Review: Trust management in MANETs

Savita Semplay, Rajni Sobti and Veenu Mangat
Panjab University, UIET
sobtirajni@yahoo.com veenu.mangat@yahoo.com er.savi03@yahoo.com

Abstract
Mobile Ad hoc Wireless Networks (MANET) is an infrastructure less, self organized, and multi hop network. MANET is autonomous system in which nodes have to act as host and as routers. So, for packet forwarding, nodes rely on cooperation of its neighbor nodes. Cooperation of nodes depends on the trust of the node who is participating in network. Trust management becomes very important for the successful operation of MANET. This paper focus on trust management in MANET which includes properties of trust and different trust management metrics required for MANET.

Keywords - Trust, Trust management, Properties, Metrics.

INTRODUCTION
A mobile ad hoc network (MANETs) is an autonomous system which consists of a loosely connected set of MANETs nodes and can be implemented by using various techniques like Bluetooth or WLAN for example. In MANETs, has autonomous in behavior due to each node act as both host and router. MANETs nodes does not have a centralized administration mechanism thus each node act as a "router" for forwarding the traffic to other individual node in the network. It is an infrastructureless in which network of mobile and wireless machine nodes connected with radio shown in fig 1. These networks can be set up at any place and time. These networks work without any pre-existing infrastructure. MANETs is a system of mobile nodes (and associated hosts) connected by wireless links where nodes are organize and maintain a routing structure among themselves and move randomly; thus, it has dynamic topology which may change rapidly and unpredictably. Such a network may be connected to the larger Internet.

Mobile ad hoc networks (MANETs) have neither fixed communication infrastructure nor any base stations (BSs) MANET has peer-to-peer multihop mobile wireless networks and comprises a set of wireless devices; does not require a fixed infrastructure or centralized administration. Because mobile nodes have limited transmission range, distant nodes communicate through multihop paths. Their ease of deployment makes MANETs an attractive choice for a variety of applications. MANET’s topologies changes frequently because of no cellular infrastructure.

MANETs has multi-hop wireless links in which host’s move frequently see in fig 2.
An ad-hoc network is a LAN or other small network, particularly with wireless connections, in which some of the network devices are part of the network only for the period of a communications session.

Major features of MANETS
- Rely on Infrastructureless.
- No Availability of Central Authority.
- Dynamic Topology
- Application Specific
- Physical protection of computers

b) Type of MANETs
There are different types of MANETs including:
- In MANETs (Intelligent vehicular ad hoc networks):- which is generally used for tracking unexpected situations using artificial intelligence like for example vehicle accidents and vehicle collision.
- Vehicular ad hoc networks (VANETs) – Enables efficient communication with another vehicle
- Internet Based Mobile Ad hoc Networks (iMANET) – mainly used for linking mobile nodes.
A mobile ad hoc network (MANET) does not have a centralized infrastructure and it form a temporary network where nodes communicate through multi-hops.

Due to the characteristic of MANETs, trust management is required for nodes who want to participate as to provide an acceptable level of trust relationships among themselves.

Trust management in MANET is extremely challenging than in traditional centralized environments due to dynamic nature and characteristics of MANETs which creates difficulty due to change in topology and result in uncertainty and incompleteness.

Trust management in MANETs is desired when a participating Nodes wants a communication session and establish a network with satisfactory level of trust among themselves, without any previous interactions.

The rest of this paper is organized as follows. In section 2, we generally describe the characteristic and challenges of MANETs. We also introduce the main application of MANETs in section 3.

Section 4 surveys general introduction of Trust management in MANETs and why Trust management is required in MANETs, Trust management definition and interesting type of trust. In Section 5 we also introduce the main properties of trust in MANETs. In section 6, we discuss metrics used to measure the performance of existing MANETs trust management schemes. Section 7 concludes this paper.

CHARACTERISTIC AND CHALLENGES

Mobile Adhoc Network (MANET) is used to provide communication to each other nodes via radio waves, having collection of autonomous mobile nodes. The mobile nodes can directly communicate with each other in radio range.

MANETs have several significant characteristics and challenges. They are as follows:

- **Dynamic topologies:**
  MANET is an infrastructureless and networks are fully distributed which can work at any place without any need of infrastructure. So they are highly flexible and robust. The mobile devices are heavily depend on other hosts and resources for data access because of limited storage and low computational capabilities. A trustworthy network topology must be guaranteed through efficient and secure routing protocols for Ad Hoc networks. Frequent routing updates due to dynamic nature and characteristic in MANET.

- **Bandwidth-constrained, variable capacity links:**
  Wireless links considerably have lower capacity than their hardwired counterparts. Interference conditions, fading, noise, is frequently much less than a radio’s maximum transmission rate.

- **Energy-constrained operation and Limited battery life:**
  In a MANET all of the nodes may rely on batteries. Higher Packet losses due to errors in transmission such as hidden terminals that results in collisions, interference, frequent breakage in paths caused by mobility of nodes, increased collisions.

- **Limited physical security:**
  MANET does not provide a physical protection of computers due to Limited resources, generally more prone to physical security threats than fixed-cable nets. The increased risk of eavesdropping, spoofing, selfish behavior and denial-of-service attacks should be suspiciously considered.

APPLICATIONS

Ad hoc networking allows the devices to retain connections to the network as well as straightforwardly adding and removing devices to and from the network. The set of applications for MANETs is diverse that ranges from traditional infrastructure environment into the ad hoc context. They are as follows:

- **Inter-vehicle communications:**
  It is that area of high level of mobility where ad hoc networks could really change its way to communicate with professional mobile as well as those who covers personal vehicles and no conventional (i.e. wired) solutions takes place.

- **Mine site operations:**
  There would no base station approach work for communication, it must be accomplished using nodes that are part of network in MANETs if we consider surrounding, say mines for example.

- **Automotive Applications:**
  **Automotive networks are broadly discussed**
  Currently due to this the network will provide information to the car drivers about accident-ahead warnings, congestions, helping to optimize traffic flow abot road conditions. Cars should be enabled to talk to the road, to traffic lights, and others, forming ad hoc networks of various sizes.

- **Military battlefield:**
  These provide robust and reliable communication in many forms. Most of the communication devices are installed in mobile vehicles, tanks etc. soldiers could carry these telecomm devices so that they could talk directly to other telecomm devices within the radio range and these type of communication are considered to be primitive.

TRUST MANAGEMENT IN MANETS

The notion of “Trust” is derived from social science which means reliance on another person or entity.

- Trust Management acts as a separate component of security services in networks and identified it as a unified approach.
- Trust management is used to specify and interpret security policies and relationships.

There are 2 interesting type of trust are:

- A context independent reliability
- Decision trust

Trust management includes trust establishment, trust update and trust revocation. While trust management and trust establishment are interchangeably used with reputation management but have slight difference between them.
Trust is active while reputation is passive.

Trust establishment is defined as the process of maintaining and distributing trust among nodes. While Trust management shown in fig 3, has no such infrastructure and used to deal with complex problems and manages the trust relationship among nodes.

Fig 3. Shows the main classifications of trust management system. Trust establishment includes the trust evidence, collection, trust generation and trust distribution, trust discovery and trust evaluations.

Trust in MANET should be established in a self-organized reconfiguration way. Trust management has a dynamic nature not static; defined as the degree of subjective belief about the behaviour of a particular entity.

Trust management is required for authentication purposes. Mainly there are two schemes used to evaluate trust

- Policy based trust management
- Reputation bases trust management

Policy based trust management takes binary decision and is less flexible than reputation bases trust management. Binary decision can be taken according to which request is allowed or not.

**TRUST PROPERTIES IN MANETS**

The most important properties of trust in MANET are as follows (shown in fig 4):

- **Dynamicity:** Trust in MANET is of dynamic nature, not static due to the dynamic topology, informations are either changed or incomplete. In order to capture dynamicity of trust, trust should be in binary or even discrete valued entity which represent certainty. It should be expressed in continuous variable.

- **Subjective:** In MANET, trust is subjective. Due to the dynamic network topology and have different experiences with the node, different level of trust may be determined by a trustor node against the same trustee node.

**Incomplete transitivity**
There is no necessarily transitivity of trust among two entities to third party like for example, if bob trust alice, and alice trust smir, it does not guarantee that bob also trusts smir. To use transitivity in MANET, two types of trust should be maintained by a trustor: trust in a trustee and in the trustee’s recommendation of the third party.

**Context- dependency**
In MANET, different type of trust is desired depending on a given task (for example: trust is reporting, trust in high capability, trust is computational power).

**Asymmetry**
In MANETs, trust is asymmetric means nodes having low capability may trust nodes with high capability but at the same level reciprocal is not necessarily.

Fig 5. Shows several trust properties in trust management schemes in MANET. In this figure dynamicy and weighted transitivity are frequently considered, however, some represent trust as symmetric or other as discrete variable and some not even consider as trust properly.

Trust is completely transitive as they do not capture the properties or characteristics of trust in MANET.

Trust should be fully-distributed and determined in a highly customizable way.
There could not have further work that includes all these five properties of trust shown in fig 5.

**METRICS FOR MANETS TRUST MANAGEMENT**

A trust metric has the following characteristics:

- Trust should be established based on potential risks;
- Trust should be context-dependent;
- Trust should be based on each party’s own interest (e.g., selfishness);
- Trust is learned (i.e., a cognitive process); and
- Trust may represent system reliability.

In MANETs there are many trust management schemes to evaluate trust values but no such clear parameters to evaluate network trust.

Liu et al. [2] defined trust in their model as reliability, timeliness, and integrity of message delivery to the intended next-hop. Also most trust-based protocols for secure routing calculated trust values based on the characteristics of nodes behaving properly at the network layer. Trust measurement can be application dependent and will be different based on the design goals of proposed schemes.

Conclusions:

Trust between is very important for proper operation of MANETS. Various issues for future trust management in MANETs like

- Does the trust metric used reflect the unique properties of trust in MANETs?
- How does the trust metric contribute for improving scalability, reconﬁgurability, and reliability of the proposed network?
- Does volatile network topology makes it easy to detect malicious nodes and provide physical security.

For future work we propose using of cooperation method with trust management in MANETs for computing trust value and provide security from unauthorized or malicious nodes.

**REFERENCES**
