A Review of Various Trust Based Models in MANET

Prof. Deepak Agrawal, Shradha Singh
Takshila Institute of Engineering & Technology, Jabalpur, Madhya Pradesh, India

ABSTRACT

(MANETs) Mobile Ad-hoc Networks is a group of mobile nodes that are connected dynamically, in which each node acts as a router to all other nodes. Due to the absence of centralized administration and dynamic nature, MANETs are vulnerable to various kinds of attacks from malicious nodes. Several secure routing protocols like AODV, DSR, TSR, and OLSR have been used in MANET for transmission of data. In MANET, we are using trust based QoS aware routing protocol for identifying the malicious nodes in the network. Trust is mandatory in routing for transmission of data securely. Hence trust models, trust computation is implemented in the routing protocols. In this paper, survey of several trusts based and QoS aware routing protocol is performed. In this review paper, the study of different trust based and QoS aware AODV protocols that are using trusted infrastructure and trust models is performed for preventing the attacks and misbehavior from malicious nodes in the network. The performance of trust based routing protocol has been analyzed that helps to work efficiently and can be used in various applications of MANETs for improving the security performance of the network.

Keywords : QoS Constraints, Trust prophecy, malicious nodes, and Trust based QoS routing.

I. INTRODUCTION

Mobile Ad-hoc Network (MANET) [21] is a set of mobile nodes, with no centralized administration or no fixed infrastructure. MANET is a stand-alone and autonomous communication network. [12] The infrastructure of MANET is unpredictable and due to dynamic change in topology, the routing of data is promising.

Ad-hoc networks have various applications such as in healthcare application, military applications, battle-field applications, where wired connection of fixed infrastructure is impossible or maintained. For example, Wireless fidelity, i.e. Wi-Fi (IEEE 802.11) protocol is capable of ad-hoc networking, where the access point is unavailable. In IEEE 802.11, it restricts the node to receive or send the data packets that do not participate in the network or routing. MANET (Mobile ad hoc network) is an infrastructure-less network which consists of various numbers of mobile nodes. The network in MANET is dynamically established without any centralized administration. In MANET [24], mobile nodes make certain tasks that is challenging since they have limited resources like memory, storage, CPU.

The below **figure 1** shows an ad-hoc network that comprises of various mobile nodes, i.e. A, B, C, D, E, F, and G. The network does not acquire a central hub or controller. A node communicates with other nodes B, G and F. whereas G node communicates with A and D. These nodes combine from an ad-hoc network.

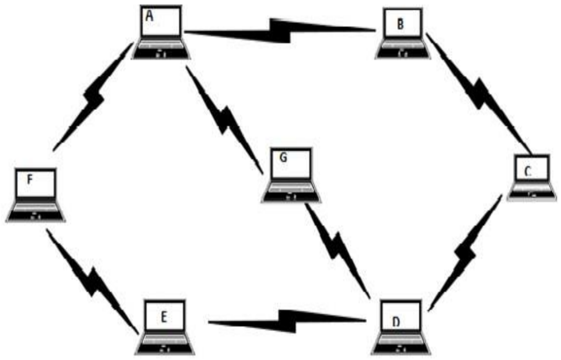

Figure 1: Mobile Ad-hoc Network

1.1 Attacks in MANET (Mobile Ad-Hoc Networks)

The Threats in MANET [15] can be categorized as attacks and misbehavior.

Attacks: the action that deliberately causes damage to the network is called as attack. The attacks [20] are further categorized as origin-based classification and nature-based classification.

An origin-based classification [17] is divided or categorized into two types, external and internal.

External attacks: The attack by a node that is not present in the network or is not able to access the network is considered as external attacks.

Internal attacks [15]: The attack caused by a node that is present in the network is considered as internal attacks. The node may be malicious or compromised. This attack is a more severe type of attack.

Nature-based classification is divided into active attacks and passive attacks.

Passive attacks: The attack [22] in which an attacker node collects the information of the routing and later uses it is considered as passive attack. The attacker nodes eavesdrop on the data packets and try to read it to get the confidential message. In a wireless network, it is easier for attackers to initiate attack in the network rather than in a wired network.

Active attacks: The active attacks [22] include the attacks like sleep scarcity torture in battery i.e battery hijacking, traffic jamming, which causes path unavailability, flooding of packet that causes congestion. Most of the active attack results in denial of service (DoS).

Misbehavior: The nodes [24] that unintentionally cause damage to other nodes in the network. This unauthorized behavior of the node is misbehavior. The goal of this node is not to launch attack, but performing some iniquitous activities in the network. For example, they may not correctly execute the MAC protocol, with the intention of getting higher bandwidth, or they may reject the forwarding packets to other nodes for saving its resources for forwarding its own packets.

Black hole Attack: Attacker node [15] reply to the intermediate node as it is the node to which it wants to communicate and send a fake message to it, and the message is not forwarded to the next node and drops the packet. An attacker node shows to other nodes that it has a shortest path to the destination.

Gray hole attack: An attacker node [15] that drops only some of the data packets and forwards some data packets are termed as the gray hole attacker. Gray-hole nodes are difficult to get detected as it behaves normally as other nodes. These attackers slow and degrade the performance of the network.

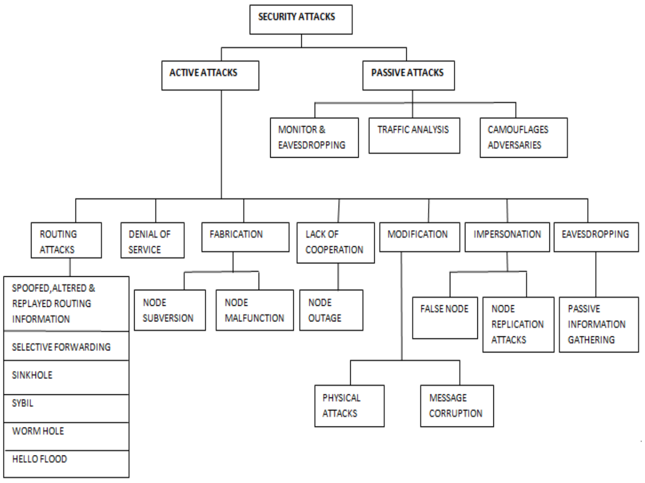

Figure 2. Classification of Security attacks [22]

1.2 Security Requirements of MANET

The security techniques of MANET [13] are not different from other networks. The aim of these techniques is to provide security from various attacks and abnormal behavior to the information and resources. The effective security technique must guarantee the following security requirements.

1. Availability: System guarantees that the services are available to the network.
2. Authentication: System provides the access to the authenticated or known nodes only. Malicious node cannot enter the system.
3. Data confidentiality: System guarantees that a message or data packet cannot be understood by other nodes out of the network. Data is encrypted using cryptographic techniques.
4. Data integrity: Data integrity represents that the message or data packet sent from the sender or server to the receiver is not attacked, misused, distorted or modified.
5. Non-repudiation: A Sender or client cannot refute or deny that the message or data packet was not sent from him to the receiver. Digital signature is implemented that guarantees the non- repudiation.

1.3 Proactive and Reactive routing protocols

In MANET [29], the routing protocol is categorized into two types.

1. Proactive (table driven) protocol
2. Reactive (on-demand) protocol
3. Hybrid protocol

Proactive protocols [29] in general maintain a sequence order of routing information in form of table. It constantly evaluates all the route links in the network frequently. These protocols distributes routing information tables to all the nodes of the network in such a manner that all nodes must have the routing information related to the routes [25], transmission of data packets through a multiple hop paths when data transmission is required. Proactive protocols are unsuitable as the routing is slower since the safeguarding of routing information table is slower. When a link failure occurs, it requires large time to rebuild the network. Various Proactive protocols [15] are DSDV (Destination Source Distance Vector), OLSR (Optimized Link State routing), WRP, FSR, and CGSR (Cluster Gateway Source Routing).

Reactive protocols are on demanded protocols, which do not maintain any table of routing information. In this protocol, the nodes discover the routing path when needed. The protocol finds the path by flooding the RREQ packets in the network. When a link failure [26] occurs, the reconstruction of the link is faster and easier. The reactive protocols [15] consume fewer bandwidths than the proactive protocols. Reactive protocols are AODV, DSR, ABR, and ACOR.

Hybrid protocols consist of features of both proactive protocol and reactive protocols. Hybrid protocols overcome the limitations of both protocols. Hybrid protocols [15] are ZRP, TORA, CGSR (Cluster Gateway Source Routing), OORP, LANMAR, HSR, ARPAM.

In MANET, reactive routing protocols [16] is efficient than the proactive protocols. It is essential to provide safety measures to the routing protocol. If the routing protocols in the network or data packets or messages are distorted during the data transmission, then the data might get compromised or hijacked by the malicious nodes.

II. LITERATURE REVIEW

2.1 Efficient And Trust Routing In Manet [6]

An algorithm is proposed by Dr. K. Thirunadana et al. [6] named as ETAR (Efficient Trust-based Ad-hoc routing). Every single node present in the network had to fulfill the challenge to join the friend node list, if the node does not fulfill the challenge; the nodes join the malicious nodes list known as a question mark list. The list is created by observing the data packets transmission through the nodes. The higher the node transmits the data packets. The higher is the rating of the node. The rating of the nodes lies between zero to10.

A. Topology:

The number of nodes that are available to participate and take part in the network is only decided through the simulation topology of the network. In MANET (Mobile Ad-Hoc Network), the topology or the infrastructure changes dynamically. Each node in the network has its distinct characteristics. Some nodes may consist of the type of addressing. Some may define the network components for nodes, and some of the nodes decide the routing protocol.

B. Challenging the neighbors:

Challenge is a test in which a node has to compete to prove its integrity and honesty. Challenge is a terminology for the authentication of the nodes present in the network.

Assume that a node challenges its neighbor node. When a network is created initially, each node is stranger to be other. Each node interacts with its neighbors in an unauthenticated manner. Suppose a node A selects one of its neighbor i.e. B and performs share friends. The node B as a response sends a friend list if the friend list is not empty. And sends the unauthenticated list if the list is empty. When the node A gets the list, the node A chooses a node to which the route is most efficient and low cost. Let us suppose that the node A chooses node C. the node A has two routes to reach the node C. One through node B and other route is already known to it. The node accepts a challenge and encrypts it with the public key of a node C. now node A sends this encrypted form through both routes and includes its own public key with the challenge. The node B sees this encrypted form as a normal data packet. Whereas the node C sees this encrypted form and decrypts the packet with the A’s public key and finds the challenge, then the node C responds to the challenge. Afterwards, the node C encrypts the response with A’s public key that it gets with the challenge. Node A receives the responses from the both nodes and after decryption, it compares both the responses. If both the responses are same, then the node, A adds node B in the bottom of its friend list.

ETAR (Efficient Trust Based Ad Hoc Routing):

The ETAR protocol is accomplished through the establishment of friend networks in MANETs. When a person meets a new group or community, he is stranger to everyone. In a company, a task is performed with the help of each employee present in the group. However, to perform in a group trust is must. The job is only completed by trusting each other in a community. With the time the trust degree increases in the number of successful job completed that leads to the formation of a group or community where jobs are efficiently completed.

The ETAR algorithm is categorized into four stages:

1. Challenge your neighbors
2. Rate your friends
3. Share friend list
4. Route through friends

The above three stages of the algorithm are periodic whereas the fourth is on demand. The authentication of the nodes is done through the completion of a challenge. Nodes that complete the challenge is placed in the friend list. The other nodes are placed in the unauthorized list. The nodes in the unauthorized list shows distrust hence are not used in the routing. The unauthorized list also contains the nodes that are degraded from the friend list. The trust value of nodes is rated by the amount of data packets they transfer to other nodes.

2.2 Ant Colony Optimization AOMDV [4]

AOMDV Protocol:

In AOMDV, RREQ packet is transmitted to the destination and establishes various reverse routes at intermediate nodes and destination node. Multiple RREPs [22] are transmitted along the reverse path to form numerous routes to the destination and sender node. The additional RREQs and RREPs are needed for discovery and maintenance of the numerous routes which lead to routing packets overhead.

Proposed model*:*

Chintan Kanani et al. proposed a model [11] in which ant while traversing a path leaves behind a volatile chemical substance called pheromone.

The main objective of this proposed algorithm [4] is that the nodes present in the network sends artificial ants to the destination nodes asynchronously. The artificial ants are the control packets, which are assigned job to find a suitable path through the destination nodes. These ants move along the path and drop the pheromone. The pheromone specifies the quality of the routes to the destination. The pheromones [12] are updated through the forward ant that finds a route towards destination and backward ant that traverse back to that route. Hence the routing table is also updated. The path with the highest pheromone is selected in the algorithm.

2.3 Trust Computations and Dynamics in MANETs [8]

In Mobile Ad-Hoc Networks (MANETs) [15], the distrusted nodes can damage the data transmission process. MANETS is deployed in harsh environments [8], hence there centralized control unit is difficult to maintain and is unable to monitor the node behavior. Therefore, establishing behavior of nodes as the trust computation is essential for the secure transmission of data. The trust computation is necessary in large-scale networks, where the networks are large and tactical. The node’s operations, sensing capabilities is different of distinctive nodes. The trust value of each node is updated after a certain period through some mathematical computations performed. However, trust computations [16] are complex due to various reasons such as mobility of nodes, changing behavior of the nodes, changing of the neighbor nodes.

In this proposed trust model, the main functional units are:

1. Trust computations
2. Trust aggregation
3. Trust propagation
4. Trust prediction

These four blocks [8] are interconnected to each other in this trust system.

In this proposed work, firstly, the computation of the trust values of all the nodes is performed. These trust values are stored in a trust value table from where they are used when required in the process of routing of data packets. All the above functional units i.e. trust computation, trust aggregation, trust propagation. Trust prediction is linked to each other in the trust model.

Trust definition:

Trust is estimated through availability, QOS, reliability, accuracy, integrity, honesty.

The trust value (T) denotes the observed trust. Confidence value (C) denotes confidence on an ascertained trust of a node.

Trust calculation consists of three mechanisms, i.e. recommendation, experience and knowledge. Through experience, the trust of a node is calculated through the neighbors of the node. These three mechanisms are necessary to denote the trust value of a node. The trust table stores the value of the nodes in a fixed update interval.

2.4 QoS Routing for MANETs [27]:

Scott Corson et al [27] proposed the routing based on QoS constraints.

In this proposed algorithm, AODV protocol and NP-complete is implemented for performing QoS routing. This algorithm is a session oriented and in each session, the route is discovered with sufficient bandwidth through NP- complete.

The QoS routing protocol:

QoS routing finds a route with required bandwidth. AODV routing protocol is used that broadcasts route discovery mechanism. In TDMA [23], the bandwidth is calculated in RREQ phase as RREQ packet is a forwarded node to node. This leaves a FP path behind, and the bandwidth for FP is calculated. Node checks, whether FP meets the required bandwidth, if not it drops the RREQ packet. For this path, no RREP is generated. When RREQ packet reaches the destination through path P, a route with satisfying bandwidth is found.

When a source node wants to find a QoS route to destination, it sends RREQ packet and the route is discovered. A path FP is set as RREQ packet is sent by the source. FA calculates the bandwidth on the partial path FP. Each node sets the entry for the QoS route and sets the state to REQ, which shows whether the request is processed and forwarded. If the required bandwidth does not meet, then the RREQ packet will be dropped. When a node drops a RREQ packet, it processes the other RREQ packet, with same broadcast ID. QoS route P [21] is found to the destination. The destination nodes send RREP packet along the path P in the reverse direction. It checks the neighbor from which RREQ is received and sends the RREP to this node. Node forwards the first RREQ and discards other RREQ with similar broadcast ID. When RREP packet reaches the source, each link on path P finds its transmission slots, and the QoS route with required bandwidth R is established. When a path is not used for a time, its entry is deleted from the routing table for ensuring that each route in routing table is fresh.

2.5 Zone Routing Protocol (ZRP) [24]

Zone Routing Protocol (ZRP) is the hybrid routing protocol that inherits the properties of both proactive and reactive routing protocols. ZRP protocol is capable in reducing the routing control overhead and reduces the drawback of both types of protocols. ZRP protocol dedicates a routing region for each mobile node that consists of its k-neighbors. A routing region is dedicated to every node present in the network area, and it consists of the mobile nodes that are present in minimum distance from other nodes. Every node is present at a distance that is predefined within the routing zone of the mobile node. Zones routing protocol consist of two protocols i.e. Inter-Zone Routing Protocol (IERP) and Intra-Zone Routing Protocol (IARP). IARP is used for the mobile nodes present inside routing area whereas IERP [34] is used for the mobile nodes present to discover the routing path between different routing areas and maintains routing tables for receiver nodes of the same routing area which is established using proactive routing protocols.

Route discovery in a routing zone is established using reactive routing protocols. Sender Node S sends RREQs packet to its neighbor nodes and initiates route discovery procedure. The RREQs packet consists of the source or sender address, destination or receiver node address and a sequence number that identifies a node. When destination is reached, the destination node sends RREP packet to the source node in the reverse path of the route.

2.6 QoS-aware and power control algorithm for MANET [10]

In the proposed work, a joint optimized QoS aware routing with the power control algorithms is implemented that provides and supports multimedia service to multiple hops MANET using 802.11b that uses low power consumption during transmission. The aim of implementing this algorithm was to provide good QoS service for multimedia applications with low power consumption during the transmission in MANET. Several assumptions were taken in this algorithm. First, the required bandwidth with received signal strength was provided to every single node. Second, the multiple rate links was provided to each node for controlling the transmission power. Packets were sent in the FCFS order at each node present in the network.

In the projected algorithm and work the path (route) consists of various nodes, including the source and destination, and their transmission power. In the route establishment phase [10], the sender node broadcast RREQ packet with its power strength and minimum bandwidth to its immediate neighbor. When a neighbor node receives the RREQ packet, its checks the distance from the source node and updates the RREQ packet and broadcasts to its neighbor. The procedure is repeated until the destination is reached. Then the RREP packet [3] is sent to the source node along the reverse path. A routing table is maintained in which the connection between the nodes is stored. Hence the route with nodes with minimum transmission power is constructed.

In route maintenance mechanism, hello packet is used. RABR sends hello packet after every fixed interval periodically for checking the links of the route. In this propose work, every node keeps an eye on the expected power during the communication between the nodes. This mechanism is efficient for the multimedia applications. As in multimedia, the packets are transmitted one by one in a sequence and in a fixed interval periodically.

2.7 2.7 (SAODV) [19]

This paper presents a secure routing protocol named as invulnerable AODV (SAODV). This routing protocol consists of various characteristics like authentication, integrity, non-repudiation of data packets. SAODV allows intermediate nodes for replying to RREQ packets. When a sender node A generates a RREQ messages, with addition to the regular signature, it can add another signature, which is computed on a RREP packet that is forwarded to the sender node A itself. Intermediate or neighbor nodes hold this second signature in the routing table with the routing information of every node. If any of the nodes present in the network receives a RREQ towards the node A, it replies to the node with RREP packet. In this, the intermediate node generates the RREP message that includes the signature of node A that was previously traversed, and signs the data packet with its own secret key. SAODV does not need more message packets than AODV. SAODV message packets are larger than AODV, since it consists of digital signatures and requires a large number of asymmetric cryptographic operations. When a node generates a routing message, it must also generate a digital signature. When a node receives a routing message, it verifies the signature. SAODV provides authentication to the AODV routing data messages. Mainly two technologies [19] are used in this protocol, i.e. digital signatures and hash chains.

2.8 Trust based AODV protocol for MANET [18]:

In TAODV [18], the network is set with some models like intrusion-detection system in the application layer or network layer such that a node can monitor the behavior of its neighbor nodes present in the network. In our trust model [18], new node, model is designed in the network layer. Additional fields are added in the routing table of a node to store the response about the neighbor nodes trustworthiness. The record stores the positive and negative evidence of the nodes when they transmit data packets to other nodes. Implementing the trust model in the routing protocol saves the consuming time, without the problem of maintenance of expiry time or validity status of nodes. For providing security in the proposed work, RSA signature [18] has been used.

The algorithm of TAODV is as follows:

1. In route discovery phases a sender node forwards RREQ packets to its neighbor nodes. In this packet key, information is also stored.
2. When RREQ packet is received by an intermediate node, the nodes store the QOS information and trustworthiness link in RREQ packet and forward it to its next neighbor nodes. This mechanism is repeated unless the destination is not reached.
3. The destination node waits for a number of RREQ packets before taking the routing decision. When all RREQ packets are received, the receiver node compares the TQI values and selects the index with minimum cost. Then it unicast the RREP packet to the sender node. When the sender node receives the RREP packet, the data transmission has been started.
4. When the path has been established the intermediate nodes checked the route status of the next nodes. The nodes which do not possess the trustworthiness and performance requirements will be removed from the path.
5. When a link is damaged or broken, a RERR packet is used to inform the other nodes that the link breakage has occurred.

When the communication is successful between two nodes, the event is called a positive event. When the communication is failed between two nodes, the event is called the negative event.

The node's faith towards other neighbor nodes honesty is called for the opinion.

Trust Updation

1. When a positive event occurs from node A to node B, the number of successful events of B in A's routing table will be increased by 1.
2. When a negative event occurs from node A to node B, the number of failed events of B in A's routing table will be increased by 1.
3. When the record of positive or negative events changes, then the value of opinion will be calculated in the opinion space.
4. When a new opinion is received, the positive and negative events are calculated again using the opinion to the evidence space.

2.9 QoS-Aware Routing Based Networks [27]

In the proposed work, QoS aware routing protocol is implemented with IEEE 802.11 that provides the best service for audio and video applications. AODV protocol is used in the proposed work in which routing table is maintained and during link breakage, Hello packets [5] are broadcasted for detecting the links.

QoS [2] provides guaranteed quality services such as bandwidth, delay, packet delivery ratio, to the users. QoS constraint is helpful in making the QoS routing protocol as NP-complete. QoS aware routing supports real time audio and video transmission and mainly bandwidth is considered. QoS-aware routing protocol provides acknowledgement about bandwidth, i.e. acknowledgement scheme to the model or algorithm and shows the flow of the requested bandwidth (i.e. admission scheme).

In route discovery phase, the source nodes sends RREQ packet to other neighbor nodes, the header of the packet stores minimum bandwidth, bandwidth request to minimize the bandwidth. The model-flag [9] represents what the source is using either admission mechanism or adaptive feedback mechanism. If the source is using admission mechanism, the node compares its bandwidth with the needed bandwidth, if the bandwidth is greater than the needed bandwidth, the node forwards the RREQ packet to its next node, else drop the packet. If the source node is using adaptive feedback mechanism, the node compares the bandwidth with minimum bandwidth mentioned in the RREQ packet. If the bandwidth is greater than the required minimum bandwidth, the node forwards the RREQ packet to the next neighbor node else updates the minimum bandwidth value in the packet. After comparison and when the RREQ packet reaches the sender node, the destination node sends the RREP packet to the source node with modification in minimum bandwidth value and the route is established. The route path along with the minimum bandwidth value is stored in the routing table of each node which is used in future in route maintenance.

2.10 A Light-Weight Routing Algorithm [1]

In this proposed work, Bo Wang et al [1] a trust based QoS model is initiated in which trust calculation and QoS constraints are estimated. QoS provides guaranteed quality services for nodes such as bandwidth, delay, and packet delivery ratio.

As the nodes present in the mobile ad-hoc network does not know each other before the route establishment. Hence communal trust relationship is established between the nodes. Trust calculated from direct communication is defined as direct trust and trust calculated from neighbor's recommendation is defined as indirect trust. Hence the trust value of a node is calculated through both direct trust and indirect trust.

Every node defines the trust value for its neighbor nodes. Hence for calculating the trust value of a node, the recommendation of neighbor nodes and its previous value is considered. The trust value of a node ranges between 0 and 1. The trust value 1 represents the complete trust on a node, whereas 0 represents distrust on a node. Two weight factors w1 and w2 [1] are considered, where w1+w2=1, i.e. the sum of the weight factors is always equal to 1. The direct trust value is calculated as the ratio of the number of forwarded packets to the number of received packets. Indirect trust value is calculated by the sum of neighbor's recommendation [1]. In this paper the nodes with higher trust value more than 0.5 are considered in the route selection. Mainly the forwarding ratio concept of the packets is considered for trust calculation. Source node monitors if there is alteration in the data packets, and decreases the forwarding ratio by 1. A node monitors and checks the forwarding behavior of a neighbor. The trust values of nodes are updated after a firm time period. A table is maintained for storing the trust values and trust information at every node.

Every node present in the network stores the trust table, such that malicious nodes are exempted from the network. Trust management includes trust estimation, trust analysis and trust updating.

Route Discovery:

When source node s wants to communicate the destination node D, then initially S checks whether a path is available or not.

Route maintenance process:

The method through which the source node S detects that if there is any change in the topology or the link is attacked or broken by attacker or malicious nodes. When a route is broken, then through route maintenance, source node S initiates other routes through available paths or route discovery mechanism. The route maintenance mechanism is used only if source node S is sending data packets to the destination node D. When a link- broken event occurs, the nodes broadcast the RERR packets to their sender nodes for selecting the optimal path with trusted nodes else the route discovery process will restart.

***Features of TQR algorithm**:*

The TQR algorithm ensures that the network is loop-free.

The set of neighbor nodes includes nodes with trust degree higher than the threshold value

VARIOUS TRUSTS USED IN THE MODELS KEY MANAGEMENT [28]

In the previous time, most of the models projected for secure routing and message transmission were based on cryptographic systems that were able of key management and providing the keys to the sender and the destination. Since the MANET is an infrastructure-less, self-configured and not based on central administrator, key management was an issue, how to manage and distribute the keys in the network, as the nodes are mobile and move in any direction. Hence the network is distributed and does not believe in Certificate Authority (CA). Mainly the key distribution is divided into two:

1. Private Key infrastructure and
2. Public Key infrastructure.

1. Private Key Infrastructure: In symmetric cryptography, private keys are used in cluster transmission. Private Key Infrastructure is further divided into key distribution protocols and key agreement protocols. Key agreement is centralized and uses third party for trustworthiness whereas key Distribution is distributed. Key agreement is most commonly used and implemented as it is more trusted for providing security to the models in MANET.
2. Public Key Infrastructure: Public Key infrastructure is also known as asymmetric cryptography that includes digital certificates and digital signatures. Public Key Infrastructure uses combination of both private keys and public keys.

Private key Infrastructure is good in multicasting, multi routing. But in dynamic topology the nodes are movable, they move freely in the network. Hence an improved technique that is efficient for dynamicity is required, Such that they make the models more secure and trusted.

Public Key Infrastructure

Every node contains a pair of public and private keys in Public Key Infrastructure. Public keys are common that is distributed to all nodes evenly. But private key is known only to the node, no other node can access that key that is required for providing security to the system. In Digital Signatures, the Certificate Authority (CA) is used for distributing the public keys and private keys to the sender and receiver for checking the authentication of certificates.

MOCA:

MOCA [25] (Mobile Certificate Authorities) is a technique in which CA (Certificate Authority) is distributed over some nodes that are specially chosen through their physical features and their security. In the MOCA protocol, node requires a certificate and sends request for certification i.e. CRQ (Certification Request) packets to MOCA, and then MOCA responds to CRQ packet with CREP (Certification Reply) which consist of a fractional signature. The node constructs a complete signature using a number of CREP packets. CREQ packets are same as RREQ packets and CREP packets are same as RREP packets. The drawback of MOCA is the overhead of number of fractional signature and the delay for generating a complete signature.

PGP trust Graphs:

A trust model is implemented for MANET, in which each and every node signs in certificates of other nodes [14]. Transitive trust is required in this trust model. If P trusts Q, and Q trusts S, then P will also trust S. The chain of certificates is followed in which nodes authenticate the message. When various nodes lie between the sender and receiver, an attacker must have to compromise a node in each and every path so that the network gets compromised. But, the network limits the certificate's length for the nodes such that an attacker cannot enter the network easily.

Public-key revocation

Certificate authority [14] invalidates the certificate for public key of a node when a node gets compromised. Hence a mechanism is required that can prevent attacker from invalidating the keys. But this problem is more complicated than the key management problem. A mechanism can be followed where the block list of nodes and information related to the invalidation of certificates of nodes can be broadcasted to nodes in the network when invalidation of certificates occurs. But, the broadcasting is limited such that no attacker other than nodes of the network may receive this information.

Intrusion Detection System (IDSS) [5]:

Intrusion is defined as a set of events to alter or compromise the availability, integrity, confidentiality of resources or unauthorized activities in a network. An IDS is a system that detects and gives alert on various misbehaviors in a network or system. The proactive routing solutions alone are not enough to prevent from the intrusion, attacks. Hence IDS [5] was implemented. IDS are basically of two types:

1. Anomaly detection based IDS
2. Signature based IDS

Ariadne:

Ariadne [26] is a secure on-demand routing protocol that prevents compromising of nodes and believes in public key cryptography or symmetric cryptography. Ariadne authenticates the routing messages i.e. it authenticates the shared confidential message between two nodes, authenticates confidential message between broadcasting nodes and authenticates digital signatures.

Initially the RREQ packet is authenticated and hashing technique is used for validating that in the node list, no node is missing. Then sender S initiates route to destination D by sharing keys Ksd and Kds for authenticating the messages. Sender adds MAC that is computed through Ksd in RREQ packet. The destination D validates the RREQ packet by the key Ksd. Each node has to authenticate to participate in the communication. The destination D authenticates and verifies each and every node present in the route list using a Tesla key, and sends RREP packet to the nodes that are valid that consist of MAC which validates the tesla condition of the node.

Route maintenance is analogous to DSR in Ariadne Routing Protocol. When a data packet [26] is not delivered to its neighbor or next node, the node sends Route Error (RERR) packet to the source node. Then the source node authenticates the RERR packet. If the response takes time, Tesla is used for authenticating the RERR packets.

Ariadne is proposed for preventing vulnerable routes from the network and chooses the most efficient and performance based path. Acknowledgement can be received through network layer or transport layer. The drawback of the protocol is its high cost.

Virendra et al [28] proposed a trust model for MANET based on key management. In the proposed model, between two nodes, pair of keys is required for providing trust between them and also implements distributed secure control for the nodes. The nodes in this self-configured network are formed in forms of clusters named as PLTDs (Physical Logical Trust Domains) that consist of only valid nodes that shares a common key for all the nodes. As nodes are mobile and are free to move, a node may be a part of many clusters, but it is not an issue. The trust value of each node is calculated and trust is updated at a regular interval of time. The drawback of the model is the use of pair of keys which may lead to low scalability.

Yan et al [28] proposed a security technique. The proposed work is evaluated in basis of trust which provides protection to data and information, and secure routing. PTB (Personal Trusted Bubble) is a trust evaluating model that requires the value of the data i.e. the confidentiality of the data, recommendation by the nodes, preferences of data, and black list of attackers for deriving the trust values of data. But the validation of the trust model is complex and tough.

Table 1. Comparison of various Research works and trust models

S.No	Features	Chintan Kanani et al [12]	Yogendra Jain et al[38]	Bo Wang et al [5]	Dr.K. Thirunadana et al [19]	Chenxi Zhu et al.[74]
1.	Routing Protocol Used	AODV	AODV	AODV	AODV	AODV
2.	Technology Used	Ant Colony Optimization	RSA Signature	NP Completeness with QoS constraints	Public Crypto System	NP Completeness problem
6.	Update trust value	No	Yes	Yes	Yes	Yes
7.	Hello packets	No	No	Yes	No	No
8.	Route Metric	No	Route with authentication	Trusted path with QoS Constraints	Shortest path+ Authentication	No
9.	Unidirectional link	Best route	No	No	No	Shortest Path
10.	Multiple Routes	No	Yes	Yes	No	No
11.	Packet loss ratio	Yes	Low	Low	Low	No
12.	Packet Forwarding Ratio	Low	Good	Better	Good	High
13.	Detection of malicious nodes	Good	Good	Good	Good	Low
14.	Throughput	Low	Good	Best	Good	Low
15.	Routing Packet overhead	Low	Low	Lowest	Low	Low
16.	Routing maintenance	High	Yes	Yes	Low	High

III. CONCLUSION

In this paper, survey of various trust based routing protocol were studied and analyzed. Among these protocol models, most of the routing protocols use the QoS service in the algorithm. Hence the performance of the routing protocols can be enhanced using trust models, QoS metrics and trusted models in the algorithm for MANET. Various types of attacks can be controlled through this trust based models. AODV protocol is used mainly for the route discovery and route maintenance when the link fails, hence is mostly used in the routing protocols.

IV. REFERENCES

[1]. T., B Wang, X Chen, W Chang, "A Light- Weight Trust- Based QoS Routing Algorithm for Ad Hoc Networks",

[2]. Pervasive and Mobile Computing 13, pp. 164-180, 2015

[3]. Suparna, Tanumoy, Sarmistha, "Trust Based energy Efficient Detection and Avoidance of

Black Hole attack to ensure routing in MANET", Applications and Innovations in Mobile Computing, pp. 157-164, 2016

[4]. P Kautoo, Dr. Piyush Shukla, Dr. Sanjay Silakari, "Trust formulization in Dynamic Source Routing Protocol using SVM", IJITCS, MECS, pp. 43-50, 2015

[5]. C. Kanani, A. Sinhal, "Ant Colony Optimization based modified AOMDV for multipath routing in MANET", IJCA, Volume 82, Pp. 14-19, Nov 2014

[6]. R. Menaka, Dr. V. Ranganathan, "A Survey of Trust related Protocols for Mobile Ad Hoc Networks". IJETAR journal, volume 3, Pp. 903-910, April 2015

[7]. Dr. K. Thirunadana, Sikamani, D. Santhosh Kumar, "Efficient and Secure Trust based Ad Hoc Routing in MANET", ICCTET, Pp. 255-258, 2015

[8]. Radha Krishna Bara, Jyotsna Kumar Mandala and Moirangthem Marjit Singh, "QoS of MANET Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack", ICIMTA , Procedia Technology 10, Pp. 530 - 537, 2014

[9]. K. Govindan, P. Mohapatra, "Trust Computations and Trust Dynamics in Mobile Ad Hoc Networks: A Survey", IEEE Communications Surveys and Tutorials 14, Pp. 279-298, 2012

[10]. G.M. Kaur, K. Kumar, "QoS Routing Protocols for Mobile Ad Hoc Networks: A Survey", IJWMC-5, Pp. 107-118, 2012

[11]. Z.K.Lee, G. Lee, H. Rai oh, H. Song, "QoS aware Routing and Power Control Algorithm for Multimedia Service over Multihop Mobile Ad Hoc Network", Wireless Communications and Mobile Computing-12, pp. 567-579, 2012

[12]. P. V Krishna, V.Saritha, et al, "Quality ofSservice enabled Ant Colony-based Multipath Routing for Mobile Ad hoc Networks", Published in IET communications- 6, Pp. 76-83, 2014

[13]. Yogendra Jain, Pankaj Sharma, "Trust based Ad Hoc on- Demand Distance Vector for MANET", NCSI Conference, Pp. 1-11, 2015

[14]. Rutvij H. Jhaveri, Sankita Patel, Devesh Jinwala, "DoS attacks in Mobile Ad-hoc Networks: A Survey", pp. 535-541, 2012

[15]. Jin Hee Cho, Ananthram Swami, Ray Chen, "A Survey on Trust Management for Mobile Ad Hoc Networks", IEEE Communication Surveys and Tutorials 13, pp. 562- 583, 2014

[16]. Sudhir Agrawal, Sanjeev jain, Sanjeev Sharma, "A survey of Routing attacks and security measures in Mobile ad hoc networks", Journal of computing, Volume 3, pp. 41-48, 2015

[17]. T. Eissa, S. A. Razak, Rashid H. Khokhar, N. Samian, "Trust- based Routing Mechanism in MANET: Design and Implementation", Springer Journal, Pp. 666-677, 2011

[18]. Pedro B. Velloso, Rafael P. Laufer, Daniel de O.Cunha , "Trust Management in Mobile Ad Hoc Networks using a Scalable Maturity-based Model", IEEE Transactions in Network-7, Pp. 172-185, 2010

[19]. A Menaka Pushpa, "Trust based Secure Routing in AODV Routing Protocol', IEEE Transaction, Pp. 1-6, 2009

[20]. S. Lu, L. Li, and K. Yan Lam, L. Jia, "SAODV: A MANET routing protocol that can withstand Black Hole attack", Published in IEEE ICCIS, pp. 421-425, 2009

[21]. A. Khokhar, L.Abusalah, M Guizani, "A Survey of Secure Mobile Ad Hoc Routing Protocols", IEEE Communication in Surveys and Tutorials-19, pp. 78-93, 2008

[22]. C Liu, J. Kaiser, "A Survey of Mobile Ad Hoc Network Routing Protocols", University of Magdeburg, Pp. 1-36, 2005

[23]. L Khelladi, D Djenouri , N Badache, "A Survey of Security issues in Mobile Ad Hoc and Sensor Networks", IEEE Communication Surveys and Tutorials, Pp. 2-28, 2005

[24]. Wendi, L Chen, B Heinzelman, "QoS-aware Routing based on Bandwidth estimation for Mobile Ad Hoc Networks", IEEE Communication, Pp. 561-572, 2005

[25]. A Perrig, Y hu, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Computer Society-2 , pp. 28-39, 2004

[26]. R Kravets, S Yi, "MOCA: Mobile Certificate Authority for Wireless Ad Hoc Networks", II Annual PKI'03, pp 1- 3, 2003

[27]. Y C Hu, A Perrig, and D B Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks", 8th Annual IICMCN Mobicom, pp. 12-23, 2002

[28]. C Zhu, M Scott Corson, "QoS Routing for Mobile Ad Hoc Networks", Flarion Technologies, Pp. 1-10, 2002

[29]. Rinzboorg, N. Asokan, "Key Agreement in Ad Hoc Networks", Computer Communication, Volume 23, Pp. 1627-1637, 2000

[30]. B Praveen Kumar,B Bharath Bhushan, P Chandra Sekhar, N Papanna, "A Survey on MANET Security Challenges and Routing Protocols", IJCTA, Volume 4, pp 248-256,2000