ISSN No. 0976-5697

Volume 2, No. 1, Jan-Feb 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Detection of Misbehaving Nodes in Mobile Ad hoc Network

S.Gopinath*
Department of ECE, Anna University of Technology, Coimbatore.
Anna University of Technology, Coimbatore, India.
gopi.vasudev@gmail.com

A.Rajaram
Department of ECE, Anna University of Technology, Coimbatore.
Anna University of Technology, Coimbatore, India.
gct143@gmail.com

Abstract— Mobile Ad-hoc Network (MANET) is an indivisible part for communication of mobile devices. It is a dynamic wireless network that can be formed without any pre existing infrastructure in which each node can act as a router. It is easy to deploy node failure and network traffic to impersonate another node in MANET. Mobile ad hoc network has no clear line of defense, so, it is accessible to both legitimate network users and misbehaviors. In the presence of misbehaviors, one of the main challenges is to design the trust reputation system that can protect MANET from various misbehaviors. The main objective of the work is to detect the misbehavior using trust based mobility system. Mobility is exploited in order to detect the misbehavior. This model is carried out in two cases which exploit mobile nodes to collect and broadcast trust information to achieve trust convergence and provides the authentication to the mobile nodes in order to detect the misbehavior. Each node would evaluate its own trust vector parameters about neighbors through monitoring neighbor's pattern of traffic in network. Simulation results shows that the mobility oriented trust system provides better detection efficiency, packet delivery ratio, low delay and good misbehaving node detection based on delay constraint.

Keyword: MANETs, Misbehavior, Packet Delivery Ratio, Detection efficiency, Delay Constraint.

I. INTRODUCTION

A. Mobile Ad-hoc Network

Mobile Ad Hoc Network (MANET) is a self-configuring system of mobile routers linked by wireless links which consequently combine to form an arbitrary topology. Thus, the network's wireless topology may alter rapidly and unpredictably. However, due to the lack of any fixed infrastructure, it becomes complicated to exploit the present routing techniques for network services, and this provides some huge challenges in providing the security of the communication, which is not done effortlessly as the number of demands of network security conflict with the demands of mobile networks, largely due to the nature of the mobile devices .e.g. low power consumption, low processing load.

B. Misbehavior in MANET

Mobile nodes are affected by different types of misbehaviors. The misbehaviors in mobile ad hoc networks can be classified in to two categories i.e. node failure and network traffic.

C. Node Failure:

Node failure occurs when the node sends a packet to the neighbor node for transmitting information, if the neighbor node does not give any reply. In figure 1 node A send a packet for transmission to node B, but B does not give any reply. That means B does not send any acknowledgement.

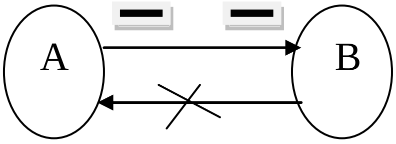

Figure 1. Node failure

D. Network Traffic:

Network traffic occurs when the node sends a packet to the neighbor node for transmitting information, but the node does not know whether the neighbor node is forwarding the packet to another node or not. In figure 2 node A send a packet for transmission to node B, but A does not know whether the B is forwarding the packet to another node or not. That means node B's status do not know to node A.

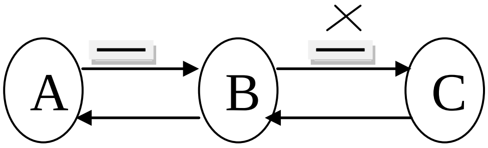

Figure 2. Network traffic

II. RELATED WORK

Kamvar and Schlosser [1] have proposed the Eigen trust algorithm allows computation of global trust values in the distributed environment. Eigen Trust presents the request to separate misbehavers from newcomers. But, it lacks the method to satisfy this request naturally. Eigen Trust is just a representative and most existing trust evaluation systems have the same requirement, but omit uncertainty the same time.

Hu and Perrig [2] have concentrated on assurance that both the source and destination nodes authenticate the messages, and moreover, the intermediate nodes have to insert their own digital signature in route request.

Buchegger and Boudec [3] suggest that despite the fact that networks only function properly if the participating nodes cooperate in routing and forwarding. However, it may be advantageous for individual nodes not to cooperate. They propose a protocol, called CONFIDANT, which aims at detecting and isolating misbehaving nodes, thus making misbehavior unattractive.

Zapata and Asokan [8] proposed the Secure Ad-hoc On-Demand Distance Vector routing protocol. Through providing security features like integrity, authentication and non-repudiation, it effectively protects the route discovery mechanism. This scheme is based on the assumption that each node should have certified public keys of all nodes in ad hoc network.

K. Sanzgiri et al [7] proposed the Authenticated Routing for Ad-hoc Networks (ARAN) secure routing protocol is an on-demand routing protocol which relies on the use of digital certificates to identifies and defends against malicious actions in the ad-hoc network.

Michiardi and Molva [4] have proposed CORE mechanism that enhances watchdog for monitoring and isolating selfish nodes based on a subjective, indirect and functional reputation. The reputation is calculated based on various types of information on each entity's rate of collaboration. Since there is no incentive for a node to maliciously spread negative information about other nodes, simple denial of service attacks using the collaboration technique itself are prevented.

Bansal and Baker [5] suggests that ad hoc networks rely on the cooperation of the nodes participating in the network to forward packets for each other. A node may decide not to cooperate to save its resources while still using the network to relay its traffic. If too many nodes exhibit this behavior, network performance degrades and cooperating nodes may find themselves unfairly loaded.

Naldurg amd Kravets [9] proposed the Security-Aware Ad-hoc Routing (SAR) which deploys a generalized framework for any on-demand secure ad-hoc routing protocol. It uses security information to dynamically control the routing selection process according to routing tables. Nodes at the same trust level must share a secret key.

III. OBJECTIVES & OVERVIEW OF THE PROPOSED MECHANISM

A. Objectives

In this paper, we propose to design a Trust Based Mobility System which attains trust convergence and authentication to the mobile nodes. The concept of trust is important to communication and network protocol designers where establishing trust relationships among participating nodes is critical to enabling collaborative optimization of system metrics. Eschenauer et al. [10] proposed the trust is defined as "a set of relations among entities that participate in a protocol. These relations are based on the evidence generated by the previous interactions of entities within a protocol. In general, if the interactions have been faithful to the protocol, then trust will accumulate between these entities." Trust has also been defined as the degree of belief about the behavior of other entities; the trust has the following features:

[a] Trust is dynamic, not static.

[b] Trust is subjective.

[c] Trust is not necessarily transitive. The fact that A trusts B and B trusts C does not imply that A trusts C.

[d] Trust is asymmetric and not necessarily reciprocal.

[e] Trust is context-dependent. A may trust B as a wine expert but not as a car fixer. Similarly, in MANETs, if a given task requires high computational power, a node with high computational power is regarded as trusted while a node that has low computational power but is not malicious (i.e., honest) is distrusted.

B. Overview of the proposed Mechanism

We propose a Trust Based Mobility System (TBMS) in MANETs without using any centralized infrastructure. It uses trust table to favor packet forwarding by maintaining a trust vector for each node. A node is reprimanded or satisfied by decreasing or increasing the trust vector value. Each intermediate node marks the packets by adding its recommendation about the neighborhood node, probability that the data packet will be successfully transmitted and evaluation about the ability of forwarding packets towards the destination node. The destination node verifies the recommendation, probability of packet forwarding values and checks the trust vector. If the recommendation and probability of packet forwarding is verified, the trust vector is incremented, otherwise it is decremented. If the trust vector value falls below a trust vector threshold value, the corresponding the intermediate node is marked as misbehavior.

IV. EFFICIENT MISBEHAVIOR DETECTION SYSTEM

A. Trust Based Mobility System

In our proposed system, by dynamically calculating the nodes trust vector values, the source node can be able to select the more trusted routes rather than selecting the shorter routes. Our system marks and isolates the misbehaving nodes from participating in the network. So the potential damage caused by the misbehaviors are reduced.

Let {Tv_1, Tv2…} be the initial trust vectors of the nodes {n_1, n2…} along the route R1 from a source S to the destination D.

Since the node does not have any information about the reliability of its neighbors in the beginning, nodes can neither be fully trusted nor be fully distrusted. When a source S wants to establish a route to the destination D, it sends route request (RREQ) packets.

When the destination D receives the accumulated RREQ message, it measures the number of packets received Prec. Then it constructs a route on Prec with the key shared by the sender and the destination.

The RREP contains the source and destination ids, the route of Prec, the accumulated route from the RREQ, which are digitally signed by the destination. The RREP is sent towards the source on the reverse route R1.

The intermediate node then verifies the digital signature of the destination node stored in the RREP packet, is valid. If the verification fails, then the RREP packet is dropped.

Otherwise, it is signed by the intermediate node and forwarded to the next node in the reverse route.

When the source S receives the RREP packet, if first verifies that the first id of the route stored by the RREP is its neighbor. If it is true, then it verifies all the digital signatures of the intermediate nodes, in the RREP packet. The digital signature includes recommendation about the neighbor node and probability that data packet received successfully. If all these verifications are successful, then the trust counter values of the nodes are incremented as

$$Tv_i = Tv_i + \alpha_1 \qquad (1)$$

If the verification is failed, then

$$Tv_i = Tv_i - \alpha_1 \qquad (2)$$

Where α_1 is the step value, which can be assigned a small fractional value during simulations. After this verification stage, the source S check the digital signature values DS of the nodes n_i.

Digital Signature includes recommendation about the neighbor node, probability that data packet received successfully.

Evaluating the recommendation is given by R_B^A which is node A's evaluation to node B by collecting recommendations

$$R_B^A = \frac{\sum_{v\in\gamma} V|A\rightarrow C| * V|C\rightarrow B|}{V|A\rightarrow C|}$$

γ is a group of recommenders.
$V|A\rightarrow C|$ is trust vector of node A to C.
$V|C\rightarrow B|$ is trust vector of node C to B.

Probability that data packets received can be defined by,

P_B^A = (1-$p_{A,B}$) * (1-$p_{B,A}$)

$p_{A,B}$ is packet loss probability from node A to node B, while , $p_{B,A}$ is packet loss probability from node B to node A.

For any node n_k, if $DS_k < DS_{min}$, where DS_{min} is the minimum threshold value, its trust vector value is further decremented as

$$Tv_i = Tv_i - \alpha_2 \qquad (3)$$

For all the other nodes with $DS_k > DS_{min}$, the trust counter values are further incremented as

$$Tv_i = Tv_i + \alpha_2 \qquad (4)$$

Where α_2 is another step value with $\alpha_2 < \alpha_1$.

For a node n_k, if $Tv_k < Tv_{thr}$, where Tv_{thr} is the trust threshold vector value, then that node is considered and marked as misbehaving node. If the source does not get the RREP packet or RERR packet for a time period of t seconds, it will be considered as a node failure or link failure.

Then the route discovery process is initiated by the source again. The same procedure is repeated for the other routes R2, R3 etc and either a route without a misbehaving node or with least number of misbehaving node, is selected as the reliable route.

V. PERFORMANCE EVALUATION

A. Simulation Model and Parameters

We use NS2.34 to simulate our proposed algorithm. In our simulation, 101 mobile nodes move in a 1000 meter x 1000 meter square region for 50 seconds simulation time. We assume each node moves independently with the same average speed. All nodes have the same transmission range of 100 meters. The simulated traffic is Constant Bit Rate (CBR).

Our simulation settings and parameters are summarized in table I

Table I. Simulation settings and parameters of TBMS

No. of Nodes	**101**
Area Size	1000 X 1000
Mac	802.11
Radio Range	100m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	80
Mobility Model	Random Way Point

B. Performance Metrics

We evaluate mainly the performance according to the following metrics.

Detection Efficiency: The ratio of detected misbehaving nodes to the total number of nodes.

Delay Constraint: The delay constraint is averaged over all surviving data packets from the sources to the destinations.

Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Average Delay: The delay is averaged over all surviving data packets from the particular source to the destination.

Throughput: The total number of packet received at the destination without any loss.

The simulation results are presented in the next part. We compare our trust based mobility system with the CONFIDANT [3] and Improved CONFIDANT [6] model in presence of misbehaving node environment.

C. Results

Nodes actual behaviors comply with the Bernoulli trial, which means that the probability that a node acts good is predetermined. If a node acts well for less than 40 percent of the interactions, it is considered as a misbehaving node. The default percentage of misbehaving nodes in the network is 20 percent.

In our First experiment, we vary the no. of misbehaving nodes as 20,30 up to 100.

Figure 3 show the results of detection efficiency for the misbehaving nodes 20, 30….100 scenarios. Clearly our TBMS scheme achieves more detection rate than the CONFIDANT and Improved CONFIDANT model.

Figure 4 shows the results of delay constraint for the misbehaving nodes 20, 30….100. From the results, we can see that TBMS scheme has higher detection of misbehaving nodes than the CONFIDANT and Improved CONFIDANT schemes.

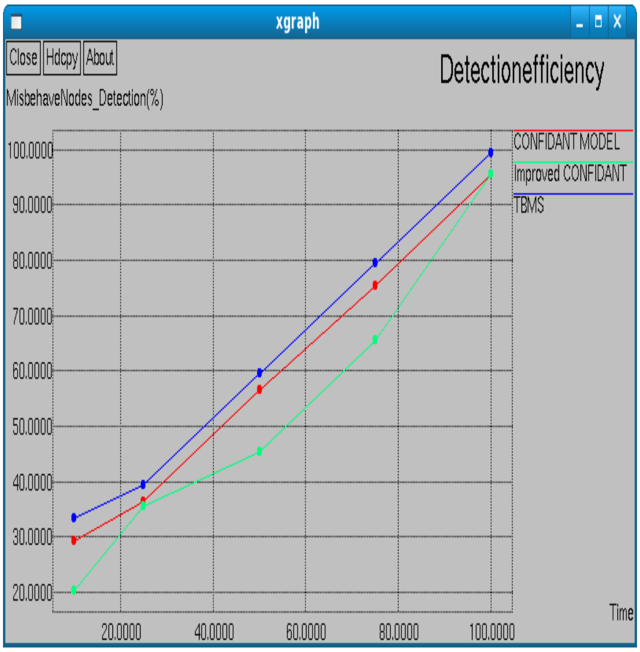

Figure 3. Detection Efficiency

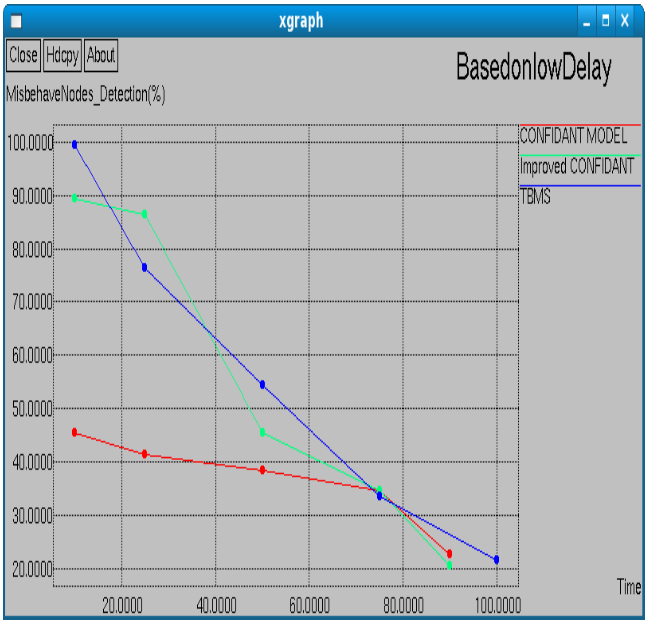

Figure 4. Based on Low Delay Constraint

In our Second experiment, we vary the number of nodes as 10, 20, 30 ,40,50,60.

Figure 5 show the results of Number of nodes Vs Packet Delivery Ratio. Clearly our TBMS scheme achieves high packet delivery ratio than the CONFIDANT and Improved CONFIDANT model.

Figure 6 shows the results of Throughput Vs Delay. From the results, we can see that TBMS scheme has less delay than the CONFIDANT and Improved CONFIDANT schemes.

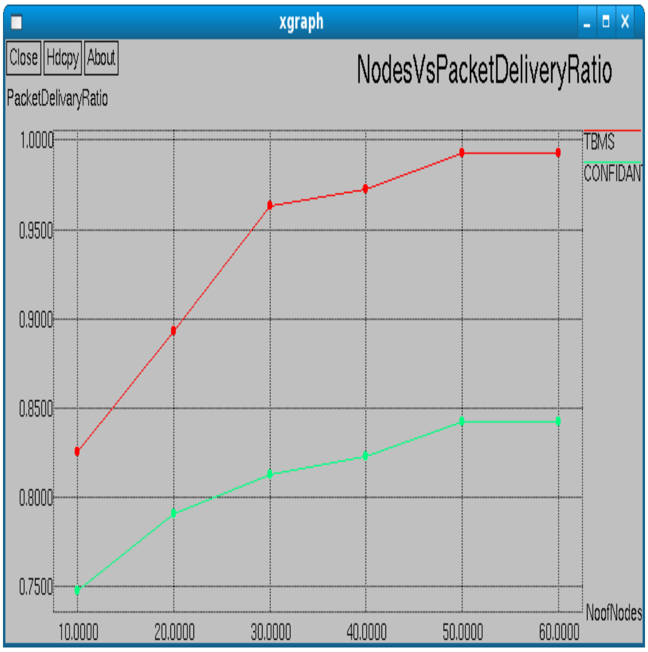

Figure 5. No of Nodes Vs Packet Delivery Ratio

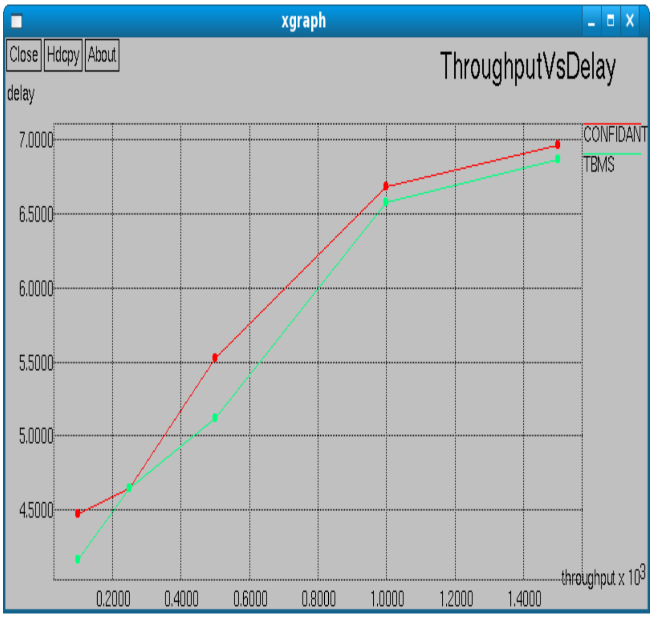

Figure 6. Throughput Vs Delay

VI. CONCLUSION

In this paper, we have developed a trust based mobility system which attains trust convergence and authentication to the mobile nodes. In the first phase of the system, detection of the misbehaving nodes is achieved. It uses trust table to favor packet forwarding by maintaining a trust vector for each node. A node is punished or rewarded by decreasing or increasing the trust counter. A node is reprimanded or satisfied by decreasing or increasing the trust vector value. If the trust vector value falls below a trust vector threshold value, the corresponding the intermediate node is marked as misbehavior. By simulation results, we have shown that the trust based mobility system achieves better detection efficiency, high packet delivery ratio attaining low delay and good misbehaving node detection based on delay constraint.

VII. REFERENCES

[1]. Kamvar, S., Schlosser, M., and Garcia-Molina, H. (2003), “The Eigen trust Algorithm for Reputation Management in P2P Networks,” Proc. Int’l Conf. World Wide Web.

[2]. Y. Hu and A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing,” IEEE Security & Privacy, 2004, pp. 28-39.

[3]. S. Buchegger and J. Boudec, “Performance Analysis of the Confidant Protocol,” Proc. Int’l Symp. Mobile Ad Hoc Networking and Computing, 2002.

[4]. P. Michiardi and R. Molva, “CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks,” Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm.and Multimedia Security, 2002.

[5]. S. Bansal and M. Baker, “Observation-Based Cooperation Enforcement in Ad Hoc Networks,” Technical Report cs.NI/0307012, Stanford Univ., 2003.

[6]. S. Buchegger and J. Boudec, “A Robust Reputation System for P2P and Mobile Ad-Hoc Networks,” Proc. Workshop Economics of Peer- to-Peer Systems (P2PEcon), 2004.

[7]. K. Sanzgiri et al., “A Secure Routing Protocol for Ad Hoc Networks,” Proc. 10th IEEE Int’l Conf. Network Protocols (ICNP ’02), IEEE Press, 2002, pp. 78–87.

[8]. M. Guerrero Zapata and N. Asokan, “Securing Ad Hoc Routing Protocols,” Proc. ACM Workshop on Wireless Security (WiSe), ACM Press, 2002, pp. 1–10.

[9]. Yi, S., Naldurg, P., Kravets, R., “Security aware ad-hoc routing for wireless networks,” Proc. of the 2nd ACM International Symposium on Mobile ad hoc networking and computing (MobiHoc’01), 2001, pp. 299-302.

[10]. L. Eschenauer, V. D. Gligor, and J. Baras, “On Trust Establishment in Mobile Ad Hoc Networks,” Proc. 10th Int’l Security Protocols Workshop, Cambridge, U.K., Apr. 2002, vol. 2845, pp. 47-66.

AUTHORS PROFILE

A. Rajaram received the **B.E.** degree in electronics and communication engineering from the Govt., college of Technology, Coimbatore, Anna University, Chennai, India, in 2006, the **M.E.** degree in electronics and communication engineering (Applied Electronics) from the Govt., college of Technology, Anna University, Chennai, India, in 2008 and he is currently pursuing the full time **Ph.D.** degree in electronics and communication engineering from the Anna University Coimbatore, Coimbatore, India. His research interests include communication and networks mobile adhoc networks, wireless communication networks **(WiFi, WiMax HighSlot GSM),** novel **VLSI NOC** Design approaches to address issues such as low-power, cross-talk, hardware acceleration, Design issues includes **OFDM MIMO** and noise Suppression in **MAI** Systems, **ASIC** design, Control systems, Fuzzy logic and Networks, **AI**, Sensor Networks.

S.Gopinath received the **B.E.** degree in electronics and communication engineering from the Govt. College of Engineering, Salem, Anna University, Chennai, India, in 2007.Currently doing **M.E. II** year in electronics and communication engineering (Communication Systems) in Anna University of technology, Coimbatore, India. His research interest includes wireless communication (**WiFi,WiMax**), Mobile Ad hoc networks ,Sensor Networks ,Neural Networks and fuzzy logic, Communication networks