The International Journal of Engineering
And Science (IJES)
||Volume|| 1 ||Issue|| 2 ||Pages|| 98-105 ||2012||
ISSN: 2319 – 1813 ISBN: 2319 – 1805

ENHANCED GREEDY PERIMETER STATELESS ROUTING PROTOCOL (E-GPSR)

[1,]Kamiya shrivastava, [2,] Asst Professor Satendra .k. Jain
[1,]M.Tech, Research Scholar
[1,2,]Department of Computer Application Samrat Ashok Technological Institute
Vidisha (M.P.)

----------Abstract----------
Wireless sensor networks are collections of large number of sensor nodes. The sensor nodes are featured with limited energy, computation and transmission power. Each node in the network coordinates with every other node in forwarding their packets to reach the destination. Since these nodes operate in a physically insecure environment; they are vulnerable to different types of attacks such as selective forwarding and sybil. These attacks can inject malicious packets by compromising the node. Geographical routing protocols of wireless sensor networks have been developed without considering the security aspects against these attacks. In this paper, a more efficient routing protocol named enhanced greedy perimeter stateless routing protocol (E-GPSR) is proposed for mobile sensor networks by incorporating the concept of 'observation time' to the existing trust based secured greedy perimeter stateless routing protocol (S-GPSR). Simulation results proves that 'Enhanced greedy Perimeter stateless Routing' outperforms the S-GPSR by reducing the over head and improving the delivery ratio of the network.

Keywords: Wireless sensor network, GPSR protocol, secured GPSR, Enhanced GPSR, compromised nodes, Sybil attack, selective forwarding attack.

Date of Submission: 1, December, 2012 ⟺ Date of Publication: 15, December 2012
---

1. Introduction

1.1 Wireless sensor Network

Wireless sensor networks (WSN) are now used in many applications including military, environmental, healthcare applications, home automation and traffic control. It consists of a large number of sensor nodes, densely deployed over an area. A wireless sensor network [1] typically consists of a very large number of small, inexpensive, disposable, robust, and low power sensor nodes working cooperatively. Wireless sensor network generally composed of a large number of distributed sensor nodes that organize themselves into a multi-hop wireless network. Each network is equipped with more than one sensors, processing units,

controlling units, transmitting units etc. Typically, the sensor nodes coordinate themselves to perform a common task. Sensor nodes are capable of collaborating with one another and measuring the condition of their surrounding environments. The sensed measurements are then transformed into [2] digital signals and processed to reveal some properties of the phenomena around sensors. Due to the fact that the sensor nodes in WSN have short radio transmission range, intermediate nodes act as relay nodes to transmit data towards the sink node using multipath. The deployment of sensor nodes based upon the application types.

Recently wireless sensor networks have drawn a lot of attention 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 inattention of the deployed nodes, attackers can easily capture and rework them as malicious nodes. Karloff and Wagner also have revealed that routing protocols of sensor networks are insecure and highly vulnerable to malicious nodes

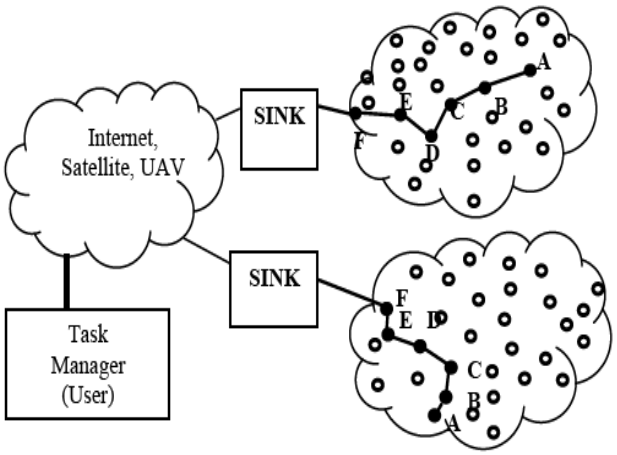


Figure 1: Basic structure of a Wireless sensor Network

It can either join the network externally or may originate internally by compromising an existing benevolent node . The attacks launched by internally generated compromised nodes are the most dangerous type of attacks. These compromised nodes can also carry out both passive and active attacks against the networks . In passive attack a malicious node only eavesdrops upon the packet contents, while in active attacks it may imitate, drop or modify legitimate packets . Sinkhole is one of the common type of active attack in which a node, can deceitfully modify the routing packets. 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, 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 and the creation of a centralized or distributed key repository to realize different security services in the network. This paper is organized as follow : Section 2 describes about the greedy perimeter stateless routing (GPSR). Section 3 deals with the Secured GPSR (S-GPSR). Section 4 elaborates the proposed Enhanced Greedy Perimeter Stateless Routing (E-GPSR) for Wireless Sensor Network. Simulation result are described in section 5. Section 6 defines the conclusion.

2. Greedy Perimeter Stateless Routing

Routing in sensor networks is very challenging due to several characteristics that distinguish them from contemporary communication and wireless ad-hoc networks. First of all, it is not possible to build a global addressing scheme for the deployment of sheer number of sensor nodes. Therefore, traditional IP-based protocols cannot be applied to sensor networks. Second, in contrary to typical communication networks almost all applications of sensor networks require the flow of sensed data from multiple sources to a particular sink. Third, generated data traffic has significant redundancy in it since multiple sensors may generate same data within the vicinity of a phenomenon. Such redundancy needs to be exploited by routing protocols to improve energy and bandwidth utilization. Fourth, sensor nodes are tightly constrained in terms of transmission power, on-board energy, processing capacity and storage and thus require careful resource management. Due to the above differences, many new algorithms have been proposed for the problem of routing data in sensor networks. These routing mechanisms have considered the characteristics of sensor nodes along with the application and architecture requirements. Almost all routing protocols can be classified as data-centric, hierarchical or location-based although there are few distinct ones based on network flow or QoS awareness. Data-centric protocols are query-based and depend on the naming of desired data, which helps in eliminating many redundant transmissions. Hierarchical protocols aim at clustering the nodes so that cluster heads can do some aggregation and reduction of data in order to save energy . Location-based protocols utilize the position information to relay the data to desired regions rather than the whole network. The Greedy Perimeter Stateless Routing is one of the commonly used location-based routing protocols for establishing and maintaining a sensor network. This protocol virtually operates in routing. In GPSR, it is assumed that all nodes recognize the geographical position of destination node with which communication is desired. This location information (i.e.) geographical position is also used to route traffic to its requisite destination from the source node through the shortest path. Each transmitted data

packet from node contains the destination node's identification and its geographical position in the form of two four-byte float numbers. Each node also periodically transmits a beacon, to inform its adjacent nodes regarding its current geographical co-ordinates. The node positions are recorded, maintained and updated in a neighborhood table by all nodes receiving the beacon. To reduce the overhead due to periodic beacons, the node positions are piggy-backed onto forwarded data packets. GPSR supports two mechanisms for forwarding data packets: greedy forwarding and perimeter forwarding

2.1 .Greedy Forwarding

In the first mechanism, all data packets are forwarded to an adjacent neighbor that is geographically positioned closer to the intended destination. This mechanism is known as greedy forwarding. The forwarding is done on a packet to packet basis. Hence, minimal state information is required to be retained by all nodes. It makes protocol most suitable for resource starved devices. The greedy forwarding mechanism is shown in Figure1. However, this mechanism is susceptible to failure in situations where the distance between forwarding node and final destination is less than the distance between the forwarding node's adjacent neighbors and destination.

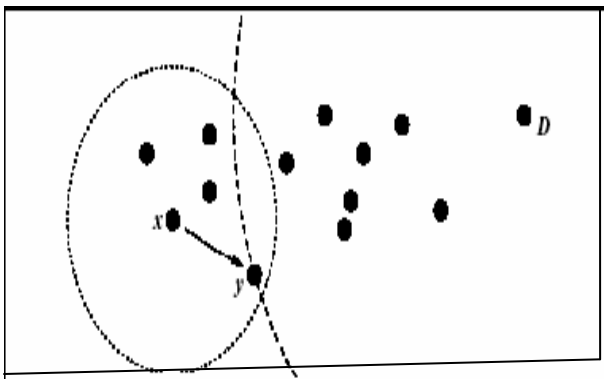


Figure 1. Greedy forwarding mechanism

2.2. Perimeter Forwarding

To overcome routing problems in such scenarios, GPSR engages perimeter forwarding mode. In perimeter mode, the data packet is marked as being in perimeter mode along with the location where greedy forwarding failed. These perimeter mode packets are forwarded using simple planar graph traversal. Each node receiving a data packet marked as in perimeter mode uses the right-hand rule to forward packets to nodes, which are located counterclockwise to the line joining forwarding node and the destination. The perimeter forwarding mechanism is shown in Figure 2. Each node, while forwarding perimeter mode packets, compares its present distance to the destination from the point where greedy forwarding has failed. If the current distance is less, packet is routed through greedy forwarding repeatedly from that point onwards. The protocol has been designed and developed based on the assumption that all nodes in the network would execute the protocol in a sincere manner. However, due to number of reasons including malice, incompetence and selfishness, nodes frequently deviate from defined standards leading to routing predicaments.

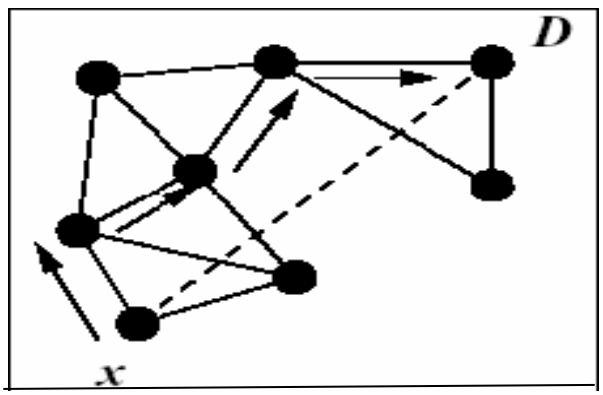


Figure 2. Perimeter forwarding mechanism

3. SECURED GREEDY PERIMETER STATELESS ROUTING (S-GPSR)

GPSR scans its neighborhood table to retrieve the next hop which is optimal and leads to the destination, during packet transmission to a known host. As there may be more than one such hop available, GPSR selects an adjacent neighbor that has the least distance to a particular destination. In S-GPSR, the trust levels used in conjunction with the geographical distances are incorporated in the neighborhood table to create the most trusted distance route rather than the default minimal distance To compute direct trust in a node, an effort-return based trust model is used . The accuracy and sincerity of immediate neighboring nodes is ensured by observing their contribution to packet forwarding mechanism. To implement the trust derivation mechanism, Trust Update Interval (TUI) of each forwarded packet is buffered in the node as (GPSR Agent::buffer packet). The TUI is a very critical component of such a trust model. It determines the time a node should wait before assigning a trust or distrust level to a node based upon the results of a particular event. After transmission, each node promiscuously listens for the neighboring node to forward the packet. If neighbor forwards the packet in proper manner within the TUI, its corresponding trust level is incremented. However, if the neighboring node modifies the packet in an unexpected manner or does not forward the packet at all, its trust level is decremented. Every time a node transmits a data or control packet, it immediately brings its receiver into promiscuous mode (GPSR Agent::tap), so as to overhear its immediate neighbor forwarding the packet . The sending node verifies the different fields in the forwarded IP packet for requisite modifications through a sequence of integrity checks (GPSR Agent::verify packet integrity). 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 checkfails or the forwarding node does not transmit the packet at all, then its corresponding direct trust measure is decremented so that the node is treated as malicious node. The S-GPSR is explained by using flow chart which is illustrated through Figure 3.

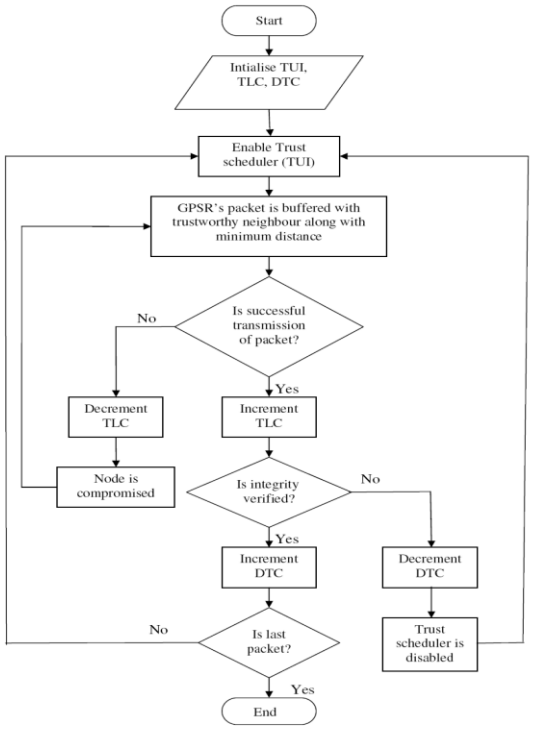


Figure 3. Flowchart of S-GPSR

4. Enhanced Greedy Perimeter Stateless Routing (E-GPSR)

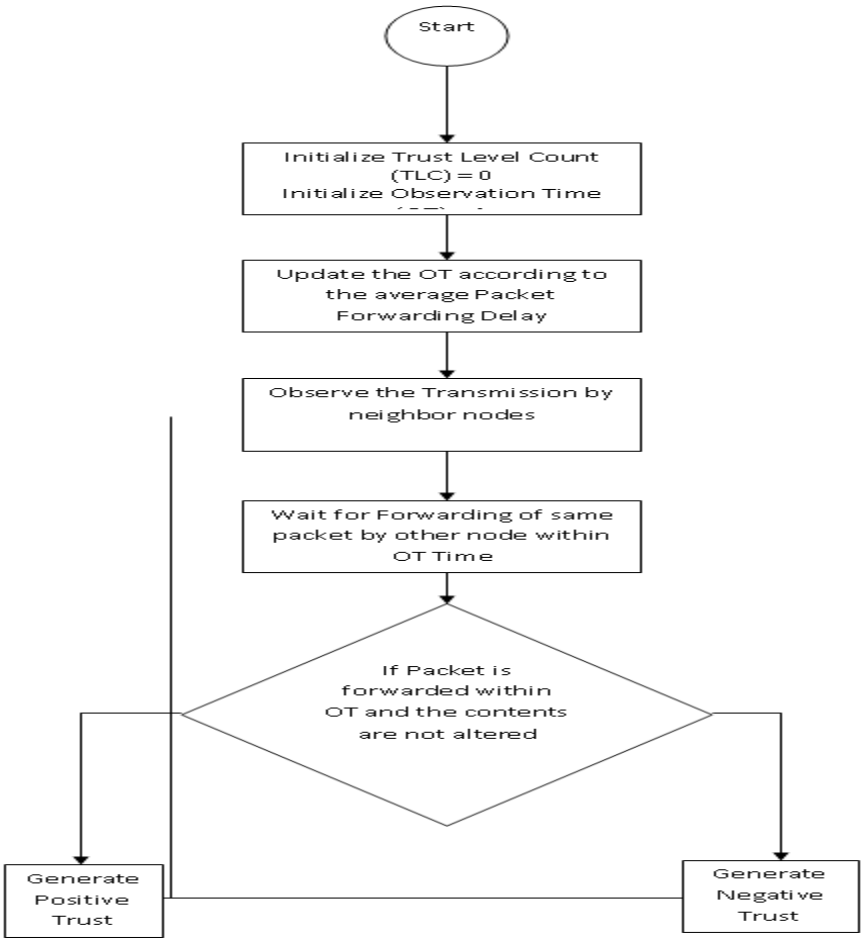
In the basic GPSR method, it scans its neighborhood table to retrieve the next hop which is optimal and leads to the destination during packets transmission or data transmission to known host. As there may be more than one such hop available , GPSR selects an adjacent neighbor that has the least distance to a particular destination. In contrast to GPSR , Secured greedy perimeter stateless routing (S-GPSR) introduced the concept of trust level which resulted a more secured routing over a geographical area or over a location based routing. But again S-GPSR lacked in terms of efficiency as a common or constant trust update interval for several nodes may be troublesome in case of heavy traffic. Efficient greedy perimeter stateless routing (E-GPSR) introduces the concept of "OBSERVATION TIME (OT)" for each node separately in addition to the trust level. Both these Observation time (OT) and Trust level (TLC) is incorporated in the neighborhood table to established the most trusted distance route rather than the default minimal distance which not optimum distance. To compute direct

trust and an optimal next node's address , an effort return based model is used . The mechanism proves to be more efficient as the analysis is being observed on the basis of the accurate and sincere contribution of the immediate neighbor nodes. The whole mechanism of generating the secure, trust base and efficient model consist of two major steps:

1. Generation of Observation time for each node.
2. Trusted route selection

4.1 GENEARTION OF OBSERVATION TIME FOR EACH NODE:

Since the trust level count (TLC) , for each node that forwards a packet is initialized ,at the same time the " Observation Time" of each node is maintained ,which is calculated on the account of the buffered forwarded data packets in the node (GPSR Agent :: buffer packet



). The Observation Time is very critical and important measure for efficient routing. It determines the time that a node takes to decide a most trusted and minimal route rather than a default minimal distance. The Observation time counter (OTC) is maintained by the observation of the neighboring nodes. The Observation Time Counter (OTC) field is updated by the monitoring of the average packet forwarding delay. Each time, if the packet is forwarded within the Observation Time the POSITIVE TRUST is generated for the particular node, else the NEGATIVE TRUST is generated for the Forwarding node

4.2 .TRUSTED ROUTE SELECTION

Whenever a packet is to be forwarded a best and optimal node is to be selected. The selection of the trusted node is done on the basis of the TRUST COUNT for each nodes. A node with best TRUST COUNT is selected as the next node to be forward the packet along with the optimal minimum distance. Every time a node transmits a data packet within an OBSERVATION TIME , its neighbors overhears it immediately (forwarding packet) . The sending node verifies the different field in the forwarded IP packets and check for integrity. If the integrity check succeeds, it confirms that the node has acted in a benevolent manner.

5. Simulation Results

The trust and the mobility model is implemented in the existing S-GPSR protocol to obtain Enhanced GPSR protocol. The E-GPSR protocol is simulated using OPNET 14.0 to emulate selective forwarding and Sybil attacks in mobile sensor networks. The network animator outputs for 100 nodes with 10 malicious nodes. The performance parameters such as delay, packet dropped, routing traffic received and traffic sent and received bits/ sec and packets/ sec is calculated.

SIMULATION PARAMETRS	VALUES
No. Of Nodes	100-150
Graphical Area	100X 100 m
Packet Size	512
Traffic Type	CBR
No . of Malicious Nodes	5 to 25
Simulation Time	100 s

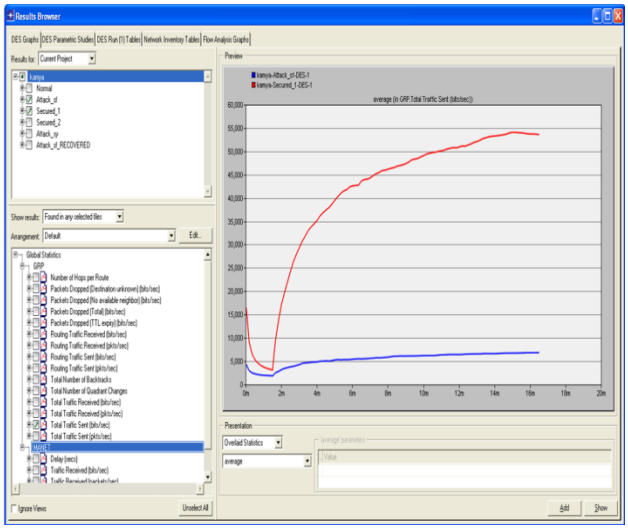


Fig : Total traffic sent in case of selective forwarding and E-GPRS method and S-GPRS

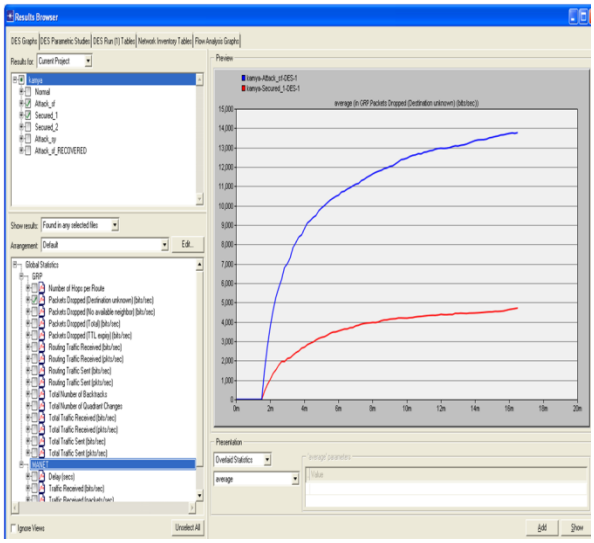


Fig : total packets dropped in case of selective forwarding attack

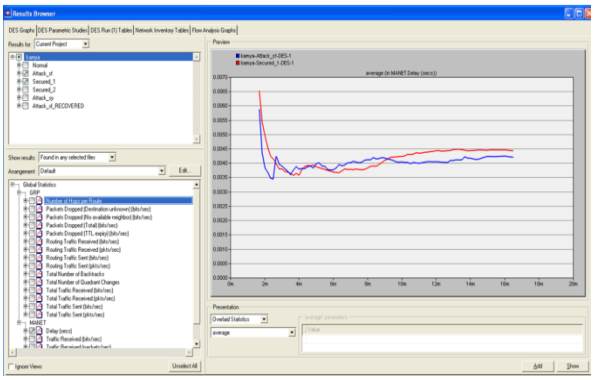


Fig : total delay in case of Selective Forwarding attack

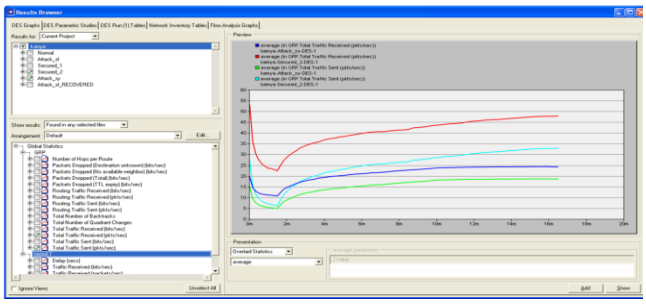


Fig : total traffic sent in case of Sybil attack

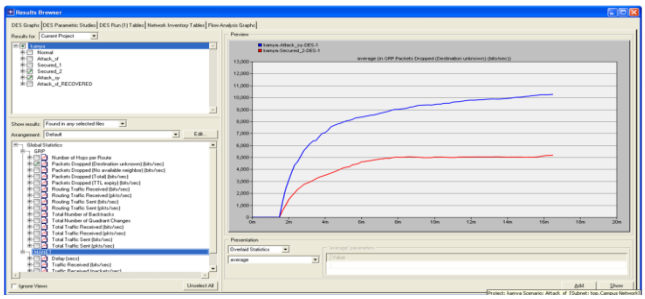


Fig : packets dropped in case of Sybil attack

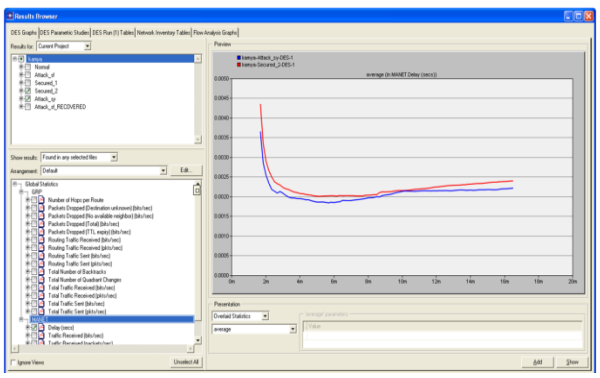


Fig :Total delay in case of Sybil attack

6. Conclusion

Enhanced greedy perimeter stateless routing protocol is implemented for mobile sensor network with different coverage area considering 100 and 150 number of nodes for simulation. It is compared with secured greedy perimeter stateless routing protocol for different number of malicious nodes. The results show that on the average, the routing overhead achieved using the E-GPSR protocol was 7o% less than the standard S-GPSR protocol. Further more, an improvement of 25% in the delivery ratio have been achieved in the E-GPSR protocol. The improvement in the above mentioned network performance is mainly due to smaller trust values, shorter routing decisions and less number of control packets taken by the trust based model implemented in GPSR to get rid of the attackers.

REFERENCES :

[1] C.Karlof & D.Wagner, (2003) "Secure routing in wireless sensor networks: Attacks & countermeasures", Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols & Applications, Anchorage, AK, pp.113-127.

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

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

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

[5] Adrian Perrig & Robert Szewczyk, Victor Wen, David Culler & J.D.Tygar,(2001) "SPINS: Security Protocols for Sensor Networks", Proceedings of ACM Seventh Annual International Conference on Mobile Computing & Networking, Rome, Italy, pp.189-199.

[6] W.Stallings, (2000) Network Security Essentials, Prentice Hall.

[7] Asad Amir Pirzada & Chris McDonald, (2005) "Circumventing sinkholes & wormholes in wireless sensor networks", Proceedings of 2nd IEEE International Workshop on Wireless Ad-hoc Networking, Columbus, USA, pp.132-150.

[8] Jamal N.Al-Karaki and Ahmed E.Kamal, (2004) "Routing Techniques in Wireless Sensor Networks: A Survey", IEEE Transactions on Wireless Communication, Vol. 11, No.6, pp.6-20.

[9] Brad Karp & H.T.Kung, (2000) "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks", Proceedings of Sixth Annual International Conference on Mobile Computing & Networking, Boston, pp.243-254.

[10] A.Pirzada & C.McDonald, (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.

[11] Asad Amir Pirzada & Chris McDonald, (2007) "Trusted greedy perimeter stateless routing", Proceedings of 15th IEEE International Conference on Networks (ICON 2007), Adelaide, Australia, pp.206-211.