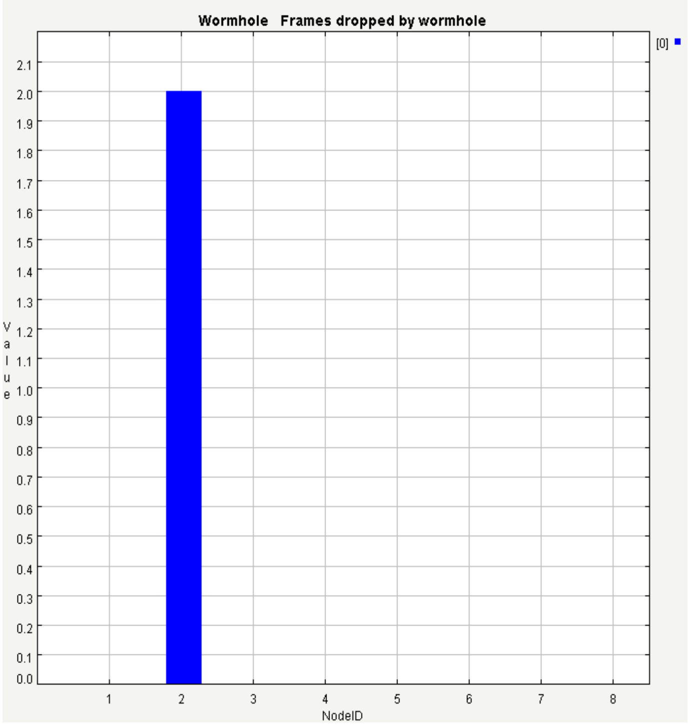

Figure.2(a)- Frame Dropped

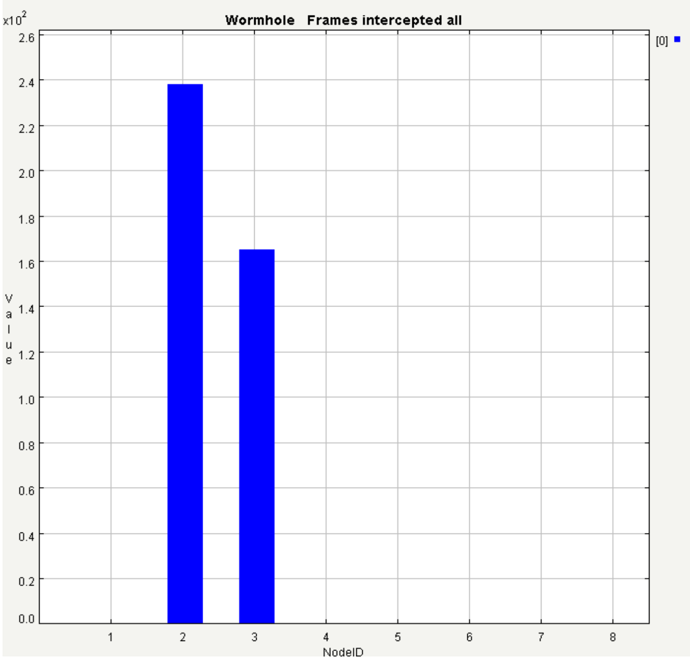

Figure.2(b)- Frame Intercept all

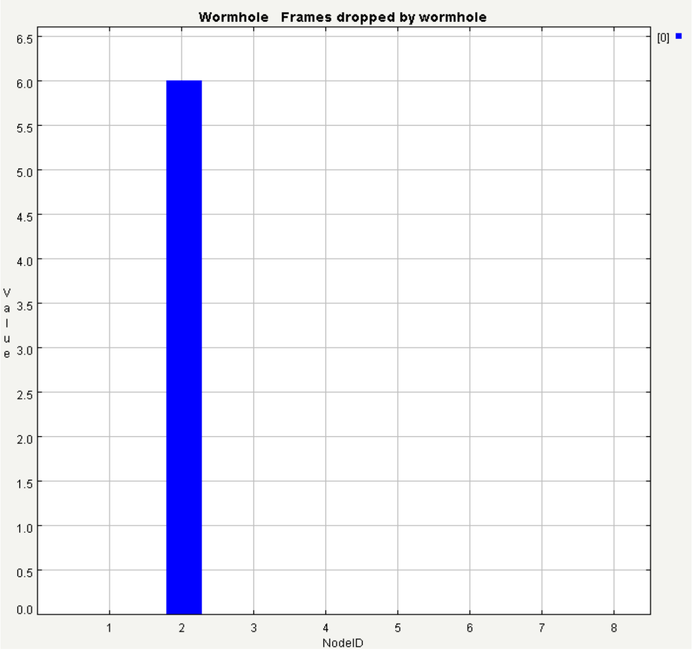

Figure.3(a)- Frame Dropped

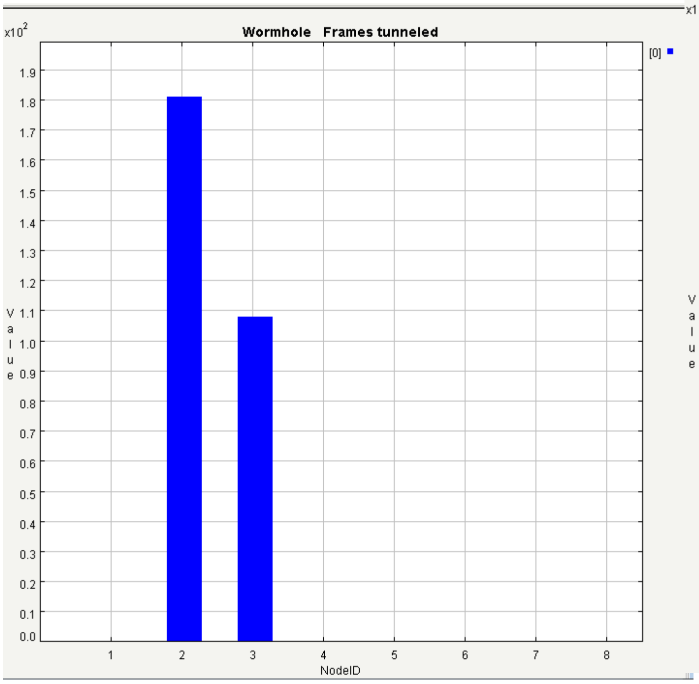

Figure. 2(c)- Frame Tunneled

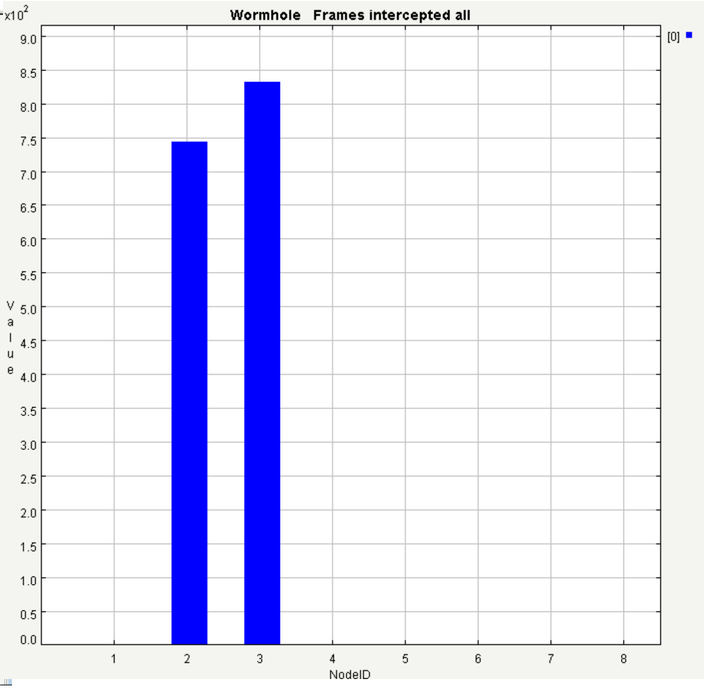

Figure.3(b)- Frame Intercepted all

2. Effect of wormhole attack on DSR routing protocol

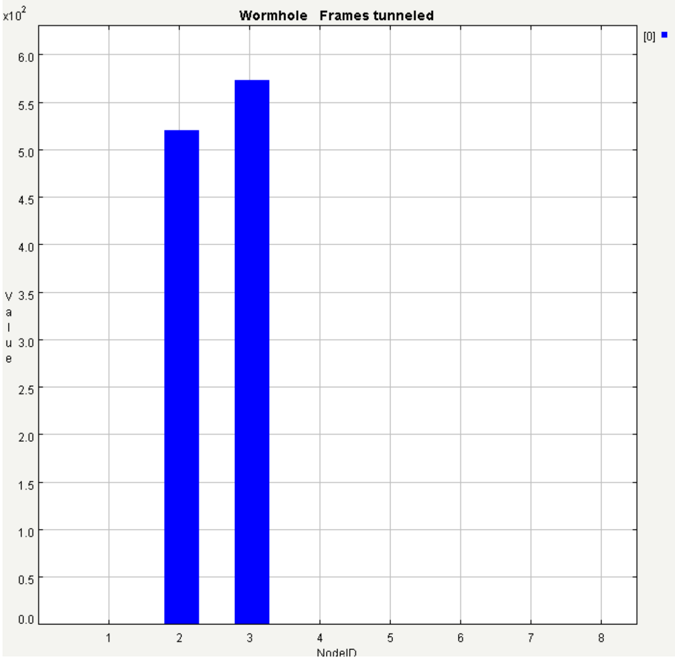

Figure.3(c)- Frame Tunneled

3. The graph shows the variation in the parameter for AODV and DSR routing protocols at different nodes.

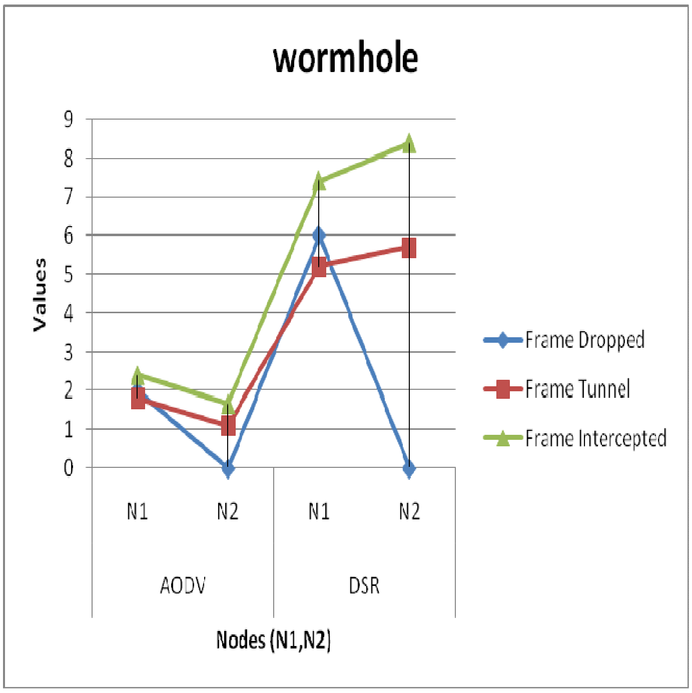

Figure.4- Effect of wormhole attack

V. CONCLUSION

In this paper, impact of wormhole attack on routing protocols has been analyzed. The implementation and simulation of wormhole attack on routing protocols in wireless sensor network is done and evaluated the effect on the data packets being sent in network using qualnet simulator. AODV and DSR routing protocols are used because it is widely used and it is vulnerable to these attacks because of the mechanisms they employs. Parameter like frame dropped, tunnel and intercepted are analyzed. The results show that the presence of wormhole attack affects the data packets being sent by the routing protocol in the wireless sensor network. Finally, it's observed that, DSR is less effective as compared to AODV routing protocol as all the parameters are positive in aodv routing protocol than in DSR protocol. Frame intercepted by wormhole attack is more in DSR routing protocol as compare to AODV protocol as shown in figure 4. So AODV routing protocol is better against wormhole attack in wireless sensor network than DSR protocol. The frame tunnel, dropped and intercept are less in AODV. The AODV protocol is reactive and DSR is proactive in nature.

REFERENCES

[1] D. Estrin et al., "Instrumenting the World with Wireless Sensor Networks," Proc. Int'l. Conf. Acoustics, Speech and Signal Processing, Salt Lake City, UT, May 2001.

[2] H. Chan and A. Perrig, "Security and Privacy in Sensor Net-19 works," IEEE Comp. Mag., Oct. 2003, pp. 103–05.

[3] E. Shi and A. Perrig, "Designing Secure Sensor Networks," Wireless Commun. Mag., vol. 11, no. 6, Dec. 2004 pp. 38–43.

[4] Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003,pp. 26 – 36.

[5] Wang, B-T. and Schulzrinne, H., "An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.

[6] Douceur, J. "The Sybil Attack", 1st International Workshop on Peer-to-Peer Systems ,2002.

[7] Newsome, J., Shi, E., Song, D, and Perrig, A, "The sybil attack in sensor networks: analysis & defenses", Proc. of

the third international symposium on Information processing in sensor networks, ACM, 2004, pp. 259 – 268.

[8] Culpepper, B.J. and Tseng, H.C., “Sinkhole intrusion indicators in DSR MANETs”, Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688.

[9] Devesh Jinwala, “Ubiquitous Computing:Wireless Sensor Network Deployment, Models, Security, Threats and Challenges”,in National conference NCIIRP-2006,SRMIST, pp.1-8,April 2006.

[10] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy,“DAWWSEN:A Defense Mechanism against Wormhole Attacks In Wireless Sensor Networks”, in The Second International Conference on Innovations InInformation Technology,pp. 1-10, 2005.

[11] D. Maltz, “The Dynamic Source Routing Protocol for Multi-Hop Ad Hoc Networks,” Nov 5, 1999. 47.

[12] G. Sklyarenko, “AODV Routing Protocol,” Institut fur Informatik, Freie Universitat Berlin, Berlin, Germany. 2005.