# Preventing Resource Exhaustion Attacks in Ad Hoc Networks

Masao Tanabe† and Masaki Aida††
†NTT Information Sharing Platform Laboratories,
NTT Corporation, 3-9-11, Midori-cho, Musashino-shi, Tokyo 180-8585 Japan
††Tokyo Metropolitan University,
6-6, Asahigaoka, Hino-shi, Tokyo 191-0065 Japan
E-mail: †tanabe.masao@lab.ntt.co.jp, ††maida@cc.tmit.ac.jp

## Abstract

*The importance of security has been recognized in ad hoc networks for many years. Consequently many secure routing methods have been proposed in this field. This paper discusses major security attacks in ad hoc networks, and proposes a number of prevention methods for resource exhaustion attacks that have severe negative effects on targeted ad hoc networks.*

Keywords: ad hoc network, security, resource exhaustion attack

## 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 on not only the Internet but also 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 in tackling security problems on the Internet and on ad hoc networks. On the Internet, there are permanent reliable nodes like authentication servers. On the other hand, because all nodes exist temporally in 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 ad hoc networks, end user terminals not only transmit and receive packets but also relay packets that belong to other users. It is, therefore, easier to eavesdrop packets in ad hoc networks than on the Internet. Besides, on the Internet, the electric power of core network equipments are always on, so electricity consumption of these equipments is never an issue. However, in ad hoc 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, ad hoc 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 ad hoc networks. Each terminal in ad hoc networks acts also as a router, so eavesdropping can not be prevented. By passive eavesdropping, important 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 ad hoc 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. By denial of service attacks, target terminal will be unable to act as a relay node, so the routes passing it will become unavailable and the ad hoc network may be divided into sub-networks unable to communicate with each other. Because each terminal handles all received data in ad hoc networks by nature, it is difficult to prevent denial of service attacks.

Signaling attacks are performed by transmitting false routing information in an ad hoc network. Some traffic routes in the ad hoc network might be intentionally altered and become less efficient. These attacks cause packet delay or excess traffic in the ad hoc 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 dropping or falsifying relay packets in the ad hoc network. 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, since all packets in ad hoc

Eighth International Symposium on Autonomous Decentralized Systems (ISADS'07)
0-7695-2804-X/07 $20.00 © 2007 IEEE

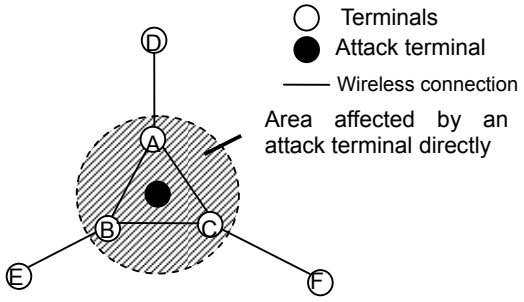


**Figure 1: An example of ad hoc network and an attack terminal**

networks are relayed by some terminals, it is difficult to prevent such attacks.

Resource exhaustion attacks can be easily performed by transmitting numerous 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 ad hoc 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 ad hoc 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 propose a number of countermeasures against resource exhaustion attacks in this paper.

The remainder of this paper is organized as follows. In Section 2, we explain resource exhaustion attacks more specifically and show their effects. In Section 3, we propose some prevention methods against resource exhaustion attacks. In Section 4, we study and evaluate each method quantitatively. Finally, Section 5 concludes this paper.

## 2. Resource exhaustion attacks and their effects

Figure 1 shows an example of an 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 numerous 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. In other words, a resource exhaustion attack affects

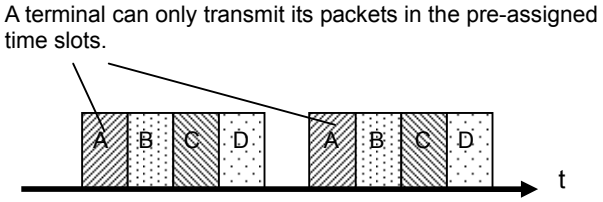


**Figure 2: Time slot method**

to not only terminals which receive packets from the attack terminal directly but also terminals which do not receive them directly. Therefore the impact range of a resource exhaustion attack is broader than that of a DoS (Denial of Service) attack.

## 3. Prevention methods against resource exhaustion attacks

As shown in Section 2, effects of resource exhaustion attacks are severer than that of DoS attacks. Therefore it is very important and necessary to prevent these attacks in ad hoc networks. Hence we propose some prevention methods against resource exhaustion attacks in this Section.

In ad hoc networks, security devices such as IDS (Intrusion Detection Systems) are not always available to detect resource exhaustion attacks. Therefore, each terminal in ad hoc networks must detect these attacks by checking incoming packets from other terminals. For this reason, each prevention method mush allow terminals to easily distinguish attack traffic from legitimate traffic. In this section, we propose three prevention methods against resource exhaustion attacks. The first two methods utilize characteristics of each communication method which allows only legitimate terminals to transmit their packets in order to classify incoming packets. The last method introduces a common secret key in the packet header to distinguish malicious packets from legitimate packets.

### 3.1 Time slot method

The first prevention method uses time slots [7]. In this method, each terminal in an ad hoc network can only transmit its packets in its pre-assigned time slots. All terminals know all time slots for all terminals (Figure 2). In this scheme, because an attack terminal does not belong to the ad hoc network, it does not have its own time slots to transmit its packets. Therefore, legitimate terminals can detect and discard illegitimate packets from the attack terminal when they receive the packets. In this method, although illegitimate packets are not transmitted to the other terminals from the received terminals, terminals which receive packets from the attack terminal must check whether they are transmitted from the legitimate terminals. This consumes some of their batteries. However, the required resources to check the

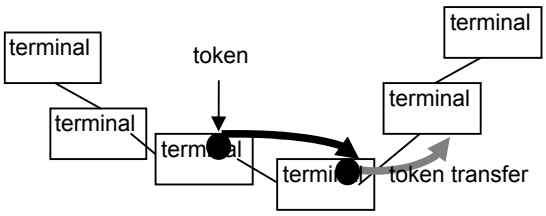


**Figure 3: Token method**

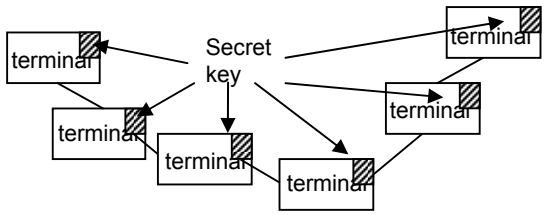


**Figure 4: Secret key method**

packets are less than that of transmitting them to the other terminals. Therefore, using this method, even terminals that receive packets from the attack terminal can persist longer.

### 3.2 Token method

The second prevention method uses tokens [8]. In this scheme, each terminal in an ad hoc network can transmit its packets only when it receives a token from the ad hoc network (Figure 3). An attack terminal cannot receive any token and therefore transmit its packets without one. Legitimate terminals can easily detect and discard illegitimate packets from the attack terminal when they receive the packets. In this method, although illegitimate packets are not transmitted to other terminals from the received terminals, terminals which receive packets from the attack terminal must check whether the packets are transmitted from the legitimate terminals by checking the headers. This consumes some of their batteries. However, the required resources to check the packet headers are less than that of transmitting them to other terminals. Therefore, using this method, even terminals that receive packets from the attack terminal can persist longer.

### 3.3 Secret key method

The third prevention method uses a secret key. In this scheme, each terminal in an ad hoc network transmit its packets with a common secret key which is given when it joins the ad hoc network. (Figure 4). Because an attack terminal not belonging to the ad hoc network cannot obtain the secret key, it transmits packets without one. Legitimate terminals can easily detect and discard illegitimate packets from the attack terminal when they receive the packets. Using this method, although illegitimate packets are not transmitted to other terminals from the received terminals, terminals which receive packets from the attack terminal must check whether the packets are transmitted from the legitimate terminals by checking the headers. This consumes some of their batteries. However, the required resources to check the packet headers are less than that of transmitting them to other terminals. Therefore, using this method, even terminals that receive packets from the attack terminal can persist longer.

## 4. Comparison of the proposed methods

In this section, we compare three prevention methods proposed in the previous sections. First, we discuss the advantages and disadvantages of an each method.

### 4.1 Time slot method

One advantage of the time slot method is that illegitimate packets from the attack terminal are not transmitted to the other terminals from the terminals which receive them directly. Another advantage is that the required resources to check the packets are less than that of transmitting them to the other terminals.

On the other hand, disadvantages of this method are that time slots must be pre-assigned in the ad hoc network and each terminal which belongs to the ad hoc network must remember not only the time slots for it but also time slots for the other terminals and must transmit its packets only in its pre-assigned time slots. This method also requires all terminals to synchronize their clocks, which is difficult to achieve. Moreover, terminals which receive packets from the attack terminal consume their batteries faster than other terminals which do not receive these packets.

### 4.2 Token method

One advantage of the token method is that illegitimate packets from the attack terminal are not transmitted to the other terminals from the terminals which receive them directly. Another advantage is that the required resources to check the packet headers are less than that of transmitting them to the other terminals.

On the other hand, disadvantages of this method are that the token is necessary in the ad hoc network and each terminal must transmit its packets only when it has the token and it must transfer the token to the next terminal when it finishes transmitting its packets or after the timeout. Besides, handling a token in the wireless ad hoc network is difficult.

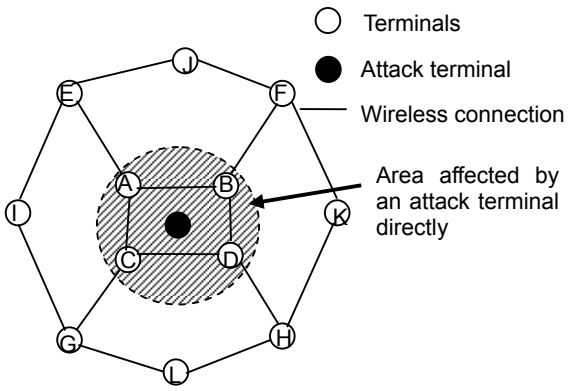


**Figure 5: Network model**

Moreover, terminals which receive packets from the attack terminal consume their batteries faster than other terminals which do not receive these packets.

### 4.3 Secret key method

One advantage of the secret key method is that illegitimate packets from the attack terminal are not transmitted to the other terminals from the terminals which receive them directly. Another advantage is that the required resources to check the packet headers are less than that of transmitting them to the other terminals.

On the other hand, disadvantages of this method are that a secret key is necessary in the ad hoc network and each terminal must receive the secret key when it joins the ad hoc network. It must include the secret key in the header of each packet it transmits, which requires substantial overhead. Moreover, terminals which receive packets from the attack terminal consume their batteries faster than other terminals which do not receive these packets.

From the above discussion, the advantages of all three proposed methods are almost the same, with some common disadvantages and different disadvantages. However, all different disadvantages do not affect battery consumption of the terminals or shorten their lifetime significantly.

Since we intend to discuss how the effects of the resource exhaustion attack could be mitigated by the countermeasures, we compare the three proposed methods with a normal scenario under which no prevention method is deployed. In particular, we focus on the battery consumption of the terminals in the 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 three prevention methods, only terminals which receive packets from the attack terminal directly are affected by the resource exhaustion attack because these terminals discard and do not transmit such packets to the other terminals. As a result, other terminals will not be affected by the attack. Of course, these terminals consume their batteries to check whether received packets have come from legitimate terminals.

From this point, we study the battery consumption of terminals by the resource exhaustion attack in the ad hoc network both in the scenario in which no countermeasure is deployed and in scenarios in which the proposed three prevention methods are used.

Figure 5 shows our network model, which is an ad hoc network with 12 legitimate terminals and one attack terminal in the center of the network. All legitimate terminals are in the same condition as each other.

This model simulates an attack when the attack terminal enters into the center of the ad hoc network. Detailed conditions of our network model are listed below.

- Number of terminals: 12
- Number of terminals affected directly by the attack terminal: 4
- An attack terminal that has an infinite battery capacity.
- Each legitimate terminal has a finite battery capacity.

In an ad hoc network that is vulnerable to resource exhaustion attacks, terminals are classified into two groups: ones that are affected by attack terminals directly and ones that are not. A network model that consists of both groups of terminals would be generalized to a considerable extent.

It is known that short interval transmission of beacon signals shorten battery life of the terminal in an ad hoc network [9]. As we explained before, in the scenario with no prevention method, when the attack terminal starts to transmit illegitimate packets to the legitimate terminals in the ad hoc network, terminals which receive these packets starts to transmit these packets to the other terminals and consume their batteries and halt at last. It equivalent to transmitting beacon signals frequently. In the case without any prevention method, this situation occurs in all terminals in the ad hoc network. But when using some prevention method, terminals which receive these packets directly from the attack terminal may shorten their battery life by handling these packets and halt earlier than in the normal condition but other terminals which do not receive these packets directly do not suffer the attack effect directly. Of course, after former terminals halt, latter terminals will not communicate with these former terminals and also may not communicate with the other latter terminals.

In our network model, in the case with no prevention method, four terminals (A, B, C, D) which receive packets from the attack terminal directly start to transmit these packets to the other terminals (E, F, G, H) and consume their batteries and halt. By this, other eight terminals will not communicate with these four terminals (A, B, C, D). Then next four terminals (E, F, G, H) start to transmit these packets

to the other terminals (I, J, K, L) and consume their batteries and halt. By this, remaining four terminals will not communicate with not only these four terminals (E, F, G, H) but also themselves. Then, last four terminals (I, J, K, L) start to transmit these packets and consume their batteries and halt.

On the other hand, in the case of using some prevention method, four terminals (A, B, C, D) which receive packets from the attack terminal directly starts to check whether these packets come from the legitimate terminals or not and discard them and do not transmit them to the other terminals. By this, these four terminals (A, B, C, D) may consume their batteries earlier than in the normal situation, but other eight terminals (E, F, G, H, I, J, K, L) will not suffer any effects of this attack terminal even indirectly.

In short, 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 some prevention method, even terminals which receive packets from the attack terminal 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 [10].

$BCR_t$: 2.5e-07 J/bit

$BCR_r$: 1.5e-07 J/bit

From these rates, a terminal which relays packets consumes its battery about 2.67 times faster than a terminal which only receives packets. In our network model, four terminals (A, B, C, D) will halt in both cases consequently, but in the case of using some prevention method, these four terminals survive about 2.67 times longer than in the case without prevention method.

Next, we discuss the differences in the proposed three prevention methods. As we explained before, advantages of these three methods are almost the same. However, there are differences in the disadvantages of implementing these methods in the ad hoc network. In the time slot method, time slots must be pre-assigned in the ad hoc network and each terminal which belongs to the 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, the token is necessary in the ad hoc network. 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 wireless ad hoc network is difficult and missing token will cause serious problems in the network. In the secret key method, the secret key is necessary in the ad hoc network. Each terminal must receive the secret key when it joins the ad hoc network and transmit the secret key in the packet header whenever it transmits packets. However, the key pre-distribution method has already been studied in sensor networks [11], therefore it is not difficult to establish secret key pre-distribution method also in ad hoc networks.

In these three methods, the easiest method to implement in the ad hoc network is the secret key method because only secret key has been delivered to the legitimate terminals before transmitting their packets.

## 5. Conclusions

This paper has presented some security issues in ad hoc 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.

We have proposed three prevention methods against the resource exhaustion attacks: time slot, token and secret key. We have shown how each prevention method prevents the resource exhaustion attacks along with its advantages and disadvantages.

Finally, we briefly discussed the differences in the proposed three prevention methods and made it clear that the secret key method is the easiest method to implement in an ad hoc network.

We will conduct a comparative evaluation of the effectiveness of three prevention methods in our future work.

## 6. 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] IEEE 802.4h-1997: "IEEE Standard for Token Passing Bus Access Method and Physical layer Specifications--Alternative Use of BNC Connectors and Manchester-Encoded Signaling Methods for Single-Channel Bus Physical Layer Entities"

[8] H. Lee, J. Yeo, S. Kim, and S. Lee: "Time slot assignment to minimize delay in ad-hoc networks," IST Mobile Communications Summit 2001 (Sept. 2001).

[9] Toh, C-K.: "AD HOC MOBILE NETWORKS: PROTOCOLS AND SYSTEMS," Prentice Hall, 2002.




0-7695-2804-X/07 $20.00 © 2007 IEEE

[10] 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).

[11] D. Westhoff, J. Girao, M. Acharya: "Concealed Data Aggregation for Reverse Multicast Traffic in Sensor Networks: Encryption, Key Distribution and Routing Adaptation," IEEE Transactions on Mobile Computing, October 2006.