Survey Report on MANETs Trust Management

S. Venkatesh Babu and Dr. C. Kezi Selva Vijila

Received 18 January 2017; Accepted 22 March 2017; Available online 28 March 2017

Address For Correspondence:
S. Venkatesh Babu, Asst. Professor, Christian College of Engineering and Technology, Oddanchatram, Dindigul, India.
E-mail: venkateshloower6@gmail.com

Copyright © 2017 by authors and American-Eurasian Network for Scientific Information (AENSI Publication). This work is licensed under the Creative Commons Attribution International License (CC BY).

ABSTRACT
The distributed wireless network has grown in the field of social networks, compares and mainly is distracter relief center, military application which requires a co-operative environment for the effective distribution of network functions and services. One such network is mobile ad-hoc network which is open network without a stable topology where the frequency of nodes joining and leaving the network is high. In such an unstable environment the reliability of the interacting node is an important concern. The nodes among the distributed network may include nodes that are selfish and misbehaving in nature which leads to poor outcome in terms of result gathering, co-operation and throughput. The detection of threats that are imposed by un-trust nodes are unfolded in to many methods that are termed as Trust Management in MANETs. The trust of nodes are evaluated based on the trust parameter shared between the nodes with the use of objective function, which defines the degree of trust based on the node behavior. The trust parameters are gathered by the nodes in direct or indirect manner in direct method the node will observer the behavior of its neighbor nodes and evaluate the trust based on its observation but in indirect method the nodes will collect the trust parameter from its neighbor nodes to calculate the trust value. The development of the various trust management methods is to fulfill the requirement of a secure distributed mobile network. This paper outlines the various trust management mechanisms which operates in vibrant and ambiguous MANET environment.

KEYWORDS: Trust Management, Trust Evaluation, Selfish, Misbehaving

INTRODUCTION
The growth of mobile wireless networks has given hands in the development of mobile application, internet services for information sharing, routing and location based service. Mobile ad hoc network (MANET) is one such network that is flexible to operate in all kinds of environment without any centralized administration. In which nodes can communicate with each other where every node has the capability of forwarding the packets of other nodes [1]. In some cases the wireless network may have centralized access point through which the communication can take place between nodes through the access points only. These kind of network can be used to setup network with little effort in the situations like hurricane and earthquake disasters, and for exchanging most critical information in the battlefield [2].

In ad hoc network the nodes are capable of forwarding the packets of the other nodes since there won’t be any direct links between the nodes this point will become worse if the forwarding node alters or doesn’t forward the packet of others. In such cases the network in not trusted and the objective of the network is difficult to realize. Trust management is one of the important security component of the network that provides a secure environment for ad hoc network by preventing the selfish and malicious nodes by monitoring their behaviors. Confidentiality is another important inclusion of Trust management system. The trust management system functions around the evaluation mathematics. The evaluation mathematics depends on the trust values provided...
by the nodes [3]. The direct, indirect means of trust value calculation are involved. In direct method the node will monitor the behavior of other nodes by considering some parameters and in indirect method the node will get the trust value from nearby trusted neighbor. But due to dynamic nature of MANET it will be difficult to gather the values. The development of trust management helps to develop a secure ad-hoc network. The design of trust management has several bottleneck such it’s very tedious to calculate the trust value very precisely, and it has to consider the following metrics such as energy, mobility and congestion.

The paper is organized as follows. In Section 2 trust model is discussed followed by discussion on various trust model in session 3. Then in Section 4 other security related issues are outlined with the concluding session.

**Trust Management System:**

Ad hoc network is self-configuring network in which node can join and leave the network automatically so there is no procedure to determine the honesty of the nodes. Trust is a concept of social that defined the degree of belief for an entity [20]. The trust is the attribute of a node that is associated with the behavior of a node [4]. The behavior parameter are assigned based on the context of the network that is assigned automatically or allocated by the network designer. Different Metrics are used for the evaluation of trust. In which both district and continuous values are used for the measurement of trust. In some cases the threshold, fuzzy, probability, hop distance values, etc., are used as trust metrics. The trust based evaluation process is three fold history analysis, suggestion and learning. In the first case every host will measure the trust value of its own and also the neighbor these values are updated in the trust table which is managed by all the nodes in the network this happens at regular intervals [5]. The updated values of trust table is shared among the neighboring nodes as suggestions and based on shared this values the nodes will aggregate the values. The process of aggregation is called as learning. These three process are carried out independently and collectively contribute to the Trust management in MANETs. The trust in some case as in [6] has properties like Transitivity, Asymmetry and Personalization. Providing trust based security in ad-hoc network gains higher security and improves network efficiency in terms of reliability and confidentiality. This paper discusses various trust based security method deployed in ad hoc networks like MANETs.

**Nomenclature of Trust Management:**

The discussions on this paper is aligned towards trust management it is important to define the term trust. Trust is stated as the amount of willing that one depends on another even the one don’t have any control over the another and also negative concerns may come up for another [7]. The trust and trustworthy are two terms looks analogous but have different level of security in a distributed systems. If an algorithm related to trust fails than the dependent security policy of the system fails, but the trustworthy function is one that is designed in a manner that it won’t fail [8]. The evaluation function is mainly based on behavior of a node so it is important to craft a way to detect and justify the behaviors is gaining momentum [9] [10].

The security functions in MANETs work around to prevent the security attack and or elements one such attack if it happens. The behavior is classified as selfishness and malicious. A node in the distributed system is pretend to be selfish if it tries to protect its resources from other nodes by providing some fake parameter and does breaks the network connectivity. In some cases the selfish nodes will use the resource of others by which it safeguard its resources. But the malicious nodes will do some damages to the components of the network and its functions [9]. A survey is briefed in this section based on the classification of trusted system model, the main classification [11] are as follows;

- Trust Based on Routing Protocol,
- Legacy Based systems,
- Behavior Based systems.

**A. Trust Based on Routing Protocols:**

This kind of protocols has less representation due to its complex nature. In Secure Traceroute protocol [12] in which the number of unacknowledged packets are logged and compared with a threshold value if it is greater than a detection protocol is invoked to detect the ongoing malicious activities. As stated in [13] the destination nodes are instructed to send a signed acknowledgement on successful receiving of a packet, the acknowledgement consists of unique identifier combined with the address of destination node. In special case [14] the data sender will send a probe message requesting acknowledgment from all the intermediate nodes as specified in a list, the list consists of address of all the intermediate node and at the last entry of the list is the address of the destination.

These acknowledgement are encrypted using the key which is shared between the sender and the intermediate nodes. In [15] a multi-path based protocol is stated in which cryptography key management system is used where servers and authority nodes are involved. In Secure Ad hoc on demand distance vector SAODV [16] digital signature along with hash chaining method is used to secure the routing message along the propagation path.
Gray hole attack is kind of dropping packet attack which takes place along the data path, in which the malicious nodes will behave truthful during path discovery phase after that it act as malicious node at the time of data transfer it will drop packets silently [17] which is very difficult to determine. The uncertain and unpredicted are the advantages of gray-hole attack. A abnormal scenario of gray hole attack is where a node will behave as malicious node for some defined amount of time after which it will switch to normal node, in the malicious behavior the node will silently drops packets [18] which makes the situation more critical that detection is impossible or difficult. Some of the common attack based on routing in MANETs [19] are as follows;

- Denial of service attacks, which affect the routing function.
- Attack the routing table by flooding it as the result the routing table overflows and become in consistent.
- Induces false information and consumes the valuable resources like battery, bandwidth.

The Friend-Based Ad Hoc Routing Using Challenges (FACES) is proposed in [21, 22]. This method functions by sending a challenges and a shared friend lists. The list consists of trusted nodes in the network and the list is shared among the nodes that is used for forwarding packets. In this method the node will send a challenge to facilitate authentication of nodes, the nodes that successfully gone through the authentication fill be added to the friends list and this list is shared with its nearby node the security of the list depends on the authentication procedure and there is a possibility to make replay attack . A Light-weight trust-based routing protocol [23] is used to detect the intrusion based on the trust value that are shared with node in a network. This method consider only the packet forwarding behavior of a node that is used as a trust value. The nodes independently executes the protocol by only considering the local information so the name Light Weight, but it don’t consider the other parameters like malicious activity of the nodes.

B. Legacy Based systems:

1) Public Key Based System:

The system that make use of public key cryptosystem to handle selfishness of the node in which source routing is used. The packet consists of data, source routing information and a sequence number, these three values are find a hash value that act as digital signature for that particular packet [24]. Each intermediate node receiving the packet will compute the digital signature and append this with the pervious digital signature so that the receiver will conform that packet is not altered all along the path. This scheme depends on the public key distribution of keys and management of keys, which may be energy consuming task for small mobile devices.

2) Threshold cryptography:

This depends on the public-private key pair mechanism. A server node is elected inside the network or a server is assigned by the network designer and all other nodes have to trust the server. The server node act as a registry to store the public key of other nodes. The request and response message are signed based on the private key, the nodes can request the public key from server thus the communication become private. If a node changes the public-private key pair the new key is broadcasted or send to the server. This protocol is well adopted for distributed environment. The idea first appeared in [25] in which k secret key is split into n shares based k\(\times\)n. The combination of k component will generate a valid signature, the k-1 or lesser number of key component cannot make a valid signature.

The utilization of threshold cryptography is proposed in [26]. In this method the trust is distributed in the ad-hoc network. A distributed certification authority is used to resolve the barrier faced by key distribution method like distribution, revoking and the storage of key [27]. The Certification Authority are assigned among the nodes in the network.

3) Hierarchical Public Key Infrastructure(PKI):

In this scheme the nodes trust value are distributed along with some redundant information to correct the incorrect partial signatures [28, 29]. The high light of this scheme is as follows,

- Redundant information are used to recover incorrect signature.
- Each link is assigned with key which is flooded in the network.
- All connected node will uses signed wakeup call for the replay, battery attacks are eliminated.

4) Anonymous and Certificateless Public-Key Infrastructure (AC-PKI):

This method implements public-key service without the use of public-key certificate [30]. The process starts with the support of distributed private key-generation method [25] in addition it also provide defense against pinpoint attacks, which makes AC-PKI more secure.

C. Behavior Based systems:

Behavior based system are designed to prevent ad-hoc networks form misbehaving nodes and also addresses the threat arising from selfish nodes which is normal node but contravene the networking functionality
duties. To decide the behavior trust and trustworthy of the nodes are observed, the observation leads to distinguish between misbehaving and selfish nodes in the network. In [31] state that behavior based system depends on the reliability of the node, that is the based on the honest of a node. Behavior are measured in two ways, direct and indirect measurement. In direct method the node will measure the trust value of another node by itself, but in indirect method the nodes will gather the trust value which are send by its neighbor nodes as recommendation of trust.

Behavior measurement are used to decide whom to trust and to increase the trustworthy behavior of nodes. The following three goals are stated in [31] for any good behavior detection system they are as follows,

- There should be enough information to decide between trustworthy and untrustworthy entity.
- To guide any entity to behave more like trustworthy.
- To element the node that are untrustworthy from being participating in the networking functionality.

Behavior based system can be designed [32] as centralized manner or in a distributed manner.

Distribution based trust measurement: The direct, indirect trust and hybridtrust measurement are covered under distributed trust measurement [33]. The date are collected form the nodes for a specific or set events and a conclusion is drawn based on the observed values.

The event could be the measurement of number of packets forwarded to the number of packets dropped, this event can be logged, values are collected from direct neighbors and trust are calculated based on the node experience. The trust between two nodes is called as direct trust if the two node are interacting for the first time. In another case the node will receive the trust value as recommendation from its neighbor node, this is called as transitive trust or called indirect trust. A combination of two methods is called as hybrid trust.

Centralized trust measurement: In this type of approach trust agents are used by nodes, the agent are small piece of software capable of moving from one system to another by collecting information. The centralized approach consists of three phases they are as follows,

- Trust Propagation,
- Trust Aggregation and
- Trust Prediction.

Trust Propagation: The trust calculation incurs more power of the mobile nodes and also consumes more computation resources, so as to reduce the complexity of the trust revaluation the calculated trust values are propagated to the network. Consider a network of three nodes X, Y, Z and connected as shown in fig.1 in which node Y tells X about Z so node X trust Z[34,11].

![Fig. 1: Trust Propagation](image)

The propagation is multi-hop so all the nodes will get the trust details.

Trust Aggregation: The trust value is propagated through the network each node will get more number of instance of trust value, these values are aggregated to find the exact value of trust [34] [47] [48]. The nodes that are on the path of trust propagation will become of the chain of node that trust each other.

Trust Prediction: The trust prediction is performed base on the nodes present and past behavior trust value and the recommendations received from other nodes. The designer of the process should be careful in determine the false positive and false negative values.

1) **Watchdog algorithm:**

This paper deals with the behaviour related to non-forwarding of data by a node in ad hoc network [35]. In this method tow mechanisms are propose to handle with selfishness they are watchdog and Pathrater. The watchdog mechanism works like DSR routing where passive acknowledgement are used, the forwarding nodes will have a buffer where packets are stored, the node can use passive acknowledgement to determine whether the node has forwarded the packet or not.

If the packets are stayed in the buffer for some amount of time without acknowledged than a failure count for that node is incremented by one. In the case of increased failure count above the threshold the node will intimate the source node about the selfishness of the node.

The algorithm pathrater mechanism functions along with the source routing protocol. Each node is assigned with a null rating value as 0.5, the nodes are discovered while performing source routing. The ratings value for a node are incremented by 0.01 up to 0.8 at regular interval if the route is stable or there is no link breakage. If the node receives the error message about the link breakage the rating of the node is decremented by .05 which can be either upstream or downstream. On the reception of selfish node the rating is assigned with a negative value. The negative value is slowly incremented or reset to zero after a particular time period. Some node may have
multiple paths so the same destination, so in this situation the node will take the average value of all the path value for rating.

2) **Confidant Protocol:**

This is dynamic ad hoc network protocol which has different versions as stated in [36] [37] [38] [39]. The older system uses the passive observation to detect the packet forward nature of any node. Bayesian theory is used to update the value of the observation on a node. The past and present behavior are used to assign the weight values while calculating the behavior values. The behavior value is compared with a defined threshold and if the calculated value goes up the node is a malicious node.

A main advantages of this method is that a node will reject a neighbor’s recorded value of another node if the value is different from its own recording. The node will decided the trust value of another node based on the trust value stored in the trust table. A node increments the trust value if the received information is same as the nodes own value, or else the value is decremented. In some case the agents are used to exchange context information about the neighbor nodes, and consists of three operation like querying, storing and access the table of context information as described in [40]

3) **Fuzzy logical Trust:**

The accurate values can be produce by fuzzy logical trust calculation [41]. The fuzzy logic uses the value between 0 and 1 which are assigned to a variable. As in the previous method it also uses the threshold as lime indicator for the trust value, if the trust value goes up the node is not trusted. The range of value will gives different meaning like very trustworthy or very untrustworthy and medium trustworthy or medium untrustworthy.

4) **Secure and Objective based Incentive:**

As CONFIDANT this method also share the information with its one hop neighbors [42]. This method mainly focus the non-forwarding behavior of the node, it calculates the ratio of number of packets passively acknowledged to the number packet send to the node for forwarding. The ratio will be fair if the node handles more packets. Each node will send the updated value in a periodic manner or when some changes occurred.

**Other Related Discussion:**

A node will have its own behavior value of any node without interacting with its neighbors, this mechanism will leads to liar node vulnerability problem. The malicious or selfish node will tries to publish their fault information to influence the other node to have false value, this will leads to false calculation of trust value. The strategy is to mix the both misbehave and normal behavior value together distract the calculation of trust values, this is done by liar node [38]. Brain washing is one kind of liar mechanism in which a node surrounded by lying node will be forced to believe the value given by the liar nodes. When the node moves to other area which may surrounded by honest node than the node will start to believe the honest nodes value since the value are of in larger deviation. A habit of liar node is that it will tell the other node correct value for a certain period of time so that is gain the trust of other nodes and after which it starts to tell lies, this is called as intoxication. A strange behavior hide and seek is played by some nodes, in which the node will appear using an identity at one time and disappears all of sudden before reappearance with different identification (Node ID), this is stated as identity spoofing [43]

The second hand (indirect observation) information is useful to estimate the accurate value for behavior in faster manner [43]. The second hand information are obtained after performing the deviation test, if the values are not too deviated than it’s accepted if not it is discarded. In this method two registers are use one to record the positive value and another for negative value. Network-level security can be increase using a monitoring system which will monitors the node continuously. The monitoring system are a small agent that are attached to all the nodes in the network [44]. An overview of the monitoring system is present here, it consists of two functions one is monitoring the security of node and the second one is monitoring the network security. The system model consists of Measurement Entity (ME), Voting Entity is attached to group of trusted nodes. The ME is a repository which consists of observed entity along with the metric and metric calculating methods, and metric limits if any. The VE is contains the same information as that of ME, but it act as organizer role in voting process. The process is show in listing of Monitoring System.

**Step 1:** IF ME detects suspicious activity in the neighboring node.
**Step 2:** Report it all VE about the FINDING.
**Step 3:** Report all ME about the FINDING by VE.
**Step 4:** MEs report the suspected nodes observation to VE.
**Step 5:** VE aggregate the result send to Monitoring system.
**Step 6:** Monitoring system take countermeasure based on the voting result.
**Step 7:** In validate the node using Node ID or IP address of the node.
In on demand routing if the route request reaches the group of attackers, than to route requester will be landed inside the attackers group [45]. If some malicious node takes control of any functionality of the network or node it may distract the honesty collaborative functionality of the network this type of attack become more critical if the network has no centralized co-ordinates [46]. Some of the complex attack are discussed in [43] and [44] in which a resource exhaustion happens. The attacker will select some node and continuously sends packets, forcing it to do work so that it will consume more energy and avoid the node to go to sleep node.

Conclusion:
In this paper, we surveyed many trust schemes based on MANTEs to provide security based on trust values. The trust values are calculated based on many methods by using the value obtained by direct or indirect method. Each method will some provide some limitation and advantage but the in many situation node level security is provided to a secure version of protocol. Some attacks are discussed to provide insight for design security algorithms.

REFERENCES