STUDY ON SECURE ROUTING MECHANISM IN MANET USING TRUST MODEL

[1]K.Ranjithsingh, [2]Dr. D. Maruthanayagam
[1]Research Scholar, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India
[2] Head/Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India.

Abstract: MANET is a nature of wireless network without a rigid topology and consists of lay down of self-organized nodes. It is a lay down of mobile devices that can be communicate to each other without have cabled network. In communication purpose, they do not need help from network infrastructure. MANET (Mobile AdHoc Networks) is second-hand in many real world applications. Some of them consist of battlefield applications; liberate work applications, civilian applications like outdoor meeting, money transfers, and ad-hoc classrooms. ***There are many advantages of ad hoc networks. However, they also throw security challenges***. The security attacks might be either internal or external attacks or both. The internal attacks are cause by collude nodes in the MANETs. The nodes are randomly, repeatedly and impulsively mobile. It is a dynamic, infrastructure less and decentralized network. The self-configuration ability of AdHoc networks constitutes an extensive variety of applications in tactical and common life. Security is foremost problem faced by the Ad Hoc networks due to its open environments. The intrinsic features of Mobile AdHoc networks make it susceptible to ***many security attacks*** which may completely or partially ***destroys and changes the information*** contents and functionality of the networks. ***This paper aims to provide better understanding of routing protocols, classification of routing protocols, security attacks, trust models and various types of trust model***.

Keywords: Mobile Ad Hoc networks, Routing mechanism; Trust model , MANETs, trust, Trust computation, Trust Propagation , Mobile networks and Attacks.

I.INTRODUCTION

MANET is the identity or self configuration ability of AdHoc networks that is created by a collection of adaptive mobile nodes with no aid of a rigid infrastructure otherwise centralized management. Each node is able to transfer the information by means of communication with other nodes within its communication range with a wireless transmitter and receiver. If a node wants to communicate with other nodes that are out of its coverage area, its need to cooperate with other nodes in between; this is known as ***multi-hop communication***. Hence, each node has to operate together a router and a host at the equal time. Mobile adhoc network is made with collection of adaptive nodes with the purpose of self contain and have capability to connect to nearby wireless node and configure them without having any dependency on any pre-defined network infrastructure. Fraudulent activities are done by one or more colluding nodes that work together. The colluding nodes attempt to hide from view their activities in order to maintain their malicious remain hidden. Thus the colluding nodes compromise single or many nodes in the adhoc network so as to carry out the fraudulent activities and cause troubles in the networks with their internal attacks.

The main internal attacks they cause include resource consumption attack, fabrication attack, replay attack and black hold attack. In MANETs, formation of the cluster for resource management, that is to be collection of computers interlinked. Formation of the cluster base on the data lines series of nodes. In MANETs a ***cluster-based communication*** infrastructure is used for broadcasting. It also reduces collision in networking, energy consumption, and delay in packet transmission. It also improves throughput of the network [1], performance of features such as limited bandwidth usage, virtual circuit support and power consumption. In the case that pure adhoc networks, trust management becomes very difficult by central authority and further nodes in the MANET and their interdependency. It is very challenging to have trusts calculated from different levels [8]. For ambiguity reasoning a method is proposed [4], the name of the method is known as Demp-ster-Shafer Theory. According to this theory some range of probabilities can be used instead of using single number of probabilities. Some mass functions ignore such ambiguities. It is achieved by Bayesian theorem. According to this theory, the posterior probability gets changed. This is done as evidence that helps in getting probability values from the environment required [3]. The difference between the beliefs is used in evidence in the Demp-ster-Shafer theory.

The network topology often changes because of the mobility of adaptive mobile nodes as they go inside, go into, or go elsewhere of the network. As MANETs happen to extensively used, the security problem has one of the main fields of concern. In MANETs, both the ***active and passive attacks*** can effect. For passive attacks, packets contain furtive information might be eavesdrop, which violates confidentiality. Active attacks, including inject packets to invalid destinations into the network, modify the contents of the packets, deleting packets and impersonate other nodes violate availability, authentication, integrity, and non-repudiation. ***Proactive approaches such as cryptography and authentication*** and many other techniques have been proposed and implemented. However, these applications are not sufficient. If we have the ability to detect the attack before it is going to occur, we can stop any malicious node from doing any damage to the system or any data. Here is where ***the concept of trust based system*** comes in.

The main aim of the trust model is to provide combined solution for preventing malicious activities and uniform resource utilization by load balancing of packets being forwarded. The trust model represents how to ***calculate the trust of the routing path by using trust value*** of individual nodes. The reactive routing protocols of MANET look for the routes and are created as and while required. When a starting

position (source) wants to send to end position (destination), it invokes the route discovery mechanisms to hit upon path to the end position. For example: Ad-Hoc Ondemand Distance-Vector (AODV), Dynamic MANET On demand (DYMO), Dynamic Source Routing (DSR). Most Trust security scheme recommended for MANETs have a tendency to build upon some fundamental assumption concerning the trustworthiness of the participating nodes and the fundamental networking systems without present any specific method for trust establishment. The existing trust based mechanisms of MANETS are Trust AODV (TAODV), Trust Based DSR, Adaptive SAODV (A-SAODV), Friend based Ad hoc routing using Challenges to Establish Security (FACES), Cooperation of Nodes-Fairness in Dynamic Ad-hoc Networks(CONFIDANT), Friendship Based AODV (FrAODV), Secure Routing Using-Trust (SRT), Trusted AOMDV and Secure Adhoc on demand distance vector Routing (SAODV).

In this paper, ***research work will be focus on scheme a secure routing mechanism based on trust model*** for MANET in a self organized way as a substitute of using centralized servers. It will aims several most important features like Nodes achieve trusted routing behaviors mainly according to the trust relationships among them; a node which performs misbehavior will finally be the detected and the denied to whole network; and System performance will improve by avoid the requesting and the verifying certificates at each routing step. The nodes will assist; trust each other by forward the packet from one node to one more (another) because of the low down transmission power of apiece ad-hoc node limit its communication range. This research will expand the routing table and routing messages of ADOV with the trust information which will be updated unswervingly through monitoring in the neighborhood. The more the positive events will collect, the higher the belief value in the opinion will be. Our propose trust model will concentrate trust formation and trust usage for routing decisions. In trust formation phase, every node will collect the network data like packets forwarded, packets delayed and packets dropped etc., based on the trust node will calculate. Though collection of statistics is performed regularly, it will use only when requested routing path contains the node as intermediate node. All intermediary nodes calculate their trust values using best equations while the route from source to the requested destination.

II.CLASSIFICATION OF ROUTING PROTOCOLS

Routing protocols defines the rules which govern the ride of message packet from source node to the destination node in a network. There is various type of routing protocols in MANET; each one of them is apply accordingly to the network situation.

Proactive Routing Protocols

Proactive routing protocols otherwise called as table driven routing protocols. In this each node maintaining the routing tables for which contain the information regarding the network topology still without requiring it [8]. This characteristic although useful for power consumption, datagram traffic and incur substantial signaling traffic [12]. While the network topology changes, routing tables are reorganized periodically. ***Proactive protocols are not fitting for large networks*** as they want to retain the node entry intended for all nodes in the routing tables of every node [13]. These protocols need to maintain the dissimilar amount of routing tables unreliable from protocol to protocol. There are a variety of familiar proactive routing protocols. **Example: OLSR, DSDV, WRP** etc.

i)Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV):

DSDV [14] is urbanized on the root of Bellman–Ford routing [15] algorithm with several modifications. In this protocol, every mobile node has a routing table in this network. Each of the routing table contains the listing of all accessible destinations and the series of hops to everyone. Each table entry is tag with a sequence number, which is originating by the destination node. Periodic transmission update the table of routing assists to maintain the information of this network topology. If there is any new important change for the routing information, the updates are transmitting instantly. Hence, that the routing information may be update either event driven or periodic. DSDV protocols require each mobile node to announce its possess routing table to its present neighbors in the network. The advertisement is completed either by broadcasting or multicasting. By the advertisements, the neighboring nodes can know regarding any change that has occurred in the network due to the actions of nodes. The routing update might be sent in two way: one is called a „full dump‟ and the another is called „incremental.‟ in full dump, the whole routing tables are sent to neighbors, where as in incremental renew, only the entry that they require changes are sent [6].

ii) Wireless Routing Protocol (WRP):

WRP [15] belong to common class of the path-finding algorithms [14, 16, 17], definite as situate of the distributed shortest path algorithms that determine the paths using information about the length and the second-to-last hop shortest path to every destination. WRP reduces the number of cases in which a temporary routing loop can occur. For the routing purpose, each node should maintain four things:

1. Link-cost table
2. Distance table
3. Routing table
4. Message retransmission list (MRL).

WRP use periodic updates of transmit the message to the neighbors node. Update message of the nodes in response list (which has be formed by using MRL) be supposed to send acknowledgments. Nodes in the list of response are supposed to send an idle Hello message to ensure connectivity still its unchanged from the last update. A node can make a decision whether its routing table to update after receiving an update message from a neighbor and always it looks for a better path by using the new information. Its relay backs that the information to the original nodes when the node get a better path, therefore they can be updating their tables. The original nodes update its MRL after getting the acknowledgment. Therefore, each time the constancy of the information of routing is checked by every node in this protocol, which help

to remove the routing loops and always tries to find out the greatest solution for routing in the network [6].

iii) Cluster Gateway Switch Routing Protocol (CGSR):

CGSR [18] consider a clustered wireless mobile network as a substitute of a „flat" network. For the network structuring into separate groups but interconnected, cluster heads are selected by using cluster head selection algorithm. These routing protocols attain a distributed processing mechanism by forming the several clusters in the network. Still, disadvantage of this protocol is to, frequent change or cluster selection heads may affect the routing performance and it may be resource hungry. CGSR use the DSDV protocol as essential routing scheme and, therefore, it has the similar overhead as DSDV. However, it changes the DSDV by using hierarchical cluster-head-to-gateway routing method to traffic of the route from source to the destination. Gateway nodes are the nodes with in communication ranges of two heads or more heads of the cluster. ***First, a packet send to its cluster head*** by a node, and then from the ***cluster head to a gateway the packet is send*** to another cluster head, and until then the cluster head destination node is arrived. Then the packet is transmitting from the own cluster head to the destination [6].

Reactive Routing Protocols

Reactive routing protocols are called as ***ondemand routing protocols***. In this routing protocol is exposed when its needed nodes start route detection on demand basis. Source node observes the available routes of the route cache to destination from the source if the route is not available then it initiate route discovery process. Source nodes consult the available route of its route cache to destination from source otherwise if route is not present then it initiates the route discovery. The source node, in the packet, includes the destination address of the node as well address of the intermediate nodes to the destination.

Route maintenance: Due to the dynamic topology, the network cases of route failure between nodes happen because of the link breakage and that, so the maintenance of route is done. Reactive protocols contain acknowledgement mechanism because of which maintenance of route is achievable. Due to route discovery mechanism, the reactive protocol adds latency to network. For each intermediate node involved to add latency in route discovery process. These protocols reduce the routing overhead however at the cost of latency increased in the network. Therefore, in these situation protocols are suitable, where the low down routing overhead is necessary. There are various familiar reactive routing protocols there in MANET for **example TORA, DSR, AODV and LMR** [6].

i) Dynamic Source Routing (DSR): Dynamic Source Routing based on source route method in reactive protocol [9]. In DSR, the protocol is base on the algorithm (link state algorithm) in which source begins with route discovery ondemand basis. The sender find out the route from the starting place to the target and it's containing the address of intermediate nodes to route record in the packets. ***DSR was intended to multi hop networks*** with small Diameters. DSR (Dynamic Source Routing) is a beaconless protocol in which no HELLO messages are swap between nodes to notifying them of their neighbors in the network [2].

ii) Ad Hoc On-Demand Distance Vector Routing (AODV) [10]: AODV is fundamentally an enhancement of DSDV. But, in this routing is a one of the reactive routing protocol instead of proactive. It reduces number of broadcasts by create a routes base on demand, which it is not in case for DSDV. When any source node needs to fire a packet to destination node, then it broadcasts route (RREQ) request packet. The neighboring nodes broadcast packet to their neighbor's nodes and broadcasting process continue until the packet reached the destination. During the route request forwarding process, intermediate nodes records address of neighbor when it's received first copy of broadcast packet. These records are stored in corresponding route tables, which helps to establish a reverse path. If later received the additional copy of same route (RREQ) request, these packets are discarded. These replies are sent by using reverse path. For the route maintenance, can restart a route discovery process while a source node moves. If any possible intermediate node moves inside a particular route, neighbor of the floated node can detect the failure link and send a failure link notification to their corresponding upstream neighbor. This process continues till the link failure notification information reached the source node. Based on the received information, the source may make a decision to reinitiate the route discovery phase [6].

iii) Associativity-Based Routing (ABR): ABR [11] protocol describe a newest kind of routing metric association degree of stability for the mobile adhoc networks. In these routing protocol, based on degree of the association constancy of mobile nodes, that the route is selected. Each node occasionally generate beacon to broadcast its existence. Based up on received the beacon message, the neighbor node update its corresponding associativity table. For every received beacon, the receiving node associativity tick with the beacon node is increased better than before. If high (top) value of associativity ticks for any particular beacon node then node is relatively static. Associativity tick is reset while any neighboring node moves out of the neighborhood of any other node [6].

iv) Signal Stability–Based Adaptive Routing Protocol (SSA): SSA [19] protocol focuses on attain the most stable routes throughout an adhoc network. The protocol performs on demand route discovery based on signal strength and location stability. Based upon the signal strength, these adaptive routing protocols identify the strong and weak channels in the network. SSA can be alienated into two helpful protocols: One is Static Routing Protocol and another one is Dynamic Routing Protocol. DRP using two tables: Routing Table and Signal Stability Table. SST records the corresponding signal strengths of neighboring nodes get by using periodic beacons from the every neighboring node link layer. This signal strength is recorded at the same time as strong or weak. DRP can receive all transmission and, after processing, and it passes all those to that SRP. SRP passes the packet to the node's upper layer of the stack if it is the destination node. Otherwise, it looks for destination in the route-table and forwards the

request packet to the neighbors. In the corresponding destination if find the route table has no entry, it's initiate the finding process of route. By using the strong channels, Route-request packet is forward to the neighbors. The destination, after getting the request, decide the first incoming request packet and then sends backward the reply. The DRP reverse the elected route and propel the route-reply message send back to the originator of route request. DRPs of the nodes along with the path keep informed to their route tables accordingly. If in the case of link failure, then the intermediate nodes sent an error message to the source indicating which channel has failed. The source in turn sends a remove message for alert the all nodes about the broken link and starts a new route-search process to discover a new path to the destination [6].

v) Temporarily Ordered Routing Algorithm (TORA) [20]: TORA is type of reactive routing with a few proactive enhancements wherever the links between nodes are established and generating a (DAG) Directed Acyclic Graph of the route from the starting place node to the end. This protocol uses a „„link reversal"" model in route discovery. Route discovery queries are broadcast and propagate throughout the network until it's reached the destination or a node that has such information about how to reach the destination node. TORA define a parameter, term height. The height is to measure the distance of the responding node"s distance up to required destination node. In the route discovery phase, corresponding parameter is return to the querying node.

III. CONCEPT OF TRUST

Trust Evaluation is implemented according to normal human psychology and subsequent behavior. In real world environments, when making decision, people normally trust the person they know personally and/or have known from someone else. They trust them till they are in a good relation with them. So how much trust a person can have on other is a relative term, if he is in communication with the person than it is supposed to be trustworthy otherwise not. The MANETs are generally architecture independent networks, the work is disseminated and required the mutual cooperation of all nodes in the network, and it's based up on the trust that these nodes would act as expected. However, taking each and every node to be trustworthy may not be always true, as some nodes may be compromised and behave selfishly or even maliciously to disrupt the network operation. Cryptographic Employing mechanisms are able to protect the integrity and correctness of the information being transmit in this system, but the mechanisms cannot be answer the question about the reliability of each party and forecast their behaviors. By evaluating the reliability of related parties, it is simple to take appropriate security measures and make appropriate decision on any security issues. Examine the wireless networks vulnerabilities and state that we must embrace the trust based mechanisms for increasing the security in MANETs.

Trust is extracted from social relationship. It is always established between two parties for a specific action. In particular, trusts in terms of one party faith the other to perform an action. For perform an action, trust might be referred as belief or reputation of one entity to other [19]. ***Trust in entities is based on the fact*** that the trusted entity should not act misbehavior in a particular situation. As no one can ever be absolutely sure of this fact, trust is solely dependent on the belief of the trustor. Trust may be calculated indirectly or directly depending upon the nature of protocol. While in most of the proposals it is calculated indirectly with the use certification method. In this case no direct trust can be establish between two nodes ***rather than nodes turn into dependent of the earlier calculations of other neighboring nodes.***

Definition and Calculation of Trust:

In case of trust again may confusions in the meaning of trust because in networks of wired whether the node is reliable or not is recognized by certification mechanism which is direct or an indirect method of trust calculation. On the basis ***reliability and non-maliciousness can be guild together.*** While marking a node as malicious or no reliable in MANETs is not easy due to dynamic changing topology. It is very tricky to incorporate certification mechanism in adhoc networks, because of the maliciousness and reliability has to be take care as separate problem. In wireless network reliability/security is a global issue while trust is a local issue of the routing and as in the ***existing trust based routing proposal*** authors have given a trust based model without specifying a ***security analysis*** of the proposed model against attacks. ***Therefore there is need to develop a trust based model*** considering security as an important parameter. Calculation of trust for an individual node or a path is done in several papers [20-24]. But it is not clearly mentioned in any of the referenced paper that how nodes can compute and announce the trust among the network. Although a detailed method is presented in [16] but again calculation of advertise trust is not clearly mentioned.

Design of Trust Model

The use of trust as the factor for design and development of secure systems is a new and upcoming method in the field of MANETs. The security features of trust model are able to directly applied to decrease the probability of node for being attack or being compromise on the network and therefore improves the routing [5]. A trust model should be able to fit in various scenarios of the system. In an open MANET, nodes may be open to leave or join the network anytime at will. Before they are join the network, some nodes may or may not previously know each other before they join the network. As well the direct interaction experience of the network, the pre-shared knowledge, if any, is too quite important for a node to apply trust evaluation and must taken into the account in a trust model. The application of Stationary Secure Database is to provide secured, trusted repository to get the information for mobile nodes regarding the most recent misuse signatures and to find the most recent patterns of normal user activity. The use of Stationary Secure Database to mine new difference rules is helpful to IDS for the three motives. In First, it would be fast and accomplished of mining rules as faster than slower, mobile nodes because of SSD be fixed. Secondly, the processing time used to mine the new rules will not take away from the processing time of the mobile nodes. And thirdly, the Stationary Secure Database is capable of containing a large amount of storage capacity to store great quantity of audit data collected from the nodes. It is very probable that the mobile nodes will not contain enough storage to store large amounts of the audit data, but by uploading the audit data to the SSD, no data is deleted because of lack of storage space.

Type of Trust Models

In this section, we describe the trust models that suitable for application to MANET based on the concept of trustworthiness of peer nodes.

i) Distributed Public-Key Model

The Distributed Public-Key Model is based up on the threshold cryptography to distribute the private key over a number of servers of the Certification Authority [25]. An (n, t+1) scheme allows any t+1 servers out of total of n servers to combine their partial keys to create the complete secret key. Similarly, it does ***require that at least t+1 server*** have to be compromise to ***obtain the secret key***. These schemes are quite robust but have a number of factors that's limit the application to be pure adhoc networks. Primarily it's require a distributed central authority and an extensive pre-configuration of servers and, secondly the t+1 server might not be accessible to any node desiring authentication and finally asymmetric cryptographic operations are well-known to drain precious node batteries.

ii) **Resurrecting Duckling Model**

Resurrecting Duckling Model makes use of the hierarchical graph of master-slave relationships [26]. The slave (duckling) considered the first nodes that send it a secret key through a secure channel as its master (mother duck). The slave always obeys the master and gets all instructions and access control lists from its master. The slave further becomes a master to other devices with whom it can share a secret key through secure means. This master-slave bond can only be broken either by a master, a timeout or an event, after which the slave is no longer bonded and looks for another master. This model is most appropriate security in large-scale dumb sensor nodes wherever pre-configuration have to be avoided. As this model uses a hierarchical security chain it is not appropriate for application to ad-hoc networks.

iii) **Friend Recommendation Model**

The Friend Recommendation Model [27] is based on a trust chain between nodes in network to create trusted community. A pair of the friend nodes, before join the network, which assumed to have a mutual trust between them, is capable of create a security association between them to participate in MANET operations. The friendship mechanisms are able to ***speed up creation process of trusted community*** in network**.** Each node needs to meet and establish mutual trust with other nodes, which requires a lot of time and effort. In friend recommendation if node A wishes to have a trust relation with node B, node A wants to have at least one node in node B's friend list, node C, to authenticate its identity. If no node in B's friend list that have to physically meet node A before, recommended request will then be forwarded to next hop in a same manner. When a node that knows the identity of node A is found, the information is sent back to node B to complete the authentication process. However, if no one in the chain knows about node A's identity, node A then must name at least one node, node D, that it has met before to act as a reference node. Node B then will do same process to the authenticate node D's identity. If the identity of node D is known by any node B's friends in the chain list, the identity of node A then is considered authenticated.

iv) **Localized Trust Model**

The localized trust model [28] is based on trustworthiness of node by their own local community. In localized trust model, if any k maintains the trusted entities, an entity is trusted, so it's contained by certain time period with Tcert. Those k entities are naturally among the entities one hop neighbors. If a node is trusted by it is local community, then it is worldwide recognized as a trusted node or else, a locally distrusted entity is considered as unreliable in entire network. K and T cert are two significant parameters with Tcert, typify the time-varying feature of a trust relationship. The options for setting k are to set k as a worldwide fixed parameter that is respected by each entity in the system. For these case, k proceeds as system-wide trust threshold method. The k parameter is tuned according to density of the network and the system robustness requirements. If a node could not find k neighbors in certain location, it may roam to meet more nodes or wait for new nodes to move in. They developed a scalable share update scheme, optimization techniques that greatly enhance the efficiency and robustness of their algorithms and protocols. As this model has scalability feature architecture to facilitate practical deployment in a potentially large scale network with dynamic node membership it is suitable for application to ad hoc networks.

v) **Bayesian Network-Based Model**

The Bayesian Network-Based Model [29] is focused on trust and reputation of node in the network based on a Bayesian Network Model. A trust value of one node is more valuable to other nodes. A node build two type of trust in the another node, trust in competence in providing service and trust in reliability in providing recommendation about others node. Since nodes are heterogeneous, they judge other's node behavior by different criteria. One node can trust another node if their criteria are similar. Even though both node tell the truth, they not trust each other if their norm are different. A Bayesian network is relationship network that uses statistic methods to represent probability relationships between different elements. Every Bayesian network have root node T, which will have two values, ***"unsatisfying" and "satisfying", denoted by 0 and 1, respectively***. Each node called leaf node is related with conditional probability (CP) table. Once getting nodes' CP tables in a Bayesian network, a node can compute the probabilities that the corresponding root node is trustworthy in different aspects by using Bayes rules. Nodes can set various conditions according to their needs. With the Bayesian networks, nodes can deduce trust in the different feature that they require from the corresponding probabilities. That will save nodes much effort in building each trust separately, or developing new trust when conditions change. After each interaction, nodes update their Bayesian networks respectively. As this model provided an easy way to present a complex and correlative relationship of nodes, ***this model is suitable in both small and large size MANET.***

Trust and its properties in MANET

Trust, is a directional connection between two elements and assumes a noteworthy part in building a relationship between nodes in a system [3]. In trust the nodes will implement the principles characterized in the network by administrator and that the participation of the group will be represented by

obviously characterized imperatives. Trust is characterized as a firm faith in the functionality of a node to act reliably, safely, and dependably inside a predefined setting. Trusted framework is characterized as a substance whose security components are segregated from unapproved clients; the framework can be distinguished, content controlled and secure, and overseen by an able specialist. As for unarranged systems, this basically suggests each sharing node has the important security parts that offer the security administrations which can't be superseded in an unapproved way. Every node would then be able to be trusted to perform organizing related administrations as well as end framework administrations. For a node to be trusted node it has to follow the below characteristics.

- Must be active in the network for a particular period of time.
- Must not misbehave i.e., not causing any packet failure or data modification or illegal actions.
- Must not leave the network without handling its data to its neighbors.
- Must be active in routing table updates and packet forwarding without any delay.

Furthermore, trust administration has various importances in a few higher subjective procedures like interruption recognition, validation; get to administration, ***key administration for powerful routing.*** The dynamic nature and qualities of MANETs end in vulnerability and wholeness of the trust.

IV. *Security Attacks in MANET*

Attacks in the ad-hoc network are of two categories: i) passive attack and ii) active attack. Passive attack occurs which disrupt the operation of the network that means it does not modify the content information. This kind of attack is less injurious but more composite to find as it does get in the way with operation. ***To overcome this some powerful encryption technique*** can be used for encrypt the data while transmission. In contrast, the active attack is the one, in which vigorously modifies, change and demolish the data of being transmit, thus troublemaking the information exchange. Active attack can be categorized into e***xternal attack and internal attacks***. An external attack comes from the node which does belong to the part of the network. This can be prohibited by some security mechanism such as ***firewall and encryption***. Internal attacks will bring out from within the network. These attacks are more severe and difficult to detect. There are many different types of adhoc network among which some of the frequent attacks are: Denial of Service, Black hole attack, Wormhole attack, Byzantine attack, Resource consumption attack.

IV.CONCLUSION

Security mechanism is important in order to ***ensure the secure communication between end to end users*** in mobile adhoc networks. Passive attacks like timing attacks can be avoided with the Notify and Go mechanism at the source and destination zone broadcasting at the destination. Active attacks like Black hole attacks in the routes can be observed and selected a new route without attacker by the Homomorphism Message Authentication scheme. ***In this paper, routing protocols for MANET, which are generally categorized as proactive and reactive protocols.*** The attempt has been prepared on the comparative study of Proactive and Reactive routing protocols has been presented. Due to its open nature it is difficult to maintain the trust and resource constraints; hence the ***trust is the desired challenge for best performance***. This survey analyses all the possible trust management for secure routing with necessary protocols. ***There are various inadequacies in different routing protocols*** and it is complicated to make a decision routing protocol for different situations as there is tradeoff between various protocols.

V.REFERENCES

[1]. X. Li, M.R. Lyu & J. Liu, ”A trust model based routing protocol for secure ad hoc networks” in Proc., IEEE aerospace conference , vol. 2, pp. 1286–1295, March 2004.

[2]. A.A. Pirzada, C. McDonald, Trust establishment in pure ad-hoc networks, in: 1465 Wireless Personal Communications, vol. 37, pp. 139–168, 2006.

[3]. Kari Sentz,”Combination of Evidence in DempsterShafer Theory”, Computer and Information Science journal ,vol. 853, pp.37- 72, 2002.

[4]. M.R.Ebenezar jebarani1and T.Jayanthy ,”An Analysis of Various Parameters in Wireless Sensor Networks using Adaptive FEC Technique” International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.3, September 2010.

[5]. Dewan, P. and P. Dasgupta. Trusting Routers and Relays in Ad hoc Networks. in Proceed-ings of First International Workshop on Wireless Security and Privacy (WiSr 2003) in con- junction with IEEE 2003 International Conference on Parallel Processing Workshops (ICPP). 2003. Kahosiung, Taiwan: IEEE.

[6]. M. G. Zapata, Secure Ad Hoc On-Demand Distance Vector (SAODV) Routing," ACM Mobile Computing and Communication Review (MC2R), Vol. 6, No. 3, pp. 106-107, July 2002. [2] Y. Hu, D. B. Johnson, and A. Perrig, SEAD: Secure Eficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02), pp. 3-13, June 2002.

[7]. Y. Hu, A. Perrig, and D. B. Johnson, Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks," Proceedings of the 8th Annual International Conference on Mobile Computing and Networking (MobiCom'02), pp. 12-23, September 2002. [4] Perrig, R. Canetti, D. Tygar and D. Song, \The TESLA Broadcast Authentication Protocol," RSA CryptoBytes, 5 (Summer), 2002.

[8]. Robinpreet Kaur & Mritunjay Kumar Rai, A Novel Review on Routing Protocols in MANETs, Undergraduate Academic Research Journal (UARJ), ISSN : 2278 – 1129, Volume-1, Issue-1, 2012.

[9]. C K Toh, Ad Hoc Mobile Wireless Networks, Prentice Hall Publishers , 2002.

[10]. G.Vijaya Kumar , Y.Vasudeva Reddyr , Dr.M.Nagendra , Current Research Work on Routing Protocols for MANET: A Literature Survey, International Journal on Computer Science and Engineering Vol. 02, No. 03, 2010, 706-713.

[11]. Tarek Sheltami and Hussein Mouftah “Comparative study of on demand and Cluster Based Routing

protocols in MANETs", IEEE conference, pp. 291-295, 2003.
[12]. Elizabeth M. Royer"A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks" University of California, Santa Barbara Chai-Keong Toh, Georgia Institute of Technology, IEEE Personal Communications, pp. 46-55, April 1999.
[13]. Krishna Gorantala , "Routing Protocols in Mobile Ad-hoc Networks", A Master' thesis in computer science, pp-1- 36, 2006.
[14]. Perkins CE, Bhagwat P (1994) Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. Proceedings of ACM SIGCOMM 1994:234–244.
[15]. Cheng C, Riley R, Kumar SPR, Garcia-Luna-Aceves JJ (1989) A Loop Free Extended Bellman-Ford Routing Protocol Without Bouncing Effect. ACM SIGCOMM Computer Communications Review, Volume 19, Issue 4:224– 236.
[16]. Humblet PA (1991) Another Adaptive Distributed Shortest-Path Algorithm. IEEE Transactions on Communications, Volume 39, Issue 6:995–1003.
[17]. Rajagopalan B, Faiman M (1991) A Responsive Distributed Shortest- Path Routing Algorithm Within Autonomous Systems. Journal of Internetworking Research and Experiment, Volume 2, Issue 1:51–69 Parvathavarthini et al., International Journal of Advanced Research in Computer Science and Software Engg 3(2), February - 2013, pp. 251-259 © 2013, IJARCSSE All Rights Reserved Page | 259.
[18]. Chiang C-C, Wu H-K, Liu W, Gerla M (1997) Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel. Proceedings of IEEE SICON: 197–211.
[19]. D. H. McKnight and N. L. Chervany, "The meanings of Trust," MISRC Working Paper Series, Technical Report 94-04, Arlson School of Management, University of Minnesota, 1996.
[20]. Z. Ye., S. V. Krishnamurthy and S. K. Tripathi, "A Framework for Reliable Routing in Mobile Ad Hoc Networks". In the Proceedings of 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM) 2003, 270-280.
[21]. M. Virendra, M. Jadliwala, M. Chandrasekaran, S. Upadhyaya, "Quantifying Trust in Ad-Hoc Networks". In the Proceedings of IEEE international Conference on Integration of Knowledge Intensive MultiAgent systems (KIMAS) 2005, 65-71.
[22]. Z. Liu, A. W. Joy and R. A. Thompson, "A Dynamic Trust Model for Mobile Ad Hoc Networks". In the Proceedings of 10th IEEE international workshop on Future Trends of Distributed Computing Systems (FTDCS) 2004, 80-85.
[23]. L. Eschenuer, V. D. Gligor, J. Baras, "On Trust Establishment in Mobile Ad-Hoc Networks". Security Protocols: 10th International Workshop, 2002, 47-62.
[24]. A. A. Pirzada and C. McDonald, "Establishing Trust in Pure Ad-hoc Networks". In the Proceedings of the 27th Australasian conference on Computer Science 2004, 47-54.
[25]. L. Zhou and Z. J. Haas, "Securing ad hoc networks," IEEE Network Magazine, 1999.
[26]. F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks," Security Protocols: 7th International Workshop, Cambridge, 2000.
[27]. S. A. Razak, S. Furnell, N. Clarke, and P. Brooke, "Building a Trusted Community for Mobile Ad Hoc Networks Using Friend Recommendation," Springer, 2007.
[28]. J. Zhung, H. Luo, and P. Zerfos, Selfsecuring ad hoc wireless networks: ISCC, 2002.
[29]. Y. Wang and J. Vassileva, "Bayesian network-based trust model," Proceedings of the IEEE/WIC International Conference on Web Intelligence (WI'03), 2003.

ABOUT THE AUTHORS

K.Ranjithsingh received his **M.Phil** Degree from Periyar University, Salem in the year 2008. He has received his **M.Sc.,** Degree from Madurai Kamaraj University, Madurai in the year 2002.He is working as Assistant Professor at **PGP** College of Arts & Science, Namakkal. He has **16** years of experience in Academic Field. He is pursuing his Ph.D. (Part-Time) Degree at Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India. His areas of interest include Mobile Computing, Cryptography and Network Security.

Dr.D.Maruthanayagam received his **Ph.D** Degree from Manonmaniam Sundaranar University, Tirunelveli in the year 2014. He received his **M.Phil** Degree from Bharathidasan University, Trichy in the year 2005. He received his **M.C.A** Degree from Madras University, Chennai in the year 2000. He is working as **HOD Cum Professor**, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India. He has above **18 years** of experience in academic field. He has published **5 books**, more than **35 papers** in International Journals and **30 papers** in National & International Conferences so far. His areas of interest include Computer Networks, Grid Computing, Cloud Computing and Mobile Computing.