Conviction Scheme for Classifying Misbehaving Nodes in Mobile Ad Hoc Networks

S. Sridhar[1] and R. Baskaran[2]

[1] Dept. of Computer Applications, Easwari Engineering College, Chennai
ssridharmca@yahoo.co.in
[2] Dept. of Computer Science and Engineering, CEG, Anna University, Chennai
dr.baskaran10@gmail.com

Abstract. A Mobile ad-hoc network (MANET) is a wireless network, self-configuring, capable of self-directed operation, hastily deployable and operates without infrastructure. Nodes cooperate to provide connectivity, operates without centralized administration. Nodes are itinerant, topology can be very dynamic and nodes must be able to relay traffic since communicating nodes might be out of range. The dynamic nature of MANET makes network open to attacks and unreliability. A node may be unsuccessful to cooperate during routing, sometimes may even disturb the routing transaction. The Qos parameters like PDR, throughput and delay are affected directly due to such behavior of nodes and it is termed as misbehaving nodes. A trust-based system can be used to track this misbehaving of nodes, spot them and isolate them from routing and provide reliability. In this paper a trust based reliable AODV protocol is presented which implements a trust value for each node. Every node is defined as reliable node if its trust value is greater than threshold value, if not it's a misbehaving node. This enhances reliability in AODV routing and results in increase of PDR, decrease in delay and throughput is maintained. This work is implemented and simulated on NS-2. Based on simulation results, the proposed protocol provides more consistent and reliable data transfer compared with normal AODV, if there are misbehaving nodes in the MANET.

Keywords: Ad-hoc, AODV, MANET, Trust, Misbehaving node, Qos.

1 Introduction

Mobile ad-hoc network is an extraordinarily testing vibrant network. They don't rely on existing infrastructure to support communication. Each mobile node acts as an end node when it is the source or destination of a communication and forwards packets for other nodes when it is an intermediate node of the route. Mobile Ad-Hoc network [1] is a system of wireless mobile nodes that self-organizes itself in dynamic and temporary network topologies. Mobile ad hoc networks are suitable for dynamic environment where no infrastructure or temporarily established mobile applications are used, which are cost effective. Ad hoc networks are easier to deploy than wired networks and are found many applications, such as in rescue, battlefields, meeting

N. Meghanathan et al. (Eds.): CCSIT 2012, Part II, LNICST 85, pp. 586–593, 2012.

rooms etc., where either a wired network is unavailable or deploying a wired network is inconvenient. Distributed state in unreliable environment, dynamic topology, limited network capacity, variable link quality, interference and collisions, energy-constrained nodes, flat addressing, scaling issues, heterogeneity are few challenges faced by MANET. Mobile ad hoc network routing protocols face some challenges like node mobility that causes frequent topology changes , the changeable and erratic ability of wireless links and packet losses. Mobile nodes also face troubles like limited power, computing and bandwidth resources.

There have been many ad-hoc routing protocols, which fall into several categories: proactive routing protocols such as dynamic Destination-Sequenced Distance-Vector routing (DSDV), Optimized Link State Routing (OLSR), Topology Broadcast based on Reverse Path Forwarding (TBRPF), on-demand routing protocols such as Dynamic Source Routing (DSR), AODV, Signal Stability-based Adaptive routing (SSA). Proactive routing protocols have little delay for route discovery and are robust enough to link breaks and obtain a global optimal route for each destination. However, their routing overhead is also high. On-demand routing protocols are easy to realize and their overhead is low. But routes in on-demand routing protocols are easy to break in the case of topology variations. In AODV [2] node doesn't have any information about other nodes until a communication is needed. By broadcasting HELLO packets in a regular interval, local connectivity information is maintained by each node. Local connectivity maintains information about all the neighbors.

Recent Qos solutions are planned to operate on trusted environments and totally assume the participating nodes to be cooperative and well behaved [3,4]. Such assumptions are not valid in dynamic environments like MANETs. Providing different quality of service levels in a persistently changing environment is a challenge because: Unrestricted mobility causes QoS sessions to suffer due to recurrent path breaks, thereby requiring such sessions to be reestablished over new paths. The link-specific and state-specific information in the nodes is inherently imprecise due to the dynamically changing topology and channel characteristics. Hence, incorrect routing decisions may chop down Qos parameters performance. Inadequate bandwidth, storage space and battery life also drastically influence the performance of the QoS parameters.

This traditional AODV is to perform its job based on the trust values calculated for each node and to decide whether to take part or to be isolated from routing. The trust value is calculated for each node and based on this trust value AODV decides whether the corresponding node is still reliable or not. If nodes trust value is less than the threshold then the node is declared to be misbehaving node and an alternate path is selected. This trust based routing mechanism helps to identify and eliminate misbehaving nodes in MANET and performs an efficient and effective routing, which results in improving Qos parameters like PDR, throughput and delay.

2 Literature Survey

Mobile ad hoc networks are apt for mobile applications either in antagonistic environments where no infrastructure is available, or temporarily established mobile

applications, which are cost decisive. In recent years, application domains of mobile ad hoc networks gain more and more significance in non-military public organizations and in commercial and industrial areas. Medium access control, routing, resource management, quality of service and security are the research areas for mobile ad hoc network. The importance of routing protocols in dynamic networks has directed a lot of mobile efficient ad hoc routing protocols.

A security-enhanced AODV routing protocol called R-AODV (Reliant Ad hoc On-demand Distance Vector Routing) [5] uses a modified trust mechanism known as direct and recommendations trust model and then incorporating it inside AODV. This enhances security by ensuring that data does not go through malicious nodes that have been known to misbehave. Each node is given a trust value and this value is associated with the possibility of the node to perform a packet drop. With the inclusion of trust mechanism, it is expected that using R-AODV would result in a higher percentage of successful data delivery as compared to AODV. It is also expected that the normalized routing load and end-to-end delay would increase.

A framework for estimating the trust between nodes in an ad hoc network based on quality of service parameters using probabilities of transit time variation, deleted, multiplied and inserted packets, processing delays to estimate and update trust [6]. This paper clearly shows that only two end nodes need to be concerned and attain reduced overhead. The framework proposed in this paper is applicable and useful to estimate trust in covert unobservable and anonymous communications. This results in detecting regular packets drops and delay detection.

A schema is formed via direct and indirect approach to compute trust value among anonymous nodes [7]. To evaluate trust values the parameters like reputation, knowledge, observation and context were used. The trust schema that is build is used to allow resource to be shared among trusted nodes. The result obtained is then mapped with the access privileges to take appropriate actions.

A routing protocol, which adds a field in request packet and also stores trust value indicating node trust on neighbor based on level of trust factor [8]. The routing information will be transmitted depending upon highest trust value among all. This not only saves the node's power by avoiding unnecessary transmitting control information but also in terms of bandwidth (channel utilization), which is very important in case of MANET. The malicious node can attack on the control packet and misbehave in the network. A trusted path is used irrespective of shortest or longest path, which can be used for communication in the network. It calculates route trust value on the complete reply path, which can be utilized by source node for next forthcoming communication in the network. Thus security level is improved and also malicious node attacks are prevented in the network.

A trust model introduced in the network layer leads to a secure route between source and destination without any intruders or malicious nodes in the network [9]. This trust based routing protocol concentrates both in route and node trust. Node Trust Calculation Process is done by introducing a new data structure neighbor table in each node of the MANET. Node trust is calculated by the collective opinion of node's neighbors. The resultant trust value is placed in trust value field of neighbor table. Node trust calculated based upon the information that one node could collect

about the other nodes. Route Trust Calculation Process is done using a modified extended route table. With this minimum overhead, eliminates the malicious node as well as establish a best-trusted route between source and destination.

TAODV [10], an enhanced AODV protocol was proposed with a concept of trust values for calculating trust values of nodes. The changes made to the existing protocol are, two new control packets TREQ (Trust request) & TREP (Trust Reply) and a modified extended routing table with four new fields; positive events, negative events, route status, opinion. This provided a reliable routing.

3 Proposed Work

Routing in mobile ad hoc networks is pretentious due to the dynamic nature of nodes, which are not stable and keep moving. But still nodes communicate with each other and exchange data within the available nodes on the network. The architecture of the proposed work is presented in Fig. 1.The node trust plays a very crucial role in MANET routing. Trust factor here focuses on identifying the misbehaving nodes and helps nodes to select an alternate path to carry on routing successfully. The proposed work concentrates on identifying misbehaving nodes using the trust level values. For every node a trust level value is calculated and if this value decreases below the threshold value then the node is declared as misbehaving node and an alternate path is selected.

The trust level value calculation is based on two main parameters qrs and qrf, where qrs is defined as rate of success which is calculated based on number of neighboring nodes who have successfully received (rreq) from the source node and qrs defined as rate of failure which is calculated based on number of successful replies (rrep) received by the source node which has sent rreq.

$$Qrreq_i = \frac{qrs - qrf}{qrs + qrf} \cdots Qrreq \neq 0 \tag{1}$$

$$Qrrep_i = \frac{qrs - qrf}{qrs + qrf} \cdots Qrrep \neq 0 \tag{2}$$

$$TL = T_i(rreq) * Qrreq_i + T_i(rrep) * Qrrep_i \tag{3}$$

Where, TL is the trust level value and T_i(rreq) & T_i (rrep) are time factorial at which rreq and rrep are sent by the nodes respectively and it is calculated as 1 plus hop counts and i varies from 1 to number of nodes taking part in routing and Qrrep and Qrreq are intermediate values. Using the above-mentioned formula the trust level value is calculated for each node during routing and is checked against the threshold value (assumed to be as 5). If lesser than threshold then node is a misbehaving node

and will not be suitable for further routing and an alternate path is selected for further routing. This checks every node with its trust value to make itself robust and trustworthy for effective and efficient routing.

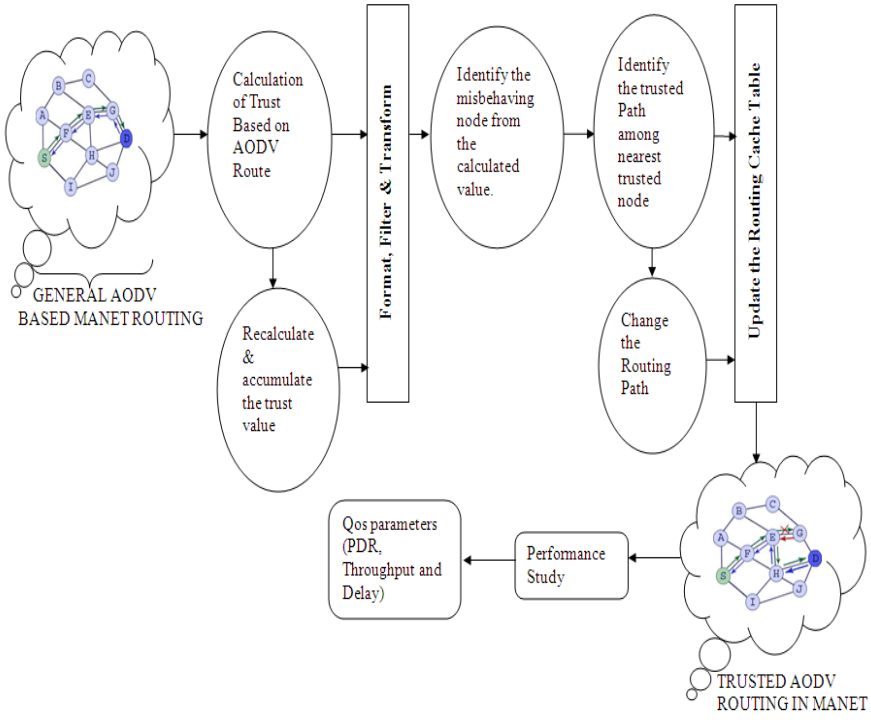


Fig. 1. Architecture of trust based AODV routing in MANET

4 Evaluation Results

The recital of proposed trust based AODV protocol is analyzed using NS-2 simulator. The network is designed using network simulator with maximum of 50 nodes. Other parameters based on which the network is created are given in Table1. Results are obtained from this simulation applying both general AODV and proposed AODV protocols. The proposed AODV protocol has shown good improvement over the QoS parameters like PDR & Delay. PDR is increased and delay is reduced compared to the general AODV. Throughput is maintained. Graphs are used to compare the results of the existing AODV and proposed AODV protocol and clearly indicate the improvement of the proposed protocol.

Table 1. Simulation Parameter Values

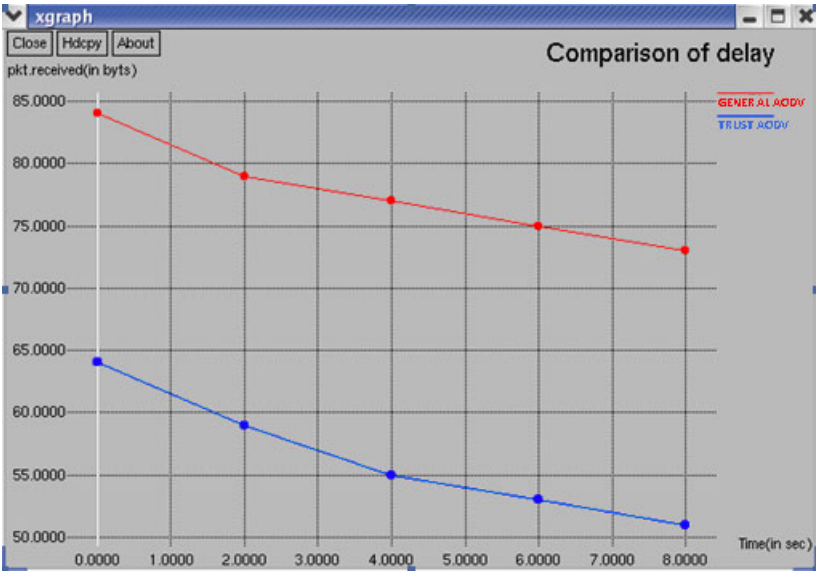
Parameter	Value
Network size	1600 x 1600
Number of nodes	50
Transmission range	250 meters.
Movement speed	100 kbps
Traffic type	CBR
Packet size	5000
Simulation time	30 minutes.
Maximum speed	100 kbps
Time interval	0.01 sec.
MAC layer protocol	IEEE 802.11
Protocol	AODV
NS2 version	2.34

Simulation results were obtained and compared. The results show a good improvement than the exiting approach. The proposed protocol has performed well than the existing AODV protocol which lacks in Qos parameters like PDR and delay when compared with the proposed AODV protocol. The results obtained are shown in Table 2, which shows the values obtained using general AODV and proposed AODV at different node sizes. The traditional AODV is affected due to the existence of misbehaving nodes, which results in low packet delivery ratio and also causes the delay to increase. The proposed protocol has shown improved Qos parameters values where trust values are used to identify the misbehaving nodes in the route and immediately take an alternate path to successfully complete the routing. This approach of the proposed AODV protocol has resulted in an increased packet delivery ratio and a decreased delay involved in routing.

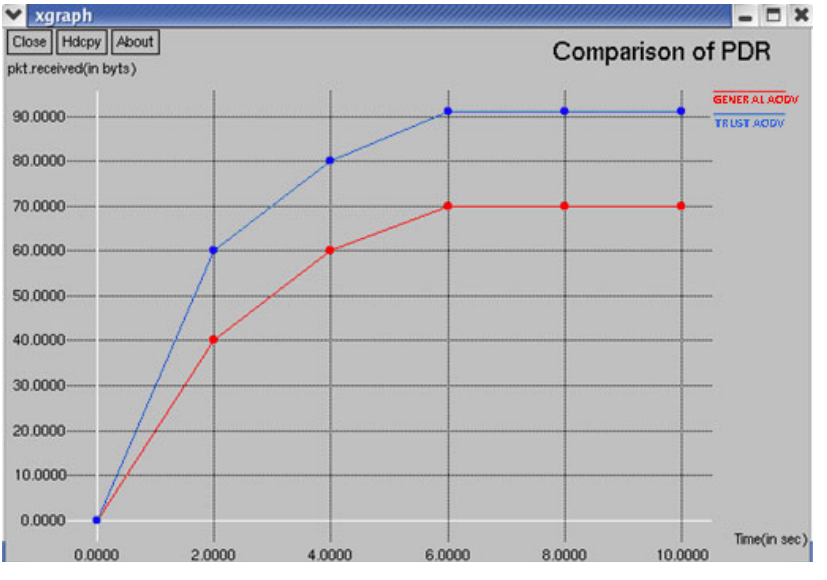
Table 2. Comparison of Result with node size

Node Size	General AODV			Proposed Trust based AODV		
	PDR	Delay	Throughput	PDR	Delay	Throughput
25	82.98	0.24615	75771.43	92.20	0.22153	75771.43
50	70.05	0.84972	114559.89	91.06	0.64979	114559.89
100	64.43	1.44347	148339.67	90.03	0.92683	148339.67
200	62.36	1.65589	150748.56	84.32	0.93536	150748.56
300	60.65	1.78687	150836.74	81.26	0.94825	150836.74

Graph 1 indicates how the proposed protocol has shown a good decrease in Delay when compared to the general AODV. Graph 2 shows the increase in PDR when compared with the general AODV.



Graph 1. Comparison of general AODV Delay and Trust based AODV Delay



Graph 2. Comparison of general AODV PDR and Trust based AODV PDR

5 Conclusion and Future Enhancements

In this paper, a trust based AODV protocol is proposed. Trust level values for each node are calculated to identify the misbehaving nodes during routing. A node is declared as misbehaving nodes if their trust level value is less than the threshold value and this leads to an alternate path selection for further routing. This trust based routing mechanism has proved to be increasing the performance of the proposed protocol and also shows good improvement of Qos parameters like PDR and delay. The same scheme can also be implemented on other MANET routing protocols and also implement some techniques for authenticating the packet and the node which take part in routing.

References

1. Kortuem, G., Schneider, J., Preuitt, D., Thompson, T.G.C., F'ickas, S., Segall, Z.: When Peer to-Peer comes Face-to-Face: Collaborative Peer-to-Peer Computing in Mobile Ad hoc Networks. In: 1st International Conference on Peer-to-Peer Computing, Linkoping, Sweden, pp. 75–91 (August 2001)
2. Perkins, C., Royer, E., Das, S.: Ad hoc on-demand Distance Vector Routing, RFC-3651
3. Hu, Y.: Enabling Secure High-Performance Wireless Ad Hoc Networking, PhD Thesis, Carnegie Mellon University, CMU (2003)
4. IIyas, M.: The Handbook of Wireless Ad Hoc Network, CRC (2003)
5. Jassim, H.S., Yussof, S.: A Routing Protocol based on Trusted and shortest Path selection for Mobile Ad hoc Network. In: IEEE 9th Malaysia International Conference on Communications (2009)
6. Umuhoza, D., Agbinya, J.I.: Estimation of Trust Metrics for MANET Using QoS Parameter and Source Routing Algorithms. In: The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (2007)
7. Abu Bakar, A., Ismail, R., Jais, J.: Forming Trust in Mobile Ad -Hoc Network. In: 2009 International Conference on Communications and Mobile Computing (2009)
8. Mangrulkar, R.S., Atique, M.: Trust Based Secured Adhoc on Demand Distance Vector Routing Protocol for Mobile Adhoc Network (2010)
9. Menaka, A., Pushpa, M.E.: Trust Based Secure Routing in AODV Routing Protocol (2009)
10. TAODV: A Trusted AODV Routing protocol for Mobile ad hoc networks (2009)