A New Routing Attack in Mobile Ad Hoc Networks

Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong

Department of Computing and Information Technology,
Fudan University, Shanghai, 200433, China

Pyi_edu@yahoo.com.cn, zldai@guanghua.sh.cn, szhang@fudan.edu.cn, ypzhong@fudan.edu.cn

Abstract

Mobile ad hoc networks will often be deployed in environments where the nodes of the networks are unattended and have little or no physical protection against tampering. The nodes of mobile ad hoc networks are thus susceptible to compromise. The networks are particularly vulnerable to denial of service (DOS) attacks launched through compromised nodes or intruders. In this paper, we present a new DOS attack and its defense in ad hoc networks. The new DOS attack, called Ad Hoc Flooding Attack(AHFA), can result in denial of service when used against on-demand routing protocols for mobile ad hoc networks, such as AODV, DSR. The intruder broadcasts mass Route Request packets to exhaust the communication bandwidth and node resource so that the valid communication can not be kept. After analyzed Ad Hoc Flooding Attack, we develop Flooding Attack Prevention (FAP), a generic defense against the Ad Hoc Flooding Attack in mobile ad hoc networks. When the intruder broadcasts exceeding packets of Route Request, the immediate neighbors of the intruder record the rate of Route Request. Once the threshold is exceeded, nodes deny any future request packets from the intruder. The results of our implementation show FAP can prevent the Ad Hoc Flooding attack efficiently**.**

Keyword: mobile ad hoc networks, routing protocol, security, denial of service, Ad Hoc Flooding Attack

I. Introduction

Mobile Ad hoc Network is an autonomous system of mobile nodes connected by wireless links. Each node operates not only as an end-system, but also as a router to forward packets. The nodes are free to move about and organize themselves into a network. Mobile ad hoc networks does not require any fixed infrastructure such as base stations, therefore, it is an attractive networking option for connecting mobile devices quickly and spontaneously, such as military applications, emergent operations, personal electronic device networking, and civilian applications like an ad-hoc meeting or an ad-hoc classroom.

The mobile ad hoc networks have several salient characteristics, such as Dynamic topologies, Bandwidth-constrained, variable capacity links, Energy-constrained operation, Limited physical security [1]. Due to these features, mobile ad hoc networks are particularly vulnerable to denial of service attacks launched through compromised node.

In this paper, we present a new attack, the Ad Hoc Flooding Attack, which results in denial of service when used against all previously on on-demand ad hoc networks routing protocols. In this attack, the attacker either broadcasts a lot of Route Request packets for node ID who is not in networks so as to congest in links. To defend routing protocols against the Ad Hoc Flooding attack,

we develop a generic secure component, called Flooding Attack Prevention (FAP), which can be applied to AODV routing protocol to allow that protocol to resist the rushing attack.
Our main contributions in this paper are the presentation of the Ad Hoc Flooding Attack (AHFD), the development and analysis of our new secure solution that demonstrates that it is possible to secure against the Ad Hoc Flooding Attack, and a general design that uses this component to resist the Ad Hoc Flooding Attack.
In wired network, there is flooding attack, too. It is popularly called SYN flooding attack. It works by an attacker sending many TCP connection requests with spoofed source addresses to a victim's machine. Each request causes the targeted host to instantiate data structures out of a limited pool of resources. Once the target host's resources are exhausted, no more incoming TCP connections can be established, thus denying further legitimate access [2][3][4][5]. The goal of SYN flooding attack is to exhaust the resource of victim host. The Ad Hoc Flooding Attack in this paper is to consume and exhaust the resource of the whole network and it does not attack some node. The SYN flooding attack is launched at transport layer and the Ad Hoc Flooding Attack is launched at network layer.
The rest of the paper is organized as follows. Section 2 provides an overview of related work. Section 3 addresses the model of Ad Hoc Flooding Attack to mobile ad hoc network. Section 4 describes our approach to resist the Ad Hoc Flooding Attack. In section 5, we present the simulation experiments. And section 6 concludes the paper.
This document is a template for papers submitted to International Journal of Information Technology. If your paper is intended to this journal, please observe this format. Do not change the fonts or line spacing to squeeze more text into a limited number of pages.

II. Related work

The papers of mobile ad hoc networks security can be classified in three categories: key management, secure network routing, and intrusion detection. Capkun, Buttyan and Hubaux propose a fully self-organized public key management system that can be used to support security of ad hoc network routing protocols[6]. Zhou and Hass first proposed to use threshold cryptography to securely distribute the Certificate Authority private key over multiple nodes to form a collective CA service[7]. Routing security has been most noted by its absence early in the discussion and research on ad hoc routing protocols. Since then several ad hoc routing protocols that include some security services have been proposed: SRP[8], Ariadne[9], ARAN[10], SEAD[11]. SRP[8] assumes the existence of shared secrets between all pairs of communicating nodes and leverages this for MAC authentication, such that fake route requests are not accepted at the destination and routes set in route replies cannot be modified. In Ariadne[9], end-to-end authentications are got by one-way hash chain and MAC authentication. ARAN[10] relies on public key certificates to retain hop-by-hop authentications. SEAD[11] use elements from a one-way hash chain to provide authentication for both the sequence number and the metric in each entry. Yongguang Zhang developed an Intrusion Detection architecture and evaluated a key mechanism in this architecture, anomaly detection for mobile ad-hoc networks [12]. Yih-Chun Hu presents Rushing Attack[13], which is that an attacker that can forward ROUTE REQUESTs more quickly than legitimate nodes can do so, can increase the probability that routes that include the attacker will be discovered rather than other valid routes. The above secure protocols are not able to prevent the Ad Hoc Flooding Attack in mobile ad hoc network, because the attacker is compromised node who owns legitimate key.

To prevent SYN flooding attack in Internet, a lot of solution approaches have been presented so far. They can be roughly categorized as: firewall and router filtering, operating system improvements, and protocol improvements. Firewalls are already being used to monitor packet traffic, and protect systems from malicious access. As a countermeasure to flooding attacks, Schuba et al. mentions that firewalls can be configured as a relay, or as a semi-transparent gateway [2]. In RFC 2267, Ferguson and Senie described network ingress filtering that can prevent attackers from using forged source addresses to launch a denial of service (DOS) attack [14]. Solaris/SUN has considered implementing

several OS revisions to handle DOS attacks. An information bulletin announced that SUN considered using priority queues to grant requests originating from addresses that have given successful handshakes in the past [15]. Aura and Nikander described weaknesses of state protocols, and methods to change state protocols into stateless ones. State protocols have an upper limit on number of simultaneous connections, because there is a limited space available for storing connection state information. When this limited space is exhausted, new connections are refused. To remedy this, the state information is stored on the client rather than on the server [16]. The above solutions are designed to prevent SYN flooding attack in wire network. They can not hold back Flood Attack in mobile ad hoc network, because the mechanism of the Flood Attack is different from the SYN flooding attack.

III. The model of Ad Hoc Flooding Attack

We introduce here a new attack, which we call the Ad Hoc Flooding Attack, which acts as an effective denial-of-service attack against all currently proposed on-demand ad hoc network routing protocols, including protocols that were designed to be secure. In particular, existing on-demand routing protocols, such as DSR [17], AODV [18], LAR [19], and some secure routing protocols, such as SRP [8], Ariadne [9], ARAN [10], SAODV [20][21], can not be immune from the Ad Hoc Flooding Attack. We now describe the Ad Hoc Flooding Attack in terms of its effect on the operation of AODV [18]. Other protocols such as DSR [17], Ariadne [9], SAODV [20], and ARAN [10] are vulnerable in the same way.

A. Overview of AODV routing protocol

In AODV, path discovery is entirely on-demand. When a source node needs to send packets to a destination to which it has no available route, it broadcasts a RREQ (Route Request) packet to its neighbors. Each node maintains a monotonically increasing sequence number to ensure loop free routing and supersede stale route cache. The source node includes the known sequence number of the destination in the RREQ packet. The intermediate node receiving a RREQ packet checks its route table entries. If it possesses a route toward the destination with greater sequence number than that in the RREQ packet, it unicasts a RREP (Route Reply) packet back to its neighbor from which it received the RREQ packet. Otherwise, it sets up the reverse path and then rebroadcasts the RREQ packet. Duplicate RREQ packets received by one node are silently dropped. This way, the RREQ packet is flooded in a controlled manner in the network, and it will eventually arrive at the destination itself or a node that can supply a fresh route to the destination, which will generate the RREP packet. As the RREP packet is propagated along the reverse path to the source, the intermediate nodes update their routing tables using distributed Bellman-Ford algorithm with additional constraint on the sequence number, and set up the forward path.
AODV also includes the path maintenance mechanism to handle the dynamics in the network topology. Link failures can be detected by either periodic beacons or link layer acknowledgments, such as those provided by 802.11 MAC protocol. Once a link is broken, an unsolicited RRER packet with a fresh sequence number and infinite hop count is propagated to all active source nodes that are currently using this link. When the source node receives the notification of a broken link, it may restart the path discovery process if it still needs a route to the destination.

B. Ad Hoc Flooding Attack

Flooding RREQ packets in the whole network will consume a lot of resource of network. To reduce congestion in a network, the AODV protocol adopts some methods. A node can not originate more than RREQ_RATELIMIT RREQ messages per second. After broadcasting a RREQ, a node waits for a RREP. If a route is not received within round-trip milliseconds, the node may try again to

discover a route by broadcasting another RREQ, up to a maximum of retry times at the maximum TTL value. Repeated attempts by a source node at route discovery for a single destination must utilize a binary exponential backoff. The first time a source node broadcasts a RREQ, it waits round-trip time for the reception of a RREP. If a RREP is not received within that time, the source node sends a new RREQ. When calculating the time to wait for the RREP after sending the second RREQ, the source node MUST use a binary exponential backoff. Hence, the waiting time for the RREP corresponding to the second RREQ is 2 * round-trip time. The RREQ packets are broadcast in an incrementing ring to reduce the overhead caused by flooding the whole network. The packets are flooded in a small area (a ring) first defined by a starting TTL (time-to-live) in the IP headers. After RING TRAVERSAL TIME, if no RREP has been received, the flooded area is enlarged by increasing the TTL by a fixed value. The procedure is repeated until an RREP is received by the originator of the RREQ, i.e., the route has been found.

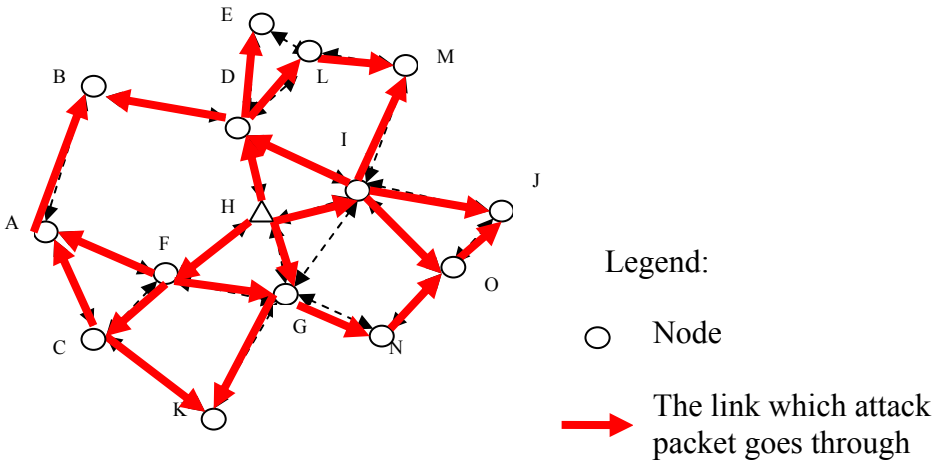

Fig.1 The Ad Hoc Flooding Attack

In the Ad Hoc Flooding Attack, the attack node violates the above rules to exhaust the network resource. Firstly, the attacker selects many IP addresses which are not in the networks if he knows the scope of IP address in the networks. Because no node can answer RREP packets for these RREQ, the reverse route in the route table of node will be conserved for longer. The attacker can select random IP addresses if he can not know scope of IP address. Secondly, the attacker successively originates mass RREQ messages for these void IP addresses. The attacker tries to send excessive RREQ without considering RREQ_RATELIMIT within per second. The attacker will resend the RREQ packets without waiting for the RREP or round-trip time, if he uses out these IP addresses. The TTL of RREQ is set up to a maximum without using expanding ring search method. In the Flooding Attacks, the whole network will be full of RREQ packets which the attacker sends. The communication bandwidth is exhausted by the flooded RREQ packets and the resource of nodes is exhausted at the same time. For example, the storage of route table is limited. If mass RREQ packets are coming to the node in a little time, the storage of route table in the node will exhaust so that the node can not receive new RREQ packet. As a result, the legitimate nodes can not set up paths to send data. Figure 1 shows that an example of RREQ Flooding Attack. Node H is attacker and it floods mass RREQ packets all over the networks so that the other nodes can not build paths with each other.

C. *Comparison between Ad Hoc Flooding Attack and SYN Flooding Attack*

The SYN flooding attacks exploit the three-way handshake mechanism in TCP/IP protocol and its limitation in maintaining half-open connections. When a server receives a SYN request, it returns a SYN/ACK packet to the client. Until the SYN/ACK packet is acknowledged by the client, the connection remains in half-open state for a period of up to the TCP connection timeout, which is typically set to 75 seconds. The server has built in its system memory a backlog queue to maintain all half-open connections. Since this backlog queue is of finite size, once the backlog queue limit is reached, all connection requests will be dropped. If a SYN request is spoofed, the victim server will never receive the final ACK packet to complete the three-way handshake. Flooding spoofed SYN requests can easily exhaust the victim backlog queue of server, causing all the incoming SYN requests to be dropped.

Table 1. contrast between SYN Flooding Attack and Ad Hoc Flooding Attack

Name	SYN Flooding Attack	Ad Hoc Flooding Attack
Attack method	TCP connection requests with spoofed source addresses	Flooding mass RREQ packets
Victim	host	Mobile ad hoc networks
Protocol	TCP/IP	On-demand routing protocol
Protocol layer	Transport layer	Network layer
goal	Denial of service in host	Denial of service in the whole networks

We compare between SYN Flooding Attack and Ad Hoc Flooding Attack in table1. The common goal of two attacks is denial of service. But they are different in attack method, victim, protocol and so on. Therefore, the Ad Hoc Flooding Attack is a new attack model in mobile ad hoc networks.

IV.The approaches to prevent the Ad Hoc Flooding Attack

In this section, we describe a set of generic mechanisms that together defend against the Ad Hoc Flooding Attack: *Neighbor suppression.* The way efficiently prevents the Ad Hoc Flood Attack.
The method of neighbor suppression is used to prevent RREQ Flooding Attack. Mobile ad hoc networks are multi-hop wireless networks, and the node sends and receives packets through its neighbor nodes. If all neighbor nodes around the node refuse to forward its packets, the node can not communicate with the other nodes in mobile ad hoc networks. The node has been isolated from the network in practice even if it is still in the networks in location. Figure 2 shows that a topology of mobile ad hoc network. The node H communicates with the other node through node D, F, G and I. If neighbor node D, F, G and I refuse to receive packets from node H, node H can not send any packet to the other nodes.

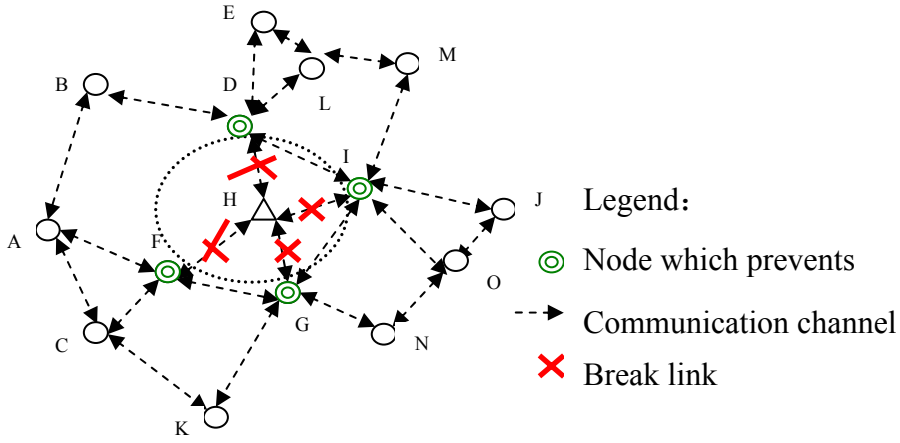

Fig.2 neighbor nodes isolate attacker

We design the method of neighbor suppression according to the above feature of mobile ad hoc network. The main idea of neighbor suppression is that each neighbor calculates the rate of RREQ originated by intruder. If the rate exceeds some threshold, all neighbors will not receive and forward packets from intruder. We define two tables in every node: Rate_RREQ and Blacklist. The table of Rate_RREQ records the rate of RREQ which every neighbor node originates, and does not record times of forwarded RREQ. The Rate_RREQ has two colums: Node_ID and RREQ_time. Node_ID includes all neighbor node ID. RREQ_time records times which neighbor node originates RREQ. The process is Algorithm 1.

```
Algorithm 1. calculate time of RREQ
Step1. received a RREQ;
Step2. if the RREQ is forwarded then quit;
Step3. look up node ID who send the RREQ in the table of Rate_RREQ;
Step4. find node ID and RREQ_time:=RREQ_time+1;
```

To calculate the rate of RREQ and find the intruder, the Algorithm 2 is run one time every second.

```
Algorithm 2. find the intrusion
    For every item of Rate_RREQ do
        If RREQ_time > threshold then put Node_ID into Blacklist and RREQ_time:=0;
        Else RREQ_time:=0;
```

Because RREQ_time sets up 0 every second, it can stand for rate which every neighbor node originates. If the time exceeds the threshold, we may make a judge that it is intruder.
When node receives a packet, node firstly look up source ID of packet. If source ID is in Blacklist, node directly discards the packet. If source ID is not in Blacklist, node disposes the packet by normal process.
The threshold is the maximum of originating RREQ in a period time, such as 1 second. If the frequency of originating RREQ of the attacker exceeds the threshold, the node will not receive the RREQ from the attacker any more. To clarify, we take node H and its neighbor node D, I, F, G for example in figure 1. If the frequency which node H originates RREQ exceeds the threshold, node F will deny the RREQ packets from node H. similarly, node D, I, G will deny the RREQ packets form node H. As a result, the Ad Hoc Flooding Attack from node H is prevented by its neighbor nodes.

V. Evaluation

A. Experimental setup

To study the feasibility of our Flooding Attack Prevention (FAP), we have implemented Ad Hoc Flooding attack and Flooding Attack Prevention (FAP) in a network simulator and conducted a series of experiments to evaluate its effectiveness. We used the wireless networks simulation software, from Network Simulator ns-2 [22]. It includes simulation for wireless ad-hoc network infrastructure, popular wireless ad-hoc routing protocols (DSR, DSDV, AODV and others), and mobility scenario and traffic pattern generation.

Our simulations are based on a 1000 by 1000 meter flat space, scattered with 50 wireless nodes. The radio propagation range for each node is 250 meters and channel capacity is 2 Mb/s. Each simulation is executed for 900 seconds of simulation time.

A traffic generator was developed to simulate constant bit rate sources. The size of data payload is 512 bytes. Five data sessions with randomly selected sources and destinations are simulated. Each source transmits data packets at the rate of 4 packets/s. The number of data sessions was held constant to limit the number of variables in the experiment, and because of the time required to run the large simulations with more data sessions.

The random waypoint model is utilized as the mobility model. In this model, a node selects a random destination within the terrain range and moves towards that destination at a speed between the pre-defined minimum and maximum speed. Once the node arrives at the destination, it stays at its current position for a pause time. After being stationary for the pause time, it randomly selects another destination and speed and then resumes movement. The minimum speed for the simulations is 0 m/s while the maximum speed is 20 m/s. The selected pause time is 0 seconds.

The MAC layer used for the simulations is IEEE 802.11, which is included in the ns-2. The transport protocol used for our simulations is User Datagram Protocol (UDP). The traffic files are generated such that the source and destination pairs are randomly spread over the entire network. The scenario files determine the mobility of the nodes. Duration of the simulations is 900 seconds. There is one misbehaving node in the scenario and it moves according to the same mobility model as the other nodes.

We use the following metrics to evaluate the performance of our Flooding Attack Prevention (FAP). Packet delivery rate: the ratio between the number of packets originated by the application layer CBR (continuous bit rate) sources and the number of packets received by the final destination. Packet delivery ratio is important as it describes the loss rate that will be seen by the transport protocols, which in turn affect the maximum throughout that the network can support. The metric characterizes both the completeness and correctness of the routing protocol.

B. Simulation results of Ad Hoc Flooding Attack

The system performance has been observed in five scenarios. The first scenario is that there are not attacking nodes in mobile ad hoc networks. In order to carefully observe the impact on performance of mobile ad hoc networks, we assume that rates of attacking packets are respectively 10packets/s, 20packets/s, 30packets/s, 40packets/s. In other words, the intruder respectively floods 10, 20, 30, 40 packets every second. We calculate packet delivery rate every 100s. At 100s of simulation experiment, we totalize packet delivery rate from 0 to 100s. At 200s of simulation experiment, we totalize packet delivery rate from 100 to 200s. The rest may be deduced by analogy. There is not attacking packets from 0 to 300s in all scenarios. The intruder starts to attack at 300s. The simulation results are as follows.

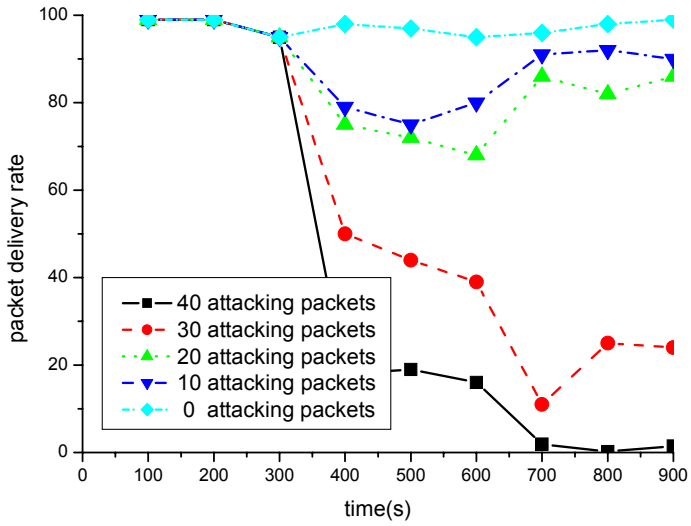

Fig.3 Packet delivery ratio under five scenarios

In Fig.3, we observe that packet delivery ratio go down when intruder floods attacking packets at 300s. The average packet delivery ratio is 97% without attack and most packets get to the destination nodes. However, the average packet delivery ratio decline from 97% to 9.4% when intruder floods 40 packets every second. In other words, most packets can not get to the goal and those packets are discarded by nodes for network congestion. It implies that Ad Hoc Flooding Attack can result in denial of service of whole network. Interestingly, the network seems to have some recoverability. When the rate of attacking packets is less than 20 packets/s, the performance becomes better after a period. But when the rate of attacking packets is more than 30 packets/s, the network can not bear the attack any more and the performance goes down quickly.

C. Simulation results of Flooding Attack Prevention

The system performance has been observed in six scenarios. Similarly, we calculate packet delivery rate every 100s. The first scenario is that there are not attacking nodes in mobile ad hoc networks. Fig.4 shows the packet delivery ratio of network is average 96%.

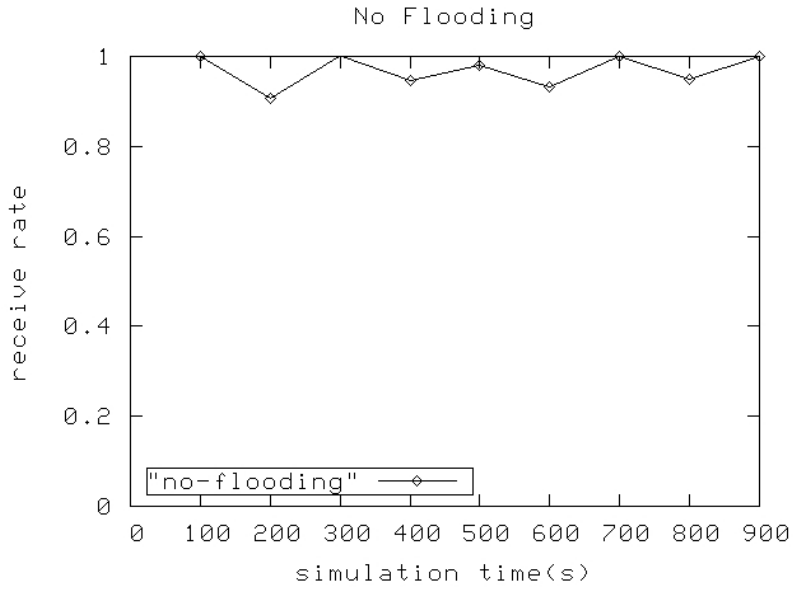

Fig.4 The performance under no attacking packets

Fig.5 and Fig.6 shows the performance under 10 and 20 attacking packets every second and Flooding Attack Prevention. There is not attacking packets between 0 and 300s. The intruder launches Ad Hoc Flooding Attack from 300s to 900s. At 600s of simulation, FAP in nodes takes effect. We can observe that the performance has got better after 600s. But the improvement is not obvious since the damage of attack is little. In AODV protocol [18], a node should not originate more than 10 RREQ messages per second. Therefore, the threshold of FAP set up 15.

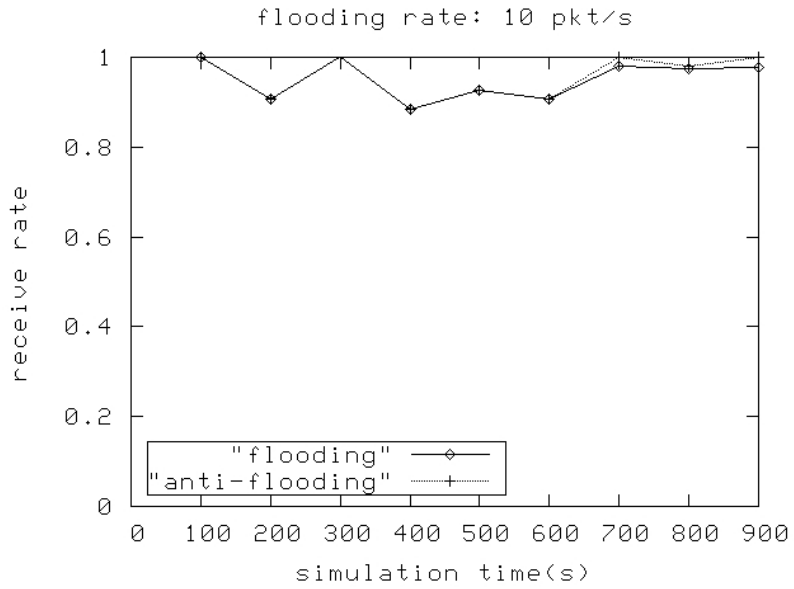

Fig.5 The performance under 10 attacking packets every second and Flooding Attack Prevention

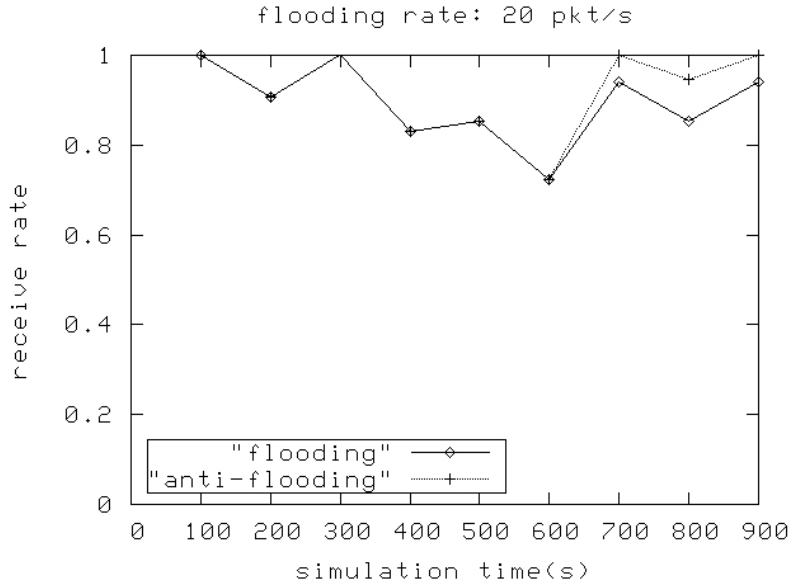

Fig.6 The performance under 20 attacking packets every second and Flooding Attack Prevention

Fig.7 shows the performance under 30 attacking packets every second and Flooding Attack Prevention. When the AODV protocol is integrated with FAP, the packet delivery ratio increases from 50% to 80%.

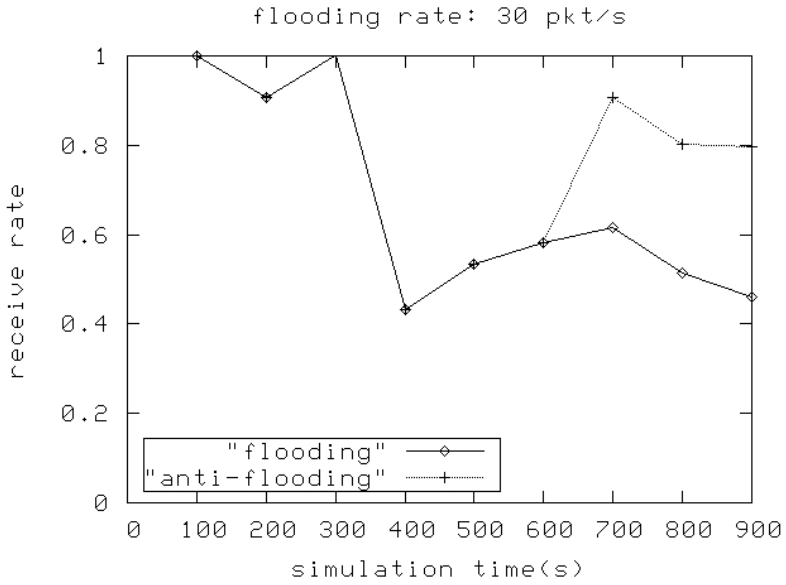

Fig.7 The performance under 30 attacking packets every second and Flooding Attack Prevention

Fig.8 and Fig.9 shows the performance under 40 and 50 attacking packets every second and Flooding Attack Prevention. With more attacking packets every second, the performance of network falls quickly. The packet delivery rate gets to 1.2% in Fig.9. When FAP takes effect at 600s, the performance becomes better and packet delivery rate keep up about 80%. It implies that the Flooding Attack Prevention efficiently resists the Ad Hoc Flooding Attack by identifying the attackers and isolating them from the networks.

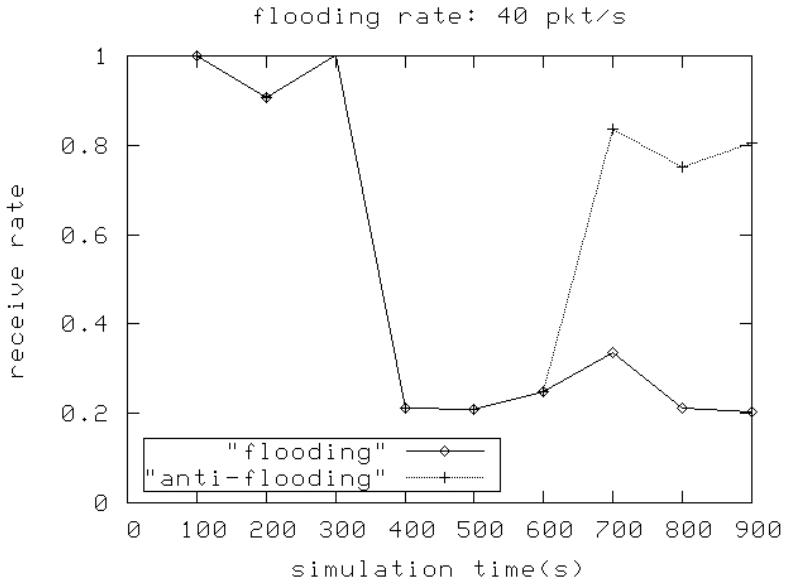

Fig.8 The performance under 40 attacking packets every second and Flooding Attack Prevention

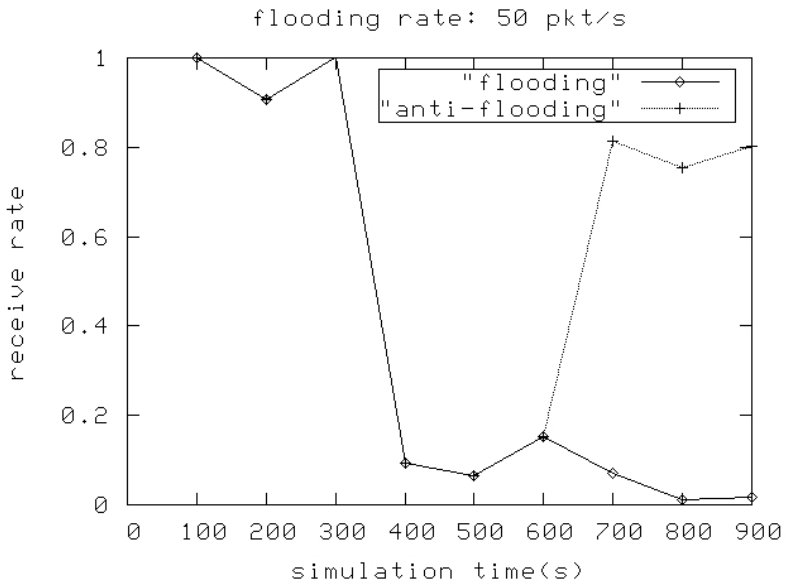

Fig.9 The performance under 50 attacking packets every second and Flooding Attack Prevention.

VI. Conclusion

In this paper, we have described the Flooding Attack, a novel and powerful attack against on-demand ad hoc routing protocols. This attack allows attacker to mount a denial of service attack against all on-demand routing protocols for mobile ad hoc networks, even secure on-demand routing protocols. We design the Flooding Attack Prevention (FAP) to resisting this attack. The results of our implementation show the Flooding Attack Prevention efficiently defense the Ad Hoc Flooding Attack with little overload.

References

[1] S. Corson， J. Macker， Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations，RFC 2501，January 1999

[2] C. Schuba, I. Krsul, M. Kuhn, E. Spafford, A. Sundaram, D. Zamboni, Analysis of a Denial of Service Attack on TCP, Proceedings of the 1997 IEEE Symposium on Security and Privacy.

[3] Haining Wang, Danlu Zhang, and Kang G. Shin, Detecting SYN Flooding Attacks, IEEE INFOCOM'2002, New York City, 2002

[4] Karthik Lakshminarayanan, Daniel Adkins, Adrian Perrig, Ion Stoica, Taming IP packet flooding attacks, Computer Communication Review 34(1): 45-50 (2004)

[5] Abraham Yaar, Adrian Perrig, Dawn Xiaodong Song, SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks, IEEE Symposium on Security and Privacy 2004

[6] Srdjan Capkun, Levente Nuttyan, Jean-Pierre Hubaux, Self-organized public-key Management for mobile ad hoc networks, IEEE Transactions on mobile computing, Vol.2, No.1, January-March, 2003

[7] Lidong Zhou, Zygmunt J. Haas， Securing ad hoc networks， IEEE Networks Special Issue on Network Security，November/December, 1999

[8] P.Papadimitratos, Z.Haas, Secure routing for mobile ad hoc networks, in Proceedings of the SCS communication Networks and Distributed Systems Modeling and Simulation Conference, San Antonio, TX, January 27-31,2002

[9] Yih-Chun Hu, Adrian Perrig, David B. Johnson. Ariadne: A secure On-Demand Routing Protocol for Ad hoc Networks， in Proceedings of the MobiCom 2002, September 23-28, 2002, Atlanta, Georgia, USA

[10] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer. A Secure Routing Protocol for Ad Hoc Networks, In Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP)， November 2002

[11] Yih-Chun Hu, David B. Johnson, and Adrian Perrig， SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks，in Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA 2002), pp. 3-13, IEEE, Calicoon, NY, June 2002

[12] Yongguang Zhang & Wenke Lee, Intrusion Detection Techniques for Mobile Wireless Networks, Mobile Networks and Applications, 2003

[13] Yih-Chun Hu, Adrian Perrig, and David Johnson, Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols, ACM Workshop on Wireless Security (WiSe 2003) September 19, 2003 Westin Horton Plaza Hotel, San Diego, California, U.S.A.

[14] P. Ferguson, D. Senie, Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2267, January 1998

[15] CIAC, H-02: SUN's TCP SYN Flooding Solutions, Information Bulletin, October 1996

[16] T. Aura, P. Nikander, Stateless Connections, Proc. of 1st International Conference of Information and Communication Security (ICICS97), Lecture Notes in Computer Science 1334, November 1997, P. 87-97, Springer 1997

[17] David B. Johnson, David A. Maltz, Yih-Chun Hu, The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), Internet-Draft, draft-ietf-manet-dsr-09.txt, 15 April 2003, http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-09.txt

[18] Charles E. Perkins , Elizabeth M. Belding-Royer , and Samir R. Das, Ad hoc On-Demand Distance Vector (AODV) Routing ， RFC 3561 ， July 2003 ， http://www.ietf.org/rfc/rfc3561.txt

[19] Young-Bae Ko and Nitin Vaidya, Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. In Proceedings of the Fourth International Conference on Mobile Computing and Networking (MobiCom'98), pages 66－75, October 1998.

[20] Manel Guerrero Zapata, Secure Ad hoc On-Demand Distance Vector Routing. ACM Mobile Computing and Communications Review (MC2R), Vol 6. No. 3, pp. 106-107, July 2002

[21] Manel Guerrero Zapata and N. Asokan， Securing Ad-Hoc Routing Protocols， In Proceedings of the 2002 ACM Workshop on Wireless Security (WiSe 2002), pages 1-10. September 2002

[22] http://www.isi.edu/nsnam/ns/index.html

Ping Yi was born in 1969. He received the BSc degree in department of computer science and engineering from the PLA University of Science and Technology, Nanjing, China, in 1991. He received the MSc degree in computer science from the Tongji University, Shanghai, China, in 2003. He is currently a Ph.D. candidate at the department of Computing and Information Technology, Fudan University, China. His research interests include mobile computing and ad hoc networks security.