International Journal on Applications in Engineering and Technology
Volume 2: Issue 4: April 2016, pp17- 20. www.aetsjournal.com ISSN (Online) : 2455 - 0523

A Survey On Trust Based Routing Mechanisms In MANETs

R.Vijayakumar , R.Shruthi , Dr.K.R.Shankar Kumar

Abstract— Mobile Adhoc networks are type of wireless network which are infrastructure less, self organizing highly mobile and quickly deployable. There is no central authority the communication occurs hop by hop based on cooperation among the nodes. Trust is evaluated on the basis of observation, experience and knowledge. The dynamic nature and characterteristics of MANETs often result in uncertainty and incompleteness of the trust evidence, which is continously changing over the time. Trust computation and management are quite challenging issues. This paper elucidates the comparison between these protocols based on the trust mechanisms, mertis and demerits.

Keywords - MANET,Trust Management,Routing,Protocols

I. INTRODUCTION

MANET is a self-configuring system of mobile nodes connected by wireless links which contains a network area with nodes. It is a group of mobile devices communicating through a wireless medium. Mobile ad hoc network does not rely upon any fixed support infrastructure. Each node in the network must be able to take care of routing of the data and can discover multi-hop paths. Routing is the act of moving information across an network from source to destination through intermediate nodes. The routing protocol can be categorized into three types based on topology. They are i) Proactive routing protocol ii) Reactive routing protocol iii) Hybrid routing protocol. The proactive or table driven routing protocols maintain routing information of all nodes in the network. Each node maintains information of other nodes in the routing tables and regularly updates information when node moves. A reactive or on-demand routing protocol does not maintain any update information instead when a route is desired a procedure is invoked find route to reach destination. Reactive protocol minimizes the network traffic overhead.

II. TRUST MANAGEMENT

'Trust' is one of the most complex concepts in social relationships, which is also an abstract psychological cognitive process. The concept of 'trust' is introduced in MANETs to measure an expectation or uncertainty that an entity has about another's future behaviors. Trust based source routing in Mobile Ad-hoc Network (MANETs) presents a dynamic trust prediction model to evaluate the trustworthiness of nodes, which is based on the nodes historical behaviors, as well as future behaviors through extended fuzzy logic rules prediction. Trust prediction mechanisms allow a node to evaluate trustworthiness of other nodes, which not only help in malicious node detection, but also improve network security performance and robustness. The mobile nodes can know whether and how much they can trust other mobile nodes with help of trust mechanisms.

Trust management, including trust establishment, trustupdate, and trust revocation is much more challenging inMANETs than in traditional wired environments. Forexample, collecting trust information or evidence toevaluate trustworthiness is difficult due to dynamicchanges in network topology induced by node mobility ornode failure. Further, resource constraints often confinethe trust evaluation process only to local information.Trust mechanism is incorporated in the routing protocolsto provide security in MANET against different attackssuch as blackhole, wormhole, selfish attack, DoS attacksetc. Trust is a value that is computed on the basis of nodes'action or behavior. Trust can be implemented in variousways such as reputation, subjective logic from opinion ofneeds, probabilistic value etc as there are no particulardefinition of trust. Following are the properties that trustmetric should exhibit:Trust is dynamic that changes with time, locationetc. MANET has dynamic changing topologyand highly mobile so the trust value should bebased on temporary and local information.

- Trust is context dependent i.e. its value dependson the task given to a node, it may be high forone task but same node may have lower trustvalue for other task
- Trust is asymmetric, it means that if a node Atrusts a node B then there is no guarantee that node B also trusts node A in return.
- Trust is subjective; the node may have differenttrust values for the same node in different situations due to changing network topology.
- Trust is a composite value i.e., the trust values obtained from different sources canbeaggregated to get a single value with differentweight values to each. This combined trust valueis more accurate than individual values.

III. TRUST BASED ROUTING PROTOCOL IN MANETS

1) AODV

Ad-hoc on-demand distance-vector routing protocol uses an on demand approach for finding routes. A route is established only when it is required by a source node for

R.Vijayakumar , Assistant Professor CSE, Sri Ramakrishna Engineering College, Coimbatore
R.Shruthi , Assistant Professor CSE, Sri Ramakrishna Engineering College, Coimbatore
Dr.K.R.Shankar Kumar, Professor ECE , Rangananthan Engineering College, Coimbatore

transmitting data packets. It employs destination sequence numbers to identify the most recent path. The source node and the intermediate node store the next-hop information corresponding to each flow for data packet transmission. In an on-demand routing protocol, the source node floods the routereq packet in the network when a route is not available for the desired destination.

2) DSR

Dynamic source routing protocol (DSR) is an on-demand routing protocol designed to restrict the bandwidth consumed by control packets in ad hoc wireless networks by eliminating the periodic table-update messages required in the table-driven approach. The basic approach in DSR protocol during the route construction phase is to establish a route by flooding routereq packets in the network. The destination node, on receiving a routereq packet, responds by sending arouterep packet back to the source, which carries the route traversed by the routereq packet received.

3) DSDV

Destination-Sequenced Distance Vector (DSDV) routing protocol is a pro-active, table-driven routing protocol. Every node will maintain a table listing all the other nodes it has known either directly or through some neighbors. Every node has a single entry in the routing table. The entry will have information about the node's IP address, last known sequence number and the hop count to reach that node. Along with these details the table also keeps track of the nexthop neighbor to reach the destination node, the timestamp of the last update received for that node. The DSDV update message consists of three fields, Destination Address, Sequence Number and Hop Count. Each node uses two mechanisms to send out the DSDV updates, they are periodic updates and trigger updates.Updation in table and sequence number leads toprevent problem like loops and count to infinityproblem. In this mechanism, routes to alldestinations are readily available at every nodeat all times. The tables are exchanged between neighbors at regular intervals to keep up-to-date view of the network. Neighbor node use missing transmissions to detect broken links in the topology. When a broken link is found, it is assigned a metric value of infinity and the node that detected broken link broadcasted an update packet, to inform others that the link is chosen.

4) SEAD

Secure Efficient Ad-hoc Distance Vector Routing protocol based on DSDV routing protocol. It uses efficient one-way Hash functions to provide authentication for both the sequence number and metric field in each routing entry. They avoid asymmetric cryptography to protect against dos attack and to overcome limited cpu processing capability.

5) CONFIDANT

CONFIDANT is enhancement of DSR routing and based on selection of selfish and unselfish nodes. Trust and routing calculation process is evaluated by experience, observation and behavior of other nodes, present in the network. It identifies routing misbehavior and maintains the provision of correct forwarding and traffic diversion.

6) SLSP

The Secure Link State Protocol (SLSP) for mobile ad hoc networks is responsible for securing the discovery and distribution of link state information. The scope of SLSP may range from a secure neighborhood discovery to a network-wide secure link state protocol. SLSP nodes disseminate their link state updates and maintain topological information for the subset of network nodes within R hops, which is termed as their zone. SLSP protects link state update packets from malicious alteration, as they propagate across the network.

7) BISS

Building Secure Routing out of an Incomplete Set of Security Associations (BISS), prior to the route discovery the sender and the receiver can establish a secure route, only the receiver has security associations established with all the nodes on the chosen route. Thus the receiver will authenticate route nodes directly through security associations. The sender will authenticate directly the nodes on the route with which it has security associations and indirectly to the node which does not have security associations.

8) SPREAD

Security Protocol for Reliable data delivery (SPREAD) provides data confidentiality security service in routing protocols. It uses secretsharing scheme between neighboring nodes tostrengthen data confidentiality. It overcomes theproblem of eavesdropping and colluded attacks.

9) Friendship Based AODV (FrAODV)

Essia et al. [11] proposed Friendship based AODV whichconsists of evaluation algorithms that evaluated forwardand reverse path between source and destination. In thisscheme, it is assumed that each node has identity whichcan't be forged by any other malicious node and numberof malicious nodes is always less than the number of goodnodes. Every node stores a list of friends with friendshipvalues ranging from 0 to 100. More the friendship values,more trustable the node is.

10) Secure AODV Routing Protocol based on Trust Mechanism

Harris Simaremare et al. [13] proposed AODV routingprotocol based on trust mechanism using the concept oflocal trust and global trust. Local trust is based on totalnumber of received packets and total number of forwardedpackets with reference to specific nodes. Global trust isbased on total number of packets received and total number of packets forwarded in network. Trustcalculation is done before communication starts. Thisscheme can withstand blackhole attack and DoS attack.Each node should get all the activity information from itsneighbor to calculate the trust. In order to ensure the nodescan hear all the activities of his

neighbors, each node willrun in promiscuous mode. The simulations are done onNS-2 and the performance analysis is done in terms ofpacket delivery ratio, end to end delay and routingoverhead.

TABLE 1. STRENGTH AND WEAKNESS OF DIFFERENT PROTOCOLS

Protocol	Modification	Performance parameters	Strength	Weakness
Khuran [5]	RRDU, RRDU_REP andreliability list areused	Handles attacks andsecure routing	Simple implementation, secure route	Overheads as packets are modified
Pushpa [6]	Based on node trust and route trust, modified the RREP and RREQ packet and Neighbor table	Throughput,packet drop	Ensure trusted Route betweenSource and destination	Complex architecture, overhead
Subramanian [7]	Based on calculating trust value for every node	Packet delivery ratio, delay, throughput	Detects misbehaving nodes andisolate them	Overheads and lack of authentication of nodes and packets.
Wadbude [8]	Uses hash chain,digital signature andprotocol enforcement mechanism	Overheads, end to end delay	Security and authenticity	Message overhead, complex cryptographic operations
Subramanian[9]	Based on threshold value the node behavioriseither trustworthy ornot	Packet delivery ratio, delay and throughput	Packet dropping nodes are identified and not involved in routing	Overhead
Sharma [10]	Modified routing table and assumes that intrusion detection system are used	Packetdelivery ratio, delay, average latency andnetwork throughput.	Simple operations based on recommendation rather any cryptographic operations	Malicious nodes can attack as there is no packet authentication
Islam [11]	Used EXPLICIT NO packet to inform non availability	Packet delivery ratioand delay	Simple architecture and energy conserving	Overhead and non availability of nodes even when trustworthy
Simaremare [12]	Used local trust and global trust concept to findthetrust level	Packetdelivery ratio, delay and routing overhead	Remove the attacker node before communication starts	Nodes work in promiscuous listening mode

11) TRUST DSR (TDSR)

TDSR [14] uses trusted route for packet transmission andreduces the number of packets dropped by node. It workson the basis of positive or negative acknowledgement received after the transmission of a packet. The trust of anode is computed on the basis of all the successful and unsuccessful transmissions by a node in a stipulated timeperiod i.e. by counting the number of ACK (Positiveacknowledgement) and NACK (Negativeacknowledgement) sent by a node. TDSR finds the secureroute from source to destination in a network. Every nodemaintains a table recording all its neighbors along withtheir trust values and update the entries periodically. Thetrust of a node in the network is evaluated based on itsperformance in the network. If a node successfully transmits a packet it sends a positive acknowledgement to the sender resulting in up gradation of its trust value.Packet drop results in negative acknowledgement causing reduction in the trust value of a node. The table storing thetrust value of all neighbors is broadcasted periodically sothat the information about the most trusted node is known to all. Trust value of a node helps in choosing the most trusted route from source to destination. In this way, trustvalue for each forward route from source to destination is computed based on the trust values of the intermediate nodes and then the route with the minimum trust worth(greater or equal to some trust threshold value is selected for transmission.

IV. CONCLUSION

MANETs are vulnerable to various types of attacks. Due to its infrastructure less property it is more vulnerable to malicious attacks. The trust based on demand routing protocols are used to have a secure routing. In trust based mechanism the nodes routes packets through intermediate nodes. The intermediate node must satisfy the trust factor. Thus various trust based on demand routing protocols are reviewed in this work.

REFERENCES

[1] Santhosh kumar and Suveg Moudgil, Detection of selfish node in DSR based MANET using reputation based mechanism, International journal of Research in IT, ISSN 2249-9482.

[2] TameemEissa, ShukorAbdulRazak, RashidHafeezKhokhar,NormaliaSamian, Trust-BasedRouting Mechanismin MANET Designand Implementation.MobileNetwAppl Springer Science BusinessMedia,LLC2011.

[3] Q. He, D. Wu, and P. Khosla, SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad- Hoc Networks, Proc.IEEE Wireless Communicationsand Networking Conf., vol. 2, pp. 825-830.

[4] S. Senthilkumar and J. William, A survey on reputation based selfish node detection techniques in mobile ad hoc networks, JATIT, Vol 60 no 2 ISSN 1992-8645.

[5] RekhaKaushik and JyotiSinghai, Detection and isolation of reluctant node using reputation based scheme in ad hoc networks, IJCNC, Vol 3 No 2.

[6] J. Sengathir, R. Manoharan and R. Rajkumar, Markovian process based reputation mechanisms to detecting selfish nodes in manets-A survey.

[7] Wadbude,Durgesh,andVineetRichariya.AnEfficientSecureAODVRoutingProtocolinMANET."InternationalJournalofEngineeringandInnovativeTechnology(IJEIT),vol.1,pp.274-279,April2012.

[8] Subramanian, Sridhar,andBaskaranRamachandran."QOSAssertioninMANETRoutingBasedonTrustedAODV(ST-AODV)",inInternationalJournalofAdhoc,Sensor&UbiquitousComputing, vol.3,no.3,June2012.

[9] Sharma, Pankaj."Trustbasedsecureaodvinmanet."JournalofGlobalResearch in ComputerScience,vol.3,no.6, pp.107-114, June2012.Islam,M.Hassan,andMisbahZareen."MitigatingtheeffectofmaliciousnodeinMobileAdHocNetworksusingTrustbasedExplicitNoTechnique."InternationalJournalofComputerNetworksandCommunicationsSecurity, vol.1,no.6,pp.210-215, November2013.

[10] Simaremare,H.,Abouaissa,A.,Sari,R.F.,&Lorenz,P.SecureAODVRoutingProtocolBasedonTrustMechanism. "InWirelessNetworksandSecurity,SpringerBerlinHeidelberg,pp. 81-105, 2013.

[11] AnkitAggarwalandBhumikaGarg,"SurveyonSecureAODVForAdHocNetworksRoutingMechanism",inInternationalJournalofAdvancedResearchinComputerScienceandSoftwareEngineering,vol.2,March2012.

[12] KannanGovindanandPrasantMohapatra, "TrustcomputationsandTrustdynamicsinMobileAd-hocNetworks:ASurvey",in:IEEEcommunicationsurveysandtutorials,vol. 14,no.2,pp.279-298,secondquarter2012.
[13] Eissa, T., Razak, S. A., Khokhar, R. H., &Samian, N. (2013). Trust-based routing mechanism in MANET: design andimplementation. Mobile Networks and Applications, 18(5), 666-677.
[14] Simaremare, H., Abouaissa, A., Sari, R. F., & Lorenz, P. "Secure AODV Routing Protocol Based on Trust Mechanism." In Wireless Networks and Security , Springer Berlin Heidelberg, pp. 81-105, 2013
[15] Khatri, Pallavi. "TDSR: Trust based DSR Routing Protocol for Securing MANET." International Journal Of Networking And Parallel Computing 1.3 (2013): pp. 42-48.
[16] R. Vijayakumar and K.R. Shankar Kumar,"Advanced Secured Model for On-Demand Distance Vector Routing Protocol in Manet", Middle-East Journal of Scientific Research 22 (9): 1353-1358, 2014