Volume 3, Issue 6, June 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Trust Based Theoretical Framework for Mobile Ad-Hoc Networks

Arvind Sharma, Dr. Neeraj Kumar
CSE Dept, Thapar University, Patiala
Punjab, India

Abstract:- A mobile ad-hoc network (MANETs) consists of mobile nodes that collaborate with each other using wireless link to route both data and control packets. They are basically characterized by the use of dynamically changing topology, decentralized routing mechanism and lack of existing infrastructure. MANETs can work correctly if participating nodes cooperate in routing. In this paper we propose a new approach based on trust relationship among the nodes which makes them to cooperate in a wireless environment. This trust framework is used to identifying malicious behaviour of nodes in MANETs.

Keywords: - AODV, DSR, MANETs, Grudger Protocol.

I. INTRODUCTION

MANETs are example of wireless mobile communication. In MANETs, mobile nodes are dynamic and arbitrarily stationed in such a manner that communication between nodes does not rely on any existing network infrastructure. The nodes in the MANETs are basically moveable mobile devices with resource limitations like power, computation ability and storage capacity. Moreover, there is not availability of existing infrastructure or centralized authentication, these networks are self-organized and source to destination communication may require routing information via several intermediate nodes. In MANETs, a node has to rely on neighbour nodes to route a packet to the destination node due to the lack of infrastructure and the limited transmission range of a node. However, all network functions are based on the nodes mutual effort. There are most widely used routing protocols for MANETs, such Ad hoc On Demand Distance Vector Routing Protocol (AODV) [1] and as Dynamic Source Routing (DSR) [2]. These protocols are based on the assumption that all nodes will have to cooperate. In MANETs, no route can be established; no packet can be forwarded without nodes cooperation. However, collaborative behaviour, such as forwarding other node messages, cannot be taken for awarded. We can identify two types of uncooperative nodes: malicious and selfish. Malicious behaviour refers to the broad class of misbehaviour in which nodes are either faulty and therefore cannot follow a protocol and intentionally try to attack the system. Selfishness refers to non-cooperation in certain network operations. In MANETs, both malicious nodes and selfish nodes are mischievous nodes, which may affect the performance of the network severely. Due to the ad hoc nature of MANETs, accomplish cooperation in such networks is one of the challenging issues. There are unique characteristics of MANETs that raise certain requirements for the security mechanism.

There is un-accessibility to trusted authorities that makes traditional security methods and system insufficient for application in MANETs because of open structure, absence of existing infrastructure. This type of problem faced with the presence of malicious nodes in MANETs. So, requires a trust based algorithm to mitigate the effect of such nodes. In Trust based routing, to allow an unknown node to forward data, nodes perform a trust-based decision. Trust is a well-known sociological concept that humans on a daily basis base decision on and also it is the abrupt level that one node in network can put on another node for a specific action based on direct or indirect observations on behaviour of that node [3]. The incorporation of trust with existing protocol makes detection of untrustworthy nodes and takes trust based route selection strategies for ad hoc routing protocols and thereby increase the effectiveness of the network. Trust based solutions provide a method to select neighbours based on their trust value which is derived from previous interactions. So, we proposed novel model that may select a misbehaving node, we also propose a generic trust evaluation mechanism to alleviate this problem. We introduce the concept of real-time trust formation, which continually evaluates trust value during an interaction and allows interaction to terminate if the selected node misbehaves, with a strong bias towards recently observed behaviour.

1.2 Security Issues in MANETs:-

In addition to availability, confidentiality, integrity, authentication, access control and non-repudiation, the mobile ad hoc networks also raise the following issues.

In MANETs, a mobile node has some limitations with respect to bandwidth, computing power, and battery power that can lead to application-specific trade-offs between security and resource consumption of the mobile device. However, to do this intermediate node achieves no benefits. So there may be a possibility that some nodes refuse to forward packets and thereby decrease the efficiency of the network in term of throughput and packet delivery ratio. A selfish node may try to save their resources like battery power and computation ability by not participation in forwarding messages [4]. With increasing the number of selfish nodes, there may be result of making a non-collaboration environment between other nodes. The well-behaved nodes will be affected in addition to exploiting their resources.

However, the route advertisement by mobile nodes should be real idea of the topology of the network. Malicious nodes can draw attention to themselves by means of false routing advertisements. The fake route that exhibits properties of good routes is preferred over real routes and put in to route cache for long time. The routing information itself can be equally important rather than the Message content itself in a military application. The traceability of nodes, both a physical location and the tracking down of a node identity based on its routing traffic is also an important issue to be considered. This security issues are to be considered in MANETS because of its characteristics like vulnerability of channels, nodes, absence of infrastructure and dynamically changing topology.

1.3 Security Attack's in MANETs

In this paper, we are concerned with the attacks on the routing schemes. Any attack on ad hoc networks can be categorized as active and passive attacks. In an active attack, the misbehaving node actively disturbs the normal operation of the network while in a passive attack the malicious entity only listens to the traffic without disturbing the network [5]. In this section, we present the attacks using modification, impersonation and fabrication. In the attacks using modification the malicious node announces better routes than the other nodes in order to be inserted in the ad-hoc network by changing the route sequence number, modified hop count. In the attacks using impersonation the malicious nodes usurps the identity of another node by spooling MAC address of other nodes. In the attacks using fabrication the malicious node generates traffic to disturb the good operation of an ad-hoc network, by routing disruption like falsifying route error messages, corrupting routing state, routing table overflow attack, replay attack and black hole. In *Routing loops*, a malicious node may modify routing packets in such a way that the packets traverse in a cyclic manner, so that the packet does not reach the intended destination [6]. A *black hole attack* is used by a malicious node which makes all the traffic travel through it by claiming to have the shortest route to all other nodes in the network [6]. However, instead of forwarding the packets, the malicious node simply drops it. A special case of black hole attack is g*ray hole* attack in which a malicious node may selectively drop packets, [7]. Other attacks towards MANETs include partitioning and replay attacks. Replay attacks are attacks where the attacker replays the already sent packets to the network. If some reply route requests are replayed, the obsolete information may get stored in the routing table which might course some nodes to be unreachable. Moreover, *worm hole attack* is another variant of reply attack in which a group of cooperating malicious nodes can pretend to connect two distant points in the network with a low-latency communication link called wormhole link, causing interruption in normal traffic load and flow [8]. All of the problems presented in this section can severely harm the network. This may reduce the efficiency of the network and the network will function in a suboptimal way. Hence, new routing schemes will have to be devised, taking all the above problems into considerations. Some of the related works and new secure routing schemes that are being developed are analyzed in the following sections.

The remainder of this paper is organized as follows. Related work is discussed in Section 2 followed by a description of the proposed Trust framework in Section 3. Conclusions and future work are outlined in Section 4.

II. RELATED WORK

Trust is an important aspect of MANETs. In wireless environment, Trust computations and management are highly disputed issues in wireless environment because of various mobile device constraints, and the arbitrary movement of mobile nodes. So, there is no direct application of techniques that fits MANETs. In MANETs, an untrustworthy node in network may causes for damage and unfavourable affect the quality and reliability of data. Therefore, trust based routing; analysis the trust value of a node has a positive influence on the confidence with which one node may perform data or control transactions with other node. In this work we present a detailed survey on various trust computing approaches that are aimed towards MANETs. Marti et al. [9] proposed a scheme called *watchdog and pathrator* for routing misbehaviour mitigation. In this scheme, every node has a Watchdog process that monitors the direct neighbours by promiscuously listening to their transmission. No penalty for the malicious nodes is awarded. Buchegger et al. [10] proposed the *Cooperation of Nodes: Fairness in Dynamic Ad hoc Networks (CONFIDANT*) is an extension to DSR. This scheme determines trust based on both direct and indirect observations and behaviour of nodes. However, this scheme also able to detect mischievous nodes. Moreover, the important aspect of this work is bonus scheme for nodes that participate in faithful participation. Michirardi et al. [11] proposed the scheme called "A collaborative reputation mechanism to encode node cooperation in mobile ad-hoc networks (CORE)". This scheme differentiates the selfish node and malicious node. In MANETs, the nodes which not cooperate with other nodes for saving battery for its own communication is called "selfish node" while these nodes does not cause of any damage for other node. The malicious node in MANET behaves mischief and can damage other nodes by doing any suspicious activity. Buchegger et al. [12][13] explained a scheme based on biological example proposed by Dawkins, which explains the survival chances of birds grooming parasites off each other's head. MANETs, grudger nodes are introduced which employ a neighbourhood watch by keeping track of what is happening to other nodes in the neighbourhood, before they have a bad experience themselves. They also share information of experienced malicious behaviour with friends and learn from them.

III. PROPOSED WORK

Many trust management schemes have been proposed to measure trust values and most of the trust-based protocols for secure routing calculated trust values based on the characteristics of mobile nodes at the network layer. Trust analysis can be application dependent and will be different based on the design goals of proposed schemes. The node trust value plays a vital role in MANET routing. Trust factor here focuses on identifying the nodes which not suitable for reliable routing and helps to select an alternate path to carry on routing successfully using reliable nodes. The proposed work

concentrates on identifying these unreliable nodes using the trust values calculated for each node. Our proposed protocol chooses the most reliable and secure path to the destination based on the trust values of other nodes.

3.1 Component of proposed protocol:

There are basically four primary components of proposed protocol:

- Initialize
- Update
- Management
- Monitor

These processes provide the foundation for the trust based routing protocol.

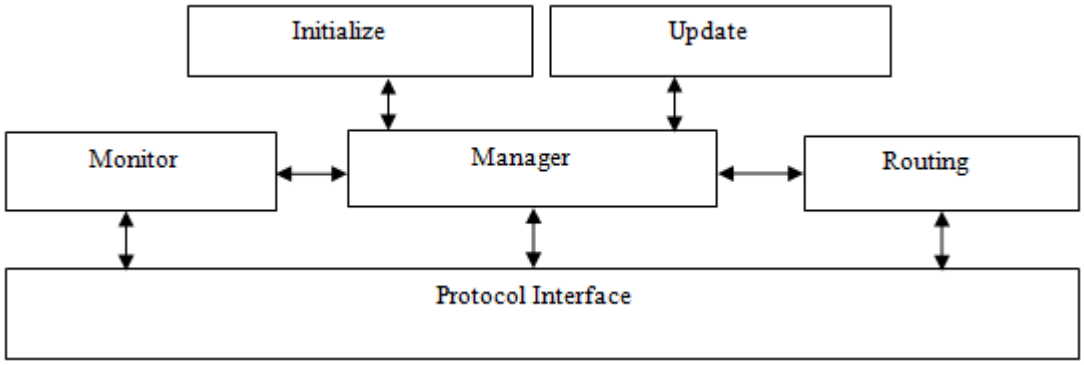

Fig.1**:** Proposed architecture

Based on the analysis, components to manage the following tasks are needed:

Initialise: This module include the functions that are used to assign initial trust value when nodes are come across the network at starting and will be encountered form Route Reply's or route are snooped. All the nodes on first route will be unknown and therefore, a default trust value of each unknown node need to be found out. In an environment with many malicious nodes, it would be best to assign a low trust value. The trust value of a known route nodes is used to base the assignment of the initial trust value for the new node.

Update: The update module of trust framework is defined functions for updating previous trust values. As defined earlier trust is subjective and depends on a given nodes experience in a given situation. So, the function designed here is aims to function in domains with several malicious nodes. A function for updating trust can depend on several parameters. In the list below some of the possible parameters are listed.

- Previous trust values.
- Lowest/Highest trust value ever assigned.
- Number of positive/negative experiences of past.
- Value of an experience in term of positive and negative Acknowledgments.

Manager: The manager module of the trust framework manages tasks like initialise, update and routing based on trust values. It also store trust values about all known nodes during run time, and it also offers functions to query for information about stored trust values. It also functions as the main interface between the existing implementation of underlying protocol and the Initialise and Update modules of present trust framework.

Routing: this module of trust framework is performing task of the route selection based on the trust value of the nodes and selects the best route based on trust evaluation. The routes are evaluated and the route with the highest rating should be used. This means that the best route will be believed as one that has the highest trust rating, which means that it has the minimum number of malicious nodes.

Monitor: This module in trust framework is used to define the mechanism that is responsible to adjust the trust values based on received acknowledgements. It is important that a missing acknowledgement discovers as soon as possible because the trust values are used on routing selecting decisions. The trust update module modifies the trust values for nodes on the stored route when an acknowledgement is received and also the trust values should be settled in a negative way when a requested acknowledgement is not received because the packet is considered dropped.

3.2. Identification of Relationships between Neighbours in an Ad Hoc Network

In an ad hoc network, the relationship of a node i to its neighbour node j can be any of the following types:

- **Node i is a stranger to neighbour node j:**
  Node i has never sent / received messages to/from node j. So, their levels of trust values between each other will be very low. Every new node entering in MANETs will be a stranger to its neighbour nodes. There may be high probability that stranger nodes behave as malicious in MANETs.
- **Node i is an acquaintance to neighbour node j:**
  Node i has sent / received few messages from node j. So, their mutual levels of trust values are neither too low nor too high to be reliable. There may be chances of malicious behaviour of nodes will have to be noticed.
- **Node i is a friend to neighbour node j:**
  Node i has sent/received plenty of messages to/from node j. The trust levels between them are reasonably high. Probability of misbehaving nodes may be very less.

The above relationships are represented as a Friendship table in each node of an ad hoc network. Consider the node 1 in Fig 2. The friendship table of node 1 is represented as shown in Table 1. A trust estimator is used in each node to evaluate the trust level of its neighbouring nodes. The trust level is a function of various parameters like length of the association, ratio of the number of packets forwarded successfully by the neighbour to the total number of packets sent to that neighbour, ratio of number of packets received intact from the neighbour to the total number of received packets from that node and average time taken to respond to a route request.

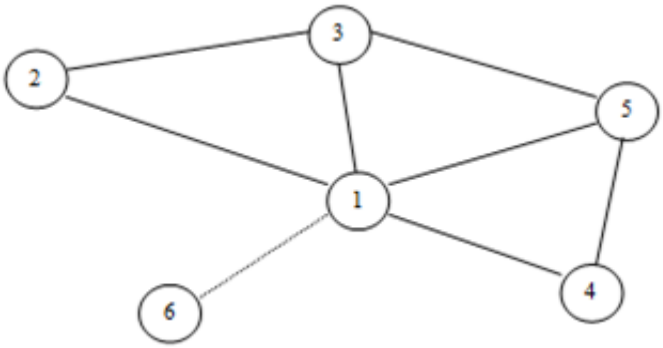

Fig.2: Nodes in MANETs

Table 1: Relationship Table of Node 1

Neighbour Nodes	Relationship
2	F
3	F
4	A
5	F
6	S

The threshold trust level for a stranger node to become an acquaintance to its neighbour is represented by T_{acq} and the threshold trust level for an acquaintance node to become a friend of its neighbour is denoted by T_{fri}. The relationships are represented as:

$$R_{i \rightarrow j} = F \text{ when } T \geq T_{fri}$$
$$R_{i \rightarrow j} = A \text{ when } T \leq T_{acq} < T_{fri}$$
$$R_{i \rightarrow j} = S \text{ when } 0 < T < T_{acq}$$

The relationship between nodes is asymmetric, i.e. $R_{i \rightarrow j}$ is a relationship evaluated by node i based on trust levels calculated for its neighbour node j. Also, $R_{j \rightarrow i}$ is the relationship from the friendship table of node j. This is evaluated based on the trust levels assigned for its neighbour node i. Asymmetric relationships suggest that the direction of data flow may be more in one direction. In other words, node i may not have trust on node j the same way as node j has trust on node i or vice versa.

3.3. Routing Mechanism

When any node in MANETs wants to send messages to a destination node, it first spoofed route cache of the source node. If any route to destination available in cache then is selects that route to send packets. However, if there is not any route available in route cache then it sends the ROUTE REQUEST to all the neighbouring nodes in the network. The ROUTE REPLY obtained from its neighbour is sorted by trust ratings. This means that high trust value node should be selected. The source selects the most trusted path. If it's one hop neighbour node is a friend, then that path is chosen for message transfer. If its one-hop neighbour node is an acquaintance, and if the one hop neighbour of the second best path is a friend choose F. Similarly an optimal path is chosen based on the degree of friendship existing between the neighbour nodes.

Table 2: Path Chosen Based on Proposed Scheme

Next hope neighbour in best path P1	F	F	A	A	S
Next hope neighbour in best path P1	A	F	F	S	F

The source selects the shortest and the next shortest path. Whenever a neighbouring node is a friend, the message transfer is done immediately. This eliminates the overhead of invoking the trust formation between friends. If it is an acquaintance or stranger, transfer is done based on the ratings.

IV. CONCLUSION AND FUTURE WORK

In this paper we have covered the basic traits of MANETS. We have also analyzed the different types of issues and attacks in MANETs. It also exhibits new vulnerabilities to malicious attacks or lack of co-operation. Trust based mechanism includes the notion of friends, acquaintances and strangers. This proposed scheme of trust based routing increase the security level and also straight the nodes cooperation. This framework also determines and isolates the malicious node from routing and data forwarding. For the purpose of simulation, we have assumed forwarding defection as the only possible misbehaviour. The next step is to do simulation based performance analysis of trust framework on the existing protocol like AODV and DSR by introducing possible attacks. Further improvement in the protocol is to be done by changes in the broad category of relationships used. Future work will be to evaluate and incorporate suitable solutions in the extended trusted framework based protocol.

References

[1] C. Perkins, E. Royer and S. Das, "Ad hoc on-demand distance vector routing", RFC-3651, Jul. 2003.

[2] D. Johnson, D. Maltz, Y. Hu, and J. Jetcheva, "Dynamic Source Routing Protocol for mobile Ad hoc Networks", Internet Draft, Internet Engineering Task Force, Mar. 2001.

[3] J. Li, R. Li, and J. Kato, "Future Trust Management Framework for Mobile Ad- Hoc Networks:Security in Mobile Ad Hoc Networks," *IEEE Commun. Mag.*, vol. 46, no. 4,pp. 108-114, Apr. 2008.

[4] B. Ishibashi, R. Boutaba, "Topology and mobility considerations in mobile ad hoc networks," *Ad Hoc Netw. J.*, vol. 3, no. 6, pp. 762-776, Nov. 2005.

[5] S. Murphy, "Routing Protocol Threat Analysis" Internet Draft, draft Murphy-threat-0. txt,October 2002.

[6] P. Papadimitratos, Z. J. Haas, "Securing the Internet Routing Infrastructure" EEE Communications, vol. 10, no. 40, pp. 60-68, October 2002.

[7] Ernesto J Caballero, "Vulnerabilities of Intrusion Detection Systems in Mobile Ad-hoc Networks–The routing problem" TKK T-110.

[8] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet Leashes: A Defence against Wormhole Attacks in Wireless Ad hoc Networks," Proc. 22nd Annual Joint Conf. IEEE Computer and Communications Societies (Infocom'03), San Francisco, CA, April 2003.

[9] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad Hoc Networks," Proc. 6th Annual ACM/IEEE Mobile Computing and Networking,Boston, MA, Aug. 2000, pp.255-265.

[10] S. Buchegger and J. Y. Le Boudec, "Performance Analysis of the Cooperation Of Nodes Fairness In Dynamic Ad-hoc Networks (CONFIDANT)," *Proc. 3rd IEEE/ACM* Symposium on Mobile Ad Hoc Networking and Computing, Lausanne, CH, pp. 226-236, June 2002.

[11] Michirardi, P., Molva, R. 2002. "Core: A collaborative reputation mechanism to encode node cooperation in mobile ad-hoc networks", in CMS'02 Communication and Multimedia Security Conference.

[12] Richard Dawkins. The selfish Gene., Oxford University press, 1980 edition, 1976.

[13] Sonja Buchegger and Jean-Yves Le Boudec. Nodes Bearing Grudges: "Towards Routing Security, Fairness and robustness in Mobile ad hoc networks". In proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network–based processing, Pages 403– 410. Canary Islands, Spain. January 2002.

