私立東海大學資訊工程學系研究所

碩士論文

指導教授：林祝興 博士

Dr. Chu-Hsing Lin

移動式隨意網路洪氾攻擊預防之研究

Flooding Attack Prevention in Mobile Ad-hoc Networks

研究生：胡哲維

(Che-Wei Hu)

中 華 民 國 一 〇 〇 年 六 月

東海大學碩士學位論文考試審定書

東海大學資訊工程學系 研究所

研究生 胡 哲 維 所提之論文

移動式隨意網路洪氾攻擊預防之研究

經本委員會審查，符合碩士學位論文標準。

學位考試委員會
召 集 人 詹進科 簽章

委 員 詹進科

[illegible]

楊中皇

指 導 教 授 簽章

中華民國 100 年 6 月 28 日

Abstract

Mobile ad hoc networks are usually deployed in many environments, such as the environment is not easy to build by wired or fixed nodes. The nodes in the network are unattended and easy be attacked because of congenital weak physical protection. Mobile ad hoc networks are vulnerable to the denial-of-service (DOS) attacks. Flooding DOS attacks are new and powerful attacks against on-demand Ad Hoc routing protocols. In 2005, the single scheme proposed to resist such attack was the Flooding Attack Prevention. In 2006, another scheme to resist this kind of attacks was proposed by using Avoid Mistaken Transmission Table. In this thesis, we present a new and more efficient solution to inhibit flooding attack in Mobile ad hoc networks. In our scheme, legal nodes can use Priority and Trust Value and Neighbor Nodes List Table to distinguish attack nodes and refuse to forward packets for them, and hence the flooding attacks can be defended. According to the results of NS2 network experiment, we show that our scheme can inhibit the flood hit with lower costs and more efficient. Our scheme can only use a few storage and defense attacker faster.

Keywords: Flooding attack; FAP; AMTT; Trust and Priority Value; RREQ threshold; DATA threshold;

摘要

移動式 Ad hoc 網絡通常部署在許多有線或固定節點不容易建立的環境中。例如:節點在網絡中無人看守，所以容易受到攻擊，因為先天的節點非常不易保護,移動式 Ad hoc 網絡非常容易受到 DOS 的攻擊,DOS 的攻擊是針對 AODV 協定的攻擊方式，在 2005 年，學者提出了一種抵制這種攻擊的法稱為 Flooding Attack Prevention (FAP)。 2006 年，另一位學者提出了一種能夠預防洪氾攻擊的一種傳輸表，名為 Avoid Mistaken Transmission Table (AMTT)。

在本論文中,我們提出了一個新的和更有效的解決方案,用來在 Mobile ad hoc networks 中抑制 Flooding Attack。在我們提出的方法裡，合法的節點可以使用優先權表以及真值表以及利用鄰居節點列表來區分哪一個是攻擊節點，並拒絕為他們轉發封包，這種方式可以有效的防禦。根據洪氾攻擊的實驗，我們證明了我們的方法能夠抑制洪氾攻擊,並且可以降低成本,而且更有效率。

關鍵詞: 洪氾攻擊; FAP ; AMTT ; 真值表 ; 優先權表 ; RREQ threshold; DATA threshold;

致謝

在碩士班的兩年生涯中，首先要感謝父親以及母親的支持與鼓勵，讓我可以在這兩年中無後顧之憂的專心在學業與研究上。同時，也要感謝三位指導教授林祝興老師與劉榮春老師以及江輔政老師在學生這段求學過程中的指導，在這兩年的研究過程中，經過多次的報告、討論與修正，三位老師指導我研究方向不遺餘力，沒有你們，學生的碩士論文無法如此順利的完成。在此也要感謝參與學生碩士班口試的委員：詹進科教授、楊中皇教授、陳雍宗教授。由於教授們的指正與建議，使得學生這篇碩士畢業論文更加充實完整。

此外也感謝東海大學資訊安全實驗室的夥伴們，因為有你們，讓我的碩士生活更加的充實與多彩多姿。感謝鎮宇學長、佳穎學長、煒程學長、浩天學長、慶儒學長、蓉蓉學姊，帶我參與計畫的撰寫與執行，並對我論文的研究提出寶貴的意見。感謝逸竹、冠翰、信雁以及諸位同學相互的鼓勵與支持，讓我們能一起進入實驗室，也一起參加口試順利畢業。因為有你們，實驗室總保持著歡樂的氣氛。感謝女友洵玫、詩蓓學妹、泓彥學弟、棠濰學弟及信斌學弟，在臨近畢業前夕的幫忙，讓我能專注準備畢業論文及口試。

最後再次感謝所有的父母、師長及親友們，感謝你們的支持、鼓勵與包容，在此哲維致上最高的感謝。謝謝大家。

胡哲維 謹上 2011/7

Contents

Figure List

Table List

Chapter 1
Introduction

A mobile Ad Hoc network (MANET) is a new kind of mobile multi-hop wireless networks. It does not require any fixed infrastructure like the base station. It maintains the network connection and data transmission by the cooperation and self-organization among all the mobile nodes in the network. Several mature and widely-used routing protocols include Optimized Link State Routing protocol (OLSR)[19][20], Dynamic source routing (DSR)[21], Topology Broadcast based on Reverse-Path Forwarding (TBRPF)[2], Ad-hoc on-demand distance vector (AODV) [3] and so on.

Meanwhile, to gain more efficient defense effects against flooding attacks , many secure routing protocols for Ad Hoc network have been proposed. In wired-networks, Denial of Service attacks (DoS) or Distributed Denial of Service (DDoS) attacks are a kind of flooding attack that if not found early enough, they will cause damages on hosts seriously. Along with the extensive use of the wireless network, flooding attack is an ubiquitous and typical attack that results in denial of services when used against all previous on-demand routing protocols for Ad-hoc networks.

Ping Yi et al first introduced a typical attacking model which is composed of RREQ flooding attack and DATA flooding attack. To mitigate these two attack patterns, they developed a Flooding Attack Prevention Scheme (FAP)[10] . Then another scheme was proposed by Shaomei Li et al. is called the Avoiding Mistaken Transmission Table (AMTT)[11].

In this thesis, we present Priority and Trust Value (PTV) scheme to mend the weakness of FAP and AMTT simultaneously. In our scheme, each node sets a priority and trust value and neighbor nodes list table for cooperating to record the status of its neighbor nodes and find out which broadcasts mass Route Request (RREQ). And so nodes can effectively distinguish attacks and refuse to forward packets for them. By this way, flooding attacks are defended.

Chapter 2
Background

2.1 Overview of ADOV Protocol

AODV[3] routing algorithm is based on DSDV algorithm, and designed for mobile Ad-hoc network routing protocols. AODV algorithm is mainly to reduce the broadcasting needs in the quantity. In addition, it has unicast and multicast routing capabilities of them.

The Ad Hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an Ad hoc network [11][14][15][16][17]. Path discovery is entirely on-demand in AODV. It allows mobile nodes to obtain routes quickly for new destinations. And it does not require maintaining routes information. AODV is a reactive and stateless protocol which establishes routes only as desired by a source node using Route Request (RREQ) and Route Reply (RREP) messages.

When a source node needs to send packets to a destination node to which it has no available route, it will broadcast RREQ packets and wait RREP packets within one round-trip time, as shown in Fig.1.

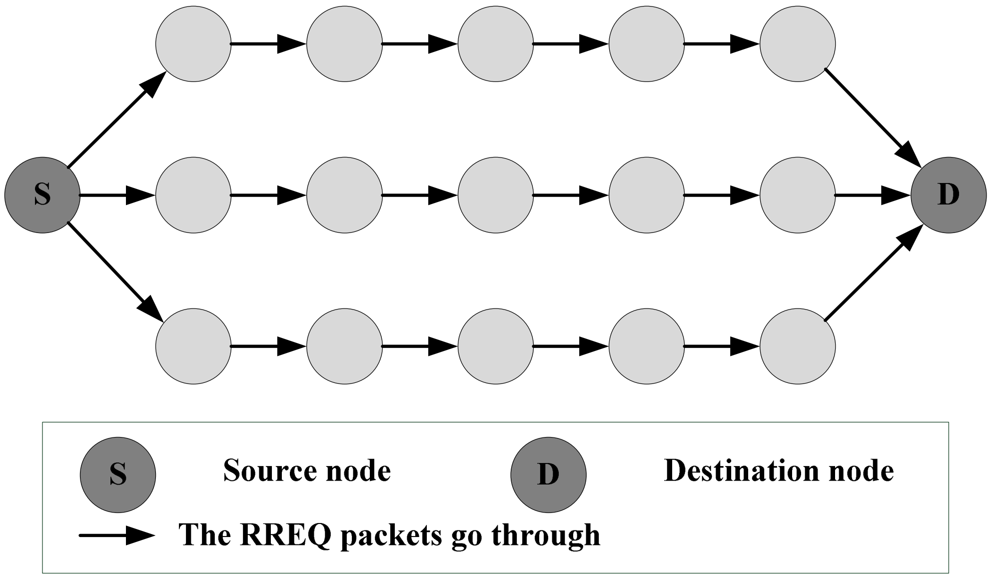


Fig. 1: The forwarding route of RREQ.

If the node does not receive the RREP packet, it will try again to discovery route by broadcasting another new RREQ packet. If over the maximum of TTL, the node will stop route discovery.

Each node maintains an increasing sequence number to ensure loop free routing and supersede the stale route cache. The source node includes the known sequence number of the destination in the RREQ packet. When an intermediate node receives a RREQ packet, it will check 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 Route Reply (RREP) packet back to its neighbor from which it has 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 new route to the destination, which will generate the RREP packet. Fig.2 and Fig.3 show the RREP packets go through and the routing path, respectively.

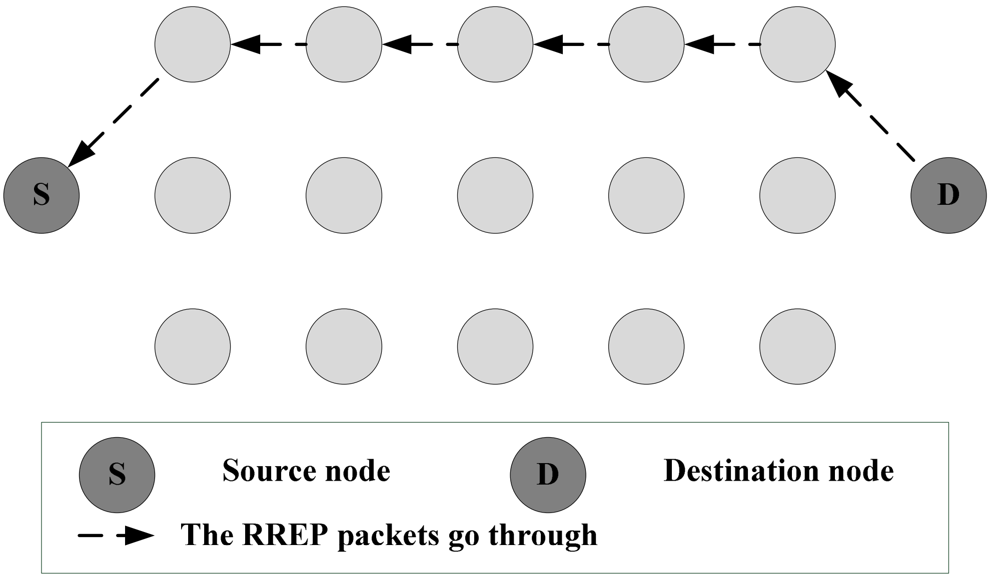


Fig. 2: The RREP packets go through.

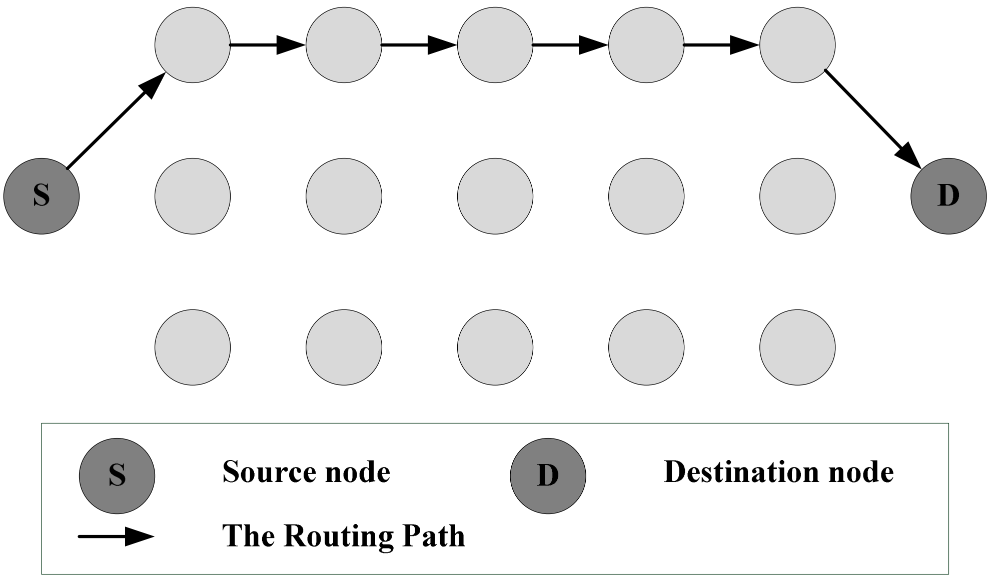


Fig. 3: The Routing Path

2.2 Flooding Attack in Mobile Ad hoc Network

The major modes of flooding attack are the RREQ flooding attack and the DATA flooding attack. In RREQ flooding attacks, the attacker selects many IP addresses which don't exist in the networks as destination addresses. Then it successively originates massive RREQ messages with max TTL value for these void IP addresses. Then the whole network will be full of RREQ packets sent by the attacker. Since these destination addresses are invalid, no node can answer RREP packets for these RREQs, the reverse routes in the route table of midway nodes will be occupied for longer time and be exhausted soon.

In data flooding attacks, the attacker first sets up paths to all nodes in the networks, after that, it sends large quantities of useless data packets to all nodes along these paths. The excessive data packets in the network clog the network and deplete the available network bandwidth for communication among nodes in the network.

The resources of nodes in Ad-hoc networks are very limited, and both attacks are able to exhaust the available network bandwidth for communication such that the other nodes can not communicate with each other due to congestion in the network. Especially when attacking node employs RREQ flooding attack and data flooding attack simultaneously, the whole network performance would be deteriorated dramatically.

2.3 Overview of FAP and AMTT Scheme

2.3.1 FAP (Flooding Attack Prevention)

In 2005, Flooding Attack Prevention (FAP) proposed by Yi, et al. [10] is a generic defensive scheme against the Ad Hoc Flooding Attack in mobile Ad-hoc networks. Two typical attacking crime patterns are the RREQ flooding attack and the DATA flooding attack.

To counteract the RREQ flooding attack, the neighbor suppression scheme is adopted. It is used to prevent the RREQ flooding attack. And Path Cutoff is used to terminate the DATA flooding attack. Neighbor suppression let node sets up the processing priority and threshold for its neighbor node. The priority of node is in inverse proportion to its frequency of originating RREQ.

The threshold is the maximum numbers of originating RREQ in a period of 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. And the RREQ flooding attack will be defended by neighbor nodes of attacker, as shown in Fig.4.

However, when the attacker activates the DATA Flooding Attack, the neighbor nodes are difficult to recognize. Because the neighbor nodes can not judge whether a DATA packets is useless in the network layer.

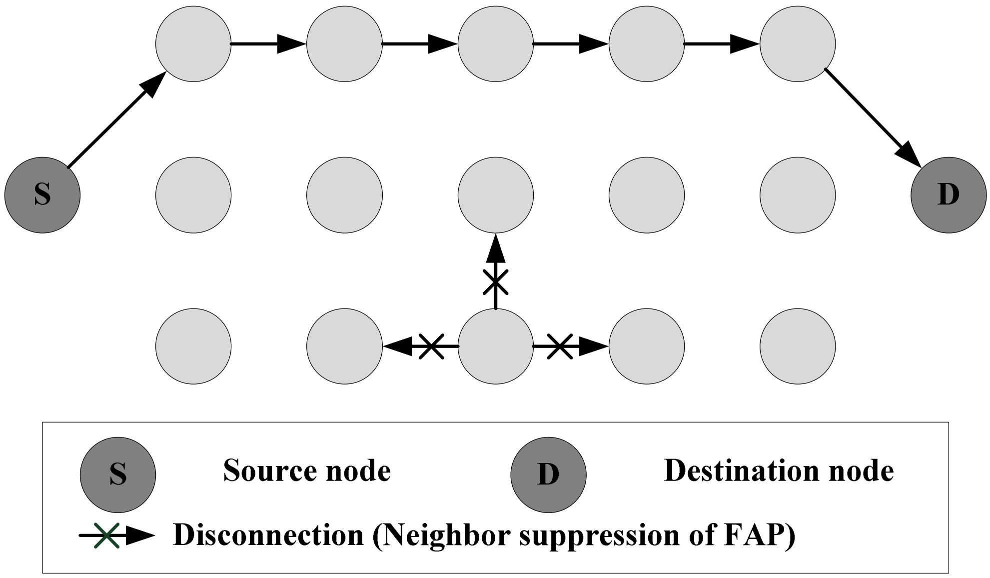


Fig. 4: Neighbor suppression of FAP

Block the RREQ broadcasting by 1/Freq

The destination node can easily recognize it in the application layer when it receives these useless DATA packets. The attacker needs to set up a path to victim before originating DATA Flooding Attacks. When the victim finds the DATA Flooding Attack, it can cut off the path from the attacker in order to prevent the Flooding Attack from the attacker.

So the victim node originates the Route Error (RERR) message back to the attacker as shown in Fig. 5. The RERR message indicates that IP address of victim node is unreachable. The intermediate nodes which the RERR passes through will delete the route from the attack to the victim node. The RERR message may cut off some paths which are not related with the DATA Flooding Attack, and these paths may be repaired by the origination nodes hereafter. With the paths on which the attacker carries out DATA Flooding Attack cutting off gradually, the DATA

Flooding Attack is terminated as shown in Fig. 6.

In order to avoid attacker rebuild routes to other nodes, only the destination node can respond RREQ packets.

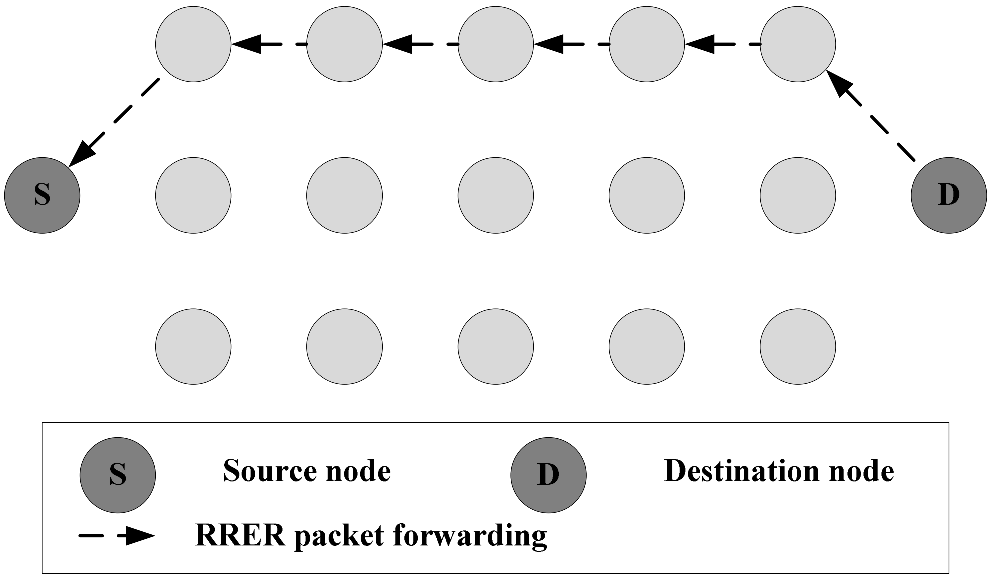


Fig. 5: RERR packet forwarding

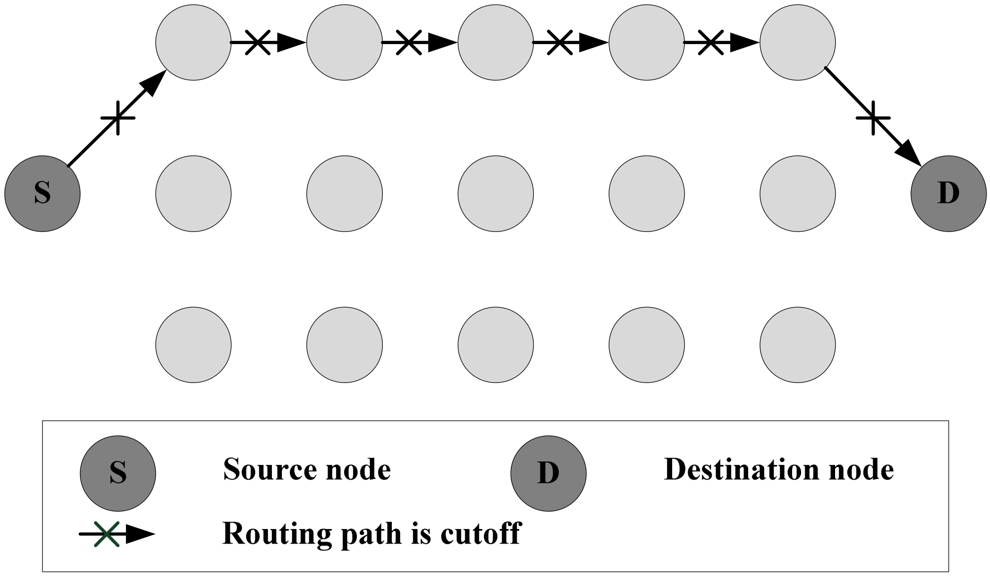


Fig. 6: Routing path is cutoff

2.3.2 AMTT (Avoiding Mistaken Transmission Table)

In the AMTT[11] scheme, each node establishes an avoiding mistaken transmission table. This table is used to record received RREQ packages and to enroll existed legal communication routes as shown in Table 1.

Table 1: Format of AMTT and Parameter description

S IP Addr	D IP Addr	RREQ Num	Seq Num	Vald indic	Comm Rec

Symbol	Parameter Description
S IP Addr	The source IP Address
D IP Addr	The destination IP Address
RREQ Num	Number of RREQ packages
Seq Num	Sequence number of RREQ
Vald indic	Validity Indication, 0 indicates this route is legal, 1 Indicates it is illegal
Comm Rec	Number of Data Packages Passed Through

When node A wants to send package to node B, it sends RREQ package. Every node receiving this RREQ adds an item in its AMTT, fills the source IP address, destination IP address, sequence number according to the package, and sets the RREQ Num as 1. Fig. 7 shows the RREQ passing through. After that, whenever receives a RREQ with the same source IP address, destination IP address and sequence number, this RREQ Value will increase by 1. All nodes do the same collect to the received RREQ packages. Table 2 shows the RREQ value and Parameter description.

Table 2: RREQ Value and Parameter description

S IP Addr	D IP Addr	RREQ Num	Seq Num	Vald indic	Comm Rec
S's IP	D's IP	1	s	NULL	NULL

Symbol	Parameter Description
S IP Addr	The source IP Address
D IP Addr	The destination IP Address
RREQ Num	Number of RREQ packages
Seq. Num	Sequence number of RREQ
Vald indic	Validity Indication, 0 indicates this route is legal, 1 indicates it is illegal
Comm Rec	Number of data packages passed through

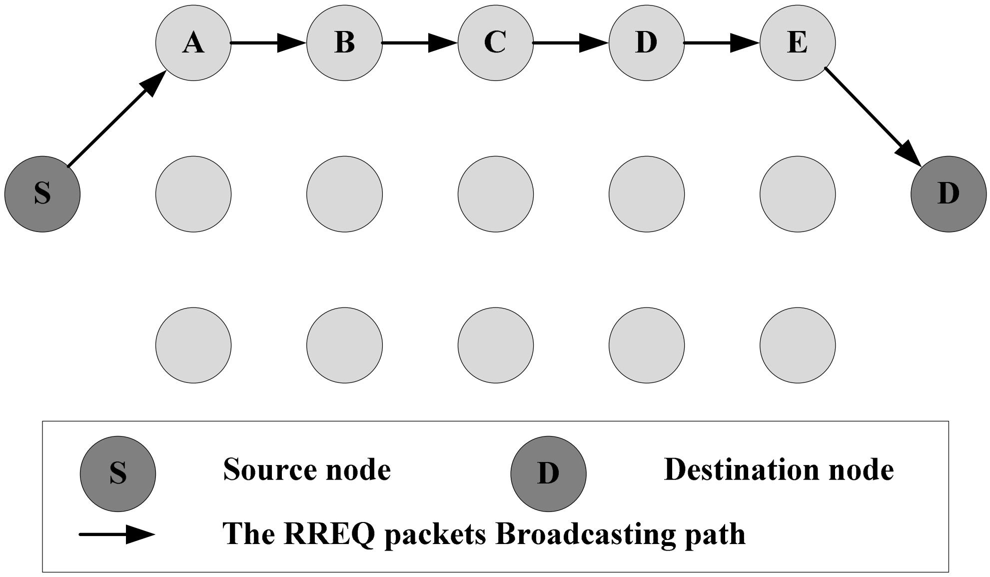


Fig. 7: The nodes write the AMTT records from the RREQ passing through

After the destination node receives RREQ from the source node, it adds corresponding item in its AMTT, and then sends the RREP package back to the source node along the routing path, as shown in Fig. 8. When this RREP reaches intermediate nodes, its validity is checked by them. If the destination node is found legal, they search their AMTTs, and set corresponding items' Validity Indication as 1. Otherwise, they discard this RREP package and do not set the Validity Indication, as shown in Table 3.

Table 3: Validity Indication and Parameter description

S IP Addr	D IP Addr	RREQ Num	Seq Num	Vald indic	Comm Rec
S's IP	D's IP	1	s	1	NULL

Symbol	Parameter Description
S IP Addr	The source node IP Address
D IP Addr	The destination node IP Address
RREQ Num	Number of RREQ packages
Seq Num	Sequence number of RREQ
Vald indic	Validity Indication, 0 indicates this route is legal, 1 Indicates it is illegal
Comm Rec	Number of Data Packages Passed Through

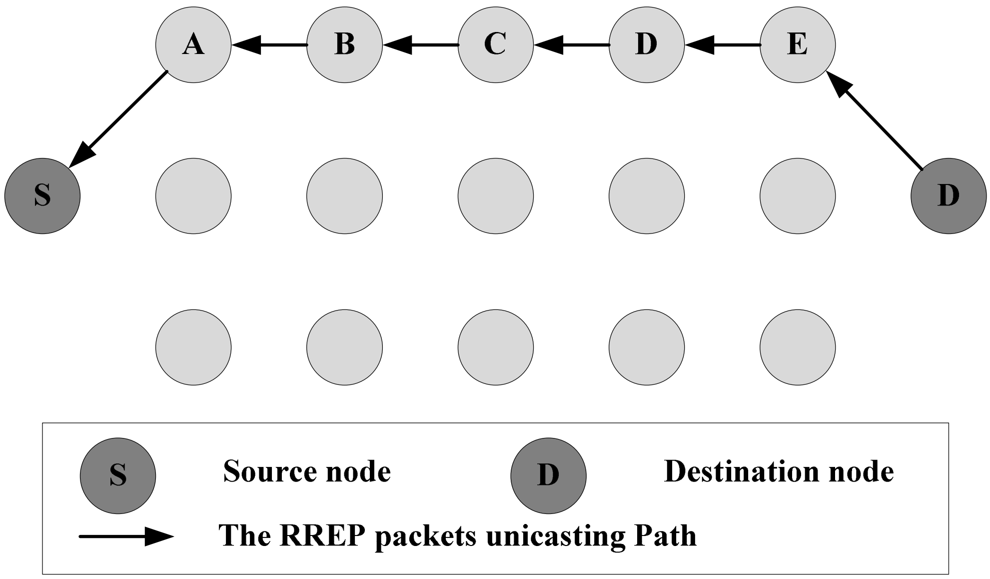


Fig. 8: The nodes write the AMTT records from the RREP passing through

When a node forwards a data package, it will set the Communication Record of the item whose source IP address and destination IP address in its AMTT to 1, as shown in Table 4.

Table 4: Communication Record and Parameter description

S IP Addr	D IP Addr	RREQ Num	Seq Num	Vald indic	Comm Rec
S’s IP	D’s IP	1	s	1	1

Symbol	Parameter Description
S IP Addr	The source node IP Address
D IP Addr	The destination node IP Address
RREQ Num	Number of RREQ packages
Seq Num	Sequence number of RREQ
Vald indic	Validity Indication, 0 indicates this route is legal, 1 Indicates it is illegal
Comm Rec	Number of Data Packages Passed Through

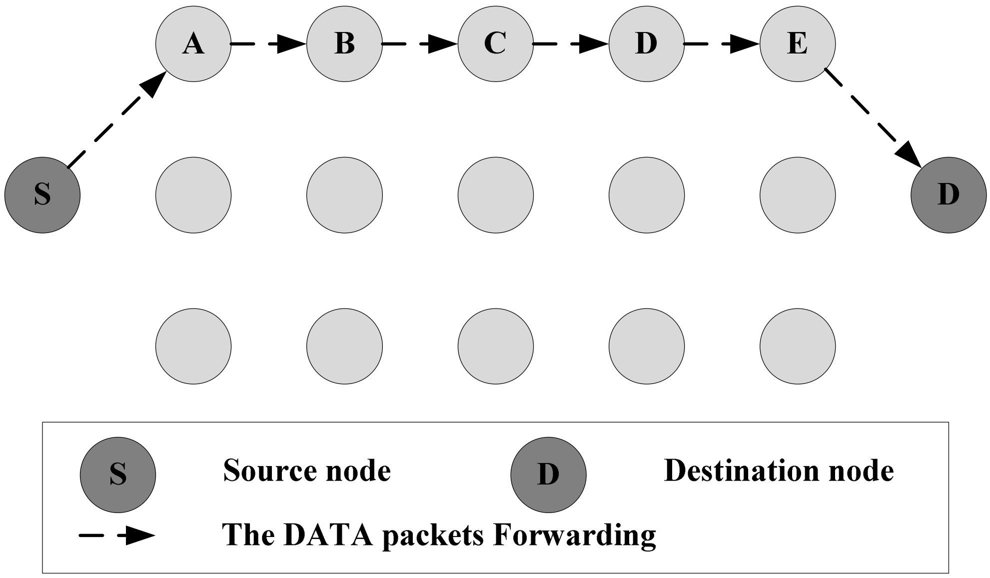


Fig. 9: The midway nodes record the numbers of DATA packets

In this way, whenever sending a data package, midway nodes set the corresponding communication record in their AMTTs to 1, as shown in Fig. 9. Each node periodically (such as 4*(Round Trip Time)) does collect of its AMTT's for every item's communication record, and deletes the item whose increasing value is less than the average value of all the items' increasing values.

By this way, if a legal communication is broken off because of the mobility of the destination node or other reasons, the nodes included in the old route will delete these invalid items related to this communication with the lapse of time, and the resource of AMTT will not be occupied in vain.

After two nodes finish their communication, the source node will send Rout Announcement (RANC) to intermediate nodes, as shown in Fig. 10. All the nodes receives RANC will delete corresponding items in their AMTTs.

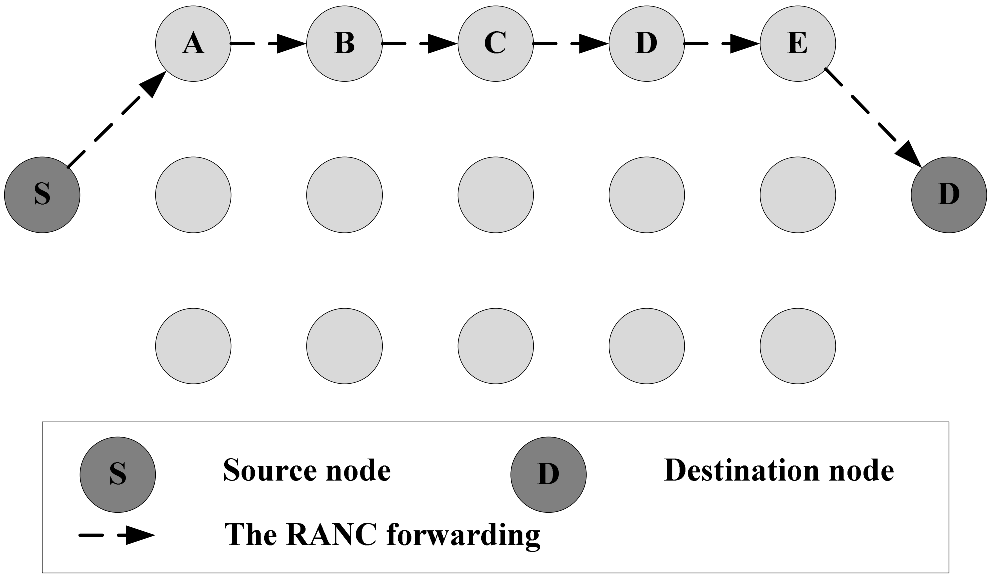


Fig. 10: The nodes receive RANC and delete items of their AMTTs

Let's assume that one node T's AMTT has n items. Their Source IP Address, Destination IP Address and RREQ Num are respectively (Si , Di , RVQi) , here $0 \le i < n$. Node T periodically (such as average Round Trip Time) and ordinally collect each source node's RVQall = (RVQ0+ RVQ1+......+RVQi +RVQn-1), the RREQ number sending from Si to all Di (i = 0,1,......,(n−1)).

Then it will compare RVQall with its threshold, assume it is threshold. If RVQall overruns threshold, node T will search all the Validity Indication and Communication Record of the items whose Source IP Address is Si. If all these items' Validity Indication and Communication Record are null, it can decide Si as attacker, and refuses to forward packets from Si any more. Every legal node does the same thing periodically, so they can distinguish illegal nodes and resist RREQ flooding attack in time.

Meanwhile, whenever data packets reach node T, node T will search its AMTT before forwarding it. If there is an item for this packet and its Validity Indication is 1, node T will forward it, otherwise it will discard it. Because illegal node can not pass security authentication, it will not build link with legal nodes. Then its neighbor nodes' AMTTs will not have the items whose Validity Indication is 1 for this node, so no node will forward the data packets from this illegal node. This successfully resists data flooding attack.

Chapter 3
Our Scheme

There are very obvious attacking features embedded in the process of activating flooding attacks in the Ad-hoc networks. Firstly, the attackers broadcast massive RREQ packets ignoring the rule of RREQ_RATELIMIT. Secondly, the attackers select massive fake addresses which are not in this network. Thirdly, attackers also send large and useless DATA packets to victim nodes by setting up legal routing paths in order to consume the resource of networks, especially the bandwidth.

Our scheme uses the Priority and Trust Value (PTV) and threshold of neighbor nodes to detect the flooding attacks. We use "HELLO" packets to collect the status of neighbor nodes in the Neighbor Nodes List Table (NNLT). Nodes also use the value of Hop Count in RREQ packets to identify the source node address in order to avoid nodes faking the address or the value of hop counts. So it is easy to prevention flooding attacks at the first hop node and the whole networks can maintain well

.

3.1 Priority and Trust Value Scheme

In our PTV(Priority and Trust Value Scheme) scheme, each node build a PTV table to record the packets passing through itself and set the priority and trust value for each source node. The node can decide to forward packets or not by PTV. Priority and Trust value can be upgraded or downgraded according to the received packets.

When attacked nodes were damaged or normal nodes were hacked, those neighbor nodes still can use the PTV scheme to recovery connection or prevent the attack, as shown in Table 5 and Table 6.

Table 5: Format of RREQ PTV(RPTV) and Parameter description

S IP Addr	**RREQ Num**	**Time Stamp**	**RREP Num**	**RPT Value**

Symbol	**Parameter Description**
S IP Addr	The source node IP Address
RREQ Num	Number of Received RREQ packages
Time Stamp	The time when first RREQ packet be received
RREP Num	Number of Received RREP packages
RPT Value	The Priority and Trust Value of RREQ

The PTV of DATA (DPTV) packages record the status of DATA packages passing through. It also records the numbers of DATA packages which has the same source and destination addresses. Nodes can hold and queue DATA packages if the value of DATA Num is over the threshold, it will wait for the answers from the destination node. If the node receives error messages, the value of DPTV will be set as 0 and the connection is blocked, else it will be set as 1 and the transmission is continued.

Table 6: Format of DATA PTV(DPTV) and Parameter description

S IP Addr	D IP Addr	DATA Num	DPT Value

Symbol	Parameter Description
S IP Addr	The source node IP Address
D IP Addr	The destination node IP Address
DATA Num	Number of DATA packages
DPT Value	The Priority and Trust Value of DATA Value 0: means this node is an attacker Value 1: means this node is normal

3.2 Neighbor Node List Table (NNLT)

The node broadcasts "Hello" packets to find neighbor nodes. When the node receives "Hello" packets from its neighbor node, it will record the source address. According to the data collecting from Hello packets, the node can recognize how many nodes around itself.

Nodes also broadcast "Hello" packets periodically to check if its neighbors are still available. At the same time, the node records the neighbors IP address in the PTV table. And the nodes will delete the record when its neighbor nodes are dead (nodes removed away or do not answer the HELLO packet).

Nodes can also collect the same information when it receives RREQ packets. By this way, the node can prevent the attacker from faking its address to cheat and reducing the storage size of PTV.

For example, there are three nodes node *(x, y, z)* around node *k*. When the nodes change “Hello” packets, the NNLT of node *k* will write node *x*, node *y* and node *z* addresses into the table. And so node *k* has three neighbor nodes in NNLT, as shown in Table 7. NNLT also records those nodes LOD (Live or Dead) status. Node *k* can then delete PTV of nodes since LOD value is 1(because when the value equal 1, the node was died).

Table 7: Format of Neighbor Node List Table (NNLT) and Parameter description

N IP Addr	LOD	RPT Value

Symbol	Parameter Description
N IP Addr	The Neighbor node IP Address
LOD	The node Live or Dead Value 0: means this node is Live Value 1: means this node is Dead
RPT Value	The Priority and Trust Value from RREQ PTV

3.3 The Definition of RREQ Threshold

In the normal stage (without attacks), each node uses *RREQ_RATELIMIT* to limit the frequency of broadcasting RREQ. If the sending frequency of RREQ is over this limit, the node will stop sending RREQ to neighbors.

But at the attack scenario, the node will ignore the rate limits and SEND MASS RREQ to neighbors to exhaust all network resource. If the node has n neighbor nodes, and according to the definition of RFC 3561, the default sending frequency of RREQ packets for each node is *RREQ_RATELIMIT* , so the max RREQ packets from its neighbor nodes are *N* RREQ_RATELIMIT*. Because of this, we define the Max and Min RREQ Threshold for each node as equation (1)(2). Table 8 shows the parameter description of our algorithm.

Pseudo code of our scheme

We assume that the neighbor node number is 5;
*MaxThreshold=5*10=50(Frequency);*
MinThreshold=10(Frequency);
Timer=1/ Frequency;

```
if ( RREQ_RATE > MaxThreshold  &&  timer < 0.02)
{
(Priority and Trust Value 0) Nodes stop to sending any packets
} else if( RREQ_RATE >MinThreshold && RREQ_RATE< MaxThreshold  &&  (timer > 0.02 && timer < 0.1))
{
(Priority and Trust Value 1)
The nodes hold packets and forward packets
```

By the rule of *RREQ_RATELIMIT*
} else if(*RREQ_RATE* <*MinThreshold* && timer > 0.1)
{
(Priority and Trust Value **2**)
The node forward packets properly }

RREQ_RATELIMIT = 10

N are the numbers of neighbor nodes. And *RREQ_RATELIMIT* is defined by RFC 3561 and the default value is 10[11].

Table 8: The Parameter Description of our Algorithm

Symbol	Parameter Description
RREQ_RATE	The total number of RREQ at that time
RREQ_RATELIMIT	Defined by RFC 3561 and the value is 10
MinThreshold	The minimum threshold of the RREQ
MaxThreshold	The maximum threshold of the RREQ
Status	The status of the RREQ PTV
Timer	The reciprocal of time

3.4 The Definition of DATA Threshold

We define the Max DATA package threshold according to the default Maximum

Transmission Unit (MTU) of 802.11 by [13]. We define DATA threshold for node as (1).

$$DATA\ Threshold = Bandwidth\ \frac{MTU}{n} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Bandwidth is the bandwidth of 802.11x, like 802.11b for 11 Mbps.MTU is the default maximum transmission unit of 802.11x, and the value is 2312 bytes. And n is the numbers of neighbor nodes.

For example, if the Ad-hoc networks use 802.11b for its connection bandwidth, and there are 5 nodes beside it, we can get the DATA Threshold as 121 (11Mbps/2272bytes/5) for this node.

3.5 The Level of Priority and Trust Value

We define three levels of Priority and Trust Value, as shown in Table 9. Level 0 is the lowest; it means that this node is trustless and is an attacker. Nodes neighboring this node should not forward any packets for it. Level 1 is low; it means this node is not worthy to be trusted. Nodes neighboring this node should hold RREQ packets and forward these RREQ by the rule of *RREQ_RATELIMIT*. Level 2 is normal; it means this node is normal and trustable. Nodes neighboring this node will forward packets sent from it directly.

Table 9: The Three Level of Priority and Trust Value

Level	Status	Actions
0	Lowest	The node stop to sending any packets
1	Low	The node hold packets by the rule of *RREQ_RATELIMIT*
2	Normal	The node forward packets properly

3.6 The Level of Priority and Trust Value

The methods to defense the RREQ Flooding Attack

At the beginning, the nodes exchange “HELLO” packets and write the information of neighbor nodes into NNLT. But now the value is null in PTV.

When the nodes start to connect with each node, they broadcast RREQ packets. The nodes will receive the RREQ packets from their neighbor nodes. After receiving RREQ packets, the node will compare the source address at the header of RREQ packets with NNLT. The node will write the information of received RREQ packets which its source node address is in NNLT into RREQ PTV table.

If the source node of RREQ packets is already in RREQ PTV table, the node will forward or drop it according to the value of its PTV. The first record of the source node address in PTV is set as 2 (normal).

If the receiving frequency of RREQ packets is over the Max RREQ Threshold which we define, the node will drop all RREQ packets and block this connection. The Priority and Trust Value of this source node will be set as 0 (lowest).

If the receiving frequency of RREQ packets is over the Min RREQ threshold which we define and not over the max RREQ threshold, the node will forward the RREQ packets and wait for any RREP packets sent back in two of Round Trip Time (RTT). If there are no any RREP packets sent back, the node will downgrade Priority and Trust Value as 1(low) or maintaining the original value. After another two of Round Trip Time (RTT), there are still no any RREP packets sent back, the node will downgrade the Priority and Trust Value as 0(lowest) and block this connection. Else this value will keep as 1 and forward RREQ packets by the rate of RREQ_RATELIMIT.

If the receiving frequency of RREQ is not over the Min RREQ Threshold, the node will set the Priority and Trust Value of this source node address as 2(normal) and forward the RREQ packets directly.

When the Priority and Trust value in RREQ PTV table is set as 0, each node will check the RREQ receiving frequency from this node in each 8*(Round Trip Time). The same procedure will also be executed when Priority and Trust value is 1. If after eight of Round Trip Time and the RREQ receiving frequency is not over the Min RREQ Threshold, the node will upgrade the Priority and Trust value to the upper level. The node will keep the original Priority and Trust value when the receiving RREQ frequency is over min threshold.

The methods to defense the DATA Flooding Attack

When the source and destination node set routing path legally, the first node of this routing path will create Priority and Trust Value for the DATA packets. The node will write the source and destination addresses into DATA PTV when it receives the RREP packets. After the source node starting sending DATA packets, the node will check the Priority and Trust value of this source and destination. If the DPT value is NULL, the node will set this value as 1 firstly and forward these DATA packets.

In periodically time such as 1 second if the receiving frequency of DATA packets which comes from the same source address is over the DATA threshold, the node will hold this connection and wait for any RERR packets.

If the node receives any RERR packets for this source address, the node will set Priority and Trust value as 0; else the node will queue and forward DATA packets obeying the DATA Threshold by FIFO.

If there is no any RERR packets sent back, it does not mean that there is no DATA flooding attack happened. This kind of situation could be happened when the source node and destination node are cooperated or any midway node keeps the RERR packets.

In order to avoid the DATA flooding attacks from occurring like this situation, the node controls the DATA packets forwarding rate when the node does not receive any RERR packets and the receiving DATA packets numbers is over DATA Threshold. And according the method, the node can reduce the DATA packets flooding in the network and stop the DATA flooding attacks.

Chapter 4
Simulation results

4.1 Experimental environment

We implemented Ad Hoc Flooding attack and Priority and Trust Value (PTV) 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.

Our simulations are based on a 1000 by 1000 meter space, contains 50 random nodes. The radio range for each node is 250 meters and bandwidth is 2 Mb/s. Each simulation is executed for 900 seconds of simulation time. The data size of 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, as shown in Table 10.

Table 109:The experimental environment

Symbol	Parameter Description
Simulation size	1000 m X 1000 m
Node number	50 random nodes
Transmission range	250 meters
Bandwidth	2Mb/s

Simulation time	900 /s
Data payload	512 bytes
Data rate	4 packets/s

Our simulation environment has been conducted and is shown in Fig 11. The physical size of the simulation environment are on 1000m by 1000 meters space. And 50 homogeneous nodes are deployed randomly in our simulation scenario. The transmission range of each node is 250m. Each simulation is executed for more than 900 seconds.

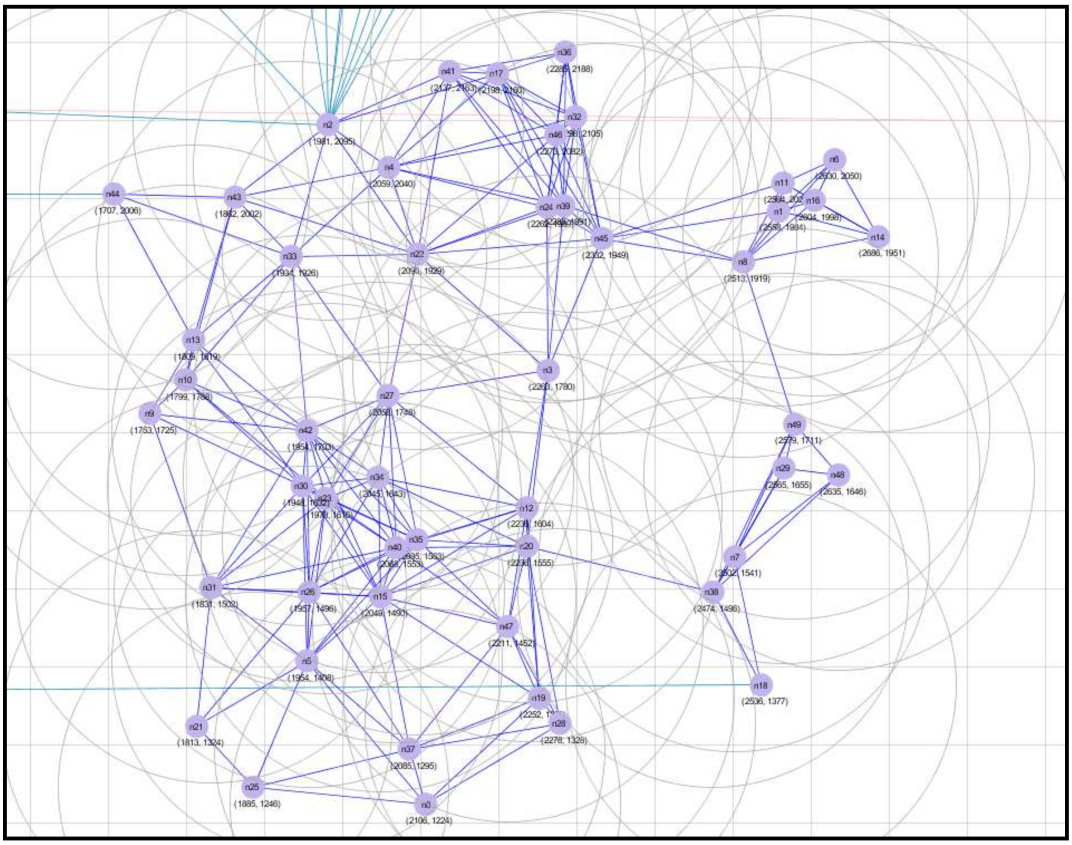


Fig. 11: The environment of our simulation

In our approach, each node can only need to record the neighbor nodes in NNLT. As illustrated in Fig.12, node 2 only records neighbor node 4, node 17, node 22, node 33, node 41, and node 43to its neiboring nodes because of the limitation of transmission range.

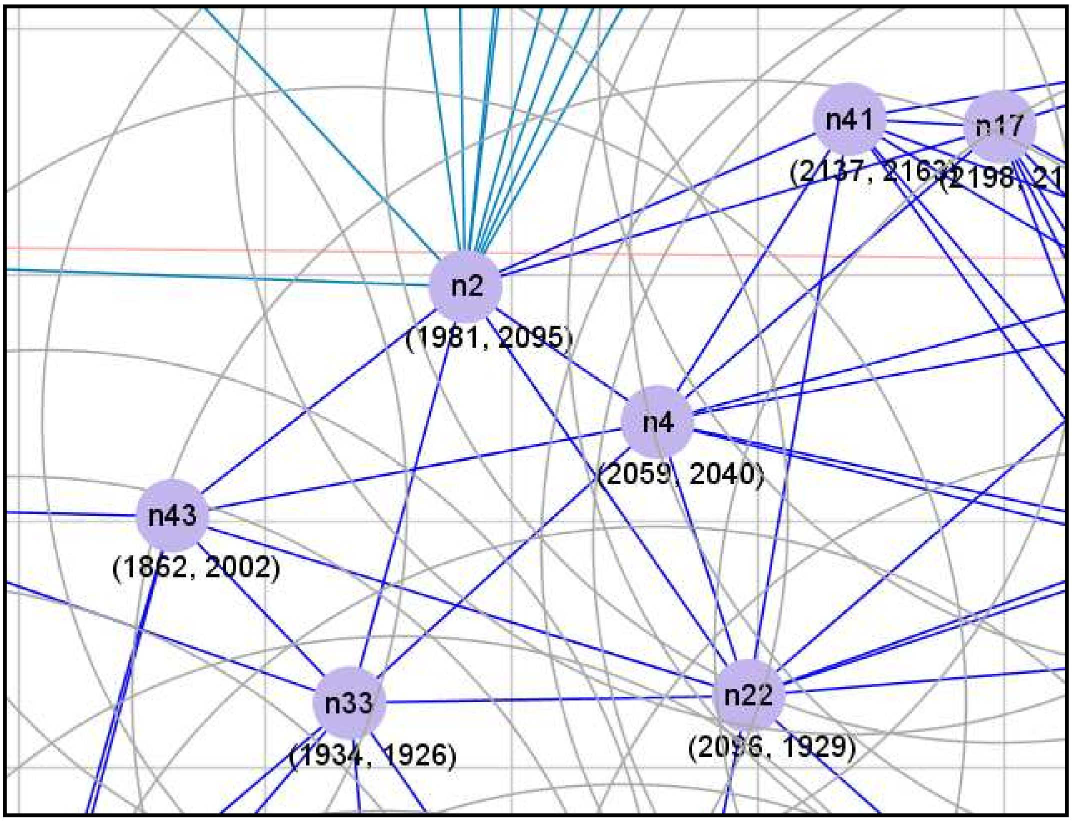
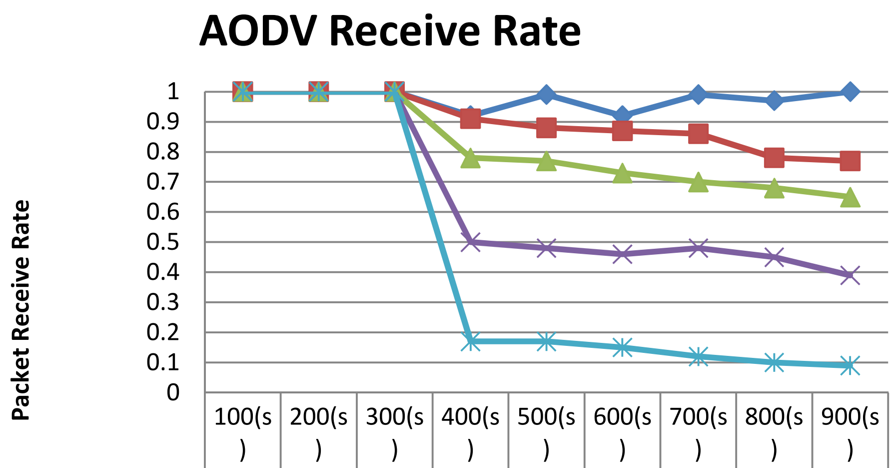


Fig. 12: The environment of our simulation: neighbors of node

4.2 Simulation Results of Ad Hoc Flooding Attack

The first scenario in Fig. 13 is that there are not attacking nodes in mobile Ad-hoc networks. In this simulation we assume that rates of attacking packets are respectively 10packets/s, 20packets/s, 30packets/s, and 40packets/s. In other words, the intruder respectively floods 10, 20, 30, 40 packets every second. The intruder starts to attack at 300s. The simulation results are as follows, shown in Fig. 13.



	100(s)	200(s)	300(s)	400(s)	500(s)	600(s)	700(s)	800(s)	900(s)
0 Attacking packets	1	1	1	0.92	0.99	0.92	0.99	0.97	1
10 Attacking packets	1	1	1	0.91	0.88	0.87	0.86	0.78	0.77
20 Attacking packets	1	1	1	0.78	0.77	0.73	0.7	0.68	0.65
30 Attacking packets	1	1	1	0.5	0.48	0.46	0.48	0.45	0.39
40 Attacking packets	1	1	1	0.17	0.17	0.15	0.12	0.1	0.09

Fig. 13: AODV Receive Rate

The Ad Hoc Flooding Attack can result in denial of service of whole network. When the rate of attacking packets is more than 30 packets/s, the network can’t bear the attack anymore and the performance goes down quickly.

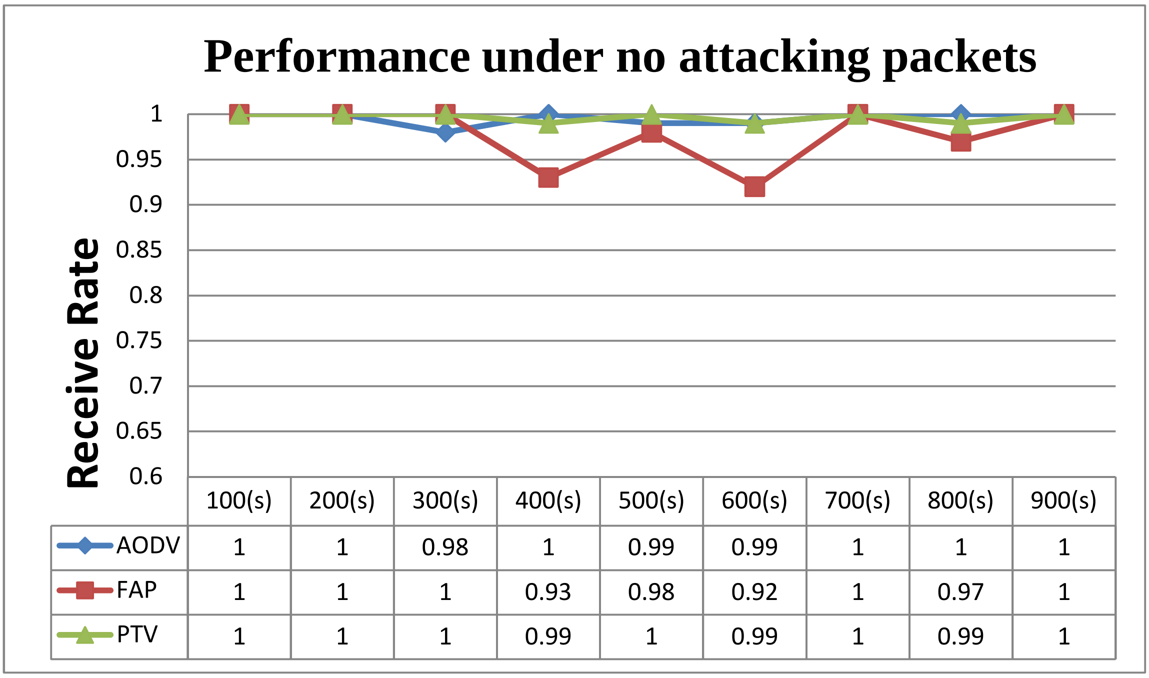
4.3 Simulation Results of Priority and Trust Value

4.3.1 Receive Rate

We define receive rate for node as (2).

$$\text{Receive Rate} = \frac{\text{Drop Packets}}{\text{Total Send packets}} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

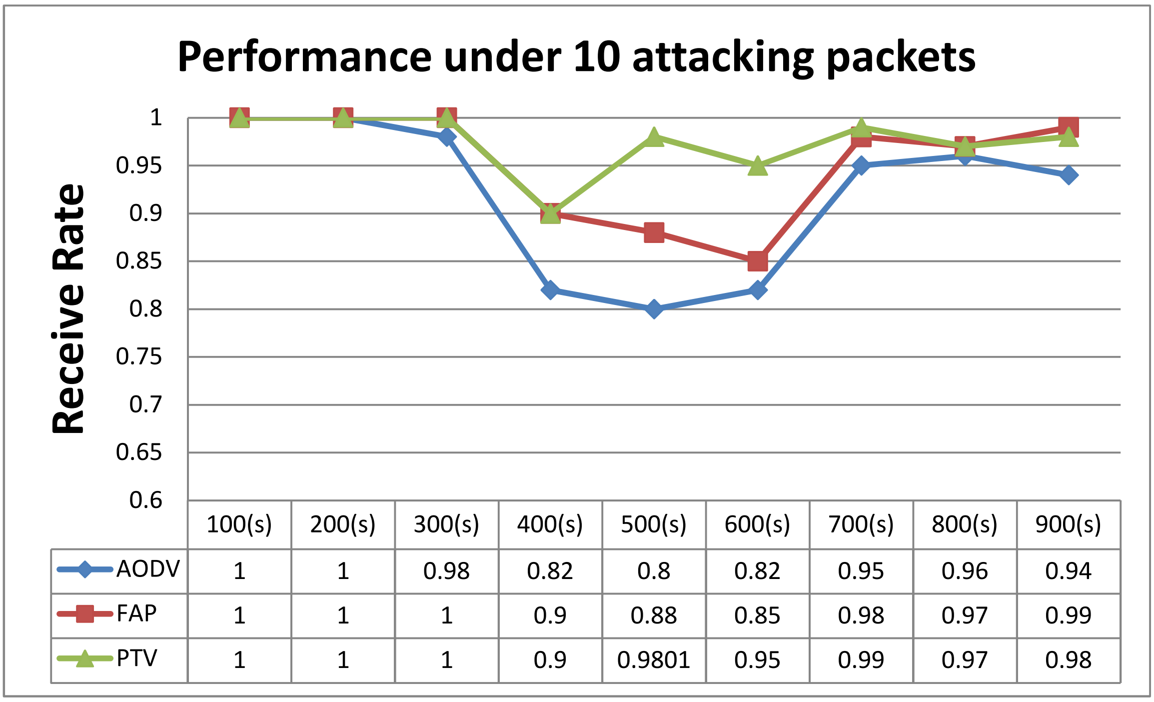
The first scenario is that there are not attacking nodes in mobile Ad-hoc networks. Fig.14 shows the packages receive rate of network. The Simulation results in first scenario about the same.



	100(s)	200(s)	300(s)	400(s)	500(s)	600(s)	700(s)	800(s)	900(s)
AODV	1	1	0.98	1	0.99	0.99	1	1	1
FAP	1	1	1	0.93	0.98	0.92	1	0.97	1
PTV	1	1	1	0.99	1	0.99	1	0.99	1

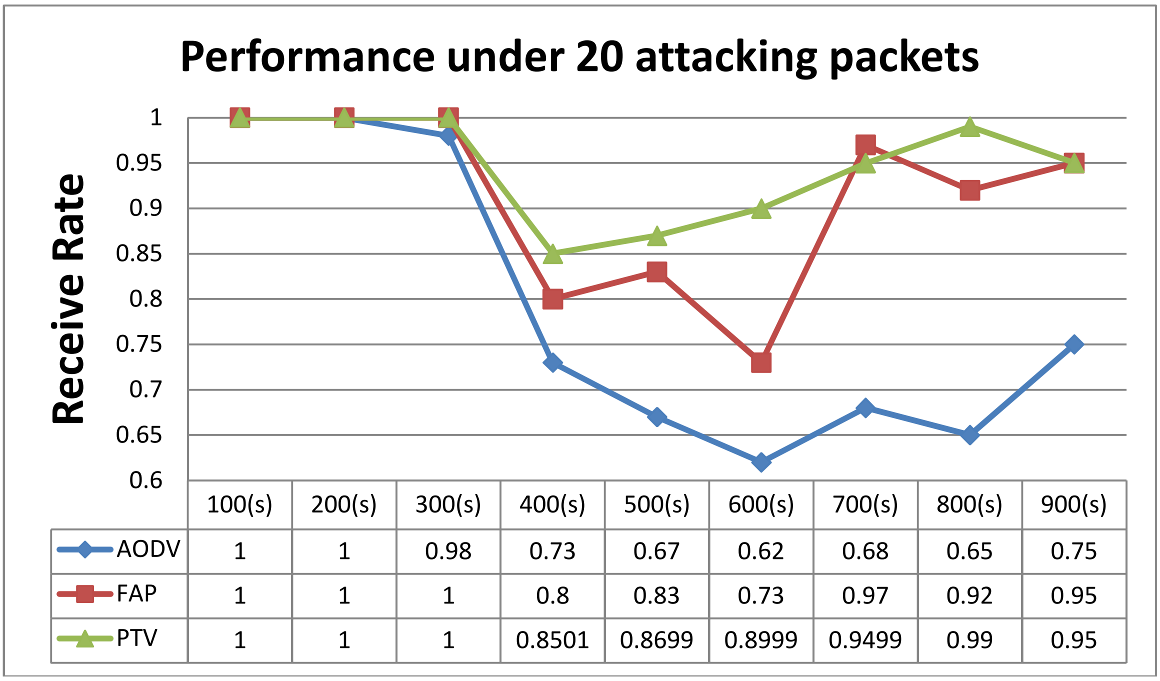
Fig. 14: Performance under no attacking packets

Fig.15 shows the performance under 10 attacking packets every second and Flooding Attack Prevention and our scheme PTV. There is not attacking packets between 0 and 300s. The intruder attack from 300s to 900s in network. At 600s of simulation, FAP in nodes takes effect. We can observe that the performance has got better after 600s. But in our scheme PTV, Between 300s to 400s of simulation, PTV in nodes takes effect earlier than FAP. The average receive rate of 10 attacking packets is 97.4%.



	100(s)	200(s)	300(s)	400(s)	500(s)	600(s)	700(s)	800(s)	900(s)
AODV	1	1	0.98	0.82	0.8	0.82	0.95	0.96	0.94
FAP	1	1	1	0.9	0.88	0.85	0.98	0.97	0.99
PTV	1	1	1	0.9	0.9801	0.95	0.99	0.97	0.98

Fig. 15: The performance under 10 attacking packets in AODV, FAP and PTV

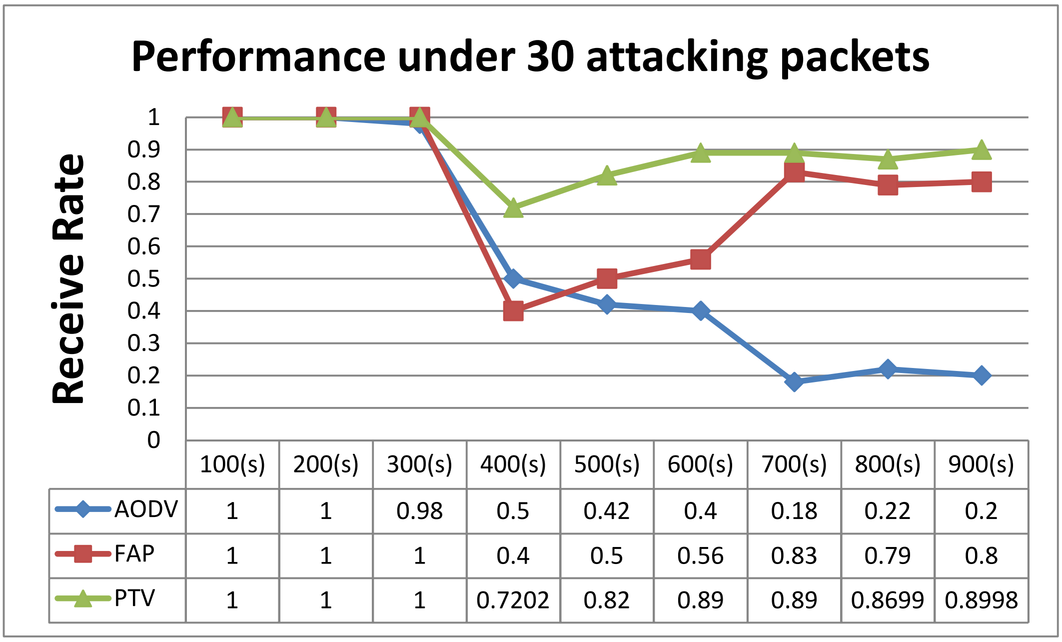


	100(s)	200(s)	300(s)	400(s)	500(s)	600(s)	700(s)	800(s)	900(s)
AODV	1	1	0.98	0.73	0.67	0.62	0.68	0.65	0.75
FAP	1	1	1	0.8	0.83	0.73	0.97	0.92	0.95
PTV	1	1	1	0.8501	0.8699	0.8999	0.9499	0.99	0.95

Fig. 16: The performance under 20 attacking packets in AODV, FAP and PTV

Fig.16 shows the performance under 20 attacking packets every second and Flooding Attack Prevention and our scheme PTV. There is not attacking packets between 0 and 300s. The intruder activates attack from 300s to 900s in our network simulation.

At 600s of simulation, FAP in nodes takes effect. We can observe that the performance has got better after 600s. But in our scheme PTV, Between 300s to 400s of simulation, PTV in nodes takes effect earlier than FAP. Our performance can be more clearly display in green line. And the average receive rate of 20 attacking packets is 94.5%.



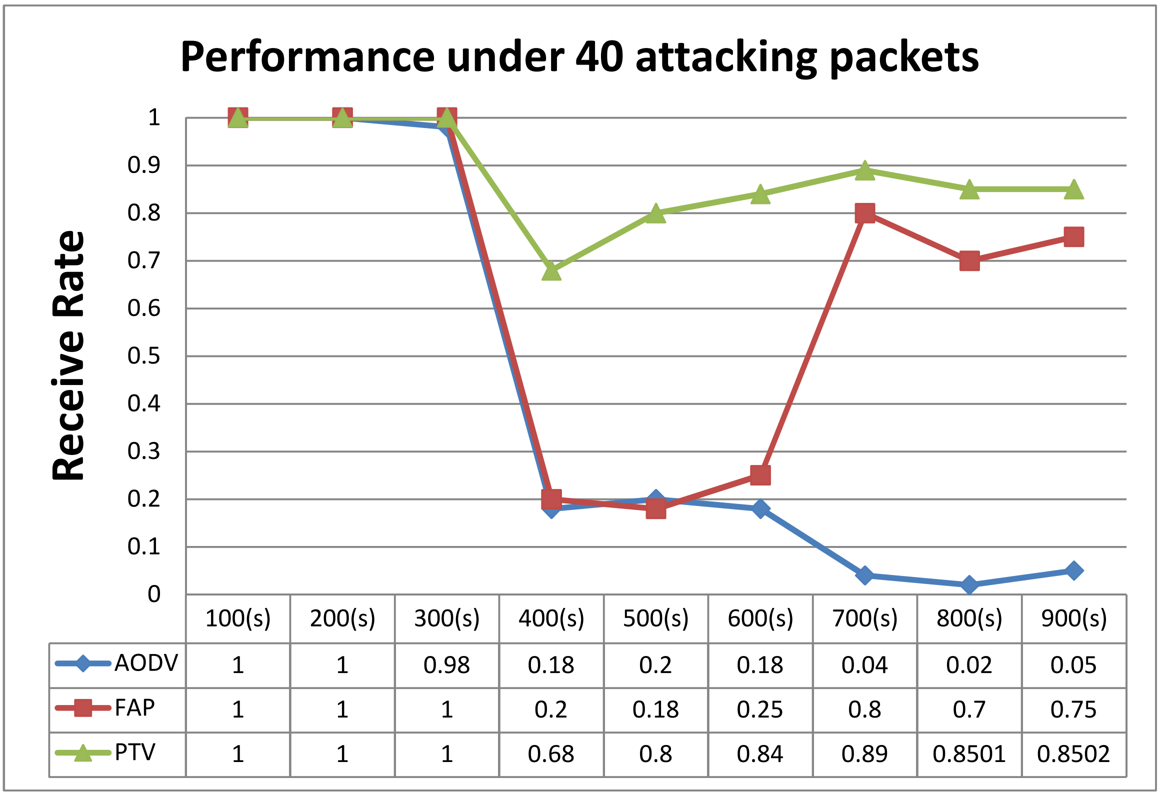
	100(s)	200(s)	300(s)	400(s)	500(s)	600(s)	700(s)	800(s)	900(s)
AODV	1	1	0.98	0.5	0.42	0.4	0.18	0.22	0.2
FAP	1	1	1	0.4	0.5	0.56	0.83	0.79	0.8
PTV	1	1	1	0.7202	0.82	0.89	0.89	0.8699	0.8998

Fig. 17: The performance under 30 attacking packets in AODV, FAP and PTV

And Fig.17 shows the performance under 30 attacking packets in AODV, FAP and

PTV. FAP performance has got better after 600s and the range between 50% to 80%. In our scheme PTV, the performance has got better after 300s to 400s and the range between 70% to 90%. And the average receive rate of 30 attacking packets is 89.8%.

Fig.18 shows the performance under 40 attacking packets in AODV, FAP and PTV. With more attacking packets every second, the performance of network falls quickly. The packet receive rate gets to 2.0% in Fig.18. When FAP takes effect at 600s, the performance becomes better and packet delivery rate keep up about 80%.But in our PTV scheme, it takes effect between 300s to 400s, and packet delivery rate keep up about 85%. And the average receive rate of 40 attacking packets is 87.8%.



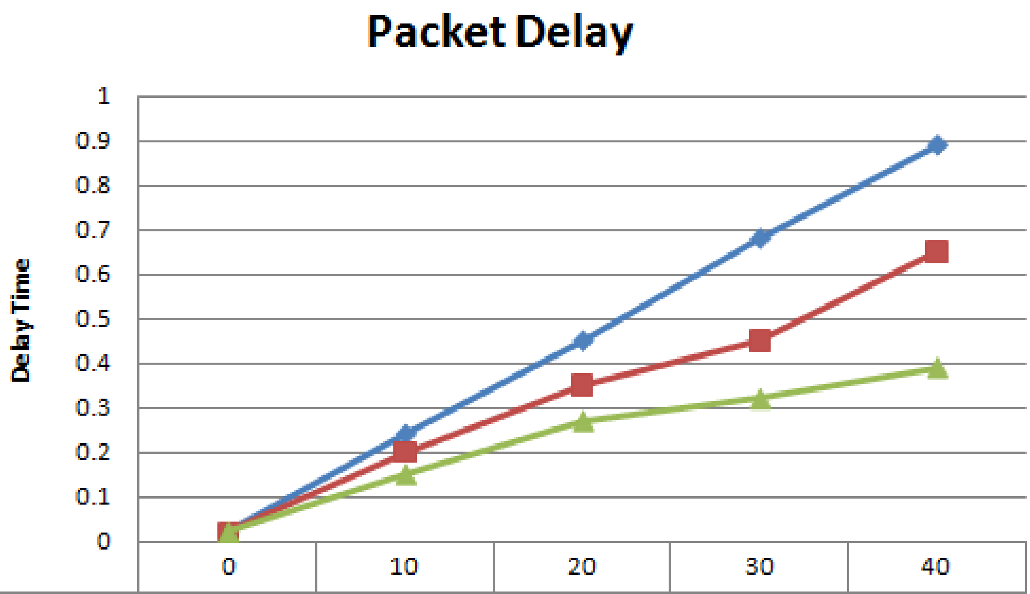
	100(s)	200(s)	300(s)	400(s)	500(s)	600(s)	700(s)	800(s)	900(s)
AODV	1	1	0.98	0.18	0.2	0.18	0.04	0.02	0.05
FAP	1	1	1	0.2	0.18	0.25	0.8	0.7	0.75
PTV	1	1	1	0.68	0.8	0.84	0.89	0.8501	0.8502

Fig. 18: The performance under 40 attacking packets in AODV, FAP and PTV

4.3.2 Packet Delay

Packet delay usually refers to the signal or data packets on the network the required transmission time, the IP network is concerned, and end-to-end delay is defined by source-node generated packets through different network equipment and circuit to the receiver end of time. We define end-to-end delay for node as (3).

$$End - to - End \ \ Delay = Arrival \ \ Time - Send \ \ Packets \ \ Time \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$



	0	10	20	30	40
AODV	0.02	0.24	0.45	0.68	0.89
FAP	0.02	0.2	0.35	0.45	0.65
PTV	0.02	0.15	0.27	0.32	0.39

Fig. 19: The performance under attacking packets in AODV, FAP and PTV

Fig.19 shows the performance under 0-40 attacking packets in AODV, FAP and PTV. With the increase in the number of packets, packet delay increases more and more. We can see that AODV significantly increased, but all of the PTV scheme always under 0.4s.We can know the PTV structure better than AODV and FAP. The average of AODV packet delay is 0.456/s, FAP is 0.334/s, and PTV is 0.23/s.

4.3.3 Packet Jitter

In the Ad-hoc, many packets must be in the queue waiting to be transmitted, each packet sent to the destination from the time are not the same, and this difference is the jitter. We use the following formula as (4):

Jitter rate (jitter) = delay variation (delay variance),

Jitter = [(recvtime (j)-send time (j)) - (recvtime (i)-send time (i))] / (ji), which j>

i………………….(4)

The packet jitter of AODV, FAP, PTV as shown in Fig. 20, Fig. 21, and Fig.22.

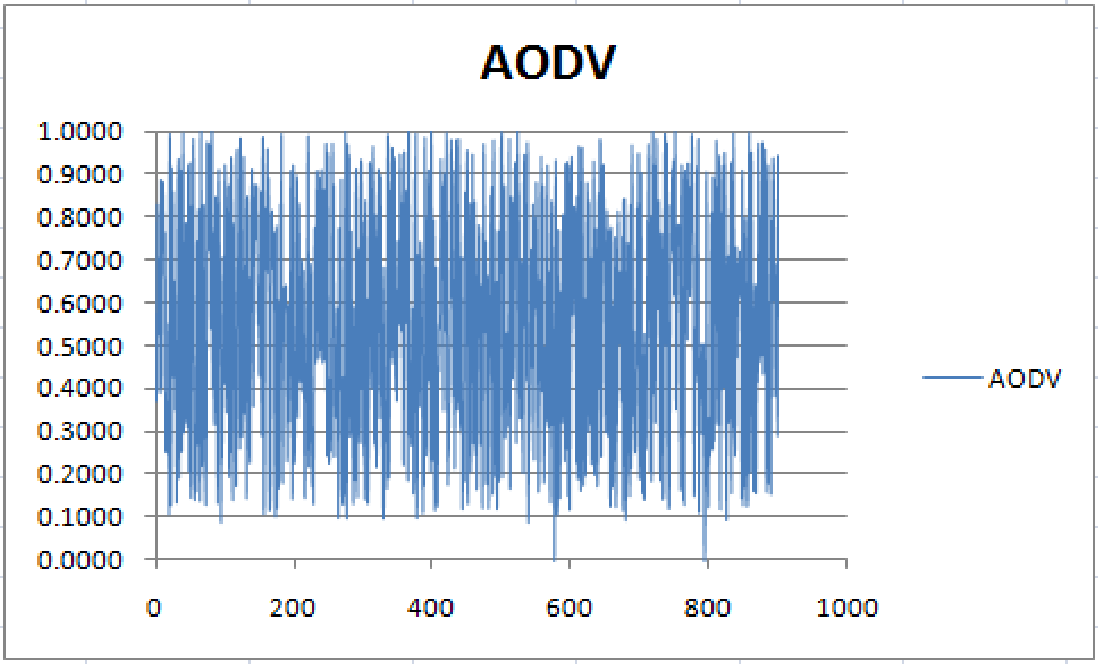


Fig. 20: The packet jitter of AODV

According to the Fig. 20, the AODV packet jitter was 0.456 seconds.

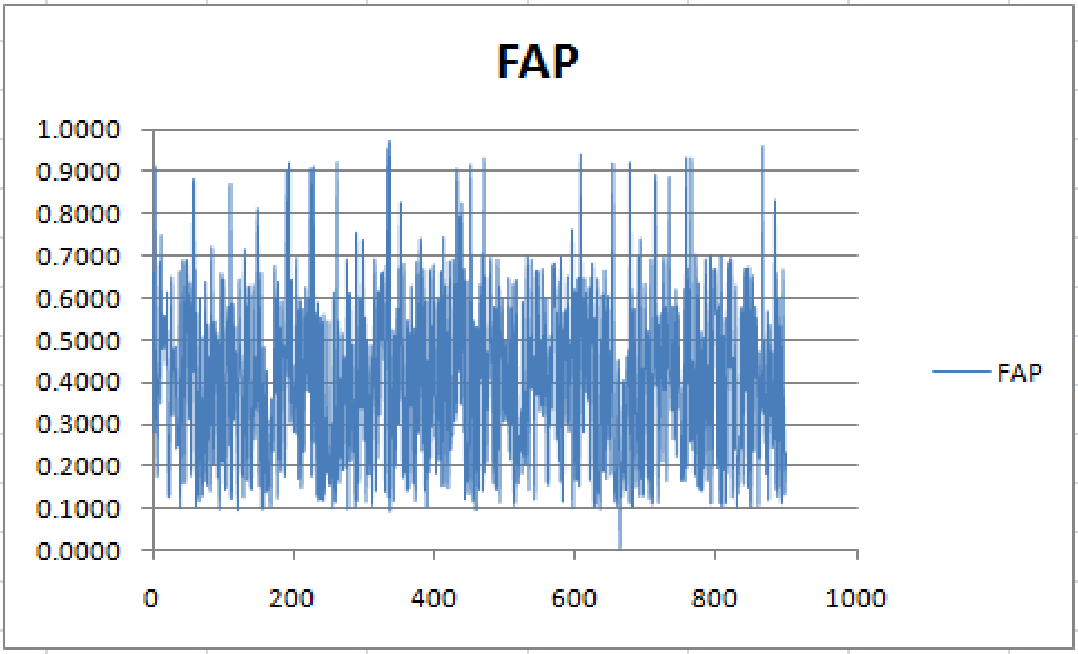


Fig. 21: The packet jitter of FAP

According to the Fig. 21, the FAP packets jitter was 0.334 seconds.

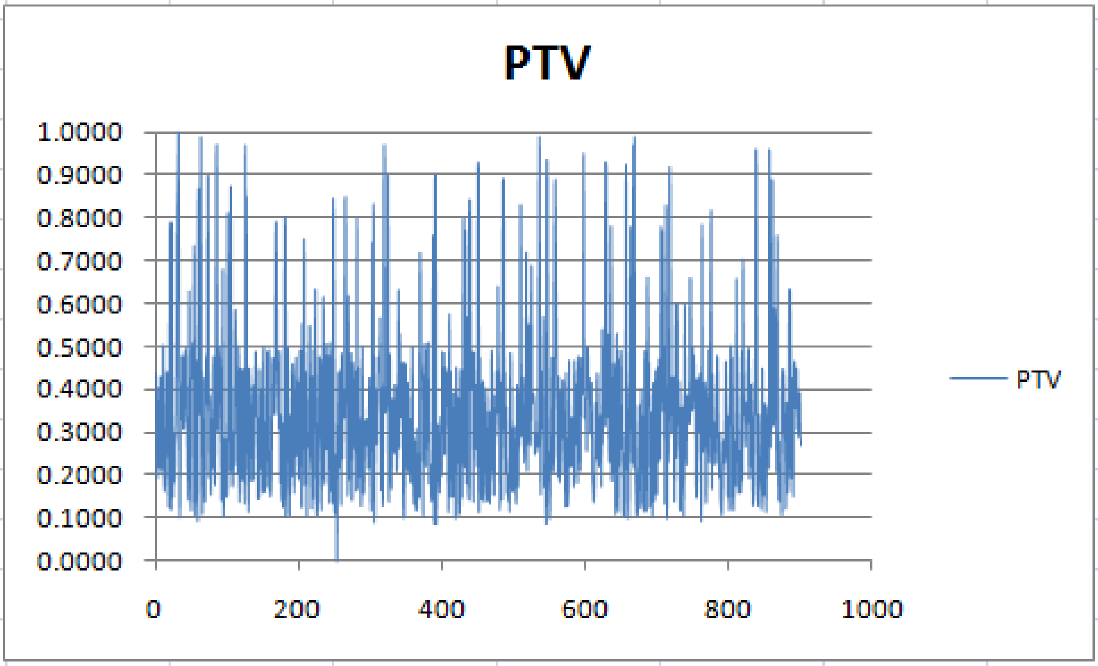


Fig. 22: The packet jitter of PTV

According to the Fig. 22, the PTV packets jitter was 0.23 seconds.

The samples are recorded every 10 seconds, the results show in Fig. 23. The blue line is the average of AODV packet jitter, the red line is the average of FAP packet jitter, and the green line is the average of PTV packet jitter.

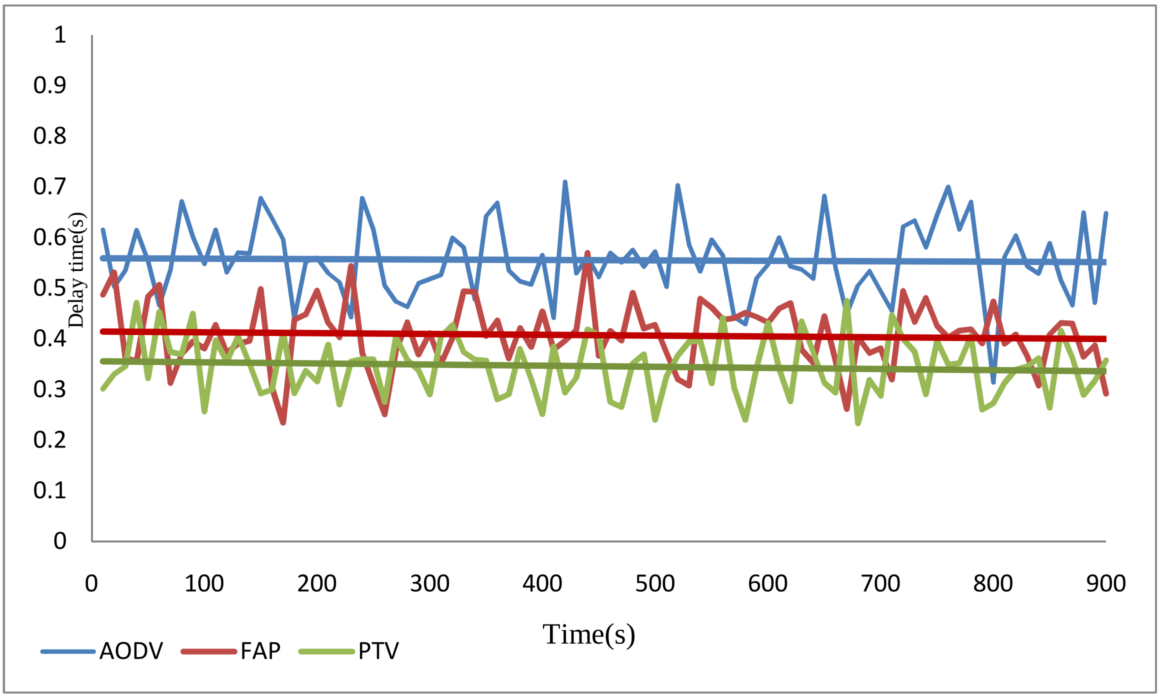


Fig. 23: The packets jitter of PTV

The samples are recorded every 100 seconds, the results show in Fig. 24. The blue line is the average of AODV packet jitter, the red line is the average of FAP packet jitter, and the green line is the average of PTV packet jitter.

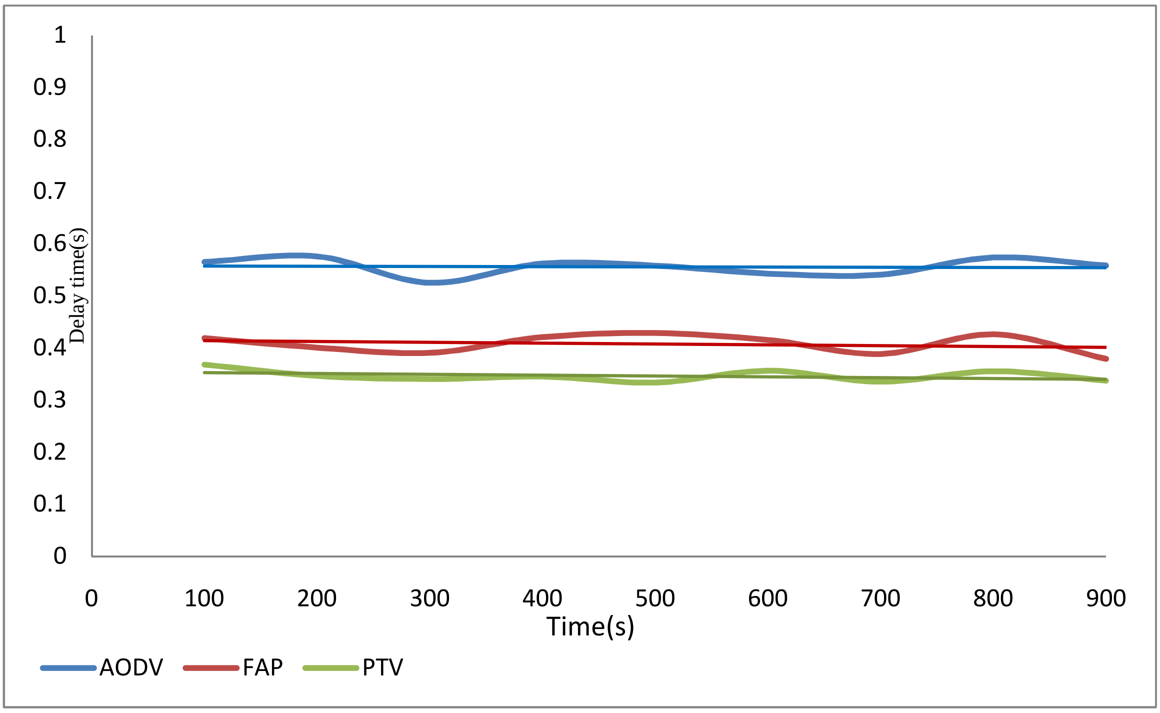


Fig. 24: The packets jitter of PTV

According to the Fig. 24, the AODV packet jitter was 0.456 seconds, the FAP packets jitter was 0.334 seconds, and the PTV packets jitter was 0.23 seconds. We can see that our approach PTV is better than AODV and FAP.

Chapter 5

Conclusion and Future Work

The results of our scheme, we compared with the FAP and AODV as shown in Table 11.

Table 11 Compared with the PTV FAP and AODV

	PTV	**AODV**	**FAP**
Defense attack	**faster**	slower	Normal
Storage	**few**	large	Normal
Delay	**Min.**	Max.	Mid.
Jitter	**Min.**	Max.	Mid.
Receive rate	**Best**	bad	normal

Mobile Ad Hoc network (MANET) has widely used in many applications, such as Ad Hoc meeting, military application and emergent operation, etc. However it has several obvious limitations in nature, for instance, bandwidth constraint and energy constraint. Moreover, all previously on-demand ad hoc routing protocols are vulnerable to Route Request packets flooding attack and DATA packets flooding attack.

In this thesis, we propose a Priority and Trust Value Scheme to inhibit the two types of flooding attack in ad hoc network. The ad hoc network inhibits flooding attack by the nodes neighboring the attacker. The nodes neighboring the attacker can stop the flooding attack quickly and let the whole network works as there is no flooding attack accrued. Comparing with FAP and AMTT, our scheme PTV can be found attackers earlier than them.

The major contributions of our scheme are summarized as follows. Firstly, our scheme is able to detect and stop the flooding attack from the first node's neighboring the attack node. This let nodes inhibit flooding attack more quickly. The second one is our scheme can inhibit the flooding attack launched by two or more attack nodes working together. The third contribution is that fewer storage spaces and less calculation loads are needed for our propoased approach. The nodes in Ad Hoc network only record N nodes information, where N is the number of nodes neighboring itself. This is more suitable to be used in LANs in which the traffic of each node is almost equal. Finally, it is quite efficient and cost-effective to restore the normal network operational profile from the attacking maneuver after applying our PTV scheme.

Bibliography

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

[2] B. Bellur, R. G. Ogier, and F. L., “Templin. Topology Broadcast based on Reverse Path Forwarding (TBRPF),” Internet Draft. Draft-ietf-manet-tbrpf05.txt., March 2002.

[3] C. Perkins, E. B. Royer, and S. Das, “Ad hoc On-Demand Distance Vector (AODV) Routing,” Internet Draft, draft-ietf-manet-aodv.txt, 2003.

[4] Q. Xie, “Dynamic Source Routing (DSR),” Internet Draft, draft – ietf-manet-dsr.txt, 2003.

[5] Z. J. Haas, and M. R. Pearlman “The Zone Routing Protocol (ZRP) for Ad Hoc-Networks,”http://people.ece.cornell.edu/haas/wnl/Publications/draft-ietf-manet-zone-zrp-02.txt, 1999, Retrieved Date: 2007.

[6] A. Yaar, A. Perrig, D. X. Song, “SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks,” IEEE Symposium on Security and Privacy, May, 2004.

[7] S. Capkun, L. Nuttyan, J. P. Hubaux, “Self-organized Public-key Management for Mobile Ad hoc Networks,” IEEE Transactions on Mobile Computing, Vol.2, No.1, January-March, 2003.

[8] L. Zhou, Z. J. Haas, “Securing ad hoc networks,” IEEE Networks Special Issue on Network Security, November/December, 1999.

[9] P. Papadimitratos, Z.Haas, “Secure Routing for Mobile Ad hoc Networks,” Proceedings of the SCS communication Networks and Distributed Systems Modeling and Simulation Conference IEEE Communications Surveys (2002), San Antonio, TX, Jan. 27-31, 2002, pp. 2-21.

[10] Ping Yi, Zhoulin Dai, Yiping Zhong, and Shiyong Zhang, “Resisting Flooding Attacks in Ad hoc Networks,” Proceedings of International Conference on Information Technology: Coding and Computing (ITCC'05), April, 2005.

[11] Shaomei Li, Qiang Liu, Hongchang Chen, Mantang Tan, “A New Method to Resist Flooding Attacks in Ad Hoc Networks,” Wireless Communications, Networking and Mobile Computing, 2006, WiCOM 2006. International Conference on 22-24 Sept. 2006.

[12] RFC 3561, Ad hoc On-Demand Distance Vector (AODV) Routing, July, 2003.

[13] David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta G. Jetcheva, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) for Mobile Ad Hoc Networks for IPv4,” IEEE Internet Draft (2007), Feb. , 2002.

[14] “Structure of the IEEE 802.11 MAC Frames,” http://www.wireless-center.net/Wireless-Internet-Technologies-and-Applications/1925.html

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

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

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

[18] Karthik Lakshminarayanan, Daniel Adkins, Adrian Perrig, Ion Stoica, "Taming IP Packet Flooding Attacks, " Computer Communication Review 34(1): 45-50 ,2004.

[19] Thomas H. Clausen, Gitte Hansen, Lars Christensen and Gerd Behrmann ,"The Optimized Link State Routing Protocol Evaluation through Experiments and Simulation," Proceeding of Wireless Personal Multimedia Communications, September 2001.

[20] T. Clausen, P. Jacquet, A. Laouiti, P. Muhlethaler, A. Qayyum and L. Viennot,"Optimized Link State Routing Protocol," Proceedings of IEEEINMIC, Lahore, Pakistan, December 2001.

[21] J. G. Jetcheva, D. Johnson, D. Maltz, and Y. Hu., "Dynamic Source Routing (dsr)," Internet Draft, draftietfmanetdsr06.txt, Nov. 21, 2001.