An Efficient Secure Trust Based Adaptive Routing Misbehavior in MANET

S. Kanimozhi[1]
[1]PG Scholar, Department of CSE,
Faculty of Engineering, Avinashilingam University,
Coimbatore, Tamil Nadu, India

M. Anitha[2], D.Arthi[3]
[2 , 3.] Former PG Scholar, Department of CSE,
Faculty of Engineering, Avinashilingam University,
Coimbatore, Tamil Nadu, India

Abstract: **Ad hoc networks are widely used in military and other research areas. With nodes which can move randomly and connect to any nodes, it is impossible for ad hoc networks to own a fixed infrastructure. Routing is always the most significant part for any networks. During the lookup process of routing, no information is send back to originator, this result in fewer packets overhead. As per security concern, signature scheme is added in a routing process. Before sending the packet, source generates the signature with peer ID of destination and then forwards the packet to the IP address as per routing table. The packet will be decrypted only the system matched with the signature otherwise just forwards the packet to the next system. Then each node keeps the signed contact records of its earlier contacts, based on this the next contacted node can detect if the node has dropped any packet or not. Trust based Adaptive Routing algorithm is proposed from the tradeoff between trust degree and link delay. This algorithm is implemented based on AODV (Ad hoc On-demand Distance Vector) protocol and provides effective routing strategy combined with security signature scheme by considering the QoS parameters such as end-to-end delay, energy consumption, packet loss and packet delivery ratio.**

Keywords – AODV; QoS; Security Signature scheme; Trust based Adaptive Routing;

I.INTRODUCTION

Ad hoc Network is a collection of nodes that do not need to rely on predefined infrastructure to keep the network connected. In Ad hoc Networks, a node has limited transmission range and also acts as routers. There are no specific routers, servers, access points for MANET. Because of its fast and easy of deployment, robustness, and low cost, typical MANET applications could be find in the following areas like military applications, rescue operations etc. Security of Ad hoc Networks is considered from attributes such as ease of use, privacy, reliability, verification and right to use control. Ad hoc Networks maximize total network throughput by using all available nodes for routing and forwarding. A node may misbehave by agreeing to forward the packet and then failing to do so due to selfish behavior, malicious or broken. Misbehaving nodes can be a significant problem.

QoS is a difficult task in the research area, because the topology of an ad hoc network will constantly change. Sustaining a certain quality of service is very challenging, while the network condition constantly changes [6]. The different applications may have different Quality of Service (QoS) requirements, which may be better satisfied by using different routing methods or metric types. Hence it is necessary to consider multiple metrics for selecting an efficient path.

Networks must provide protected, expected, quantifiable, and sometimes assured services. Achieving the required QoS by managing end-to-end delay, available bandwidth, packet overhead and throughput is the major challenging task in MANET routing. This kind of multi-metric QoS routing problems can be solved with an efficient routing strategy.

To make the routing strategy perform best, an efficient routing strategy named Tracer Routing is presented. Tracer routing enables the initiator to trace the whole routing process. It is also designed to control the routing path. Peer-ID based signature schemes is combined with tracer routing strategy and offer the initiator of each query to identify malicious nodes. A key feature of this scheme is from other protocols an alternate routing is constructed only by detecting malicious nodes. An address routing message attack is proposed by combined tracer routing with Peer-ID based signature scheme.

The rest of the report is organised as follows. In Section 2, related works are reviewed. Section 3 gives the problem formulation. Section 4 describes the trust model implementation and also describes the Security Signature Scheme in MANET. Section 5 elaborates the Simulation Environment. Section 6 gives the result and analyse the algorithm under variable simulation environments. Finally Section 7 concludes the work.

II. RELATED WORKS

A. Routing Protocols

Nekkanti and Lee extended AODV (Ad hoc On- demand Distance Vector) using trust factor and security level at each node [1]. Their approach deals differently with each route request based on the node’s trust factor and security level. In a typical scheme, routing information for every request would be encrypted and use different levels of encryption based on the trust factor of a node.

Buchegger and Boudec initiated a new design to develop a routing protocol by introducing a “trust manager” in their scheme [5]. They determined trust levels based on self-monitored information while employing reputation collected from both direct and indirect observations and experiences. They explained about sustainable relationship between the total number of nodes in the network, the maximum number of malicious nodes the system can tolerate, and the minimum number of friends per node needed to achieve high easiness, and a given level of trust.

B. Trust based Management Scheme

Buchegger and Boudec also developed a reputation-based trust management scheme called CONFIDANT (Cooperation Of Nodes-Fairness In Dynamic Ad-hoc NeTworks) based on both direct and indirect observations to detect misbehaving nodes [2]. The unique feature in this work is an incentive mechanism for altruistic nodes to be paid as a result of cooperation.

Soltanali, Pirahesh Niksefat, Sabaei proposed a distributed mechanism to deal with selfish nodes as well as to encourage cooperation in MANETs based on the combination of reputation-based and currency-based incentive mechanism mitigating their defects and improving their advantages [9]. Compared to existing works, this work considers more aspects of trust such as dynamicity, weighted transitivity, and subjectivity. However, it used only packet forwarding behaviors to evaluate a node's trust and standard performance metrics to evaluate the proposed trust scheme.

Balakrishnnan, Varadharajan, Tupakala, Lucs described a trust model to strengthen the security of MANETs and to deal with the issues associated with recommendations [10]. Their model utilizes only trusted routes for communication, and isolates malicious nodes based on the evidence obtained from direct interactions and recommendations. Their protocol is described as robust to the recommender's bias, honest-elicitation, and free-riding. This work uniquely considered a context-dependency characteristic of trust in extending DSR.

Moe, Helvik, Knapskog identified a trust-based routing protocol as an extension of DSR based on an incentive mechanism that enforces cooperation among nodes and reduces the benefits that selfish nodes can enjoy (e.g., saving resources by selectively dropping packets). This work is unique in that they used a hidden Markov model (HMM) to quantitatively measure the trustworthiness of nodes. In their work, selfish nodes are benign and selectively drop packets [11].

C. Security Signature Management Scheme

Paul and Westhoff studied a context-aware mechanism for detecting selfish nodes by extending DSR with a context-aware inference scheme to punish the accused and the malicious accuser [3]. However, the use of digital signatures to disseminate information about the accused and the malicious accuser may not be viable in a resource-constrained MANET environment.

Li, Lyu, Liu also discussed AODV and adopted a trust model to guard against malicious behaviors of nodes at the network layer [12]. They represented trust as opinion stemming from subjective logic. The opinion reflects the characteristics of trust in MANETs, particularly dynamicity. The key feature is to consider system performance aspects by dealing with each query based on its level of trust. Depending on the level of trust of nodes involved in the query, there is no need for a node to request.

Sen analyzed a trust-based mechanism to detect malicious packet dropping nodes based on reputation of neighboring nodes, and take into account the decay of trust over time [8]. This work assumes that a pair of public/private keys can be preloaded to prevent identity-related attacks.

III. PROBLEM FORMULATION

In all the related works, the authors consider overhead as important metric for efficient and reliable routing. Even though packet overhead metric is considered, for reliable multimedia applications multiple QoS metrics has to be considered. Most of the existing works were on finding feasible path based on packet overhead for trust based routing in MANET.

In the trust based routing, to transfer the data packet from source to destination commonly user TCP/IP protocol in networking. In this TCP/IP process, before transferring the data connection has been established. Each node forwards the query to the next node. During the lookup process no information is send back to the originator, resulting in less packet overhead. To make the routing strategy perform best, we present an efficient routing strategy, called tracer routing. Tracer routing enables the initiator to trace the whole routing process.

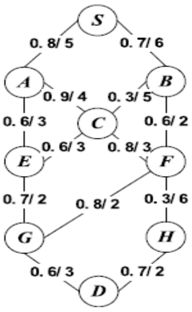

Fig 1. Sample topology

IV. PROPOSED WORK

A. Trust model implementation

1) Trust model

Trust models have vulnerabilities that can be exploited by malicious nodes. In the simple trust model, trust is established according to two observations: direct and indirect. A direct observation is packet forwarding behaviour [7]. An indirect observation arises from interactions with neighbours who report about their own direct observations. Each node derives a trust degree value for each of its neighbours (nodes that are within its transmission range). This value is a measure of the level of trust in its neighbour. Let $T_{i,j}(t)$ denote the degree of trust of node i in its neighbour j at time t. The trust degree value is limited to a continuous range from 0 to 1. The trust degree 0 denotes complete distrust whereas the value 1 represents absolute trust.

A Trust based QoS model essentially captures trust derivation, computation and application in a multi-QoS constraints environment. Each node monitors its neighbour nodes' forwarding behaviour to judge their trust degree using the trust model. Malicious nodes can be isolated from the network. The remaining nodes are trusted. Establishing an effective QoS evaluation model under the trusted network environment is a significant problem. In this section, the solution to this challenge is given.

2) Trust based Adaptive Routing

Routing is one of the primary functions in MANETs which each node has in order to perform connection between nodes that are not directly with each other's range and this forms a challenge to perform [4]. The major challenges are designing routing protocol for MANET. Moreover, determining a packet route requires a node to know at least the availability information to its neighbours. However, changing topology special routing protocols have been proposed to face the routing problem in MANETs. Since routing is a basic service in such a network, which is a prerequisite for other services, it has to be reliable and trustworthy. Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile adhoc networks (MANETs) and other wireless ad-hoc networks. The AODV Routing protocol uses an on-demand approach for the discovery of routes, that is, a routeis established only when it is required by a source node for transmitting data packets.In this protocol each node forwards the query to the next node. During the lookup process no information is send back to the originator, resulting in less packet overhead. To make the routing strategy perform best, an efficient routing strategy, called tracer routing is proposed. Tracer routing enables the initiator to trace the whole routing process.

a) Routing Table model: Path selection between source and destination is the procedure to follow on this model. Getting the systems IP address in a LAN and decides the source, destination and the intermediate systems for our routing process. Using any database form the routing table with columns like source address, destination address and router addresses. After creating the routing table enters the ip address in the respective columns.

b) Packet forwarding: It is the procedure to route the packet from source to destination via routers. As per this procedure by comparing IP addresses in the routing table the packet will be forward to next IP address. By using IP addresses in the routing table, the path selected by the user according to the respective path the packet will be forward and finally reach destination.

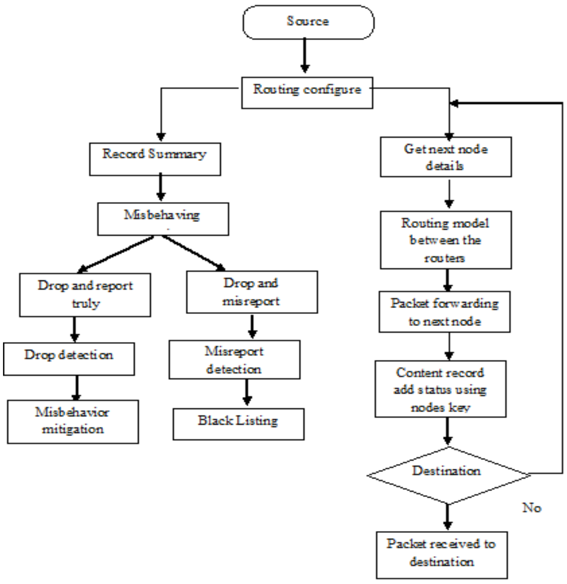

Fig 2. System Architecture

B. Security Signature Scheme

An efficient routing strategy named Tracer Routing is combined with a peer-ID based signature scheme offers the initiator with each query to identify malicious nodes. A key feature of this scheme is from other protocols that alternate routing is constructed only by detecting malicious nodes. Routing message attack is addressed by combining tracer routing with Peer-ID based signature scheme is proposed.

Any techniques of verifying the Peer-ID of remote, peer can work with tracer routing. In this scheme, the initiator appends a signature to a query. When an intermediate peer *x* receives the message (including query and its signature), *x* verifies the message and discards the polluted or forged one using the initiator's public key. Recall that the public key is the Peer- ID of initiator. Then *x* forwards the message it received to the next hop. At the same time, *x* sends an acknowledgement (including the Peer-ID of the next hop, query and the signature generated using the private key of *x*) to initiator. The process is repeated until the query reaches the target. Before sending the packet, source generates the signature with peer ID of destination and then forwards the packet to the ip address as per routing table. The packet will be decrypted only the system matched with the signature otherwise just forwards the packet to the next system.

1) Contact Records

The two nodes also exchange their current vector of buffered packets (as a step of contact record generation). In this way, one node knows the two set packets of the other node buffers at the beginning of the previous contact and the beginning of the current contact, which are denoted. A mischievous node may drop a packet but keeps the packet ID and also pretending as that it still buffers the packet.

The next contacted node may be a better relay for the dropped packet according to the routing protocol, which can be determined when two nodes exchange the destination (included in packet ID) of the buffered packets. In this case, the mischievous node should forward the packet to the next contacted node, but it cannot since it has dropped the packet. Thus, the next contacted node can easily detect this misbehavior and will not forward packets to this misbehaving node.

2) Witness Node

To detect the inconsistency caused by misreporting, a node selects random nodes from the contact record as the witness node of this record and transmits the summary of this record to the node when it contacts. Here, the nodes contacted a long time ago are not used since they may have left the network.

After detection, the witness node floods an alarm to all other nodes. The alarm includes the two inconsistent summaries. When a node receives, it verifies the inconsistency between the included summaries and the signature of the summaries. If the verification succeeds, this node adds the appropriate misreporting node into a blacklist and will not send any packets to it. If the verification fails, the alarm is discarded and will not be further propagated. A misreporting node will be kept in the blacklist for a certain time before being deleted.

A node deletes the records received from the contacted node right after this contact, since these received records are only used to check if the contacted node has dropped packets recently. The witness node should keep its collected record summaries for a long enough time to detect misreporting. For simplicity, our scheme uses a time-to-live parameter, which denotes the time for the collected summaries to be stored before being deleted.

3) Blacklist

To mitigate routing misbehavior, the number of packets sent to the misbehaving nodes is reduced. If a node is detected to be misreporting, that particular node should be blacklisted and should not receive packets from others. A node cannot simply blacklist, since a normal node may also drop packets due to buffer overflow. In the following, how to mitigate routing misbehavior without affecting normal nodes too much when misbehaving nodes do not misreport is focused.

A metric forwarding probability (FP) is maintained for each node based on if the node has dropped, received and forwarded packets in recent contacts, which can be derived from its reported contact records. The nodes that frequently drop packets but seldom forward packets will have a small FP and will receive few packets from others. This scheme borrows ideas from congestion control to update FP. More specifically, it combines additive increase, additive decrease, and multiplicative decrease to differentiate misbehaving nodes from normal nodes.

V.SIMULATION ENVIRONMENT

The simulation tool used to implement the proposed work is NS2 which works on Ubuntu Operating System. The network consists of 15-100 mobile nodes randomly placed in a 500m × 500m simulation area .The protocol used for simulation is AODV.. Traffic type required is Constant Bit Rate (CBR) and the channel capacity provided is 2 Mbps. Pause time is set as 10 s and the total simulation time is 100 s. The transmission power of each node is set as 1.5 joule and the receiving power of each node is set as 1.0 joule. The hardware required for the experiment is Intel core i5 processor with RAM capacity of 4GB. Hard disk capacity is 320 GB.

VI. RESULT AND ANALYSIS

The simulation studies involve random networks with 50-100 nodes. The distance of each link is distributed uniformly in [10,200] and the delay of each link in [0, 50].The maximum allowable delay is [30,160].The protocol used in this simulation is AODV. In this simulation node 1 is set as source node and node 15 is set as destination node. The experiment is simulated and analyzed by varying number of nodes, pause time and node mobility. The utilization of energy and packet overhead and delay under each environment is analyzed. The algorithm is continued for 20-30 iterations. The packet delivery ratio and packet loss of nodes by using the proposed algorithm is calculated and it is compared with existing TQR algorithm. The Packet delivery ratio is calculated by considering the ratio of data packets received by the destinations to those generated by the sources. By using the proposed algorithm the packet overhead will be high when compared to existing routing algorithm. The proposed algorithm can converge to the solution satisfying the QoS requirements. The performance of proposed algorithm is shown in Fig 3.

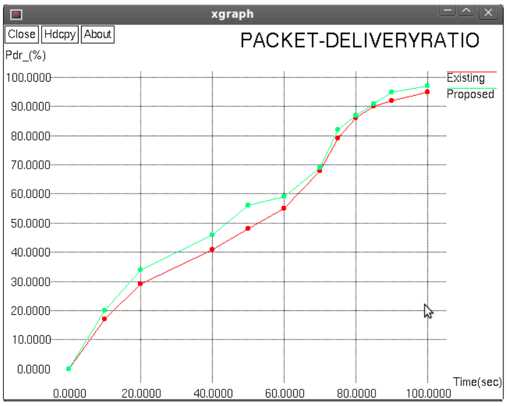

Fig 3 Performance of Trust based Adaptive algorithm on PDR

VII. CONCLUSION

A secure ad hoc network has to meet different security requirements such as secrecy, reliability ease of use, Authentication and non-repudiation. Different digital attacks have been developed to challenge the security of mobile Ad hoc networks. Trust is playing a growing security role in an open environment where unknown devices can join or leave the system at any time. Also, due to limited processing and battery power, existing encryption based security mechanism appear too burdensome to be considered viable solutions trust is an assessment based on experience that is shared through networks of people. These shared experiences lead to trust development that augments and decays with time and frequency of interactions. Since communication is becoming persistent and it is only natural to use the notion of pervasive trust where trust relationships are ubiquitous throughout the system. Trust can be used as a measure of certainty for a given operation such as routing in a network.

ACKNOWLEDGEMENT

S.Kanimozhi is pursuing M.E. in Avinashilingam Institute for Home Science and Higher Education for Women University, Coimbatore. I did my B.E. in SSM College of Engineering, Namakkal. I am living in Dharmapuri, Tamil Nadu.

M.Anitha did my M.E. in Avinasilingam Institute for Home Science and Higher Education for Women, Coimbatore University. I did my B.E. in Vivekananda College of Engineering, Thiruchengode. Also did my M.B.A. in Barathiar University, Coimbatore. I am living in Thiruchengode, Tamil Nadu.

D.Arthi did my M.E. in Avinasilingam Institute for Home Science and Higher Education for Women University, Coimbatore. I did my B.E. in Maharaja Engineering College, Avinashi. I am living in Coimbatore, Tamil Nadu.

REFERENCES

[1] Rajiv K. Nekkanti and Chung-wei Lee, "Trust Based Adaptive On Demand Ad Hoc Routing Protocol", in *ACMSE '04*, April 2-3, 2004, Huntsville, Alabama, USA.

[2] S. Buchegger and Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic ad-hoc networks)," in *Proc. MobiHoc*, 2002, pp. 226–236.

[3] Krishna Paul and Dirk Westhoff, "Context aware inferencing to rate a selfish node in DSR based ad-hoc networks" in *Proceedings of the IEEE Globe-com Conference, Taipeh, Taiwan*, 2002. IEEE.

[4] Yogendra Kumar Jain, Nikesh Kumar Sharma, "Secure Trust Based Dynamic Source Routing in MANETs", in International Journal of Scientific & Engineering Research Volume 3, Issue 8, ISSN 2229 – 5518, August - 2012

[5] Sonja Bucheggar and Jean Yves Le Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness and Robustness in Mobile Ad Hoc Networks", *Proceedings of the Tenth Euromicro Workshop on Parallel, Distributed and Network-based Processing,* pages 403-410, Canary Islands, Spain, January 2002, IEEE Computer Society.

[6] Pankaj Sharma, Yogendra Kumar Jain, "Trust Based Secure AODV in MANET" in *Proceedings of Journal of Global Research in Computer Science*, Volume 3, No. 6, June 2012.

[7] Mohana, N.K.Srinath, AmitL.K, "Trust based Routing Algorithms for MANET", in Proceedings of International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 8, August 2012.

[8] Jaydip Sen, "A Distributed Trust and Reputation Framework for Mobile Ad Hoc Networks", *Springer-Verlag Berlin Heidelberg* 2010, CNSA 2010, CCIS 89, pp. 538-537, 2010.

[9] S.Soltanali, S.Pirahesh, S. Niksefat and M. Sabaei, "An Efficient Scheme to Motivate Cooperation in Mobile Ad Hoc Networks," *Int'l Conf. on Networking and Services, Athens, Greece*, pp. 98-103, 19-25 June 2007.

[10] V. Balakrishnan, V.Varadharajan, U.K. Tupakula and P.Lucs, "Trust and Recommendations in Mobile Ad Hoc Networks", *Proceedings of 3rd International Conference on Networking and Services (ICNS 2007), Athens, Greece*, pp. 64-69, 2007.

[11] M. E. G. Moe, B. E. Helvik, and S. J. Knapskog, "TSR: Trust- based Secure MANET Routing using HMMs", *Proc. 4th ACM Symposium on QoS and Security for Wireless and Mobile Networks*, Vancouver, British Columbia, Canada, 27-28 Oct.2008, pp. 83-90.

[12] Xiaoqi Li, Lyu, M.R., Jiangchuan Liu, "A Trust Model Based Routing Protocol for Secure Ad hoc Networks", IEEE Proceedings on Aerospace Conference, 2004, vol. 2.