Quantitative Comparative Study of Selected Routing Protocols in MANET based on Security

Bodhy Krishna S.
Research Scholar, Department of Computer Science, Sree Narayana Guru College, Coimbatore, India

C. Chandrasekar, PhD
Asst.Professor, PG and Research Dept. of Computer Science, Govt. Arts College, Karur, Tamilnadu, India

ABSTRACT
Mobile ad-hoc network (MANET) is a sub class of ad-hoc network and it dynamically forms a temporary network without any support of central administration. Ad hoc network is a collection of wireless mobile nodes without any fixed infrastructure. The network is ad hoc because it does not rely on any pre-existing network infrastructure like routers in wired networks. Such networks have no fixed topology due to the high degree of node mobility. Node mobility may cause the routes change. Hence, routing in MANET is a critical task due to its highly dynamic environment. To accomplish this task, a variety of routing algorithms have been proposed and also the number remains increasing day by day. These protocols fall in to mainly three categories---Proactive, Reactive and Hybrid. But, it is difficult to determine which protocol performs best under a number of different scenarios. This paper presents the qualitative comparison of selected proactive routing protocols DSDV, OLSR and CGSR based on security.

General Terms
MANET Protocols, Comparative Study

Keywords
MANET, Proactive routing protocols, DSDV, OLSR, CGSR, Comparative study.

1. INTRODUCTION
Traditional networks need wires, which may be difficult to set up in some situations. Wireless networks have become increasingly popular in the computing industry since their emergence in 1970s.It allows users to access information and services electronically, irrespective of their geographic location. It allows mobility and flexibility with reduced cost. In fact the field of wireless and mobile communications has experienced an unprecedented growth during the past decades. However, there is increasing demand for connectivity in situations/places where there is no base station/infrastructure available. This is where ad hoc network came into existence. Wireless networks can be classified into infrastructure networks and infrastructure less networks or mobile ad hoc networks (MANETs).

A Mobile Ad hoc Network (MANET) is a network consisting of a collection of mobile nodes capable of communicating with each other independent of the network architecture. These nodes can communicate with each other without the use of predefined infrastructure or centralized administration [1]. MANETs are autonomously self-organized and self-configuring networks in which node mobility is very high which causes frequent and unpredictable topology changes.

Routing means to choose a path. Routing in MANET means to choose a right and suitable path from source to destination. Routing terminology is used in different kinds of networks such as in telephony technology, electronic data networks and in the internet network. Here work is more concern about routing in mobile ad hoc networks. Routing protocols in mobile ad hoc network means that the mobile nodes will search for a route or path to connect to each other and share the data packets. Protocols are the set of rules through which two or more devices (mobile nodes, computers or electronic devices) can communicate to each other. In mobile ad hoc networks the routing is mostly done with the help of routing tables. These tables are kept in the memory cache of these mobile nodes. When routing process is going on, it route the data packets in different mechanisms. The first is unicast, in which the source directly sends the data packets to the destination. The sec is multicast, in this the source node sends data packet to the specified multiple nodes in the network. The third is broadcast; it means the source node sends messages to all the near and far nodes in the network. Routing has two basic types, which are as under.

- **Static Routing:** is done by the administrator manually to forward the data packets in the network and it is permanent. No any administrator can change this setting. These static routers are configured by the administrator, which means there is no need to make routing tables by the router itself.
- **Dynamic Routing:** is automatically done by the choice of router. It can route the traffic on any route depend on the routing table. Dynamic routing allows the routers to know about the networks and the interesting thing is to add this information in their routing tables. In dynamic routing the routers exchange the routing information if there is some change in the topology. Dynamic routing is more flexible than static routing. It has the capability to overcome the overload traffic. Dynamic routing uses different paths to forward the data packets.

There are several routing protocols in MANET. These routing protocols can be divided into three categories[2]: proactive (table driven routing protocols), reactive (on-demand routing protocols), and hybrid.
In proactive protocols, each and every node maintains complete information about the network topology by continuously evaluating routes to all the nodes so that when a packet needs to be forwarded the route is already known and can be immediately used. Reactive routing protocols do not make the nodes initiate a route discovery process until a route to a destination is required. That is, routes are discovered on demand and aren't famous before hand as in proactive protocols. Hybrid Protocol is an improvement of the above mentioned two, or the combination of two. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding.

Any MANET routing protocol exhibits two types of properties:

- **Qualitative** such as loop freedom, security, demand based routing, distributed operation, multi-path routing etc.
- **Quantitative** such as throughput, delay, route discovery time, **packets** delivery ratio, jitter etc.

Obviously, most of the routing protocols are both qualitatively and quantitatively enabled. A lot of simulation studies were carried out in paper to analyze the quantitative properties of routing protocols.

A number of comparative studies/ review papers on various MANET routing protocols have been proposed, which highlights some of the quantitative analysis or comparison between different types of protocols.

Our effort is to add security to the three most popular proactive routing protocols designed for MANETs- DSDV, OLSR & CGSR and then do the comparison of these protocols based on quantitative properties.

2. PROACTIVE ROUTING PROTOCOLS

Proactive protocols are known as proactive since they maintain the routing information before it is needed. Each and every node in the network maintains routing information about how to reach every other node in the network. It continuously evaluates all the routes within a network regardless of whether or not it is needed. This means the protocol maintains fresh lists of destinations and their routes by periodically distributing routing tables throughout the network. So that when a packet needs to be forwarded, a route is already known and can be used immediately. Once the routing tables are setup, then data (packets) transmissions will be as fast and easy as in the traditional wired networks. Unfortunately, it is a big overhead to maintain routing tables in the mobile ad hoc network environment. Proactive protocols produce higher routing efficiency than reactive protocols in the network with scattered traffic. But proactive protocols use more bandwidth and resources like battery power, than reactive protocols. Thus, the proactive protocols cannot be used in resource critical solutions. It relies on an underlying routing table update mechanism that involves the constant propagation of routing information.

There are various existing proactive routing protocols. The areas in which they differ are the number of necessary routing tables and the methods by which the changes in the network topology are broadcast. The routing protocols that are presented in this paper are DSDV, OLSR and CGSR.

2.1 Destination-Sequence Distance Vector (DSDV) routing protocol

DSDV (Destination-Sequence Distance Vector) [3], [4] is a predictably performing routing protocol designed by Charles E. Perkins and Pravin Bhagwat. It is a table-driven, unicast MANET routing protocol. This protocol is based on Bellman-Ford algorithm [5]. The improvements made to the Bellman-Ford algorithm include freedom from loops in routing tables. Every mobile node in the network maintains a routing table. It contains the list of all possible destinations in that network. An entry in the table stores the destination address, the next hop towards the destination, the cost metric for the routing path to the destination in terms of hop count and a destination sequence number created by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, so that routing loops can be avoided. Preference is given to the route with the greater sequence number. Routing table updates are periodically transmitted throughout the network in order to maintain updated information in the table. These route updates can be either time-driven or event-driven. In time -driven, every node periodically transmits updates including its routing information to its immediate neighbors. But in event-driven, a node propagates its changed routing table since the last update in an event-triggered style.

In DSDV there are two ways for sending routing table updates. One is known as *full dump* and it carries full routing information during the update. So, it requires many packets. During periods of infrequent movement, these packets are transmitted occasionally. The other, known as incremental packets are used to transmit only that information which has changed since the last full dump. Incremental packets may fit in one packet. The mobile nodes maintain an additional table where they store the data sent in the incremental routing information packets.

2.2 Optimized Link State Routing (OLSR) Protocol

The Optimized Link State Routing (OLSR) protocol [6] is a modification of original Link State routing and it was modified for improved operation in ad hoc networks. But, it can also be used in other wireless networks. It is a proactive and non-uniform link state routing approach. In the original Link State algorithm, each node broadcasts its link state information to all other nodes in the network. But in OLSR only fewer nodes re-broadcast link state information there by reducing the overhead.

The main feature of OLSR is its use of *multipoint relays* (MPRs) to reduce the overhead of network floods. The MPR set for a given node is the set of neighbours that covers the two-hop neighbourhood of the node. We could also say that MPR of a node N is the minimal set of N's one-hop neighbors such that each of N's two-hop neighbors has at least one of N's multipoint relays as its one-hop neighbor.

When a node broadcasts a message, all of its neighbours will receive the message. But, only those nodes in its MPR set which have not seen the message before rebroadcast the message. Other neighbours process the message but not rebroadcast it. Therefore, the overhead for message flooding can be greatly reduced.

Node selects their MPR independently from its set of neighbours in different ways. One is through the periodic exchange of *Hello messages*. Each node periodically transmits a list of neighbours within a Hello message. An attribute including the directionality of the link to a neighbor is associated with each neighbour. The node is labeled *symmetric* if the link to the neighbour is bidirectional, or *asymmetric* if a Hello has been received from that node but the link has not been confirmed as bidirectional. A node obtains complete knowledge of its two-hop neighbour set at that point of time when a node receives this Hello message from each of its neighbours. Further, it knows the link with that neighbour is bidirectional if its own address is listed in the Hello message. Then the status of that neighbour can be updated to be symmetric.

OLSR may use an extraction algorithm for MPR selection [7] which is as follows. Each node starts with an empty MPR set. The N is defined to be the set of one-hop neighbours with

which there exists bidirectional connectivity and the set of *N2* is the set of two-hop bidirectional neighbours. The first nodes that are selected for the MPR set are those nodes in *N* that are the only neighbours of some node in *N2*. Next, the degree of each node *n* in *N* that is not in the MPR set is calculated., where the degree is the number of nodes in *N2* that are not covered by nodes in the MPR set, the node in *N* that has the highest degree is included in the MPR set. Once all the nodes in *N2* are covered, the process terminates.

Routing path within the network can be determined when each node's MPR set is selected. Each node maintains a route to every other node in the network as OLSR is a proactive protocol. Nodes periodically exchange topology control (TC) messages with their neighbours to diffuse topology information. The TC message for a given node only lists its connections to those neighbours that have selected it as an MPR. Those neighbours are called *MPR Selectors*. Only this set of nodes is advertised within the network.

The link state update is sent whenever a change of the MPR set has been detected. The period of link state exchange is set to a minimum value if the MPR set has been changed. If the MPR set remains stable, the period is increased until it reaches a refresh interval value. Each node obtains network topology information and constructs its routing table through link state messages. Only MPRs are included as intermediate nodes in routes used in OLSR.

2.3 The Clusterhead Gateway Switch Routing (CGSR) Protocol

The Clusterhead Gateway Switch Routing (CGSR) [8] is a hierarchical routing protocol which uses similar proactive routing mechanism as DSDV. It differs from the previous protocols in the type of addressing and network organization scheme employed. It uses a hierarchical network topology, unlike other table driven approaches that employ flat topologies [9]. CGSR is a clustered multihop mobile wireless network with several heuristic routing schemes. The cluster structure improves performance of the routing protocol because it provides effective membership and traffic management. Cluster construction and clusterhead selection algorithms are important components of cluster based routing protocols.

In cluster construction, mobile nodes are aggregated into clusters and a special node termed cluster-head is elected for each cluster which coordinates the members of the cluster. To elect a node as the cluster head a cluster head selection algorithm is used within the cluster. The problem of having a cluster head scheme is that changing of the cluster heads frequently can adversely affect routing protocol performance as nodes are busy in cluster head selection instead of packet relaying. So, a Least Cluster Change (LCC) clustering algorithm is introduced to improve the performance of CGSR. Using LCC, cluster heads only change when two cluster heads come into contact, or when a node moves out of contact of all other cluster heads [10].

When a node as cluster head comes under the range of another cluster head, a tie is broken either using lowest ID or highest connectivity algorithm. All member nodes of a cluster can be reached by the cluster head within a single hop, thereby enabling the cluster head to provide improved coordination among nodes that fall under its cluster.

CGSR modifies DSDV by using hierarchical clusterhead-to-gateway routing approach to route traffic from source to destination. Gateway nodes are nodes that are within communication range of two or more cluster heads. These gateway nodes are responsible for communication between the cluster heads. A packet sent by a node is first routed to its cluster head, and then the packet is routed from the cluster head to a gateway to another cluster head, and so on until the cluster head of the destination node is reached. The packet is then transmitted to the destination.
In this method, each node must keep a "cluster member table" where it stores the destination cluster head for each mobile node in the network. These cluster member tables are broadcast by each node periodically using the DSDV algorithm. After receiving broadcasts from other nodes, a node updates its cluster member table. Along with the cluster member table, each node must also maintain a routing table which is used to determine the next hop in order to reach the destination. In CGSR, when forwarding a packet, a node first checks both its cluster member table and routing table and tries to find the nearest cluster-head along the routing path to the destination. Next, the node will check its routing table to determine the next hop used to reach the selected cluster head. It then transmits the packet to this node.

3. SECURITY ADDITIONS

3.1 Trust based DSDV

TDSDV [11] proposed Trusted Destination Sequenced Distance Vector (TDSDV) Routing Protocol for MANET is a proactive secured routing protocol. It gains some of the inherent qualities of the distance vector algorithm. In such kind of proactive routing protocols, each node repeatedly maintains state-of-the-art routes to every other node in the network, Routing information at regular intervals are transmitted throughout the network. In order to preserve routing table stability, when the route discovery process is initiated, the two state-of-the art estimations such as bandwidth and variance residual energy will be calculated. The routing table is updated at every node by discovering the variation in routing knowledge about all the existing destinations with the number of nodes to the destination.

When the attacker tries to impersonate as intermediate node this TDSDV protocol will recognize the intruder using Intruder Detection Methodology, and redirect the path to the destination. In addition, to offer loop freedom, this protocol TDSDV uses succession count, which is offered by the destination node. When a route has already existed before traffic arrives, transmission takes place without any delay. Else, traffic packets must wait in queue till the node gets routing information equivalent to its destination. In case of highly dynamic network topology, the proactive schemes need a noteworthy quantity of resources to maintain routing information up-to-date and reliable.

3.2 Trust based OLSR

In TOLSR [12], trust-based analysis of the OLSR protocol using trust specification language is presented and the authors show how trust based reasoning can allow each node to evaluate the behavior of the other nodes. They have presented a trust-based solution for securing the OLSR Ad hoc routing protocol in three steps. The first step was the analysis of the implicit trust relations in OLSR. This analysis highlights the possible measures to make OLSR more reliable by exploiting the operations and information already existing in the protocol.

To detect misbehaving nodes, they have developed in the second step, trust-based reasoning by correlating information provided in the OLSR messages received from the network.

The integration of this reasoning allows each node to check the consistency of the behavior of other nodes and validate trust relationships established implicitly. Finally, the third step complements the second by offering two complementary solutions: prevention to resolve certain vulnerabilities of OLSR protocol, and countermeasures to stop and isolate malicious nodes. These proposals correspond to the trust reasoning that has been done by each node. Simulation results illustrate the effectiveness of trust-based reasoning and countermeasures to stop and isolate misbehaving nodes.

After the detection of misbehaving nodes, the solutions of prevention and countermeasures to resolve the situations of inconsistency, and counter the malicious nodes are provided. How a node can detect misbehavoring nodes by reasoning about information received from the network is investigated. Anomaly detection includes the consistency verification in OLSR messages (TC and HELLO) and trust-based reasoning that can be performed by each node in the network.

Although it is a continuous process, the detection must progress from the reception of the link discovery messages to the construction of the routing table, giving the particular evolution of trust among nodes during these operations. The authors address the countermeasure concerns in the basic operations in OLSR (neighbourhood discovery and MPR selection) and the distribution of information about trust relations and attack detection to alert the other nodes. For this, the time-stamp mechanism proposed by SOLS and the provable identity mechanism presented previously are set up respectively to ensure the freshness and authentication of messages.

3.2 Trust based CGSR

TCGSR [13] provides prevention from as well as detection of malicious node in the network i.e. a malicious node present in the network is detected before it attempts its malicious behaviour. The proposed technique requires little computation work which is valuable according to limited battery power characteristic of mobile nodes. The proposed technique makes use of CGSR routing protocols that reduces routing overhead by routing data packets through cluster head and gateway nodes. Also, it adds almost negligible latency in the network.

The proposed technique prevents and detects malicious node in the network based on its MissRatio. CGSR (Cluster head Gateway Routing) protocol is used as a routing protocol.The step by step working of the proposed technique is as explained below: Initially, two set of node, U and V, are taken. U consists of set of suspicious nodes and V consists of set of nodes to which cluster head multicasts data packet. Next, the variables hit, miss and TotalTries are initialized to 0.

The gateway node sends data packet to cluster head. The cluster head multicasts data packet to some selected nodes within its cluster whose PortAddresses have been specified in the header section of the packet. If any node i, where i Є U, tries to access data packet from the cluster head, the cluster head first checks its PortAddress and compare it with the PortAddresses of nodes chosen for multicasting data packet. If PortAddress is among the chosen nodes then Hits and TotalTries of node i are incremented else its Misses and TotalTries are incremented. Then HitRatio and MissRatio of node i is calculated by taking Misses, Hits and TotalTries values. If MissRatio of node crosses t (the threshold value), then the node is considered as malicious node else the node is genuine node.

In this proposed technique, the malicious behavior of the node is detected before it attempts its malicious behavior on the data packet i.e. data packets are prevented from the security threats as well as malicious nodes present in the network are also detected. Every cluster head within the network performs this operation. In this way malicious node is detected during data packet forwarding time.

4. SIMULATION RESULTS AND PERFORMANCE COMPARISONS

This section described the simulation tool, Simulation parameters and simulation results. The performances of the secure versions of DSDV, OLSR and CGSR routing protocols are evaluated on the basis of the performance matrices, throughput, packet delivery ratio and average end-to-end delay.

4.1 Simulation Tool

In this paper the simulation of OLSR, DSDV, and CGSR routing protocols is done by using network simulator (NS-2) software due to its simplicity and availability. The network simulator NS-2 is discrete event simulation software for network simulations. There are several network simulators, specifically ns-1, ns-2 and ns-3. All of them are discrete-event computer network simulators, primarily used in research and teaching. ns-3 is free software, publicly available under the GNU GPLv2 license for research, development, and use.

Ns-2 began as a variant of the REAL network simulator [REAL Network Simulator] in 1989. NS2 provides substantial support for simulation of TCP, routing and multicast routing protocols over a wired and wireless network. Ns-2 is written in C++ programming language and Object Tool Common Language (OTCL). C++ for data per event packets and OTCL are used for periodic and triggered event. NS-2 includes a network animator called nam animator which provides visual view of simulation. NS-2 preprocessing provides traffic and topology generation and post processing provide simple trace analysis. AWK programming is used for trace file analysis.

To run a simulation with ns-2, the user must write the simulation script in OTCL, get the simulation results in an output trace file, and analyze the results by using the awk command, Perl scripts, or any other trace analysis available program. For this thesis, we analyze the ns-2 trace files and to calculate the quantitative metrics that we use for the evaluation of the tested routing protocols.

4.2 Simulation Parameter

A simulation study was carried out to evaluate the performance of the secure version of MANET routing protocols DSDV, OLSR and CGSR such as TDSDV, TOLSR and TCGSR based on the metrics throughput, packet delivery ratio and average end-to-end delay with the following parameters:

Table 1. Simulation parameters employed for the comparative study

Parameter	Value
Radio model	TwoRay Ground
Protocols	TDSDV,TOLRR,TCGSR
Traffic Source	Constant Bit Rate

Packet size	1024 bytes
Max speed	10 m/s
Area	1000 x 1000
Number of nodes	50
MAC	Mac/802_11
Simulation time (Sec)	20, 40, 60, 80 & 100

4.3 Simulation Results

4.3.1 Throughput

It is the ratio of the total amount of data that reaches a receiver from a sender to the time it takes for the receiver to get the last packet. When comparing the routing throughput by each of the protocols, TDSDV has high throughput. It measures of effectiveness of a routing protocol.

Table 2: Comparison of throughput

Pause Time (Sec)	Protocol		
	TCGSR	TOLSR	TDSDV
10	1432	3987	3120
25	3438	8908	8701
50	7898	14343	14243
75	14879	17809	17309
100	21233	24569	24069

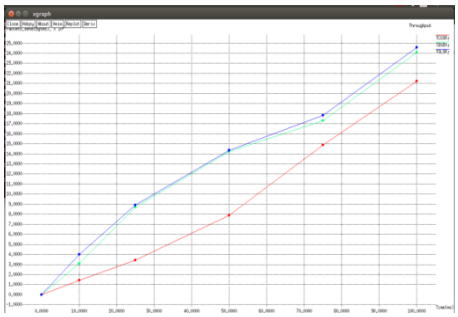

Figure 1: Comparison of Node Throughput for 50 Nodes

4.3.2 Packet delivery Ratio

Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted by a traffic source and the number of packets received by a traffic sink. It measures the loss rate as seen by transport protocols and as such, it characterizes both the correctness and efficiency of ad hoc routing protocols. A high packet delivery ratio is desired in any network. PDR value of TOLSR is higher than all other protocols.

Table 3.Comparison of packet delivery ratio

Pause Time (Sec)	Protocol		
	TCGSR	TOLSR	TDSDV
10	87	95	94
25	88	95	94
50	89	96	95
75	89	97	97
100	90	98	97

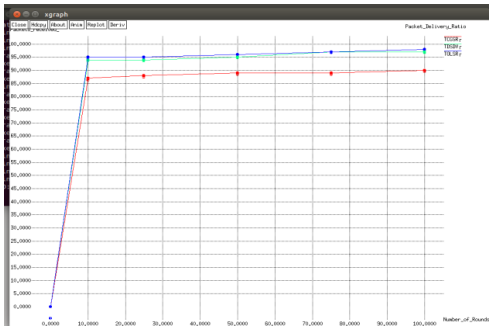

Figure 2: Comparison of PDR for 50 Nodes

4.3.3 Average End-to-End delay

The packet End-to-End delay is the average time that a packet takes to traverse the network. This is the time from the generation of the packet in the sender up to its reception at the destination's application layer and it is measured in seconds. It therefore includes all the delays in the network such as buffer queues, transmission time and delays induced by routing activities and MAC control exchanges. TOLSR has the shortest End-to-End delay.

Table 4. Comparison of average end-to-end delay

Pause Time (Sec)	Protocol		
	TCGSR	TOLSR	TDSDV
10	0.4522	0.3452	0.3852
25	0.8431	0.6431	0.6831
50	0.9272	0.8272	0.8872
75	1.213	0.7563	0.7863
100	1.333	1.1243	1.1743

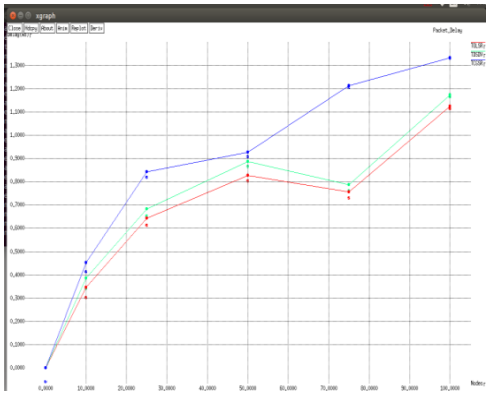

Figure 3: Comparison of Average End-to-End delay for 50 Nodes

5. CONCLUSION AND FUTURE WORK

Routing in Mobile ad-hoc networks is much more difficult than in conventional networks because of its dynamic topology and unpredictability in wireless links. The design of the routing protocols are driven by specific goals and requirements based on respective assumptions about the network properties or application area. Each protocol introduced in this paper has its own advantages and disadvantages in different MANET settings or environments. Therefore, it is hard to say which one is the best. The study suggests that not a single routing protocol is best suited for all scenarios of MANET. So, the choice of routing protocol should be done carefully according to the requirements of the specific application.

In this paper, we performed a quantitative comparative study of different proactive routing protocol using some parameters. The three proactive routing protocols taken in to consideration are DSDV, OLSR & CGSR and their core architecture is described. The basic actions related to these routing protocols are studied in detail. Each routing protocol has unique features. The comparison of the routing protocols indicates that the design of a secure ad hoc routing protocol constitutes a challenging research problem against the existing solutions.

DSDV, CGSR and OLSR have distinctive characteristics which makes the one better suited than the other one, depending on the situation. The OLSR protocol is more efficient in networks with high density and highly sporadic traffic. But the best situation is when between large numbers of hosts. It also has QoS support and their performance depends a lot from the network environment. DSDV works most efficiently in small networks as its control overhead is high. We have also seen the structure and the working of the cluster-based routing protocol. It is best suited for large networks. Cluster-based approaches on routing in mobile ad-hoc networks are good methods to decrease network traffic and routing overhead.

This thesis work also includes the study and performance comparisons of the trusted version of the three protocols with respect to the metrics packet delivery ratio, average end to end delay and throughput. The result of simulation indicates that performance of TOLSR is certainly superior to the other protocols in terms of throughput, packet delivery ratio and end to end delay.

In the future, the reasons that cause this variation on the results can be examined and explained in a more analytic and precise manner. Another direction for our future work is to further analyze the impact of the packet size on the Throughput and other performance metrics.It is possible to change the mobility and density of the network by directly modifying the speed and the number of nodes. It is also possible to change the characteristics of the network by changing the transmit power. Other new protocols performance could be studied.

6. ACKNOWLEDGEMENT

Special thank and recognition goes to the experts who have inspired and motivated us through this research. We would also like to thank Bharathiar University for supporting this research.

7. REFERENCES

[1] C.Sivaram murthy, B.S.Manoj, Ad hoc wireless Networks Architectures, and protocols, Pearson Edu, 2004.

[2] Roberto Carlos Hincapi´e, Blanca Alicia Correa, and Laura Ospina, “Survey on Clustering Techniques for Mobile Ad Hoc Networks,”pp.1-8

[3] C.Perkins ,Praving Bhagwat, “Highly dynamic destination sequenced distance vector Routing (DSDV) for Mobile computers”.

[4] Charles E. Perkins and Elizabeth M.Royer. “Ad-hoc on-demand distance vector routing”. Technical report, Sun Micro Systems Laboratories, Advanced Development Group, USA

[5] R. Dube et al., "Signal Stability based Adaptive Routing (SA) for Ad- Hoc Mobile Networks," PerS. Commun., Feb. 1997, pp. 36-45

[6] P. Jacquet, P. Muhlethaler, A. Qayyum, “Optimized Link State Routing Protocol”, Internet Draft, draft-ietf-manetolsr- 00.txt, November 1998.

[7] A. Laouiti, A.Qayyum, and L.Viennot, “Multipoint Relaying; An Efficient Technique for Flooding in Mobile Wireless Networks,” in Proceeedings of the 35th Annual Hawaii International Conference on System Science (HICSS’ 2002), Waikoloa, HI, January 2002.

[8] C.-C. Chiang, “Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel,” *Proc. IEEE SICON ’97*, Apr. 1997, pp. 197–211.

[9] C.Siva Ram Murthy and B.S.Manoj, “Ad-Hoc Wireless Networks: Architectures and Protocols”, *Pearson Education*, ISBN 0132465698, 9780132465694, May 2004.

[10] Elizabeth M. Royer and Chai-Keong Toh, “A Review of Current Routing Protocols for Ad Hoc MobileWirelessNetworks”, *IEEE Personal Communication*, April 1999.

[11] MohdZamirArif, et al. “ Trusted Destination Sequenced Distance Vector Routing Protocol for Mobile Ad-hoc Network” International Journal of Computer Applications September 2013

[12] Asma Adnane, Christophe Bidan , Rafael Timóteo de Sousa Júnior “Trust-based security for the OLSR routing protocol” Elsevier April 2013

[13] Kaur et al., International Journal of Advanced Research in Computer Science and Software Engineering 3(7), July - 2013, pp. 273-281