INVESTIGATION ON WSN ROUTING PROTOCOL IN IEEE802.15.4 BASED WSN UNDER WORMHOLE ATTACK

T. Karthikeya, P. Manimegalai

Dept. of ECE, Karpagam Academy of Higher Education, Coimbatore, India. vtkarthi18@gmail.com, manimegalai.vairavan@gmail.com

ABSTRACT

Wireless sensor networks (WSNs) is one of the most challenging technologies with many application ranging from health care to military applications. In many important military and commercial applications, it is critical to protect a sensor network from malicious attacks. One of these attacks which is hard to detect and mitigate is wormhole attack which presents a demand for strengthen the security mechanisms in the network. In this paper, the performance of zigbee based wireless sensor networks using routing protocols with wormhole attacks has been investigated. This Paper illustrates how wormhole attacks can affects the performance of Ad hoc On-Demand Distance Vector (AODV) routing protocol, Optimized Link State Routing (OLSR) and Zone Routing Protocol (ZRP) in zigbee based WSN by using Qualnet Simulator 5.0. The metrics used to analyse the performance of routing protocol of WSNs are throughput, Average end-to-end delay and total energy consumption of sensor network.

Keywords — Routing protocols, AODV, OLSR, ZRP, wormhole attack, throughput, IEEE 802.15.4.

I. INTRODUCTION

Wireless sensor network is one of the most growing technologies for sensing and performing the different tasks. Such networks are beneficial in many fields, such as environmental control, military, industries, health monitoring, etc. However, these networks are easily prone to malicious nodes and physical attacks due to its deployment in hostile environment, distributed nature, multi-hop communications and untrusted broadcast transmission media. Security is a fundamental requirement for these networks. Sensor networks are particularly vulnerable to several key types of attacks. Attacks [1] can be performed in a variety of ways, particularly Denial-of-Service (DOS), jamming, flooding, eavesdroping, node tampering and hole attacks.

In WSN, many routing protocols are vulnerable to security attacks like wormhole, sink hole, black hole and other attacks [2,3,4]. A wormhole attack is one of the severe attacks in WSN and adhoc networks 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 receives packets at one location in the network, tunnels them to another location and retransmits them there into the network. tunnels them to another location and retransmits them into the network. The wormhole attack can form a serious threat in wireless networks, especially against many routing protocols of WSN. In this paper an attempt has been made to compare the performance of different routing protocols such as AODV, OLSR and ZRP with wormhole attacks in IEEE802.15.4 based WSN.

The rest of the paper is structured as follows. Section II describes the overview of reactive, proactive and hybrid routing protocols. In Section III, Wormhole attacks have been discussed. Section IV and V discusses about the Simulation environment and results. Finally, a conclusion summarizes the paper.

I. ROUTING PROTOCOLS

A. Reactive Routing Protocol: The AODV routing protocol [5] is intended for Mobile Ad hoc NETwork (MANET) and sensor networks. AODV is a reactive routing protocol [5]. It uses an on-demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. AODV has two basic operations: route discovery and route maintenance. AODV uses Route Request (RREQ), Route Reply (RREP) and Route ERR or (RERR) messages to find and maintain the routes. In route discovery, when a source node requires a route to the destination node for which it does not have a route, it broadcasts a RREQ packet in the network. An RREQ packet includes source IP address, destination IP addr-e ss, source sequence number, destination sequence number, request ID, and hop count

If a node receives a route request that has the same source address and request ID fields as in previous route request packets, it discards the packet. Otherwise it checks if there is an entry in its routing table for the destination address. If there is that address, then the destination sequence number in the table is compared to the destination in its routing table, and if it cannot reach the destination through that route, it increments the destination sequence number and sends a route request. Therefore, the destination sequence number indicates the route freshness. If a router has an entry for the destination in its table, and the sequence number for the request is lesser than the sequence number for the destination in its table, and the sequence number for the request by the router is fresher than the one known by the router that sends the request. In this case the receiver sends a RREP. The RREP is forwarded back to the source node through the route where the request is received. In route maintenance, when a link breakage in an active route is detected, the node notifies this link breakage by sending a RERR message to the source node. The source node will reinitiate the route discovery process if it still has data to send.

B. Proactive Routing Protocol: OLSR is a proactive routing protocol [6] optimized for mobile ad hoc networks, which can also be used for WSN. The protocol inherits the stability of a link state algorithm which uses hello and Topology Control (TC) messages to discover and then disseminate link state information

throughout the network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths.

OLSR minimizes the overhead from flooding of control traffic by using only selected nodes, called Multipoint Relay (MPR), to retransmit control messages. This technique significantly reduces the number of retransmissions required to flood a message to all nodes in the network.

Secondly, OLSR requires only partial link state to be flooded to provide shortest path routes. The minimal set of link state information required is, that all nodes, selected as MPRs, must declare the links to their MPR selectors. Additional topological information, if present, may be utilized e.g., for redundancy purpose. OLSR may optimize the reactivity to topological changes by reducing the maximum time interval for periodic control message transmission.

Furthermore, as OLSR continuously maintains routes to all destinations in the network, the protocol is beneficial for traffic patterns where a large subset of nodes are communicating with another large subset of nodes, and where the [source, destination] pairs are changing over time. The protocol is particularly suited for large and dense networks, as the optimization done using MPRs works well in this context.

C. Hybrid Routing Protocol: ZRP is a hybrid wireless networking routing protocol [7] that uses both proactive and reactive routing protocols when sending information over the network. ZRP was designed to reduce the control overhead of proactive routing protocols and decrease the latency caused by routing discovered in reactive routing protocols.

ZRP is formed by two sub protocols, a proactive routing protocol: IntrA-zone Routing Protocol (IARP) is used inside routing zones and a reactive routing protocol: Inter-zone Routing Protocol (IERP)is used between routing zones, respectively. A route to a destination within the local zone can be established from the proactively cached routing table of the source by IARP; therefore, if the source and destination is in the same zone, the packet can be delivered immediately.

II. WORMHOLE ATTACKS

In wormhole attack [8], an attacker or a malicious node can eavesdrop or receive data packets at a point and transfer them to another malicious node, which is at another part of the network, through an out-of-band channel. The second malicious node then replays the packets.

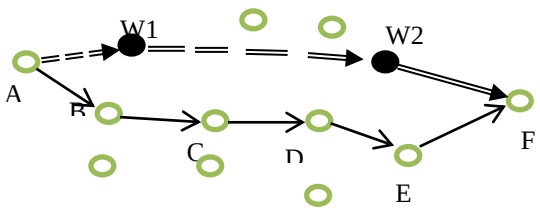
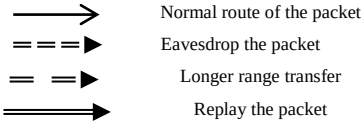


Figure 1: Wormhole attack



This makes all the nodes that can hear the transmissions by the second malicious node believe that the node sent the packets to the first malicious node is their single-hop neighbor and they are receiving the packets directly from it. For example, the packets sent by node A are also received by node W1, which is a malicious node. Then node W1 forward these packets to node W2 through a channel which is out of band for all the nodes in the network except for the adversaries. Node W2 replays the packets and node F receives them as if it was receiving them directly from node A. The packets that follow the normal route, i.e A-B-C-D-E-F, reach node F later than those conveyed through the wormhole and are therefore dropped because they do more hops. Wormholes are typically established through faster channels.

The figure 1 shows the illustration of wormhole attack. Wormholes are very difficult to detect and can impact on the performance of many network services such as time synchronization, localization and data fusion. This attack also forms a serious threat in wireless networks, especially against routing protocols. Routing can be disrupted when routing control messages are tunneled. This tunnel between the two colluding attackers is referred as wormhole.

III. SIMULATION ENVIRONMENT

The performance analysis of different routing protocols such as AODV, OLSR and ZRP with wormhole attack in IEEE 802.15.4 based WSN is simulated using Qualnet 5.0 [9]. The table I shows the configuration of simulation parameters used for the WSN scenario.

TABLE I: Simulation parameters

Parameters	Value
Terrain Size	400 x 400 m^2
Number of Nodes	50
MAC Protocol	MAC 802.15.4
Routing Protocols	AODV, ZRP,OLSR
Items send	1000 packets
Packets Size	50 bytes
Simulation time	18 minutes
Mobility model	Random Way Point
Mobile speed (mps)	10 mps
Wormhole attack (no's)	1 to 10
Energy model	Mica-Motes
Full Battery Capacity	1200 mA.h

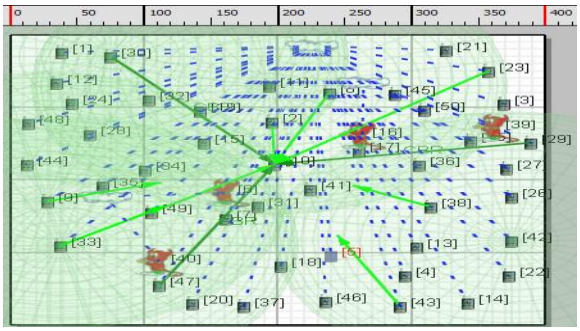


Figure 2: WSN Scenario with Wormhole attack

Figure 2 illustrated the wireless sensor network scenario, consisting of 50 nodes deployed over a terrain with size of 400 x 400 m^2. In this scenario, the nodes

30, 47 and 29 are considered as source nodes to send the sensed data towards the PAN co-ordinator (node 10) in presence of wormhole attacks.

IV. Simulation Result and Discussion

The impact of wormhole attacks on different routing protocols such as AODV, OLSR and ZRP of WSN with fixed and mobile nodes is studied. From this, the performance metrics [10] such as throughput, end-to-end delay and energy consumed by nodes in transmit, receive, idle and sleep mode are determined.

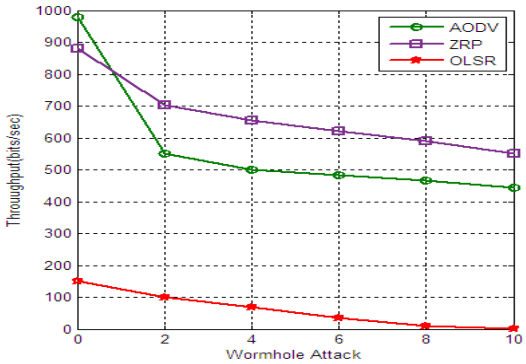


Figure 3: Throughput due to wormhole attack on AODV, OLSR and ZRP for static WSN.

Figure 3 shows the effect of throughput on AODV, OLSR and ZRP routing protocol in the presence of wormhole attack. It is observed that the throughput decreases with increased number of wormhole attacks for all the routing protocols. It is clear that ZRP has highest throughput and OLSR has lowest throughput. Further the performance of ZRP and AODV is better than OLSR under wormhole attacks comparatively. The reason for the degradation of throughput performance of routing protocols is due to the increased packet loss in the presence of wormhole attack.

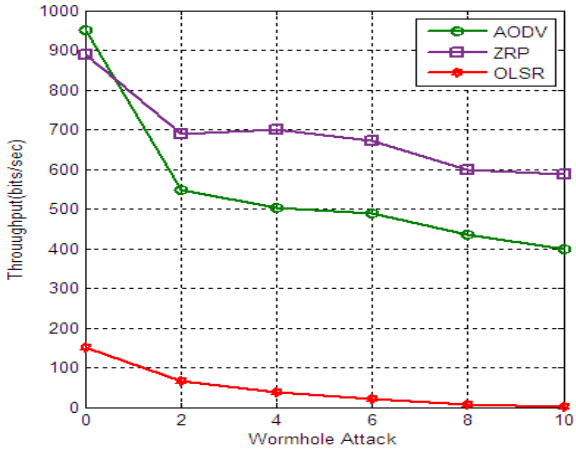


Figure 4: Throughput due to wormhole attack on AODV, OLSR and ZRP for mobile WSN with node speed 10 m/s.

It is inferred from the figure 4 that the throughput is decreased with increased number of wormhole attacks. It shows that performance of ZRP and AODV is better in terms of throughput than that of OLSR comparatively. ZRP has highest throughput than that of AODV and OLSR.

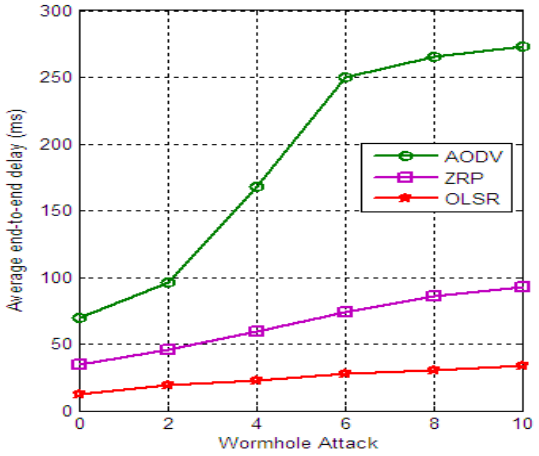


Figure 5: Average end-to-end delay due to wormhole attack on AODV, OLSR and ZRP for static WSN.

Figure 5 portrays the effect of average end-to-end delay of AODV, OLSR and ZRP routing protocol by increasing the wormhole attacks in static WSN. The result depicts that the average end-to-end delay also increases with increased number of wormhole attacks for all the three routing protocols. On comparing the three routing

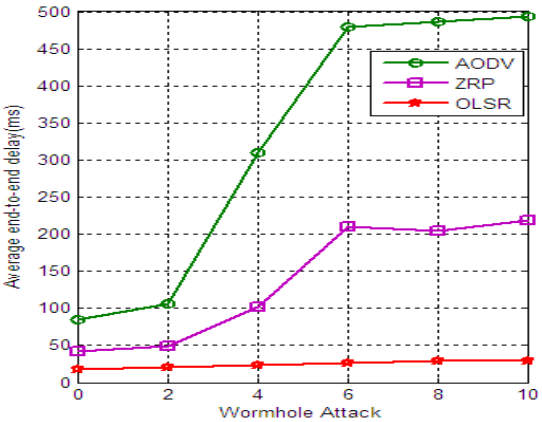


Figure 6: Average end-to-end delay due to wormhole attack on AODV, OLSR and ZRP for mobile WSN

Figure 6 depicts the average end-to-end delay analysis of AODV, OLSR and ZRP routing protocol due to wormhole attack in mobile wireless sensor network with node speed of 10 m/s. It is also inferred that the average end-to-end delay increases drastically with various number of wormhole attacks for three routing protocols. It shows that OLSR and ZRP routing protocol performed better than AODV comparatively. AODV has highest delay while OLSR has lowest delay due to regular update of routing table.

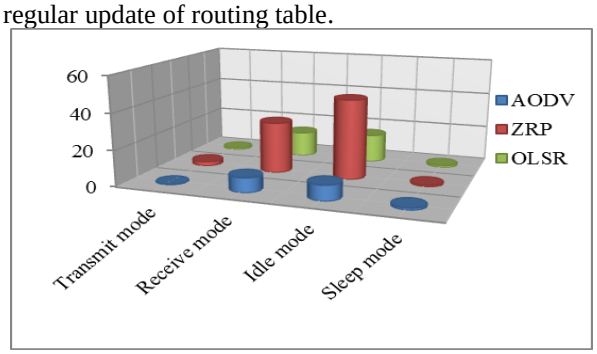


Figure 7: Energy Consumed in Static WSN without Wormhole attack.

TABLE II

Energy Consumed (mJoule)	AODV	ZRP	OLSR
Transmit mode	0.36	2.5	0.99
Receive mode	8.2	28.66	14.1
Idle mode	8.5	44.47	15.8
Sleep mode	1.2	0.91	1.1

Figure 7 and table II shows the energy consumption of nodes in transmit, receive, idle and sleep mode in static wsn without wormhole attack. The AODV has very less energy consumption than that of OLSR and ZRP. AODV performed better than OLSR and ZRP in terms of Energy consumption.

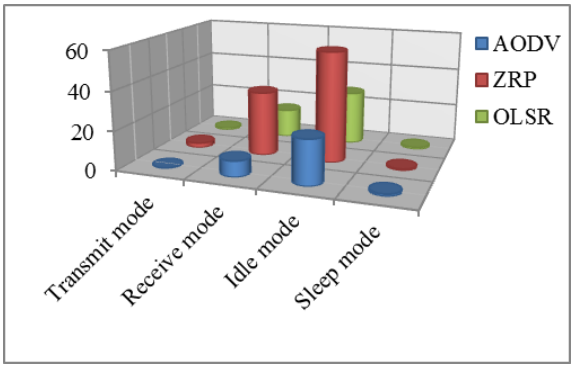


Figure 8: Energy Consumed in mobile WSN without Worm hole attack

TABLE-III

Energy Consumed (mJoule)	AODV	ZRP	OLSR
Transmit mode	0.38	2.4	0.99
Receive mode	8.1	33.2	14.9
Idle mode	22.88	56.8	27.7
Sleep mode	1.11	0.82	1.05

Figure 8 and table-III shows the energy consumption of nodes in transmit, receive, idle and sleep mode in mobile wsn without wormhole attack. It is clear that the AODV has very less energy consumption than that of OLSR and ZRP. Hence AODV performed better than OLSR and ZRP in terms of Energy consumption.

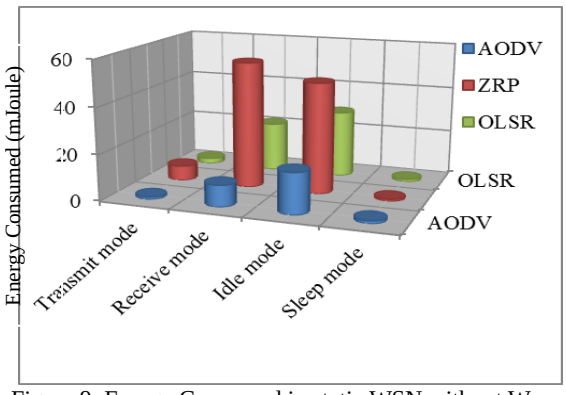


Figure 9: Energy Consumed in static WSN without Worm hole attack

TABLE-IV

Energy Consumed (mJoule)	AODV	ZRP	OLSR
Transmit mode	1.08	6.58	2.3
Receive mode	9.4	55.1	21.62
Idle mode	18	48.35	29.3
Sleep mode	1.2	0.87	1.1

Figure 9 and table-IV illustrates the energy consumption of nodes in transmit, receive, idle and sleep mode in static wsn with wormhole attack. It is inferred that the AODV has very less energy consumption than that of OLSR. Hence AODV has better performance than OLSR and ZRP in terms of Energy consumption.

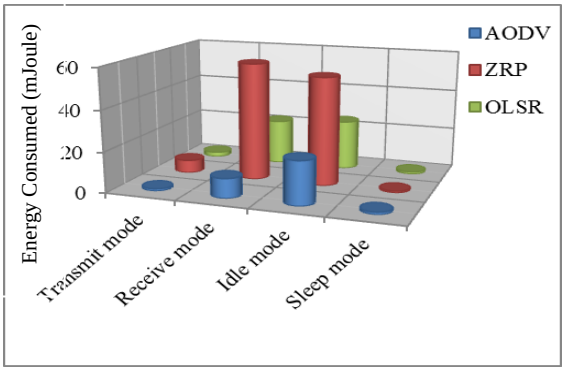


Figure 10: Energy Consumed in mobile WSN with Worm hole attack

TABLE-V

Energy Consumed (mJoule)	AODV	ZRP	OLSR
Transmit mode	1.08	6.37	2.3
Receive mode	9.6	57.7	22.17
Idle mode	21.4	53.163	24.5
Sleep mode	1.2	0.834	1.1

Figure 10 and table-V shows the energy consumption of nodes in transmit, receive, idle and sleep mode in mobile wsn with wormhole attack. It is inferred that the AODV has very less energy consumption than that of OLSR and ZRP. Hence AODV has better performance than OLSR and ZRP in terms of Energy consumption.

II. Conclusion

In this investigation, the performance metrices such as throughput, average end-to-end delay, node energy consumption of AODV, OLSR and ZRP routing protocols with wormhole attacks is evaluated in static and dynamic wireless sensor networks. It is verified through the simulation results that the decreased throughput, increased average end-to-end delay, and more energy consumption for increased wormhole attacks degrades the performance of routing protocols such as AODV, OLSR and ZRP. However, ZRP has highest throughput and OLSR has lowest average end-to-end delay, due to very less throughput of OLSR and more energy consumption of ZRP and OLSR, AODV has better overall performance in terms of throughput and end-to-end delay than other two protocols comparatively. Finally, it is concluded that the routing protocols AODV OLSR and ZRP are still vulnerable to wormhole attacks. Hence it is required to design a secure routing protocol to prevent the security threats in wireless sensor networks in future.

References

[1] X. Chen, K. Makki, K. Yen and N. Pissinou, Sensor network security: A survey. IEEE Communications Surveys and Tutorials 11(2): 52-73 (2009).

[2] E. Cayirci and C. Rong, Security in Wireless Ad Hoc and Sensor Networks, Wiley (2009).

[3] Y. Wang, G. Attebury and B. Ramamurthy, A survey of security issues in wireless sensor networks. IEEE Communication. Surveys and Tutorials 8(2): 2–23 (2006).

[4] Padmavathi, G. & Shanmugapriya, D., A survey of attacks, security mechanisms and challenges in wireless sensor networks. International Journal of Computer Science and Infor-mation Security (IJCSIS) 4(1): 1-9 (2009).

[5] C. Perkins, E. Belding-Royer, and S. Das, RFC 3561: Ad-hoc on-demand distance vector (AODV) routing, July (2003).

[6] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum L. Viennot, Optimized Link State Routing Protocol, IEEE INMIC Pakistan (2001)

[7] Z.J. Haas, M. R. Pearlman, and P. Samer, The Zone Routing Protocol (ZRP) for Ad Hoc Net-works, Internet Draft (2003). available at:http:// tools.ietf.org/id/draft-ietf-MANETs-zone-zrp-4.txt.

[8] Y. C. Hu, A. Perrig and D.B. Johnson, Wormhole Attacks in Wireless Networks. IEEE Journal on Selected Areas in Communications 24(2): 370–80 (2006).

[9] Scalable Network Techologies, Qualnet simulator [Online].

[10] Anjali Goyal, Sandip Vijay and Dharmendra Kumar Jhariya, Simulation and Performance Analysis of Routing Protocols in Wireless Sensor Network using QualNet. International Journal of Computer Applications 52(2): August (2012).