Secure Communication Method Using Invitation Process in Mobile Ad Hoc Networks

MASAO TANABE, MASAKI AIDA
The Graduate School of System Design
Tokyo Metropolitan University
6-6 Asahigaoka, Hino-shi, Tokyo 191-0065
JAPAN
tanabe@computer.org, maida@sd.tmu.ac.jp

Abstract: - The importance of security in mobile ad hoc networks has been recognized for many years, and many secure routing methods have been proposed in this field. This paper discusses major security attacks in mobile ad hoc networks and focused on resource exhaustion attacks as the most important security issue. We reviewed countermeasures including the methods that we proposed before for these attacks and propose a highly secure communication method that is based on a very efficient invitation process for handling new members. We evaluate the method from the viewpoint of implementation and make it clear that it is more useful than the methods that we proposed before as a countermeasure against resource exhausting attacks. We also study and evaluate the method from the viewpoint of stability and clarify that it makes the network stable on condition that it decreases the members who are expelled from the network when the attacker is found.

Key-Words: - Mobile ad hoc network, Security, Communication method, Community, DDoS attacks

1 Introduction

As Internet acceptance is now widespread, many defense mechanisms have been proposed to counter the emerging security issues [1] [2] [3]. Security issues faced by not only the Internet but also mobile ad hoc networks have been recognized for many years and many defense approaches have been studied and implemented [4] [5] [6]. However, there are some differences between tackling security problems on the Internet and those on mobile ad hoc networks. On the Internet, there are permanent reliable nodes like authentication servers. On the other hand, because all nodes exist temporally in mobile ad hoc networks, we cannot expect to have any permanent node in the network. Moreover, on the Internet, routers or switches which compose the Internet are operated by Internet service providers or network carriers. Because they are separated from end users, it is impossible for end users to eavesdrop packets on the Internet. However, in mobile ad hoc networks, end user terminals not only transmit and receive packets but also relay packets for other users. It is, therefore, easier to eavesdrop packets in mobile ad hoc networks than on the Internet. Moreover, core network equipment of the Internet is supplied by mains power and the electricity consumption of the equipment is not an issue. However, in mobile ad hoc networks, all devices, including those that work as routers, must run on their own batteries, so it is important to reduce their electricity consumption and it is preferable not to use any encryption or authentication protocols since they raise the power consumption. Because of such requirements, mobile ad hoc networks pose the following security issues:

- Passive eavesdropping
- Denial of service attacks
- Signaling attacks
- Flow disruption attacks
- Resource exhaustion attacks.

Passive eavesdropping is possible because of the nature of mobile ad hoc networks. Each terminal in a mobile ad hoc network acts also as a router, so passive eavesdropping is inevitable. Passive eavesdropping can disclose confidential data or send it to a rival company, for example. The easiest way to prevent this is to use encryption, but this raises the consumption problem mentioned earlier.

Denial of service attacks can be launched easily because in mobile ad hoc networks each terminal inherently handles all data received from other terminals. An attacker only has to transmit many packets near the target terminal, which receives these packets directly or via other terminals and handles them and so becomes unable to process other data. When under denial of service attacks, the target terminal is unable to act as a relay node, so

the routes passing it will become unavailable and the mobile ad hoc network may be divided into isolated networks unable to communicate with each other. Because each terminal inherently handles all received data, it is difficult to prevent denial of service attacks.

Signaling attacks are performed by transmitting false routing information in a mobile ad hoc network. Some traffic routes in the mobile ad hoc network might be intentionally altered and become less efficient. These attacks cause packet delay or excess traffic in the mobile ad hoc network, but their effects are not fatal. To prevent such attacks, each terminal checks the legitimacy of the received routing information before adopting it and relaying it to the other terminals.

Flow disruption attacks are performed by delaying, dropping, or falsifying relay packets. The attacker can simply relay packets in an unfair manner to achieve a negative impact. This attack causes packet delay, packet loss or packet falsification, so some terminals retransmit packets creating redundant traffic. Although these effects are not fatal, it is difficult to prevent such attacks since all packets in mobile ad hoc networks are relayed by some terminals.

Resource exhaustion attacks can be easily performed by transmitting excessive packets from one or several attack terminals. All terminals reachable from the attack terminal can be targets and their batteries can be intentionally exhausted to disable further packet handling. Resource exhaustion attacks may split the attacked mobile ad hoc network into sub-networks that cannot communicate with each other. Effects of resource exhaustion attacks are severer than those of denial of service attacks because in resource exhaustion attacks, more terminals will become unavailable at the same time. Because each terminal inherently handles all received packets in mobile ad hoc networks, it is difficult to prevent resource exhaustion attacks.

Since among these attacks resource exhaustion attacks are the most difficult to prevent and their effects are severe, we proposed a number of countermeasures against resource exhaustion attacks in mobile ad hoc networks [7]. These countermeasures can also defend against denial of service attacks.

In this paper, after reviewing these countermeasures against resource exhaustion attacks, we propose a highly secure communication method in mobile ad hoc networks that uses an efficient invitation process for handling new members.

The remainder of this paper is organized as follows. In Section 2, we briefly review the countermeasures we have already proposed for resource exhaustion attacks and show their disadvantages. In Section 3, we propose a new secure communication method for mobile ad hoc networks; it offers an efficient invitation process for handling new members. In Section 4, we study and evaluate this method. Finally, Section 5 concludes this paper.

2 Countermeasures against Resource Exhaustion Attacks and Their Disadvantages

Fig.1 shows an example of a mobile ad hoc network.

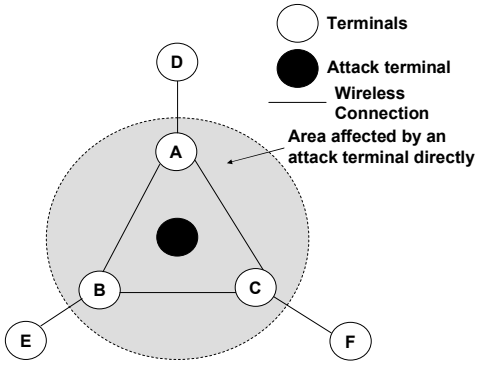

Fig. 1 Example of Mobile Ad Hoc Network and an Attack Terminal

Terminals A, B and C have wireless connections with each other and with terminals D, E, and F, respectively. On the other hand, terminals D, E and F have a wireless connection with only one node which is A, B, and C, respectively. When an attack terminal occupies the centroid of A, B, and C and begins a resource exhaustion attack, that is, transmitting excessive numbers of packets, terminals A, B and C which can receive these packets start processing them, consume their batteries and finally halt. As a result, not only terminals A, B and C but also terminals D, E, and F lose their wireless connections with other terminals because they become isolated.

We proposed three following prevention methods against resource exhaustion attacks:

- Time slot method
- Token method
- Secret key method.

In the time slot method, each terminal can transmit its packets only in its pre-assigned time slots. All terminals know all time slots for all terminals. In this scheme, because an attack terminal does not belong to the mobile ad hoc network, it does not have its own time slots for transmission.

In the token method, each terminal can transmit its packets only when it receives a token from the mobile ad hoc network. An attack terminal cannot receive any token and therefore cannot transmit its packets.

In the secret key method, each terminal transmits its packets with a common secret key which is given when it joins the mobile ad hoc network. Because an attack terminal cannot obtain the secret key, it transmits packets without one.

Using these methods, legitimate terminals can easily detect and discard illegitimate packets from the attack terminal when they receive the packets and illegitimate packets are not transmitted to other terminals from the received terminals. However terminals which receive packets from the attack terminal directly must check whether the packets are transmitted from legitimate terminals. This consumes some of their batteries. However, the resources required for packet checking are less than those need to transmit them to other terminals. Therefore, using these methods, even terminals that receive packets from the attack terminal directly can have longer lifetimes.

In the time slot method, time slots must be pre-assigned and each terminal belonging to the mobile ad hoc network must remember not only its time slots but also those for the other terminals and transmit its packets only in its pre-assigned time slots. This method also requires all terminals to synchronize their clocks, which is extremely difficult in practice. In the token method, each terminal must transmit its packets only when it has the token and transfer the token to the next terminal when it completes packet transmission or after timeout. Unfortunately, handling tokens in a mobile ad hoc network is difficult and a missing token will cause serious problems in the network. In the secret key method, each terminal must receive the secret key when it joins the mobile ad hoc network and transmit the secret key in each packet header. Moreover, once the secret key becomes known to the attacker, the attacker can easily conduct attacks.

3 Secure Communication Method in Mobile Ad Hoc Networks Using Invitation Process

In this section, we propose a new secure communication method for mobile ad hoc networks that uses an efficient invitation process for network joining and describe the specification of the method.

3.1 Proposal of Secure Communication Method in Mobile Ad Hoc Networks Using Invitation Process

As shown in Section 2, all of our countermeasures to resource exhaustion attacks have problems when implemented in mobile ad hoc networks. Therefore, in this section we propose a new highly secure communication method in mobile ad hoc networks that offers an efficient invitation process for handling new members.

In mobile ad hoc networks, security devices such as IDS (Intrusion Detection Systems) are not always available to detect attacks. Therefore, each terminal in mobile ad hoc networks must detect these attacks by checking incoming packets from other terminals. For this reason, any secure communication method must allow terminals to easily distinguish attack traffic from legitimate traffic.

First, we assume that the initial mobile ad hoc network is composed of members who know each other well and never transmit attack packets to the other members. We feel that this is a reasonable assumption given the desire to achieve highly secure communication. In addition, we assume that only communication between members in this mobile ad hoc network is allowed. We call these members in the initial mobile ad hoc network "the initial members". A new member who wants to join the mobile ad hoc network can do so only if he knows one of the initial members; he is accepted as a temporary member.

A temporary member cannot transmit and receive packets freely. He can only transmit and receive packets via his inviting member and so must be near his inviting member. The inviting member is responsible for the packets transmitted by the temporary member. Although this assumption of spatial closeness restricts the locations of these members, it highlights the responsibility of the inviting member. If a temporary member transmits an attack packet and if the member detecting the attack packet is not the inviting member, the network expels not only the temporary member but also the inviting member and its subordinates. Here,

we call the temporary member "a subordinate" of the inviting member.

After a certain period, the temporary member will be approved as a regular member and will be able to transmit and receive packets freely. However, even after it becomes a regular member, once it transmits an attack packet, not only it but also the inviting member and its subordinates will be expelled from the mobile ad hoc network.

Moreover, in this method, we assume that each member can detect attack packets by comparing them against known attack signatures. This detection method has already been introduced in some existing Intrusion Prevention Systems (IPS) [8] [9].

In this communication method, the attacker can not become the member of the mobile ad hoc network easily, and even if it becomes a regular member, it will be expelled from the mobile ad hoc network soon after its illegal packets are detected by another member in the mobile ad hoc network.

Using Fig.2, we explain this proposed communication method. In this figure, members A, B, C, D, E, F and G are the initial members of the mobile ad hoc network. Member H wants to join the network. In this example, member E and member H are assumed to be familiar with each other. At first, member E invites member H into this mobile ad hoc network, and allows member H to transmit and receive packets via member E. After a certain period, member H will become a regular member and become able to transmit and receive packets freely. However, once member H transmits attack packets, the network expels not only member H (regardless of its status) but also member E. This mobile ad hoc network will then consist of only members A, B, C, D, F, and G.

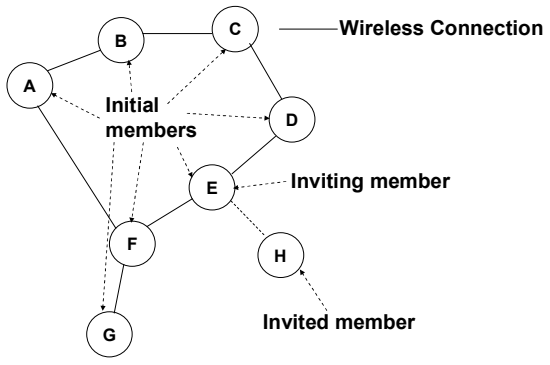

Fig. 2 Secure Communication Method in Mobile Ad Hoc Network

3.2 Specification of the Proposed Method

Next, we describe the specification of the proposed method. Concretely, we specify the action of the members by describing each stage shown in Fig.3.

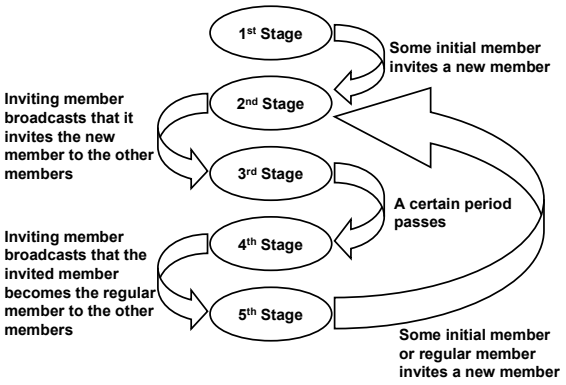

Fig. 3 Stage Transition of Proposed Method

(1) 1st Stage: Initial Stage without Any Temporary Member

In this stage, all members in this mobile ad hoc network can transmit and receive packets freely. That is, they receive all packets transmitted by other members in this mobile ad hoc network and if necessary they transmit these packets again to the other members. They do not check the packets transmitted by the initial members in this mobile ad hoc network. Of course, they check the source address of the received packet and discard it if its source address is not that of some initial member.

(2) Transition from 1st Stage to 2nd Stage

This transition occurs when an initial member invites a new member.

(3) 2nd Stage: Stage After Some Member Invites a New Member

In this stage, a temporary member is accepted by an inviting member. No other members are aware of this fact.

(4) Transition from 2nd Stage to 3rd Stage

This transition occurs when the inviting member informs the other members that it has invited a temporary member and indicates its address.

(5) 3rd Stage: Stage of Temporary Member Existence

In this stage, all members in the mobile ad hoc network recognize that the inviting member has accepted a temporary member.

(i) Members other than inviting member or temporary member

A member other than the inviting member or temporary member must check packets transmitted by the temporary member via the inviting member. Therefore, it first checks the source addresses of received packets. When its address is the inviting member, it checks whether the packet was transmitted by the temporary member. If the packet was generated by the inviting member, the member receives it without any action and if necessary transmits it again. However, if the packet was transmitted originally by the temporary member, the member must check whether the packet is an attack packet or not before receiving it. When it is not an attack packet, the member receives it and if necessary transmits it again. However, when it is an attack packet, the member discards it and transmits to the other members the fact that the temporary member is an attacker and both the temporary member and the inviting member and its subordinates are expelled. As is obvious, a received packet is discarded if its source address is not that of either an initial member or a regular member.

Initial and regular members can transmit packets to all members including temporary members freely. However, packets intended for a temporary member must be transmitted to the appropriate inviting member. Of course, at that time each packet must clearly show that its final destination address is the temporary member.

(ii) Inviting member

The inviting member must transmit not only its own packets but also packets from the temporary member. To avoid being expelled from the mobile ad hoc network, it must check packets from the temporary member before it relays them.

Moreover, because the true destination of packets from the temporary member is either the inviting member or another member, it must check their destination and if they are packets destined for another member, it keeps the destination address and indicates clearly that they were generated by the temporary member and relays them to the other member.

It must also receive not only packets destined for it but also packets destined for the temporary member. When the true destination of a received packet is the temporary member, the inviting member keeps the source address and relays the packet to the temporary member. Also in this case, it checks the source address of the received packet and discards it if its source address is not that of either an initial or regular member.

(iii) Temporary member

The temporary member can transmit packets only via the inviting member. It inserts the true destination address into the destination address field and transmits it to the inviting member.

It receives legal packets only via the inviting member so it checks the source address of the received packet and discards it if its source address is not that of either an initial or regular member. Because the source addresses of received packets via the inviting member are not changed by the inviting member, the temporary member can detect the originating member from the source address of the packet.

(6) Transition from 3rd Stage to 4th Stage

This transition occurs after a certain period passes.

(7) 4th Stage: Stage When the Temporary Member Has Become a Regular Member

In this stage the temporary member becomes a regular member. However, most members other than the inviting member do not know of this fact.

(8) Transition from 4th Stage to 5th Stage

This transition occurs when the inviting member broadcasts to both initial and regular members that the temporary member has become a regular member and its address.

(9) 5th Stage: Stage When the Temporary Member Has Joined and Has Already Become the Regular Member

In this stage, all members in the mobile ad hoc network recognize that the temporary member has become the regular member and its address.

(i) Member other than inviting or temporary member

A member that is not an inviting member nor a temporary member must check packets that were transmitted by a regular member directly. It first checks the source address of the received packet. If the packet was transmitted by a regular member, the member then checks whether the packet is an attack packet or not before receiving it. If it is not an attack packet, the member receives it and if necessary transmits it again. However, when it is an attack packet, the member discards it and transmits the fact that the regular member is an attacker and both the regular member and its inviting member and its subordinates are expelled. Also in this case, the packet is discarded if its source address is not that of either an initial or regular member.

(ii) Inviting member
The inviting member transmits and receives packets freely. Of course in this case, it checks the source address of the received packet and discards it if its source address is not that of either an initial member or regular member. However, after the temporary member has been recognized as an attacker, it and its subordinates will be also expelled from the mobile ad hoc network along with the temporary member.

(iii) Regular member
The regular member can also transmit and receive packets freely in the mobile ad hoc network. Of course in this case, it checks the source address of the received packet and discards it if its source address is not that of either an initial or regular member.

(10) Transition from 5th Stage to 2nd Stage
This transition occurs when some initial member or regular member invites a new member.

3.3 Proposal of Packet Header Format

Next, we propose the packet header format for the mobile ad hoc network that uses this secure communication method.

As shown in Section 3.1, in this method we must distinguish from the packet header whether the packet was generated by the inviting member or the temporary member and also distinguish whether the packet is to the inviting member or to the temporary member. This means we need option fields for both destination address and for source address. In order to make it easy to implement this secure communication method in the mobile ad hoc network, we assume that one initial or regular member has only one temporary member at any time. In other words, after the temporary member becomes a regular member, the inviting member can have another temporary member. With this assumption, we need only one additional bit for the destination address and one additional bit for a source address. The optional field takes the value of "1" only when the packet is generated by the temporary member or the packet is intended for the temporary member (Fig.4). In the example of Fig.4, DA optional field is "1" and SA optional field is "0", so this packet is destined for the temporary member who was invited by the member whose address is "DA". It also denotes that this packet was not generated by a temporary member.

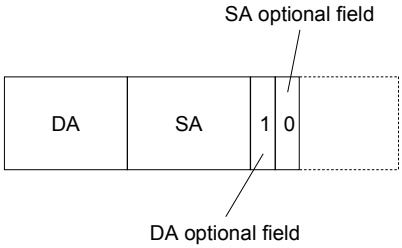

Fig.4 Example of Packet Header Format

4 Evaluation of Proposed Secure Communication Method

In this section, we study and evaluate the proposed secure communication method in mobile ad hoc networks.

4.1 Evaluation from the Viewpoint of Implementation

First we evaluate the proposed secure communication method using invitation process from the viewpoint of implementation.

This proposed method needs optional fields to distinguish whether the packet was generated by or intended or the temporary member or not. These optional fields incur substantial overhead. Moreover, the members in the mobile ad hoc network must respond appropriately in each stage as described in Section 3.2. However, this method does not have any effect on the communication protocol used in the mobile ad hoc network. Therefore, we can implement this secure communication method regardless of which communication protocol is used. This method affects only the action of members in the mobile ad hoc network. A new member who wants to become a regular member in the mobile ad hoc network can accept this change in order to keep the network secure.

We note that two of our previous countermeasures, the time slot method and the token method, demand more changes to the communication method than this secure communication method. The time slot method requires all terminals to synchronize their clocks, which is difficult in practice. Handling tokens is difficult and missing tokens will cause serious

problems in the network. As a result, we can say that the secure communication method is superior to the time slot method and the token method from the viewpoint of implementation in mobile ad hoc networks.

4.2 Evaluation from the Viewpoint of Stability

Next we evaluate the proposed secure communication method from the viewpoint of stability.

We will now show how a mobile ad hoc network that uses this method evolves over time. First, we discuss the characteristics of our method. In our method, the initial members create the network and they never transmit attack packets. In other words, they never become attackers. On the contrary, it is possible for the regular members to issue attack packets. That is, they may become attackers. Moreover, at the beginning of the network only the initial members exist and the number of the members in the network increases because the initial members invite new people to become members of the network. Therefore, the initial members have more subordinates than the regular members. Moreover, among the regular members, a member who is close to one of the initial members has more subordinates than a member who is distant from one of the initial members. Therefore, the number of members in the network would decrease sharply if a regular member who is close to one of the initial members or an initial member itself starts to transmit attack packets and is recognized as the attacker and consequently both it and its subordinates are expelled from the network. We think this is the key issue with our proposal. We show an example of a member family tree in Fig.5.

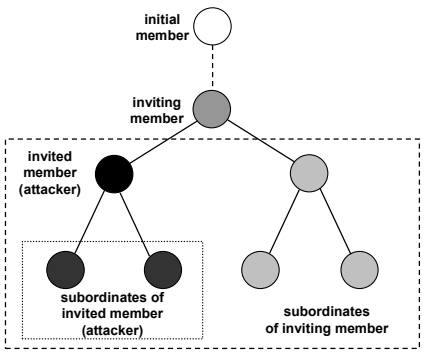

Fig. 5 Example of a Family Tree of an Inviting Member

Therefore we propose two methods to resolve this issue as follows:

1. *limit the total number that each member can invite*
   This method holds the number of members in the network to a slow increase because a member who has already invited the predetermined number of members can not invite a new member.
2. *decrease the members who are expelled from the network when some regular member is recognized as the attacker.*

In order to confirm the efficiency of these two proposed methods, we conducted simulations. First, we conducted simulations of the first method using the following conditions:

- the number of initial members : one
- the initial member is not expelled
- the proportion of the attackers to the normal members among the temporary members arriving to the network : 2 : 1
- the delay between the start of an attack from the time at which the attacker became a regular member: 10 time units
- the arrival rate of temporary members to the network : 10 members/unit time
- the arrival distribution of the temporary member to the network : Poisson distribution.

Here, we assume that no initial member can be expelled because the network could disappear if initial members could be expelled.

We show the result of this simulation in Fig.6. From this figure, we can find that the number of the members in the network is not stabilized and indeed the expansion of the network halts contrary to our expectations. We consider the reasons for this result as follows:

- The reason why the network stops expanding is that the number of members in the network decreases to one and the initial member can not invite any new member because it has already invited the predetermined number of members.
- The number of subordinates expelled is extremely large if the attacker starts to transmit attack packets some time after it became a regular member. In this case, the number of members in the network decreases sharply.

- Since we limit the number of the members that each member can invite, the member will invite a predetermined number of members to the network and will not be able to invite any other new members soon. On the other hand, the number of members in the network does not increase monotonously even if we increase the number of the members that each member can invite.

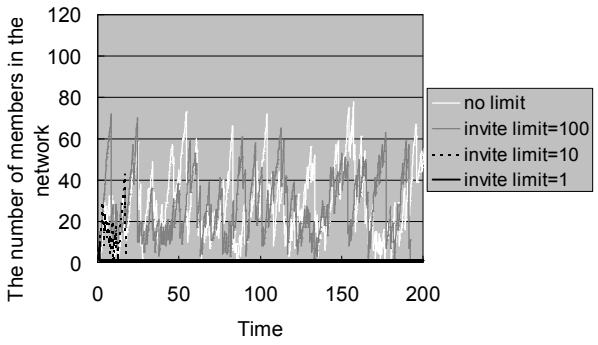

Fig. 6 First Method for Resolving the Issue

Next, we consider the second method. We can categorize members who are expelled into the following four groups:

1. the attacker
2. the inviting member who invited the attacker
3. the subordinates of the attacker
4. the subordinates of the inviting member who are not subordinates of the attacker.

In our proposed secure communication method, the inviting member is responsible for the temporary member. For this reason, the inviting member tends to invite only reliable people in order to avoid being expelled from the network. On the contrary, the attacker does not fear that it will be expelled from the network. Therefore, we can regard the subordinates of the attacker as unreliable members. The fourth category is deemed reliable and is not expelled when the inviting member is expelled.

We study this situation using the mathematical model.

We assume that the mean of the number of members that are subordinates of the member is m when we pick up a member. We define the downward degree of a member j is $d(j)$. Here the downward degree of a member is the number of members that it invited directly. We define the degree distribution as $p(k)$. Namely,

$$p(k) = P_r\{d(j) = k\}. \quad (1)$$

We define the average degree d and the variance of degree v_d respectively as follows:

$$d := \sum_{k=0}^{\infty} k \cdot p(k),$$

$$v_d := \sum_{k=0}^{\infty} (k-d)^2 \cdot p(k).$$

When we pick up a member, we define the probability that the downward degree of the member that invited it is k as $q(k)$. This probability $q(k)$ is proportional to both the downward degree k and the degree distribution $p(k)$. Using a proportionality constant C,

$$q(k) = C \cdot k \cdot p(k). \quad (2)$$

Here,

$$1 = \sum_{k=0}^{\infty} q(k) = C \cdot d. \quad (3)$$

Therefore,

$$q(k) = \frac{k}{d} \cdot p(k). \quad (4)$$

As a result, the mean of number of members that are expelled from the network in the original proposed method is expressed as follows:

$$m \times \sum_{k=0}^{\infty} k \cdot q(k) = \frac{m}{d} \cdot (v_d + d^2).$$

On the contrary, when the subordinates of the inviting member who are not subordinates of the attacker are not expelled from the network, the mean of number of members that are expelled from the network is m. Therefore the proportion of the mean of number of members that are expelled from the network in both methods is expressed as follows:

$$\frac{1}{d} \cdot (v_d + d^2).$$

Next, we conducted a simulation of the second method using the same conditions as the first simulation except for the following condition:

- the subordinates of the attacker are expelled but the subordinates of the inviting member who are not subordinates of the attacker are not expelled.

We show the result of this simulation in Fig.7. It shows that the growth in the number of members in

the network differs significantly from growth under our original secure communication method.

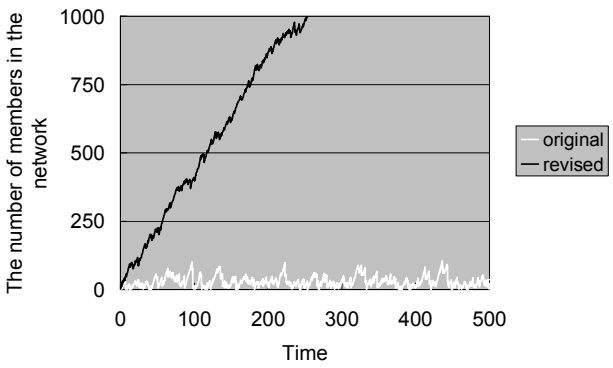

Fig. 7 Second Method for Resolving the Issue

We consider that this result occurs for the following reasons:

- In this method, the expelled members are the subordinates of the attacker, the attacker, and the inviting member of the attacker. Under our simulation conditions, the number of members expelled is almost constant because the delay between becoming a regular member and the start of attack packet transmission is fixed.
- It is obvious that the number of members in the network increases because this revised method expels fewer members when the attacker is expelled.

Though it is desirable for attackers that the number of expelled members in the network is large when the attacker is expelled, this situation is undesirable for the members who are not attackers. Therefore we recognize that the second method is effective from this standpoint.

5 Conclusion

This paper studied some security issues in mobile ad hoc networks and focused on resource exhaustion attacks as the most important security issue.

We then briefly reviewed countermeasures for resource exhaustion attacks that we proposed and show their disadvantages. We then proposed a new secure communication method in mobile ad hoc network that offers an efficient invitation process to handle new members.

Finally, we briefly evaluated the proposed secure communication method from the viewpoint of implementation and made it clear that the proposed secure communication method is more useful than the method that we proposed as a countermeasure against resource exhausting attacks in a mobile ad hoc network. We also evaluated the proposed secure communication method from the viewpoint of stability and clarified that it makes the network stable on condition that it decreases the members who are expelled from the network when the attacker is found and the initial members are not expelled.

Acknowledgements

This research was partially supported by the Grant-in-Aid for Scientific Research (S) No.18100001 (2006--2010) from the Japan Society for the Promotion of Science.

References:

[1] J. D. Howard, An analysis of security incidents on the Internet, *PhD thesis*, Carnegie Mellon University, August 1988.

[2] C. Meadows, A formal framework and evaluation method for network denial of service, *In Proceedings of the 12th IEEE Computer Security Foundations Workshop*, June 1999.

[3] J. Mirkovic, P. Reiher, A Taxonomy of DDoS Attack and DDoS Defense Mechanisms, *ACM SIGCOMM Computer Communications Review 2004* (April 2004).

[4] Hu, Y.-C., Perring, A., and Johnson, D. Packer leashes, A defense against wormhole attacks in wireless ad hoc networks, *In Proceeding of IEEE Inform 2003* (San Francisco, Apr. 1-3. 2003).

[5] Karlof, C. and Wagner, D., Secure routing in wireless sensor networks: Attacks and countermeasures, *In Proceeding of the 1st IEEE International Workshop on Sensor Network Protocols and Applications* (Anchorage, AK, May 11, 2003).

[6] Wood, A. and Stankovic, J., Denial of service in sensor networks, *IEEE Computer* (Oct. 2002), 54-62.

[7] M. Tanabe and M. Aida, Preventing Resource Exhaustion Attacks in Ad Hoc Networks, *In Proceeding of the 2nd IEEE International Workshop on Ad Hoc. Sensor and P2P Networks* (Sedona, AZ, March 21, 2007).

[8] *McAfee Network Security Platform*, available at http://www.macafee.com/us/products/network-security-platform.aspx

[9] *DefensePro*, available at http://www.radware.com/Products/ApplicationNetworkSecurity/DefensePro.aspx

Masao Tanabe

Received his B.E. and M.E. degrees in Electronics and Communication Engineering from Waseda University, Tokyo, Japan, in 1985 and 1987, respectively. He joined NTT Laboratories in April 1987. He is also a graduate student of the Graduate School of System Design, Tokyo Metropolitan University. His current interests include security issues in communication networks. He is a member of the IEEE and the IEICE.

Masaki Aida

Received his B.S. and M.S. in Theoretical Physics from St. Paul's University, Tokyo, Japan, in 1987 and 1989, respectively, and received the Ph.D. in Telecommunications Engineering from the University of Tokyo, Japan, in 1999. In April 1989, he joined NTT Laboratories. From April 2005 to March 2007, he was an Associate Professor at the Faculty of System Design, Tokyo Metropolitan University. He has been a Professor of the Graduate School of System Design, Tokyo Metropolitan University since April 2007. His current interests include traffic issues in computer communication systems. He received the Young Researchers' Award of IEICE in 1996. He is a member of the IEEE, the IEICE, and the Operations Research Society of Japan.