ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

Analysing the effect of Wormhole Attack on Routing Protocol in Wireless Sensor Network

Gurpreet Kaur[1], Er. Sandeep Kaur Dhanda[2]

Student, CSE/IT Department, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib (Punjab), India[1]

Asst. Prof., CSE/IT Department, Baba Banda Singh Bahadur Engineering College, Fatehgarh Sahib (Punjab), India [2]

Abstract: Wireless Sensor Networks consist of large number of sensor nodes with sensing, computation, and wireless communications capabilities. A distributed network of sensor nodes perform critical tasks in many application areas such as target tracking in military applications, detection of catastrophic events, environment monitoring, health applications etc. Security is the main concern in wireless sensor network. The wireless sensor network is vulnerable to different types of attacks that breach the security of the network. The wormhole attack is one of the severe attacks on wireless sensor network. It tunnels the packets from one end to another end by corrupting it. Routing protocols plays a major role of forwarding the data packets by identifying and maintaining the routes in the network. Competence of sensor networks relay on the strong and effective routing protocol used. In this paper, the effect of wormhole attack on routing protocols like AODV, DSR, ZRP and ANODR is analysed on behalf of parameters like throughput, delay and energy consumption.

Keywords: WSN- wireless sensor network, AODV, DSR, ZRP, ANODR

I. INTRODUCTION TO WIRELESS SENSOR NETWORK

The advancements in wireless communication technologies enabled large scale wireless sensor networks (WSNs) deployment. Due to the feature of ease of deployment of sensor nodes, wireless sensor networks (WSNs) have a vast range of applications such as monitoring of environment and rescue missions [1]. To deliver crucial information from the environment in real time it is impossible with wired sensor networks whereas wireless sensor networks are used for data collection and processing in real time from environment [3].. There are two main applications of wireless sensor networks which can be categorized as: monitoring and tracking. Battery powered nodes are a common feature of many WSN applications, where recharging or replacement would not normally be feasible, and so are considered to be disposable. Many methods of powering these devices have been explored, including solar power, but they remain to be seen typically as "one-use" devices [2].

Wireless sensor networks are composed of independent sensor nodes deployed in an area working collectively in order to monitor different environmental and physical conditions such as motion, temperature, pressure, vibration sound or pollutants. The main reason in the advancement of wireless sensor network was military applications in battlefields in the beginning but now the application area is extended to other fields including industrial monitoring, controlling of traffic and health monitoring. Limited constraints such as size and cost results in constraints of energy, bandwidth, memory and computational speed of sensor nodes. The topology of the WSNs can vary from a simple star network to an advanced multichip wireless mesh network. The propagation technique between the hops of the network can be routing or flooding. In WSN, there are various types of attack. The attack [13] is categorized into two types. They are active attack and passive attack. Active attack which disrupts the communication between sender and receiver is easily detected. Passive attack which disrupts the communication between sender and receiver is difficult to identify in the network. The network performance degrades higher level in passive type of attack.

II. ATTACKS ON WIRELESS SENSOR NETWORK

Wireless sensor networks are susceptible to wide range of security attacks due to multichip nature of the transmission medium. Also wireless sensor networks have an additional vulnerability because nodes are generally deployed in an unprotected environment. Although there is no standard architecture of the communication protocol for wireless sensor network, hence there is no need to characterize the possible attacks and security solution in different layers with respect to ISO-OSI model. There are different types of attacks on different layers. Thus WSNs are vulnerable to different network layer attacks such as black hole, grey hole, wormhole etc. the wormhole attack is one of the severe attack on the network.

Wormhole Attack: Wormhole attack is one of the Denial-of-Service attacks effective on the network layer, that can

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

affect network routing, data aggregation and location based wireless security. [6] Wormhole attack is the type of denial of service attack that interrupt routing operations even without the knowledge of encryptions methods The wormhole attack may be launched by a single or a pair of collaborating nodes..Wormhole attack is a severe type of attack on wireless sensor network. In wormhole attack, a pair of attackers creates the tunnels to transfer the data packets and reply them into the network. This attack has a tremendous effect on wireless networks, specially against routing protocols. In type of two ended wormhole. One end tunnels the packet via wormhole link and other end on receiving the packets and reply them to the local area. Wormhole attack does not require MAC protocol information as well as it is immune to cryptographic techniques. [7] 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.

Types of Wormhole attack are as:

1. Wormhole using out of band channel: - In two ended wormhole, a high bandwidth channel is placed between end points to create a wormhole link.
2. Wormhole using packet relay: - one or more malicious nodes create packet-relay-based wormhole attacks. In this type of attack malicious node replays data packets between two far nodes and this way fake neighbours are created.
3. Wormhole using protocol distortion: - In this only one malicious node tries to attract network traffic by distorting protocol. They do not affect the network routing much but it is harmless.

III. ROUTING PROTOCOLS

A routing protocol specifies how router communicates with each other, disseminating information that enables them to select routes between any two nodes on a computer network. Routing algorithms determine the specific choice of route. . A routing protocol shares this information first among immediate neighbours, and then throughout the network. This way, routers gain knowledge of the topology of the network. The term routing protocol may refer specifically to one operating at three layers of OSI model. There are various routing protocols that have been proposed for routing data in wireless sensor networks. The proposed mechanisms of routing consider the architecture and applications along with the characteristics of sensor nodes. There are few routing protocols that are based on quality of service awareness or network flow whereas all other routing protocols can be classified as hierarchical or location based and data centric. 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.

A. AODV Routing Protocol: AODV (Adhoc on Demand Distance Vector) is a reactive protocol [12].The reactive routing protocols do not periodically update the routing table like table driven proactive protocols.It is the modification of DSDV (Destination Sequence Distance Vector). It provides uncast, multicast broadcast. It works on, on demand algorithm. It searches for route between nodes only as decide by source nodes. These routes are maintained as long as they are needed by source. AODV builds route using route request and route reply query cycle. It is the loop free, self starting scale to large number of nodes. AODV is a well known distance vector routing protocol [9] and it works as follows. Whenever a node wants to communicate with another node, it looks for an available path to the destination node, in its local routing table. If there is no path exists, then it broadcasts a route request (RREQ) message to its neighbourhood nodes. Any node that receives this message for route discovery looks for a path leading to the respective destination node.
The important feature of AODV is the maintenance of time based states. This means that routing entry which is not used recently is expired. The intermediate nodes store the route information in the form of route table. Control messages used for the discovery and breakage of route are as follows:
- Route Request Message (RREQ)
- Route ReplyMessage (RREP)
- Route Error Message (RERR)

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 [10].
DSR is designed to restrict the bandwidth which is consumed by control packets in wireless adhoc networks by

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

eliminating periodic table update message requires in table driven approach.

C. ZRP (Zone Routing Protocol): ZRP is an amalgam variety of routing protocol [4]. This is the first routing protocol with reactive and proactive. The zone routing protocol (ZRP) [11] aims to address the problems by combining the best properties of both the proactive and reactive approaches.it was proposed to reduce the control overheads of proactive routing protocol which means that time is wasted on update the routing table and decrease the latency which is caused by route discovery in reactive protocol. The zone routing protocol (ZRP) aims to address the problems by combining the best properties of both the proactive and reactive approaches. [5]. the proactive routing protocol is intra-zone routing protocol (IARP) is used inside routing zones. Reactive outing protocol is inter-zone routing protocol (IERP) is used between routing zones. In proactive a route of source to destination within local zone can be created from sources. If source to destination packet are of same zone then packet can delivered immediately. In reactive the source node sends route request to nodes of the border which contain its own address the destination address and unique sequential no. Each border node check its local zone for destination .If destination is not a member of this local zone then border node add its own address to route request packet and forward packet. If destination is member of local zone then it sends route reply on reverse path back to the source.

IV. SECURE ROUTING PROTOCOLS

Wireless networks are different 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. 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. For Security purposes, a secure routing protocol (ANODR) is used for routing in WSN. For Security purposes, a secure routing protocol (ANODR) is used for routing in WSN.

A. ANODR (Anonymous on-demand Routing (ANODR) Protocol): It is designed to provide a net-centric anonymous and untraceable routing scheme for wireless ad-hoc network. Anonymous On-demand Routing Protocol is designed to provide an anonymous and untraceable routing scheme for wireless ad-hoc networks. It is based on table-driven AODV routing protocol. As in other routing protocols network routes are open to all i.e. packets sent in wireless manner then any adversaries can trace the network route and infer the pattern of the packets that are being communicate between communicating parties. This may pose a serious threat to network. It's a challenging constraint for routing and data forwarding. The ANODR protocol allows you to protect the wireless communication from being traced and without removing your device`s battery. The adversaries should not trace the data packets that are sent by ANODR secure routing protocol. It provides untraceable path for data communication. The threats of being eavesdropped by others are less [8]. ANODR provides the following security services:

1. Negligibility- based on anti-tracing such that signal interceptors cannot trace signal transmitters mobility pattern via wireless signal tracing (with non-negligible probability defined on the victim network's size).

2. Confidentiality and anonymity- The path follow by the packets should not be traced by any adversaries.

3. Traffic flow confidentiality- Conceals the message content through encryption.

4. Identity-free routing- The identity cannot be stole by other.

5. One-time packet contents such that any two wireless transmissions are indistinguishable with each other in regard to a cryptanalyst.

The ANODR configuration is based on AODV parameter settings. ANODR parameters use the same terminology as AODV's parameters, except the name is changed from AODV to ANODR. These services are provided at the Network Layer and Link Layer to protect the IP and link layer protocols.

V. SIMULATION SETUP

Qual Net 4.5.1 Network Simulator tool is used to evaluate the performance of different routing protocols in Wireless sensor networks. In this simulation, we have tested routing protocols with scalability of nodes. The nodes are deployed randomly in a terrain of size 1500 * 1500m. CBR is used as data traffic application with multiple source and destination. It consists of basic network entities as sensor nodes (mobile) and PANS coordinator. The PAN coordinator used is fully functioned and other remaining nodes are reduced function devices having limited constraints like energy, power etc. the wormhole attack is implemented on random number of node in network. The simulation time is 150 seconds. The performance of different routing protocols is analysed on behalf of metrics like throughput, delay and energy consumption. The parameters used in the simulation are summarized in the table below:

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

A. **Simulation Parameters**

Terrain Size	1500*1500
Mobility Model	Random Way Point
Radio/Physical Layer	802.15.4
Energy Model	Micaz
Wormhole Attack	Threshold and All Drop
Speed	30m/s
Routing Protocols	AODV, DSR,ZRP,ANODR
No. of Nodes	10,20,30
Simulation time	150 Sec
Data Traffic Rate	CBR
Parameters	Throughput, Delay, Energy Consumption
Device Type	FFD,RFD

B. **Scenario Design**

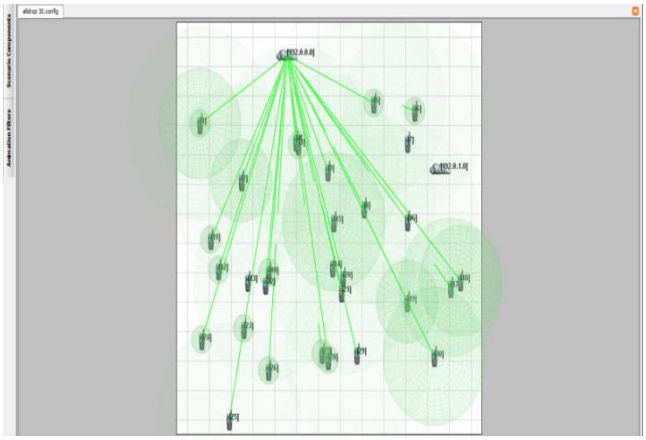

Figure1. 3D analyser Scenario

VI. RESULT AND EVALUATION

We evaluate the effect of wormhole attack on different routing protocols on the basis of metrics like throughput, end-to-end delay and energy consumption in WSN. The attacks effect the routing of the data from source to destination by changing their path or say the routing table information of different protocols. The wormhole attacks works in two different modes namely in threshold and all drop mode. To analyse the performance of the routing protocols by varying the nodes, the metrics used to evaluate the performance are given below.

A. Wormhole threshold technique: In threshold technique the wormhole drops any packet with size greater than or equal to the threshold value.

1. Throughput in bits/sec.

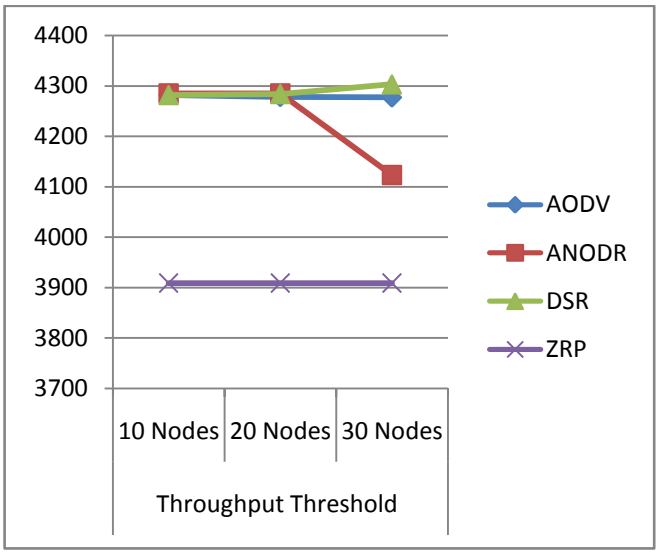

Figure2. Throughput

The above graph shows the variation in throughput of different routing protocols in wsn under wormhole attack. In wormhole threshold technique, the throughput of ZRP routing protocol is very less as compared to other routing protocols and its stable with increase in number of nodes. The throughput of ANODR secure routing protocol is decreasing rapidly when nodes are increased. In ANODR the data is communicated in encrypted format using cryptographic algorithms so its throughput decreases with density. In this throughput of DSR protocol is higher than other protocols. The overall throughput decreases slowly with increase in number of nodes.

2. Delay in seconds

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

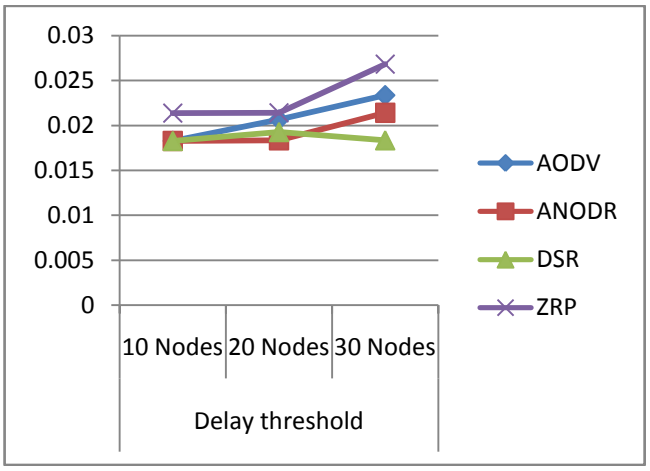

Figure3. End-to-end Delay

The above graph shows the variation in end-to-end delay of different routing protocols in wsn under wormhole attack. In this delay of ZRP routing protocol is higher than other routing protocols and it further increase with increase in number of nodes. The delay of ANODR is less as compared to other routing protocols but more from DSR routing protocol as in this, the delay decreases with density of nodes.

3. Energy consumed in receive mode in mj

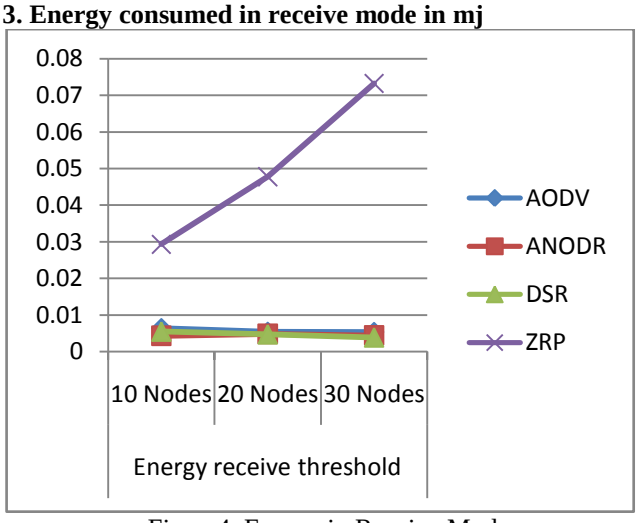

Figure4. Energy in Receive Mode

The above graph shows the variation in the energy consumed by different routing protocols under wormhole attack in energy receive mode. In this ZRP protocol consumes large amount energy in receive mode while other routing protocols consumed nearly equal amount of energy.

4. Energy consumed in transmit mode in mj

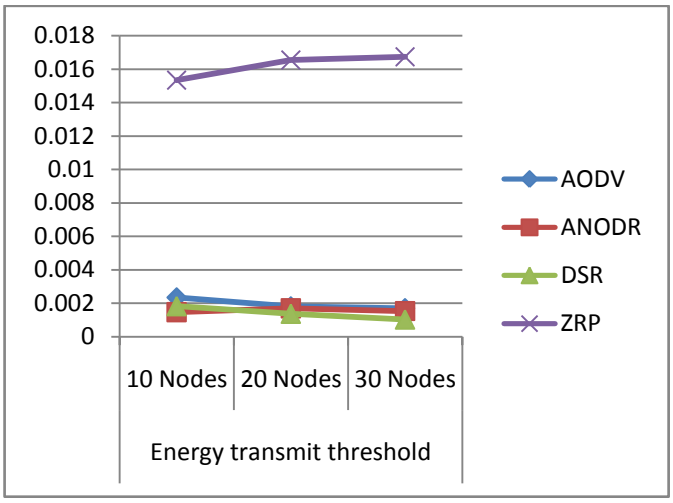

Figure5. Energy consumed in Transmit Mode

In this ZRP routing protocol consumes large amount of energy as compare to other routing protocols and it further increases with increase in number of nodes. The other protocols consumed less amount of energy in transmit mode.

B. Wormhole All drop technique: In this, the infected nodes by wormhole attack can drop all the data packets that it received. The data cannot be sent to the destination node i.e. a sink is created at that infected node that drop all the data packets.

1. Throughput in bits/sec.

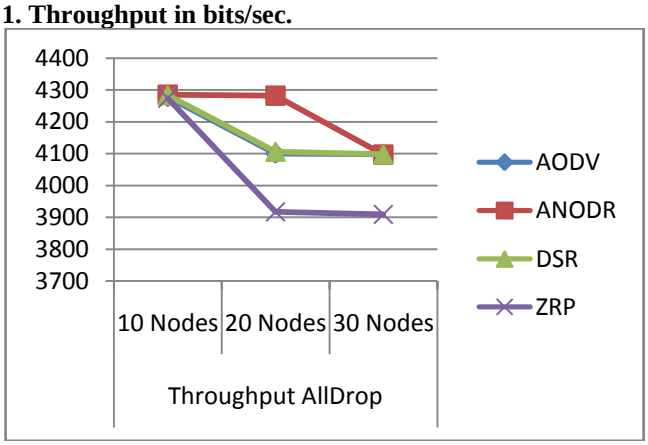

Figure6. Throughput

The above graph shows the variation in the throughput of routing protocols under wormhole all drop technique. In this, the throughput of ZRP routing protocol is very less as compared to other routing protocols. With scalability of nodes it decreases. The ANODR protocol has higher throughput but it also decrease with increase in number of nodes. The AODV and DSR protocols have same throughput and performs identically in the network.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

2. End-to-end Delay in seconds

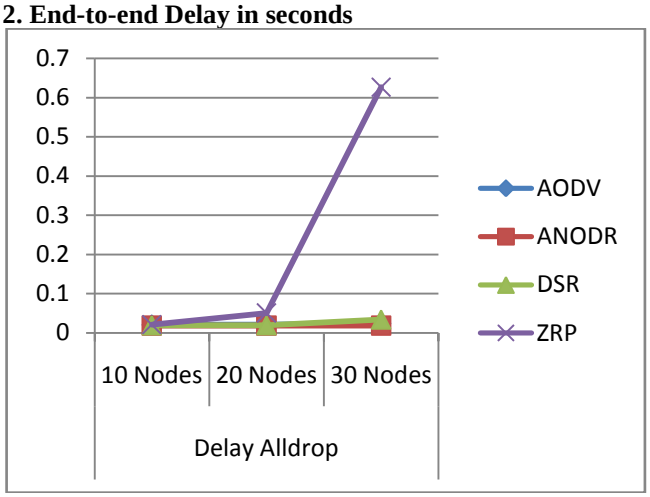

Figure7. End-to-end Delay

The above graph shows the variation in the end-to-end delay of different routing protocols under wormhole all drop technique. In this the end-to-end delay of ZRP routing protocol increases to higher extent as compare to other routing protocols AODV, DSR, and ANODR. The delay increases rapidly with increase in number of nodes.

3. Energy consumed in Receive mode in mj

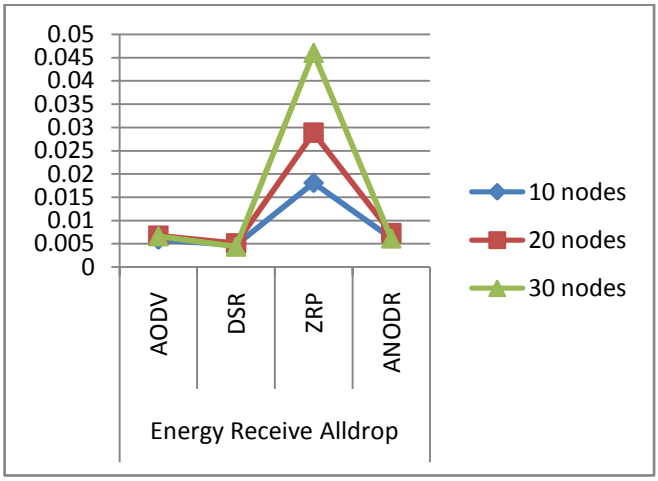

Figure8. Energy consumed in Receive Mode

This graph show the variation in the energy consumed in receive mode by routing protocols. In this ZRP consume more amount energy as compare to other routing protocols. With increase in number of nodes its consumption also increases. The DSR routing protocol consumes less amount of energy than other routing protocols.

4. Energy consumed in Transmit mode in mj

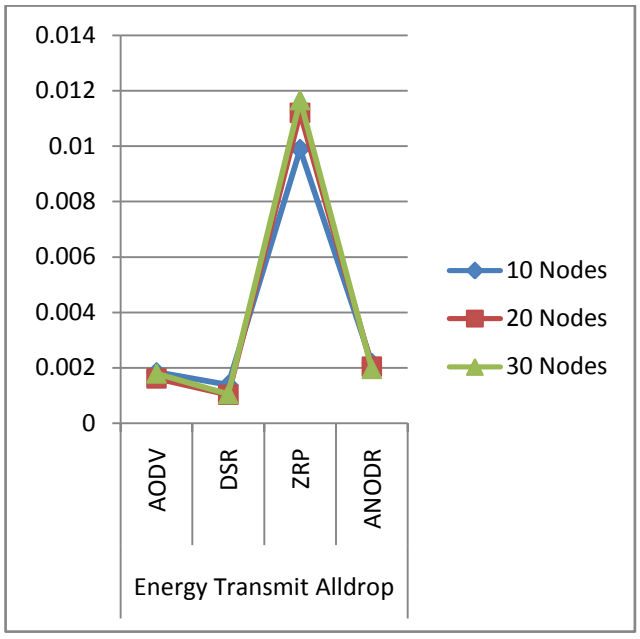

Figure9. Energy in Transmit Mode

In this ZRP routing protocol consumes more energy in transmit mode with increase in number of nodes it consumes more energy while other protocols consumed less amount of energy. The DSR routing protocol consumes less amount of energy in transmit mode.

In energy consumption ZRP protocol consumes more energy in both transmit and receive mode. In transmit mode data is sent from source to destination and in receive mode different nodes receive the data. The DSR routing protocol consumes less amount of energy and it is considered as best in energy consumption.

VII. CONCLUSION

In this paper we present different routing protocols in wireless sensor network and how the attack named wormhole attack can affect the routing. The performance of different routing protocols can be evaluated on the basis of different parameters like throughput, end-to-end delay and energy consumption. Wireless sensor networks have an additional vulnerability because nodes are generally deployed in unprotected environment. Although there is no standard architecture of the communication protocol for wireless sensor network. The throughput of DSR routing protocol under wormhole threshold mode is more than other protocols as shown in fig.2. The ANODR protocol also performs well under threshold mode. The end-to-end delay of DSR protocol is also less as compared to others and ZRP protocol performs worst under wormhole threshold mode as shown in fig.3. The DSR protocol consumes less amount of

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 8, August 2013

energy both in energy consumed in transmit and receive mode as shown in fig. 4 and 5. The ANODR secure protocol also performs well for wireless sensor network under wormhole threshold mode.

In wormhole all drop mode, it drops all data packets so in this the throughput and end-to-end delay of ANODR routing protocol is considered as best as throughput is more and delay is less as compared to other routing protocols. With increase in number of nodes the throughput decreases but no effect on end-to-end delay as shown in fig.6 and 7. The energy consumption of DSR routing protocol is less for both energy transmit and receive mode than other protocols and ANODR protocol consumed nearly equal energy consumption as shown in fig. 8 and9. It is concluded that for wormhole all drop mode ANODR routing protocols is well performed.

REFERENCES

[1] C. Haigaug, W. Huafeng, H. Jinchu and G. Chuanshan, "Event-based Trust Framework Model in Wireless Sensor Networks", In the proceedings of the IEEE International Conference on Networking, Architecture and storage,June. 2008.

[2] J. Jeong, X. F. Jiang and D. E. Culler, "Design and Analysis of Micro-Solar Power Systems for Wireless Sensor Networks", Electrical Engineering and Computer Sciences, University of California at Berkeley, 2007.

[3] M. Ismail, M.Y. Sanavullah, "Security topology in wireless sensor network with routing optimization", In proceeding in International Conference on Wireless Communication and Sensor Networks, Dec 2008.

[4] Subramanya Bhat M., Shwetha.D., Devaraju.J.T, "A Performance Study of Proactive, Reactive and Hybrid Routing Protocols using Qualnet Simulator", International Journal of Computer Applications, Vol. 28, August 2011.

[5] Jogendra Kumar, "Performance Analysis of Energy Efficient Routing Zone Routing Protocol over AODV and DSR Routing Protocols on CBR, Research and Reviews", Journal of Engineering and Technology ,vol.1, December 2012.

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

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

[8] Jiejun Kong, Xiaoyan Hong, "ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks", ACM, 2004.

[9] T.Taleb, E.Sakhaee, A. Jamalipour, K.Hashimoto, N. Kato, Y. Nemato, "A stable routing protocol to support its services in vanet networks" IEEE Transactions on Vehicular Technology, November 2007.

[10] D.Johnson, D.Maltz, Yih, 2003. "Dynamic Source Routing Protocol for Mobile AdHoc",http://www.ietf.org/internet-drafts/ draft ietf manet-DSR-09.txt, IETF Internet draft.

[11] SreeRangaRaju, Jitendranath Mungara. 2010.
"Performance Evaluation of ZRP over AODV and DSR in Mobile Adhoc Networks Using Qualnet" European Journal of Scientific Research, Vol. 45.

[12]Kamini, Rakesh K "VANET Parameters and Applications: A Review", Global Journal of Computer Science and Technology, September 2010.

[13] Majidmeghdadi, Suatozdemir, Inangiller, "A Survey On wormhole based attacks and their countermeasures in wireless sensor networks",IETE Technical Review, VOL 28, ISSUE 2, 2011.

BIBLIOGRAPHY

Gurpreet Kaur is currently pursuing M.Tech in CSE(E-Security) in BBSBEC, Fatehgarh Sahib, Punjab, India. Her research area is Attacks in Wireless sensor network.

Er. Sandeep Kaur Dhanda is currently serving as Assistant professor in Computer Science and Engineering at BBSBEC, Fatehgarh Sahib, Punjab, India. Her research area is parallel computing.