Performance Analysis of Trust Based AODV for Wireless Sensor Networks

P.Samundiswary and P.Dananjayan
Dept. of Electronics and Communication Engineering
Pondicherry Engineering College, INDIA.

ABSTRACT

Recent advances in wireless networks have prompted much research attention in the area of wireless sensor network (WSN). Sensor network consists of hundreds to thousands of low power multifunctioning sensor nodes operating in hostile environment with limited computational and sensing capabilities. These sensor devices are susceptible to various attacks such as selective forwarding or sinkhole attacks when operated in a wireless medium. Reactive routing protocols such as ad-hoc on demand distance vector routing (AODV) of sensor networks have been developed without considering security aspects against these attacks. In this paper, a secure routing protocol named secured ad hoc on demand distance vector routing (S-AODV) is proposed for mobile sensor networks by incorporating trust based mechanism in the existing AODV. Zigbee hardware prototype is also implemented and tested by increasing the sizes of data and distances in indoor and outdoor environment. Simulation results prove that S-AODV outperforms the AODV by reducing the overhead and improving the delivery ratio of the networks.

Keywords

Wireless sensor networks, Secured ad-hoc on demand distance vector routing, Sink hole, Route trust, Node trust. .

1. INTRODUCTION

Recently wireless sensor networks have drawn a lot of interest due to broad applications in military and civilian operations. Sensor nodes in the network are characterized by severely constrained, energy resources and communicational capabilities. Due to small size and unattention of the deployed nodes, attackers can easily capture and rework them as malicious nodes. Karlof and Wagner [1] also have revealed that routing protocols of sensor networks are insecure and highly vulnerable to malicious nodes. It can either join the network externally or may originate internally by compromising an existing benevolent node [2]. These compromised nodes can also carry out both passive and active attacks against the networks [3]. In passive attack a malicious node only eavesdrops upon the packet contents, while in active attacks it may imitate, drop or modify legitimate packets [4]. Sinkhole is one of the common types of active attack in which a node can deceitfully modify the routing packets [5]. So, it may lure other sensor nodes to route all traffic through it. The impact of sinkhole is to launch further active attacks on the traffic, which is routed through it.

Due to limited capabilities of sensor nodes, providing security and privacy against these attacks is a challenging issue to sensor networks. In order to protect network against malicious attackers, number of routing protocols have been developed to improve network performance with the help of cryptographic techniques. Security mechanisms used in these routing protocols of sensor networks detect the compromised node and then revoke the cryptographic keys of the network. But, requirements of such secure routing protocols include configuration of the nodes with encryption keys [6], the creation of a centralized or distributed key repository to realize different security services [7] and clock synchronisation in the network.

In addition, secure routing protocols utilising cryptographic methods also require excessive overheads. However, only few routing protocols such as secured dynamic source routing protocols (S-DSR) for wireless sensor networks address the security mechanism by using trust based model against various attacks [8]. S-DSR forwards the packets to successive nodes given in the source node route header by checking its trust levels rather than the shortest route only. Moreover, S-DSR chooses the most trustworthy path computed by the source node using the trust based model to a particular destination by circumventing intermediate malicious nodes. However the performance of S-DSR will be degraded for higher malicious nodes and mobility conditions. In contrast, in AODV the header of packet transmitted from source node contains only the next hop address for a desired destination to improve the performance for larger mobile nodes situations. AODV selects the routing path by using two methods for routing such as route discovery and route maintenance to transmit data from source to destination. But the selected shortest routing path of AODV includes malicious or selfish nodes which is not aware by source node. In this paper, secured ad-hoc on demand distance vector routing (S-AODV) is proposed by including trust based framework mechanism which uses node trust and route trust in AODV to protect nodes from sinkhole attacks in sensor network with mobility model for nodes and Zigbee hardware model using AODV is also implemented. This S-AODV is simulated by using ns-2.32 for different coverage areas of 300m×300m and 500m×500m with 150 and 200 numbers of nodes considering mobile nodes in the network. The paper is organized as follows: Section 2 explains about the ad-hoc on demand distance vector routing. Section 3 describes about the proposed secured ad-hoc on demand distance vector routing of wireless sensor network. Section 4 deals with the implementation of Zigbee hardware model with AODV protocol. Results are discussed in Section 5 to obtain delay measurement using hardware prototype , delivery ratio, delay and routing overhead of the proposed security mechanism and conclusions are drawn in Section 6.

2. AD-HOC ON DEMAND VECTOR ROUTING

Routing protocols of WSN can be classified as 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. AODV routing protocol is one of the most popular reactive routing protocols of wireless sensor networks. Being a reactive routing protocol AODV uses traditional routing tables, one entry per destination and destination sequence numbers (DSN) are used to determine whether routing information is up-to-date and to prevent routing loops [9]. This will greatly increase the efficiency of routing processes. AODV consist of two routing phases such as discovery and maintenance. Various types of control messages are used in the routing process of AODV.

2.1. Control Messages in AODV

Route Request Message (RREQ), Route Reply Message (RREP), Route Error Message (RERR) and HELLO Messages are the control messages used for the discovery and breakage of route.

2.2 Route Discovery and Route Maintenance

AODV has two basic operations: route discovery and route maintenance. Route discovery is initiated when a source node wants to find a route to a new destination or when the lifetime of an existing route to a destination has expired. The process is initiated by broadcasting of RREQ as shown in Figure.1.The source node broadcasts an RREQ packet which is in turn rebroadcasted by the neighbour nodes until the sought route is discovered. Upon receiving an RREQ, an intermediate node with a ‘fresh enough’ route to the destination or the destination node itself unicasts an RREP packet back to the source node. This is possible because each node receiving the RREQ caches the route back to the originator of RREQ. A route is said to ‘fresh enough’ when the DSN of the sought route in the recipient node’s routing table is greater than the DSN in the RREQ packet itself. A G flag is set in the RREQ for establishing a reverse route between destination node D and source node S. If a node forwards an RREP over a link that is likely to have errors, the node should set the ‘A’ flag in the RREP. This would require an RREP acknowledgement (RREP-ACK) from the RREP recipient to its immediate sender/forwarder [10].

There are two modes of route maintenance. To maintain connectivity, nodes may: (a) Periodically broadcast HELLO packets to their neighbors, and (b) Use acknowledgement based mechanisms at the link or network layers. Upon detecting a link break, a node could choose to repair the link locally (if the destination is no farther than MAX_REPAIR_TTL hops away) or send an RERR packet to notify its upstream nodes. An RERR message contains the list of those destinations which are not reachable due the loss of connectivity.

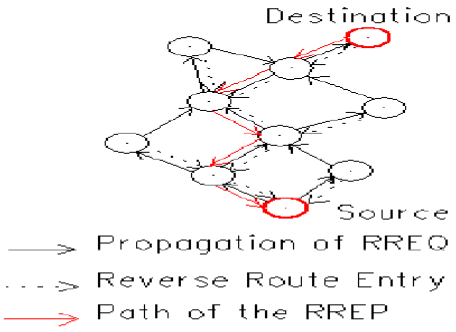

Figure 1.Discovery of route

3. SECURED AD HOC ON DEMAND DISTANCE VECTOR ROUTING

In S-AODV, the trust levels are incorporated in packet header of source node to create the most trusted route rather than the default shortest route. To compute direct trust in a node, an effort-return based trust model [11] is used in the existing AODV protocol. The salient changes made in AODV to function as S-AODV are

- Each node maintains an additional data structure called the neighbours’ trust table. It contains neighbouring node IDs, their corresponding trust values.
- Each route table entry for a given destination stores all the routes from that node to the destination with the highest DSN. The corresponding route trust values as advertised by the nodes named as *advertised route trust value* (ATV) and the computed *route selection value* (RSV) are stored. Each route to a destination can be identified by unique Rid. The Rid with the highest RSV is stored in the advertised Rid field and advertised to the upstream nodes.
- The RREQ packet has two additional fields: the *omit node flag* and the *omit node ID*. The omit node flag, if set, indicates that the node ID mentioned in the omit node ID field should be precluded from the route to the destination. The rest of the packet is same as that in the AODV protocol.
- The RREP packet has additional fields to accommodate the route trust and the recommender node’s ID. For every RREP, the intermediate node increments the number of hops by one and caches the route trust sent by the downstream node from the route trust field. If the node has individually computed its own trust value on the route then update the route trust and the recommender ID fields with its own route trust value and its node ID.
- R_ACK is the modified version of the RREP-ACK message of the AODV protocol. The RREP-ACK is used to acknowledge the receipt of a RREP (with its A bit set) over an unreliable link. Apart from performing the same task as RREP-ACK, an R_ACK functions as a report packet. A report packet would be initiated by the destination to inform the source and the intermediate nodes of the number of packets it received so far since the last transmission of R_ACK.

3.1 Trust Framework and Computation

There are two trust values associated with the S-AODV protocol. They are route trust and node trust [12].

3.1.1Route trust

Route trust is computed by every node for each route in its routing table. It is a measure of the reliability with which a packet can reach the destination, if forwarded by the node on that particular route. The route trusts are initially unknown. RREQ's are sent by source node S and the routes are established to the destination node D as in AODV. All RREQs have the G flag set so as to establish reverse route from D to S. Each node keeps track of the number of packets it has forwarded through a route. D periodically sends R_ACK packets to S at an agreed interval between S and D. The R_ACK packets are readable by all the nodes on the route. Each intermediate node on the reverse route from D to S checks the R_ACK packets to compute its route trust. Route trust is calculated as a ratio of the number of packets received at D to the number of packets forwarded by the node under consideration (from S to D on that route).

3.1.2 Node trust

Every node also maintains node trust on each of its neighbours. Node trust helps a node X incredibly in evaluating the recommendation of a neighbour N's trust on a route passing through N. The current number of route requests (r) generated by N that will be entertained by X is directly proportional to X's node trust on N. Initially when the network is setup, the proposed scheme functions almost like AODV. In the beginning, a node does not have any information about the credibility of its neighbours, i.e., nodes can neither be fully trusted nor be fully distrusted. So all nodes have 50% initial node trust with r = R/2 and this trust remains unchanged until a initial time $t_{init.}$ Node trust is computed based on the difference between the nodes' ATV to the destination and the observed trust value (OTV) computed for the current data transfer. When a node X forwards or generates an RREP, X advertises its trust on the route under consideration to its immediate upstream node P. Node P caches this route trust value as ATV of node X on that route and compares it with the OTV. The node X receives an incentive if the OTV is within an admissible range of ATV. Otherwise, it is penalized. The penalties and the incentives are inversely proportional to the node's distance from the destination: the farther a node from the destination, lesser is the information it has on the downstream nodes' behaviour. A node which is only one-hop from the destination is solely responsible for packets reaching the destination. So its trust on the route is based on only its own behaviour and link between itself and the destination. But a node which is, say, three hops away from the destination, would have less information about the downstream route conditions and node behaviour.

3.2 Route Selection Criteria

The node S may get several RREP packets in response to its RREQ packet to D. The route selection criterion is dependent on node trust on the immediate downstream neighbour N that recommended the route which has trusted route on the sought route. The route selection criterion is inversely proportional to the number of hops in the route. Many methods can be devised for selecting a route from the available routes. A source node calculates the RSV for all its available routes to the destination and it finally chooses the route which has the highest RSV. If two routes have the same RSV then the following criteria are used to break the tie: i) the routes with highest trusted route are selected. ii) If the routes have same route trust values then the route with the highest immediate downstream neighbours' node trust (as perceived by the source/immediate upstream node) is chosen. iii) If the immediate downstream neighbours' node trust is also the same, then the shortest route is chosen. iv) If all the above are same then it will choose randomly among those routes with same RSVs.

4. ZIGBEE HARDWARE PROTOTYPE MODEL USING AODV

The ZigBee hardware model is implemented to transfer data from one PC to another in indoor and outdoor model. The block diagram of the entire model is shown in Figure.2. The system consists of two PCs which are connected by a wireless link using ZigBee technology. The data from the PC is fed to the source node which is connected to the PC using a RS232 cable through the serial port of the PC. The source node in turn receives it and transmits it to the second node or the relay node .The second node upon receiving the data transmits it to the third node (relay node) and third node in turn transmits it to the fourth node which is the destination node.

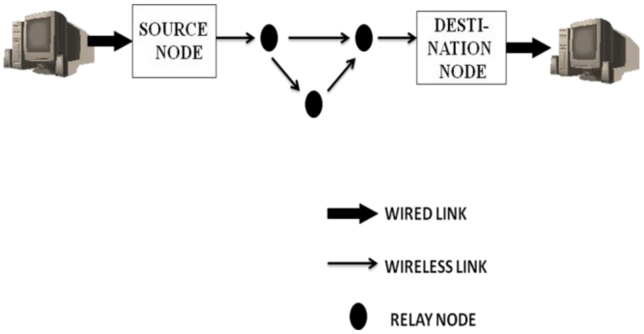

Figure 2. Block diagram of the hardware prototype

The ZigBee hardware prototype is built with one source, one destination and two relay nodes. Each node of the hardware prototype model is equipped with a ZigBee transceiver [13] which receives the data from the previous node and transmits it to the next node. ZigBee module operates within the industrial, scientific and medical (ISM) 2.4 GHz frequency band. This module requires minimal power and provides reliable delivery of data between remote devices. AODV routing is done in ZigBee module. The specifications of ZigBee are given in Table.1.

4.1 Source and Destination Node Architecture

Figure.3 and Figure.4 explains the source node and destination node architectures respectively. Microcontroller 8051 is used in all nodes except source node. Microcontroller 4013 is used in the source node. Crystal oscillator frequency is set as 11.0592 MHz. Baud rate is set as 9600 bps using bray terminal. Max232 acts as interface between microcontroller and RS232. Pins 1 and 3 of 7805 voltage regulator are provided with 1μF capacitors for stability purpose. The snapshot of all the nodes is shown in Figure.5, Figure.6 and Figure.7.

Table 1. Specifications of ZigBee

Parameters	Values
RF Data Rate	250,000 bps
Supply Voltage	2.8 – 3.4 V
Number of Channels	16 Direct Sequence Channels
Transmit Power Output	1mW
Receiver Sensitivity	-92 dBm
Indoor/Urban Range	Up to 100 ft. (30 m)
Outdoor Range	Up to 300 ft.(100 m)
Operating Frequency	2.4 GHz

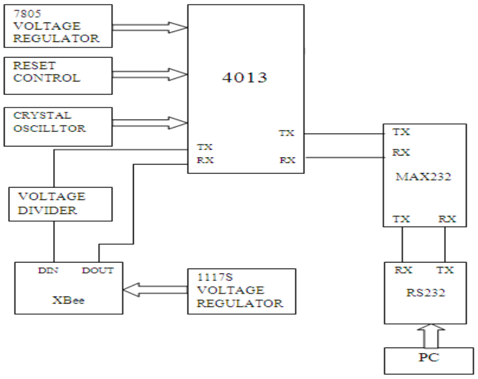

Figure 3. Source node architecture

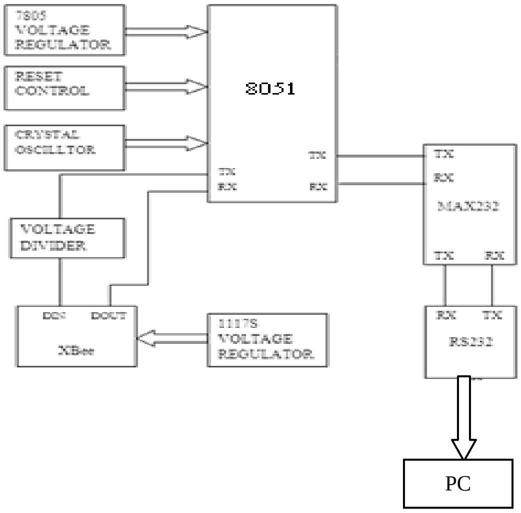

Figure 4. Destination node architecture

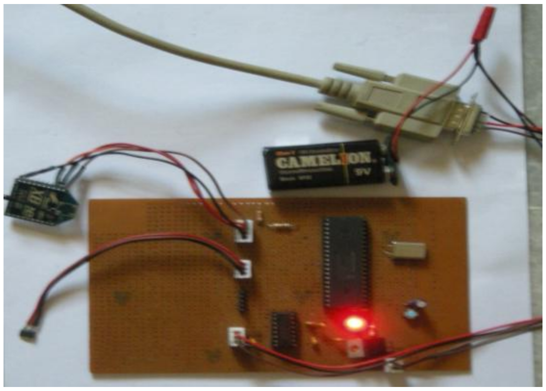

Figure 5.Source node

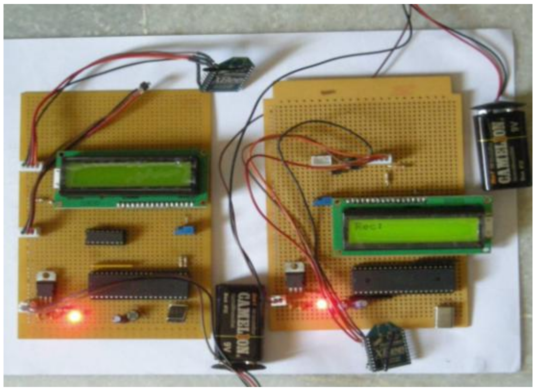

Figure 6. Relay nodes

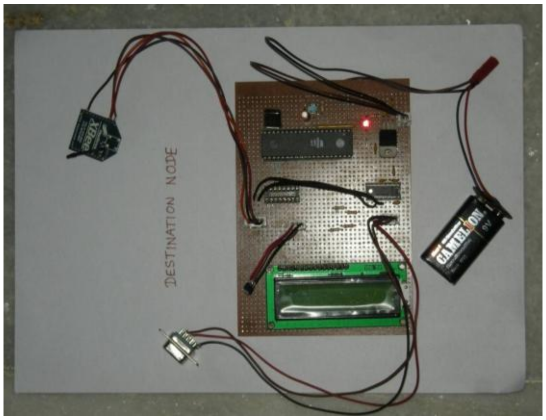

Figure 7. Destination node

5. SIMULATION RESULTS AND DISCUSSION

5.1 Results using S-AODV

The trust and mobility model is implemented in the existing AODV protocol to obtain the S-AODV protocol. The S-AODV protocol is simulated using Network Simulator-2.32 to emulate selective forwarding and sinkhole attacks in the mobile sensor network. The performance parameters such as delivery ratio, delay and routing overhead are calculated for two different number of nodes (150 and 200) by varying the number of malicious nodes from 5 to 25 with various coverage areas such as 300×300 (m^2) and 500×500(m^2). The parameters used in the simulation are listed in Table 2.

Table 2. Simulation Parameters

Simulation Parameters	**Values**
Number of Nodes	150 and 200
Geographical area(m^2)	300×300, 500×500
Packet Size(bytes)	512
Traffic Type	CBR
Number of malicious nodes	5 to 25
Mobility model	Random way point
Pause time(s)	20
Simulation time(s)	100

5.1.1 Delivery ratio

Delivery ratio of S-AODV is higher than that of AODV for 150 and 200 nodes with different coverage area of 300×300(m^2) and 500×500 (m^2) which is shown in Figure 8(a),Figure 8(b),Figure 8(c) and Figure 8(d). S-AODV outperforms AODV by providing delivery ratio of nearly 28% for increased values of malicious nodes which is illustrated in Figure 8(a) and Figure 8(c). Figure 8(b) and Figure 8(d) reveals that there is increment in the delivery ratio of S-AODV of approximately 18% compared to that of AODV for higher values of malicious nodes considering coverage area 500×500 (m^2) .

S-AODV improves the delivery ratio by increasing the forwarding rate by preferring the trusted routes for transmitting the packets from source to destination. Moreover, S-AODV selects or deselects the neighbour node for routing process based on their node trust and route trust levels to avoid the malicious node.

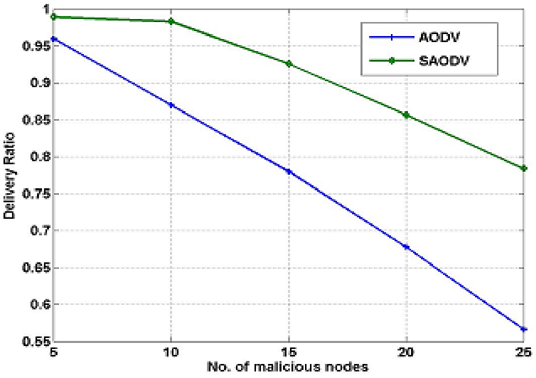

Figure 8(a).Delivery ratio with respect to no. of malicious nodes for 150 nodes with coverage area 300×300(m^2)

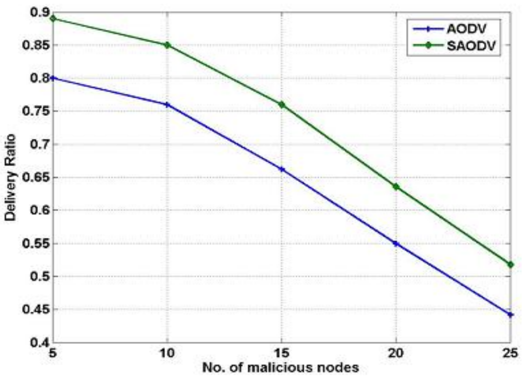

Figure 8(b). Delivery ratio with respect to no. of malicious nodes for 150 nodes with coverage area 500×500(m^2)

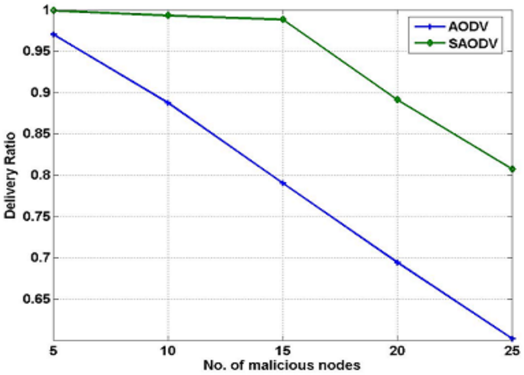

Figure 8(c). Delivery ratio with respect to no. of malicious nodes for 200 nodes with coverage area 300×300(m^2)

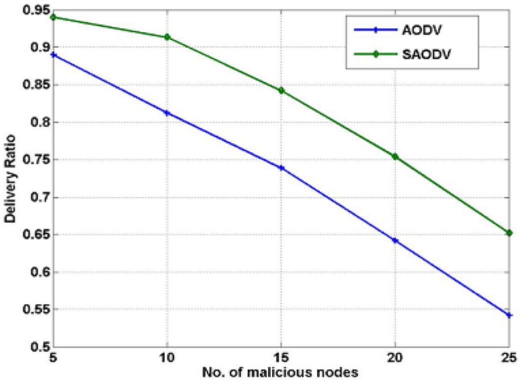

Figure 8(d). Delivery ratio with respect to no. of malicious nodes for 200 nodes with coverage area 500×500(m2)

5.1.2 Routing overhead

S-AODV has an overall lower routing overhead compared to that of AODV which is revealed through the results shown in Figure 9(a), Figure 9(b), Figure 9(c) and Figure 9(d). The routing overhead of S-AODV is lesser by roughly 65 % (average) than that of AODV for 150 nodes and 200 nodes with coverage area 300×300(m^2) which is shown in Figure 9(a) and Figure 9(c).

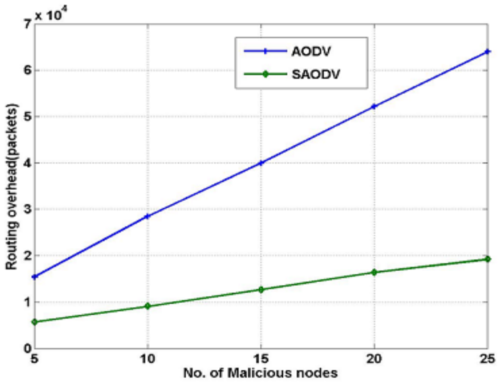

Figure 9(a). Routing overhead Vs no. of malicious nodes for 150 nodes with coverage area 300×300(m2)

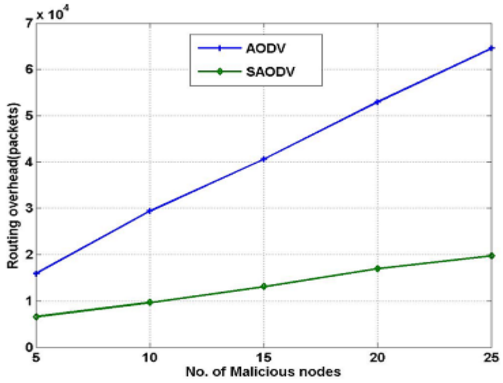

Figure 9(b). Routing overhead Vs no. of malicious nodes for 150 nodes with coverage area 500×500(m^2)

However routing overhead of S-AODV and AODV increases, S-AODV achieves significant reduction in routing overhead by 68% nearly for increased values of malicious nodes, compared to that of AODV. The reduced overhead is due to less number of control packets generated for each data packet transmitted by trusted route in S-AODV.

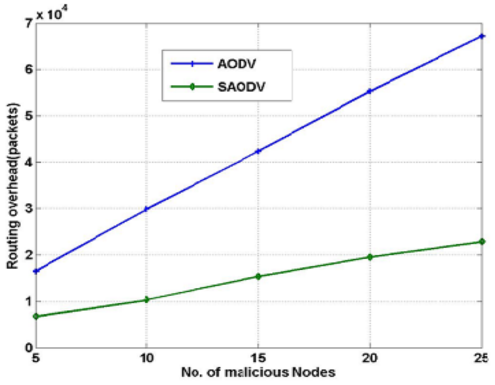

Figure 9(c).Routing overhead Vs no. of malicious nodes for 200 nodes with coverage area 300×300(m^2)

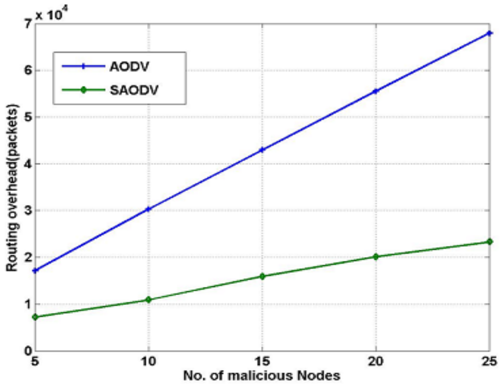

Figure 9(d).Routing overhead Vs no. of malicious nodes for 200 nodes with coverage area 500×500(m^2)

5.1.3 Delay

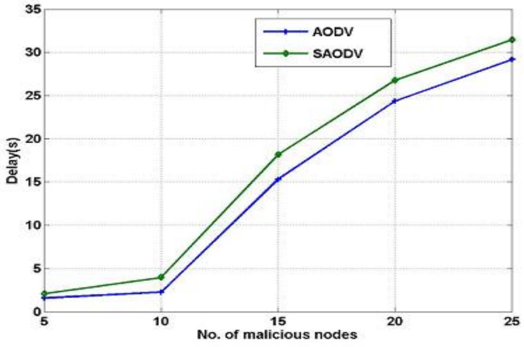

Figure 10(a). Delay for varying no. of malicious nodes for 150 nodes with coverage area 300×300(m^2)

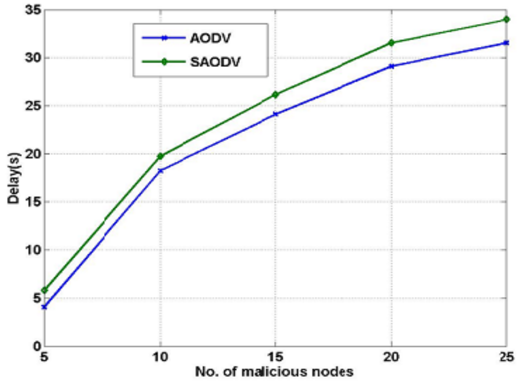

Figure 10(b). Delay for varying no. of malicious nodes for 150 nodes with coverage area 500×500(m^2)

Delay of S-AODV protocol is higher than that of AODV protocol which is verified through simulation results shown in Figure 10(a), Figure 10(b), Figure 10(c) and Figure 10(d).When numbers of malicious nodes are increased further, S-AODV increases delay approximately by 10% than that of AODV protocol for 150 and 200 nodes with coverage area 300×300 (m^2) exposed in Figure 10(a) and Figure 10(c). The increment in the delay of S-AODV is due to the trusted path taken by source node to transfer the data to required destination to avoid the malicious node.

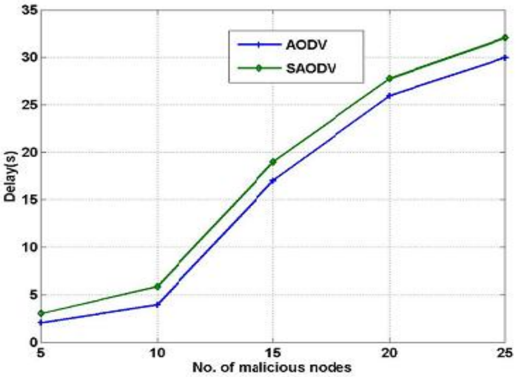

Figure 10(c). Delay for varying no. of malicious nodes for 200 nodes with coverage area 300×300(m^2)

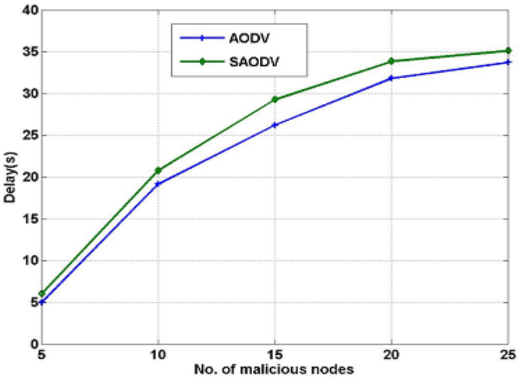

Figure 10(d). Delay for varying no. of malicious nodes for 200 nodes with coverage area 500×500(m^2)

5.2. Observations done using ZigBee Prototype Model

The hardware prototype has been tested in indoor and outdoor environments by transferring data of different byte sizes and varying distances. The delay measurement obtained for increased values of distances with data sizes of 5000 and 10000 bytes in indoor and outdoor regions are shown in Figure 11(a),Figure 11(b),Figure 11(c) and Figure 11(d). When the distance and data size increase, delay increases both in indoor and outdoor environments which are proved through the results revealed in Figure 11(a),Figure 11(b),Figure 11(c) and Figure 11(d). In indoor, data has been transferred to a maximum distance of 25m without any packet loss successfully which is shown in Figure 11(a) and Figure 11(b). Figure 11(c) and 11(d) illustrate that data of 5000 and 10000 bytes have been delivered fruitfully to a distance of 100m in outdoor region.

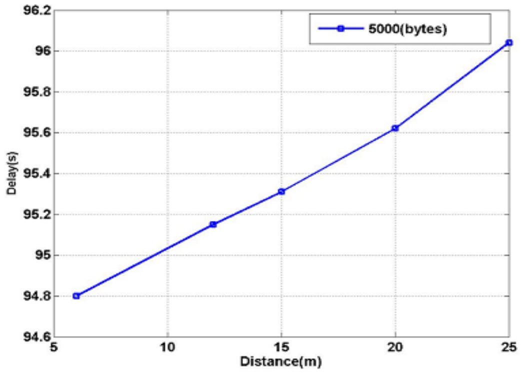

Figure 11(a).Delay for various distances in transmitting 5000 bytes in indoor environment

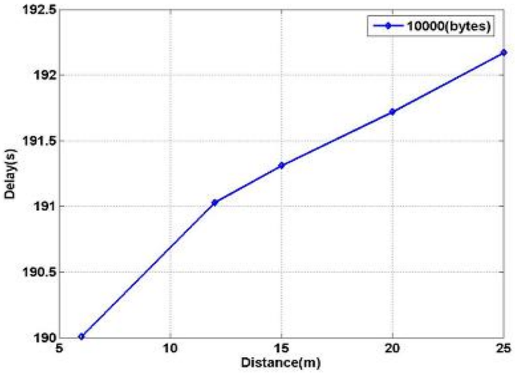

Figure 11(b).Delay for various distances in transmitting 10000 bytes in indoor environment

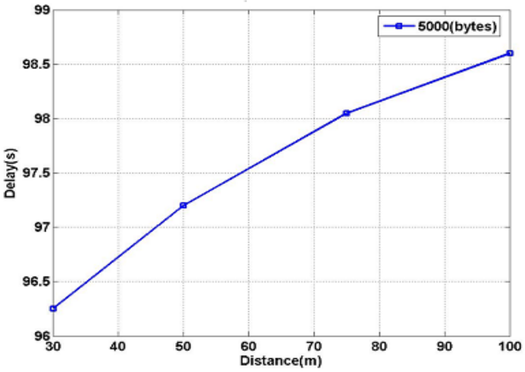

Figure 11(c).Delay for various distances in transmitting 5000 bytes in outdoor environment

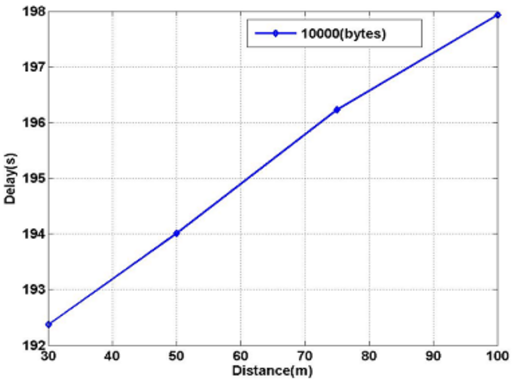

Figure 11(d).Delay for various distances in transmitting 10000 bytes in outdoor environment

6. CONCLUSION

The prototype of the ZigBee network was built with four nodes and data was transferred from one PC to another via the ZigBee module. The hardware prototype was tested under various indoor and outdoor environments and the delay measurements were done by varying data size and distance. Observations done using ZigBee network model prove that if distance and data size are increased, delay also increases. It is also demonstrated through observations that data has been delivered effectively without any loss of data for a maximum distance of 25m and 100m in indoor and outdoor environment. Secured ad hoc on demand distance vector routing protocol is implemented for mobile sensor networks with different coverage areas considering 150 and 200 numbers of nodes for simulation. It is compared with ad hoc on demand distance vector routing protocol for different number of malicious nodes. The results show that on the average, the routing overhead achieved using the S-AODV protocol was 65% less than the standard AODV protocol. Further more, an improvement of 18-28% in the delivery ratio have been achieved in the S-AODV protocol. The improvement in the above mentioned network performance is mainly due to trusted route and less number of control packets taken by the trust based model which is implemented in AODV to get rid of the malicious nodes that were acting as selective forwarding or sinkhole attackers.

7. ACKNOWLEDGMENTS

The authors would like to convey their gratitude to Mr.R.Ragothaman and Mr.V.Vignesh, B.Tech students of Pondicherry Engineering College for their contribution in completing this work.

8. REFERENCES

[1] Karlof, C. and Wagner,D. 2003. "Secure routing in wireless sensor networks: attacks & countermeasures", *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols & Applications*, Anchorage, AK, May.

[2] Carter,S. , Yasinac, A. and Hu, Y.C. 2002. "Secure position aided ad-hoc routing protocol", *Proceedings of the IASTED Conference on Communications & Computer Networks (CCN),* Cambridge, MA, USA, pp.329-324, November.

[3] Hu,Y.C., Perrig, A. and Johnson,D.B.2002. "Ariadne: A secure on-demand routing protocol for ad-hoc networks", *Proceedings of the Eighth Annual International Conference on Mobile Computing & Networking (MobiCom)*, Atlanta, Georgia, USA, pp.12-23, September.

[4] Dahill, B., Levine, B.N., Royer, E. and Shields, C.2002. "A secure routing protocol for ad-hoc networks", *Proceedings of the IEEE International Conference on Network Protocols (ICNP),* Paris, France, pp.78-87, November.

[5] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler and Tygar, J.D. 2001. "SPINS: Security Protocols for Sensor Networks", *Proceedings of ACM Annual International Conference on Mobile Computing & Networking*, Rome, Italy, July.

[6] Asad Amir Pirzada and Chris Mcdonald. 2004. "Secure pervasive computing without a trusted third party", *Proceedings of the IEEE/AC International Conference on Pervasive Services (ICPS'04),*Beirut, Lebanon, July, 2004.

[7] Stallings,W. 2000. Network Security Essentials, Prentice Hall.

[8] Pirzada,A. and McDonald, C. 2005. "Circumventing sinkholes & wormholes in wireless sensor networks", Proceedings *of 2nd IEEE International Conference on Workshop on Wireless Ad-hoc Networking*, Columbus, USA, June.

[9] Perkins,C. Royer,E and Das,S. 2003. "Ad hoc on-demand distance vector routing", RFC-3651, *IETF Network Working Group*, July.

[10] Asar Ali and Zeeshan Akbar.2009. " Evaluation of AODV and DSR Routing Protocols of Wireless Sensor Networks for Monitoring Applications, *Thesis Report, Department of Electrical engineering with Telecommunication*, Blekinge Institute of Technology, October.

[11] Pirzada,A. and Mc. Donald, C.2004. "Establishing trust in pure ad-hoc networks", *Proceedings of 27th Australasian Computer Science Conference(ACSC)*, Dunedin, New Zealand, vol. 26, no.1, pp.47-54, January.

[12] Kamal Deep Meka, Mohit Virendra and Shambhu Upadhyaya. 2006. "Trust Based Routing Decisions in Mobile Ad-hoc Networks", *Proceedings of 2nd Workshop on Secure Knowledge Management*, Brooklyn, New York, September.

[13] Pinedo-Frausto, E.D.2008. "An experimental analysis of ZigBee networks",Proceedings *of 33rd IEEE international conference on Local Computer Networks (LCN),* Montreal, Canada, pp.723–729, June.