SECURED REACTIVE ROUTING PROTOCOL FOR MOBILE NODES IN SENSOR NETWORKS

P.SAMUNDISWARY AND *P.DANANJAYAN
Department of Electronics and Communication Engineering
Sri Manakula Vinayagar Engineering College
*Pondicherry Engineering College
Pondicherry
INDIA
pdananjayan@rediffmail.com, pdananjayan@pec.edu

Abstract:-Wireless sensor networks have drawn a lot of attention recently due to their broad applications in both military and civilian operations. Sensor nodes in the network are characterized by severely constrained energy resources and communicational capabilities. Since, these nodes are frequently established in a physically insecure environment, they are vulnerable to different types of active attacks. These attacks can inject malicious packets by compromising the node. Routing protocols are common target of these compromised nodes. Secured reactive routing protocols have recently been developed by using cryptographic algorithms against these attacks. However these routing protocols entail a number of prerequisites during both network establishment and operation phases .In contrast, trust based routing protocols locate trusted routes rather secure routes in the network. In this paper, a secure routing protocol named secured dynamic source routing protocol (S-DSR) is implemented for mobile sensor networks by incorporating trust based mechanism in the existing dynamic source routing protocol (DSR). Simulation results prove that S-DSR outperforms the DSR by reducing the routing overhead and improving the delivery ratio of the network.

Keywords:-Wireless sensor networks, Malicious nodes, DSR protocol, Secured dynamic source routing protocol, Trust Model ,Sinkhole attack.

1. Introduction

Wireless Sensor Networks (WSNs) are expected to have applications in many areas such as homeland security, environmental monitoring and healthcare systems. WSNs are usually comprised of massive number of small, inexpensive, self-powered and multi-functional sensor nodes which are deployed in a region of interest. Sensor nodes are equipped with sensors, embedded microprocessor and radio transceivers [1]. The schematic diagram of sensor node component is shown in Fig.1. These nodes are modeled to have the limited capabilities in terms of computation, communication, energy, storage, reliability and other aspects. Each node in the network basically acts like a router. The nodes communicate over a short distance via a wireless medium and collaborate to accomplish a common task such as transfer of sensed and processed data. The communication architecture of wireless sensor networks is shown in the Fig.2.

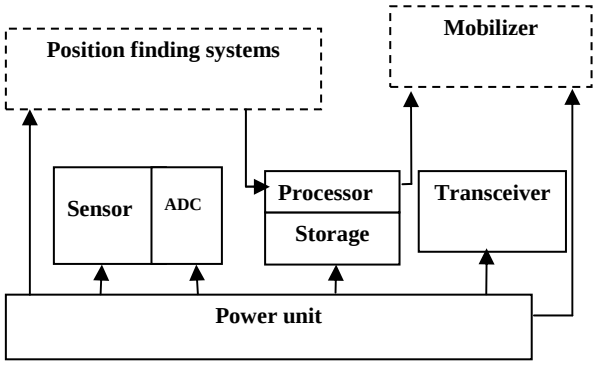

Fig.1. Schematic diagram of sensor node component

WSNs have become a major research domain in the communications community. Security and energy consumption were identified to be the most challenging research issue and contradicting problems. Security plays an important role in WSNs since the nodes of these types of networks are deployed in hostile environment. Due to the small size and unattended deployment of nodes, the

attackers can easily capture and convert them as malicious nodes. The malicious nodes can either join the network externally or may originate internally by compromising an existing benevolent node [2]. These nodes can carry out both passive and active attacks against the networks [3]. In passive attacks a malicious node only eavesdrops upon the packet contents, while in active attacks it may imitate, drop or modify legitimate packets [4]. A common type of active attack is a sinkhole [5] in which a node, can deceitfully modify the routing packets. Another type of such a colluded attack is a wormhole [6] in which a malicious node tunnels the packet from one end of the network to another.

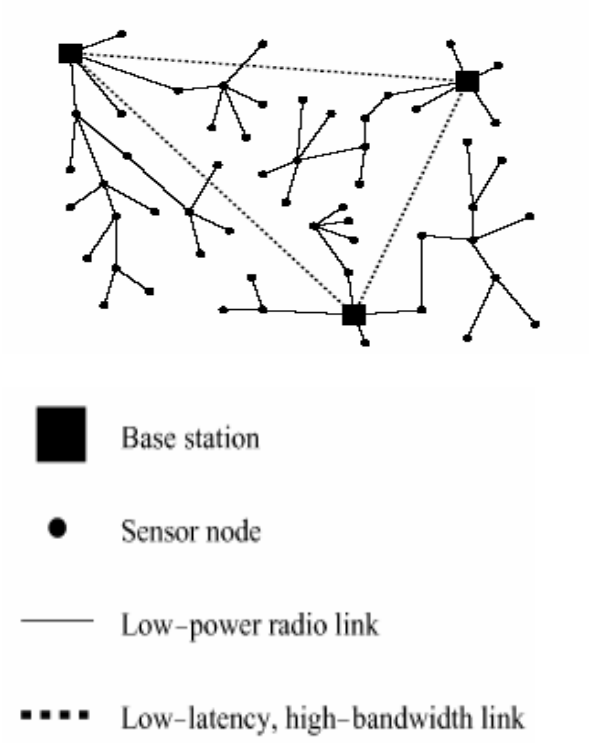

Fig.2. Communication architecture of wireless sensor network

Due to limited capabilities of sensor nodes, providing security and privacy against these attacks is a challenging issue in sensor networks. In order to protect network against malicious attackers, numbers 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 [7] and the creation of a centralized or distributed key repository to realize different security services in the network. In addition, secure routing protocols utilising cryptographic methods also require excessive overheads [8]. Instead, trust based security scheme is used to safeguard the nodes of wireless sensor networks in the presence of malicious nodes. Trust models are influenced by the human behaviour model. According to Denning [9], trust cannot be treated as a property of trusted systems but rather it is an assessment based on experience that is shared through networks of people. As in real life, two entities with no previous mutual experience put confidence in each other's competence so as to realize their respective goals. These shared experiences lead to trust development that augments and decays with time and frequency of interactions [10].

Dynamic source routing protocol is the well known reactive routing protocol developed for wireless sensor networks where all nodes can faithfully execute in a munificent manner. However, such an altruistic stance is difficult to achieve in real life. So these protocols are more often executed by nodes that divert from basic requirements of participation. In order to maintain the impromptu nature of the sensor networks without making any extraneous assumptions, a trust based mechanism is applied to the DSR protocol to defend against compromised nodes. However, secure routing protocol such as secured dynamic source routing (S-DSR) protocol using trust scheme is available to evade sinkhole and wormhole attacks for static nodes of the sensor network. In this paper, an attempt has been made to implement S-DSR protocol in a mobile sensor network to circumvent sinkhole and wormhole attacks by including trust model in the dynamic source routing protocol. This S-DSR is simulated by using ns-2.30 for coverage areas of 300x300 m^2 and 500x500 m^2 with 150 and 200 numbers of nodes considering 40%mobile nodes in the network. The paper is organized as follows: Section 2 describes about the dynamic source routing protocol. Secured dynamic source routing protocol is explained in section 3. Simulation results are discussed in Section 4 to obtain delivery ratio, delay, routing overhead of the S-DSR and conclusions are drawn in Section 5.

2. Dynamic Source Routing Protocol

Dynamic Source Routing (DSR) protocol is an on-demand protocol designed to restrict the bandwidth consumed by control packets by

eliminating the periodic table- update messages. The major difference between this and other on-demand routing protocols(adhoc on demand distance vector routing protocol) is that DSR protocol is beacon less and hence does not require periodic hello packet (beacon) transmissions, which are used by node to inform its neighbours about its approach[11].

The DSR protocol is also a reactive routing protocol [12], which uses IP source routing. All data packets are affixed with a DSR source route header that contains the complete list of nodes. So, the packet has to traverse in the order given in the source route header to reach a particular destination. Each intermediate node, upon receiving a data packet, forwards the packet to the next hop as listed in the source route header [13]. DSR protocol consists of two phases such as route discovery and route maintenance.

2.1 Route Discovery

During route discovery, the source node broadcasts a ROUTE REQUEST packet with a unique identification number. The ROUTE REQUEST packet contains the address of the target node to which a route is desired [14]. All nodes that have no information regarding the target node append their IP addresses to the ROUTE REQUEST packet and rebroadcast it. In order to control the spread of the ROUTE REQUEST packets, the broadcast is done in a non propagating manner with the IP field being incremented in each route discovery. The ROUTE REQUEST packets keep on spreading until the time they reach the target node or any other node that has a route to the target node. Route discovery process with ROUTE RQUEST mechanism is shown in Fig.3. The recipient node creates a ROUTE REPLY packet, which contains the complete list of nodes that the ROUTE REQUEST packet had traversed. Route discovery process with ROUTE REPLY scheme is illustrated in Fig.4.The target node may respond to one or more incoming ROUTE REQUST packets depending upon implementation. Similarly, the source node may accept one or more ROUTE REPLY packets for a single target node. In the proposed model, DSR with multi-path is used [15] in which each ROUTE REQUEST packet received by the destination is responded by an independent ROUTE REPLY packet.

For optimization reasons, a PATH CACHE or a LINK CACHE scheme is maintained by the nodes [16]. When the nodes either forward or overhear the data and control packets to the other nodes, all types of information is added to their respective route cache. This information is used to limit the spread of control packets for subsequent route discoveries**.**

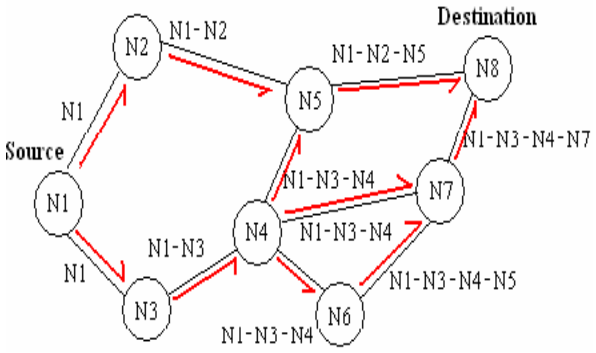

Fig.3.Route discovery process with route request

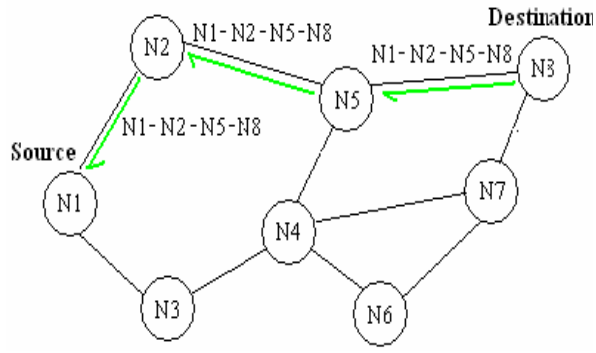

Fig.4.Route discovery mechanism with route reply

2.2. Route Maintenance

Routing maintenance refers to that each DSR node maintains a ROUTE CACHE which is used to record the route information of every hop to reach the other nodes .Otherwise, every node can snoop from the data packet transmitted by the neighbour. The process of the snooping can be used to analyse the route information recorded in the front of data packet, so that the node can record route information to its ROUTE CACHE if the route is a new one. Thus, more and more route information would be recorded to the ROUTE CACHE by the node and reduce the time in flooding the broadcast RREQ. Meanwhile the bandwidth of each node can also be saved. The process of routing maintenance detects the changing of network topology, and it knows whether the route is still available or not. When an

intermediate node removes from the range of wireless transmission or it is shutdown, the route is no longer available to use. When the upstream node detects the route failure by MAC layer protocol, it sends a RERR message to its upstream and source node. On receiving RERR, source node deletes all route information which includes the failure route from its ROUTE CACHE. If necessary, source node reinitiates a route discovery process in order to establish a new route to destination node. DSR can maintain numerous routes for one destination node. If the main route fails, a backup route can be used to transfer data. Thus, this mechanism avoids DSR flooding of RREQ frequently.

The drawback of this protocol is that the route maintenance mechanism does not locally repair a broken link. ROUTE CACHE information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than table-driven protocols.

Other drawback of DSR protocol is that this protocol is exposed to different types of attacks such as sinkhole and wormhole. Sinkhole attack may lure other sensor nodes to route all traffic through it which is described in Fig.5. The impact of sinkhole is that it can be used to launch further active attacks on the traffic, which is routed through it. On the other hand, the impact of the worm hole attack is that the tunnel essentially emulates shorter route and so network nodes prefer to use it rather than other alternate longer routes.

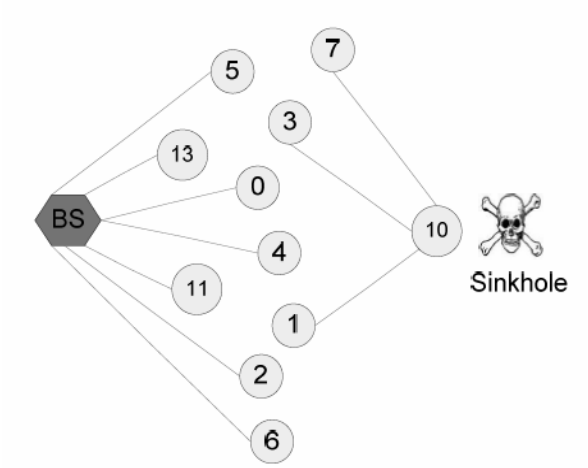

Fig.5. Sink hole attack

3. Secured Dynamic Source Routing Protocol

To detect and evade sinkholes and wormholes in the network, an effort return based trust model is used [17**]**. The trust model essentially performs the function of trust derivation, computation and application. During trust derivation, each node derives trust levels from directly experienced events. For accurate derivation of trust, the participating nodes need to support the features such as promiscuous mode operation, omni-directional transceivers and comparable transmission and reception ranges of transceivers. During trust computation, the monitored events are normalized and assigned weights so as to compute the direct trust in other nodes. These computed levels are then associated with the routing process during trust application.

The trust model uses the inherent features of the DSR protocol to derive and compute the respective trust levels in other nodes [18]. Each node executing the trust model, measures the accuracy and authenticity of its immediate neighboring nodes by monitoring their participation in the packet forwarding mechanism. The sending node verifies the different fields of source route header in the forwarded IP packet for requisite modifications through a sequence of integrity checks. If the integrity checks succeed, it confirms that the node has acted in a benevolent manner and so its direct trust counter is incremented. On the other hand, if the integrity check fails or the forwarding node does not transmit the packet at all, then its corresponding direct trust measure is decremented. The direct trust in a node y by node x is denoted by T_{xy} . It is given by the equation.1

$$T_{xy} = P_P \times P_A \quad (1)$$

where,

P_P is the situational trust category packet precision

P_A is the situational trust category packet acknowledgment

The category P_P and P_A are employed in combination to shield the DSR protocol from attacks. Detection and evasion process in S-DSR are used to eliminate sinkhole and wormhole attacks.

3.1. Detection Process

Each node buffers the DSR source route header and each forwarded packets for the Trust Update Interval (TUI) before transmitting the packet. The TUI is a very critical component of trust model and determines the time a sending node should wait after transmitting a packet until it overhears the retransmission by its neighbour [19]. After transmission of the packets, each node promiscuously listens for the neighbouring node to forward the packet. If the neighbour forwards the packet in the proper manner within the TUI, its corresponding trust level is incremented. However, if the neighbouring node modifies the packet in an unexpected manner, its trust level is decremented. This interval is critically related to the mobility and traffic of the network. If this TUI interval is made too small, it may result in ignoring of the retransmissions by an inefficient neighbor. Similarly, a large TUI value may cause energy costs and also induce errors due to nodes getting out of reception range.

3.2. Evasion Process

In the DSR, the LINK CACHE is first scanned for a working route to the destination, before initiating a new route discovery. If there is no unavailability of a route from the LINK CACHE in the DSR, then Dijkstra algorithm [20] is used to find the route to reach the destination. This algorithm returns the shortest path to any destination in terms of number of hops. But, if the status of the link end node is classified as a wormhole, the cost of that link is set to infinity. So, a modified variant of the search algorithm is implemented , which finds routes with the maximum trust level, thereby evading any possible sinkholes and wormholes. There may be circumstances in which the source node may not have sufficient trust information regarding all the mobile nodes in the computed path of DSR protocol [21]. To deal with such situations, a salvaging mechanism is implemented in S-DSR. In S-DSR, the forwarding nodes verify the trust levels of all nodes present in the packet's source route header, instead of checking the connectivity of the next hop. With the standard DSR protocol, all immediate nodes blindly forward the packets to the succeeding nodes listed in the source route header.

However in the S-DSR protocol, the trust level of all the remaining nodes in the source route is first verified for the existence of a sinkhole or a wormhole. Only in case of absence of such malicious nodes, the packets are forwarded as per the source route header. However, in case where malicious nodes are present in the source route header, that particular packet is dropped and a corresponding ROUTE ERROR packet is sent to the originator of the data packet.

4. Simulation Results and Discussion

The trust and mobility model is implemented in the existing DSR protocol to obtain the S-DSR protocol. The S-DSR protocol is simulated using ns-2.30 [22] to emulate sinkhole and wormhole attacks in the mobile sensor network. The performance parameters such as delivery ratio, delay and routing overhead are calculated by varying the numbers of malicious nodes from 5 to 25 .The parameters used in the simulation are listed in Table 1.

The sample NAM output is shown in Fig.6 for the mobile sensor network with six malicious nodes. Using S-DSR protocol, the packets will reach the destination node from the source nodes leaving the compromised nodes

Table.1 Simulation Parameters

Simulation Parameters	Values
Simulation time (s)	100
Simulation area (m^2)	300×300 and 500×500
Number of nodes	150 and 200
Number of malicious nodes	5 to 25
Mobility model	Random way point
Traffic type	CBR
Packet size(bytes)	512

4.1. Delivery Ratio

It is the ratio between the numbers of packets received by the application layer of the destination nodes to the number of packets sent by the source nodes. Delivery ratio of S-DSR is higher than that of

DSR which is proved through Fig.7(a), Fig.7 (b),Fig.7(c) and Fig.7(d). On increasing the values of malicious nodes, S-DSR outperforms DSR by providing nearly 45% for 150 and 200 nodes. The improvement in delivery ratio is due to trusted path and elimination of attackers

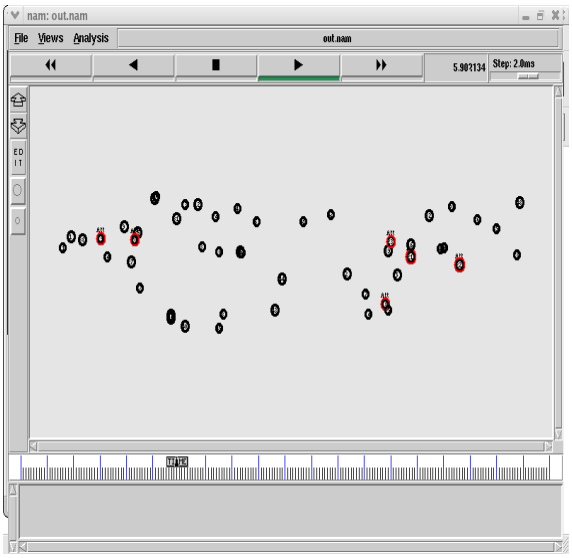

Fig. 6.NAM output of mobile sensor networks with six malicious nodes

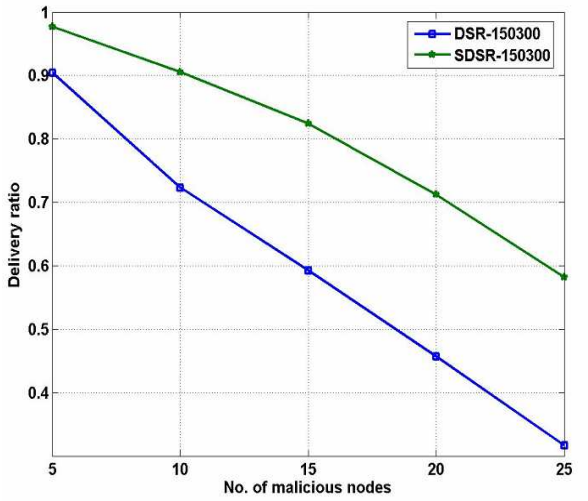

Fig. 7(a) Delivery ratio Vs no. of malicious nodes for 150 nodes with coverage area 300x300 m^2

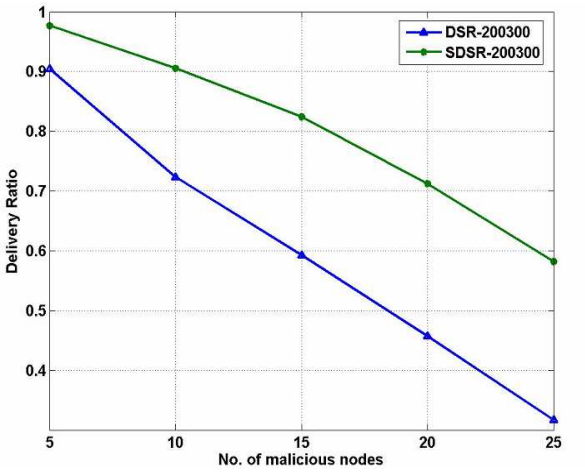

Fig. 7(b) Delivery ratio Vs no. of malicious nodes for 200 nodes with coverage area 300x300 m^2

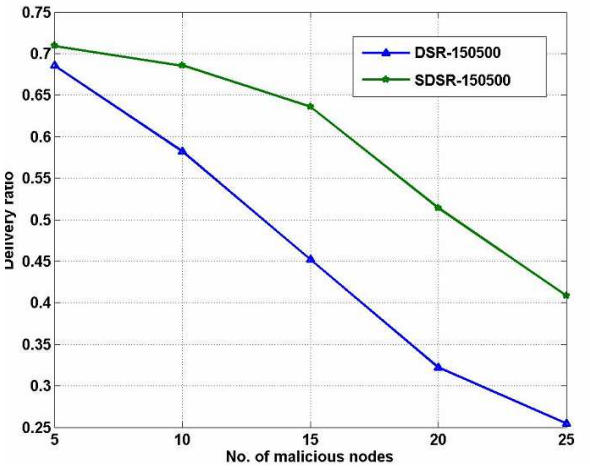

Fig. 7(c) Delivery ratio Vs no. of malicious nodes for 150 nodes with coverage area 500x500 m^2

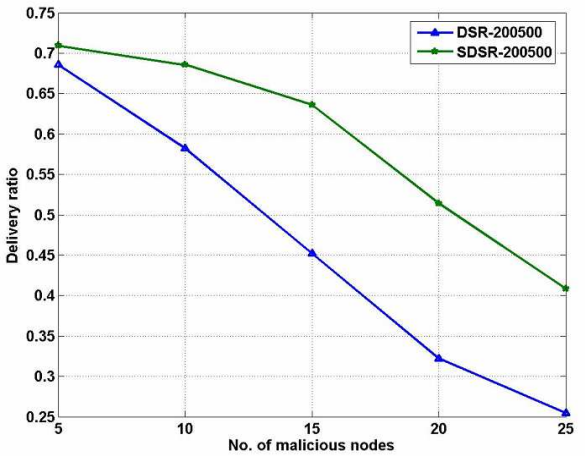

Fig. 7(d) Delivery ratio Vs no. of malicious nodes for 200 nodes with coverage area 500x500 m^2

4.2. Routing Overhead

It is the ratio between total numbers of control packets generated to total number of data packets received during simulation time. S-DSR has an overall lower routing overhead compared to that of DSR. This is proved through the results illustrated in Fig.8(a), Fig.8(b), Fig.8(c) and Fig.8(d). S-DSR achieves significant reduction in routing overhead of nearly 70% compared to that of DSR for higher values of malicious nodes. The reduced overhead is due to less number of control packets generated for each data packet in S-DSR.

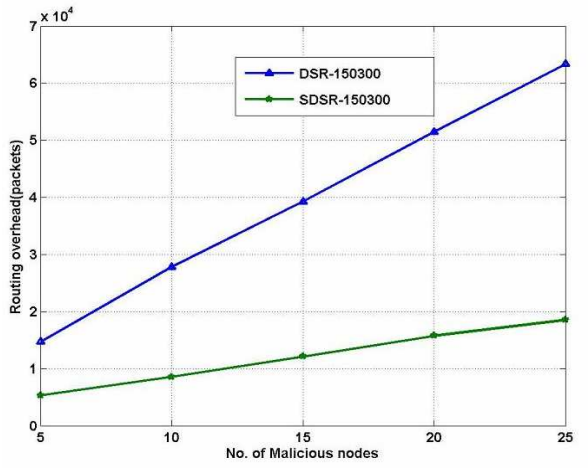

Fig.8 (a) Routing overhead Vs no. of malicious nodes for 150 nodes with coverage area 300x300 m^2

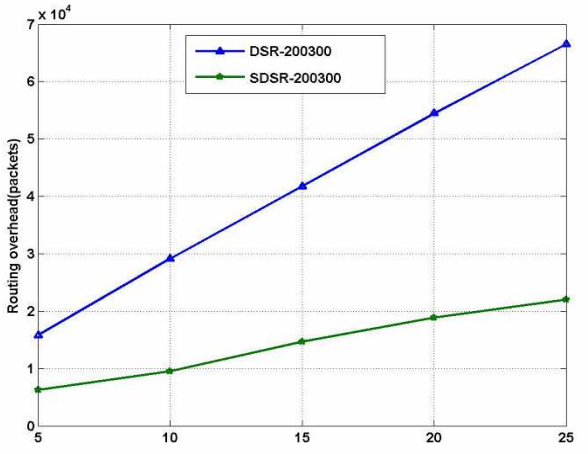

Fig.8 (b) Routing overhead Vs no. of malicious nodes for 200 nodes with coverage area 300x300 m^2

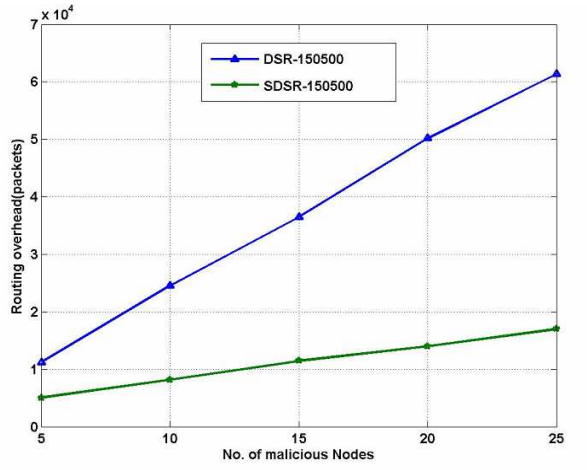

Fig.8 (c) Routing overhead Vs no. of malicious nodes for 150 nodes with coverage area 500x500 m^2

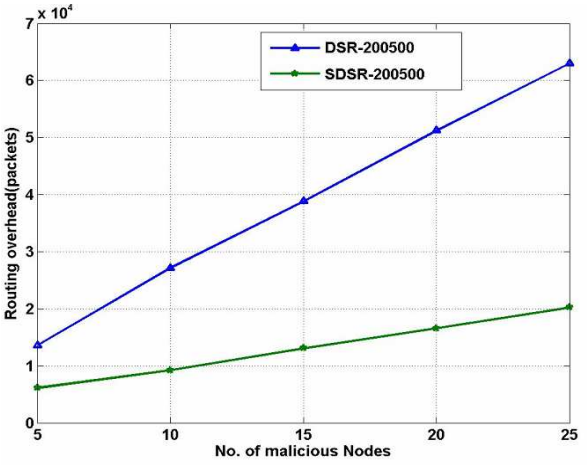

Fig.8 (d) Routing overhead Vs no. of malicious nodes for 200 nodes with coverage area 500x500 m^2

4.3. Delay

Delay is the time (in seconds) taken by packets to reach their respective destinations. Delay of S-DSR protocol is higher than DSR protocol for large number of malicious nodes .This is verified through simulation results shown in Fig.9(a), Fig.9(b), Fig.9(c) and Fig.9(d). The additional delay of S-DSR protocol is permissible compared to that of DSR protocol which varies between 3%-6%. This is due to the fact that, the routes obtained from the LINK CACHE information of the node are not optimal in terms of hops but instead consists of nodes that have been found to more trustworthy than the others.

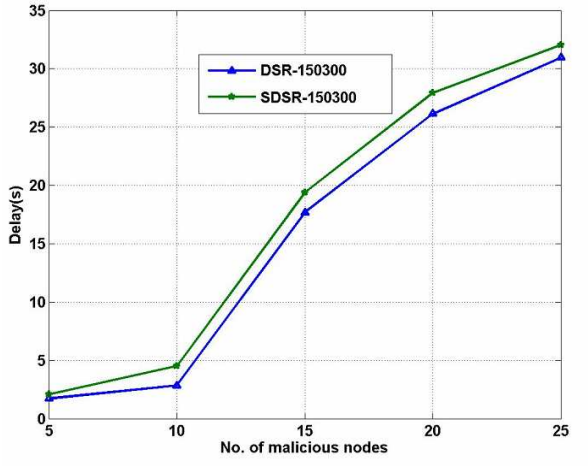

Fig. 9(a) Delay Vs no. of malicious nodes for 150 nodes with coverage area 300x300 m^2

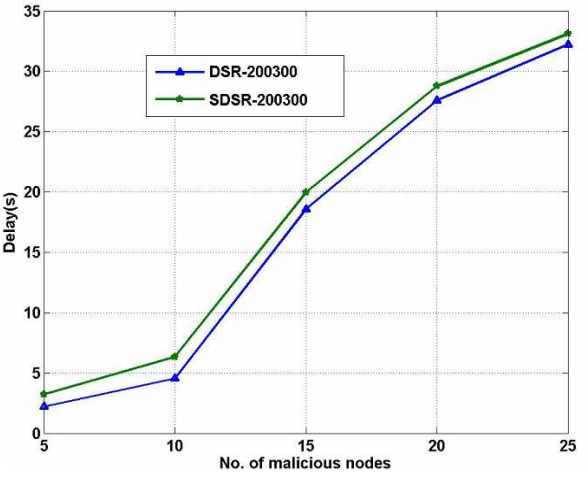

Fig. 9(b) Delay Vs no. of malicious nodes for 200 nodes with coverage area 300x300 m^2

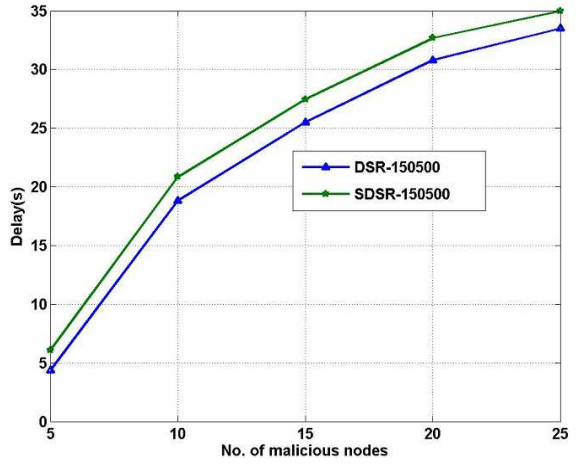

Fig. 9(c) Delay Vs no. of malicious nodes for 150 nodes with coverage area 500x500 m^2

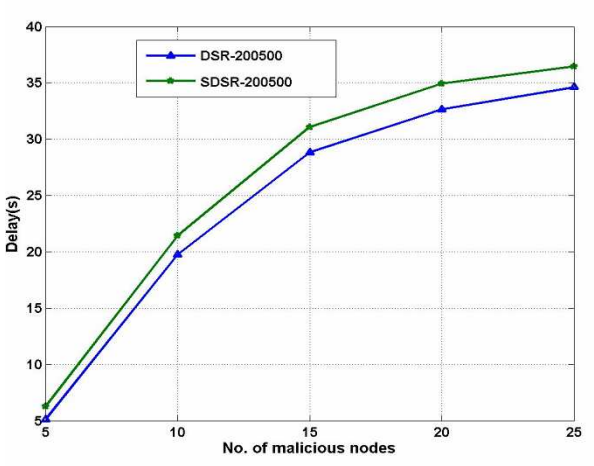

Fig. 9(d) Delay Vs no. of malicious nodes for 200 nodes with coverage area 300x300 m^2

5. Conclusion

Secured dynamic source routing protocol is implemented for mobile sensor network by using ns-2.30.It is also compared with dynamic source routing protocol by varying the number of malicious nodes from 5 to 25 considering 150 and 200 nodes for different coverage areas of 300x300 m^2 and 500x500 m^2. The results show that on an average, improvement of 45% in delivery ratio and reduction of 70% in routing overhead is achieved using the S-DSR protocol than the standard DSR protocol. In addition, an increment of nearly 5% in delay has been obtained in S-DSR protocol, which is a acceptable factor even with 40% malicious nodes in the network. This is mainly due to suitable trust values and proper routing decision taken by S-DSR to get rid of the nodes that were acting as sinkholes or wormholes.

References

[1] Jamal N.Al-Karaki, and Ahmed E.Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey", *Proceedings of 1st ACM International Workshop on Wireless Sensor Networks and Applications*, Alanta, Georgia, USA, 2002.

[2] S.Carter and A.Yasinac, Y.C.Hu, "Secure position aided adhoc routing protocol", *Proceedings of the IASTED Conference on Communications and Computer Networks*

(CCN), Cambridge, MA, USA, pp.329-324, November, 2002.

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

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

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

[6] Y.C.Hu, A.Perrig and D.B.Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks", *Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications Societies*, San Francisco, CA, USA, vol.3, pp.1976-1986, 2003.

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

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

[9] D.Denning, "A New Paradigm for Trusted Systems", *Proceedings of ACM New Security Paradigms Workshop*, Novascotia, Canada, pp. 36-41, September 2004.

[10] A.Amir Pirzada, C.Mc.Donald and A.Datta , "Performance Comparison of Trust Based Reactive Routing Protocols", *IEEE Transcations on Mobile Computing*, Vol.5 No.6 , June 2006.

[11] G.Siva Ram Murthy and B.S.Manoj, "Ad Hoc Wireless Networks Architectures and Protocols",Pearson Education,2nd Edition,2007

[12] Gaurav Sethi and Manoj Kumar, "Simulation and Comparison of Communication Protocols in Adhoc Networks", *Proceedings of 7th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications*, Cambridge, UK, February 2008.

[13] G.E.Rizos,D.C. Vasiliadis and E.Stergiou, "Comparative Study of Demand Driven Routing Protocols over Mobile Adhoc Networks", *Proceedings of 13th WSEAS International conference on Communications*, Rodos Island, Greece, July 2009.

[14] Abdullah Gani, Qi Han, Nor Badrul, Anuar and Omar Zakaria, "Enhancing DSR Protocol Performance in Mobile Adhoc Network using ACK Reply", *WSEAS Transcations on Communications*,Vol.8,No.2, pp.227-236, February 2009.

[15] D.B.Johnson, D.A.Maltz, and Y.Hu, "The dynamic source routing protocol for mobile ad-hoc networks", *Internet Engineering Task Force on Mobile Adhoc Networks, (IETF MANET)*, February 2003.

[16] A.Nasipuri and S.Das, "On-demand multi-path routing for mobile ad-hoc networks", *Proceedings of the Eight International Conference on Computer Communications and Networks*, Boston, USA, pp.64-70, October, 1999.

[17] Houssein Hallein,Seyed A .Shahrestani, "Mitigating of the Effects of Selfish and Malicious Nodes in Adhoc Networks", *WSEAS Transcations on Computers*,Vol.8,No.2,February 2009.

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

[19] Asad Amir Pirzada and Chris McDonald, "Circumventing Sinkhole and Wormholes in Wireless Sensor Networks", *Proceedings of 2nd IEEE International Workshop on Wireless Adhoc Networking*, Columbus, USA, June 2005.

[20] E.W.Dijkstra, "A note on two problems in connection with graphs", *Numerische Mathematics*, pp.83-89, 1959.

[21] A.Pirzada, A.Datta and C.Mc.Donald, "Trust based routing for ad-hoc wireless networks," *Proceedings of 12th IEEE International Conference on Networks (ICON'04)*, Singapore, pp.326-330, November 2004.

[22] I.Downard, "Simulating sensor networks in ns-2," *NRL Formal Report* 5522-04-10, Naval Research Laboratory, 2004.

Bibliography

P. Samundiswary received the B.Tech degree in 1997 and M.Tech degree in Electronics and Communication Engineering from Pondicherry Engineering College, India in 2003. She is pursuing her Ph.D. programme in the Dept. of Electronics and Communication Engineering, Pondicherry Engineering College affiliated to Pondicherry University, India. She is currently working as Assistant Professor in the Dept. of Electronics and Communication Engineering at Sri Manakula Vinayagar Engineering College affiliated to Pondicherry University, India. Her research interests include wireless communication and wireless sensor networks.

P.Dananjayan received Bachelor of Science from University of Madras in 1979, Bachelor of Technology in 1982 and Master of Engineering in 1984 from the Madras Institute of Technology, Chennai and Ph.D. degree from Anna University, Chennai in 1998. He is working as a Professor in the Dept. of ECE, Pondicherry Engineering College, Pondicherry, India. He is also a Visiting Professor to AIT, Bangkok. He has more than 70 publications in National and International Journals. He has presented more than 150 papers in National and International conferences. He has produced 9 Ph.D candidates and is currently guiding six Ph.D students. His areas of interest include Spread spectrum Techniques and Wireless Communication