Location-Aided Secure Routing Scheme in Mobile Ad Hoc Networks*

Do-hyeon Lee, Sun Choi, Ji-hyeon Choi, and Jae-il Jung

Department of Electronics and Computer Engineering, Hanyang University
17 Haengdang-dong, Sungdong-gu, Seoul, 133-791, Korea
{dohyeon,sun0467,whizkid}@mnlab.hanyang.ac.kr,
jijung@hanyang.ac.kr

Abstract. This paper proposes a new routing scheme that uses geographical position information to minimize the number of intermediate nodes that make a routing path, and to guarantee reliability and security in route establishment process. To achieve this purpose, we first describes the *projection-line*, the *shadow-line*, and three types of route request (RREQ) packet to select the closest node to the destination. The *safety table* is then newly defined by adding a specific subfield to a routing cache to identify the misbehaving nodes. The suggested scheme decreases the number of hops to make up routing path in comparison with the existing one, and exclude malicious nodes from route establishment process.

Keywords: location-aided routing, trust-based routing, security, MANET.

1 Introduction

In MANET, the route from source to destination may consist of a number of intermediate nodes [1]. Minimizing these intermediate route nodes is an important issue in MANET. To achieve this purpose, many routing protocol using the geographical position information have been suggested [2]-[4]. Geographic routing algorithms are intended to reduce unnecessary routing messages by using the location information from a GPS, and to restrict the number of the neighbors forwarding a route request message.

However, most of the existing geographic routing algorithms do not consider that they are exposed to security threats. Any malicious node (internal attacker) can send a false route message including the modified location information to be in the route [5]. Although the shortest route is established between source and destination, the route may be not secure because the malicious node can belong to the route. An attacker in the route can inject packets into the network to consume valuable network resources. Consequently, it is very important to realize reliable and secure routing protocols [6]-[8].

* This research was supported by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment). (IITA-2006-(C1090-0603-0016)).

O. Gervasi and M. Gavrilova (Eds.): ICCSA 2007, LNCS 4706, Part II, pp. 131–139, 2007.

In this paper, we propose the routing scheme that can solve this problem. Our routing scheme finds the shortest route with a novel location-aided routing algorithm and by isolating a malicious node the most secure path with a route cache called a safety table.

This paper is organized as follows. Section 2 presents three components to support a secure routing solution for the proposed scheme. In Section 3, we describe the routing scheme to provide reliability and security in detail. Section 4 compares the effect of the proposed scheme with the effect of the existing one in terms of packet delivery success rate, routing protocol overhead, and path length. We present our conclusion in Section 5.

2 Components for Secure Route Establishment

In this section, we propose a routing scheme to reduce intermediate nodes of routing path and to guarantee route establishment with security. We first assume that each node knows the current positional information of every node existing in a routing domain [2, 3]. We also assume that each node periodically confirms the location of neighbors with mobility, analyzes a message sent by its neighbors and stores such information in the safety table. The reason that the proposed scheme uses positional information and Safety Table are as follows:

- to establish a routing path that always aims for the destination node
- to minimize the number of intermediate nodes that make a routing path
- to guarantee reliability and security in route establishment process

2.1 Projection-Line and Shadow-Line

To achieve the purpose we have mentioned earlier, we suggest two lines as shown in Fig. 1, namely *projection-line* and *shadow-line*. The projection-line is guideline from the sending node to the destination, and its direction always aims for the destination. The shadow-line indicates the distance from the sending node to its neighbor represented on the projection-line. It is used to select the nearest node to the destination among neighbors.

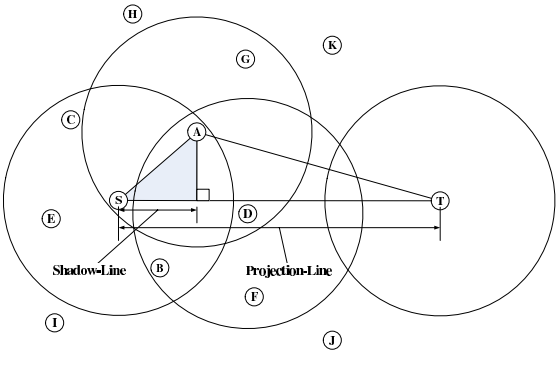
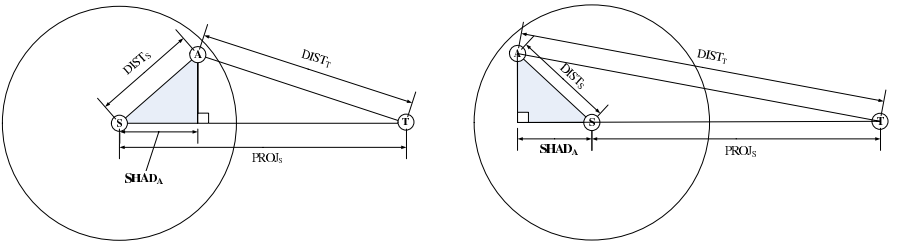


Fig. 1. The projection-line and shadow-line

When any node S (x_S, y_S) wants to transmit data to the destination node T (x_t, y_t), the node S first generates a projection-line to establish a routing path to node T, denoted as $PROJ_S$. The value of $PROJ_S$ can be calculated by using the following equation:

$$PROJ_S = \sqrt{(x_t - x_s)^2 + (y_t - y_s)^2} \tag{1}$$

And then, if node S (the first sending node) chooses node A for the next hop comparing SHAD of its neighbors, node A (the second sending node) also generates a projection-line to node T, denoted as $PROJ_A$. By this process, we can continuously get the projection-line with direction to the destination.



(a) Node A's the positive shadow-line (b) Node A's the negative shadow-line

Fig. 2. Example of the shadow-line

To acquire a shadow-line, we need three elements as shown in Fig. 2(a), that is, $PROJ_S$, $DISTS_A$ and $PROJ_A$. The $PROJ_S$ is calculated by the node S and transmitted in the RREQ packet to node A. When node A receives the RREQ from node S (first sending node), it can get the location information of node S and calculate the distance between the node S and itself, denotes as $DIST_{SA}$. The $PROJ_A$ means the distance between the node A and node T, and it can be calculated like $PROJ_S$. Then, the node A can calculate its shadow-line $SHAD_A$ by using the following equation:

$$SHAD_A = \frac{DIST_S^2 - DIST_T^2 + PROJ_S^2}{2 \times PROJ_S} \tag{2}$$

In the case of that the node A has a negative value of $SHAD_A$ as shown in Fig. 2(b), it means that the position of node A is further than node S from the destination. According to the previous states, the next hop having a negative value of SHAD is not added to the routing path.

2.2 Safety Table

In the case of using GPS information, the position of each node becomes known to every node. So if any node is intending malicious behavior, such as modification, impersonation or fabrication, participates in the route establishment process, this route cannot provide reliability and security at all. To solve these problems, each node additionally maintains a route cache called a safety table. It can be used to detect the malicious node by comparing information in the safety table with message received from its neighbors.

Table 1 describes Safety Table managed by each node. It is composed of four fields such as Node_ID, Node_MA, Node_RC, SHAD_N. First, Node_ID represents neighbor node's identifier (e.g. IP address). In the second place, Node_MA indicates normal or malicious attributes of adjacent node. And then, Node_RC records the number of malicious behaviors that a node tried to before. Lastly, SHAD_N records the value obtained from the formula (1).

Table 1. Structure of the safety table

Node_ID	Node_MA	Node_RC	SHAD_N
A	TRUE	0	$SHAD_A$
B	TRUE	0	$SHAD_B$
C	TRUE	1	$SHAD_C$
…	…	…	…
N	TRUE	0	$SHAD_N$

Initialization of Safety Table: Let Node_MA be set to *TRUE* (boolean logic) that means normal node. As shown above, Node_RC is set to "0". If Node_RC is larger than "3", we will judge this Node_ID as an obviously malicious node. SHAD_N records neighbor node's SHAD value calculated by itself. Since we assume that every node knows the position of the other node in a routing domain, a node can calculate SHAD value of its neighbors.

Detection of Malicious Node: When any node receives RREQ packet from its neighboring node, it will compare SHAD value calculated by itself with SHAD value received from neighbor. In the case of that two values are identical, we will examine whether Node_RC is less than the maximum permissible value, namely "3". If it is true, Node_MA is set to *TRUE* or RREQ packet received from its neighbor is immediately discarded. In the case of that two values is not identical, Node_MA is set to *FALSE* and Node_RC will be increased by one. Then, it broadcasts RERR packet including information of malicious Node_ID to its neighbor node and discards RREQ packet.

3 Location-Aided Secure Routing scheme

To establish a reliable and secure routing path, we define three types of route request (RREQ) packet, that is, route request inquiry; I-type RREQ: {*PROJs*, *Location_send*, *Location_dest*}, route request candidate; C-type RREQ: {$SHAD_N$}, and route request decision; D-type RREQ: {IP_S, IP_D, *Seq_num*, *Securable_NodeID*}.

3.1 Route Discovery

The sending node calculates the shadow-line of neighbors and records it in the SHAD_N field of the Safety Table. Because we assume that the sending node knows the positional information of neighbor and destination node, it can calculate the

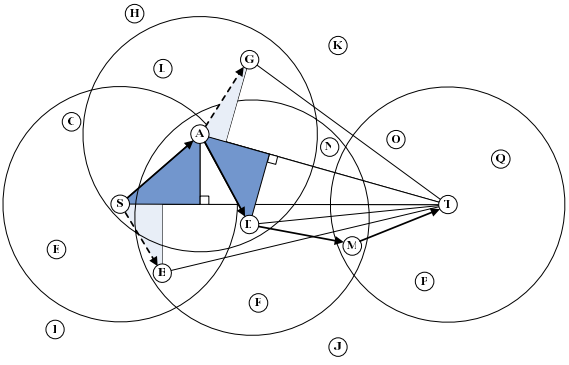


Fig. 3. Example of route discovery

shadow-line to utilize $PROJ_S$, $PROJ_A$ and $DIST_{SA}$. After that, the sending node manages the shadow-line in the safety table to detect malicious behavior of any node.

The following describes the process to select a next hop node for guaranteeing reliability and security using the concepts of safety table, shadow-line, and RREQ we have shown above.

Step 1. The sending node requests the shadow-line of neighbors by broadcasting I-type RREQ packet including $PROJ_S$ and positional information of the sending, destination node. The neighbors which received I-type RREQ packet recognize the position of the sending, destination node. And then, the neighbor can calculate $DIST_{SA}$, $PROJ_A$ using the positional information of the sending, destination node in I-type RREQ packet and it can finally obtain shadow-line of itself.

Step 2. The neighbors respond to the sending node by sending C-type RREQ packet including shadow-line of themselves. Then, the sending node which received C-type RREQ packets temporarily selects a node with the largest shadow-line as a next intermediate node for making up a routing path and examines whether this shadow-line is identical to that of the sending node. If identical, the sending node additionally examines whether Node_RC recording the number of malicious behavior of the selected node is less than the maximum permissible level. Finally, if the two conditions are satisfied, the selected node is determined as the next hop node. Otherwise, this node is excluded from the object of the intermediate node and one other node with the second-largest shadow-line selected as the next intermediate node. Through the repetition of this process, we can determinate the next hop node with considered reliability and security.

Step 3. The sending node makes D-type RREQ packet by inserting the selected node's ID in Securable Node ID field and broadcasts this D-type RREQ packet to neighbors. Neighbors that receive D-type RREQ packet compares the Node ID in Securable Node ID field with that of itself, and the neighbor with the same Node ID will eventually perceive itself as the next hop node. After this, according to Step 2, 3, this next hop node also looks for a next intermediate node which is the nearest to the destination and can guarantee safety, as shown in Fig. 3.

3.2 Route Maintenance

In mobile ad-hoc network environment (MANET), each node usually investigates a link status (either stable or unstable) among neighbors by periodically exchanging a Hello message [1]. When any intermediate node on the routing path detects the unstable status of the link due to limitation of transmission power, the intermediate node sends route error message (RERR) to the source, and the source will initiate a route re-establish to destination. In our case, this approach enabled us to increase control overhead in the routing domain because we use three types of route request packet for finding the path from the source to the destination.

To solve this problem, we consider that the intermediate node detecting the link error will carry out a route re-establishment to destination (as shown in Fig. 3). This can be done because the intermediate node still maintains a path from source to itself and knows the positional information of neighbors, the destination node. In this approach, we can reduce control overhead and latency to find another path from source to destination which is additionally generated due to three types of route request packet.

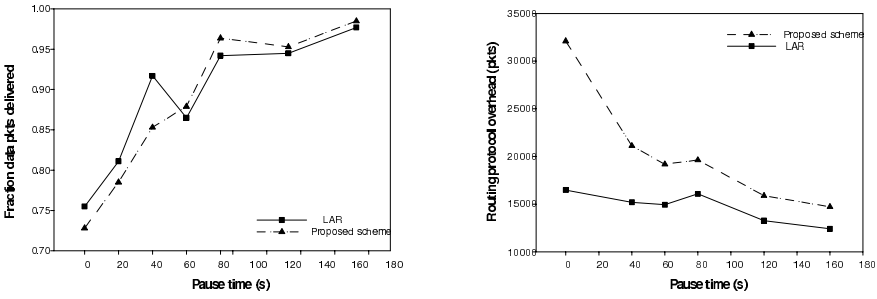
In cases where any intermediate node lost the link to the next hop, the node re-broadcasts route request packet (RREQ) to neighbors for finding another next hop with satisfaction of two conditions: closer to the destination than any others, providing safety (reliability and security) without generating a route error message (RERR). When the next hop does not have the route information from itself to the destination, we need to re-establish the route from itself to the destination by an additional RREQ packet. But when the next hop has the information, it generates RREP packet including the route information from itself to the destination and sends it to the intermediate node selecting itself as the next hop. Then, the intermediate node which received this packet updates the route cache of itself, and forwards the result to the source so that the entire route information is updated.

4 Simulations Results and Analysis

We compare the effect of the proposed scheme with the effect of the LAR in terms of packet delivery success rate, routing protocol overhead and the number of hops. We assume that the average number of mobile nodes is 50 including 10 malicious nodes in a 1500 meter x 300 meter square region, and each node moves with an average speed of 20 m/s. To compare the efficiency of the proposed scheme, we evaluate the effect of varying the pause times of 0, 40, 60, 80, and 160 seconds in the highest mobility cases. We simulate CBR traffic flows originated by the six sending nodes. Each CBR flow sends at 2Kbps, and uses 64-byte packets. Each simulation lasts for 600 seconds of simulated time.

5 Packet Delivery Success Rate and Routing Protocol Overhead

Figure 4(a) illustrates the effect of the average packet delivery rate with different pause times. We assume that the number of mobile nodes is 50 in simulated region. The packet delivery success ratio of the proposed scheme decreased by 2-5% in high



(a) Packet Delivery Success ratio (b) Routing Protocol Overhead

Fig. 4. Effect of Packet Delivery Success ratio and Routing Protocol Overhead with different pause time

mobility (at pause time 0-60 sec), and increased for a small amount in low mobility (at pause time 60-180 sec). The reason of that we have the relatively lower performance in the highest mobility is the disconnection due to selecting a nearest next hop to the destination as we have described in Section 3. In the case of that simulated nodes have low mobility, run with pause time > 180, we can see that this problem decreases dramatically from Fig. 4(a). As the result of this, we can predict that it represents generally similar performance between LAR and the proposed scheme.

Figure 4(b) illustrates the effect of the average routing protocol overhead with different pause times. As the mobile nodes is moving rapidly, the control packet overhead of the proposed scheme increased by 10-35% in high mobility (pause time 0-60 sec), and increased by 5-10% in low mobility (pause time 60-180 sec). This is the result we expected. We have suggested three types of route request packets (I-type, C-type, and D-type RREQ) for excluding malicious nodes from route establishment process, which might find the nearest node to the destination. Consequently, it could have higher control message than LAR. However, this is the trade off which we have considered especially for network security and reliability.

4.3 Path Length

Figure 5 illustrates the effect of the average number of hops with different pause times. In the proposed scheme, the number of hops for delivering all packets to the destination decreased by 10-40% in high mobility (pause time 0-60 sec), and decreased by 40~50% in low mobility (pause time 60-180 sec). In general, the previous location-aided routing algorithm chooses the routing path with the first arrived route request packet to the destination. However, we suggest that the sending node chooses the relay node which has the largest shadow-line value, and located at the nearest to the destination. It could be possible since we assume that each node knows the current position of neighbors by analyzing location information sent by them as we have described in Section 2.

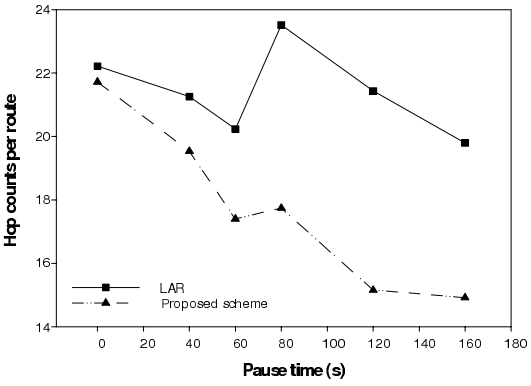


Fig. 5. Effect of Path length with different pause times

5 Conclusions

This paper has proposed a routing scheme to improve routing efficiency and to guarantee a reliable and secure route establishment by using positional information of each node in mobile ad hoc networks. To achieve this purpose, we have first introduced the shadow-line, which select the closer next hop to the destination, and the safety table, which detects malicious node among neighbors. And then, we described the process to select a intermediate node with the concepts of the shadow-line, safety table, and three types of route request (RREQ) packet.

We have compared the effect of the proposed scheme with the effect of LAR in terms of packet delivery success rate, routing protocol overhead, and path length in highest mobility cases. In high mobility, the proposed scheme makes path length more efficient, but we have relatively lower performance in the other cases. We consider that this is the tradeoff especially for network security and reliability. In cases where simulated nodes have low mobility, however, we have verified that this problem is decreased dramatically. As the result of this, we note that it represents similar or better performance in comparison with the conventional technique even if the process of excluding malicious nodes is included in the route establishment process.

References

1. Macker, J.P., Corson, M.S.: Mobile Ad Hoc Networking and the IETF. ACM SIGMOBILE Mobile Computing and Communications Reviews 2(2), 9–14 (1998)
2. Ko, Y.B., Vaidya, N.H.: Location-Aided Routing in Mobile Ad Hoc Networks. ACM Wireless Networks 6(4), 307–321 (2000)
3. Wang, N.-C., Wang, S.-M.: An efficient location-aided routing protocol for mobile ad hoc networks. In: Proceeding of the 11th International Conference on Parallel and Distributed System (ICPADS 2005), vol. 1, pp. 335–341 (2005)

4. Karp, B., Kung, H.T.: GPSR: Greedy Perimeter Stateless Routing for Wireless Networks. In: Proceedings of the 6th annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 2000) (August 2000)
5. Hubaux, J.-P., Buttyan, L., Capkun, S.: The Quest for Security in Mobile Ad hoc Networks. In: Proceedings of the ACM Symposium on Mobile Ad hoc Networking and Computing (MobiHOC 2001), pp. 146–155 (October 4, 2001)
6. Li, H., Singhal, M.: A Secure Routing Protocol for Wireless Ad Hoc Networks. In: Proceedings of the 39th Hawaii International Conference on System Sciences, vol. 9, p. 225a (January 2006)
7. Chuanhe, H., Jiangwei, L., Xiaohua, J.: A Secure Routing Protocol SDSR for Mobile Ad Hoc Networks. In: Jia, X., Wu, J., He, Y. (eds.) MSN 2005. LNCS, vol. 3794, pp. 269–277. Springer, Heidelberg (2005)
8. Nekkanti, R.K., Lee, C.-w.: Trust based adaptive on demand ad hoc routing protocol. In: ACM Southeast Regional Conference, Proceedings of the 42nd annual Southeast regional conference, pp. 88–93 (April 2004)