Secure Communication Method in Mobile Wireless Networks

Masao Tanabe
Tokyo Metropolitan University
6-6, Asahigaoka, Hino-shi, Tokyo 191-0065 Japan
+81-42-585-8600
tanabe@computer.org

Masaki Aida
Tokyo Metropolitan University
6-6, Asahigaoka, Hino-shi, Tokyo 191-0065 Japan
+81-42-585-8627
maida@cc.tmit.ac.jp

ABSTRACT
The importance of security has been recognized in mobile wireless networks for many years. Consequently many secure routing methods have been proposed in this field. This paper discusses major security attacks in mobile wireless networks, and proposes a highly secure communication method in mobile wireless networks, especially in mobile ad hoc networks.

Categories and Subject Descriptors
C.2.1 **[Computer-Communication Networks]**: Network Architecture and Design – *Distributed networks, Wireless communication.*

General Terms
Design, Security

Keywords
mobile wireless network, security, communication method

1. INTRODUCTION
As the Internet becomes widespread, many defense mechanisms have been proposed to counter the emerging security issues on the Internet [1][2][3]. Security issues faced by not only the Internet but also mobile wireless networks have been recognized for many years and many defense approaches have been studied and implemented [4][5][6]. However, there are some differences in tackling security problems on the Internet and on mobile wireless networks. On the Internet, there are permanent reliable nodes like authentication servers. On the other hand, because all nodes exist temporally in mobile wireless 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 some mobile wireless networks, especially 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 some mobile wireless networks than on the Internet. Besides, on the Internet, the electric power of core network equipments are always turned on, so electricity consumption of these equipments is never an issue. However, in some mobile wireless networks, all equipments which also work as routers are operated by their own batteries, so it is important to reduce their electricity consumption and it is preferable not to use any encryption or authentication protocols that require more electricity. Because of such requirements, some mobile wireless networks pose the following security issues:

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

Passive eavesdropping can be performed because of the nature of some mobile wireless networks. Each terminal in some mobile wireless networks acts also as a router, so eavesdropping can not be prevented. By passive eavesdropping, confidential data might be unveiled or sent to the rival company, for example. The easiest way to prevent this is to use encryption, but this creates electricity consumption problem mentioned earlier.

Denial of service attacks can be launched easily because in some mobile wireless networks each terminal handles all data received from other terminals by nature. An attacker only transmits numerous data near the target terminal, so the target terminal will receive these data directly or via other terminals and handle them and become unable to process other data. When under denial of service attacks, the target terminals is unable to act as a relay node, so the routes passing it will become unavailable and the mobile wireless network may be divided into isolated networks unable to communicate with each other. Because each terminal handles all received data in some mobile wireless networks by nature, it is difficult to prevent denial of service attacks.

Signaling attacks are performed by transmitting false routing information in a mobile wireless network. Some traffic routes in the mobile wireless network might be intentionally altered and become less efficient. These attacks cause packet delay or excess traffic in the mobile wireless network, but their effects are not fatal. To prevent such attack, 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 or

Mobilware '08, February 12-15, 2008, Innsbruck, Austria.

dropping or falsifying relay packets in some mobile wireless networks. Attacker can simply relay packets in an unfair manner to achieve negative impacts. This attack causes packet delay, packet loss or packet falsification, so some terminals retransmit packets and useless traffic might be increased. Although these effects are not fatal, it is difficult to prevent such attacks since all packets in some mobile wireless networks are relayed by some terminals.

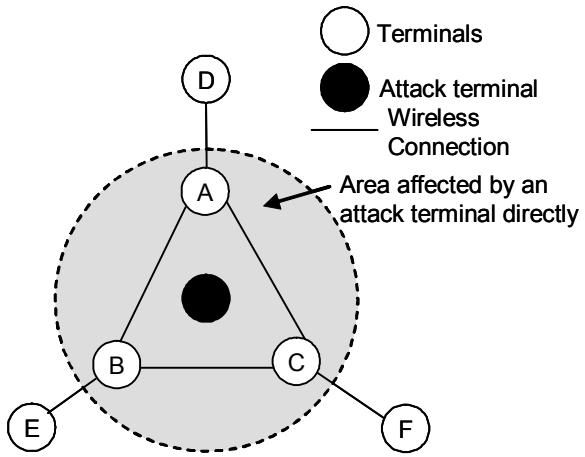

Figure 1. An example of mobile ad hoc network and an attack terminal

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

Among these attacks, resource exhaustion attacks are the most difficult to prevent and their effects are severe, and therefore 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, we study these countermeasures against resource exhaustion attacks briefly, and we propose a highly secure communication method in some mobile wireless networks, especially in mobile ad hoc networks..

The remainder of this paper is organized as follows. In Section 2, we study countermeasures which we have already proposed for resource exhaustion attacks briefly and show their disadvantages. In Section 3, we propose a new secure communication method in mobile ad hoc network. In Section 4, we study and evaluate this method quantitatively. Finally, Section 5 concludes this paper.

2. COUNTERMEASURES AGAINST RESOURCE EXHAUSTION ATTACKS AND THEIR DISADVANTAGES

Figure 1 shows an example of a mobile ad hoc network. 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 enters into the center of A, B, and C and begins a resource exhaustion attack, that is, transmitting excessive packets, three terminals A, B and C which can receive these packets start processing them, consume their batteries and halt at last. 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 these resource exhaustion attacks:

- Time slot method
- Token method
- Secret key method

In time slot method, each terminal can only transmit its packets 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 to transmit its packets.

In 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 transmit its packets without one.

In 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 not belonging to the mobile ad hoc network 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 the legitimate terminals. This consumes some of their batteries. However, the required resources to check the packets are less than that of transmitting them to other terminals. Therefore, using these methods, even terminals that receive packets from the attack terminal directly can persist longer.

In the time slot method, time slots must be pre-assigned and each terminal which belongs to the mobile ad hoc network must remember not only the time slots for it but also time slots 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 ends to transmit its packets or after the timeout. Besides, handling token in the mobile ad hoc network is difficult and 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 the packet header whenever it transmits packets. In addition, once the secret key is unveiled to the attacker, the attacker can easily transmit their packets.

3. SECURE COMMUNICATION METHOD IN MOBILE AD HOC NETWORKS

As shown in Section 2, all countermeasures which we proposed against resource exhaustion attacks have disadvantages to implement in mobile ad hoc networks. Therefore, in this section we propose a new highly secure communication method in some mobile wireless networks,

especially in mobile ad hoc networks.

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, proposing 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 send attack packets to the other members. We feel that this a reasonable assumption 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 member". When new member wants to join the mobile ad hoc network, if the new member knows someone in the initial members then it will be allowed to join the mobile ad hoc network temporarily. If the new member does not know anyone in the initial members then it will not be allowed to join the mobile ad hoc network.

Even when the new invited member is allowed to join the mobile ad hoc network temporarily, it can not transmit and receive packets freely in the mobile ad hoc network. It can only transmit and receive packets via the inviting member which is the initial member. Therefore, the inviting member is responsible for the packets which are transmitted by the invited member. Moreover, the inviting member must be near the invited member in this stage. Although this assumption restricts the locations of these members, it also makes the inviting member responsible for the invited member. Moreover, once the invited member transmits the attack packet, not only the invited member but also the inviting member will be expelled from the mobile ad hoc network. This assumption too makes the inviting member responsible for the invited member.

After a certain period, the invited 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 the attack packet, not only it but also the inviting member 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 with known attack signatures.. This detection method has already been introduced in some existing Intrusion Prevention Systems (IPS).

In this communication method, the attacker can not become the member of the mobile ad hoc network easily, and even if it will be invited or become the regular member, it will be expelled from the mobile ad hoc network soon after transmitting illegal packets will be discovered by the another member in the mobile ad hoc network.

Using Figure 2, we explain this proposed communication method. In this figure, members A, B, C, D, E, F and G are the initial member of the mobile ad hoc network. Member H is the new member, which wants to join the mobile ad hoc network. In this example, member E and member H are assumed to be familiar with each other. At first, member E invites member H to this mobile ad hoc network, and therefore member H can transmit and receive packets via member E in this mobile ad hoc network. After a certain period, member H will become a regular member and it will be able to transmit and receive packets freely in this mobile ad hoc network. However, once member H transmits attack packets in this mobile ad hoc network while it is an invited member or after it becomes the regular member, not only member H but also member E will be expelled from this mobile ad hoc network. This mobile ad hoc network will then consist of only members A, B, C, D, F and G.

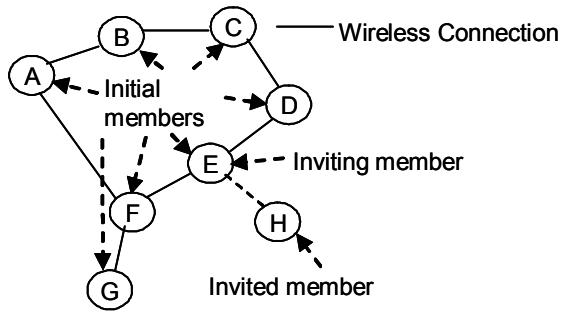

Figure 2. Secure communication method in mobile ad hoc network

3.1 Specification of Member Action

Next, we define the action of the members in the mobile ad hoc network using this secure communication method.

3.1.1 Initial Stage without Any Inviting Member

In this stage all members in this mobile ad hoc network can transmit and receive packets freely. So they receive all packets which were transmitted by other members in this mobile ad hoc network and if necessary they transmit these packets again to the other members in this mobile ad hoc network. They do not need to check all packets which are 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 of some initial member.

3.1.2 Stage when an Invited Member Has Just Joined

In this stage the inviting member broadcasts to the other initial member that it has the invited member and has become the inviting member. By this broadcasting, all members in the mobile ad hoc network recognize that the inviting member has the invited member.

3.1.3 Stage when the Invited Member Has Joined but Has not Become the Regular Member Yet

(1) Not inviting member

In this stage a member that is not an inviting member must check packets which were transmitted by the invited member via the inviting member. Therefore, it first checks source addresses of received packets. When its address is the inviting member, it checks whether the packet was transmitted by the invited member. If the packet was transmitted 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 invited 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 the fact that the invited member is an attacker and the inviting member also should be expelled to the initial members other than the inviting member. Also in this case, they check the source address of the received packet and discard it if its source address is not of some initial member.

On the contrary, the member can transmit its packets to all members that include both the inviting member and the invited member freely until the invited member has been recognized as an attacker. However, when it transmits packets to the invited

member, it transmits them to the inviting member. Of course, at that time it must show clearly that the final destination address of them is the invited member.

(2) Inviting member

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

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

And it must also receive not only packets destined for it but also packets destined for the invited member and if necessary transmit it again. When the true destination of received packets is the invited member, the inviting member remains the source addresses of them and relays them to the invited member. Also in this case, it checks the source address of the received packet and discards it if its source address is not of some initial member.

(3) Invited member

The invited member can transmit its packets only via the inviting member. So it inserts their true destination address in the destination address fields of them and transmits them to the inviting member.

On the contrary, 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 of some initial member. And because the source addresses of received packets via the inviting member have not changed by the inviting member, the invited member can detect the true source member from the source address of the packet.

3.1.4 Stage when the Invited Member Has Become the Regular Member

In this stage the inviting member broadcasts to the other initial member that the invited member has become the regular member and its address. After this broadcast, all members in the mobile ad hoc network recognize that the inviting member has the regular member and its address.

3.1.5 Stage when the Invited Member Has Joined and Has Already Become the Regular Member

(1) Not inviting member

In this stage a member that is not an inviting member must check packets which were transmitted by the invited member directly. So it must check source addresses of received packets. If a packet was transmitted by the invited 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 the fact that the invited member is an attacker and the inviting member also should be expelled to the initial members other than the inviting member. Also in this case, it discards it if its source address is not of some initial or regular member.

On the contrary, the member can transmit its packets to all members that include both the inviting member and the invited member freely until the invited member has been recognized as an attacker.

(2) Inviting member

In this stage, the inviting member transmits and receives packets as the same as the not inviting member. Of course in this case, it checks the source address of the received packet and discards it if its source address is not of some initial member or regular member. However, after the invited member has been recognized as an attacker, it will be expelled from the mobile ad hoc network.

(3) Invited member

In this stage, the invited 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 of some initial member. However, after it has been recognized as an attacker, it will be expelled from the mobile ad hoc network.

3.2 Proposal of Packet Header Format

Next, we propose the packet header format in the mobile ad hoc network using this secure communication method.

As shown in section 3.1, in this method we must distinguish from the packet header whether packets from the inviting member or from the invited member and also distinguish whether packets to the inviting member or to the invited member. So we need option fields that show whether the packet was transmitted from the inviting member or the invited member. These fields are necessary both for a destination address and for a 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 member has only one invited member at any time. In other words, after the invited member becomes the regular member, the inviting member can have another invited member. With this assumption, we need only one bit for a destination address and one bit for a source address. And we define that the optional field is “1” only when the packet was transmitted by the invited member or the packet was destined for the invited member (Figure 3). In the example of Figure 3, DA optional field is “1” and SA optional field is “0”, so this packet is destined for the invited member which was invited by the member whose address is “DA”. It also denotes that this packet is not transmitted from the invited member.

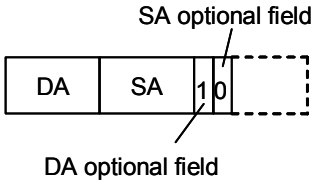

Figure 3. Example of packet header format

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 in the Point of Implementation

First we evaluate the proposed secure communication method in the point of implementation.

This proposed method needs optional fields to distinguish whether the packet was transmitted from the invited member or not. These optional fields require substantial overhead. And also

members in the mobile ad hoc network must take their action in an each stage which we mentioned in section 3.1. However, this method does not have any effect on the communication protocol used in the mobile ad hoc network. Therefore, we can use any communication protocol of the mobile ad hoc network to implement this secure communication method. This method affects only the action of members in the mobile ad hoc network. A new member who wants to be a regular member in the mobile ad hoc network can accept this change in order to keep the network secure.

On the other hand, two countermeasures which we proposed before and discussed in section 2, that is the time slot method and the token method, need more changes to communication method than this secure communication method. The time slot method requires all terminals to synchronize their clocks, which is difficult in practice. Handling token is difficult and missing token will cause serious problems in the network. As a result, we can decide this secure communication method is superior to the time slot method and the token method in the point of implementation in a mobile ad hoc network.

4.2 Evaluation in the Point of Secure Communication

Next we evaluate this proposed secure communication method in the point of secure communication.

As we specified in section 3.1, in the mobile ad hoc network using this secure communication method, packets from the terminal which is not the member are discarded by the member which receive them and are not transmitted to the other members. By this action, the member consumes its battery. However the required resources to compare the packet with signatures are less than transmitting them to other terminals. This action also allows member terminals to easily detect and discard illegitimate packets from the attack terminal and therefore prevent illegitimate packets from being transmitted to other terminals. Moreover, terminals that receive packets from the attack terminal directly can persist longer. It is an advantage of this secure communication method that shares in common with the three methods that we studied in section 2. Consequently this secure communication method in the mobile ad hoc network should be useful as a countermeasure against resource exhausting attacks.

In order to discuss how the effects of the resource exhaustion attack could be mitigated by this secure communication method, we compare this method with a normal scenario under which no prevention method is deployed. In particular, we focus on the battery consumption of the terminals in the mobile ad hoc network.

Under the normal scenario, a resource exhaustion attack affects not only terminals which receive packets from the attack terminal directly but also terminals which do not receive these packets directly because the latter terminals receive illegitimate packets transmitted from former terminals directly or indirectly. Moreover, because former terminals transmit illegitimate packets whose destination addresses are different from them, these terminals consume their batteries to transmit them.

On the other hand, using the proposed secure communication method, only members which receive packets from the attacker directly are affected by the resource exhaustion attack because these members discard and do not transmit such packets to any other members. As a result, other members will not be affected by the attack. Of course, these members consume their batteries to check whether received packets have come from legitimate members.

As we studied before [7], in the case with no prevention method, all terminals consume their batteries at the same rate as transmitting beacon signals frequently. However, in the case of using the proposed secure communication method, even members that receive packets from the attacker directly consume their batteries only a little earlier than the others and the others' batteries do not suffer the attack effect. Battery consumption rate of transmitting packets (BCR_t) and receiving packets (BCR_r) are modeled as follows respectively.

BCR_t: 2.5e-07 J/bit

BCR_r: 1.5e-07 J/bit

From these rates, a terminal which relays packets with no prevention method consumes its battery about 2.67 times faster than a terminal which only receives packets using the proposed secure communication method [8].

Moreover, in the case of the secret key method which we proposed before and discussed in section 2, once the secret key is revealed by the attacker, secrecy in the mobile ad hoc network can no longer be maintained and the resource exhaustion attacker will be able to transmit its illegal packets without any restriction. However, in the case of the mobile ad hoc network using the proposed secure communication method, even if the attacker becomes the invited member or the regular member, once its attack action is detected, it and its inviting member will be expelled at the same time. As a result, the initial members in the mobile ad hoc network will invite only reliable members to the network, and it will be difficult for attackers to be the invited member in the network. Consequently, the secrecy of the mobile ad hoc network will be kept and we can conclude that this secure communication method is superior to the secret key method in securing communication in a mobile ad hoc network.

5. CONCLUSIONS

This paper has studied some security issues in mobile wireless networks and the resource exhaustion attack is the most important security issue among them because it is difficult to prevent it and its effect is too severe.

Then we studied countermeasures which we have already proposed for resource exhaustion attacks briefly and show their disadvantages. Next, we proposed a new secure communication method in mobile ad hoc network using invitation process efficiently for joining the new member.

Finally, we briefly evaluated the proposed secure communication method both in the point of implementation and in the point of security and made it clear that the proposed secure communication method is also useful as a countermeasure against resource exhausting attacks in a mobile ad hoc network.

We will conduct a comparative evaluation of the effectiveness of the proposed secure communication method in our future work.

6. 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.

7. 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 Comput. (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] M. Ishizuka and M. Aida: "Performance evaluation of aggregation routing over power-law placement in wireless sensor networks," IEICE Technical Report, TM2005-45 (2006-1).