A Trusted Routing Based Service Discovery Protocol with Backup Nodes in MANETs

Min-Hua Shao, Yi-Ping Lee, Yen-Fen Hou and Cheng-Yi Ho

Department of Management Information Systems, National Pingtung University of Science & Technology, 1 Hseuh Fu Road, Nei Pu, Pingtung 912, Taiwan, China

Abstract. The wireless MANET is particularly vulnerable on account of its intrinsic characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation and constrained capability. These vulnerabilities create significant challenges for routing protocols operating in the entire network. They have inspired lot of research interests regarding node connectivity in MANETs, but very few measures exist to trust-integrated cooperation for service discovery. In this paper, we employ cross-layer approaches to propose a new trusted routing based service discovery protocol called TRSDP. The TRSDP is a kind of a reactive routing protocol, improved on the Dynamic Source Routing. Moreover, a backup node mechanism for quick reconnection during link failures is provided in TRSDP in order to cope with the dynamism of such networks. Case studies involving security and service discovery scenarios were presented to demonstrate how the proposed protocol works. As a result, this paper gives a solution for the trusted and efficient cooperation of routing and service discovery in MANETs.

1 Introduction

A mobile ad hoc network (MANET) [5] is considered a collection of wireless mobile nodes that are capable of communicating with each other without relying on any infrastructure or any centralized administration. In such a network, each mobile node operates not only as a host but also a router, forwarding packets for other mobile nodes in the network that may be outside wireless transmission range. Therefore, wireless MANET is particularly vulnerable due to its intrinsic characteristics, including of open medium, dynamic topology, absence of central authorities, distributed cooperation and constrained capability [4]. Routing plays an important role in the security of the entire network [1]. Most of the research on MANETs has focused on issues dealing with the connectivity between mobile nodes mainly through routing protocols to cope with the dynamism of such networks and the arising problems thereof. However, solving the problem of connectivity alone is not sufficient for the adoption of MANETs. Because their basic role is to allow mobile users to exchange data and user other's services, there also is a need for service discovery [2].

In academic literature, service discovery mainly was addressed in the context of wired networks and most of their solutions are centralized, where services are stored

Shao M., Lee Y., Hou Y. and Ho C..
A Trusted Routing Based Service Discovery Protocol with Backup Nodes in MANETs.
DOI: 10.5220/0003559901150122
In *Proceedings of the 8th International Workshop on Security in Information Systems* (WOSIS-2011), pages 115-122
ISBN: 978-989-8425-61-4

in a central server directory, and relied on powerful infrastructure nodes and reliable links. By contrast, design of mechanisms proposed for service discovery in MANETs that must cope with node mobility, unstable channel conditions and nodes with limited energy and availability significantly differs from traditional wired solutions. There exist three basic architectures that a service discovery approach can adopt, that is, directory-based、directory-less and hybrid architectures. In order to benefit from information available at the routing protocol, we couple cross-layer techniques with directory-less architectures to propose a new trusted routing based service discovery protocol called TRSDP. The proposed scheme is based on integrating the routing process with the service discovery process and further, redundant transmissions of service discovery packets at the application layer are avoided, and energy is saved. Considering efficiency and quality of route service against the dynamic nature of MANETs, we introduce reputation-based trust model and backup routes mechanism into the popular and widely used Dynamic Source Routing (DSR) [8]. In which, the communicating parties can select the most reliable route based on trust relationship among nodes and then feedback the connection experience to maintain the relationship. Therefore, TRSDP is a solution which looks after both sides of secure and efficient.

The rest of this paper is structured as follows: In section 2, we present the proposed scheme in detail. In section 3, evaluating the proposed scheme through experiment and analyze the result. The conclusion is in section 4.

2 TRSDP Routing Protocol

In this section, we propose an efficient trust-based service discovery routing protocol called as TRSDP routing protocol for MANETs. TRSDP is based on DBR^{2}P [7] routing protocol, we divided it into three phase: 1.Route discovery phase 2.Backup node setup phase 3.Route maintenance phase.

2.1 Route Discovery Phase

At first, source node will set trust threshold (TT) and service of destination node (DS). Source node will search node which can provide service and correspond to trust threshold from route cache and trust cache, if intermediate nodes can match trust value between source and destination node, then connect it; otherwise, source node can’t search destination node cause by it cannot provide service and correspond to trust threshold from route cache and trust cache, it will send RREQ packet. Algorithm 1 deals with the source node of enable route discovery, and algorithm 2 deals with the examining of route cache.

Algorithm 1:

```
//DS: Service of destination node
//TT: Trust threshold

For each node in cache
  If the route cache exist DS Then
    Check timestamp of route cache;
  Else
    If the trust cache is expire Then
      Update the trust cache;
    End If
    If the node is match TT in trust cache Then
       Insert the node address in Target address field of
         RREQ;
       Forwarding the RREQ packet by unicast send to neighbor
         nodes which must meet TT;
    Else
       The must meet TT of node cannot be found, failed to
         connect;
    End If
  End If
End For
```

Algorithm 2:

```
//TT: Trust threshold

If the timestamp of route cache is expire Then
  Delete the record;
Else
  If the destination node has match TT Then
    If trust value of all intermediate nodes in the main path
      >= TT Then
      Connect it;
    Else
      If trust value of all intermediate nodes in the backup
        path >= TT Then
        Connect it;
      Else
        Insert the destination node address in target address
          field of RREQ;
        Search neighbor nodes from trust cache are matching
          TT;
      End If
    End If
  Else
    Search neighbor nodes from trust cache are matching TT;
  End If
End If
```


To avoid trust value deviation from record change of trust cache, we will the check the record data. If record data expires, it will update data by searching trust value to assure accuracy of trust value.

After intermediate node receives RREQ packet, the node checks itself if it is the destination node at first. If not, next it checks it has received the same RREQ packet by examining #Rid (Route request ID) in RREQ packet. Suppose the node receives the packet at the first time; the node will record <#Rid,1> corresponded with time-stamp of #Rid in RREQ sequence and number of receive both locating in route dis-cover cache. It will search destination node which can provide service and correspond

to trust threshold from route cache and trust cache, if intermediate node can match trust value between source and destination node, then it replies RREP packet to source node. If it cannot search destination node which can provide service and correspond to trust threshold from route cache and trust cache, then it chooses node which can match trust threshold from trust cache, and forwards RREQ packet, detailed procedure shown in algorithm 3.

```
Algorithm 3:
//RD: Route discovery cache
//DS: Service of destination node
//<#Rid,C>: C is a counter
//TT: Trust threshold
//index: The intermediate node's IP

 While the intermediate node doesn't meet the conditions for
   DS
   If the <#Rid,1> existing in RD Then
     If the Address[i] of RREQ == index Then
       If n>=3 || expire in RD Then
         Drop packet;
       Else
         C=C+1; //<#Rid,C+1>
       End If
     Else
       Drop packet;
     End If
   Else
     Newly added <#Rid,1> into RD;
     Update the timestamp of RD;
   End If
   For each node in route cache
     If the route cache exist DS Then
       Check timestamp of route cache;
     Else
       If the trust cache is expire Then
         Update the trust cache;
       Else
         If node is match TT in trust cache Then
           Insert the node address in Target address field of
             RREQ;
           Forwarding the RREQ packet by unicast send to neigh-
             bor nodes which must meet TT;
         End if
       End if
     End if
   End For
 End While
Reply RREP
```

If the timestamp does not expire or the total receive times of same RREQ packet are less than two, intermediate node receives the same #Rid in RREQ packet again; then the node will add one to the receive times as <#Rid,n+1>. If the timestamp expire or receive times of same RREQ packet are more than two, intermediate node will drop the packet. If destination node receives RREQ packet, it will reply RREP packet to source node, detailed procedure shown in algorithm 4.

```
Algorithm 4:
//RD: Route discovery cache
//<#Rid,C>: C is a counter

Set D = 0;              // Initialization
 If C!=0 Then
   If the timer is expire in RD Then
     Select backup nodes;
   Else
     C=C+1;
     Save <#Rid,C> into Address[i];
   End if
 Else
   <#Rid,1> into Address[i];
   Start timer of RD;
   Do
     If D==1 Then
       Forward the RREP packet according to RREQ Address[i];
     End If
     Insert trust value in RREP packet;
     Reply RREP packet by Address[i] of RREQ;
     The intermediate node according to RREP updates route
       cache and trust cache;
     Update timestamp of trust cache;
     D=1;
   While(not source node)
   Connect it;
 End If
```


In order to avoid the course of RREQ delivery being a loop, the node will check if its own IP address exists in address[i] in RREQ packet when intermediate node receives RREQ packet. If not, it will drop the RREQ packet.

2.2 Backup Node Setup Phase

When destination node receives RREQ packet at the first time, it will reply RREP packet. Forward through intermediate nodes, along the reverse paths back to the source node, this can create a two-way link. In our scheme, when destination node receives RREQ packet, it will record information in the route table and start a timer, then keep receiving all RREQ packets in certain time until the time finishes then reply RREP packet. The amount of time can allow user to adjust follow according to network environment. After timer expires, the destination node goes to build backup path phase.

The destination node will pick out some backup nodes from address[i] which was recorded at route discovery cache, and meanwhile sent backup set message to notify each backup node. At the same time, the backup path will be saved in backup route cache.

2.3 Route Maintenance Phase

When the information is transmitting, the node cannot receive the reply from downstream node which means the path is invalid, and then enter route maintenance

phase. First of all, detecting invalid path node will check itself is a backup node or not. If it is, it will directly replace the main route with a backup route from its own backup route cache. If it is not, the node will send a route break packet to the upstream node. Then similarly, the receive route break packet node checks if it is destination node. If not, the route break packet be forward to upstream node continually, until backup node receives. When the source node receives the packet, finding out there is no substitutive path to destination node. The source node will restart route discovery phase.

3 Analysis

We have implemented TRSDP routing protocol in Java environment. The essence of a perfect information security can be classified into three parts: 1.Confidentiality 2.Integrity 3.Availability. In the paper, we focus on the data integrity and the path availability.

1) Data integrity: Each node only recognizes part of the network topology in MANET, it has to cooperate with other trusty nodes to gain correct route information and deliver information completely. Based on many secure route protocol references, link meeting the requirement of trust is connected through a relationship like interpersonal trust, excluding malicious nodes from the linking path to ensure data integrality.

2) Path availability: Because of each node has high mobility in MANET; network topology will change quickly and be easy to disconnect. As soon as the link disconnects, original DSR route protocol will restart route discovery. However, it wastes much time and influences the real-time of data transfer. The important issue in MANET is how to build backup path and improve the path availability.

3.1 Security Scenario

In [6], scholars defined trust rate into three security levels. We refer to their research, setting the trust threshold (TT) previously to divide the trust in three levels which are ranges from zero to one. If the value approaches one is on behalf of the node has higher reliability. On the other hand, low reliability signifies that the node does not accumulate enough of trust value. To make trust degree clearer in representation, we separate the range into three parts. We simulate the scenario by 23 nodes; an example of the randomly generated topology is given in Fig. 1.

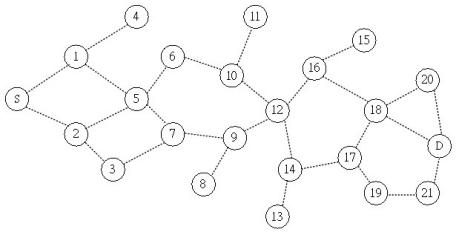

Fig. 1. The randomly generated topology.

3.1.1 Case 1: Low Security Level

Using TRSDP routing protocol at low security level, nodes can send RREQ packet to establish paths when trust values are more than zero. Consequently, they build up 25 paths. Node S、2、5、12、17 and 18 are backup nodes.

3.1.2 Case 2: High Security Level

Using TRSDP routing protocol at high level, nodes can send RREQ packet to establish paths if the trust values are more than 0.66. There are two paths connected. Node S is a backup node.

3.1.3 Discussion

In the preceding sections, number of paths at high security level is less than that at low security level under the same network topology. The reason is that users require higher security, so the node will not send RREQ packet to neighbor nodes whose thresholds are lower than the trust. Therefore, it will minimize the risk of that malicious nodes exist in paths.

A low security level has 25 paths that include malicious node induced by low security threshold. Suppose trust value of malicious node is less than 0.5 [3]. In case 1, trust value of node 14 to node 17 is 0.28, which is lower than 0.5. So node 17 is recognized as a malicious node in routes even though its trust threshold is qualified. The useful paths passing through node 17 will break in all probability. Therefore, in our scheme we combined backup path to avoid time waste because of new route discovery. Suppose that node 14 does not receive ACK packet from node 17. It will go to build backup path phase. Node 14 sends route break packet to the upstream node, as shown in fig. 2.

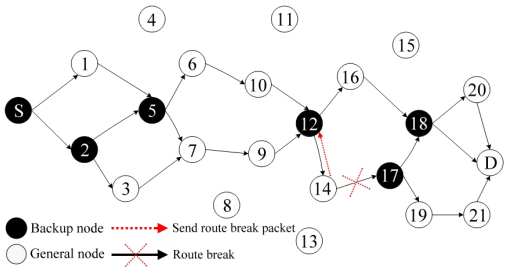

Fig. 2. Route breaks and repair.

Node 12's Backup Routing Table	
Destinaton	Backup Route
D	12→16→18→20→D
	12→16→18→D

Fig. 3. Backup routing table.

When node 12 receives the route break packet, if it is the backup node, it will search backup path from backup path table. There are two substitutive paths be found, node 12 will choose one of them as main path to deliver data (As the show in fig. 3.). Thus, it avoids data transfer delay induced by restarting route discovery in original DSR.

4 Conclusions

Wireless market today is overcrowded with large number of different devices and mobile devices are inherently scarce in resources, necessitating the need to cooperate among them for performing tasks that cannot be done alone. This cooperation is in the form of services that are offered by other device in MANETs. In this paper, we use the idea of providing routing-layer support for service discovery to propose a trusted routing based service discovery protocol with backup nodes. The integrated protocol, TRSDP, can take advantage of the ability of obtaining service information along with routing information from the same message by piggybacking service information onto routing messages. This way, redundant transmissions of two message-producing processes are lightened, and energy is saved. Specifically, the establishment trust-aware routes with backup nodes can be conducted at the same time, that is, only trustworthy intermediate nodes can participate in activities of data forwarding and backup restoration. Therefore, the proposed scheme can provide a better tradeoff between reliability and efficiency.

Acknowledgements

The author would like to thank the anonymous reviewers for their valuable comments and suggestions. This paper was supported in part by the National Science Council, Taiwan, under contract NSC 98-2410-H-020-007-MY2.

References

1. Ververidis, C. N., Polyzos, G. C.:Service Discovery for Mobile Ad Hoc Networks: A Survey of Issues and Techniques. IEEE Communications Surveys & Tutorials, 3rd Quqrter (2008) 30-45
2. Deng, H., Li, W., Agrawal, D. P.:Routing security in wireless ad hoc networks. IEEE Communications Magazine, Vol.40(10). (2003) 70-75
3. Poonam, K. G., Misra, M.:Trust Enhanced Secure Multi-Path DSR Routing. International Journal of Computer Applications, Vol.2(2). (2010) 63-69
4. Shao, M. H., Huang, S. J.:Lightweight Anonymous Routing for reliability in Mobile Ad-Hoc Networks. Journal of Research and Practice in Information Technology, Vol.41(2). (2009) 171-180
5. Corson, S., Macker, J.:Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration. IETF WG Charter
6. Wang, B., Wei, R.:Zero-knowledge trust negotiation. In Proceedings of CSCWD 2009. (2009) 390-395
7. Wang, Y. H., Chao, C. F.:Dynamic backup routes routing protocol for mobile ad hoc networks. Information Sciences, Vol.176 (2). (2006) 61-185
8. Johnson, D. B., Maltz, D. A.: Dynamic source routing in ad hoc wireless networks. Mobile Computing. (1996)