Prevention of MANETS from Malicious Node Attacks

Sruthi R
PG Scholar, Department of CSE (PG)
Sri Ramakrishna Engineering College,
Coimbatore.

Vijayakumar R,
Assistant Professor, Department of CSE(UG),
Sri Ramakrishna Engineering College,
Coimbatore.

ABSTRACT
Mobile Ad-hoc Network (MANET) is the network which forms when needed with no existing or fixed infrastructure. It is an autonomous system of mobile hosts connected by wireless links. The mobile hosts are free to move independently in any direction. Due to the infrastructure-less design and self-organized mobile nodes the MANETs are prune to different problem, such as routing attacks, security breach problem, one among them is malicious node attack. The malicious node attack is an active attack which causes severe damage to the network. The malicious node can misroute, modify data packets. The proposed trust based mechanism is used to detect and isolate the malicious node from the network. The trust mechanism evaluates the trust value along with the reputation score and isolates the malicious node from active path. The proposed model is simulated using network simulator (NS2).

Keywords
MANET, trust, malicious node, trust value, reputation score

1. INTRODUCTION
A mobile ad-hoc network is a collection of wireless nodes. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. This kind of network is well suited for the mission critical applications such as emergency relief, military operations, and terrorism response where no pre deployed infrastructure exits for communication [10]. Due to its intrinsic nature of lacking of any centralized access control, secure boundaries (mobile nodes are free to join and leave and move inside the network) and limited resources mobile ad-hoc networks are vulnerable to several different types of passive and active attacks.

1.1 Reputation mechanism
Reputation based mechanism in Mobile ad-hoc networks (MANETs) is used to keep track of the quality of the behavior of the nodes. Basically reputation is an opinion formed on the basis of watching node behavior by direct or indirect observation of the nodes, through route or path behavior, number of retransmissions generated by the node, through acknowledgment message and by overhearing node's transmission by the neighboring nodes. One of the main goals for using reputation in a network of entities interacting with each other is to provide information to help assess whether an entity is trustworthy .This helps in detection of malicious nodes. Another goal is to encourage entities to behave in a trustworthy manner, i.e. to encourage good behavior and to discourage untrustworthy entities from participating during communication.

1.2 Ad-hoc on Demand Routing Protocol
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 transmitting data packets. It employs destination sequence numbers to identify the most recent path [13, 14, 15]. 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 Route-Request packet in the network when a route is not available for the desired destination.

1.3 Dynamic Source Routing
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 Route-Request packets in the network. The destination node, on receiving a Route-Request packet, responds by sending a Route-Reply packet back to the source, which carries the route traversed by the Route-Request packet received[14,15].

2. RELATED WORK
In [1] Akanksha Jain introduces an intrusion detection system along with AOMDV protocol to detect the malicious node. The Ad-hoc on demand multipath routing protocol is used, a separate IDS is incorporated to detect the malicious node in the network. The protocol detects only the malicious mode attack by black hole attack.

A. Rajaram and S. Palaniswamy [2], propose a security protocol based on trust mechanism on MAC layer approach. The protocol attains confidentiality and authentication of packets in both routing and link layers of manets. The protocol operates in two phases, in the first phase the malicious node is detected and isolated using trust based mechanism and in the second phase the encryption and authentication on CBC-X mode is incorporated. The protocol increases the packet delivery ratio. A distributed reputation mechanism is integrated on dynamic source routing protocol. The protocol detects the malicious node activity by single or multiple black hole attack. A fully distributed and trust based public key certificate management system is used to avoid security threats in mobile ad-hoc networks. Threshold cryptography and public key certificate is issued for authentication [3].

Marchang N et al [4] propose a light weight trust based routing protocol. It is light weight in the sense that the intrusion detection system used for estimating the trust that one node has for another consumes limited computational resource. Moreover it uses only local information for estimation. Bo Wang et al [5], propose a light weight protocol along with the Qos metrics. The Qos metrics is combined with the AODV routing protocol called QAODV is used to detect the malicious activity.

H Yang H Y. Luo [6], focuses on the fundamental security problem of protecting the multi-hop network connectivity between mobile nodes in a MANET. They identify the security issues, discuss the challenges to security design, and review the state-of-the-art security proposals that protect the MANET link- and network-layer operations of delivering packets over the multi-hop wireless channel. The complete security solution should span both layers, and encompass all three security components of prevention, detection, and reaction.

3. PROPOSED SYSTEM

The proposed trust based mechanism is a robust node exclusion mechanism. It uses a distributed and self-organized trust and reputation system. The system controls node access to the network monitors node behavior and excludes misbehaving nodes.

The monitor module gathers information about the neighbors of a node to infer their behavior. All nodes act as witnesses, monitoring actions performed by their neighbors and generating a behavior evaluation. The behavior is monitored by number of packets transmitted by each node. The trust module requires a minimum amount of behavior evaluation before rating the trust level. The trust value is evaluated as average of direct trust value, indirect trust value and path trust value. The evidences are sent periodically when the trust level of a given neighbor is lower than a specific threshold defined as the minimum tolerated trust in the network. The reputation value is calculated in the reputation module. Two different processes update the reputation value, the reputation degradation and reputation improvement. In the degradation process, the reputation decreases whenever the node receives an evidence message. The reputation value is increased whenever the node transmits packets properly to the neighbor node. The mechanism excludes misbehaving nodes when the reputation drops below a certain threshold. The malicious node is excluded from the active path of the network. The access control mechanism authenticates the newly added node in the network.

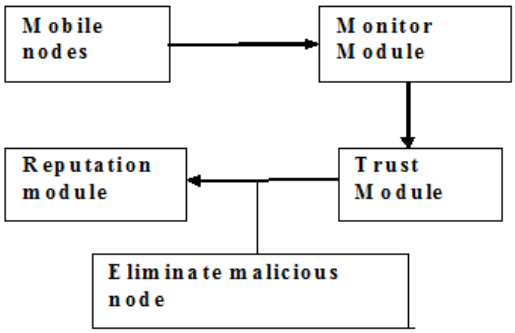

Fig 1 Architecture

Fig 1 is the architecture of the proposed trust based mechanism.

3.1 Monitor module

The monitor module monitors the behavior of the neighbor nodes in the network. The monitor module gathers information about the neighbors of a node to infer their behavior. All nodes monitor actions performed by their neighbors and generating a behavior evaluation for neighbor node that represent cooperativeness and well-behavior of a node.

3.2 Trust module

The trust module evaluates the trust value for each node in the network. Analyzing the trust level of a node has a positive influence on the confidence with which an entity conducts transactions with the node. The trust value is evaluated such that it is taken as the average of direct trust value of node, indirect trust value (recommendations of a node from its neighbors) and path trust (whole trust value along the routing path each node possess) [9,11,12]. The trust level ranges from 0 to 1, where 1 represents the most trustworthy a node and 0 represents the untrustworthy node. The threshold value is assigned as 0.4, so that each node should have trust value minimum of 0.4.

3.3 Reputation Module

The reputation module is responsible for assessing the reputation of nodes, which is based on the evidences received from witnesses [7, 8]. Two different processes update the reputation value, the reputation degradation and reputation improvement. In the degradation process, the reputation decreases whenever an evidence message is generated,

$$R^i = \max(R^{i-1} - u, 0) \quad 1$$

Where R^{i-1} is the previous reputation score and u is the reputation update value.

In the improvement process, the reputation value grows periodically to allow nodes to recover the reputation when they perform good actions.

$$R^i = \min(R^{i-1} + u, R_{\max}) \quad 2$$

Where R_{max} is the maximum reputation value. The threshold value is assigned as 0.4, so that each node should have reputation score minimum of 0.4.

If the trust value and reputation score goes below the threshold value, then the node is declared as malicious and it is isolated from active path of the network by sending alert message to all nodes.

4. EXPERIMENTAL SETUP AND ANALYSIS

The overall goal of the simulation experiments is to measure the accuracy and robustness of the trust based routing protocol.

Fig 2 Simulation parameter values

Number of nodes	15
Dimension of simulation area	800 x 600
Routing protocol	Ad-hoc on demand routing protocol
Simulation time (seconds)	100
Transport layer	TCP
Packet size (bytes)	1000
Traffic type	CBR
Traffic speed(m/s)	Random

To validate the detection and exclusion efficiency of proposed method against malicious node attack, Network Simulator (NS2) is used.

4.1 Packet Delivery Ratio

The packet delivery ratio is the ratio of packets which are successfully delivered to the destination compared to number of packets sent out by the sender.

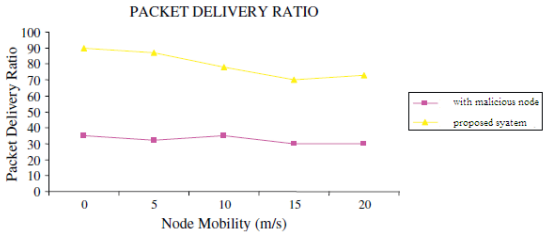

Fig 3 Packet delivery ratio

From fig 3 the packet delivery ratio is about 24 % when malicious node present in the network. It is increased to 73 % by isolating malicious node by proposed mechanism.

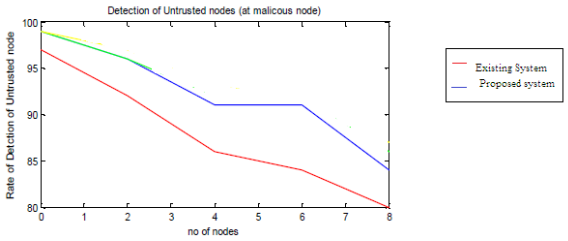

Fig 4 Percentage of malicious node detection

Fig 4 shows that more than 45 % of malicious node is detected by the proposed system when compared to existing system.

5. CONCLUSION AND FUTRE WORK

MANET is characterized by a highly dynamic network topology. Due to its dynamic topology and infrastructure less network it is prune to various attacks. The malicious node attack is kind among them. The proposed Trust based mechanism is a reputation based method to detect and isolate malicious node from the network. The monitor module monitors the behaviour of the neighbour nodes whether the packets are delivered properly to the destination. In trust module the trust value for each node is calculated such that based on the trust value malicious node is detected and isolated from the network. The reputation score is evaluated by reputation degradation and reputation improvement process. The simulations are performed using network simulator (NS2). The future scope is to incorporate the mechanism in other on-demand routing protocols and to improve the performance of the network. Selfish node is an active attack which severe damage to the network, using the proposed mechanism the selfish node is detected and isolated from the network.

6. REFERENCE

[1] Akanksha Jain, Trust based routing mechanism against black hole attack using AOMDV-IDS system in MANET format, IJETAE ISSN 2250-2459.

[2] A. Rajaram and Dr S. Palaniswami, Malicious node detection system for mobile ad hoc networks, IJCSIT Vol (2) ,2010, 77-85.

[3] Mawloud Omar, Yacine Challal, Abdelmadjid Bouabdallah, Reliable and fully distributed trust model for mobile ad hoc networks, computers and security 28 (2009) 199- 214.

[4] N. Marchang, R. Datta , A light weight trust based routing protocol for mobile ad hoc networks, IET information security 6 (2) (2012) 77-83.

[5] Bo Wang, Xunxun Chen, Weiling Chang, A light weight trust based QOS routing algorithm for ad hoc networks, pervasive and mobile computing 13 (2014) 164-180.

[6] H Yang H Y, Luo F Ye S W,Lu L Zhang, Security in mobile ad hoc networks: Challenges and solutions, University of California Postprints Year 2004, Paper 618.

[7] G.V.S. Raju ,Rehan Akbani, Mobile Ad Hoc Networks Security, University of Texas at San Antonio, Annual review of communication, volume 58.

[8] Lyno Henrique G. Ferraz, Perdo B. Velloso, Otto Carlos M.B. Duarte, An accurate and precise malicious node exclusion mechanisms for ad hoc networks, Ad hoc networks 19 (2014) 142-155.

[9] Ing-Ray Chen, Jia Guo, Fenye Bao, Jin-Hee Cho, Trust management in mobile ad hoc networks for bias minimization and application performance maximization, Ad Hoc Networks 19 (2014) 59–74.

[10] Neha Shrivastava, Anand Motwani, Survey of malicious attacks in MANET, International Journal of Computer Applications (0975 – 8887), Volume 80 – No 14, October 2013.

[11] Hui Xia, Zhiping Jia, Lei Ju, Xin Li, Edwin H.-M. Sha, Impact of trust model on on-demand multi-path routing in mobile ad-hoc networks, Computer Communications 36 (2013) 1078–1093.

[12] Jin-Hee Cho, Ing-Ray Chen, On the tradeoff between altruism and selfishness in MANET trust management.

[13] Anit kumar, Pardeep Mittal, A comparative study of AODV and DSR routing protocols in Mobile ad-hoc networks, ijarcsse, Volume 3, Issue 5, May 2013, ISSN: 2277 128X .

[14] Durgesh Wadbude, Vineet Richariya, An efficient secure AODV routing protocol in MANET, IJEIT, Volume 1, Issue 4, April 2012, ISSN: 2277-3754.

[15] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, Review of Various Routing Protocols for MANETs, International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011.