World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:3, No:8, 2009

Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks

M. Pushpalatha, Revathi Venkataraman, and T. Ramarao

***Abstract*—**Trust and Energy consumption is the most challenging issue in routing protocol design for Mobile ad hoc networks (MANETs), since mobile nodes are battery powered and nodes behaviour are unpredictable. Furthermore replacing and recharging batteries and making nodes co-operative is often impossible in critical environments like military applications. In this paper, we propose a trust based energy aware routing model in MANET. During route discovery, node with more trust and maximum energy capacity is selected as a router based on a parameter called 'Reliability'. Route request from the source is accepted by a node only if its reliability is high. Otherwise, the route request is discarded. This approach forms a reliable route from source to destination thus increasing network life time, improving energy utilization and decreasing number of packet loss during transmission.

***Keywords*—**Mobile Ad Hoc Networks, Trust, Energy, Reliability, AODV, TEA-AODV.

I. Introduction

MOBILE Ad Hoc Networks [1, 2] are formed by devices that are able to communicate with each other using a wireless physical medium without having to resort to a pre-existing network infrastructure. A fundamental characteristic of ad hoc networks is that they are able to configure themselves on-the-fly without the intervention of a centralized administrator.

Routing protocols in MANET's are generally classified as pro-active and re-active [2]. The re-active protocols had gained more attraction as it reduces routing overheads. Many of the work reported on routing protocols have focused only on shortest path, power aware and minimum cost [2]. However much less attention has been paid in making the routing protocol to choose a more reliable route.

In critical environments like military operations, data packets are forwarded to destination through reliable intermediate nodes[2]. Hence our work focuses on augmenting the existing re-active protocols and making them reliable. We have used AODV (Ad hoc on-demand distance vector) as the base on-demand routing protocol for our model. The technique used is more generic and can be applicable to other on demand protocols like Dynamic source routing protocol (DSR) [2].

The paper is organized as follows: In Section II, we briefly describe the related work. In Section III, we describe our proposal as an extension of AODV. In Section IV, we evaluate the performance via simulation.

II. Related Work

Considerable amount of work that has been done in energy aware routing and little work is done in trust evaluation. This section gives the overview of some proposed protocols that are related to energy balance and trust evaluation in reactive protocols. In [3], Gupta Nishant and Das Samir had proposed a technique to make the protocols energy aware by using a new routing cost metric which is the function of the remaining battery level in each node on a route and number of neighbours of the node. This protocol gives significant benefits at high traffic but at low mobility scenarios. In [4], Rekha Patil etal, has proposed an approach in which the intermediate nodes calculate cost based on battery capacity. The intermediate node judges its ability to forward the RREQ packets or drop it. This protocol improves packet delivery ratio and throughput and reduces nodes energy consumption. M.Tamailarasi etal, [5] has discussed the mechanism that integrates load balancing approach and transmission power control approach to maximize the life span of MANET. The results of this proposal reduce the average required transmission energy per packet compared to the standard AODV.

In [6] Pushpalatha & Revathy have proposed a trust model in DSR protocol that categorize trust value as friend, acquaintance and stranger based on the number of packets transferred successfully by each node. Route from source to destination is determined by selecting the most trusted path. Here battery capacity is not considered as an issue for selecting the path between source and destination. Results show that the packet loss is very minimum when compared to the conventional DSR. Huafeng Wu & Chaojian Shi1 [7] has proposed the trust management model to get the trust rating in peer to peer systems, and aggregation mechanism is used to indirectly combine and obtain other node's trust rating. The result shows that the trust management model can quickly detect the misbehaviour nodes and limit the impacts of them in a peer to peer file sharing system. The above papers have dealt the parameters battery power or trust of a node individually. Our proposal combines these two parameters to discover a reliable route between the source and destination.

M. Pushpalatha is with the Department of Computer Science and Engineering, S.R.M University, Chennai, India (phone: +91 9940237641; e-mail: lathamarudappa@yahoo.co.in).

Revathi Venkatraman is with the Department of Computer Science and Engineering, S.R.M University, Chennai, India (e-mail: revathivenkat@ yahoo.com).

T. Ramarao is with the Telecommunication and Engineering Department, S.R.MUniversity, Chennai, India (e-mail: ramarao@ieee.org).

III. Trust Based Energy Aware AODV (TEA-AODV) Model

This section presents a novel efficient reactive routing algorithm that generates a reliable route between source and destination.

A. Overview of AODV

It is one of the most popular MANET routing protocols [8] named as re-active or on-demand protocols. Upon arrival of data if no route exist, source broad cast a route request to the destination. Each intermediate node hop automatically builds a reverse route to the source and also rebroadcast the route request .The destination replies to the first route request and send a route reply in the direction it was received. The conventional AODV finds the shortest path between the source and destination. Our objective is to generate "reliable routing" instead of minimum hop routing.

B. TEA-AODV Mechanism

The two main parameters that make the routing algorithm more reliable are trust value of each node and battery capacity of each node. Before seeing the algorithm in detail, trust estimation and power consumption mechanism are explained below.

1) *Trust Evaluation*

Trust value of each node is evaluated based on the various parameters like length of the association, ratio of number of packets forwarded successfully by the neighbors to the total number of packets sent to that neighbour and average time taken to respond to a route request [6]. Based on the above parameters trust level of each node can be of the following types:

a) Node i is a stranger(S) to neighbour node j

If node i has never send/ received messages to/from node j.

b) Node i is a acquaintance (A) to neighbour node j

If node i has send/receive few messages from node.

c) Node i is a friend (F) to neighbour node j

If node i has send/receive plenty of message to/from node j.

Trust value is initially set to zero. It is incremented based on how many numbers of packets are successfully transmitted from node i to node j. Following Table I show the trust levels and corresponding trust value that is used to determine the reliable route.

TABLE I
Trust Estimation of a Node

Trust level	Trust value
F	0.7 - 1.0
A	0.4 - 0.6
S	0.0 – 0.3

2) *Power Consumption*

Every node in the MANET calculates its power consumption and finds the remaining energy periodically. Each node may operate in any of the following modes [9, 10]:

a) Transmission mode

The power consumed for transmitting a packet is given by the Eq (1)

$$\text{Consumed energy} = P_t * T \quad (1)$$

Where P_t is the transmitting power and T is transmission time.

b) Reception mode:

The power consumed for receiving a packet is given by Eq (2)

$$\text{Consumed energy} = P_r * T \quad (2)$$

Where P_r is the reception power and T is the reception time. The value T can be calculated as

$$T = \text{Data size} / \text{Data rate} \quad (3)$$

Hence, the remaining energy of each node can be calculated using Eq (1) or Eq(2)

$$\text{Rem energy} = \text{Current energy} - \text{Consumed energy} \quad (4)$$

Other two modes like sleep and idle are not considered in our proposal. Initially every node has full battery capacity say 100% which is assigned to current energy .On each transmission or reception of a data packet the remaining energy is found using the Eq(4). If the remaining energy falls below 50%, that node will not act as a router to forward the packets.

3) *Reliability Relation*

In Table II, the relationship of trust value and the remaining energy of each node is given which determines the reliability of a node.

TABLE II
Reliability Value of Each Node

Trust Value	Remaining Energy %	Reliability (R)	Reliability Value
0.7 – 1.0	80 - 100	Very Very high	1.0
0.4 – 0.6	80 - 100	Very high	0.8
0.7 – 1.0	50 - 79	High	0.6
0.4 – 0.6	50 - 79	Medium	0.4
0.0-0.3	50 - 100	Low	0.2
-	00-40	Very low	0.0

4) *TEA-AODV Algorithm*

Route request

1. When source node wants to communicate with another node (destination),if no routing information is available, it initiates path discovery by sending the route request that contains source id, broadcast id, destination id

and trust values of each neighbour and reliability of source node and, hop count.

2. On accepting the route request the neighbour node calculates its reliability using Table II by checking its trust value and the remaining energy and takes the following decision.

If the reliability is very low (0.0)

The node discards the route request

Else if

The reliability is an acceptable value,cumulative reliability is found by adding the predecessor reliability with its reliability. If the node has already received the route request with same source address and same broad cast id and if the cumulative reliability is less than the cumulative reliability of current route request, the previous route request path is rejected and the current route request path is recorded.

3. The route request is then forwarded to the intermediate nodes's neighbours which contains trust values of each neighbour and cumulative reliability. Each time when route request is forwarded from one node to another, hop count is incremented and that is also send along with the route request.

Route Reply

1. When two or more route request reaches the destination from the same source and same broadcast id and in different path, it selects the most reliable path by finding the average reliability . Average reliability is computed as follows:

Avg reliability = Cumulative reliability / Number of hops

2. If average reliability of one path is greater than reply another path, that path is selected and the route is send by the destination in that path to the source.

3. The source receives the new path and sends the packet in that reliable path and record the path for future use.

IV. Simulation Setup and Results

We simulated our proposal using Opnet 14.5 [11]. In our experiments 50 nodes are in a rectangular area of 1500m X 300m. Each node uses IEEE 802.11 standard MAC layer. The radio range is of 250m. Each packet (data) size is 512 bytes and data rate is 11 Mbps. Initial energy of a battery of each node is 3.6 Watts which is mapped to 100%. The power consumed for transmission of each packet is 280 mA and reception of each packet is 180 mA. Simulation runs for 900 seconds.

The results in Fig. 1 and Fig. 2 shows that TEA-AODV experience a high end to end delay because route selection is based on trust and energy level not on the minimum number of hops. The results in Fig. 3 and Fig. 4 shows that number of packets dropped in TEA-AODV is minimum compared to conventional AODV. Number of packets dropped is 50% more in conventional AODV. In TEA-AODV packet drops can be reduced to 0 % if mobility of nodes is predicted in the algorithm.

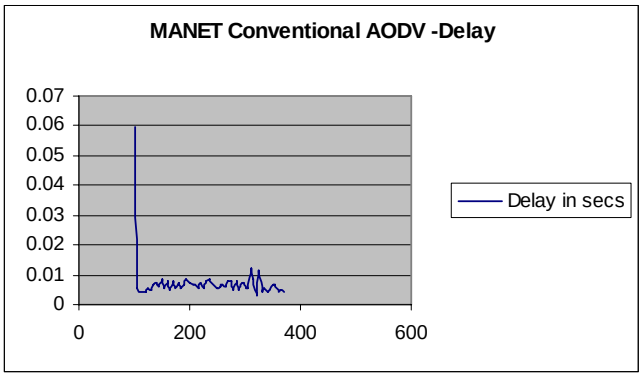

Fig. 1 AODV Delay

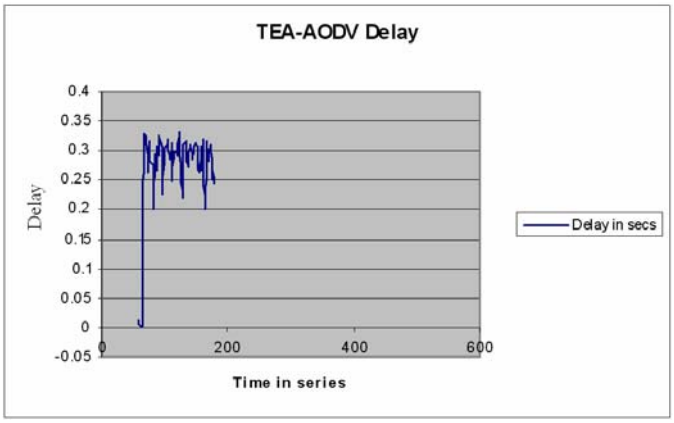

Fig. 2 TEA-AODV Delay

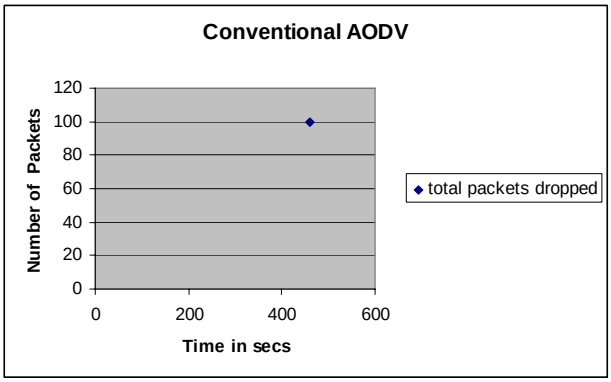

Fig. 3 Packet drop in Conventional AODV

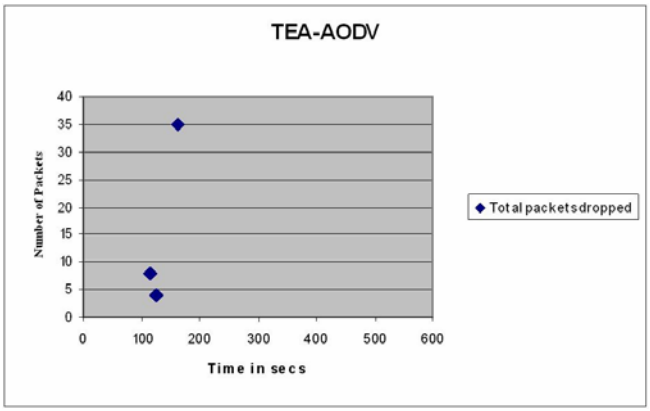

Fig. 4 Packet drop in TEA-AODV

V. Conclusion and Future Work

Our proposed work is an extension of conventional AODV. This novel protocol can work in critical environment like military scenarios. The simulation results shows that our approach decreases packet drops and improves reliability .The life time of the network and each node is increased by choosing more reliable node as a router to route the packets. Our future work will highlight the mobility issues and our proposal can be extended to other reactive protocols also.

Acknowledgment

The authors wish to acknowledge SRM University, Chennai, India for its continual support to carry out this work.

References

[1] C. Sivaram Murthy and B.S Manoj, "Ad Hoc Wireless Networks", Pearson Education, Second Edition India, 2001.
[2] "Tutorial on wireless ad hoc networks" by David Remondo, Second International Conference in Performance Modeling and Evaluation of heterogeneous networks, July 2004.
[3] Gupta Nishant, Das Samir, "Energy-aware on-demand routing for mobile Ad Hoc networks," Lecture notes in computer science ISSN: 0302-743, Springer, International workshop in Distributed Computing, 2002.
[4] Rekha Patil , A.Damodaram, "Cost Based Power Aware Cross Layer Routing Protocol For Manet", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, December 2008.
[5] M.Tamilarasi, T.G Palani Velu, "Integrated Energy-Aware Mechanism for MANETs using On-demand Routing", International Journal of Computer, Information, and Systems Science, and Engineering 2;3 © www.waset.org Summer 2008.
[6] M.Pushpalatha, Revathi Venkatraman, "Security in Ad Hoc Networks: An extension of Dynamic Source Routing", 10th IEEE Singapore International conference on Communication Systems Oct 2006,ISBN No:1-4244-0411-8,Pg1-5.
[7] Huafeng Wu1, Chaojian Shi1," A Trust Management Model for P2P File Sharing System", International Conference on Multimedia and Ubiquitous Engineering, IEEE Explore 978-0-7695-3134-2/08, 2008.
[8] "An AODV Tutorial' by Ravindra Vaishyapaiyan, www.cse.ucsc.edu/~ravindra/aodv.html.
[9] Laura, Eenergy Consumption Model for performance analysis of routing protocols in MANET,Journal of mobile networks and application 2000.
[10] LIXin MIAO Jian –song," A new traffic allocation algorithm in AD hoc networks, "The Journal of China University of Post and Telecommunication", Volume 13. Issue 3. September 2006.
[11] OPNET Technologies,www.opnet.com.