The Security Improvement of MSR Protocol over MANET

XU Jian-zhen[1], LIANG Ke-hui[1], ZHANG Wen-wen[2]

1. College of Computer, Nanjing Univ. of Posts & Telecommunications, Nanjing, China

2. College of Communication & Art , Nanjing Univ. of Posts & Telecommunications, Nanjing, China

Abstract: In this paper, we introduce the reputation mechanism into MSR(Multipath Source Routing) in Mobile Ad Hoc Network(MANET). This mechanism maintains a reputation table in each node. Before routing setup, the source node will verify the reputation degree of each node. If a node's reputation degree is lower than the limited value, it will be isolated. As a result, several safe routing paths are established between source node and destination node. Then the routing security in MANET is improved. The simulation results show that the improved routing protocol has a better packet delivery fraction and lower End-to-end delay in MANET which includes malicious nodes.

Keywords: Ad Hoc Network; MSR; Routing Security; Reputation Mechanism

1. Introduction

Recently, there has been significant research interest in the area of Mobile Ad Hoc Network[1][2]. Most researches in MANET routing protocols concern more about their performance rather than their security. In MANET, one malicious node can mislead routing by attacking routing protocols, resulting in the collapse of the network. Thus, with the widespread application of MANET, the research in MANET routing protocols safety has become increasingly important.

There are single-path routing and multi-path routing protocols[3][4][5][6] in MANET. The later is classified backup multi-path routing and parallel multi-path routing. Parallel multi-path routing which has great research value uses two or more paths for data transmission at the same time, it provides higher bandwidth and reliability.

The typical multi-path routing protocols in MANET are based on single path routing protocols AODV[7](Ad Hoc On Demand Distance Vector Routing) and DSR[8] (Dynamic Source Routing). As a parallel multi-path routing protocol, MSR[9][10] is an expansion of DSR. To improve the security of MSR, this article addresses the reputation mechanism in this routing protocol and proposes a new routing protocol called MSRRM (Multipath Source routing Based on Reputation Mechanism). In this new protocol, the source node and destination node can establish several higher creditability paths through maintaining reputation table in each node. Thus, the routing security in MANET is enhanced.

2. Msr Introduced and Security Analysis

MSR protocol is an extension of DSR. It inherits all the advantages of DSR in addition to the capability of multi-path routing. Furthermore, it employs a probing mechanism to fetch on-demand the dynamic path states. This mechanism can be used to refresh the information in cache, to delete stale path and find new one in time. MSR can improve performance by giving application the freedom to use multiple paths within the same path service. However, this routing protocol is totally based on the cooperation and reliance among all the nodes in MANET. This is not realistic in applications. Lacking of reputation mechanisms, MSR protocol will involve the malicious nodes in the routing setup process. Those malicious nodes will disrupt the network by inserting wrong routing update information, replaying or modifying the routing information.

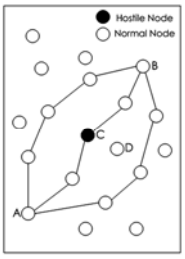

Figure 1.

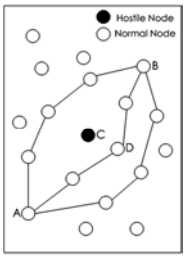

Figure 2

As is shown in Figure 1, in a MANET, there are three paths between node A and B. The middle path has a malicious node C. Node C will broadcast a large number of malicious routing packets and those packets will occupy most of the network bandwidth. As a result, the data transmission is out of success. The malicious node can not be isolated due to the lack of appropriate mechanism in MSR, consequently the insecurity problem of routing in MANET is increasingly acute.

3. Msrrm Protocol

To solve routing protocol insecurity problems in MSR, this paper proposes an improved protocol called MSRRM, which is based on node reputation mechanism. Through the reputation mechanism, all the malicious nodes will be isolated and several safe routing paths will be established between the source and destination node. In this way, the

routing security in MANET is enhanced. As is shown in Figure 2, through the validation of the reputation value, MSRRM protocol will isolate the malicious node C and choose node D in the routing path then a safety path is established. MSRRM protocol mainly includes two parts: the part of reputation management, as well as the part of routing discovery and maintenance.

3.1 Reputation Management

Reputation is a stimulating tool for cooperation among nodes. It is used to disting-uish between trustworthy and untrustworthy nodes and prevent the misbehaviors. If a node pays no attention to its own reputation and goes on misbehaviors continually, it will be isolated and discarded.

Reputation mechanism[11][12] is mainly used for resisting the internal attack. This mechanism includes two modules: the reputation information-gathering module and the reputation value-evaluation module. The information-gathering module pays an important role in the collection of the information from other nodes, then the reputation value-evaluation is responsible for the analysis to quantify. So that each node can get a reputation table which contains the identities of other nodes and the relative reputation values. This reputation table is used to guide the behaviour of the node during the routing establishment. A node's reputation information will be sent to its adjacent nodes by means of HELLO message periodically.

In this mechanism, a node's reputation includes two parts: subjective reputation value and indirect reputation value. There are five constants in the mechanism: T_{max}, T_{min}, T_{lim}, T_0, $\triangle T$, which means maximum level, minimum level, threshold, initial value and change in threshold respectively. We define $T_{i,j}$ as the reputation value of node j to i. While $T_{i,j} \geq T_{lim}$ (i≠j), node i regardes node j credible. Otherwise, node j cann't be trusted. T_{max} in this mechanism is used to prevent the malicious node from being isolated because of high reputation value. T_{min} is used to prevent the node from being isolated forever. When a node's reputation is lower than T_{lim}, it will be isolated. T_0 is the initial value, generally it is large or equal to T_{lim}. $\triangle T$ is change in threshold, when a node's reputation value change is large than $\triangle T$, the node will broadcasting the event.

There is a four-tuple array <ID, T^d, T^c, T> in reputation table. ID is the number of node. T^d is direct reputation value. T^c is indirect reputation.T is the reputation value of the node. $T_{i,j}$ is the reputation evaluation of node j to i, then we have

$$T_{i,j} = \delta T_{i,j}^{d} + (1-\delta) T_{i,j}^{c} \quad (1)$$

$T_{i,j}^{d}$ is direct reputation of node j to i; $T_{i,j}^{c}$ is indirect reputation of node j to i. $\delta \in [0, 1]$, it's the degree of trust between direct and indirect reputation value. After a node receives some data from another node, it will update its T^d ,and this called one update cycle. If there are f_m errors and s_m rights during the mth update cycle of a node, we have the initial values of s and f in $m+1$ update cycle.

$$s_{m+1}^{0} = \left(\frac{\lambda_1 s_m + \lambda_2 s_{m-1} + \lambda_3 s_{m-2}}{3} \right) \left(\frac{s_m}{s_m + f_m} \right) \quad (2)$$

$$f_{m+1}^{0} = \left(\frac{\lambda_1 f_m + \lambda_2 f_{m-1} + \lambda_3 f_{m-2}}{3} \right) \left(\frac{f_m}{s_m + f_m} \right) \quad (3)$$

λ_1、λ_2、λ_3 are the weight of s and f in the first three update cycles. generally, $\lambda_1 > \lambda_2 > \lambda_3$ and $\lambda_1 + \lambda_2 + \lambda_3 = 3$. Define the mth T^d as T^{d_m}, then

$$T^{d_m} = \frac{s_m + 1}{s_m + f_m + 2} \quad (4)$$

We have the increment of direct reputation value is $\Delta T^d = T^{d_m} - T^{d_{m-1}}$, then we can update T^d by $T^d = T^d + \Delta T^d$.

When node i receives the reputation information from another node, node i will view the node's reputation value first. If this node is not a malicious node, then node i updates its T^c. Otherwise, no deal. If node i receives reputation about node j to k, then we update T^c of node k.

$$T_{i,k}^{c} = T_{i,k}^{c} + (T_{j,k} - T_{i,k}^{c}) T_{i,j} \quad (5)$$

3.2 Route Discovery and Maintenance

a) Path finding

MSRRM retains the routing discovery mechanism of MSR whereby multiple paths can be returned. To initiate the routing discovery, the source node will check its reputation table first, then send RREQ messages to the nodes whose reputation value is larger than T_{lim}. Each RREQ identifies the source and destination of the routing discovery, which contains unique request identification(ID). When another node receives this RREQ and is the destination of the routing discovery, it returns an RREP to the source of the routing discovery. Otherwise, it will check if this RREQ is duplicated or not by the ID. If it is not the duplicate, it appends the ID and rebroadcasts the packet. Otherwise, it will discard this duplicate RREQ.

Each routing discovered is stored in the routing cache with a unique routing index. So it is easy for us to pick multiple paths from the cache. To achieve high path independence, the disjoint paths are preferred in MSRRM. There is no looping problem in MSRRM, as the routing information is contained inside the packet itself; routing loops, either short-or long-lived, cannot be formed as they can be immediately detected and eliminated.

b) Route Maintenance

A link of a routing can be disconnected because of mobility, congestion and packet collisions. In MSRRM, routing maintenance works through RERR(Route Error) and probing. It works as follows:

(1)When a node discovers the active routing is broken, the node will send RERR to source node which will remove the routing from the routing table as soon as it receives the RERR.

(2) The source node detects the routing state by sending probing packets periodically to each path. If a routing

978-1-935068-01-3 © 2009 SciRes.

path interrupted, the source node will get RERR from intermediate node and delete the routing path from routing table.

(3) If there is only one routing left, the source node will check its RTT. When the RTT is lower than a limit value, it means the routing path is in a good condition, and the source node will continue use the routing path. Otherwise, the source node begins a new routing discovery process as mentioned above.

4. Performance Evaluation

We use NS2.33 to conduct the simulation. NS2 is a free and open source application where its code can be modified and extended as desired the range of features it provides.

4.1 Simulation Environment

To get the performance of MSRRM under different number of malicious nodes, we set the malicious nodes range from 0 to 100, step 10. Our simulation model a network of 300 mobile hosts placed randomly with a 1200*1200 sq. meter area. Each node had a radio propagation range of 300 meters and channel capacity is 2Mb/s. The speed of the hosts moving was 5m/s. 40 nodes are randomly chosen to be CBR(constant bit rate) sources. Each source was characterized by a rate of 1 packet/sec and the packet size was 512 bytes. Each run executed for 300 seconds of simulation time. We used free space propagation model as the radio propagation model, and IEEE802.11 Distributed Coordination Function (DCF) as the medium access control protocol.

4.2 Simulation Results and Analysis

In the simulations, we use the "Packet Delivery Fraction" "End-to-end delay" and "routing overhead" to evaluate the performance of MSRRM. Packet Delivery Fraction: It is the ratio between the number of packets received by the destination nodes to the number of packets sent by the source nodes.

Figure 3 shows the Packet Delivery Fraction comparison between two protocols in MANET. When there was no malicious node, both of these two protocols got good Packet Delivery Fraction at about 0.95. But with the increase of the malicious node, the Packet Delivery Fraction of the MSR declined rapidly. When the number of malicious node was up to 100, the Packet Delivery Fraction was 0.2. While the Packet Delivery Fraction of MSRRM was about 0.88. By using of reputation mechanism, MSRRM can reduce the impact of the malicious nodes and increase the Packet Delivery Fraction.

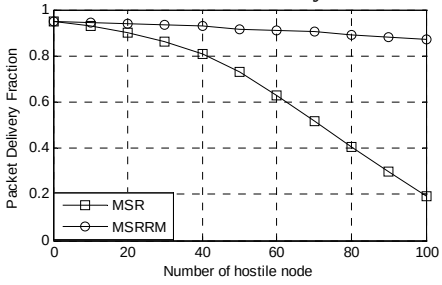

Figure 3. The comparison in Packet Delivery Fraction

Figure 4 plots the End-to-end delay against the number of malicious node in MANET. Both of MSR and MSRRM had low End-to-end delay if no malicious node in MANET. However, with the increase of malicious node, both of their End-to-end delay were increased. When there were 100 malicious nodes, the End-to-end delay of MSRRM was about 30ms half of MSR. Therefore, MSRRM has a better End-to-end delay than MSR in MANET which includes malicious node.

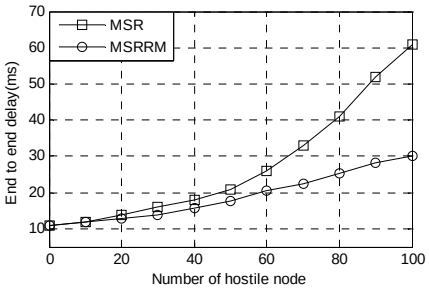

Figure 4. The comparison in End-to-end delay

Figure 5 shows the routing overhead against number of malicious node. Because of the periodically and triggered updating of the reputation information, MSRRM had more control overhead than that of MSR. And with increase of malicious node, the control overhead of MSRRM increased faster than MSR.

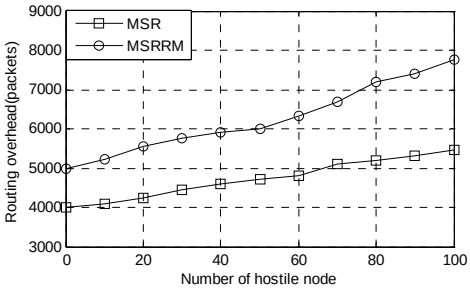

Figure 5. The comparison in routing overhead

5 Conclusions

In this paper, based on the study of MSR, we introduce the node reputation mechanism to enhance the routing security in MANET and propose a new routing protocol called MSRRM. In MSRRM, all the node's reputation degree will be validated between source and destination node before the routing established. If a node's reputation degree is lower than the limited value, the node will be isolated. In this way, we can improve the route security in MANET. Simulation results show that MSRRM has a better packet delivery fraction and lower End-to-end delay than MSR in MANET with malicious nodes. The drawback of MSRRM may be the larger processing overhead of originating the packets. Fortunately the computer is becoming more and more powerful , so it may not be the obstacle to the deployment of MSRRM. Further work might focus us on limiting the number of path in MSRRM to reduce the routing overhead, so that

we can achieve higher security and performance.

REFERENCES

[1] Su. Xu, Boppana. Rajendra V, "Crosscheck mechanism to identify malicious nodes in ad hoc networks," Security and Communication Network, 2009, 2(1), p45-54.

[2] Izhak. Rubin, Runhe Zhang, "Robust throughtput and Routing for mobile ad hoc wireless networks," Ad Hoc Network, 2009, 7(2), p265-280.

[3] Panayiotis Kotzanikolaou, Rosa Mavropodi, Christos Douligeris. "Secure Multi-path Routing for Mobile Ad hoc Networks,Ad hoc networks, " 2007, Vol 5(1): 87-99

[4] Peng Yang, Biao Huang, "Multi-path Routing Protocol for Mobile Ad Hoc Network," 2008 International Conference on Computer Science and Software Engineering, pp 1024-1027.

[5] S. Mueller, D. Ghosal, "Multipath Routing in Mobile Ad Hoc Networks:Issues and Challenges," Lecture Notes in Computer Science, Springer, Berlin, 2004, pp. 209-234

[6] X. P. ping , Y. Caiyu, "Novel multi-path routing scheme for UWB Ad hoc network," Journal on Communications, 2005, pp. 89-96.

[7] C. E. Perkins, E. M. Royer, and S. Das, "Ad hoc On-demand Distance Vector (AODV)," RFC 3561, July 2003.

[8] D. Johnson, D. Maltz, and J. Broch, "DSR The Dynamic SourceRouting Protocol for Multihop Wireless Ad Hoc Networks,"chapter 5, pages 139–172. Addison-Wesley, 2001.

[9] L. Wang, Y. Shu, M. Dong, et al, "Adaptive Multipath Source Routing in Ad Hoc Networks", in ICC 2001, pp 866-871.

[10] Linifang Zhang, Zenghua Zhao, Yantai Shu, et al, "Load balancing of multipath source routing in ad hoc networks," International Conference on Communications ICC 2002

[11] L. Buttyan and J. P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks", In ACM Journal For Mobile Networks (MONET), Special Issue On Mobile Ad Hoc Networks, 2003.

[12] P. Michiardi and R. Molva, "Core: a Collabo- rative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," in IFIP-Communications and Multimedia Security Conference, Portoroz, Slovenia 2002.

978-1-935068-01-3 © 2009 SciRes.