TRUST BASED SECURITY IN MANET

Pooja Pilankar[1], Puja Padiya[2]

[1]*Department of Computer Engineering, Ramrao Adik Institute of Technology, Navi Mumbai, India*
pilankar.pooja.13co2018@gmail.com
[2]*Department of Computer Engineering, Ramrao Adik Institute of Technology, Navi Mumbai, India*
puja.padiya@gmail.com

Abstract

Mobile ad-hoc network (MANET) is one of the most propitious area in research and development of wireless network. Popularity of mobile device and wireless networks significantly increased over the past years. MANET has no centralized control to handle the network, so this may cause to fails the functioning. This characteristic force a component node to be careful when communicating with other nodes as the behavior of nodes change with time and environmental conditions, so the security issues may arise like impersonation etc. Therefore behavior of node should consider improving the security of MANET. This is mostly important in big network where heterogeneous nodes are the parts of network for e.g. tactical and social network. The behavior of node is shown in the form of numerical value called as trust. Trust is calculated and aggregated and shared among network. Every node's generated trust is on the basis of serious study, others node opinion, and previous interaction and their own policy. In this report, we have analyzed different proposed trust based mechanism and trust evaluation based security solution. These techniques are proposed to make trust security solutions more effective.

Keywords: *Manet, Trust, Smrti, Maturity-Based Model, Rep, Truism*

----------***----------

I. INTRODUCTION

Mobile Ad hoc Networks MANETs is a wireless communication technology. This allows people to communicate. It does not have a fixed infrastructure as the users are continuously moving. Ad hoc network handles the network by own i.e. to set up a network etc. Each node is having the ability to build a network by finding the node to communicate and share the data via radio waves. MANETs have several significant characteristics and challenges [4] for e.g. Dynamic topology, Distributed operation, Light-weighted Terminal etc. Mobile ad hoc networks are vulnerable to security problems than the wired networks, there are different types of security solutions are used like cryptography and IDS etc. to avoids the security attacks but the malicious attackers block or modify the data traffic traversing them by refusing the cooperation and violates authenticity and confidentiality of network so these type of nodes are difficult to identify as they are act as a validate user, so we use a concept of TRUST to solve such problems, trust is calculated on the basis of reputation, direct, indirect trust (recommendation). In which we calculate the degree of dependence on other nodes by which we then decide whether to communicate with that node or not.

MENET have certain security issues which might not be resolved by other security mechanism because of some problem. Trust management is necessary because predetermined behavior of node can avoid many further malicious communications and let the trustworthy nodes communicate smoothly.

In following report we have discussed some trust calculation techniques and analyze them on the basis of different parameters. So this paper is organized as related work is described in section 2 then followed by Trust Models are discussed in subsections of section 3 then those models are analyzed in section 4. After that the paper is concluded and mentions some future work in section 5.

II. RELATED WORK

There exist some related trust based techniques. In [9] trust evaluation mechanism for MANETs is shown as decentralized. Here trust calculation is shown as a generalized shortest path problem on a weighted directed graph. In this mechanism vertices represent nodes and weighted edges shows the opinions that one node has about the other node in the edge direction. Recommendations on the basis of others opinion and their own policies are given as a value to edges. Each recommendation has two values trust and confidence value. First is node's own trust calculation and other is preciseness of trust value allotment. In such a graph, an indirect trust relation without previous immediate experience is established by the theory of semirings. In [7] Pervasive Trust Model (PTM) the trust is formed by using two information sources i.e. previous knowledge (direct) and recommendation (indirect) then they have evaluated trust in two separate spaces i.e. belief space which is formed from previous knowledge and evidence space which formed by past and current experience, and they have used Pervasive Recommendation Protocol (PRP) only to exchange trust values. In [8] Secure and Objective Reputation-based Incentive (SORI). SORI scheme takes concept of reputation rating which based on packet forwarding ratio of a node. It consists of three components, 1.Neighbors Monitoring: - This component used to collect information of neighboring node about the behavior of

packet forwarding. 2. Reputation Propagation: - It providing information sharing of other nodes with its neighbor. 3. Punishment: - It includes the process of removing the packet from the network. This scheme can't differentiate between the selfish and malicious node

III. TRUST BASED SECURITY MODELS

In this section we will study three different Trust based security models in detail. All the models are focused on calculation of trust.

A. Secure MANET routing Trust Intrigue (SMRTI):

This Model is used in Trust Enhanced Security Architecture for MANET [3]. Here Model performs the function of finding the trustworthy node, packets as well as routes. Also it allows the architecture to take precise security decisions. Here we will see different decisions of SMRTI. First decision is toeither accept or reject a route from a route discovery. Second is to ignore or record a route from a forwarded packet. Third is to discard or forward a packet. Fourth is to forward a packet for a former hop. Fifth is to send a packet to adjacent hop. Sixth refresh or cancel the key for a node. Finallychoose route for the communication.

Trust Evaluation

A trust evaluation for a node, a packet, and a route, consider each nodes direct and recommended trust are set to some threshold value ( ). A positive trust evaluation for a node (packet or route) depends on whether the computed trustworthiness for the node (or packet or route) is at least ' '.They have set highest priority for the direct trust compared to the recommended trust because personal experiences take higher precedence over the recommendations received from others.

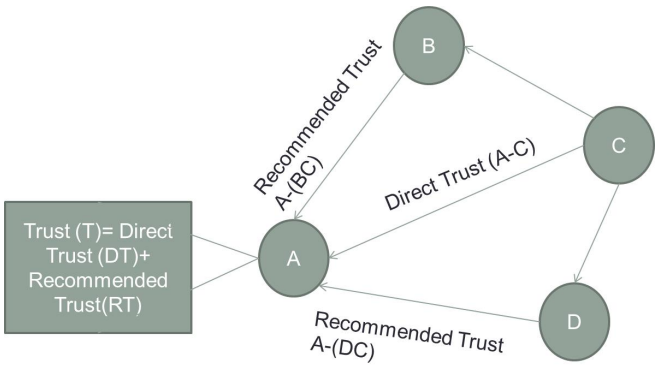

Fig. 1: Trust Evaluation

1) Direct Trust: Direct Trust is a trust calculated for one node on another node. It is depend on evidence found during the communication with other node. On that basis the evidence are categories as positive events or negative events.Positive events are route request, route reply, route error or data flow. On the other hand the negative events are ofsuspicious behavior like flooding, packet droppingand modification of route sequence number, addition or deletion of routes and fabrication. Here trust is calculated in the certain range of -1 to +1 which gives limited possible Tvalue because trust is continuously calculated in MANET.

2) Recommended Trust: In SMRTI the node that gives recommendation about particular node is called as recommender. The nodes which are recommended is called as a recommendee. Here recommendations are obtain from the route packet. Then SMRTI identify a nodes willingness to send further or dispose packet. SMRTI derives recommendation only one time forcommunication. So, that it cannot get influenced by malicious routes. For e.g.In Figure 1 Node B(recommender)provides recommendation to node C about node A(recommendee). This process will be followed by all nodes in the trust network and store the Tvalue of previous node in the route on the data flow sequence. While calculating recommended trust the positive and negative events are also considered to avoid the presence of malicious node in the network.

In this model, it prevents a node's false opinion so that it overcomes the issue of recommender's bias and also prevents the nodes from other two issues like honest elicitation and free riding behavior.

B. Maturity-Based model:

In this section we will study Maturity based model [3]. This model is based on human tendency like humansmaintain a trust relationship on their neighbors. Same here also this model works on same concept. Here one protocol also introduces to share the recommendation about other node. Main concept is applied here is Relationship Maturity, Which improve the effectiveness of model.

1) Trust Model: Here the trust model works on calculation of trust obtain from its neighbor. Basically every node gives some random trust level to their every neighbor. Trust model gives the trust value which shows the previous behavior of node with their specific neighbor. This information will be considered as a future behavior of neighbor. It will also include the recommendation of others node. The recommendation is calculated because lack of monitoring capability which happens due to resource unavailability.

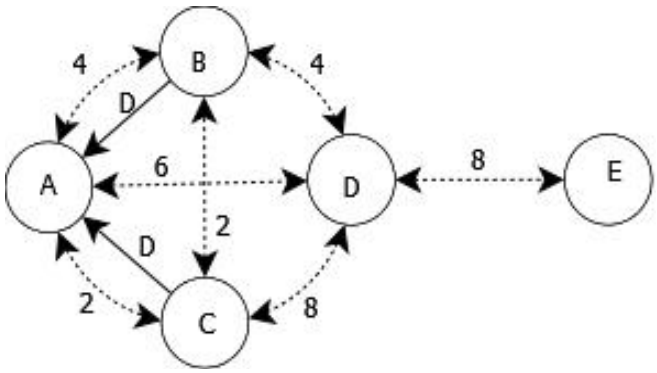

Fig. 2: Example: Node A receives recommendations about node D [3]

Recommendation from neighbors is used to obtain precise trust level. So, on such basis the relationship maturity concept is work by getting the age factor of trust relationship. Age factor meaning the time spent for communication with particular node. So on age factor the preference is set to long term relationship with particular neighbor than short term. Figure 2dotted arrow shows neighbors and number indicates time spent with that node. They are also knows as relationship maturity parameter. A solid arrow shows a recommendation and pointed towards the letter indicates target node. In this recommendation influence same neighbors of different node. Node D is a common neighbor of node A, B, and C. Node B and C send their recommendation of D to node A. Now node A will choose the recommendation received by C. Because it has a higher number which show it has spent more time withD than B. Here recommendation receive from D about E will be ignored because E is not a neighbor of A.

Each node forwards the trust value to their neighbor. Here the trust level is ranging from 0 to 1. Where 0 indicates less trustworthy node and 1 indicates more trustworthy node. Thetrust node is divided into two parts Learning plan and Trust plan. The Learning Plan performs the function of gathering and converting information like behavior of each neighbor into knowledge. It is based on 3 components as shown in Figure 3.The Behavior Monitor observes neighbors and collects information about their behavior. It should observe others activities and gives them to classifier and also tell to the Recommendation Manager if new neighbor is added.

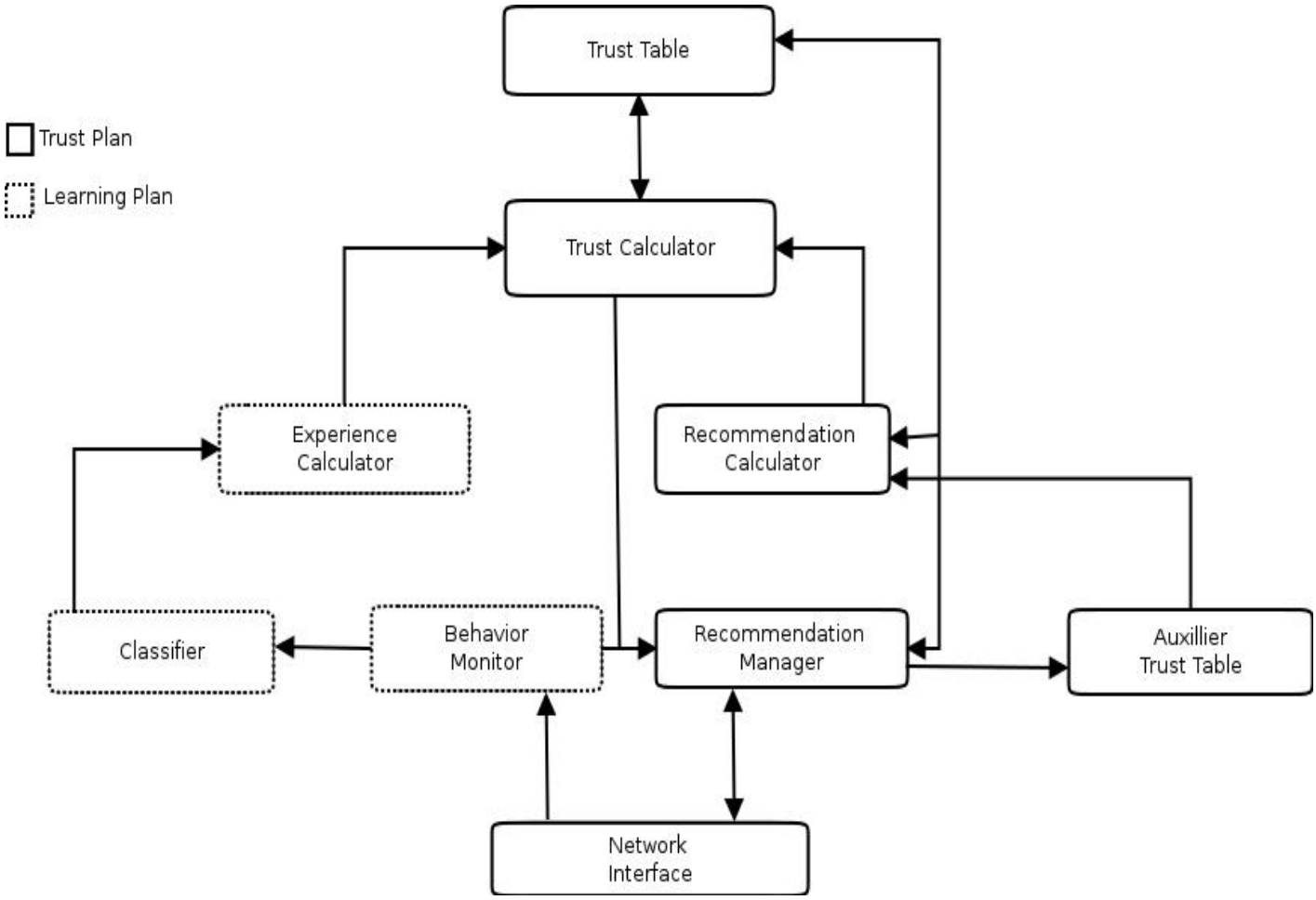

Fig. 3: Trust system component [15]

The classifier is a component for the information collected by the monitor. Classifier then checks the quality of information on the basis of previous data. After that it forwards its decision to the Experience Calculator. Then it derives half trust value based on obtained information from classifier.

Trust plan defines how to evaluate the trust level of each neighbor. It is done by using information provided by learning plan. It also exchanged information with its neighbors. It is based on five main components as displayed in fig. 3. Every node should maintain Trust Table. It contains trust level of every node. Every entry belongs to certain time. So, as soon as the node is out of the range all the related entries should remove from the table. There is one more table which is not compulsory named as Auxiliary Trust Table (ATT). It contains multiple values for each trust level differs by spent time. This then shows the relationship maturity.

Recommendation Manager is used to send, Receive and store the recommendation. The communication between Network Interface and Recommendation Manager is done with the help of REP. Recommendation Manager perform two function. Initially recommendation saved in the Auxiliary Trust Table(ATT). Later it sends to the recommendation calculator component. It then derive all recommendation for requested neighbor. Then the computed is given to the Trust calculator. Then it derive the trust level on the basis of trust value obtain from Experience Calculator and Recommended Calculator. The trust calculator indicates the Recommendation Manager the necessity of sending trust recommendation advertisement.

2) The Recommendation Exchange Protocol (REP):
The REP works with Recommender Manager. This protocol permits the nodes to share their recommendation with their neighbors so that all the data are transferred in one hop. The protocol set TTL block to 1 while broadcasting message with IP. It contains 3 types of messages. 1. Trust Request (TREQ) 2. Trust Reply (TREP) and 3. Trust Advertisement (TA) messages. When the node connects for the first time, it sends A TREQ to its entire neighbor with IP address of new neighbor as a destination or required node. Then neighbor will receive that request and check for the target node as their neighbor then that will reply to that request as containing recommendation about target node. It waits for certain time t_{REP} to abstained collision. The node also maintains the TREP threshold. The threshold is decided by considering the trust level of re-questing node to limit the TREQ. It will minimize the effect of malicious node. Prior to forward TREQ messages, Node observe for certain time t_{REQ}, here it collects maximum no of new neighbors. After t_{REQ} it will send the single TREQ which contain multiple node's IP. After that requesting node will wait for certain time out period in which it only accepts the recommendation. After that it will discard the recommendation. It also checks for the change in trust level. If it found such cases it notifies to the entire neighbor so that it prevent all the long process of getting recommendation.
In this way the Maturity Model works on this REP Protocol.

C. Trust Based Information Sharing Model (TRUISM):

In this model trust is one of the attribute of node. It represents the trustworthiness of a node in network it is obtain while the communication takes place between two nodes at a particular time. TRUISM also works on trustwillingness properties.

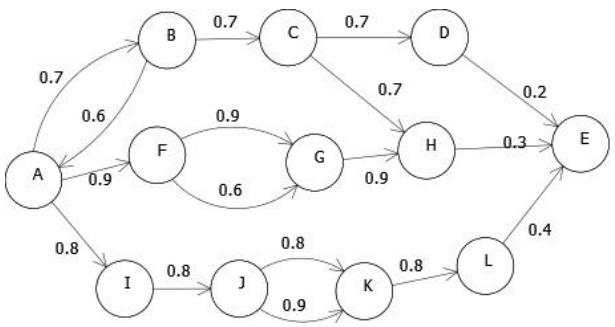

Fig. 4: A general trust network [1].

In which a node wish to trust to share the information. Figure 4 shows a general trust network in MANET. In this the nodes are shown by circle and nodes are interconnected by an arrow and trust on node is shown by arrow's pointer for e.g. the arrow from A to B show the trust of A on B. Therefore A and node B can communicate. The basic properties, sets, and functions of TRUISM are described below.

1) Properties: TRUISM has the following basic properties of a trust model:

Terminology: Service Provider node –n_{sp}, Service Requester node – n_{sr}, Time t, Service Context c_i, Trust Value -Tvalue. Distance Based Aging - DBA. Direct Trusted neighbor - DTN, Connected Neighbor - CN,

Context-dependent:Trust of n_{sp} onn_{sr} to share information in $c_i$at t is not compulsorily same for other c_i

Time based aging: If there is no communication between n_{sp} and n_{sr} then as the time passes the Tvalue get reduces.

DBA:Recommendations comes from nearer nodes are receiving more weight over nodes which are farther away.

DTN: If some node n_{sp} trusts a node n_{sr}. Then$n_{sr}$is n_{sp}'s DTN. Figure 4 show that I, B, and F are DTNs of A.

CN: If n_{sp} trusts n_{sr} n_{sp}isn_{sr}'s CN. Hence, CN is fundamentally inverted of DTN. In figure 4 A is a CN of nodes I, B, and F.

2) Recommendation Trust Model:

Recommendation Trust (Rec) is the opinion about a node who wants to communicate. The node gets this opinion from its DTNs. So, only personal interaction is consider to calculate actual trustworthiness but sometimes recommendation can affect trust evaluation for e.g. the first communication with a node without any past communication. In TRUISM rec is consider from n_{sr} to n_{sp}. In which it may traverse multiple hops contains no of intermediate node.

3) Recommendation Trust Development:

In this model when some node n_{sr} wants to communicate to some node n_{sp} then it sends the request to its CNs. Then these CNs will add their opinion about n_{sr} to the received request and forward it to their CNs. Now this will go on till the intended node i.e. n_{sp}. Here request comes from n_{sr} which will pass through multiple hops. DTN is exactly opposite to the CN. Here every time nodes receives the recommendation by their DTN. Therefore here the malicious nodes and their recommendations can be avoided. The equation for the calculation of recommendation trust is shown below.

$$REC_{nsp,ni}(n_{sr})=REC \text{ X } \delta \quad (1)$$

Where,

- Rec is recommendation Tvalue from ni from nsr
- $\delta = 1 - \frac{(1-Tnsp(ni,t))*\Psi}{10}$ Is the aging factor (path reliability based)
- ΨIs the hop length from nsp to nsr

nsp gets the recommendation from neighbor node or intermediate node i.e. ni about nsr at particular time t.δis the weighted element that fulfill the path reliability based aging property. Here, $Tnsp(ni,t)$ is the Tvalue of nsp for ni at t. The value of checks that the recommendation value comes from near nodes which are the node will have more weight than the nodes which are farther away. Nearer nodes means nodes with minimum distance and more Tvalues. The value shows the recommendation from nearer node i.e. with less distance and maximum Tvalue which have higher precedence than the node which are farther.

4) Recommendation Trust Progression Algorithm:

This algorithm implements two properties. The "path reliability based aging" and "buffering on the fly". In this trust is collected by sending request to their respective neighbor after that the neighbor will reply if they have the Tvalue stored about requested node. So basically two processes are performed first is to send the request for the recommendation to all neighbors. Second is after receiving request, reply the recommendation back. Here two algorithms are explained one is for recommendation request and other is for recommendation reply. The first algorithm applies to RReq packet propagation. When anmiddle node which is not the intended node receives RReq packet, it evaluate recommendation trust using algorithm. Where initially CNs of $n_{sr}$is identified and then these CNs will multicast their recommendation for n_{sr} to their CNs. If the node is not a CN of n_{sr}, then equation 1 derives recommendation which shows path reliability based aging. Another important variable is timer(t) which is used because every node has to wait for all helpful recommendations. Meanwhile it merges all the received recommendation trusts and saves the merged value. Thus storing process basically implements the 'buffering on the fly' property and finally it sends the recommended data to all its CNs. This ultimately reached to the service provider. Another algorithm is also required for Recommendation Response Progression. Here explained how n_{sp} will execute after receiving request. When n_{sp} receivesRReq packet it begin a timer. Similar to first algorithm here also consider recommendations from its DTNs. It also combines these recommendations and stores the combined value. Lastly n_{sp} reply true to show request is successfully received.

Critical Issues

Here are the issues which are resolved by the TRUISM are explained.

1) Buffering on-the-fly

While Recommendation process progression the intermediate node Tvalues which are received from their DTN are not only forwarded torequesting node but also stored in their respective DTNMapping table so that every time it doesn't have to ask Tvalue for the same node. This process
of storing the value while progression is called "buffering on the fly". Which says that as eachnode carries the Tvalue for their entire neighbor. The trust progression process is always two hop away from n_{sp} regardless of their initially distance. Thus value is always 2.

2) Path Reliability Based Aging

Here the nodes which located at minimum hop distance are considered as more trustworthy node. Sometime one node doesn't have alike Tvalueon two nodes. It happens even when nodes which are equidistant. Also the nodes are considered trustworthy on the basis of Tvalue they hold irrespective of their distance.

In this chapter we have thoroughly studied three different techniques. SMRTI, here it takes decisions of routing in MANET on the basis of direct trust and recommended trust. Next is Maturity Model, here the trust is based on previous individual experiences and on the recommendations of others using REP and last is TRUISM, in which multi hop recommendation trust management scheme is present and alsorecommendation routing protocol named buffering on the fly has been introduce to reduce the recommendation traffic; it also ensures a fastest and scalable trust based information.

IV. COMPARATIVE ANALYSIS

In trust exactly how trust is computed depends on the particular protocol. Techniques which are discussed above in table I are as follows SMRTI (Secure MANET Routing with Trust Intrigue) which takes the routing related decisions based on Direct and recommended trust, Maturity Model is human-based model which builds a trust relationship between nodes in an ad hoc network. The trust is based on previous individual experiences and on the recommendations of others, we take third method for comparison is TRUISM (Trust based Information Sharing Model) which implement time, path, distance based aging as a new feature. So these methods are differing by some features like trust models, context is use, goals, Design Consideration, advantages, disadvantages and their respective trust calculation methods etc. Ultimately all techniques are focused on calculation trust.

Table I: Comparison Of Different Trust Models

Parameters Trust based Paper	TEAM: Trust Enhanced Security Architecture for Mobile Ad hoc Networks [2]	Trust Management in Mobile Ad hoc Networks using a Scalable Maturity Based Model[15]	A Trust based Information sharing Model (TRUISM) in MANET in the presence of uncertainty[1]
Work in Environment	MANET	MANET (Single hop and multi hop)	MANE (multi hop)
Trust Model	SMRTI (Secure MANET Routing With Trust Intrigue)	Maturity Model	Recommendation Trust Model
Context in use	Based on Direct and Recommendation Trust	Based on recommendation aggregation and also neighbor sensing	Based on Direct and Recommendation Trust
Goal	Overcome Honest elicitation, Free Riding, Recommender's bias	Scalability of REP, reduce the number messages. Low resource consumption	To reduce the recommendation traffic, efficiently combine recommendations from multiple devices.
Design Consideration	System should take the decisions like Accept or reject route, Record or Ignore a route, To forward or discard a packet, etc.	System is based on Previous interaction and Opinion of neighbors	System is Context dependent, time based aging, Distance based aging, path reliability based aging
Advantage	does not require additional packets for recommendation	The recommendation aggregations and combining the recommendations with self measurement can increase the trust accuracy	Multiple recommendation, reduce traffic, successfully reflect uncertainty, It adapts human like behavior
Disadvantage	If malicious node increase the packet delivery ratio will decrease	Memory requirement to store the past value. This approach will be ineffective in spare networks	Extra time required for single recommendation. Difficult to propagate reco-mendation in opposite direction.

V. CONCLUSION

This paper reviews the trust calculation schemes used for securing Mobile Ad-hoc Network. In Literature Review wehave studied working of MANET, its Security threats and security solutions, we have chosen to study TRUST over other security solution. We also studied the basics of trust and its importance. If trust is shared among every node then we can easily avoid malicious nodes becoming a router. So this security method is useful to prevent the security threats. The security solution should be dynamic based on the changed trust relationship and therefore based on above concept of trust we have briefly explained some related trust models then we have explained three techniques. After detailed study of three techniques named as SMRTI, Maturity Model and TRUISM we compared them on the basis of some parameters.

Therefore we conclude that any of these discussed models can be used according to the security required and TRUISM is more efficient technique as it is based on recent study of trust management and it has some new concept like buffering-on-the-fly and path reliability based aging and also reduces the recommendation traffic in great volume. These features make Trust Based Information Sharing Model (TRUISM) more efficient than other models. In the future scope we can say that sometime there may be other reasons when node does not behave normally like low energy, congestion in the network, lossy links or may be destination has moved away etc. So such cases should also consider while using trust based security.

REFERENCES

[1] Bijon, Khalid Zaman, MdMunirulHaque and RagibHasan. "A trust based Information sharing model (TRUISM) in MANET in the presence of uncertainty." Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on. IEEE, 2014.

[2] Balakrishnan, Venkatesan and et al. "Team: Trust enhanced security architecture for mobile ad-hoc networks." Networks, 2007. ICON 2007. 15th IEEE International Conference on. IEEE, 2007.

[3] P. B. Velloso, R. P. Laufer, D. O. Cunha, O. C. M. B. Duarte and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model, IEEE Trans. Netw. Service Manag., Sep. 2010

[4] Semplay, Savita, RajniSobti, and VeenuMangat. "Review: Trust man-agement in MANETs." International Journal of Applied Engineering Research 7.11: 2012.

[5] Govindan, Kannan, and PrasantMohapatra. "Trust computations and trust dynamics in mobile adhoc networks: a survey." Communications Surveys and Tutorials, IEEE 14.2 279-298. 2012.

[6] England, Philip and et al. "A Survey of Trust Management in Mobile Ad-Hoc Networks." Proceedings of the 13th annual post graduate symposium on the

convergence of telecommunications, networking, and broadcasting, PGNET. 2012.
[7] Almenrez, Florina and et al. "PTM: A pervasive trust management model for dynamic open environments." First Workshop on Pervasive Security, Privacy and Trust PSPT. Vol. 4. 2004.
[8] Dalal, Renu, ManjuKhari, and Yudhvir Singh. "Different Ways to Achieve Trust in MANET." International Journal on AdHoc Networking Systems (IJANS) Vol 2. 2012.
[9] Theodorakopoulos, George, and John S. Baras. "On trust models and trust evaluation metrics for ad hoc networks." Selected Areas in Com-munications, IEEE Journal, 2006.
[10] Cho, Jin-Hee, Ananthram Swami, and Ray Chen. "A survey on trust management for mobile ad hoc networks." Communications Surveys and Tutorials, IEEE 13.4 562-583. 2011.
[11] Boukerch, A., Li Xu, and Khalil El-Khatib. "Trust-based security for wireless ad hoc and sensor networks." Computer Communications 30.11 2413-2427. 2007.
[12] Sheikh, Rashid, M. Singh Chande, and Durgesh Kumar Mishra. "Secu-rity issues in MANET: a review." Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On. IEEE, 2010.
[13] BasudevShivahare, CharuWahi and ShaliniShivhare, "Comparision of Proactive and Reactive Routing Protocol in MANET using routing protocol property", International Journal of Emerging Technology and Advanced Engineering, march 2012.
[14] Dharani, D., and P. Devaki, "A Survey on Improving the Lifetime of the Network in Mobile Adhoc Network." network 3.11 2014.
[15] Yan, Zheng, Peng Zhang, and Teemupekka Virtanen. "Trust evaluation based security solution in ad hoc networks" Proceedings of the Seventh Nordic Workshop on Secure IT Systems.2003