

A Routing Protocol Based on Trust for MANETs

Cuirong Wang^{1,2}, Xiaozong Yang¹, and Yuan Gao²

¹ School of Computer Science & Technology, Harbin Institute of Technology, 150001 Harbin, China

² Qinhuangdao School, Northeastern University, 066000 Qinhuangdao, China
wangcr@mail.neuq.edu.cn

Abstract. Ad hoc network is a peer-to-peer grid system. The combination of the Knowledge Grid and ad hoc network could have a great effect on the future interconnection environment. In the existed researches about ad hoc routing protocols, knowledge with trusted requirements is not supported. In this paper, the trust level is used as knowledge for routing. The security rather than shortest path is the primary concern of the method. The performance evaluation via simulations shows that the method is a promising trust routing algorithm for MANETs. The effects of this trust model on DSR route discovery mechanism are analyzed. Results show that our model can improve the performance of DSR route discovery.

1 Introduction

In an ad hoc network nodes cooperate in dynamically establishing wireless networks and maintaining routes through the network, forwarding packets for each other to facilitate multi-hop communication between nodes not in direct transmission range. On-demand routing protocols for mobile ad hoc networks, such as Dynamic Source Routing (DSR), generate routes for unknown destination paths on an as needs be basis. The protocols mostly employ flooding approaches to discovery routes. The flooding approach forwards a node's queries to all its neighbors, which results in traffic problems. To be effective, a query-routing strategy should forward queries only to nodes who propose certain related knowledge.

The proposed routing solutions deal only with number of hops. Connections with trust requirements are not supported. In this paper, we propose a trust-based routing algorithm for ad hoc network. Security rather than optimality is the primary concern of the algorithm. In the case of general routing algorithms, it is better to find a route very fast in order to have a good response time to the speed of topology change, than to search for the optimal route but without meaning, because the network condition is changed and this route does not exist anymore. In this paper, trust parameters of nodes are used for routing decision. To evaluate the performance of the protocol(tr-DSR), we carried out the simulations for different network conditions.

The paper is organized as follows. In Section 2, we introduce the related work. The proposed routing algorithm tr-DSR is described in Section 3. The performance evaluation and analysis of the tr-DSR are discussed in Section 4. Finally, conclusions are given in Section 5.

2 Related Work

2.1 DSR and Secure Routing Protocol

The Dynamic Source Routing protocol[1] is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. Using DSR, the network is completely self-organizing and self-configuring, requiring no existing network infrastructure or administration. In DSR, although it is possible to end up with route discovery failures to some extent, re-broadcasting route request packets with certain trust probability can be considered as a performance improvement technique[2].

In response to a single Route Discovery, a node may learn and cache multiple routes to any destination. This support for multiple routes allows the reaction to routing changes to be much more rapid, since a node with multiple routes to a destination can try another cached route if the one it has been using should fail. This caching of multiple routes also avoids the overhead of needing to perform a new Route Discovery each time a route in use breaks.

The trust of node is a very important constrain in wireless network. If a node or a route has very low trust value, this route will be dangerous. Moreover, this can have also a bad effect on the network data packets: there are some nodes that will be dropped. To this end, we propose a trust routing establishment mechanism and we apply it to the DSR routing protocol. The main feature of our work compared to the related works in this area is that it is simple and efficient according to the obtained performance enhancement comparing to the results obtained with the basic DSR protocol.

2.2 Trust Quantization

An ad-hoc network of wireless nodes is a temporarily formed created, operated and managed network by the nodes themselves. Nodes assist each other by passing data and control packets from one node to another. The execution and survival of an ad-hoc network is solely dependent upon the trusting nature of its nodes.

A number of protocols have been developed to secure ad-hoc networks using cryptographic schemes, but all rely on the presence of an omnipresent, and often omniscient, trust authority. The dependence on a central trust authority is an impractical requirement for ad-hoc networks. We present a model for trust-based communication in ad-hoc networks. In the model, a central trust authority is a superfluous requirement. The routes discovered using our model is not cryptographically secure but each one of them carries a confidence measure regarding

its suitability in the current. According to Josang[3], trust and security represent two sides of the same thing. Both these terms are so highly interconnected that they cannot be evaluated independently.

The principle drawback to find route based trust is the route discovery efficiency. So, in the simulation, we predigested the computing of trust. Each node in the network stores other node's trust value. The trust value of a node is computed and updated by trust agents that reside on network nodes[8]. In our simulation, the trust values of all nodes are stored in each node in advance. We signify trust -1 to +1, representing an unremitting range from complete distrust to absolute trust. The trust value in route R by source node S is represented as $T_S(R)$ and given by the following equation.

$T_S(R) = W_S(N_i) * T_S(N_i)$, $W_S(N_i) = 1$, $0 < W_S(N_i) < 1$ where $W_S(N_i)$ represents the weight assigned to node N_i by source node S and $T_S(N_i)$ represents the trust value in node N_i by source node S. $T_S(R)$ is a probabilistic value. To simply, in our simulation, let $T_S(R) = \min(T_S(N_i))$, i.e., $W_S(N_i) = 0$, $\forall i \neq j$, $W_S(N_j) = 1$, $T_S(N_j) = \min(T_S(N_i))$.

3 Routing Algorithm Based on Trust

In this paper, we extended DSR to trust-based tr-DSR. Each node maintains two routes to a destination[9]. This increases the number of different routes returned, giving the source a better choice from which to select two maximal trust probability routes from these replies. Although tr-DSR is capable of maintaining more than two routes, we only experimented with the two-path version, since the results in previous indicate that the largest improvement is achieved by going from one to two or three paths[2,4,5].

The routing protocol uses the path with the larger trust value of route and less delay of packet among multiple route options as two metrics unlike standard DSR protocol that only uses minimum hop count. The idea behind this is to maximize preemptive route creation by choosing the route that is expected to security. How well the trust of a route can be estimated plays a key role in the performance of this protocol. Routing data packets algorithm is as Fig.1.

4 Analysis of Simulation Results

To analyze the effects of the trust value of a node and a route computing on route discovery mechanism, we give the parameters used in our model as following.

N Average number of nodes per route;

R Average number of paths returned for the same route request and for the source-destination pair;

T Average trust probability.

A node re-broadcasts or returns a route reply with probability T. Thus, the probability that all of the nodes on a path with average length N will re-broadcast the route request or return the route reply from their cache is P^N .

```

Step 1 if (routing cache is empty) then routing discovery algorithm is run;
    { Source node S Broadcast RREQ message:
      Intermediate node x received the RREQ message re-broadcasts the RREQ or
      return a route reply with trust probability  $T_S(x)$ ;
      If source received RREP message
        { Then if number of route <2 then
          { if RREP timeout
            Then discard the RREP message
            else compute trust value of the route contained the RREP message;
              if the trust value of the route >threshold then cache the source routes
              else discard the RREP message }
          else discard RREP message } }
Step 2 if routing cache is not empty
    then search the routing cache for to the desired destination;
    routing original data packet through the route with the less number of hops;
Step 3 if (no route is found) then (discard the packet) end if.
    
```

Fig. 1. Routing data packets algorithm

The probability of at least one of the nodes on a path with average length N will not re-broadcast the route request packet is denoted by T_0 and given as follows.

$$T_0 = 1 - P^N.$$

T_0 is also the probability of this path to be broken.

Since there are different R paths to the destination and the trustless nodes behave independently on deciding to re-broadcast or not, we may assume that each of the paths has a probability of T_0 of being broken. Thus, the overall probability of all of the paths being broken, route discovery failure probability P_R , is given as follows.

$$T_R = (1 - T)^R.$$

The tr-DSR protocol algorithm is simulated in OpNet Modeler 10.0 environment. The example network consists of 50 static nodes. The routing protocol used is DSR.

Fig.2 shows that number of route replies is, on the average, four times more than the number of route requests in the standard DSR protocol.

The change of T_R with respect to T for the simulated networks described above is depicted in Fig. 3.

In our simulation, senders are randomly selected among the nodes in the system. We gradually increased the average trust probability and observed the number of route requests and route replies. Below are the simulation results of the trust-based scenarios

Trust based route reply reduced the ratio of route reply message over the number of route requests. Thus, we analyzed this ratio in our simulation.

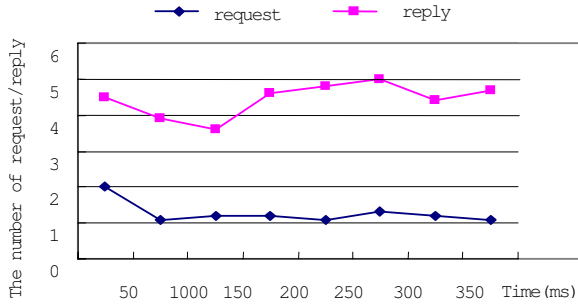


Fig. 2. The number of Request/reply ratio vs. simulation time

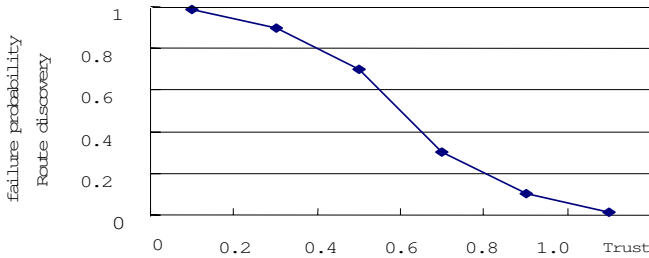


Fig. 3. Route discovery failure probability vs. trust

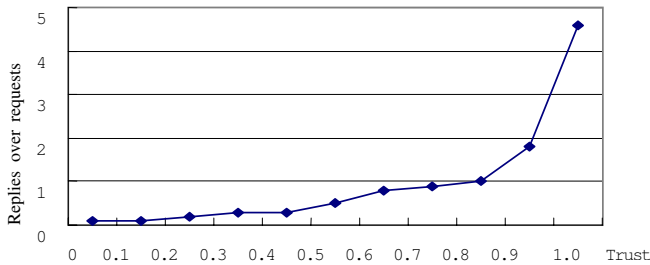


Fig. 4. Simulation results of request/reply ratio vs. trust

Fig.4 shows that even if all of the nodes are trustless, the number of route replies over number of route requests is still above the threshold value of 1 up to $p=0.2$. For this case, the route failure probability T_R can be calculated as 0.04.

The above analysis shows that some of route replies are redundant and an optimization may be possible on the number of route request re-broadcasts. If DSR is modified in such a way that the legitimate nodes rebroadcast the route requests with a probability of T , which should be engineered carefully, route discovery success ratio will still be acceptable and there will be a decrease in number of routing packets that are flooded to the network.

5 Conclusions

Ad hoc network is a nature and extensible underlying layer for Knowledge Grid because of its autonomy, self-organization, and scalability[7]. As a solution to routing reply at the semantic of the scalable Knowledge Grid, this paper proposes a trust model on DSR protocol and analyzed the effects of this trust model on route discovery success. The results for the example networks show that such a trust probabilistic route model decreasing route reply packets. When all the nodes are trustless in the network, route discovery is not so disrupted up to a certain trustless probability $1-T$ value. This is due to redundant route replies for a route request. The tr-DSR protocol performance be improved. Such a change of re-broadcast mechanism in DSR route discovery and route select phase come with some advantages. The most important advantage is the increase in network utilization by decreasing the overhead of redundant broadcasts. The tr-DSR protocol based on trust may not be cryptographically secure but they do establish relative levels of trustworthiness with them. We believe that our tr-DSR will be suited to ad hoc networks.

References

1. David, B., Johnson, D.A., Maltz, J. B.: The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks. Ad Hoc Networking, Addison-Wesley, 2001
2. Ozleyis, O., Burak B., Albert, I.: A Probabilistic Routing Disruption Attack on DSR and Its Analysis. Third Annual Mediterranean Ad Hoc Networking Workshop,2004,Jun:300-306
3. Josang,A.:The right type of trust for distributed systems. Proceeding of the ACM New Security paradigms workshop,1996,sep:119-131
4. Camp,T., Williams,B.:Comparison of broadcasting techniques for mobile ad hoc networks. Proceeding of the Third ACM International Symposium on Mobile Ad Hoc Networking and Computing(MOBIHOC 2002), Lausanne, Switzerland, 2002,Jun:194-205
5. Sasson,Y., Cavin,D., Schiper,A.:Probabilistic Broadcast for Flooding in Wireless Mobile ad hoc networks. In proceedings of IEEE Wireless Communications and Networking Conference(WCNC 2003),New Orleans, LA, 2003,Mar:1-14
6. Wu,K.,Harms,J.:QoS Support in Mobile Ad Hoc Networks. Crossing Boundaries-an interdisciplinary journal, 2001,1(1):92-106
7. Hai Zhuge: Query routing in a peer-to-peer semantic link network. Computation Intelligence, 2005,21(2):198-216
8. Pirzada, A.A., McDonald,C.:Establishing Trust in Pure Ad-Hoc Networks. Proceeding of 27th Australasian Computer Science Conference(ACSC'04),2004,26(1):47-54
9. Jie W.:An Extended Dynamic Source Routing Scheme in Ad Hoc Wireless Networks. Telecommunication System, a special issue on Wireless Networks and Mobile Computing,2003,22(1-4):61-75