EPAMP: An Anonymous Multicast Protocol in Mobile Ad Hoc Networks

Hongling Xiao[1], Hong Song[2(✉)], and Weiping Wang[2]

[1] Information Network Center, The Second Xiangya Hospital,
Central South University, Changsha 410083, China
15957231@qq.com
[2] School of Information Science and Engineering,
Central South University, Changsha 410083, China
{songhong,wpwang}@csu.edu.cn

Abstract. We propose a new anonymous multicast protocol named Encryption and Pseudo-based Anonymous Multicast Protocol (EPAMP). EPAMP is an anonymous routing protocol based on MAODV in mobile ad hoc networks. It adopts the pseudonym mechanism to hide the senders identity, and uses encryption/decryption mechanism to thwart eavesdropping and intrusion attacks. It can ensure the anonymity of senders, receivers and the communication of neighboring nodes. Performance analysis and simulation results indicate that EPAMP can ensure anonymity performance, and effectively resist collusion attacks and predecessor attacks. It brings only slight transmission delay and decrease in packet transmission rate.

Keywords: Anonymous communication · EPAMP · Multicast · Pseudonym mechanism

1 Introduction

Secure communication and users privacy attract a lot of research attention in recent years. Forwarding mechanism is one of the key components to realize communication among nodes in mobile ad hoc networks (MANTEs) How to hide the communication location and communication relationship becomes one important issue in military and confidential communications. Due to the lack of predefined and opened system structure, the attackers are more likely to intercept the information and discover the real IP address, reveal the actual position and the communication relationship among communicating nodes in the network. Therefore, it is very important to study the anonymous communication mechanism in MANETs.

The demand of anonymity in mobile network includes [1,2] sender-receiver unlinkability, mutual authentication identity anonymity, location anonymity, and network topology and motion pattern anonymity. In the past several years, there are already many works on anonymous communication mechanisms in ad hoc

G. Wang et al. (Eds.): ICA3PP 2015 Workshops, LNCS 9532, pp. 276–289, 2015.
DOI: 10.1007/978-3-319-27161-3_24

network [3–13]. ANODR [3] uses the trap door and pseudonym strategy to hide the IP addresses of the source and the destination. ASR [1] encrypts the destination address by shared key between the destination and source node. In the data transmission stage, a node uses a shared confidential TAG authentication to determine whether the received packet is transmitted to it. If it is not for its own, a replacement strategy and XOR mechanism of random number would be used to fix the packet length in order to avoid the path tracking. The Mask protocol [4] assigns a series of conflict-free pseudonyms and corresponding key values for participating nodes through the trust authority server, and uses pairwise-anonymous authentication and confusion mechanism to achieve sender anonymity, receiver anonymity and position anonymity. The broadcast mechanism and onion communication has been used in SDAR protocol [5] to communicate between the sender and the receiver. All these anonymous mechanisms can solve the problem of anonymous communication to some extend in mobile ad hoc networks.

As multicast in ad hoc networks is used widely, more and more applications can be done better to complete the tasks by using multicast, such as disaster rescue and war in the communication command. Although there are some anonymous communication mechanisms using the feature of multicast in cable network, such as SAM [8] (Secure and Anonymous Multicast), Mapper [9], they are not suitable for large-scale dynamic networks for the sake of the low efficiency and scalability. Recent researches applied multicast anonymity technology to P2P networks. The M2 protocol [11] proposes a method that combines the forwarding paths of receivers in the same group. The MAM protocol [12] constructs an efficient multicast tree with bandwidth and/or delay. The BAM protocol [13] proposes a ring structure based on Bus. All these protocols use multicast mechanism to get mutual anonymity while decreasing the cost. However, because multicast in ad hoc networks have different features, these anonymous communication strategies proposed for cable networks are not suitable for ad hoc networks. There are some problems:

(1) The attacker can obtain the information of the multicast group and the sender by eavesdropping on the plaintext packets and tracking the transmission route of the packet.
(2) Some special tags of the same packet in the multicast protocol provide the clue for the attacker to find out the important member of the multicast system through reverse tracking.
(3) The global listeners can obtain multicast topology.
(4) The agent error will affect the entire network performance. In this paper, we propose a new pro anonymous multicast protocol based on MAODV, which is Encryption and Pseudo-based Anonymous Multicast Protocol (EPAMP). EPAMP adopts the pseudonym mechanism to hide the senders identity and uses encryption/decryption mechanism to thwart eavesdropping and intrusion attack. It can ensure the anonymity of senders, receivers and the communication of neighbor nodes.

The remainder of this paper is organized as follows. Section 2 presents the design of EPAMP. Section 3 analyzes the anonymity of EPAMP. Performance analysis and evaluation are presented in Sect. 4. We conclude the paper in Sect. 5.

2 Encryption and Pseudo-Based Anonymous Multicast Protocol (EPAMP)

The main idea of EPAMP is to use pseudonyms rather than real IP address to represent the nodes in the multicast tree for multicast communication process, and to use symmetric encryption method to communicate between the initiator and receiver for data communication process, with which sender anonymity and connection anonymity can be achieved. The whole process is divided into multicast data transmission and multicast tree maintenance. Every node saves the information of its own neighbor nodes in the same multicast tree. In order to finish the work of path establishment and data transmission, every node also creates a new routing table for saving the request information and a new multicast routing table for saving the related information of data forwarding.

2.1 Multicast Data Transmission

This process is mainly to build the path of the multicast group members and to transfer data along the path.

Step 1: The source node requests constructing path (Fig. 1).

The source node S, which wants to join the multicast group or which wants to send the data to the multicast group, will send routing request packet. The format of the RREQ packet is described as followed,

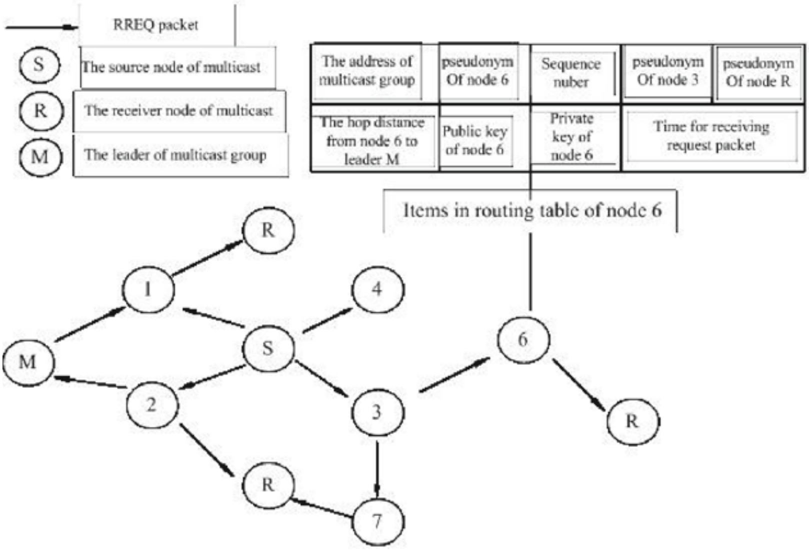
$$\{RREQ, rreqID, McastAddr, destSeq, srcpseudo, srcSeq, Hop\}$$

where rreqID in the packet is the sequence number, McastAddr represents the address of the terminal multicast group, destSeq is the latest sequence number received by the node, Srcpseudo is the nodes pseudonym generated by the hash function and its own IP address, and srcSeq is sequence number of the node and Hop is a random number. After sending out an RREQ request, the source node waits for the reply packet. If the source cannot receive the reply after several tries, it will announce itself as the leader of a new multicast group.

After receiving a RREQ request, intermediate node will judge out whether the multicast sequence number is greater than or equal to the multicast sequence number. If not, it generates its own pseudonyms and public-private key pair (PK, SK) and adds them into the routing table as following format.

(McastAddr, Mcastseq, LHCount, LcPseudo, PK, SK, NHPseudo, LPPseudo, lifetime)

The over record is used to save the information about multicast group, the intermediate node, the upstream node, the downstream node and their pseudonyms and etc. if (Hop-1)>0, then the node uses its own LcPseudo and


RREQ packet
S The source node of multicast
R The receiver node of multicast
M The leader of multicast group
Items in routing table of node 6
R
1
4
M
S
6
2
3
R
R
7

The address of multicast group	pseudonym Of node 6	Sequence nuber	pseudonym Of node 3	pseudonym Of node R
The hop distance from node 6 to leader M	Public key of node 6	Private key of node 6	Time for receiving request packet	

Fig. 1. Route request stage diagram

PK to replace srcPseudo and srcSeq of this packet and broadcast the modified packet.

Step 2: The destination replies the RREQ request. This process is shown in Fig. 2.

When the multicast member receives the request packet, it will reply the RREP packet to the source node by the original path if its multicast group sequence number is greater than or equal to the current serial number. The RREP packet is described as $\{RREP, Hop, McastAddr, destSeq, srcPseudo, PK, McastHop, leaderPseudo\}$.

The values of Hop and McastAddr come from the RREQ packet. destSeq is the current multicast group sequence number. srcPseudo is the node pseudonyms. PK is the public key in (PK, SK). McastHop is the number of hops from current node to the leader of multicast group and leaderPseudo is the leaders pseudonym.

After the intermediate node receives the RREP packet, it will check the routing table whether there is the same McastAddr and the same srcPseudo with which is in the RREP packet. If not, then the RREP packet is discarded. Otherwise, the intermediate node will record the information in RREP packet and generate a pair of public key and private key. Then After increase the value of hop and McastHop, the node modifies the value of PK and srcPseudo and forwards the RREP packert to next node in the reverse path. If the node receives several RREP packets, it will keep the information of the RREP packet with maximum sequence number or minimum Hop value.

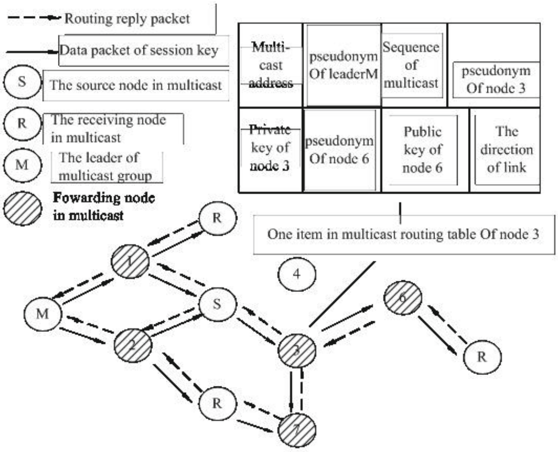

Routing reply packet
Data packet of session key
S The source node in multicast
R The receiving node in multicast
M The leader of multicast group
Fowarding node in multicast
~~Multi-cast address~~
pseudonym Of leaderM
Sequence of multicast
pseudonym Of node 3
~~Private~~ key of node 3
pseudonym Of node 6
Public key of node 6
The direction of link
One item in multicast routing table Of node 3
4
R
1
M
S
2
3
6
R
R
7

Fig. 2. The information which the node saves in the route response stage

Step 3: Path Activating. After waiting for a certain time, the source node chooses the path with the largest sequence number or the route with the minimum hops, and sends the MACT packet to activate the path. As shown in Fig. 3, the nodes m-1, m, and m+1 are three contiguous neighbor nodes in the path. When the source node S sends an MACT packet to the tree member node R it must finish the next five operations in turn.

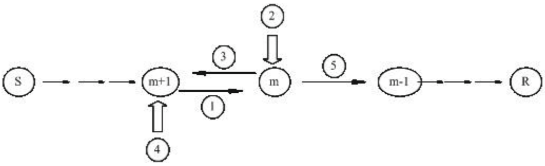


Fig. 3. The process of activating the route

Node m+1 sends a MACT message to node m. The message includes the pseudonym of node m+1 and node m, multicast group address, the pseudonym of the source node S, the session key of node m+1 and so on. All these information encrypts with the public key of node m.

After node m receives the MACT message, it lookups the item with the same pseudonym and decrypts the MACT package. Then it gets the session key of node m+1 and activates the path from node m+1 to node m.

After the path is activated, the node m sends to the node m+1 a data packet in which there are the session key of node m+1, node m-1 and node m.

After receiving the data packet, node m+1 records the session key and activates it.

Node m lookups the routing table and uses the pseudonym and public key of node m-1 to modify the MACT message. Then, MACT message is forwarded downward to the next node.

Step 4: Data transmission. After activating the transmission path, the source node can transmit data to the members of the group. The node who received data packets firstly checks whether there is an item with pseudonym srcPseudo in multicast routing table and whether the direction is in accordance with the tag. If its true, then the node can decrypt by the session key and replace srcPseudo with the pseudonym of the node, and encrypt McastAddr and load. At last, the node continually forwards the packet and repeats the process until the receiver gets the packet.

2.2 Multicast Tree Maintenance

The multicast tree maintenance process of EPAMP protocol is similar to that of MAODV. It uses encryption operation to enhance anonymity, and it includes four parts, which are pruning, splitting, merging, and repairing the link.

(1) Pruning Multicast Tree. The pruning process is taken place when a member node wants to leave the multicast group. The leaving node sends a MACT message with P tag and its own IP address. The upstream node that receiving this MACT message will decrypt it by corresponding session key and delete the information related to the leaving node. If the upstream node becomes a leaf node and it is not the member of the group, the process will be continued.

(2) Repairing the Link. When two nodes in the multicast tree are disconnected, the downstream node of the link will sends RREQ packet to repair the link. The destination IP address is set into multicast group address and the multicast group sequence number is the destination sequence number. The hops number of multicast group is set to the distance from the downstream node to the leader node. Only the member nodes of the multicast tree may be able to reply the RREQ packets. After repairing the multicast tree, the initiator node sends MACT message to update the downstream multicast tree.

If the upstream node of disconnected link is not the member node of multicast tree and it becomes a leaf node, then it sets the waiting time for pruning and does pruning operation after the time is past.

(3) Splitting Multicast Tree. If the disconnect network leads to failed repairing link, the initiator node will broadcast GRPH packet or MACT packet to split the original multicast tree into two sub-multicast tree? GRPH packet is sent out by the old multicast member, it contains the flag, update information of the leader, the hops number that GRPH packet has past, pseudonym of the leader, IP address of multicast group and the sequence number. All nodes who receive this GRPH message packet update their routing tables and multicast routing tables. MACT message with a G tag is sent out by the node who is not the member of multicast group. MACT message is used to inform the members updating. And the MACT message is forwarded by neighbor nodes and the forwarding process will not be ended until it reaches the multicast group member nodes.

(4) Merging Multicast Tree. If two multicast trees want to reconnect into a new multicast tree, the leader GL1 who has smaller group sequence number in two multicast trees will sent out the merging request. The leader GL2 with larger group sequence number becomes the leader of the new multicast tree. All members whose leader is GL1 request to join the new multicast tree by RREQ messages. After waiting for a period of time, the multicast tree with the leader GL1 select a forwarding path which distance is shortest to activate. As a result, the two multicast tree are merged into a new tree.

3 Anonymity Analysis of EPAMP

In order to understand EPAMP protocol, we use some attack models to analyze the anonymity of EPAMP protocol.

3.1 Eavesdropping Attack

EPAMP protocol uses pseudonym mechanism to achieve sender anonymity, receiver anonymity and the link of sender-receiver anonymity. And the eavesdropper cannot directly find out the real IP address of every node from the routing packets and data packets due to pseudonyms mechanism using in routing packets and data packets.

Moreover, in the stage of path initiating, multicast sender only broadcasts request with multicast address, while the receiver determines to reply the request only by multicast address and sequence number. So the attacker cant destroy data transmission, and cant trace the packet flag to find out the node who initiates the packet and the new leader after the initiating process is completed. The sender and the receiver are anonymous.

In the stage of path activating, the attacker cant distinguish the type of packets through eavesdropping because of the same format $\{pseudonym, encryptioninformation\}$ of the MACT message and session key package. Also, the eavesdropper is unable to directly associate the path from the length or appearance of the packet because the public key and the session key are changed every time after forwarding. In data transmission stag, the eavesdropper cannot get the multicast group number and the serial number or the association path. And the session key exchange using public key encryption can prevent eavesdropper gets relevant information. Furthermore, the value of Hops in EPAMP is a random number and is changed during the transmission, which will prevent the eavesdropper inferring the possible position of the leader.

3.2 Surrounding Attack

When all neighbors of a node are compromised nodes, these compromised nodes can exchange their information to infer the common node and they can judge the type of the common node through their exchanging information because all messages must pass by these compromised nodes. If they find that the node has only output packets, they can infer that the surrounded node is source node immediately. We define this attack as Surrounding attack. Surrounding attack will destroy the source anonymity.

Assuming the area of the anonymous multicast network is l*w square meter, the range of the transmission is d meters, then the communication area occupied by each node Ai is pd2. At the same time, there are N nodes in the network, including C compromised nodes with the proportion of p. Let all nodes distribute uniformly within the anonymous multicast network, then we can calculate that the number of nodes M within the communication area of each node is

$$M = \frac{\pi d^2}{lw} N \tag{1}$$

Therefore, the number of neighbor nodes surrounded the source node in the communication range is (M-1). So the successful probability of surrounding attack is

$$P_I = \begin{cases} \binom{Np}{M-1} \Big/ \binom{N}{M-1} & p \geq \frac{M-1}{N} \\ 0 & p < \frac{M-1}{N} \end{cases} \tag{2}$$

Figure 4 shows the impact of surrounding attack with different p and M. In Fig. 4, the anonymous multicast network area is 1500 * 300 m2, there are 100 nodes and the proportion of p varies from 0.5 to 0.9. We test the variation of PI when the number of direct neighbors of each node M varies from 5 to 20.

From Fig. 4 we can conclude that the success probability PI of surrounding attack is increasing with the increasing proportion p of compromised attackers. The reason is that according to uniform distribution, the probability of attackers surrounding the node will be increased when the proportion of attackers increasing. Therefore, the possibility that all attackers are located in the communication range of the sender is also increased. But when the number of neighbors of the sender is increased, the probability of surrounding the sender will reduce as the proportion of the attacker is fixed.

In addition, Fig. 4 also shows that although the attackers increase the successful proportion of surrounding attack, the probability PI just increases a little. Even if the proportion of attackers p reaches 60 % and the number of neighbors M is 5, the successful probability PI of surrounding attack is only about 7.2 %.When the number of direct neighbors increases to 20, the successful probability PI of surrounding attack declines to 7.8208e-006. This result indicates that surrounding attack is almost impossible to succeed in the density of larger networks.

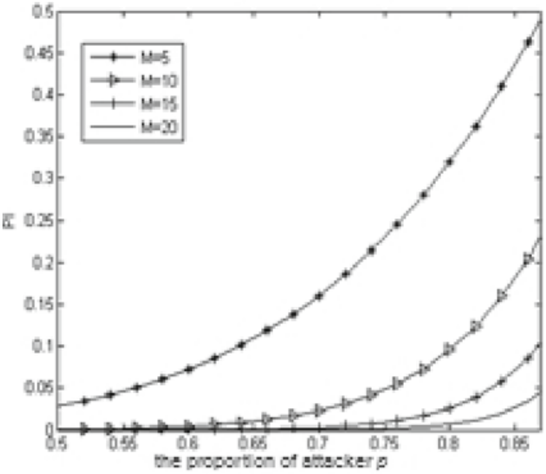


Fig. 4. PI with different p and M

3.3 Predecessor Attack

Predecessor attack is collaborated attack against anonymous protocols, in which the attacker infer the possible sender by the sending times of each node after tracking an identifiable stream of communications over a number of rounds (e.g., path reformations in Crowds) and simply logging any node which sends a message in each round.

In EPAMP protocol, every node records some information in a list, such as the multicast address, neighbor nodes and leaders pseudonym. The attacker in the forwarding path can get the content of packet according to the session keys between upstream and downstream nodes. And it also can collaborate with other attackers to determine whether they are located in the same multicast tree by the multicast address and sequence number. Thus, the compromised attacker can run a predecessor attack.

Suppose there are N nodes in the system, including C attackers, and the proportion of the attackers in the system is p. We also suppose that the probability of successful attack is Pr.

From the structure of multicast tree in EPAMP protocol, we can learn that the sender is only in the root node of the multicast tree. Therefore, any attacker can determine that its direct predecessor is the sender only when it locates the first position of the anonymous path. That is to say, when the attacker can located in the first layer of multicast tree, it has the opportunity to infer the sender. And when there is no attacker in the first layer of the tree, the predecessor attack will not succeed. So if there are k nodes in the first layer of the multicast tree, and the successful probability of predecessor attack Prl=k is:

$$\Pr\{l = k\} = 1 - \frac{\binom{N - pN - 1}{k}}{\binom{N}{k}} \tag{3}$$

Suppose there are M neighbors within the communication range of the sender, 1lM, then

$$\Pr = \sum_{m=1}^{M} \frac{1}{M} \Pr\{l = m\} = 1 - \frac{1}{M} \sum_{m=1}^{M} \frac{\binom{N - pN - 1}{m}}{\binom{N}{m}} \tag{4}$$

Suppose Ts is the number of observation rounds of the successful predecessor attack, that is to say, the predecessor attacker can infer the sender of the rerouting path with higher probability after reforming Ts rerouting paths. According to the lower bound of Chernoff in [14], the value of Ts is:

$$T_S \geq 8 \frac{M}{M - \sum\limits_{m=1}^{M} \frac{\binom{N - pN - 1}{m}}{\binom{N}{m}}} \ln N \tag{5}$$

By the Formula (5) we can conclude that, the initiator will be inferred at least $\frac{1}{2}\left[1 - \frac{1}{M} \sum\limits_{m=1}^{M} \frac{\binom{N - pN - 1}{m}}{\binom{N}{m}}\right] T$ times by the predecessor attacker with the probability $\frac{N-1}{N}$ among Ts rounds.

Figure 5 gives the relationship between Ts rounds and M direct neighbor nodes with different p in the anonymous multicast network. In Fig. 5, we suppose that there are N=100 nodes in the anonymous multicast network and the proportion p of attackers is varied from 10 % to 80 %. The situation of Ts varies with the proportion p when M is set to 5, 10, 15 and 20.

As shown in Fig. 5, with the increase of the direct neighbors number M of the sender, the rounds Ts which the successful predecessor attack requires is decreased. And Ts is also decreased with the increase of the proportion C/N. This is because the number of rerouting paths is decreased with less sender's direct neighbors and less times the attackers locating in first layer of multicast tree. When M is a certain value, the higher the proportion of the attacker, the probability of the attacker appearing in the first layer of multicast tree is higher. And the number of rounds Ts will be reduced.

Figure 5 also shows that even the proportion of attackers reaches 70 %and the number of direct neighbor nodes is 20, the rerouting rounds Ts for successful

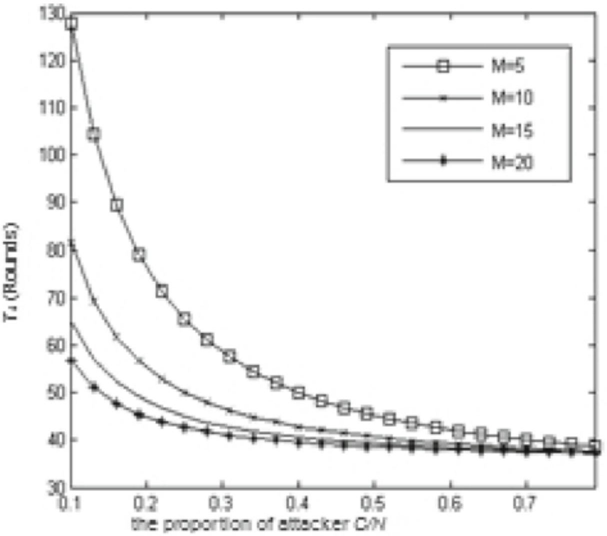


Fig. 5. Ts with different C/N and M

predecessor attack still needs about 40 rounds. That is to say, the predecessor attackers must try to compel the sender in protocol EPAMP to re-establish the forwarding path about 40 times in one data transmission process. Furthermore, the successful predecessor attacker can only get the nodes pseudonym through analyzing the content of data packet. Any captured nodes cannot give the information to determine whether its upstream node or its downstream node is leader or group member. The only thing that the predecessor attacker can do is to reduce the area of the senders location and it cant confirm the exact node, because the attacker is also surrounded by M-1 nodes.

4 Transmission Performance Analyses

We use NS2 to test the transmission costs of the EPAMP protocol. The area is set to 1500 * 300 m2 and there are 50 nodes in accordance with random distribution. The communication range of each node is 250 m and the wireless transmission rate is 2 Mbps. The movement model is random waypoint model with the maximum speed of 1 m/s, 5 m/s, 10 m/s, 25 m/s and 55 m/s, respectively. IEEE802.11 MAC protocol is used in MAC layer. The source node is randomly selected from 50 nodes. RC5 operation will need 20 ms and 930 ms is needed when the node using RSA algorithm to encryption/decryption. The cost of anonymity is measured by the data transfer rate and the transmission delay.

Figure 6 shows the effects of moving speed on transmission success rate. We can find that the transmission rate of two protocols will be declined along with the increasing node moving speed and the data successful transmission rate of EPAMP protocol is lower than that of MAODV. This is because EPAMP protocol will do encrypting and decrypting operations for each node. It requires more transmission time than that of MAODV. With the increase of the node moving speed, the number of failed links in unit time will increase, which will lead to higher probability of failure data packet transmission.

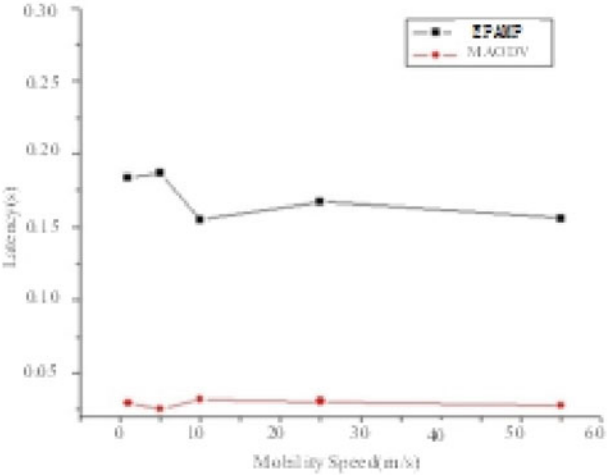


Fig. 6. Packet transmission ratio

Figure 7 shows the comparison of packet transmission delay of two protocols. The delay of the EPAMP protocol is larger than that of MAODV. Also the simulation results show that anonymous communication strategy based on encryption and decryption can receive good anonymity, but it is only applicable in wireless network of low mobility and low real-time requirements. When the node mobility rate is increased, the successful rate of data transmission is lower than that of MAODV, while the transmission delay is increased. This is because the encryption mechanism adopted in the EPAMP protocol, which will lead to decreased transmission performance. The reason for getting more anonymity with lower transmission performance mainly comes from two following parts:

First, In order to guarantee anonymity, we cancel the flags of routing request packet and reply packet in the design of data packets, so the attackers cant track the special flag. We also adopt multiple replying paths and activating process in merging multicast tree to avoid the attackers path tracing. But these measures will bring some time cost of nodes joining and multicast tree merging and path establishing.

Second, we use pseudonym mechanism instead of IP address to effectively hide the node address information. And session keys between two nodes and the public-private key pair (PK, SK) is used to encrypt/decrypt the content of transmission packet. Moreover, the relevant content in packet is modified by each

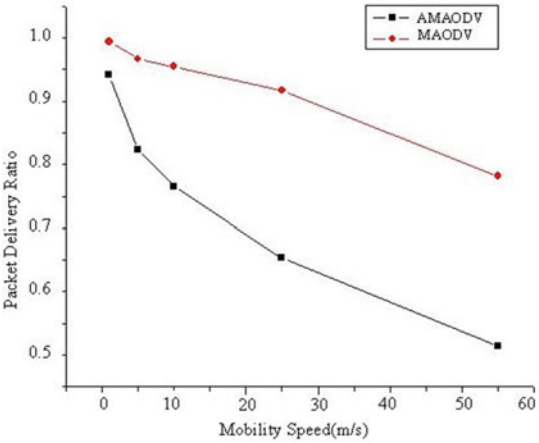


Fig. 7. The latency of packet transmission

intermediate node and is re-encrypted. At the same time, the intermediate node or receiver determines whether it is the receiver only relying on the pseudonym, which can guarantee not to disclose the relevant address information and to further enhance the anonymity.

Therefore, in order to minimize the cost of transmission and operation, (1) we just use pseudonyms to replace the IP addresses when broadcasting the request packets and reply packets because that transmitting plaintext can generate little impact on broadcasting speed; (2) When transmitting the controlling packet, we just use plaintext pseudonyms to decide whether it is the receiver, which can avoid lots of decrypting operations and can reduce the transmission time and computation cost; (3) During the data transmission process, all nodes in the path and their neighbor nodes use the same symmetry key to encrypt so that the data packet can send only once and can avoid energy wasting for many decrypting operations and repeatedly broadcasts. At the same time, the flag in data packet can also be used to avoid repeatedly broadcasting.

5 Conclusions

We have contributed a new anonymous multicast routing protocol EPAMP for providing anonymous multicast based on MAODV protocol. Anonymity analysis and transmission performance analysis results show that using pseudonym mechanism and encryption/decryption mechanism to implement anonymous multicast communication needs more transmission delay and brings lower data transmission rate, but it can effectively resist the collusion attack and the predecessor attack and it can increase the difficulty of destroying anonymous communication system and can effectively improve the anonymous performance.

Acknowledgements. This research was supported in part by the National Nature Science Foundation of China under Grant No. 61173169. The authors would like to thank the anonymous reviewers for their valuable comments.

References

1. Zhu, B., Wna, Z., Kankanhalli, M.S., Deng, R.H.: Anonymous secure routing in mobile ad-hoc networks. In: The Proceedings of 29th Annual IEEE International Conference on Local Computer Networks, pp. 102–108. IEEE (2012)
2. Hong, X., Kong, J., Gerla, M.: Mobility changes anonymity: new passive threats in mobile ad hoc networks. Wirel. Commun. Mob. Comput. **6**(3), 281–293 (2012)
3. Kong, J., Hong, X., Gerla, M.: An identity-free and on demand routing scheme against anonymity threats in mobile ad-hoc networks. IEEE Trans. Mob. Comput. **6**(8), 888–902 (2007)
4. Zhang, Z., Liu, W., Fang, Y.: MASK: anonymous on-demand routing in mobile ad hoc networks. IEEE Trans. Wirel. Commun. **5**, 2376–2385 (2006)
5. Boukerche, A., El-Khatib, K., Xu, L., et al.: SDAR: a secure distributed anonymous routing protocol for wireless and mobile ad hoc networks. In: The Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, pp: 618–624 (2004)
6. Zhang, R., Zhang, Y., Fang, Y.: AOS: an anonymous overlay system for mobile ad hoc networks. Wirel. Netw. **17**(4), 843–859 (2011)
7. Zhang. P, Jiang. Y.X., Lin. C.: P-Coding: secure network coding against eavesdropping attacks, pp. 1–9. IEEE (2010)
8. Weiler, N.: Secure anonymous group infrastructure for common and future internet applications. In: The Proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, Louisiana, pp. 401–410 (2001)
9. Bao-liu, Y., Tie-cheng, G., Min-qiang, W., et al.: Mapper: a multicast-based peer-to-peer file anonymous retrieval protocol. Acta Electronica Sinica **32**(5), 754–758 (2004)
10. Oliveira, L.B., Aranha, D.F., Gouva, C.P.L., et al.: TinyPBC: pairings for authenticated identity-based non-interactive key distribution in sensor networks. Comput. Commun. **34**(3), 485–493 (2010)
11. Perng, G., Reiter, M., Wang, C.: M2: multicasting mixes for efficient and anonymous communication. In: The Proceedings of 26th IEEE International Conference on Distributed Computing Systems, pp: 59–69 (2006)
12. Xiao, L., Liu, X., Gu, W., et al.: A design of overlay anonymous multicast protocol. In: The Proceedings of Parallel and Distributed Processing Symposium (IPDPS), pp. 1–10 (2006)
13. Wang, J., Niu, C., Shen, R.: Bus-based anonymous mulitcast in peer-to-peer overlay. In: The Proceedings of International Conference on Network and Parallel Computing - Workshops, Dalian, China, pp:148–151 (2007)
14. Wright, M., Adler, M., Levine, B., et al.: An analysis of the degradation of anonymous protocols. In: The Proceedings of Network and Distributed System Security Symposium, San Diego, California, pp. 34–43 (2002)