VOL. 10, NO. 8, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

A TRUST SCHEME FOR DISCOVERING AND QUARANTINE THE MISBEHAVIORS IN MANET

Vijayan R. and Jeyanthi N.
School of Information Technology and Engineering, VIT University, Vellore, India,
E-Mail: rvijayan@vit.ac.in

ABSTRACT

The nodes in mobile adhoc network misbehave due to topology changes, vulnerable medium, short signal range and limited energy. Mobile adhoc networks need collaboration and trust among the nodes for transmission of packets. Many existing schemes in MANETs are having less probability of detecting misbehavior of nodes. This trust scheme includes energy spent by a node; number of packet forwarded parameters in neighbor observation and recommendation trust evaluation. A most trustworthy node will act as certificate issuer. Certificates are required by highly trusted nodes for packet transmission. Misbehaved nodes are discovered and quarantined from routing packets. This scheme can be probable solution in crucial times of natural disaster, manmade disaster, military applications etc. Experimental results are presented with Qualnet Simulator. This proposed framework has shown better results in detecting misbehaving nodes.

Keywords: detecting misbehaviors, trust framework, isolation, misbehaviors.

INTRODUCTION

Mobile Ad hoc Network is a distributed wireless network with nodes mobility. Each node transfers data with the nodes in the same wireless range, and multi-hop transmission with nodes outside the wireless range. Trust is termed as a set of relations among entities participating in a protocol. The trust establishment among the nodes leads for secure packet transmission. Trust establishment schemes provide an incentive for collaboration between the nodes. The Trust is changes and dependent on particular circumstances. The nodes in the MANET are vulnerable to many types of attacks launched through compromised node.

Currently, the trust schemes are available using the schema of passing the packets, drop strategy, size, etc. Thus a new dynamic approach is needed in the system where the nodes communicate with each other and compute their own trust on whatever scenario it is in.

This scheme proposes a trust framework for discovering and isolation misbehavior nodes from participating in transmission process.

RELATED WORKS

In this (Buchegger, S. and J.Y. Le Boudec, 2002) cooperation of nodes fairness in dynamic ad hoc networks (CONFIDANT). CONFIDANT determines the value of trust using direct and indirect monitoring. By these observations, it detects the malicious nodes. CONFIDANT additionally introduces an incentive scheme to reward the genuine nodes that cooperation the routing process.

Fuzzy logic based functions gives accurate results rather than approximate results. Fuzzy logic variables may have trust values that range in degree between 0 and 1. In the proposed scheme (V.R. Ghorpade, 2008) trust decision is based on fuzzy logic and if the evaluated trust is greater than or equal to the threshold trust, then that particular node is called as a trustworthy, else it will be treated as untrustworthy and excluded from all future network operations. It specifies a range for a given trust level ranging from very untrustworthy, untrustworthy, medium trustworthy, trustworthy, very trustworthy (Farag Azzedin, Ahmad Ridha, and Ali Rizvi, 2007).

The proposed trust management framework in (V.R. Ghorpade, 2008) includes Trust agent, Recommendation agent and the Combiner. In this paper the Trust agent derives trust levels from events that are directly experienced/monitored by a node. The Recommendation agent shares trust information about nodes with other nodes in the network. The Combiner computes the final trust in a node based upon the information it receives from the trust and recommendation agents.

In this (Angelo Rossi and Samuel Pierre, 2009) watchdog component monitors its neighbour nodes for behaviour. It is responsible for monitoring the received messages with the purpose of making sure that it has forwarded the message without alteration. Intermediary nodes forward the message to its neighbour and can also verify that the next hop correctly retransmit the message. With the observed behaviour, the node can be termed as trusted or malicious.

The overview of SAODV protocol (Floriano De Rango, 2009) provides security mechanisms based on non-invertible hash functions and public key cryptography. In SAODV, hash chains are applied for the hop count authentication and immutable message contents are digitally signed so that each node, at every hop, can verify that the hop count metric was not maliciously decreased.

The energy of mobile nodes in ad hoc networks is powered by batteries with limited energy. Hence the nodes with minimal energy can turn into selfish nodes. In this research work (M. Pushpalatha, Revathi Venkataraman, T. Ramarao. 2009) the proposed scheme discriminates the selfish and the malicious nodes. The total expenditure at a node is calculated by a devised formula considering the energy spent on transmission and the reception of data packets, acknowledgments and on other nodes.

A query based trust evaluation scheme (Muhammad Ibrahim Channa, Samad Baseer, Kazi M. Ahmed. 2010) for ad hoc emergency response to keep track of the selfish and malicious nodes. The paper uses a trust evaluation scheme which uses an observer and evaluator to calculate and evaluate the trust of the neighboring node respectively. The calculated trust is then stored in the Trust Database which in turn will be used by the protocol.

A new scheme of Adaptive and Robust Reputation mechanism (Maio Wang, Fei Tao, Yujin Zhang, Guojie Li., 2010) where direct trust obtained from customers' experience and recommended trust formalized by the feedback of other customers is balanced according to the experience of the requester. Direct trust value and recommended trust value is then used to calculate the overall trust and is then validated.

The energy of mobile nodes in adhoc networks are powered by batteries with limited energy. Hence the nodes with minimal energy can turn into selfish nodes. In this research work (Vijayan R, Mareeswari V and Ramakrishna K, 2011), the proposed scheme discriminates the selfish and the malicious nodes. The total expenditure at a node is calculated by a devised formula considering the energy spent on transmission and the reception of data packets, acknowledgments and on other nodes.

A Novel Approach for Providing Security in VANET uses Certificate Authority (Vijayan. R, Sumitkumar Singh, 2011). Central authority (CA) nodes are responsible for assigning public and private keys to the requesting nodes in the network. Source nodes requests available CA node for transmission with the destination node. CA validates source and destination nodes and issue certificates for secure transmission.

THE MISBEHAVIOR TRUST SCHEME

Energy is a scarce and non-renewable resource in wireless ad hoc networks. Due to limited resource availability, nodes behave selfishly by saving the battery power without forwarding the packets.

The energy spent at each node is monitored by energy audit. A simple model presenting the energy spent at each node is depicted. Initial energy, receiving power consumption and transmission power consumption details are audited after each packet is encountered. The total node energy expenditure at a node due to another node in the network can be calculated follows.

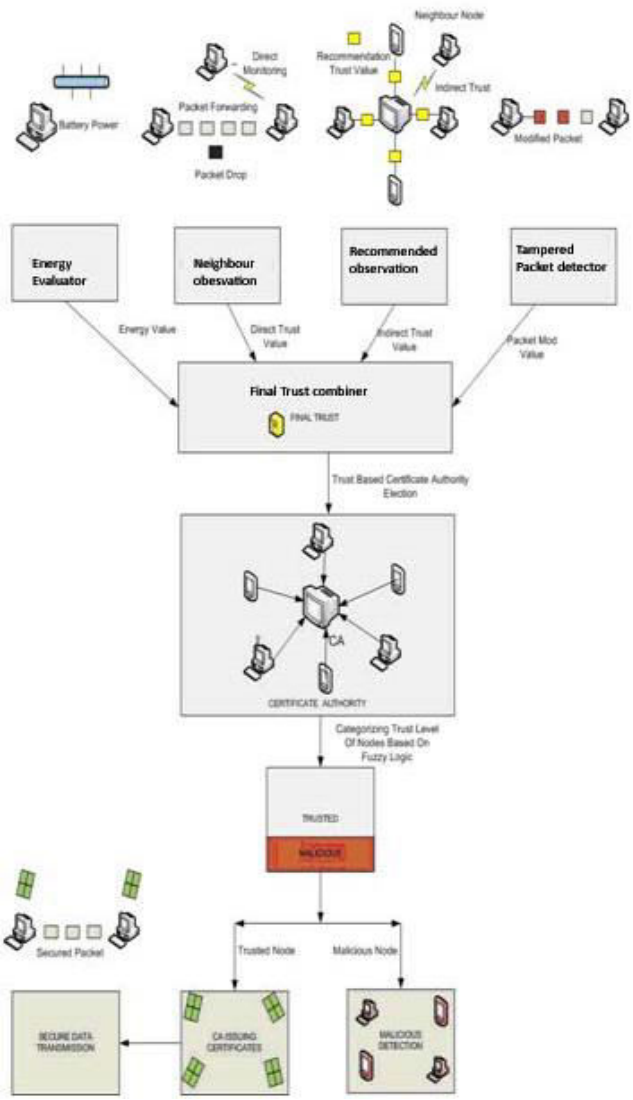

Figure-1. Misbehavior trust scheme.

Energy evaluator

Limited resource availability, nodes will be acting as selfishly by conserving its energy blocking the packets to be forwarded.

The energy utilized at each node is monitored by energy evaluator. The overall node energy utilized at a node by another node in the network can be evaluated as follows.

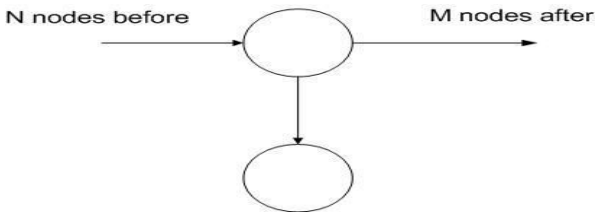

Figure-2. Energy evaluator.

$$E_{\frac{Y}{X}} = p_{n>0}\left(p_{X=Y}E_{T_{ack}} + p_{X\neq Y}E_{R_{ack}}\right) + p_{m>0}\left(p_{X=Y}E_{T_{pck}} + p_{X\neq Y}E_{R_{pck}}\right)$$

Eq - (1)

Where

E_{value} = Energy utilized at node Y due to node X
$E_{T\ ack}$ = Energy utilized for one acknowledgement
$E_{T\ pck}$ = Energy utilized for transmission of one Data packet
$E_{R\ ack}$ = Energy utilized for reception of one ACK Packet
$E_{R\ pck}$ = Energy utilized for reception of one Data packet

Tampered packet detector

Packet Tampering by malicious nodes is a security concern in MANET. An intermediate node tampers the packet content, this can be detected and the packet can be discarded. PT_{value} is a positive value at initial stage and if there is tampering of packets by a node its PT_{value} will get decreased. In this proposed scheme integrity of packet is taken in to account for trust evaluation. The route discovery phase a source node broadcasts a route discovery request (RREQ) towards a destination. This takes its journey through the network upto the intermediate node, which knows the path towards the destination, is met or until the destination node is reached. In request packets hash chains are applied for the hop count authentication so that each node, at every hop, can verify that the hop count metric was not maliciously decreased.

Neighbours observation

This component of the framework watches neighbors by passively listening to their communication; every node in the network monitors the behavior of every other neighbor by employing watch dog mechanism. It observes behavior of the packets send across the network Packet delay, packet drop, and latency by nodes. This module captures data from all the nodes and computes the direct trust level based on their behavior.

Recommended observation

This module requests trust related information of target node from the neighboring nodes. The source node will broadcast the recommendation request packet to all its neighboring nodes. This process obtains recommendation trust of a node from other nodes in the network, which also is an important factor in determining trust levels of the nodes. This component analyzes the indirect trust values obtained from the other nodes and helps in building the trust of the nodes in the network.

Recommended trust algorithm

Obtaining recommended trust

a) Node A broadcasts REQ to all the node(s) n.
b) If any node in n has direct trust value on B, then it will reply back.
c) Else if it does not have direct trust value record it will discard the REQ.
d) After receiving REPLY from nodes Indirect trust analyzer computes trust value

Final trust combiner

Trust Combiner module's task is to compute the final trust value of the target node using direct trust value and recommended trust from direct and indirect trust analyzer respectively and building trust levels of each node in the network.

$$FT_{value} = E_{value} + DT_{value} + IDT_{value} + PM_{value} \quad (2)$$

Where

FT_{value} = Final trust value
E_{value} = Energy value
DT_{value} = Direct trust value
IDT_{value} = Indirect trust value
PM_{value} = Packet modification value

For the trust value of each node, a timeout value is assigned. Once the timeout expires, the process is repeated to compute the trust levels of the nodes and make the trust of the network changes dynamically preventing the malicious behavior of nodes in the cluster. Well behaved nodes are expected to have good reputation collected and suspicious nodes automatically will have a reduced reputation values from the nodes in the cluster. This makes the MANET's reputation to be changed dynamically and make the system secure.

Reputation manager

Reputation Manager Module implements Certificate Authority to assign certificates to the nodes in the network group based on their reputation. The nodes with higher trust values computed by the Reputation collector module are the one's eligible to attain the certificates from the Certificate Authority and the nodes which are malicious are identified and denied certificates making them isolate from participating in the network which makes the system behave secure. Reputation Manager node is elected by the CA election algorithm which is designed to make the highest reputed node in the cluster to take over the responsibility of assigning and revoking certificates from the cluster nodes. Since the reputation changes dynamically Reputation Manager is also elected dynamically.

In the proposed scheme, Reputaion Manager Election algorithm, CA node is selected among group of nodes based on the nodes trust value. Each node sends CA request packet to announce it as Reputation Manager. When a trusted node receives a beacon, from one of its neighbours, it executes CA Election algorithm. Any trusted node with the highest trust value will be elected as CA. CA Reply packet is sent back to the requestor node. Timeout value is set to the CA node. When the timeout value expires or CA node fails, CA election algorithm will be invoked again. Reputation Manager strictly allows only the trusted nodes are eligible for packet transmission.

Trusted nodes need to acquire certificates from the Certificate Authority before packet transmission. Least trusted nodes are marked as malicious and do not have the privilege to transmit packets.

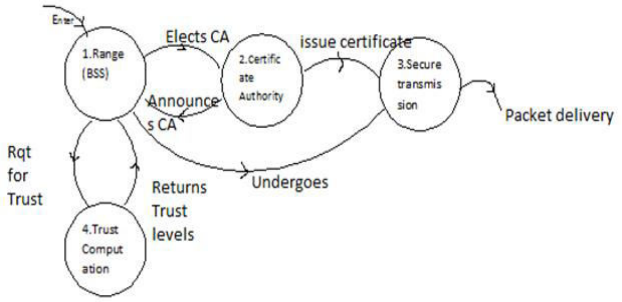

Figure-3. CA election.

Pseudo code for certificate issuing

- Source node A (SID) requests CA node to transmit data packet to Destination node B (DID).
- CA node verifies SID and DID.
- If (ID==SID) CA checks the available destination node and validation is done.
- CA sends CERTA and CERTB to Source node and Destination

$CERTA = [SID, FT_{Value}, PKA, TS]$
$CERTB = [DID, FT_{Value}, PKB, TS]$

Where

SID = Source ID
DID = Destination ID
FT_{Value} = Trust Value
PKA = Source Private Key
PKB = Destination Public Key
TS = Timestamp

- Else Invalid Source message is sent to the Source node A

After the source and destination nodes obtaining certificates from CA, it is eligible for packet transmission. Source node uses private key to hash the packet and forwards it to the destination. Only the destination node can verify the packet using its public key. Hash algorithms are least complex of cryptographic algorithms and should incur least energy cost. In this scheme MD4 is used to hash the packet. Once the timestamp value in the certificate expires, the node has to request CA node for the renewal of certificates. Without certificates data packet transmission cannot take place.

Malicious detector

A node's trust value less than an acceptable range, reputation manager identifies the node as malicious and isolated, other nodes are informed about the malicious nodes. Nodes with low trust are categorized as being misbehaving nodes in the network and are quarantine from participating transmitting packets in the network. Malicious nodes can never acquire certificates from the Reputation Manager CA node and are isolated until its trust level increases and the node becomes acceptable as trusted node.

SIMULATION ANALYSIS AND RESULTS

Qualnet 5.0 network simulator is used to simulate a wireless network with AODV protocol. Figure-4 shows a scenario with 7 nodes and the traffic flow among them. These nodes are labelled, ranging from Node 0 to Node7.Constant Bit Rate (CBR) traffic is defined between Node 1 to Node 7, Node 1 to Node 4, Node 3 to Node6, Node 2 to Node 7, Node 5 to Node 7. The simulation detects the malicious nodes based on computed trust values.

Table-1. Simulation parameters-scenario-I.

Parameter	Values
MAC	IEEE802.11
Routing protocol	AODV
Initial Energy	100
Reception Power	1.049 W
Transaction Power	1.6787W
Idle Power	0.6699W
Simulation time	1 min
No. of nodes	7
Mobility Model	Random Waypoint
Traffic type	CBR
Payload size	512 bytes

Table-2. Simulation parameters-scenario-II.e.

Parameter	Values
MAC	IEEE802.11
Routing protocol	AODV
Simulation time	1 min
Initial Energy	100
Reception Power	1.049 W
Transaction Power	1.6787W
Idle Power	0.6699W
No. of nodes	14
Mobility Model	Random Waypoint
Traffic type	CBR
Payload size	512 bytes

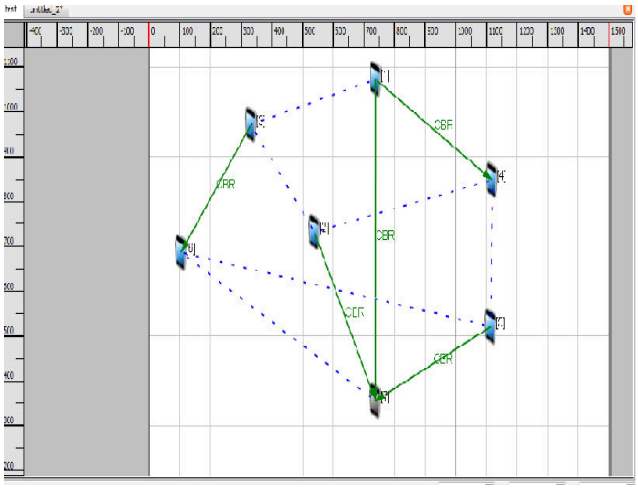

Figure-4. Simulation scenario-I.

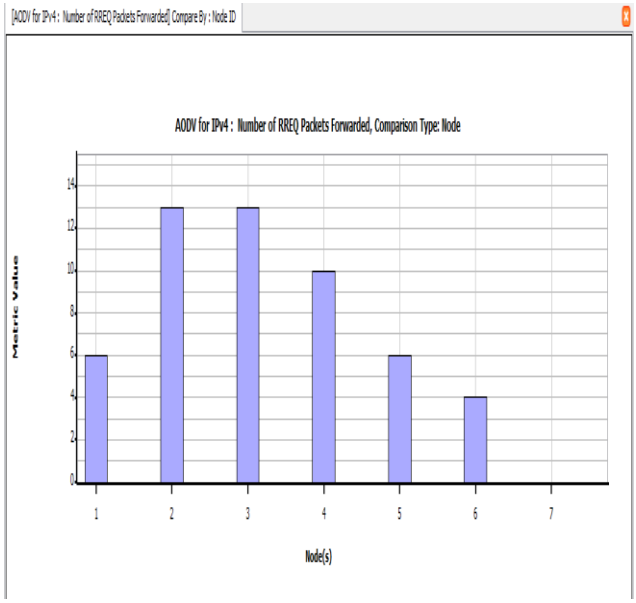

Figure-5. Metric value of the nodes.

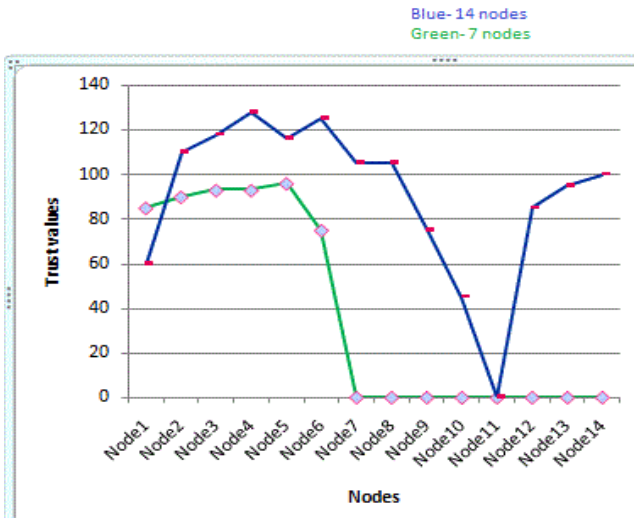

Figure-6. Trust values for two scenarios.

The graph is plotted with two different scenarios with 14 and 7 nodes as shown in Figure-6. From this implementation of our framework, Nodes 6, 7 in 7 Node model and Node 1, 10, 11 in 14 Node model are marked as malicious and isolated, building a secure network.

CONCLUSIONS

This trust scheme gives two secure levels, first is trust, and only trusted nodes can transmit packets and second packet is transmitted with the assistance from Certificate Authority to make the system reliable and secure. The malicious nodes are detected and isolated from the network. This approach provides an efficient trust scheme for discovering and quarantine the misbehaviors in MANETs and in later stages of implementation, simulation results and analysis will be published.

This proposed framework for MANET is well suited for Disaster Management and critical Military applications where the data transmission needs to be more secure and energy efficient.

REFERENCES

Angelo Rossi and Samuel Pierre. 2009. Collusion-resistant reputation-based intrusion detection system for MANETs. IJCSNS International Journal of Computer Science and Network Security. 9(11).

V. R. Ghorpade. 2008. Fuzzy Logic based Trust Management Framework for MANET. DSP Journal. 8(1).

Vijayan R, Mareeswari V and Ramakrishna K. 2011. Energy based Trust solution for Detecting Selfish Nodes in MANET using Fuzzy logic. International Journal of Research and Reviews in Computer Science (IJRRCS). 2(3).

Farag Azzedin, Ahmad Ridha, and Ali Rizvi.2007. Fuzzy Trust for Peer-to-Peer Based Systems, World Academy of Science, Engineering and Technology 27.

Floriano De Rango. 2009. Improving SAODV Protocol with Trust levels management, IDM and Incentive Cooperation in MANET, Wireless Telecommunications Symposium.

Vijayan. R, Sumitkumar Singh. 2011. A Novel Approach for Providing Security in Vehicular Adhoc Network through Vehicles Present in the Network. International Journal of Advanced Research in Computer Science. 2(1).

A. Rajaram and Dr. S. Palaniswami. 2010. A High Certificate Authority Scheme for Authentication in Mobile Ad hoc Networks. IJCSI International Journal of Computer Science Issues. Vol. 7, Issue 4, No. 5.

Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan and Niraj K. Jha. 2006. A Study of the Energy Consumption Characteristics of Cryptographic

Algorithms and Security Protocols. IEEE transactions on mobile computing. 5(2).

G.S. Mamatha and Dr. S. C. Sharma.2010. A Highly Secured Approach against Attacks in MANETS. International Journal of Computer Theory and Engineering. 2(5).

M Rajesh Babu, Selvan S. 2010. A Lightweight and Attack Resisitant Authenticated Routing Protocol For Mobile Adhoc Networks. International Journal of Wireless and Mobile Networks (IJWMN). 2(2).

Manoj V., Raghavendiran N., Aaqib M., Vijayan R. 2012. Trust Based Certificate Authority for Detection of Malicious Nodes in MANET, Global Trends in Computing and Communication Systems, Communications in Computer and Information Science. 269: 392-401.

Muhammad Ibrahim Channa, Samad Baseer, Kazi M. Ahmed. 2010. A Query Based Trust Evaluation Scheme for Emergency Response Communication Networks. IJCA Special Issue on "Mobile Ad-hoc Networks. 1(4).

Maio Wang, Fei Tao, Yujin Zhang, Guojie Li. 2010. An Adaptive and Robust Reputation Mechanism for P2P Network, Peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE ICC 2010 proceedings.

M. Pushpalatha, Revathi Venkataraman, T. Ramarao. 2009. Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks. World Academy of Science, Engineering and Technology. 3: 08-27.

Buchegger S. and J.Y. Le Boudec. 2002. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc.

Networking and Computing, June 9-11, Lausanne, Switzerland. pp. 226-236.