Securing OLSR and STAR Routing Protocols Against Packet Dropping by Malicious Nodes

Harish Shakywar
SOIT RGPV, Bhopal, India

Sanjeev Sharma
SOIT, RGPV, Bhopal, India

Santoh Sahu
SOIT, RGPV, Bhopal, India

ABSTRACT
Mobile Ad-hoc networks are those networks which has no physical links between the nodes. In MANET mobile nodes dynamically forming a network topology without the use of any existing network infrastructure or centralized administration. Routing in a MANET is challenging because of the dynamic topology and the lack of an existing fixed infrastructure. In most of their specifications it is assumed that all the nodes in the network are friendly. But in the open, collaborative MANET environment practically any node can maliciously or selfishly disrupt and deny communication of other nodes. Security in MANET is a very difficult problem to incorporate without degrading the performance of the protocol. There are various security issues associated with OLSR and STAR routing protocols among which one is packet dropping by malicious node. In this paper we have proposed one approach to minimize the packet dropping by malicious nodes in the network by applying IPSec in OLSR and STAR routing protocols and compared the results with existing without IPSec protocols. The simulation results demonstrate the success of the proposed approach and maximize the overall performance of MANET in presence of malicious nodes.

Keywords
IPSec, OLSR, STAR, MANET, Malicious node.

1. INTRODUCTION
Mobile Ad hoc networks (MANET) [1] is a kind of wireless Ad-hoc networks and is a self-configuring network of mobile routers (and associated host) connected by wireless links the union of which form an arbitrary topology. Each node of an ad hoc network can both route and forward data. The routers are free to move randomly and organize themselves arbitrarily thus the network's wireless topology may change rapidly and unpredictably. Such a networks may operate in a standalone fashion or may be connected to the larger Internet. It is an autonomous system [2] in which wireless nodes that can be dynamically be set up anywhere and anytime without using any pre-existing network infrastructure. Security [5] in Mobile Ad hoc Network is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of the its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. MANETs must have a secure way for transmission and communication and this is quite challenging and vital issue as there is increasing threats of attack on the Mobile Network. Security is the cry of the day. In order to provide secure communication and transmission engineer must understand different types of attacks and their effects on the MANETs.

The applications of the ad- hoc network are vast. It is used in areas of Sensor networks for environmental monitoring, Rescue operations in remote areas, Remote construction site and Personal area Networking, Emergency operations, Military environments, Civilian environments.

The rest of this paper is organized as follows. Section 2 gives Ad-hoc routing protocols. Section 3 briefly describes OLSR and STAR routing protocol. Section 4 discusses problem statement. Section 5 IPSec in MANETs. Section 6 describes proposed methodology. Section 7 presents simulation environment. Section 8 gives experimental results. Section 9 presents conclusion and future work.

2. AD-HOC ROUTING PROTOCOLS
The fundamental [3] idea of a routing protocol is to deliver the messages from source to destination with enhanced performance in terms of delay and security. Routing protocols are generally necessary for maintaining effective communication between distinct nodes. Routing protocol [4] not only discovers network topology but also built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes.

Routing protocols [5] in MANETs are classified into three different categories according to their functionality.

1. Reactive(On-demand) protocols
2. Proactive(Table driven) protocols
3. Hybrid protocols

Figure 1 shown classification of Ad-hoc routing protocols.

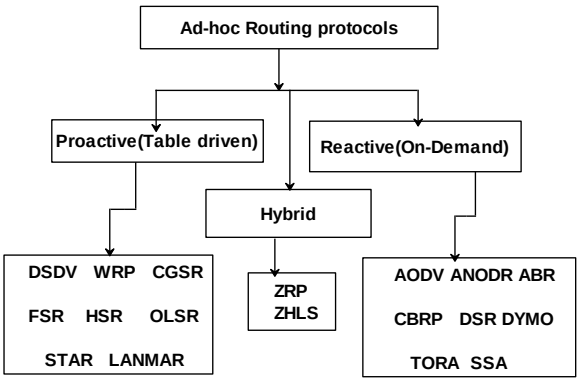

Figure 1 - Classification of Ad-hoc routing protocols

2.1 Proactive (Table driven) protocols

Proactive routing protocols [5] maintain information continuously. Typically, a node has a table containing information on how to reach every other node and the algorithm tries to keep this table up-to-date. Whenever there is a change in the network topology, these tables are update according to the changes. The nodes exchange topology information with each other; they can have route information any time when they needed. Some table driven protocols are- DSDV, FSR, OLSR, STAR etc.

2.2 Reactive (On-demand) protocols

Reactive protocols [3][5] also known as on demand driven reactive protocols. The fact they are known as reactive protocols is, they do not initiate route discovery by themselves, until they are requested, when a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destinations. The route remains valid till the destination is reachable or until the route is no longer needed. Some on-demand protocols are- AODV, DYMO, TORA etc.

2.3 Hybrid protocols

Hybrid routing protocols are a new generation of protocol. It exploits the strengths of both proactive and reactive protocols and combine them together to get better results. The network is divide into zones and use different protocols in two different zones i.e. one protocol is used within zone and the other protocol is used between them. Each zone can have different size and each node may be within multiple overlapping zones. Zone Routing Protocol (ZRP) is the example of Hybrid Routing Protocol. Normally, Hybrid routing protocol for MANETs exploit hierarchical network architectures.

3. OLSR AND STAR ROUTING PROTOCOLS

3.1 Optimized Link State Routing (OLSR) protocol

The Optimized Link State Routing (OLSR) [7] Protocol is described in RFC 3626. OLSR is a proactive routing protocol that is also known as table driven protocol by the fact that it updates its routing tables. The key concept of OLSR is the use of Multipoint Relay (MPR) to provide an efficient flooding mechanism by reducing the number of transmissions required. In OLSR, [6] each node selects its own MPR from its neighbors. Each MPR node maintains the list of nodes that were selected as an MPR; this list is called an MPR selector list. Only nodes selected as MPR nodes are responsible for advertising, as well as forwarding an MPR selector list advertised by other MPRs. OLSR has several advantages that make it a better choice over other table-driven protocols. It reduces the routing overhead associated with table-driven routing, in addition to reducing the number of broadcasts done.

3.1.1 Routing messages in OLSR

Generally [15] in the OLSR protocol two types of routing messages are used, namely, a HELLO messages and a Topology Control (TC) message.

A HELLO message is the message that is used for neighbor sensing and MPR selection. In OLSR, each node generates a HELLO messages periodically. A node's HELLO message contains its own address and the list of its one-hop neighbors. By exchanging HELLO messages, each node can learn a complete topology up to two hops. HELLO messages are exchanged locally by neighbor nodes and are not forwarded further to other nodes.

A TC message is the message that is used for route calculation. In OLSR, each MPR node advertises TC messages periodically. A TC messages contains the list of the sender's MPR selector. In OLSR, only MPR nodes are responsible for forwarding TC messages. Upon receiving TC messages from all of the MPR nodes, each node can learn the partial network topology and can build a route to every node in the network.

3.1.2 Multipoint Relays

The idea of multipoint relays is to minimize the flooding of broadcast packets in this network by reducing duplicate retransmission in the same region. Each node in the network selects a set of nodes in its neighborhood, which retransmits its packets. This set of selected neighbor nodes is called the multipoint relays (MPRs) of that node. The neighbors of any node N which are not in its MPR set, read and process the packet but do not retransmit the broadcast packet received from node N. For this purpose, each node maintains a set of its neighbors which are called the MPR Selectors of the node. Every broadcast messages coming from these MPR Selectors of a node is assumed to be retransmitted by that node. This set can change over time, which is indicated by the selector nodes in their HELLO messages.

Each node [8] selects its multipoint relay set among its one hop neighbors in such a manner that the set covers (in terms of radio range) all the nodes that are two hops away. For example, in Figure 2, Node can select nodes B, C, K and N to be the MPR nodes. Since these nodes covers all the nodes, which are two hops away. Each node determines an optimal route (in terms of hops) to every known destination using its topology information (from the topology table and neighboring table) and stores this information in a routing table. Therefore, routes to every destination are immediately available when data transmission begins. OLSR is based on the following mechanism:

- Neighbor sensing based on periodic exchange of HELLO messages.
- Efficient flooding of control traffic using the concept of multipoint relays.

- Computation of an optimal route using the shortest-path algorithm.

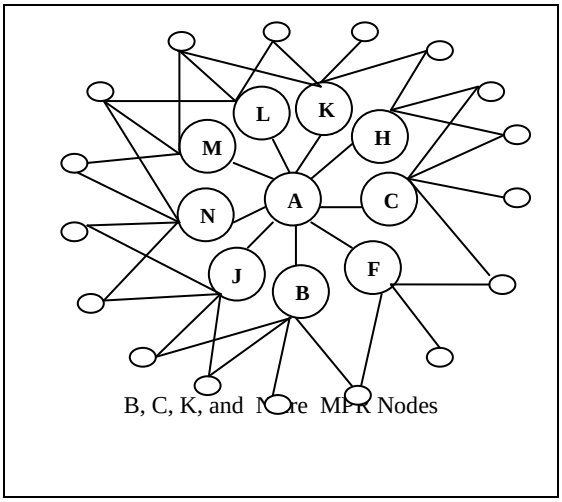

Figure 2 - Multipoint relays

3.2 Source Tree Adaptive Routing (STAR) Protocols

STAR is proposed as an efficient link-state protocol by J.J. Garcia-Luna-Aceves. STAR protocol [9] [10] , every node broadcasts its source-tree information. The source-tree of a node consists of the wireless links used by the node in its preferred path to destinations. Every node, using its adjacent links and the source-tree broadcast by its neighbors, builds a partial graph of the topology. During initialization, a node sends an update message to its neighbors. Also, every node is required to originate update messages about new destinations, the chances of routing loops, and the cost of path exceeding a given threshold. Hence, each node will have a path to every destination node.

In the absence [11] of reliable link layer broadcast mechanism, STAR uses the path-finding approach. Dijkstra's shortest path algorithm is then run on the constructed topology graph to choose a path to the destination. Thus, STAR belongs to the category of routing protocols based on minimum-weight path based routing.

STAR can operate in two ways. Optimum Routing Approach (ORA) and the Least Overhead Routing Approach (LORA). The ORA protocols attempt to update routing information quickly enough to provide optimum paths with respects to the defined metric (which may be the lowest of hops), but with LORA, the routing protocol attempts to provide feasible paths that are not guaranteed to be optimal, but involve much less control overhead. The use of the LORA approach in this table-driven routing protocol reduced the average control overhead compared to several others on-demand routing protocols.

STAR requires a Neighbor Protocol, which ensures that new neighbors and leaving neighbors are detected in finite time.

4. PROBLEM STATEMENT

The basic problem with most of the routing protocols is that they trust all nodes of network and based on the assumption that nodes will behave or cooperate properly but there might be a situation where some nodes are not behaving properly. Most Ad-hoc network [4] routing protocols becomes inefficient and shows dropped performance while dealing with large number of malicious nodes. A malicious node can silently drop some or all of the data packets sent to it for further forwarding even when no congestion occurs.

Malicious packet dropping [12] attack presents a new threats to wireless ad hoc networks since they lack physical protection and strong access control mechanism. An adversary can easily join the network and then starts to disrupt network communication by silently dropping packets. If malicious packet dropping attack is used along with other attacking techniques, such as shorter distance fraud, it can create more powerful attacks called Black hole attack, which may completed disrupt network communication. Moreover A malicious node will drop all the data packets that it receives. In addition, it will not acknowledge to the sender that it has dropped a data packet.

5. IPSec in MANETs

IPSec (IP security) developed by Internet Engineering Task Force (IETF) is a suit [3] of protocols used to secure traffic at the IP layer. The main components of IPSec are Authentication Header (AH) and Encapsulating Security Payload (ESP), which describe the IP header extensions for carrying cryptographically protected data, and Internet Key Exchange (IKE). IPSec is based on Security Associations (SAs). A security association is a simplex connection whose traffic is protected by security service designated by parameters such as the encryption algorithm, keys and lifetime. SA is uniquely identified by a tuple of Security Parameter Index (SPI), destination IP address and IPSec protocol (AH or ESP). IPSec protocol is based on the establishment of Security Association between packet sender and receiver. SA is setup in the IKE phase by Diffie Hellman algorithm. This preconfigured shared secret can then be available in most MANET systems and is essential for adopting IPSec secure communications and membership verification. Upon the establishment of membership management mechanism and the corresponding trust model in MANET, IPSec can be an appropriate choice for MANET network layer to protect both routing information and data messages. For IPSec to work, communication entities must share a public key. This key exchange process is accomplished through key management mechanisms that refer to the creation, distribution, installation, authentication, and access control of the keying material. A number of cryptographic algorithms are also specified in IPSec for authentication and encryption.

IPSec [13] can be used in two different ways. It can be used end-to-end, in which case the source and destination hosts for a datagram are responsible for all cryptographic processing. It can also be used via gateways, in which case a system near the source host is responsible for applying cryptographic operations on behalf of the source, while a system near the destination is responsible for checking and decryption.

6. PROPOSED METHODOLOGY

Proposed method combines IPSec with OLSR and STAR routing protocols. Routing protocol uses a hybrid version of the IPSec protocol, which includes both AH and ESP modes. IPSec is a protocol suit for securing IP based communication focusing on authentication, integrity, confidentiality and support perfect security forward. The significant importance of the aforementioned protocol is that it offers flexibility, which cannot be achieved at higher or lower layer abstractions in addition to the symmetric cryptographic schemes. These are 1000 times faster than asymmetric cryptographic schemes, a fact that makes IPSec appropriate to be used in handheld resources constrained devices such as PDAs. In this context, several research approaches have concluded that the usage of IPSec is appropriate in MANETs. It is widely accepted that IPSec is one of the best security protocols available at present and it is mentioned as the most reliable and efficient network layer protocol. For many applications, security at the network layer has a number of advantages over security provided elsewhere in the protocol stack [13] [14].

7. SIMULATION ENVIRONMENT

The simulations have been performed using QualNet 5.0, a software [16] that provides scalable simulation of wireless networks. The Sources destination pairs are spread Random Way Point (RWP) model in a rectangular field with 1500m × 1500m where as network size is varied as 20, 40 and 60 nodes with 10%, 20% and 30% nodes are malicious node respectively. Grid placement model are used. The pause time which affects the relative speeds of the mobile hosts, is kept constants at 30s. Maximum speed varied at 1-10m/s. Constant Bit Rate (CBR) traffic sources is used. The packet size without header is 512 bytes. At the physical layer PHY802.11b and at the MAC layer MACDOT 11 is used. The duration (Simulation time) of each experiment is 300 seconds.

7.1 Parameter metrics

We use 3 Performance Metrics.

7.1.1 Throughput: Throughput is the measure of the number of packet successfully transmitted to their final destination per unit time.

7.1.2 Packet Delivery Ratio (PDR): Packet Delivery Ratio is defined as the ratio of the number of data packets received by the destination over the total number of data packets transmitted by the sources.

Packet Delivery Ratio = (Received packets/Sent packets)*100

7.1.3 Total Packet Dropped: Total Packet dropped is the measure of the number of packets dropped in network.

8. EXPERIMENTAL RESULTS

8.1 Packet Delivery Ratio

We can observe from Figure 3. It is shown that the proposed method (IPSec-OLSR) gives better Packet Delivery Ratio than the traditional OLSR without IPSec, with varying network size and malicious nodes.

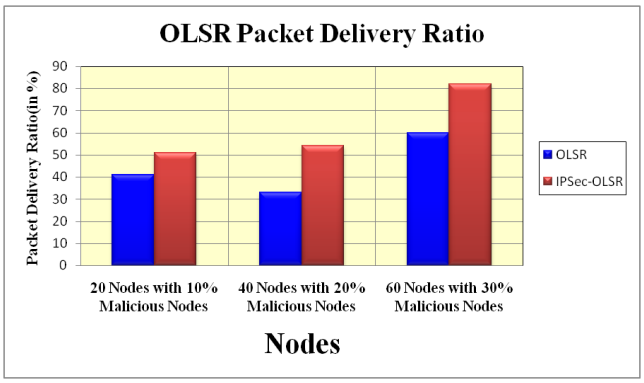

Figure 3 - OLSR Packet Delivery Ratio

From the Figure 4, it is shown that the proposed scheme (IPSec-STAR) gives better Packet Delivery Ratio compared to STAR without IPSec, with varying network size and malicious nodes. Hence the number of data packets dropping by malicious node has been minimized.

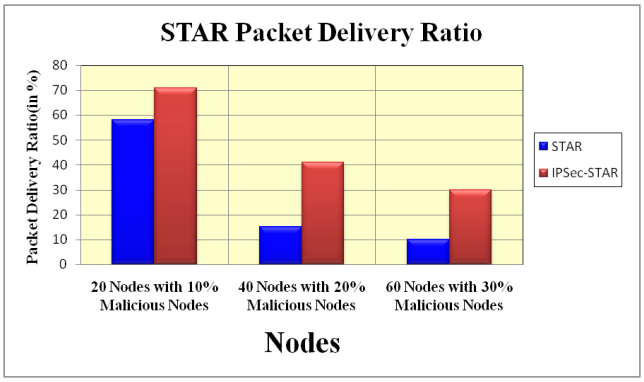

Figure 4 - STAR Packet Delivery Ratio

8.2 Throughput

Figure 5 demonstrates the throughput for OLSR (without IPSec) and OLSR with IPSec. It is clear that OLSR with IPSec has a good performance compared to OLSR without IPSec, with varying network size and malicious nodes.

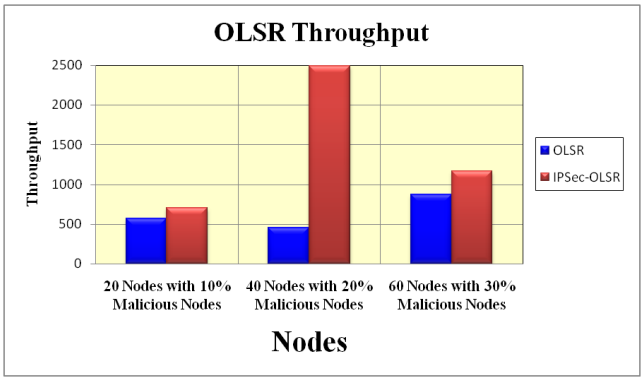

Figure 5 - OLSR Throughput

The Figure 6 indicates the achieved Throughput is higher in IPSec-STAR protocol compared to STAR without IPSec, because of the packets dropped by the malicious nodes.

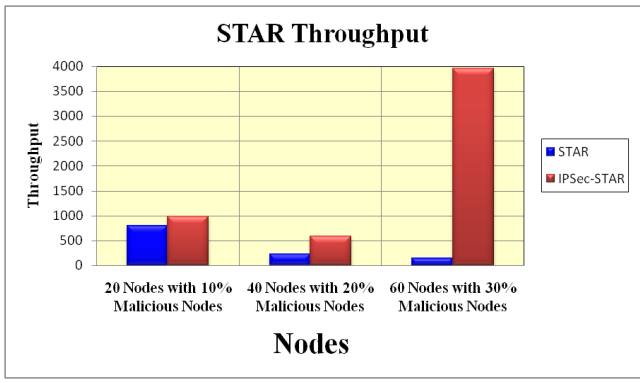

Figure 6 - STAR Throughput

8.3 Total Packet Dropped

There are several reasons for packet drops. In the given situation as we have increased number of nodes and malicious nodes. Figure 7 shown that the proposed method (OLSR with IPSec) gives lowest packet dropped than the traditional OLSR without IPSec protocol.

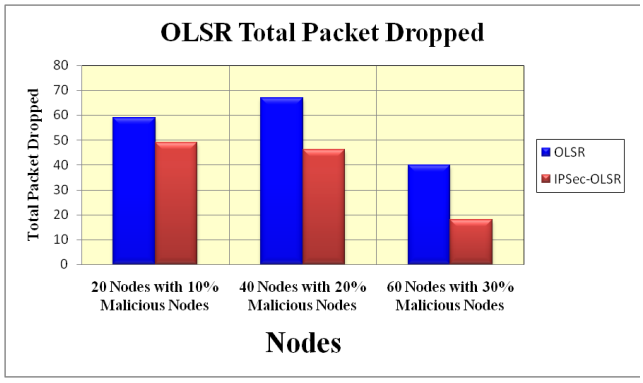

Figure 7 - OLSR Total Packet Dropped

The number of packets that are not successfully sent to the destination, called packet dropped. In terms of dropped packet, STAR without IPSec performance is the worst. Figure 8 shown that STAR with IPSec performance consistently well with increase in the number of nodes and malicious nodes.

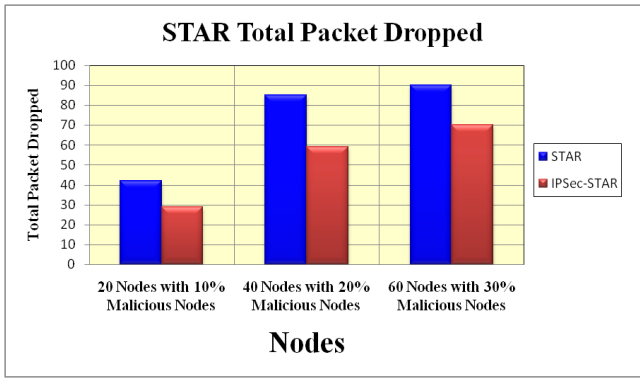

Figure 8 - STAR Total Packet Dropped

9. CONCLUSION AND FUTURE WORK

In this paper we have discussed problem of packets dropping by malicious node. Throughput and Packet Delivery Ratio decreases in the presence of malicious node. This paper estimates the applicability of IPSec for MANETs to provide security service for both control and data packets. From simulation results we analyzed that proposed approach gives better throughput and Packet delivery Ratio compared than existing without IPSec protocol and also gives less packet dropped. The performance is decrease if malicious node is not present in the network, because overhead of IPSec protocol is present in proposed approach.

In future this approach can be extended to other proactive and reactive routing protocols. We can also extend this research to secure routing protocols against other attacks such as Wormhole attack, Jellyfish attack etc.

10. REFERENCES

[1] T.V.P. Sundarajan, Karthik And A. Shanmugam, "Security And Scalability Of MANET Routing Protocols In Homogeneous & Heterogeneous Netwroks" Proceedings Of The International Conference On Mam- Machine Systems (Icomms), MALAYSIA, 11-13 October 2009.

[2] Santhosh Krishna B. V, Mrs. Vallikannu A. L, "Detecting Malicious Nodes For Secure Routing In MANETS Using Reputation Based Machanism", International Journal Of Scientific & Engineering Research, Volume 1, Issue 3, December-2010.

[3] Dr. G. Padmavathi, Dr. P. Subashini And Ms. D. Devi Aruna, "Hybrid Routing Protocols To Secure Network Layer For Mobile Ad Hoc Networks", IEEE, 2010.

[4]Aishwarya Sagar Anand Ukey And Meenachawla, "Detection Of Packet Dropping Attack Using Improved Acknowledgement Based Scheme In MANET", IJCSI International Journal Of Computer Science Issue, Vol. 7, Issue 4, No 1, July 2010.

[5] IRSHAD ULLAH AND SHOAIB UR REHMAN, "Analysis Of Black Hole Attack On Manets Using Different MANET Routing Protocols" Program Electrical Engineering With Emphasis On Telecommunication, Type Of Thesis-Master Thesis, Electrical Engineering, Thesis No : MEE-2010-2698, June 2010.

[6] BOUNPADITH KANNHAVONG, HIDEHISA NAKAYAMA, YOUSHIAKI NEMOTO AND NEI KATO."A SURVEY OF ROUTING ATTACKS IN MOBILE AD HOC NETWORKS", IEEE Wireless Communications, October 2007.

[7] T. Clausen, Ed And P. Jacquet, Ed, "IETF RFC 3626, Optimized Link State Routing Protocol (OLSR)", MANET Working Group, October 2003.

[8] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot*."Optimized Link State Routing Protocol For Ad Hoc Networks", Multi Topic Conference, 2001. IEEE INMIC 2001 62-68, Version 1-8 Apr 2010.

[9] J. J. Garcia-Luna-Aceves, Marcelo Spohn, And David Beyer, "SOURCE TREE ADAPTIVE ROUTING

(STAR) PROTOCOL."<Draft–Ieft-Manet-Star-00.Txt>. MANET Working Group INTERNET-DRAFT, 22 October 1999.

[10] J. J. Garcia-Luna-Aceves And M. Spohon, "Source-Tree Routing In Wireless Networks", Proceedings Of IEEE ICNP 1999, Pp. 273-282, October 1999.

[11] Natarajan Meghanathan, "SURVEY AND TAXONOMY OF UNICAST ROUTING PROTOCOLS FOR MOBILE AD HOC NETWORKS", The International Journal On Application Of Graph Theory In Wireless Ad Hoc Networks And Sensor Networks (GRAPH-HOC), Vol. 1, December 2009

[12] Mike Just, Evangeloskranakis And Tao Wan, "Resisting Malicious Packet Dropping In Wireless Ad Hoc Networks." Springer Link, ADHOC-NOW 2003, LNCS 2865, Pp 151-163, 2003

[13] Joshua D. Guttman, Any L. Herzog And Javier Thayer, "Authentication And Confidentiality Via Ipsec*", Appears In ESORICS, Springer LNCS, 30 June 2000.

[14] MATT BLAZE, JOHN IOANNIDIS And ANGELOS D. KEROMYTIS, "Trust Management For Ipsec." ACM Transactions On Information And System Security, Vol. 5, No. 2, Pages 95-118,May 2002.

[15] T. H. Clausen, G. Hansen, L. Christensen And G. Behrnmann, "The Optimized Link State Routing Protocol, Evaluation Through Experiments And Simulation," Proceedings Of IEEE Symposium On Wireless Personal Mobile Communications 2001, September 2001.

[16]Qualnet Documentation, "Qualnet 5.0 Model Library, Network Security", Available: Http:// Www.Scalablenetworks.Com/Products/Qualnet/Download....