www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2. Issue 11 Nov.2013 Page No. 3346-3351

Performance Analysis of ANODR and ZRP protocol against Wormhole attack in Wireless Sensor Network

Er. Gurjot Singh

Baba Banda Singh Bahadur Engineering College,
Fatehgarh Sahib, Punjab, India

Abstract: ***Wireless sensor network consist of spatial distributed sensor nodes deployed in a hostile and dense environment to gather information and propagate it to the base station for further processing. In the insecure wireless transmission medium, the enemies can analysis the data traffic against intercept-able routing information embedded in routing data packets. Allowing adversaries to trace network routing information and other critical information at the end of those routes may pose a serious threat to covert operations. Wireless sensor network has limited resources like bounded storage space, energy and computation power. In this paper, to prevent the network from wormhole attack, the ANODR, an anonymous on-demand routing protocol is implemented. The wormhole attack is one of the severe attack on WSN that can effect the networks performance. In this, attackers create a low-latency link between two points in the network. The wormhole attack tunnels the packets from one end to another end by modifying or altering its content. For route anonymity problem, the ANODR prevents strong adversaries from tracing a packet flow back to its originator and for location privacy problem, ANODR ensures that adversaries cannot discover the real identities of authenticated transmitters. The architecture of ANODR is based on technique named "broadcast with trapdoor information". The qualnet 4.5.1 simulator is opted to analyze the performance of ANODR on the basis of metrics like frame tunneled, frame dropped and intercepted.***

Keywords- *Wormhole attack, WSN, ANODR, ZRP*

1. Introduction to WSNs

When Wireless sensor network are composed of a large set of homogeneous nodes with extreme resource constraints. Each sensor node has wireless communication capability plus some level of intelligence for signal processing and data networking. These nodes are usually scattered over the area to be monitored to collect data, process it, and forward it to a central node for further processing. Military sensor networks might detect and gather information about enemy movements of people and equipment, or other phenomena of interest such as the presence of chemical, biological, nuclear, radiological, explosive materials. WSNs can support a myriad of uses including military, commercial, environmental, and medical applications. Natural environments such as remote ecosystems, disaster sites, endangered species, agriculture conditions, and forest fires can also be monitored with sensor networks[1].

Sensor networks are small, low-cost, low-power devices with the following functionality: they communicate over short distances, sense environmental data, and perform limited data processing. A typical node might have only 4MHz of processing power, 4KB of RAM, and a short transmission distance of less than 100 feet. Tiny OS is a small, open-source operating system developed to support most WSN applications. Wireless sensor networks often contain one or more sinks that provide centralized control. A sink typically serves as the access point for the user or as a gateway to another network. The sensor nodes communicate using RF, so broadcast is the fundamental communication primitive[2]. Security is one of the most difficult problems facing these networks. For certain applications of sensor networks, like military applications, security becomes very important. First, wireless communication is difficult to protect since it is realized over a broadcast medium. In a broadcast medium, adversaries/attackers can easily intercept, inject, and alter transmitted data or information. Second, sensor networks are deployed in a variety of insecure environments so the adversaries can easily steal nodes, recover their cryptographic material and behave as authorized nodes in the network. Third, the sensor networks are vulnerable to resource consumption attacks. Attackers can repeatedly send data packets to drain a node battery and waste network bandwidth. In these security sensitive deployments, secure transmission of sensitive information over the sensor network is essential. The use of encryption and authentication algorithms are primitives between two sensor devices and it requires an initial link key establishment process, which must satisfy the low power and low complexity requirements[3, 4].

1.1. Threats to wireless sensor network

In order to appreciate the challenge of securing a WSN against attack, it is necessary to consider the possible threats to its security. There are a large and increasing number of threats and attacks to which WSNs are susceptible. They can be broadly classified as attacks against the privacy of the network data, denial of service (DOS) attacks, impersonation or replication attacks and physical attacks.[5] In addition to the types of attack, it is also worth considering that attacks can be launched at any point in the network. The wormhole attack can be described as follow:

1.1.1. Wormhole Attack

Wormhole attack is one of the severe Denial-of-Service attack on the network layer, that can affect the data routing, data aggregation and localization dependent wireless security. [6] The wormhole attack may be launched by a single or a pair of nodes. In two ended wormhole, one end overhears the data packets and forwards them through the tunnel to the other end/ destination, where the packets are replayed to local area or network. For tunneled distances longer than the normal wireless transmission range of a single hop, it is easy for the attacker/ adversaries to make the tunneled packet arrive with better metric than a normal multihop route. In case when they only forward all the data packets without altering the content in them, they boost up the transmission in the network than the normal one. In majority of the cases, it either drops or selectively forwards the data packets leads to the network disruption. The wormhole attack does not require MAC protocol information and also 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 techniques simply detect the presence of wormhole in the network, while other approaches also focus on avoiding or preventing the wormhole attack. Mostly techniques require additional hardware support, time synchronization and localization information or may be confined to specific routing algorithm. Wormhole attack are simple to deploy but it may cause significant damage to network [8].

- **Wormhole using out-of-band channel**

In this, two-end wormhole, a dedicated out-of-band high bandwidth channel is placed in between end points to create a wormhole link [10].

- **Wormhole using packet encapsulation**

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

- **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 through it.

- **Wormhole using Packet Relay**

In this, only one malicious node is needed that replays packets between two far nodes and this way fake neighbors of the original nodes are created.

- **Wormhole using Protocol Deviation**

The adversary node formed the wormhole by forwarding data packets without backing off unlike a legitimate node can done thus, increases the possibility of wormhole path getting selected [10].

2. Secure Routing Protocol

Wireless networks are different from other contemporary communication and wireless ad hoc networks routing is a very challenging task in WSNs. For the deployed constrained sensor nodes it is impractical to build a global scheme for them. Mostly the applications of sensor networks have the requirement of transmitting 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 aspect in mind, 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 [9].

1. 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 severe threat to network and 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 [11]. 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 follows 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 [9].

3. Related Work

Dr.G.Padmavathi, Dr.P.Subashini and Ms.D.Devi Aruna [16] had proposed protocol ANODR- ECC with Telnet provide application layer security and it ensures route anonymity and location privacy and is robust against eavesdropping attack.For route anonymity, it prevents strong adversaries from tracing a packet flow back to its source or destination; for location privacy, it ensures that adversaries cannot discover the real identities of local transmitters. The simulation is done using network simulator qualnet 5.0 for different number of mobile nodes. The proposed model has exposed improved results in terms of Average throughput, Average end to end delay, Average packet delivery ratio and Average jitter.

Hyeon Myeong Choi, Su Man Nam, Tae Ho Cho [17] had proposed a secure routing method for detecting false report injections and wormhole attacks in wireless sensor networks. The proposed method uses ACK messages for detecting wormholes and is based on a statistical en-route filtering (SEF) scheme for detecting false reports. Simulation results show

that the proposed method reduces energy consumption by up to 20% and provide greater network security.

Annie Jesus, Suganthi Rani.A and R.Mathan [18] had presented a protocol named USOR. It is an Unobservable Secure On-demand Routing protocol for mobile ad hoc network that achieves unlinkability and unobservability by employing anonymous key establishment based on group signature. There is no security provision against the wormhole and black hole attacks in existing USOR protocol. AODV, USOR and modified USOR are implemented on ns2, and there performance is evaluated.

Varsha Sahni, Vivek Thapar and Bindiya Jain [19] had evaluated the affects of wormhole attack on performance of AODV and DSR routing protocols on varying node mobility. WSN's protocol has different security flaws and using these flaws many kind of attack possible on wireless sensor -network. Wormhole is one of these attacks. Wormhole attack causes serious affect on performance of the WSN protocol and preventing the attack has proven to be very difficult. This paper illustrates how wormhole attack affects performance of routing protocol in wireless sensor network using random waypoint mobility model with varying node mobility. They also analyze the effectiveness of WEP and CCMP security protocol against wormhole using DSR and AODV protocol.

Syed Basha Shaik and S. P. Setty [20] had analyzed the performance of AODV, DSR and ANODR in Grid placement model is evaluated for different network sizes, using QualNet5.0.2 simulator. The significance of network size for the performance of AODV, DSR and ANODR protocols is studied. From results they can conclude that at less network sizes all the protocols in Grid placement give encouraging results. DSR is giving higher throughput and packet delivery ratio for all network sizes when ANODR giving less average jitter and end-to-end delay.

4. Simulation Setup

To evaluate the performance of ANODR in wireless sensor network the QualNet 4.5.1 Network Simulator tool is used. In the simulation scenario, the nodes are deployed randomly in a terrain of size of 1500*1500m. CBR is used as data traffic application with multiple source and destination. To configure the application and for mobility of nodes profile configuration, application configuration objects are included in scenario. It consists of basic network entities as sensor nodes (mobile) and PAN coordinator. The PAN coordinator used is fully functioned and other remaining nodes are reduced function devices having limited constraints like storage, energy and power. The wormhole attack is implemented on random number of node in network. The security schemes ANODR is implemented on sensor network against wormhole attack. The performance is measured on the basis of metrics like frame dropped, frame tunneled and intercepted. The simulation time is 200 second. For simulation the different parameters are set are shown in table 1:

Terrain Size	1500*1500
Simulation Time	200sec
Radio/Physical Layer	802.15.4
No. of Nodes	50
Secure Routing Protocol	ANODR
Attack	Wormhole attack (Threshold
Traffic Type	CBR
Routing Protocol	ZRP
Energy Model	Micaz
Mobility Model	Random Waypoint
Device type	PAN coordinator, ffd and rfd

Table 1. Simulation parameters setup for QualNet simulator

1. Simulation Scenario

The nodes are placed randomly on terrain of size 1500* 1500m. There are total 20 nodes placed on terrain. One wireless cloud is placed on the terrain has configured to 802.15.4. All the nodes are link wirelessly with the wireless subnet cloud except the two nodes named 7 and 13 as shown in figure 1. The nodes 7 and 13 are link to other wireless subnet cloud have configure to wormhole attack. The nodes are made mobile nodes that move randomly on the terrain. CBR is used as data traffic application with multiple source and destination. Then secure protocol ANODR is configured on all the nodes and simulation is run for 200 seconds i.e. the simulation time. The working of simulation is shown in figure 2.

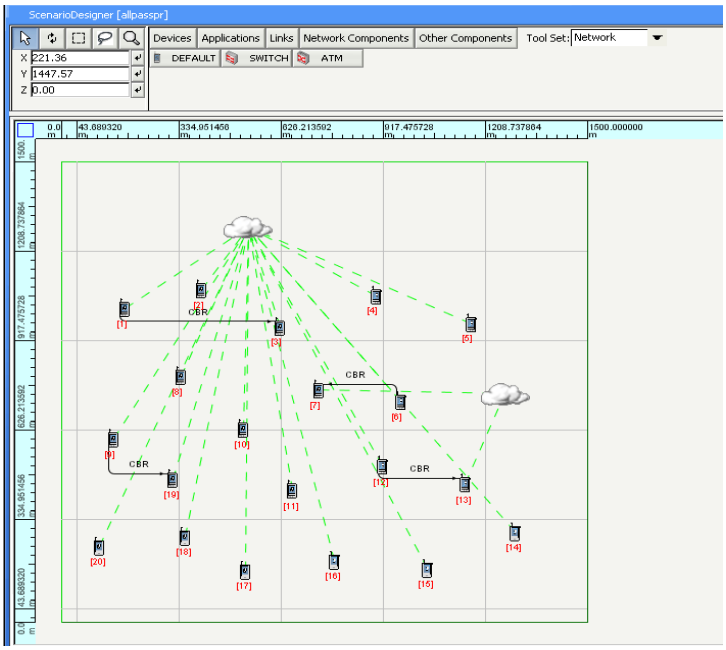

Figure 1. Simulation Scenario setup

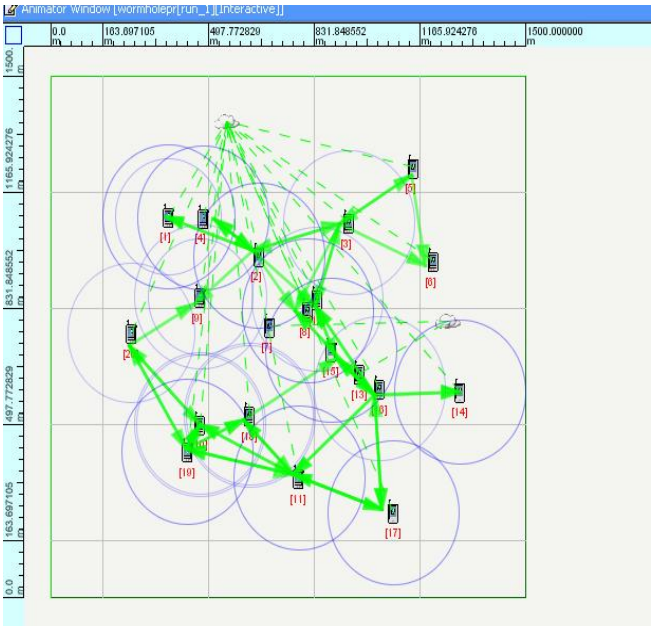

Figure 2. Working of Simulation Scenario

2. 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.)

5. Result and Discussion

This section evaluates the performance of ANODR protocol against wormhole attack in wireless sensor network. After describing our implementation and simulation setup, it has been evaluate how ANODR defends the wormhole attack in WSNs. The performance is evaluates on the basis of metrics like frame tunneled, frame dropped and intercepted.

A. ZRP Routing Protocol- Zone Routing Protocol (ZRP) [12] combines the benefits of pro-active discovery inside node's limited neighborhood (Intra Zone Routing Protocol (IARP)) [13], and also uses a reactive protocol for interaction among neighborhoods. The Broadcast Resolution Protocol (BRP) is used to forward route request. ZRP partitions the complete network in many zones. This protocol is classified as a flat protocol due to overlapping of zones. As a result network congestion can be reduced and optimal routes can be detected. [14, 15].

1. Frame Dropped-

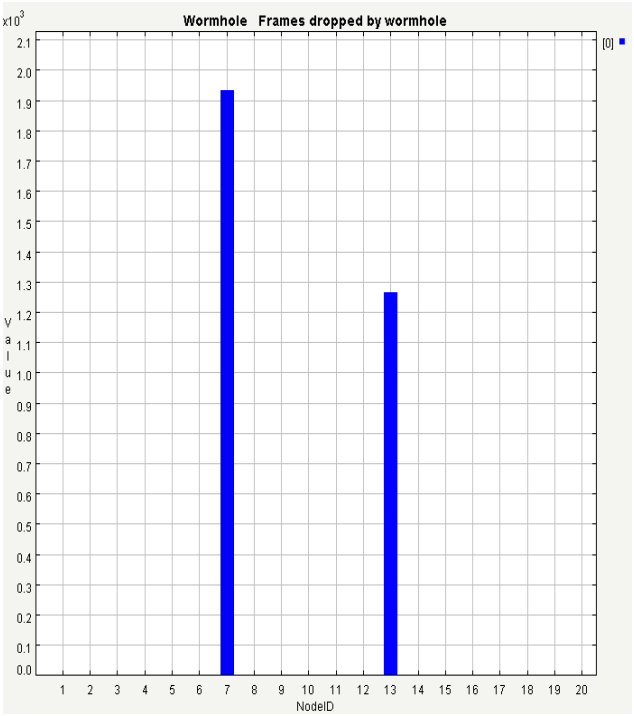

Figure 3. Frame dropped by wormhole

2. Frame Intercept-

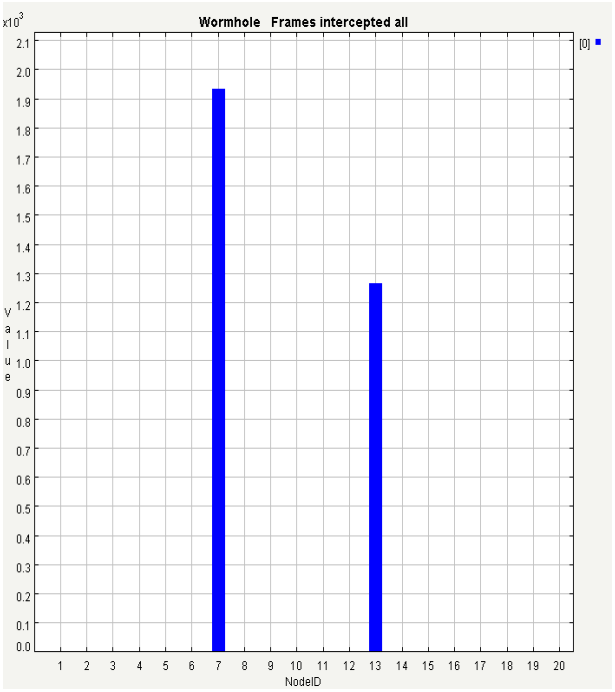

Figure 4. Frame intercept all

3. Frame tunneled by wormhole attack

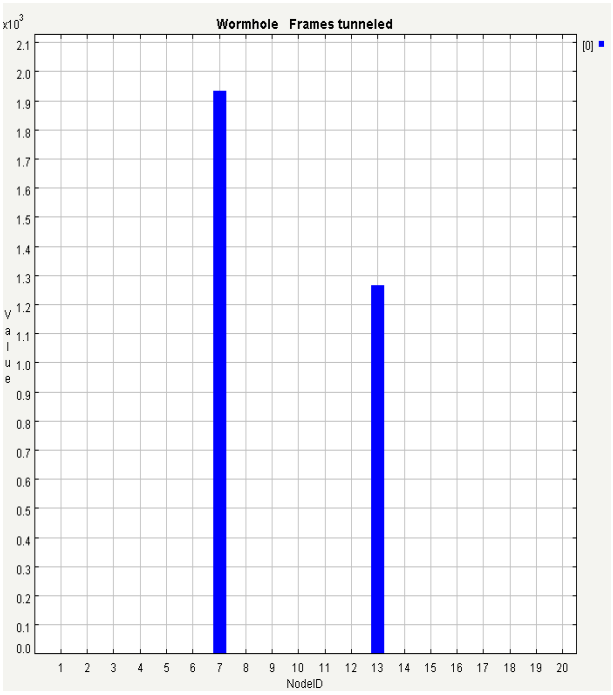

Figure 5. Frame tunneled by wormhole

The above figures 3, 4 and 5 shows the performance of ZRP routing protocol under wormhole attack. The values of frame dropped, frame tunneled and intercept by wormhole attack under ZRP protocol is 1933 at node number 7 and 1265 at node number 13.

B. ANODR protocol- It is designed to provide a net-centric anonymous and untraceable routing scheme for wireless ad-hoc network. It is based on table-driven AODV routing protocol.

1. Frame Dropped-

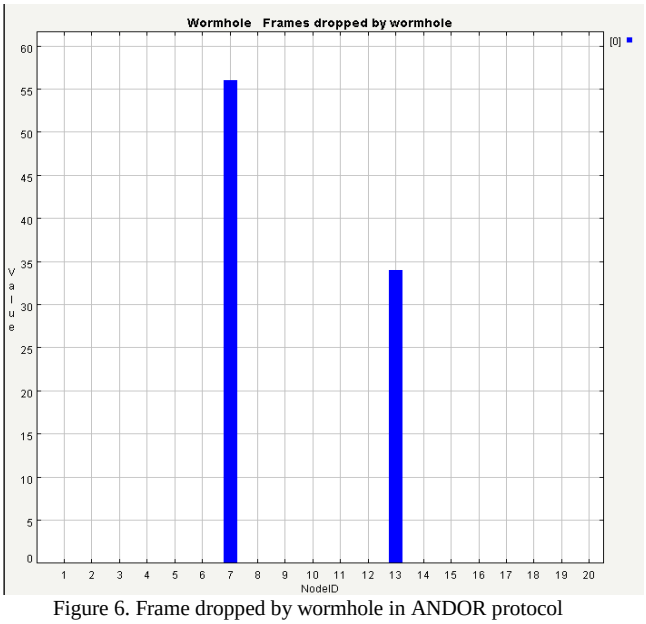

Figure 6. Frame dropped by wormhole in ANDOR protocol

2. Frame Intercept-

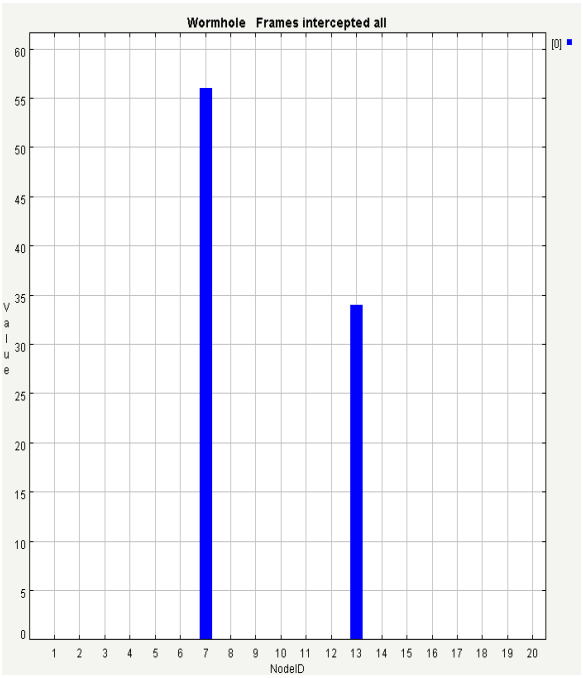

Figure 7. Frame intercept all in ANODR protocol

3. Frame Tunneled-

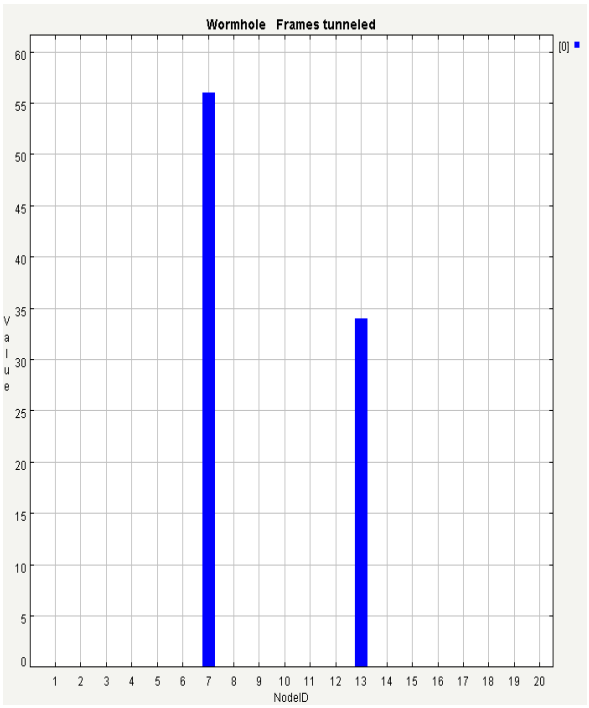

Figure 8. Frame tunneled by wormhole in ANODR protocol

The above figures 6, 7 and 8 shows the performance of ANODR secure routing protocol under wormhole attack. The values of frame dropped, frame tunneled and intercept by wormhole attack under ZRP protocol is 56 at node number 7 and 34 at node number 13. The table 1 shows the total number of frame that are effected by wormhole attack.

Table 2- Total frame drop, tunnel and intercept by wormhole attack in ZRP and ANODR protocols

6. Conclusion

In this paper, the performance of ANODR secure routing protocol is analyzed with comparison to other routing protocol i.e. ZRP. 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. 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, ZRP routing protocol is less effective as compared to ANODR secure routing protocol as all the parameters are positive in ANODR routing protocol than in ZRP routing protocol. Frame intercepted by wormhole attack is more in ZRP routing protocol as compare to ANODR secure protocol as shown in figure. So ANODR routing protocol is better against wormhole attack in wireless sensor network than ZRP routing protocol. The ZRP routing protocol is hybrid protocol, the combination of reactive and proactive routing protocols and the ANODR configuration is based on AODV routing protocol. It is designed to provide a net-centric anonymous and untraceable routing scheme for wireless sensor network. The ANODR protocol allows you to protect the wireless communication from being traced and without removing your device's battery.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey", Computer Networks Journal, Elsevier Science, Vol. 38, No. 4, pp 393– 422, March 2002.

[2] J. M. Kahn, R. H. Katz, and K.S. Pistcr, Mobile Networking for Smart Dust, ACM/IEEE International Conference on Mobile Computing (MobiCom '99), Seattle, WA, 1999, 217 – 278.

[3] J. Staddon, D. Balfanz, and G. Durfee. "Efficient tracing of failed nodes in sensor networks", Proc. of the first ACM International workshop on Wireless sensor networks and applications (WSNA), ACM Press, 2002, 122-130.

[4] Ritu Sharma, Yogesh Chaba, Yudhvir Singh, "Analysis of Security Protocols in Wireless Sensor Network", Int. J. Advanced Networking and Applications Volume: 02, Issue: 03, Pages: 707-713 (2010)

[5] David Boyle, Thomas Newe," Securing Wireless Sensor Networks: Security
Architectures", JOURNAL OF NETWORKS, VOL. 3, NO. 1, JANUARY 2008, pp. 65- 77.

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

[7] 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 In Information Technology, pp. 1-10, 2005.

[8] Er. Gurjot Singh, Er. Gurpreet Kaur, "Analyzing the Impact of Wormhole Attack on Routing Protocol in Wireless Sensor Network on Behalf of packet tunnel, dropped and intercepted", International Journal of Engineering Development and Research, Vol.1 No.1, PP. 42- 48, 2013.

[9] Gurjot Singh and Sandeep Kaur Dhanda, "Performance Analysis of Security Schemes in Wireless Sensor Network", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue. 8, pp. 3217- 3223, 2013.

[10] Gurpreet Kaur and Sandeep Kaur Dhanda, "Analyzing the effect of wormhole attack on routing protocols in Wireless Sensor Network", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2, Issue. 8, pp. 3217- 3223, 2013.

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

[12]Haas, Z.J., Pearlman, M.R. and Samar, P., "Intrazone Routing Protocol (IARP)," IETF Internet Draft, draft-ietfmanet-iarp- 02.txt, July 2002.

[13] Zygmunt J. Haas Marc R.Pearlman and Prince Samar, "The Zone Routing Protocol for Adhoc Networks", draft-ietf- manet-zone-zrp-04.txt, July 2002.

14] Haas, Zygmunt J., Pearlman, Marc R.: The Performance of Query Control Schemes for the Zone Routing Protocol, August 2001, IEEE/ACM Transactions on Networking, Vol.9, No. 4.

[15] I. Sumaiya Thaseen, K. Santhi, " Performance Analysis of FSR, LAR and ZRP Routing Protocols in MANET", International Journal of Computer Applications (0975 – 8887) Volume 41– No.4, March 2012.

[16] Dr.G.Padmavathi, Dr.P.Subashini and Ms.D.Devi Aruna, "ANODR-ECC Key Management protocol with TELNET to secure Application and Network layer for Mobile Adhoc Networks", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[17] Hyeon Myeong Choi, Su Man Nam, Tae Ho Cho, "A Secure Routing Method for Detecting False Reports and Wormhole Attacks in Wireless Sensor Networks", Wireless Sensor Network, 2013, 5, 33-40.

[18] Annie Jesus, Suganthi Rani.A and R.Mathan, " An Unobservable Secure Routing Protocol against Wormhole and Black hole Attacks in MANET", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 2, Issue 3, March 2013.

[19] Varsha Sahni, Vivek Thapar and Bindiya Jain, "Security Implications of Ad-hoc Routing Protocols against Wormhole Attack using Random Waypoint Mobility Model in Wireless Sensor Network", International Journal of Computer Science and Information Security, Vol. 9, No. 11, November 2011.

[20] Syed Basha Shaik and S. P. Setty, "Performance Comparison of AODV, DSR and ANODR for Grid Placement Model", International Journal of Computer Applications (0975 – 8887) Volume 11– No.12, December 2010.