A Survey on Trust based routing in MANETs

Chahak Sharma[1], Sahil Verma[2], Kavita[3]

[1]Student, M. Tech, ESEAR, Ambala
[2] Assistant Professor, Dept. of ECE, E-Max group of Institutions, Ambala
[3]Assistant Professor, Dept. of CSE, E-Max group of Institutions, Ambala

Abstract: **Mobile ad hoc Networks are multi-hop wireless networks which are dynamically configured without any centralized infrastructure. Trust is evaluated on the basis of observation, experience and knowledge. The dynamic nature and characteristics of MANETs often result in uncertainty and incompleteness of the trust evidence, which is continuously changing over time. Trust computation and management are quite challenging issues in MANETs due to computational complexity constraints and the independent movement of nodes. In MANETs, an untrustworthy node can adversely affect the network. In this paper, a detailed survey on the trust based routing protocols namely AODV, DSR, OLSR, DSDV, ABR etc is conducted. This paper elucidates the comparison between these protocols based on the trust mechanisms, merits and demerits.**

Keywords— **MANET, Trust baesd routing, Protocols, cipher text**

I. INTRODUCTION

MANET is composed of mobile nodes and these nodes do not have any fixed infrastructure such as access point or server to determine the route of the paths [1]. Each node in an ad hoc network relies on other nodes in a network to forward packets by using routing protocols. In MANET, both trusted and untrusted nodes have access to shared resources or information. The inherent freedom in self organized mobile ad hoc networks introduces challenges for trust management when nodes do not have any prior knowledge of each other's behavior. Hence, to assure that access to resources is given only to trusted and benign nodes, the trustworthiness among anonymous nodes needs to be ensured.

Trust is an important attribute of mobile ad-hoc networks (MANETs). It enables entities to cope with uncertainty and uncontrollability caused by the free will of others. Trust computations and management are highly challenging issues in MANETs due to computational complexity constraints and the independent movement of nodes. In MANETs, an untrustworthy node can cause considerable damage and adversely affect the reliability of data. In this paper, comprehensive survey on various trust based routing protocols that are geared towards MANETs has been done.

The rest of this paper is organized as follows. In Section 2, this paper presents a trust management, trust properties and trust mechanism. Then, Section 3 reviews various trust based MANET routing protocols and the comparison between these protocols. Section 4 concludes the paper.

II. TRUST MANAGEMENT

The notion of "Trust" was originally derived from social sciences and is defined as the degree of subjective belief about the behaviors of a particular entity [2]. Blaze et al. [3] first introduced the term "Trust Management" and claimed it as a separate and essential part of security services in networks and quoted that trust management provides a unified approach for specifying and interpreting security policies, credentials, and relationships.

Trust management in MANETs is desired when participating nodes, without any previous interactions, establishes a network with an acceptable level of trust relationships among themselves such as in applications like building initial trust bootstrapping [4], coalition operations without predefined trust, and authentication of certificates generated by another party when links are down or ensuring safety before entering a new zone [5]. Trust management has diverse applicability in decision making situations for ensuring security like intrusion detection, authentication, access control, key management, isolating misbehaving nodes for effective routing etc.

Trust management, including trust establishment, trust update, and trust revocation is much more challenging in MANETs than in traditional wired environments. For example, collecting trust information or evidence to evaluate trustworthiness is difficult due to dynamic changes in network topology induced by node mobility or node failure. Further, resource constraints often confine the trust evaluation process only to local information. Trust mechanism is incorporated in the routing protocols to provide security in MANET against different attacks such as blackhole, wormhole, selfish attack, DoS attacks etc. Trust is a value that is computed on the basis of nodes' action or behavior. Trust can be implemented in various ways such as reputation, subjective logic from opinion of needs, probabilistic value etc as there are no particular

definition of trust. Following are the properties that trust metric should exhibit:

- Trust is dynamic that changes with time, location etc. MANET has dynamic changing topology and highly mobile so the trust value should be based on temporary and local information.
- Trust is context dependent i.e. its value depends on the task given to a node, it may be high for one task but same node may have lower trust value for other task.
- Trust is asymmetric, it means that if a node A trusts a node B then there is no guarantee that node B also trusts node A in return.
- Trust is subjective; the node may have different trust values for the same node in different situations due to changing network topology.
- Trust is a composite value i.e., the trust values obtained from different sources can be aggregated to get a single value with different weight values to each. This combined trust value is more accurate than individual values.

Trust computation be direct, indirect and hybrid [6].

- Direct trust is based on nodes own observation and experience about the behavior of node. Direct trust is computed solely on the basis of nodes own view about the behavior of a particular node in the network.
- Indirect trust is evaluated on the basis of recommendations from its neighbors. It is calculated when any particular node does not have a direct trust on any node so other nodes can recommend the trust value based on their own observation and experiences.
- Hybrid trust is combination of direct and indirect trust, it uses experience and recommendations based approach to compute trust for any node.

III. TRUST BASED ROUTING PROTOCOLS IN MANETS

Routing in MANETs is on hop by hop basis and depends on network topology, route selection etc as there is no centralized infrastructure. Routing protocols can be classified as: Proactive protocols, Reactive protocols and Hybrid protocols. Proactive protocols or table driven protocols always have routes to every other node beforehand and every node maintains routing table in which routes are updated periodically or when ever any change occur. There is no delay in route discovery because routes are already available but considerable control overhead. Reactive protocols or on demand protocols find routes on demand whenever required by broadcasting route requests. It decreases the control overhead as fewer messages are exchanged but there is an increased latency in discovering the routes. Hybrid protocols are the combination of reactive and proactive routing protocols incorporating advantages of both i.e. less control overhead and delay in route discovery.

Various approaches have been proposed in the literature to secure the routing process in MANET. Cryptographic techniques used to secure the routing information from malicious attacker in wired routing protocols can't be deployed in resource constrained MANET because of high computational cost involved. Moreover, it can secure the routing information from external tampering but can't secure mobile nodes that participate in routing process.

So the trust mechanism is adopted in routing protocols to secure nodes as well as the data transmission. Different trust based routing protocols are proposed to provide security in MANET by securing nodes in routing path.

3.1 TRUST DSDV (TDSDV)

Arif et al. [7] proposed Trusted Destination Sequenced Distance Vector (TDSDV) Routing Protocol for MANET which is a proactive secured routing protocol. It inherits few characteristics of the distance vector algorithm. Each node repeatedly maintains routes to every other node in the network and routing information are transmitted throughout the network at regular intervals to ensure stability of routing table. 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 malicious node tries to impersonate as an intermediate node in a route, TDSDV protocol recognizes the intruder using Intruder Detection Methodology and redirects the path to the destination. After calculating the path in which packets are to be routed, the source node will forward certain number packets to the next hop. The number of packets sent to the first hop will become threshold value. This threshold value will be verified at every node in the path before forwarding the packets. If any of the nodes in that path got different value than threshold value then they are treated as intruder and the path is rediscovered with the new threshold value and the intruder node is discarded. This process is repeated till it reaches the destination node

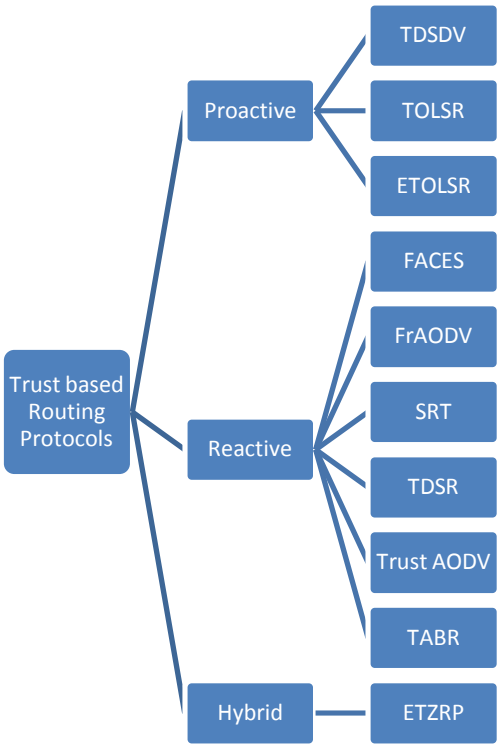

Fig.1. Trust based MANET Routing Protocols

.

3.2 TRUST BASED OLSR (TOLSR)

Adnane et al. [8] proposed a trust-based solution; TOLSR for securing OLSR protocol using trust specification language that exhibits how trust based reasoning can allow each node to evaluate the behavior of the other nodes. The solution consists of three steps. The first step deals with the analysis of the implicit trust relations in OLSR that highlights the countermeasures to make OLSR more reliable by exploiting the operations and information already existing in the protocol. The second step deals with trust-based reasoning by correlating information provided in the OLSR messages received from the network to detect misbehaving nodes. 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 preventive measures and countermeasures to resolve the situations of inconsistency and mitigate attacks are provided. 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 (neighborhood 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 and the provable identity mechanism are set up to ensure the freshness and authentication of messages.

3.3 ETOLSR (Enhanced OLSR using Trust Based System)

Balaji et al. [9] proposed Enhanced OLSR using the trust based system called Trustbased OLSR (TOLSR), a lightweight scheme which provides security against node isolation attack. Once the node is detected as attacker using EOLSR, its trust value is reduced to half of its initial value. Further, selection of attacker as MPR node is prevented since all the nodes will select only high trust node as MPR node. EOLSR detects the malicious node but could not prevent its further selection as MPR so ETOLSR is devised. Initially, all the nodes are assigned high trust value (1.0). Each node maintains the trust value based on the trust value of its neighbors. Trust value of the nodes depends on the activity of the nodes in the network and MPR node is selected based on the trust value of the node. This scheme uses HOP_INFORMATION table, 2-hop request and 2-hop reply. In Figure 2, Node A selects B and E as MPR to broadcast packets to C and F and maintains HOP_INFORMATION table show in Table 1 below.

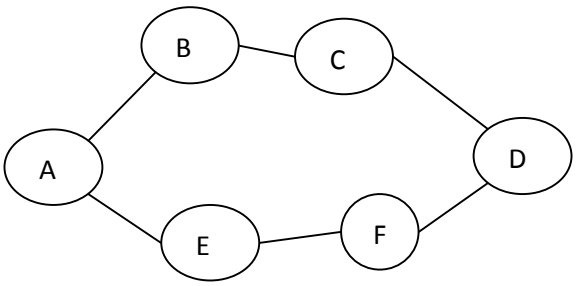

Fig. 2 Node A Selects B, E as OLSR MPR

Table 1. A's HOP_INFORMATION

HELLO message sender	2-hop neighbors
B	C
E	F

3.4 FACES (Friend-based Adhoc routing protocol using Challenges to Establish Security)

In FACES [10], trust of the nodes is calculated by sending challenges and sharing friends' lists to provide a list of trusted nodes to source node so that data transmission can occur through this trusted path. The FACES algorithm is divided into four stages as shown in Figure 3: Challenge your neighbor, Rate friends, Share friends and Route through friends. The first three stages of the algorithm are periodic, and the fourth stage is on demand basis.

Challenges are sent to authenticate the nodes. Those nodes which complete the challenge are kept in the friend list otherwise they are kept in the question mark list. In rate friends stage, rating of the friends is done on the basis of the amount of data they transmitted and rating obtained from other friends. Each friend in the list can have following three ratings: Data Rating (DR), Friend Rating (FR) and Net Rating (NR). The data rating is updated by a node for its friend on the basis of data transferred through it. This protocol requires each node to store different lists. The friendship of a node with other nodes in the network is obtained through the Share Your Friends stage. The net rating (NR) is weighted sum of data and friend rating as shown in following equation.

$$NR = \frac{W1 * DR + W2 * FR}{W1 + W2}$$

Where W1 and W2 are weights assigned to DR and FR

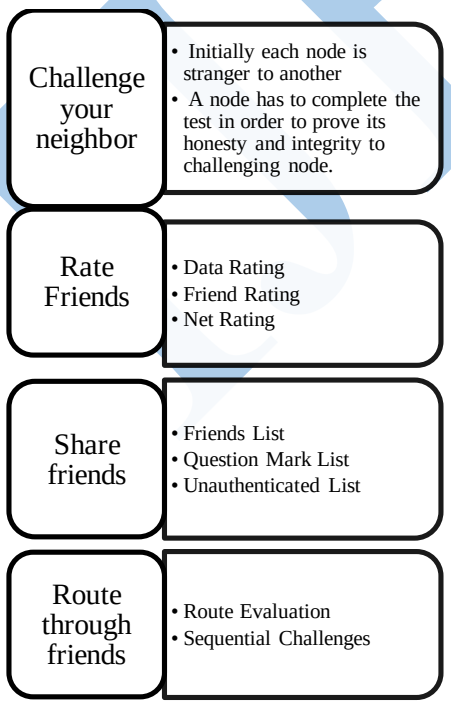

Fig. 3 Stages in FACES Algorithm

3.5 Friendship Based AODV (FrAODV)

Essia et al. [11] proposed Friendship based AODV which consists of evaluation algorithms that evaluated forward and reverse path between source and destination. In this scheme, it is assumed that each node has identity which can't be forged by any other malicious node and number of malicious nodes is always less than the number of good nodes. Every node stores a list of friends with friendship values ranging from 0 to 100. More the friendship values, more trustable the node is. The two algorithms for establishing path are described as follows:

- RvEvaluate Algorithm: This algorithm sets up reverse path from destination to source. Source node broadcasts the route request packets which can reach a destination node or an intermediate node. If RREQ reaches the destination node, it checks the friendship value of the node from which it receives the RREQ packet, as every node maintains a friendship list along with friendship value of the neighbor nodes. If the node is not a friend the node rejects the RREQ packet. Otherwise it calculates the friendship value of the route to originator from destination and then compares the current routes friendship value with the existing route's friendship values. The reverse route's friendship value (RvFwRte) is the sum of friendship values of all nodes in that path and it is calculated as follows:

$$RvFrRte = \sum_{i=1}^{n} \frac{PrFrHpi}{h}$$

  Where PrFrHpi is friendship value of that node from which the current node receives RREQ packet and h is the no. of hops between source and destination. If the friendship value of the new route is less than the existing route the new route is rejected otherwise it is registered as a friendly route.

  If RREQ packet is received by an intermediate node, it first checks the friendship value of the node from which it RREQ packet is received and next neighbor node. If one of these two nodes is not in friend list, the intermediate node rejects the RREQ packet. Otherwise it calculates the friendship value of the route to originator from destination using the previously mentioned formulae and compares it with the existing route's friendship value. If the friendship value of the new route is less than the existing route the new route is rejected otherwise the reverse path is established from current node to the previous node.
- FwEvaluate Algorithm: This algorithm sets up the forward path i.e. from source to destination during RREP forwarding. Just like RREQ

packet, RREP can be received by sender node or intermediate node. If the node receiving the RREP packet is sender node itself, it checks the friendship list and the friendship value of the node from which it receives the RREP packet i.e. the next node. If the next node is not a friend, rejects the RREQ packet. Otherwise, it calculates the friendship value of forward route to destination is calculated and compared with the existing route's friendship value. If the friendship value of the new route is less than the existing route the new route is rejected otherwise it is registered as a friendly forward route. If there is not any existing route the new route is included as a friendly route. The forward path's friendship value is formulated as:

$$FwFrRte = \sum_{i=1}^{n} \frac{FwFrHpi}{h}$$

Where FwFrHpi is friendship value of that node from which the current node receives RREP packet and h is the no hops between source and destination.

An intermediate node receiving RREP checks the friendship value of the node from which it receives the RREP packet and previous node. If one of these nodes is not friend, rejects the RREP packet. Otherwise it calculates the friendship value of the route to destination in the same way and compares it with the existing forward route's friendship value. If the friendship value of the new route is less than the existing route the new route is rejected otherwise the forward path is established from current node to the next node.

In this way after establishing friendly and secure path from source to destination, the data packets are transmitted along the chosen path.

3.6 Secure Routing Using Trust (SRT)

Elizabeth et al. [12] proposed a routing based on trust to establish an authenticated route. This scheme is based on node transition probability (NTP) and AODV. The nodes in the network are grouped on the basis of a parameter called trust rate (T_{rate}). The node first broadcasts beacon frame to find a secure route whenever it has to send data and then trust rate for each node is evaluated as:

$$T_{rate} = \frac{(r - t)}{t}$$

Where r = number of beacons received by a node and = number of beacons send by a node.

T_{rate} value partitions the nodes into 3 different categories: ally list (level2), associate list (level1), acquaintance list (level0). The nodes of the ally list send highly secured information. The nodes in associate list send medium secured information. The nodes in acquaintance list send the information that does not require any security.

An additional field "level" is added in neighbor table. Whenever a node has to send data, it checks its neighbor table. If the destination is available, it sends data packets otherwise; it searches for a node which has route to destination in its same level. If no node is found it goes to next lower level and so on. If any node within the same level is not found, trust is compromised by choosing a neighbor in the next lower level using the following formulae:

$$\text{Trust compromise} = \text{number of nodes in associate list} + 2 * \text{number of nodes in acquaintancelist}$$

Trust compromise will be low if all the nodes including destination node are in the same level because trust rate is very high as it is better to forward control packets in the same level than to forward the packets to other level. In this way after finding secure route the data packets are transmitted to the destination.

3.7 Secure AODV Routing Protocol based on Trust Mechanism

Harris Simaremare et al. [13] proposed AODV routing protocol based on trust mechanism using the concept of local trust and global trust. Local trust is based on total number of received packets and total number of forwarded packets with reference to specific nodes. Global trust is based on total number of packets received and total number of packets forwarded in network. Trust calculation is done before communication starts. This scheme can withstand blackhole attack and DoS attack. Each node should get all the activity information from its neighbor to calculate the trust. In order to ensure the nodes can hear all the activities of his neighbors, each node will run in promiscuous mode. The simulations are done on NS-2 and the performance analysis is done in terms of packet delivery ratio, end to end delay and routing overhead.

3.8 TRUST DSR (TDSR)

TDSR [14] uses trusted route for packet transmission and reduces the number of packets dropped by node. It works on the basis of positive or negative acknowledgement received after the transmission of a packet. The trust of a node is computed on the basis of all the successful and unsuccessful transmissions by a node in a stipulated time period i.e. by counting the number of ACK (Positive acknowledgement) and NACK (Negative acknowledgement) sent by a node. TDSR finds the secure route from source to destination in a network. Every node maintains a table recording all its neighbors along with their trust values and update the entries periodically. The trust of a node in the network is evaluated based on its

performance in the network. If a node successfully transmits a packet it sends a positive acknowledgement to the sender resulting in up gradation of its trust value. Packet drop results in negative acknowledgement causing reduction in the trust value of a node. The table storing the trust value of all neighbors is broadcasted periodically so that the information about the most trusted node is known to all. Trust value of a node helps in choosing the most trusted route from source to destination. In this way, trust value for each forward route from source to destination is computed based on the trust values of the intermediate nodes and then the route with the minimum trust worth (greater or equal to some trust threshold value is selected for transmission.

3.9 QTABR (Self-Adaptive Trust Based ABR Protocol for MANETs Using *Q*-Learning)

Anitha et al. [15] proposed a self-adaptive trust based ABR protocol that uses Q-Learning for finding a secure and stable route. Route is calculated as a weighted average of the trust value of all the nodes that lie in the route and further associativity ticks ensure the stability of the route. ABR protocol is a reactive (table driven) routing protocol with a metric called associativity that measures node's connectivity relationship with its neighbors. Association stability results when the number of beacons received from neighbors are greater than $ABR_{threshold}$.

$$ABR_{threshold} = \frac{2 * Transmission\ range}{Beaconing\ interval * Migrating\ speed}$$

Each node is considered as an agent and it computes two Q values: the penalty value (Q_p) when the trust value and associativity ticks of a particular node are less than the threshold and the reward value (Q_r) when trust value and associativity ticks are more than the threshold [15].

$$Q_r = (1-\alpha)\cdot Q(s_t, a_t)_r + \alpha \cdot Q(s_{t+1}, a_{t+1})_r,$$

where α is given by

$$\alpha = A_{th} + T_v,$$

$$T_v = T_{DAB} + T_{IAB}$$

$$Q_p = (1-\alpha)\cdot Q(s_t, a_t)_p + \alpha \cdot Q(s_{t+1}, a_{t+1})_p.$$

$$T_{DAB}(t) = w_1 \times CSF_{AB}(t) + w_2 \times DSF_{AB}(t)$$

$$T_{IAB}(t) = 1 - (1 - T_{DAB}(t))\,(1 - T_{ABC}(t))$$

α is the learning rate affecting Q-values, s_t represents the present state and s_{t+1} is the new state. The variable a_t represents the present action and a_{t+1} represents the action which led to s_{t+1}.

$T_{DAB}(t)$ is the trust of node B with respect to the neighbor node A, $CSF_{AB}(t)$ is the control signal forwarding ratio, $DSF_{AB}(t)$ is the data signal forwarding ratio between nodes A and B, and w_1 and w_2 are weights assigned to $CSF_{AB}(t)$ and $DSF_{AB}(t)$, respectively. $T_{IAB}(t)$ is the indirect trust value of B with the recommendation of the neighbor node C. $T_{ABC}(t)$ is the trust value sent to A by node C. Based on the values of Q_r and Q_p each node takes a decision to provide secure and stable route. Simulation results reveled that Q-learning based trust ABR protocol improves packet delivery ratio by 27% and reduces the route selection time by 40% over untrusted ABR protocol.

3.10 ETZRP (Enhanced Security of Zone-Based Routing Protocol using Trust)

Yasser et al. [16] proposed a security enhancement of ZRP based on trust calculations in which nodes constantly monitors the packets sent and acknowledgments received. The trust values of nodes are adjusted accordingly. The trust is calculated based on two parameters: previous trust values and the nature of experience evaluated on the basis of acknowledgements received. If the acknowledgement is received within the time frame then it's counted as positive experience else if it is not received within the stipulated time it IS counted as a negative experience. The nodes place their receiver in promiscuous mode and start a timer after transmitting a packet and maintain a copy of recently forwarded packets for comparison with the packet transmissions overheard by the neighboring nodes. When it hears that packet has been forwarded by a neighboring node, the sender node deletes the buffered packet, cancels the timer and confirms that the neighboring node has behaved well so the number of forwarded packets is increased. Similarly, if the neighboring node does not transmit the packet within a certain time period, its corresponding number of dropped packets is increased accordingly. A node is identified as malicious when the number of packet dropped exceeds the predefined threshold value during a fixed trust update interval. The malicious node is inserted in blacklist and further data packets originating from it are discarded to punish it.

Table 2. Comparison of Trust based MANET Routing Protocols

Protocol	Methodology	Performance Metrics	Merits	Demerits
TOLSR	Semantic properties of OLSRs in terms of trust are analyzed and implicit trust related properties in OLSR are identified to detect malicious nodes.	Detection rate	Allows to verify if the behavior of other nodes in the network Complete with the specification and Ensures efficient routing operation of OLSR validity of the topology	Implicit trust relations and no explicit which helps to identify whether the underlying assumptions for the operation of a protocol are realistic or not
TDSDV	A secure route maintenance mechanism is provided by involving threshold in terms of packets	Routing message overhead, average end to end delay, and throughput	Protects through unwanted packet flooding of the network and increases network performance	Threshold value to be treated as intruder and the path is rediscovered with the new threshold value and discarding the intruder node.
ETOLSR	Trust based OLSR. Once the node is detected as attacker using EOLSR, its trust value is reduced to half of its initial value.	Packet delivery ratio, Packets loss rate, control packet overhead	Light weight technique that does not involve much computational complexity or promiscuous listening.	This scheme is immune against DoS attacks only.
FACES	Incorporates Friend-based mechanism	Number of packets routed through malicious nodes, packet overhead, number of data packets dropped and energy consumed.	Nodes do not listen in promiscuous mode which reduces the network overhead significantly. A robust mechanism for thwarting attacks by isolating malicious nodes in the network without considering central authority.	In this protocol control overhead is increased due to periodic flooding of challenge packet and periodic sharing of friend list.
FrAODV	Evaluation algorithms that evaluated forward and reverse path between source and destination based on friendship values.	Packet delivery fraction, Normalized routing load	This protocol gives better performance in terms of QoS services like packet delivery fraction, normalized routing load.	The end to end delay is not included in performance measurement metric. The delay is more here because two evaluation algorithms are used to establish path.
SRT	Based on node transition probability and AODV to establish an authenticated route and Trust rate is evaluated.	Packet delivery ratio, throughput, end-to-end delay and trust compromise.	In terms of mobile mobility it gives better throughput, packet delivery ratio, average path length, average routing load.	The performance decreases in the presence of attacks except blackhole. The trust is calculated on the basis of control packets only.

Trust AODV	Used local trust and global trust concept to find the trust level	Packet delivery ratio, delay and routing overhead	Remove the attacker node before communication starts	Nodes work in promiscuous listening mode
TDSR	Trust is evaluated based on performance sending acknowledgement	Throughput and packets dropped	Reduces the number of dropped packets	Routing overhead is periodical broadcasting of trust value calculated to all nodes in the network
QTABR	*Q*-learning based trust routing scheme	Packet delivery ratio and packet dropping ratio	PDR increases and route selection time decreases. It is applicable to large heterogeneous networks. Since the mobile agents are flexible in nature, they can be adapted to any changes with the minimal overhead.	Q-learning is applied in route discovery phase only. End to end delay is not compared with QTABR and it increases with this scheme.
ETZRP	It finds trusted path by monitoring activities from neighbors. The trust is based on two parameters, previous trust values and the nature of experience.	Packet delivery ratio, Average end to end delay, routing packet overhead.	Increases packet delivery ratio.	Increases end to end delay and control overhead. Nodes work in promiscuous mode. Considers only packet dropping attacks.

IV. CONCLUSION AND FUTURE SCOPE

MANETs are vulnerable to different types of attacks such as blackhole, DoS, wormhole, colluding attack etc. due to its infrastructure less property. Various trust based approaches are proposed in the literature to prevent such types of attacks and to improve Quality of Services (QoS). These trust based routing protocols try to find a secure and reliable route by implementing trust mechanism. In this paper, we have reviewed currently existing trust based protocols and finally we have carried out a comparative study on these protocols on the basis of their methodology, performance metrics, merits and demerits.

REFERENCES

[1]. John, S. P., & Samuel, P. (2014). A Survey on Key Management and Certificate Exchange in Mobile Adhoc Network. *International Journal of Business Data Communications and Networking (IJBDCN)*, *10*(2), 30-46.

[2]. K. S. Cook (editor), *Trust in Society*, vol. 2, Feb. 2003, Russell Sage Foundation Series on Trust, New York.

[3]. M. Blaze, J. Feigenbaum, and J. Lacy, "Decentralized Trust Management," *Proc. IEEE Symposium on Security and Privacy*, 6-8 May, 1996, pp. 164 - 173.

[4]. R. B. Bobba, L. Eschenauer, V. Gligor, and W. Arbaugh, "Bootstrapping Security Associations for Routing in Mobile Ad Hoc Networks," *Proc. IEEE GLOBECOM*, San Francisco, CA, Dec. 2003, pp.1511-1515.

[5]. L. Eschenauer, V. D. Gligor, and J. Baras, "On Trust Establishment in Mobile Ad Hoc Networks," *Proc. 10th Int'l Security Protocols Workshop*, Cambridge, U.K., Apr. 2002, vol. 2845, pp. 47-66.

[6]. Philip England, Dr Qi Shi, Dr Bob Askwith and Dr Faycal Bouhafs, "A Survey of Trust Management in Mobile Ad-Hoc Networks", in *Proceedings of the 13th annual post graduate symposium on the convergence of telecommunications, networking, and broadcasting*, PGNET. 2012.

[7]. Mohd Zamir Arif and Gaurav Shrivastava "Trusted Destination Sequenced Distance Vector Routing Protocol for Mobile Ad-hoc Network" International Journal of Computer Applications, vol. 54, no. 15, pp. 7-12, 2012.

[8]. Adnane, A., Bidan, C., & de Sousa Júnior, R. T. (2013). Trust-based security for the OLSR

routing protocol. *Computer Communications*, *36*(10), 1159-1171.

[9]. Banothu Balaji, Mohammed Hassan Khan, T.S.N. Murthy and Tai-hoon Kim, "A Defense Mechanism for EOLSR against DOS Attacks in Ad hoc Networks Using Trust Based System", International Journal of Security and Its Applications, Vol.8, No.5 (2014), pp.51-64.

[10]. S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta, and P. Dhurandher, "FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems," Systems Journal, IEEE, Vol. 5, Issue 2, pp. 176-188, 2011.

[11]. Eissa, T., Razak, S. A., Khokhar, R. H., & Samian, N. (2013). Trust-based routing mechanism in MANET: design and implementation. *Mobile Networks and Applications*, *18*(5), 666-677.

[12]. Edua Elizabeth, N., Radha, S., Priyadarshini, S., Jayasree, S., Naga Swathi, K.:Srt- Secure Routing Using Trust Levels In Manets. European Journal of Scientific Research, Issn 1450-216x Vol. 75, No. 3 (2012), Pp. 409-422.

[13]. Simaremare, H., Abouaissa, A., Sari, R. F., & Lorenz, P. "Secure AODV Routing Protocol Based on Trust Mechanism." In *Wireless Networks and Security* , Springer Berlin Heidelberg, pp. 81-105, 2013.

[14]. Khatri, Pallavi. "TDSR: Trust based DSR Routing Protocol for Securing MANET." International Journal Of Networking And Parallel Computing 1.3 (2013): pp. 42-48.

[15]. Anitha Vijaya Kumar and Akilandeswari Jeyapal, "Self-Adaptive Trust Based ABR Protocol for MANETs Using *Q*-Learning", The Scientific World Journal, Hindawi, pp. 1-9, 2014.

[16]. ElRefaie, Y.; Nassef, L.; Saroit, I.A., "Enhancing security of zone-based routing protocol using trust," *Informatics and Systems (INFOS), 2012 8th International Conference on* , vol., no., pp. 32-39, 14-16 May 2012.

