Research article **Available online www.ijsrr.org** **ISSN: 2279–0543**

International Journal of Scientific Research and Reviews

Contemporary Trust Management Strategies for Establishing Secure Communication in the Heterogeneous Network

Rafi U Zaman[1], A. Venugopal Reddy[2], M A Raheem[3]*,and Khaleel Ur Rahman Khan[4]

[1]Information Technology Department, MJCET, Hyderabad, India
[2]JNTU, Hyderabad, India
[3] Computer Science Department, Rayalaseema University, Kurnool, Andhra Pradesh 518002, India
[4]Computer Science Engineering Department, ACE Engineering College, Hyderabad, India

ABSTRACT

Mobile ad Hoc Network (MANET) consists of several wireless mobile nodes that communicate with each other by sending and receiving messages. When a message sent by the source to reach the destination it traverse through many intermediate nodes in the network. Some intermediate nodes forwards the exact message received to the other nodes where as few act as malicious and modify the data before transmitting. In order to provide security in the network a proper trust management among the nodes is required. To identify the malicious behaviour of the nodes it is necessary to evaluate their trust values. Traditional Trust management mechanisms like direct and indirect trust evaluations are available which enable a mobile node to examine the behaviour of other node. But these trust management approaches suffer from drawback due to fake identity of the node, and hence need to be enhanced in order to adjust with the changing networking conditions. Adapting to such networking conditions reflects an interesting issue in MANET. If the node modifies the message and acts trustworthy, then there is the issue of managing trust among the nodes. The main aim of this paper is to introduce an overview of various different strategies and solutions for managing trust in heterogeneous networks. It also presents a strong analysis of the most compelling proposals by drawing their classifications, characteristics, and problems. This survey concludes with framework for comparing different trust management strategies based on network routing and packet delivery parameters

KEYWORDS: Mobile Adhoc Networks (MANETS) Trust Management Integrated Internet MANET (IIM) Network Security Load balancing Gateway Routing

***Corresponding Author**

Mohammed Abdul Raheem

Research Scholar,

Computer Science Department, Rayalaseema University, Kurnool, Andhra Pradesh 518002, India

Email: maraheem@mjcollege.ac.in, Mobile : 9948170286

INTRODUCTION

A mobile ad-hoc network (MANET) is defined as a collection of wireless mobile devices created for a specific purpose without any fixed infrastructure. The system of deciding to route a packet between the mobile devices in ad-hoc network is mainly done using various routing protocols for MANET. The Internet is an infrastructure network, whereas the infrastructure-less mobile ad hoc network provides the ease of communication on the move. As in mobile ad hoc network communication can only take place among the devices that are part of the network. For this purpose, to make mobile devices within a MANET to communicate with any of the other device in the world, the mobile ad hoc network is connected to the external network, evolving a new internetworking architecture defined as IIM or heterogeneous networks.

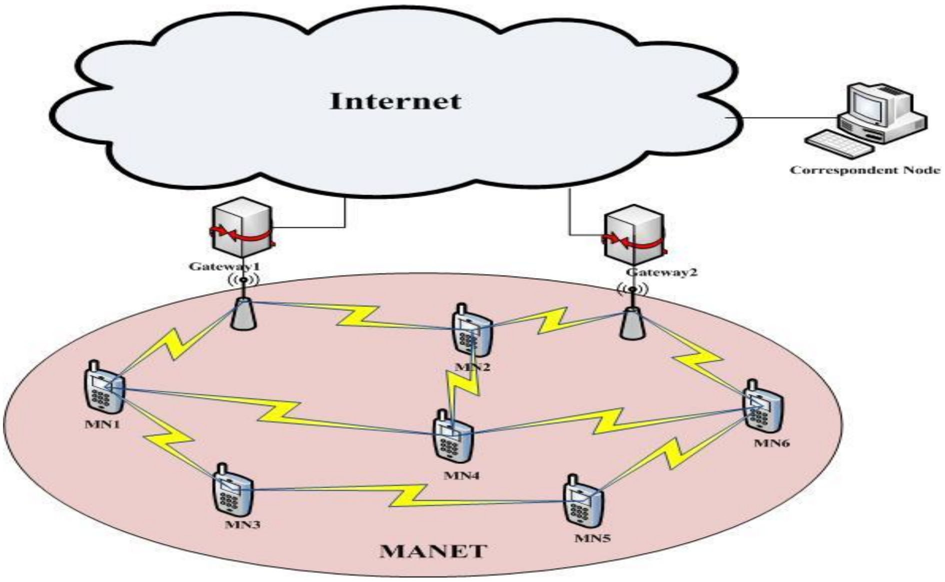


Figure 1. Architecture of Integrated Internet MANET

MANET does not support any centralized entities. They need to communicate with external network such as Internet or LAN to avail the resources provided by the external network. The interconnection of wired with wireless network is known as Integrated Internet MANET. The major issues in MANETS are the limited number of resources and applications, limited bandwidth, battery power and wireless coverage, dynamic network topology and security. Since security is one of the important challenges in MANET, therefore it is necessary to provide security of network.

Trust and trust management are one of the important issues in integrated internet MANET. The various properties of trust are it is dynamic, subjective, asymmetric, dependent on context and not inevitably transitive. Trust evaluation includes Experience, recommendation and Knowledge. It can be either distributed or centralized evaluation. The three phases of trust management are Trust propagation, aggregation and predictions. The "experience" part of trust is measured by their immediate neighbours and kept upgraded in the trust table. The neighbours also provide “suggestions” another part of trust and “learning” part of trust is a segment of aggregate trust.

Security Challenges in IIM

There are many security issues that arises in integrated internet MANET that include:

1) Interoperability: When connecting MANET with the external network such as internet, the routing Interoperability is a pivotal problem. Many ad-hoc routing protocols are depicted for MANET where no central entity exists. But for the Internet protocol every node should act as a router and must perform route discovery with the other nodes in the network. Nodes in MANET cannot acquire routing information beyond a limit and also ad-hoc routing in IP networks is not able to handle communication between both the networks. Therefore, Interoperability act as major security issues in the integrated internet MANET.
2) Connectivity: Since mobile nodes need to be connected with the external network, require the connectivity globally while moving data from one network to another network without disrupting the communication.
3) Mobility: As the mobile nodes move randomly within a network, mobility is one the vital issue in internet MANAT integration. Since nodes may enter or leave dynamically the network require to maintain a proper communication with other nodes in the network.
4) IP Signalling: The multiple hops between the two networks may lead to improper or weak signalling which causes problems in gateway discovering process. A secure gateway needs to be established between the MANET and IP network for a good communication. Multiple paths between the two networks causes high communication overhead.
5) Security Threats: The several security attacks and threats in the network include denial of service attack, forging attack, modification of messages, disclosing private data or key to unauthorized users, etc. Cause of these attacks in MANET creates many issues in the network. Similarly, attacks within the eternal network e.g., forwarding wrong data while registration. To prevent from such threats proper authentication protocols must be designed.

The remainder of this paper is organised as follows: Section 2 describes the related survey work in the area of trust management in MANET; Section 3 presents a survey on various existing strategies of trust management in MANET; Section 4 presents the framework for comparing trust management strategies in MANET; Section 5 presents the summary for comparing trust management strategies; Finally, Section 6 concludes the paper.

RELATED WORK

Various papers on the survey of strategies for the trust management in MANET are summarized below.

The work by [1] and [2] surveys the work of measuring the trust values in distributed MANET. In other strategies, [3] and [4] determine the trust within a multicast MANET and mission driven group communication systems. In [5] the trust management along with key management in the MANET is discussed. [4] surveyed the trust management issues with respect to selfish behaviour of nodes in MANET. To address the security issues

[6] and [7] surveyed the concept of trust to provide certificate revocation in MANET and secure gateway discovering technique in MANET respectively. [8] and [9] define trust based modules and secure routing in MANET. Attack behaviour and trust evidences of the nodes are determined in [10] and [11] respectively. Each of these strategies is explained in detail in the next section.

Trust Management Strategies in *IIM*

Trust plays a pivotal role in MANETS in defining the trust values among the nodes. Trust Management applies in many situations like authentication, access control, intrusion detection, etc. Trust is based on three things such as Trust establishment, Trust update and Trust revocation which are the basic factors of Trust management. Trust is evaluated based on different metrics in different ways. In the literature, several trust based approaches have been proposed. These strategies are classified as follows which explains the different concepts of trust management in MANET.

Quantifying Trust in Mobile Ad-Hoc Networks

[1] present trust domain based security architecture for MANET where trust is used to establish distributed secure control in the network. The mutual trust among the nodes is determined to make decisions in using pair wise keys for nodes in the network. The concept of Physical-logical domains which are self-organizing trust based means of grouping nodes in the network. Pair wise and group keys are established between the nodes in the network. Trust Values are evaluated based on Greedy approach, simple average of weighted products, weighted average and double weighted approach. The five phases of trust defined are monitoring, evaluating, updating, restructuring and re-establishment phases. The three trust regions are uncertain, good and bad. The pair-wise trust between the nodes in MANET is established to form group keys for the nodes in the network. But it does not assure the permissible level of security through the use of trust.

Markov Chain Trust Model For Trust-Value Analysis And Key Management In Distributed Multicast MANETs

[3] proposed multicast MANET for a sender that sends packets to several receivers through a multicast session. In MANETs, due to node mobility multicast group members often changes; thus, supporting secure authorization and authentication in a multicast MANET which is more disapproving than that in a wired network. A two-step secure authentication approach for multicast MANETs is defined where a Markov chain trust model is used to determine the trust value (TV) for each one-hop neighbour. A node’s TV is examined from its previous trust manner in the group. The node with the highest trust value in a group will be selected as the CA server, to increase reliability; the node with the second highest trust value will be selected as the backup CA server that will take over CA when CA fails. Several famous attacks have been analyzed.

The Markov chain analysis model is used to evaluate trust values of nodes in the network within a multicast group. The first phase consists of four steps creating the trust relationship among members, defining trust events for transiting a node's trust state, determining the trust values of each member, analyzing the overhead of trust establishment.

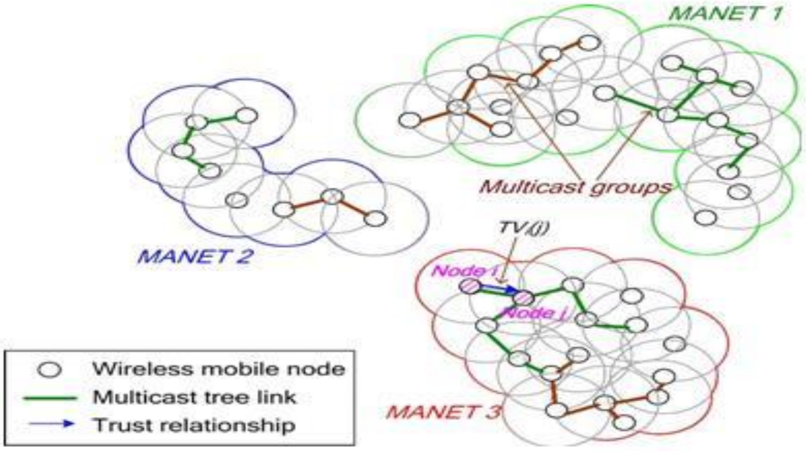
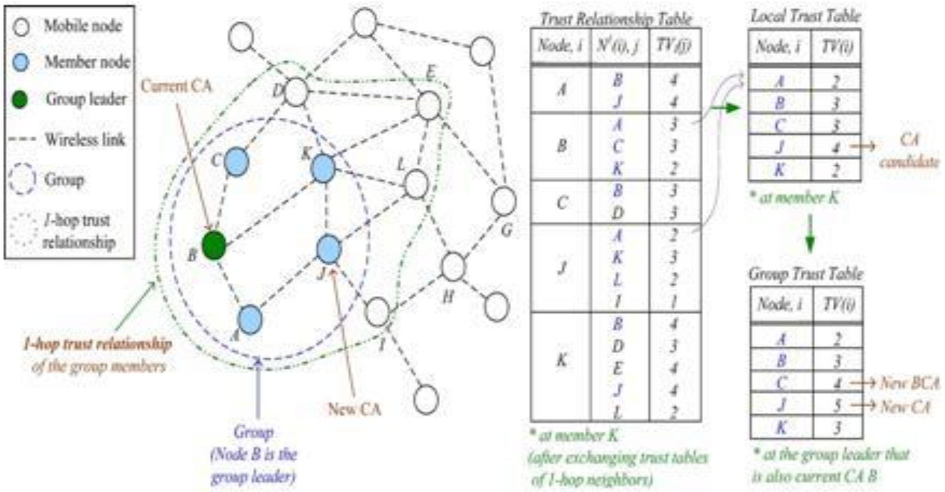


Figure 2. Multicast MANET

The different phases of CA management, authentication, and key management for Markov chain analysis in multicast MANET are defined. The message overhead and the worst-case time complexity of the trust model are determined. The secure group management and several attacks are also analyzed in multicast MANETs. Trust values as the trust chain increases is not clearly explained.



Trust Relationship Table

Node, i	$N^1(i)$, j	TV(j)
A	B	4
	J	4
B	A	3
	C	3
	K	2
C	B	3
	D	3
J	A	2
	K	3
	L	2
	I	1
K	B	4
	D	3
	E	4
	J	4
	L	2

* at member K (after exchanging trust tables of 1-hop neighbors)

Local Trust Table

Node, i	TV(i)
A	2
B	3
C	3
J	4
K	2

* at member K

Group Trust Table

Node, i	TV(i)
A	2
B	3
C	4
J	5
K	3

* at the group leader that is also current CA B

Figure 3. Trust relationships between nodes

A Survey on Trust Management For Mobile Ad Hoc Networks

[2] proposed managing trust in a distributed Mobile Ad Hoc Network (MANET) to achieve system and mission goals such as reliability, availability, re-configurability and scalability. To manage trust in military MANET, need to combine the concepts of social trust obtained from social networks with quality-of-service trust taken from information and communication networks to get a composite trust value.

Trust properties are defined as dynamic not static, subjective, transitive, context-dependent and asymmetry. Trust management in MANET is nothing but establishing, updating and relocating trust in ad-hoc network.

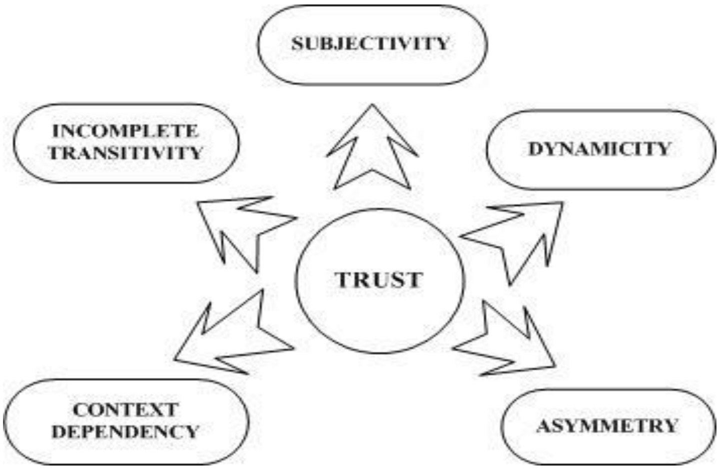


Figure 4. Trust properties in MANET

Trust concepts in different fields like economic, sociology, philosophy, psychology, organizational management, autonomic computing, communications and networking plays a vital role in cooperative and collaborative environments in MANET.

Many trust management schemes are used to observe misbehaving nodes, both malicious nodes as well as selfish nodes. The trust evaluation engine should be very strong and reduce gracefully if some confirmation or information does not provide a certain level of trust based on possible corrupted information. The different trust management metrics are defined as throughput, good put, overhead, delay and packet dropping rate which are used to evaluate trust values. Correct trust values evaluation leads to secure routing in MANET. Many trust management schemes are developed like authentication, secure routing, intrusion detection, authorization, access control and key management to provide security in ad-hoc networks. These schemes are used to provide a widespread framework for trust distribution or evaluation in MANETs. The social relationships in evaluating trust among collaborators in group setting by using the concept of social networks are not properly determined.

Modelling and Analysis of Trust Management with Trust Chain Optimization in Mobile Ad Hoc Networks

[2] present a trust management protocol in MANET for mission driven group communication system where collaboration among the mobile nodes is difficult with new alliance partners in the battlefield. So trust management in such situation is very necessary for successful collaboration among the nodes. Optimal level trust chain is used among the nodes to produce explicit trust levels based on trade off among path reliability and trust availability.

Each node evaluates trust value of the other mobile node based on QoS and social trust. QoS may hold competence to determine energy of the nodes where as social trust includes recommendations from indirect or direct observations. The concept of web trust is used to get certain level of trust among the nodes in the network.

Since the protocol is for mission based systems a group key is used as secret key for secure communication between nodes. Each node generate group key and exchange the key among them to collaborate. A new key is generated on a node disconnection from the network. Each node keeps the old information of the other node in the network.

Nodes selfish behaviour is also defined as they may drop the packets instead of forwarding the packets to the destination. Therefore selfish nodes are also detected in the system to provide security in the network.

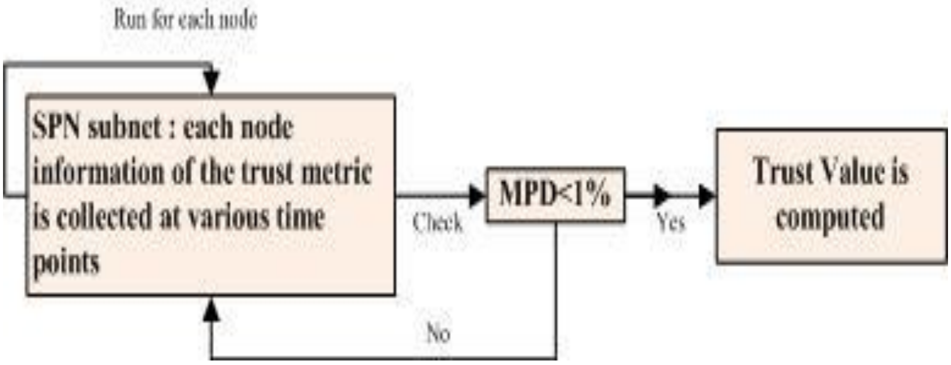

Run for each node
SPN subnet : each node information of the trust metric is collected at various time points
Check
MPD<1%
Yes
Trust Value is computed
No

Figure 5. Hierarchical modelling using SPN subnet

Hierarchical model is used with SPN subnet to evaluate the trust values of the nodes in the network. The figure shows SPN model for trust value calculation. The various levels of energy are balanced depending on its position.

Each nodes trust value is evaluated based on indirect and direct information given by recommenders. The optimal trust chain is used to evaluate most reliable trust values of the nodes and utilize the calculated trust values for communication with other nodes in the network. The disadvantage of the protocol is that there is high communication overhead in the network when trust chain length increases.

Trust Threshold Based Public Key Management in Mobile Ad Hoc Networks

Jin-Hee Cho et al. (2016) proposed composite trust-based public key management in MANET. The concept of trust based on soft security mechanism to eliminate security vulnerabilities where each node makes use of trust threshold is defined. An optimal trust threshold subsists to best meet and balance the incompatible goals between performance and security in MANET.

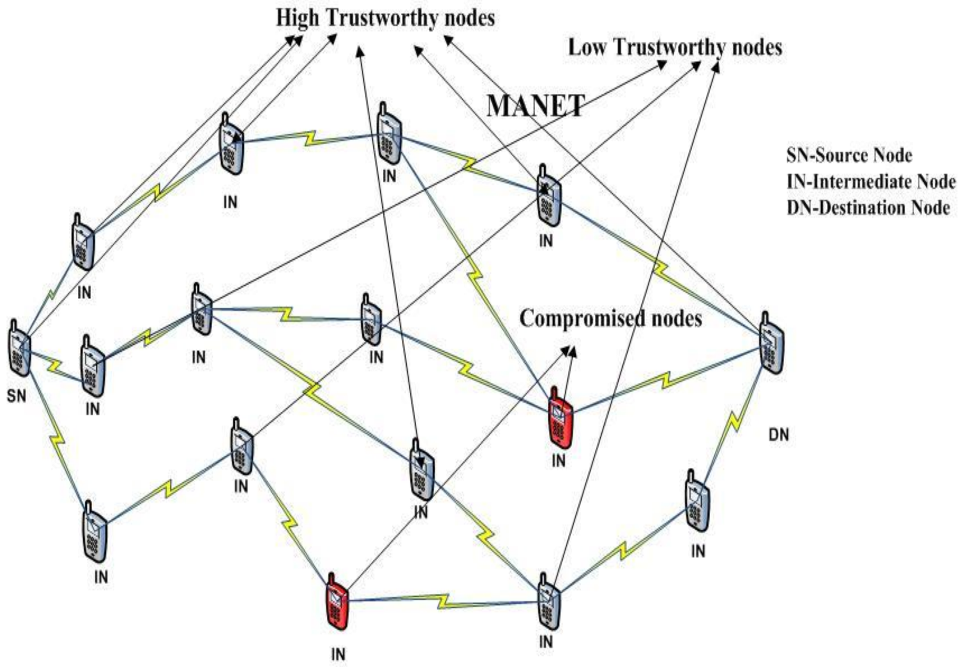


Figure 6. Trust management based on threshold in MANET

The three trust components integrity, competence and social contact are used to evaluate the trust values in ad-hoc network. These trust values are compared with the threshold value to find the untrustworthy nodes in the network.

Direct and Indirect trust values are evaluated to exchange the key among the trustworthy nodes in MANET. Direct trust is determined based on direct evidences where as indirect trust is find using one- hop neighbours recommendations.

Since MANET does not support the concept of third parties, therefore a trust based scheme is defined where pair of keys are shared among the nodes without any trusted certificate authority. An entity known as Neighbourhood trustworthy certifier issues certificates and keys to the nodes in the network. Public keys are issued, distributed and exchanged among the trustworthy nodes to have a secure communication in the network.

The design of the trust metric and trust based key management scheme clearly reflects the useful properties of trustworthy systems for MANET in the following way: (1) the use of a threshold balance the potential risk and mitigates the action of risk; (2) trust is determined based on node behaviour, evidence in the state of key management; (3) node resolve whether to trust other nodes of network in the process of key management operations in order to increase the distribution of public keys; (4) node contacts other nodes where trust over time based on last experience to new evidences is defined; and (5) enhances both security and performance, guiding to a high system reliability.

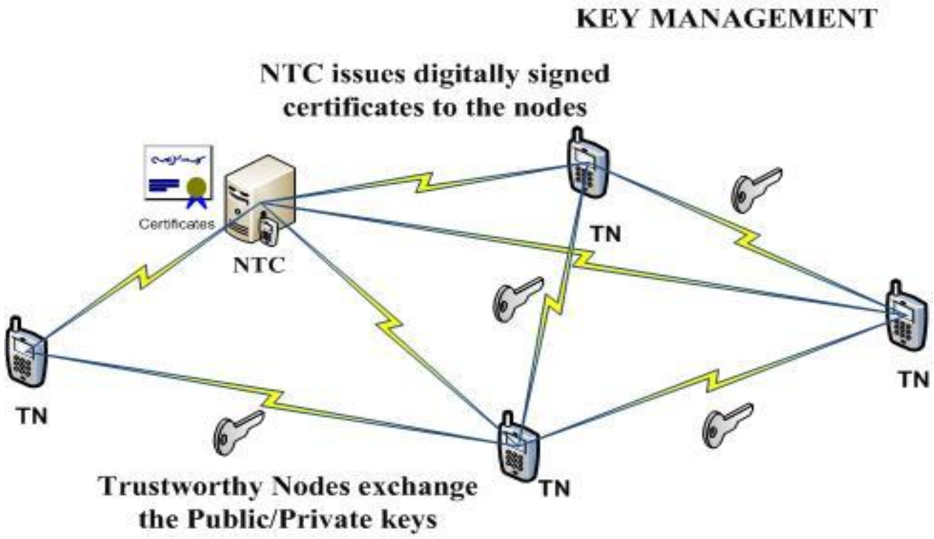

KEY MANAGEMENT
NTC issues digitally signed certificates to the nodes
Certificates
NTC
TN
TN
TN
TN
TN
Trustworthy Nodes exchange the Public/Private keys

Figure 7. Trust threshold based key management in MANET

Trust bias and service availability are used as metrics to evaluate trust among the mobile nodes in the network. The proper concept of trust to obtain secure communication among nodes in wired cum wireless networks in not determined and there is high communication cost incurred in the system.

On the Trade-Off Between Altruism and Selfishness in MANET Trust Management

[4] proposed a protocol describing the selfish and altruism behaviour of a mobile node in MANET. Nodes behave selfish in forwarding packets to another node in order to save its energy. Therefore, it is necessary to detect such selfish nodes and remove them from the network. Trust management protocol for GCS is defined to find such selfish nodes in the network. Selfish vs. Altruistic node behaviour is identified in the network.

The major properties of the trust are it should be dynamic, asymmetric, context-dependent and subjective to have a proper trust management among the nodes in MANET. Cognitive networks are used to improve the network scalability and quality of service to quickly adapt to network changes such as node failure, energy depletion, and selfish behaviour of the nodes. Social trust and QoS are the two important features to establish a trust relationship among the nodes in network. Social trust defines the social behaviour of the node with other nodes in the MANET. It is measured by the direct and indirect evidences given by neighbours of a node. QoS is also defines the level of energy needed to accomplish a task by a node.

Due to mobility of a node their trust values often changes or decay according to time as the length of trust chain grows. Demand and pricing model is used to define the selfish and altruistic behaviour of a node.

The model is used to define such node behaviour based on global and individual welfare. DP model is used to detect the selfish and unselfish nodes in the network. This model is useful for large number of nodes in the network. The selfish and unselfish behaviour of the nodes is determined to achieve reliable and scalable network dynamics.

More advanced mission model with the effect of mission characteristics such as risk, workload requirements and deadline is not considered. System reliability is not clearly measured to reach system goals.

Trust Based Certificate Revocation for Secure Routing in MANET

[6] proposed a trust based certificate revocation in MANET to provide security. In MANET, both trust management and key management are the major issues to be considered. Trust between the nodes is evaluated using both indirect and direct evidences. As in MANET the third parties are not supported, the trust is defined without any CA. The trust values of the nodes are compared with the threshold value. If trust value is found greater than threshold, then the node is trustworthy and is authenticated to share secret information with other nodes of the network. Light weight encryption and decryption techniques are defined in this strategy. Security services such as confidentiality, non repudiation, and authentication are mainly considered. Secure routing and transmission mechanisms are also determined. The procedure to discover a secure route to the destination is to send a route request packet to destination node and when it receive the request it verifies by secret shared key and sends the reply. The nodes that misbehave in the network are eliminated, therefore revocation mechanism is used. This revocation is mainly done by the neighbour node. The trust value is calculated from indirect and direct experiences to detect the malicious nodes and to remove them from the network.

The resolver is used to evaluate global value of trust of a node. The revocation coordinator sends request as Revc Req to all the nodes in the network. Certificate for malicious node and revocation coordinator is present in the revocation message with the coordinator signature. Node receiving the message verifies the signature using public key of the revocation coordinator to have message integrity.

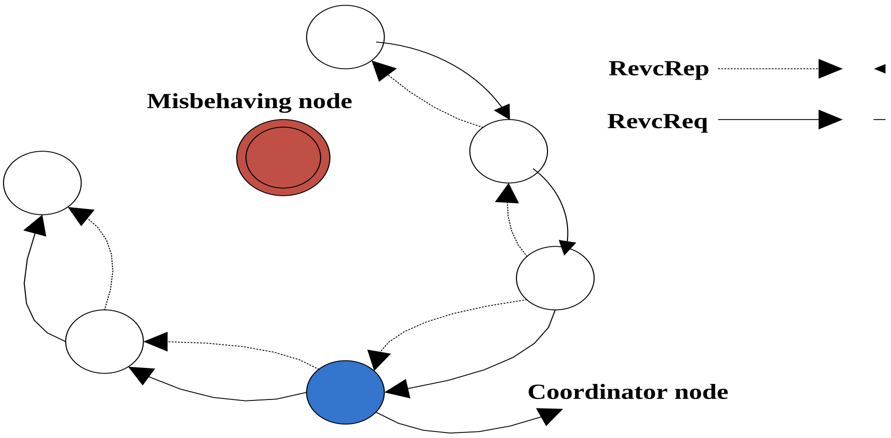


Figure 8. Revocation Request and Reply

The node sends a reply as RevcRep, then coordinator searches trust value in trust table of the node and if it is greater than threshold, the node is trustworthy and can share the information with the other nodes. If it is untrustworthy then it will not accord revocation procedure and coordinator sends the RevcRes packet to neighbours and they forward it to other neighbours.

This revocation process is used to remove the misbehaving nodes in the network. The main disadvantage of this process is that the third parties are not supported in MANET and therefore the concept to issue certificate is not clearly explained in the mechanism.

A Trust Based Gateway Selection Scheme for Integration of MANET with Internet

[12] proposed trust based gateway selection mechanism in integrated MANET. Secure gateway selection is one of the vital issues in MANET integration with external network. Gateway support both network protocols such as IP based and MANET based protocols. To transfer the information from one network to another, the gateway acts as bridge between them. Many gateway selection methods are defined. But such methods do not assure path initiated with the gateway is secure or not as there may be many malicious nodes present in the network that may drop the packets without forwarding.

The gateway route is determined based on selected value calculated as the average of trusted values, load capacity and number of hops of the nodes in the network. Trust management is needed in the network to select a secure route to the gateway. Therefore, trust value is computed based on past behaviour or recommendations for the nodes.

The node is malicious if its trust is not properly defined. The difference between the observed and actual trust denotes the trust value of a node. Minimum load availability of a node is used to define fact that congested node is malicious. Secure Route Selection Value is computed by taking the average of trust value, load and number of hops of the nodes. Path with highest value is selected as secure path to the gateway.

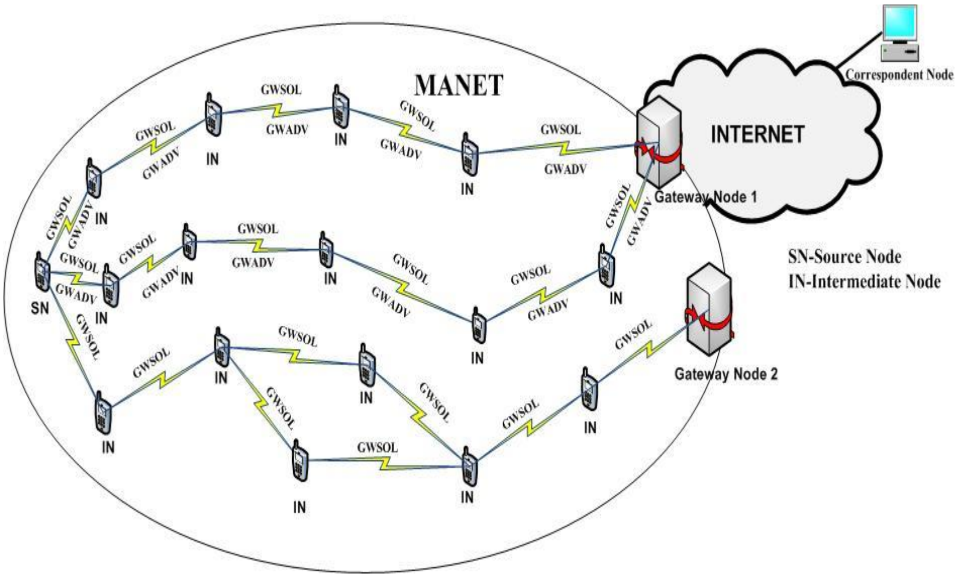


Figure 9. Trust based Gateway Selection

The secure gateway selection process is started by source node broadcasting the solicitation message to its neighbours. Neighbours on receiving message forward to other neighbours till it reaches the gateway node connected to external network. Gateway node on receiving message finds the path to requested node, if so then replies to source node. Otherwise does not send the reply to the source. It also computes the trust and load values and forward the message further. On receiving reply intermediate nodes calculate trust and load values and rebroadcast the reply till it reaches the source node. Finally, source node calculates secure path selection value select the most appropriate route to gateway and gets registered with it to connect to the internet.

The drawback of this approach is that it does show how exactly the trust values are calculated by considering only the past experiences of the nodes in the network.

A Distributed Trust Management Framework for Detecting Malicious Packet Dropping Nodes in A Mobile Ad Hoc Network

[8] proposed malicious packet dropping nodes detection method in MANET. In MANET, mobile nodes communicate with one another establishing a collaborative network therefore trust among the nodes is required. The proposed system is very interactive as problems of election algorithms used in selecting subnet of nodes for communication are absent. An authentic protocol is defined that works even in case of transient partitioning of the network and byzantine failure of the nodes.

The working of the system is that all nodes of the network observe the behaviour of their neighbours and if any unusual operation is detected then an algorithm is invoked that determine the nodes as malicious or not. The six trust based modules are defined as monitor, reputation collector, reputation formatter, reputation propagator and alarm raiser module. The first monitor module observes each neighbour node by listening to their conversation to find the malicious nodes. The reputation collector module calls a majority consensus algorithm between the neighbours of the node that is found to be malicious. In reputation formatter module the information of malicious nodes is send among the neighbour nodes in the network by using the rep-mess message. In reputation maintainer module every node preserves a global state of trust for all misbehaving nodes in the network. To have trust state a reputation table is maintained containing node id and rep-val. The reputation propagator module in order to exchange trust based certificates uses mobility of the nodes. Finally, alarm raiser module starts a response action as soon as it receives global alarm of a misbehaving node.

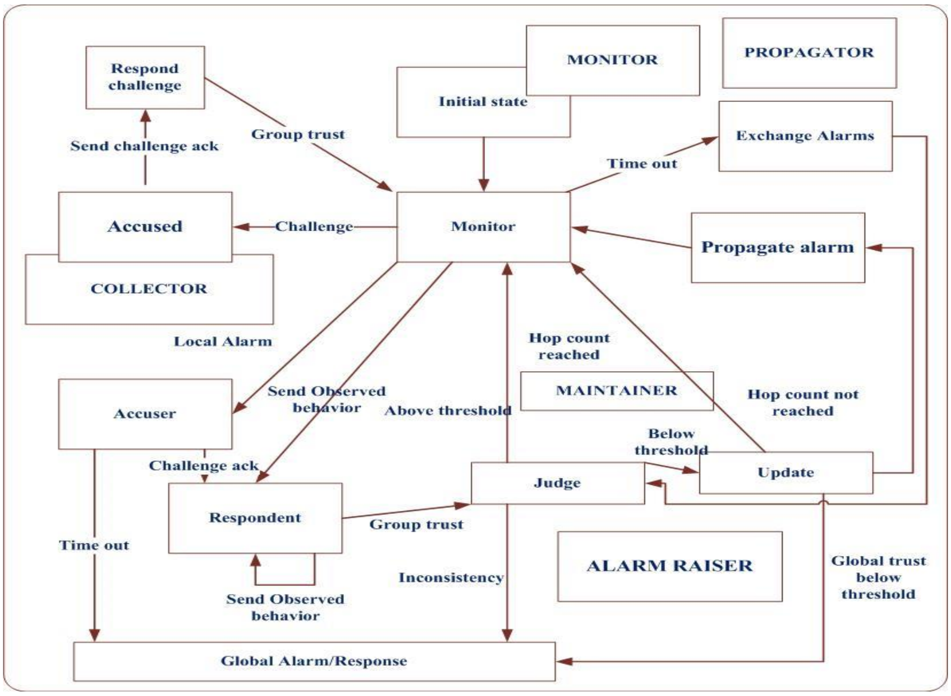


Figure 10. Working of trust based modules

The trust computation is done based on message altering, dropping of packets and false allegation of the nodes. The accused node performs activities such as dropping the adverse feedbacks, using the selective broadcast, altering the received feedbacks. If the accuser node is malicious then it broadcast wrong accusation, false accusation of feedbacks dropped, dropping and tampering of trust based certificates. If other nodes are misbehaving then they may drop trust certificates and also alters them. The drawback of this strategy is that the malicious behaviour of a node in case of high availability of a node is not determined.

Trust Based Secure Routing in AODV Routing Protocol

[9] proposed trust based secure routing protocol in AODV in MANET. In MANET the nodes communication without any trustworthiness and centralized authority creates a major issue in MANET. In the protocol trust is calculated based on node's performance continuous evaluation and neighbour nodes opinion value about the other nodes. Secure path is established between destination and the source without any misbehaving nodes. The existing routing protocol AODV is modified to provide trust based communication among the nodes. Both node and route trust is calculated.

Modified AODV routing protocol required the changes as two new control packets as trust request and reply are used, routing table is updated as four new fields are added like positive and negative events, opinion and route status. The trust value is calculated to obtain a secure route from source to destination using this approach. Node's trust is found from neighbour's opinion. Route's trust is calculated based on number of nodes send by source minus number of nodes received by destination. Source starts route establishment process by broadcasting request message to destination then when it replies back it selects the most trustworthy route to destination. The major disadvantage of this strategy is that it does not explain how clearly the malicious nodes are detected within the network.

Attack-Pattern Discovery Based Enhanced Trust Model For Secure Routing in Mobile Ad-Hoc Networks

[10] presents a trust model based on attack pattern discovery in MANET. As in multi-hop routing where central authority and infrastructure is absent the trust based secure routing is very difficult task. Some malicious nodes may drop the packets intentionally or unintentionally within a network. Nodes historical behaviour is mainly considered where the pattern discovery method is used to detect misbehaving nodes before they try to drop the packets. Three different models detecting various packets forwarding misbehaviour is also determined. This combination of trust based model and attack based pattern form a better way to weaken the damaging of the network.

The trust model derived is based on trust computation, derivation and attack-pattern discovery. First, trust is found using direct or indirect observation. Neighbour nodes behaviour is observed to evaluate trust. The ratio of dropping is calculated as proportion of no. Of packets drop to no. of packets forwarded. Two packets types are considered as control and data packets. The method of common difference is used to find malicious patterns by noting their field values of the request and reply packets.

The trust based on demand routing is used to find secure path among the nodes of the network. In this protocol HELLO packets include the fields as sent control packet, forward control packet, sent data packet, forward data packet, and distrust value. Route discovery and maintenance is performed followed by trust recommendation and update.

Adversary models modes of operations are determined to provide trust based routing. The drawback is that the malicious behaviour of the as number of nodes increases is not defined. The detailed mode of operations of the different adversary models finding various kinds of packet forwarding misbehaviour is determined where theoretical analysis and analytical results prove that the combination of pattern discovery method with trust-based model provides earlier detection of adversaries.

Design and Development of CTSR With Direct and Indirect Observations of MANET Applications

[11] proposed a model that defines development and design of collaborative trust base secure routing in MANET with direct and indirect observations. The trust management is performed to interpret reliability of the nodes deployed.

Trust value is calculated based on Dempstershafer theory and Bayesian inference of uncertain reasoning derived from indirect inspection of mobile nodes. 2-ACKT routing protocol is used for finding trust values of the nodes. Using the 2-ACKT routing protocol minimizes the communication overhead.

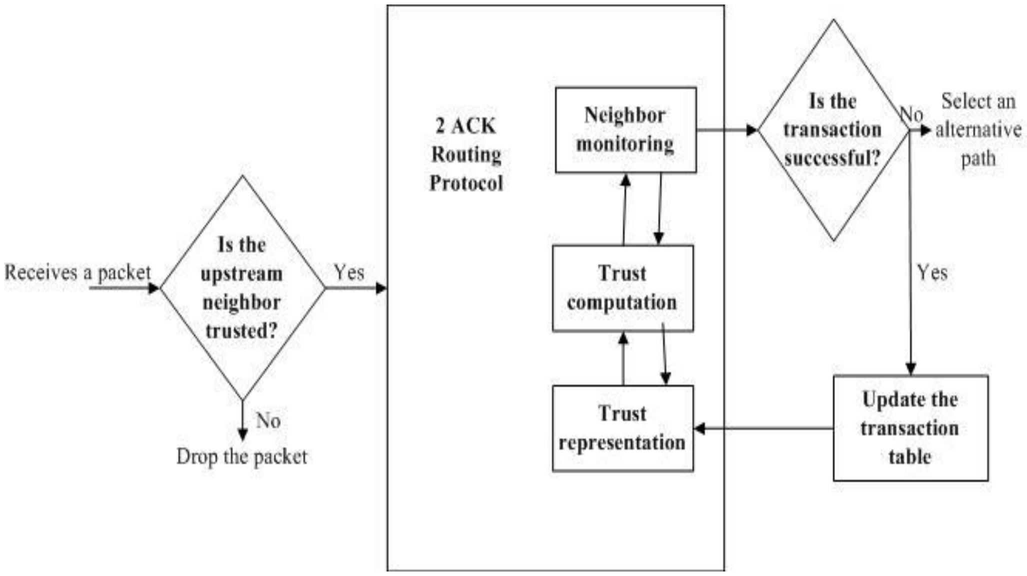


Figure 11. Block diagram of 2ACK routing protocol

Trustworthiness of a node is defined by collective information of trustiness of neighbour nodes. The time required while sending and receiving the packets is measured as trip time. As the performance of the network decrease due to the presence of misbehaving nodes the trusted nodes are found to mitigate this issue. Dempstershafer theory is used to calculate trust by indirect and direct observations. Since the establishment of DST for indirect observation in the wireless networks trust values are successfully acquired with data packets and control packets. Percentage of Trust value overhead in message increases as the number of nodes increases. But the protocol fails to explain the attack behaviours of the nodes.

A FRAMEWORK FOR COMPARING TRUST MANAGEMENT STRATEGIES

In this section, we present the comparisons of the trust management strategies based on the common parameters. In Table 1, network architecture/model of the trust management strategy is defined. The Routing Protocol is the protocol used for routing packets within the ad-hoc network. MAODV stands for multicast ad-hoc on-demand distance vector routing protocol, TCRSR is the Trust based Certificate Revocation Secure routing protocol, DSR is Dynamic Source routing and CTSR is Collaborative Trust based Secure Routing protocol. Different routing protocols can be used for routing packets in different strategies.

Table 1. Network Routing Parameters

TRUST MANAGEMENT STRATEGY	NETWORK ARCHITECTURE/MODEL	ROUTING PROTOCOL
Mohit et al.	Trust domain based security architecture	AODV
Chang et al.	Markov chain trust model	MAODV
Cho and Chen et al.	SPN subnet model	....
Cho and Chan et al.	Demand and pricing theory model	....
Rajkumar et al.	Trust based threshold revocation model	TCRSR
Manoharan et al.	Trust based gateway selection	AODV
Jaydip et al.	Distributed trust management model	DSR
Pushpa et al.	Trust based secure routing	AODV
Jhaveri et al.	Attack pattern discovery based trust model	AODV, SNBDS, TRS-PD,TRS
Sargunavathi et al.	Two way acknowledgement based trust model	CTSR

Table 2. Trust Management Parameters

TRUST MANAGEMENT STRATEGY	ATTACKS CONSIDERED	TRUST VALUE EVALUATION	METRICS
Chang et al.	On-Off, conflicting behaviour, newcomer, fake, cheating	Direct Observation	Packet delivery ratio, Average trust value
Cho and Chen et al.	Wormhole, black hole, gray hole, DOS, replay	Direct Observation	Packet dropping rate, Delay, Overhead, Throughput
Cho et al.	Packet dropping	Direct Observation	Trust value, Path reliability, Normalized trust availability
Cho and Chan et al.	Private key compromise, DOS, fake identity and recommendations, message modify	Direct and Indirect Observation	Trust bias, Service availability, information risk, comm. Cost
Rajkumar et al.	Packet dropping, Fake certificate	Direct and Indirect Observation	Average PDR, Average E2E delay, Packet drop, resilience
Manoharan et al.	....	Advertised and Observed trust value	PDR, Control overhead, Attack success rate
Pushpa et al.	Packet dropping	Direct Observation	No. of malicious nodes, Drop packets, Throughput
Jhaveri et al.	Gray hole, Packet dropping	Direct and Indirect Observation	PDR, NRO Average E2E delay, Throughput, Average Detection time
Sargunavathi et al.	Fake message broadcasting	Direct and Indirect Observation	PDR, No. of nodes, Throughput, Avg. E2E delay, Overhead

In Table 2, the trust management can defined as establishing trust relationship among the nodes. The parameters on which the trust management strategy depends are the trust managing parameters. Various attacks are considered in each strategy. To eliminate such attacks from the network proper trust value evaluation of the nodes is required. Trust can be computed from direct or indirect observation of the nodes behaviour within the network. Metrics are the parameters needed to calculate the results of the trust values evaluated. PDR is Packet delivery ratio and NRO is Normalized routing overhead of the nodes measured as the ratio of the total number of routing packets sent to the total number of data packets received. The trust management parameters are summarized in the following table below.

In Table 3, the packet delivery parameters are explained. Inversely proportional means if one metric increases then the other one decreases. If they are directly proportional then either increases or decreases simultaneously. PDR is the Packet delivery ratio measured as number of packets send over number of packets received by the nodes. Packet delivery delay refers to the time taken for a packet to be forwarded across a network from source to destination.

Table 3. Packet Delivery Parameters

Trust Management Strategy	Packet Delivery Ratio	Packet Delivery Delay
Chang et al.	Inversely proportional to mobility	....
Rajkumar et al.	Inversely proportional to speed	Inversely proportional to speed
Manoharan et al.	Inversely proportional to number of malicious nodes	Inversely proportional to number of malicious nodes
Jhaveri et al.	Inversely proportional to mobility and percentage of malicious nodes	Directly proportional to mobility and percentage of malicious nodes
Sargunavathi et al.	Directly proportional to number of nodes and node velocity	Directly proportional to number of nodes and node velocity

SUMMARY FOR TRUST MANAGEMENT STRATEGIES

Trust management in MANETs is an interesting problem. In MANET, trust management is achieved through different trust evaluation techniques. It can be summarized that an ideal trust management mechanism must address the issue to provide security of the network. Different trust management techniques were proposed by different authors to evaluate the trust values of the nodes which are not sufficient to manage trust in the network. Security of the network is taken into consideration but the usability and integrity of the messages is not addressed properly. The attacks considered by each strategy show how these attacks are detected and prevented from the malicious behaviour of the nodes. But how to identify the malicious or untrustworthy nodes is not specified correctly. The results of the strategies are discussed based on packet delivery parameters to show the performance of the nodes in terms of forwarding the packets among the nodes within the network. But how the PDR metric related to trust management is not explained. Finally, it is observed that the work done so far in MANET has focused on resolving the issues of Security based on trust management. None of the existing works provides proper solutions which address these issues.

CONCLUSION AND FUTURE DIRECTION

MANETs are highly vulnerable to many security attacks because of dynamic topology used in MANETs, its distributed operations and also of limited bandwidth. Trust as a concept has a wide variety of applications, which causes divergence in terminology of trust management. This paper provides an overview of various strategies to show how the trust management is done to establish a secure communication in the network. The framework comparing trust management strategies based on common parameters is presented. There are various strategies proposed to determine trust management in mobile ad-hoc networks but no such strategy explains the trust management approach in integrated internet MANET. As a result, the logical methods for managing trust in heterogeneous networks will be an essential part of the evolution towards future communication networks. But the realization of this perception still requires a large number of challenges to be solved related to applications and services.

As a future work, the implementation is under the way using the object oriented network simulator NS2 to evaluate trust values based on three trust metrics such as trust capability in serving request, trust integrity while sending and receiving the request and dynamic social behaviour of a node in the heterogeneous networks

REFERENCES

1. Virendra, Mohit, et al. "*Quantifying trust in mobile ad-hoc networks*." International Conference on Integration of Knowledge Intensive Multi-Agent Systems, IEEE, 2005.
2. Jin Hee Cho, Ing-Ray Chen, and Kevin S. Chan, "*A Survey on Trust Management for Mobile Ad Hoc Networks*", Elsevier, 2011.
3. B.-J. Chang, S.-L.Kuo, ”*Markov chain trust model for trust-value analysis and key management in distributed multicast MANETs*”, IEEE Transactions on Vehicular Technology, 2009; 58(5)
4. Jin Hee Cho, Ing-Ray Chen, and Kevin S. Chan, "*On the trade-off between altruism and selfishness in MANET trust management*", Elsevier, 2013.
5. Jin Hee Cho, Ing-Ray Chen, and Kevin S. Chan, "*Trust Threshold based Public Key Management in Mobile Ad Hoc Networks*," Elsevier, 2016.
6. Banoth Rajkumar and G.Narsimha, "Trust Based Certificate Revocation for Secure Routing in MANET," Elsevier, 2016; 92: 431-441
7. R. Manoharan, S. Mohanalakshmie,”*A Trust based gateway selection scheme for integration of MANET with Internet”*, IEEE-International Conference on Recent Trends in Information Technology,” ICRTIT 2011 MIT, Anna University, Chennai. June, 2011; 3-5
8. Jaydip Sen, "A Distributed Trust Management Framework for Detecting Malicious Packet Dropping Nodes in a Mobile Ad Hoc Network", International Journal of Network Security and its Applications (IJNSA), 2017; 2(4): 92- 104.

9. Menaka, A., and M. E. Pushpa. "*Trust based secure routing in AODV routing protocol.*" Proceedings of the 3rd IEEE international conference on Internet multimedia services architecture and applications. IEEE Press, 2009.
10. R. Jhaveri and N. Patel, "Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks", IJCS,2016; 30(10)
11. S. Sargunavathi and J. Martin Leo Manickam, "*Design and Development of CTSR with Direct & Indirect Observations of MANET Applications*", Mobile Networks and Application, Springer, 2016.
12. R. Manoharan, S. Mohanalakshmie, *"A Trust based gateway selection scheme for integration of MANET with Internet"*, IEEE-International Conference on Recent Trends in Information Technology," ICRTIT 2011 MIT, Anna University, Chennai. June, 2011; 3-5.