Chapter 1
Introduction

1.1 Background

In this section, the background of the routing protocol and the two types of flooding attacks in Ad hoc networks are presented. Firstly, the on-demand routing processes in MANET are introduced. Secondly, the new flooding attacks - RREQ flooding attacks and DATA flooding attacks are introduced.

1.1.1 Routing Protocol in MANET

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 or any administration center. It maintains the network connection and data transmission by the cooperation and self-organization among all the mobile nodes in the network.

There are many routing protocols in MANET. We can simply classify these routing protocols into proactive routing protocol and reactive protocol according to the characteristics of the routing protocol.

One of the routing protocols is proactive routing protocol. The nodes using this type of routing protocol broadcast routing information and update its routing table according the receiving routing information on a regular time. In this kind of routing protocol, the data packets sent from source node know the routing path to the destination node without delay. However, it consumes a lot of bandwidth of wireless network since the mobile nodes have to broadcast the routing information on a regular time schedule. In order to diminish the consumption of bandwidth which caused by

broadcasting mechanism, it could lengthen the cycle of broadcast time. At the same time, the routing table is unable to react to the variation of network topology correctly. Destination Sequenced Distance Vector (DSDV) [1] is one of proactive routing protocol.

The other is reactive routing protocol. The nodes find the routing path by broadcasting route requests when they need to communicate with each other. The bandwidth consumption is less than proactive routing protocol. On the contrary, the average delay time is longer than proactive routing protocol since the valid routing information not exit in the routing table. Ad Hoc On Demand Distance Vector (AODV) [2], Dynamic Source Routing (DSR) [3] and Zone Routing Protocol (ZRP) [4] are common reactive routing protocol.

Table 1 summarizes the differences between proactive routing protocol and reactive routing protocol.

	Proactive routing protocol	Reactive routing protocol
Average Delay Time	Short	Long
Bandwidth Using	More	Less

Table 1 The Differences Between Proactive and Reactive Routing Protocol

The routing of the Mobile Ad Hoc is always the focus of attention. Meanwhile, with the appearances of many kinds of attacks, many secure routing protocols for Ad Hoc networks are proposed [5][6][7][8].

1.1.2 Overview of AODV

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 [9]. Path discovery is entirely on-demand in AODV. It allows mobile nodes to obtain routes quickly for new destinations and does not require to maintain routes information not in active communication.

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. Figure 1.1 illustrates the format of RREQ packet and Figure 1.2 is the format of RREP packet.

Type	Control Flags	Reserved	Hop Count
RREQ ID			
Destination IP Address			
Destination Sequence Number			
Source IP Address			
Source Sequence Number			

Figure 1.1 The format of Route Request (RREQ)

When a source node needs to send packets to a destination node to which it has no available route, it will broadcast RREQ packet and wait RREP packet within one round-trip time, as shown in Figure 1.3

Type	Control Flags	Reserved	Prefix Size	Hop Count
Destination IP Address				
Destination Sequence Number				
Source IP Address				
Lifetime				

Figure 1.2 The format of Route Reply (RREP)

If the node does not receive the RREP packet, it will try again to discovery route by broadcasting another new RREQ packet. After a maximum retry times at the maximum TTL value, node stop route discovery. Repeated attempts by source node at route discovery for a single destination node must obey the rule of a binary exponential backoff algorithm. The RREQ packets are broadcast in a incrementing ring to reduce the overhead caused by flooding the whole network. After a RING TRAVERSAL TIME, if no RREP packet has been received, the flooded network is enlarged by increasing the TTL by a fixed value. This procedure will repeat until an RREP packet is received by the originator of the RREQ packet, and the routing path has been found.

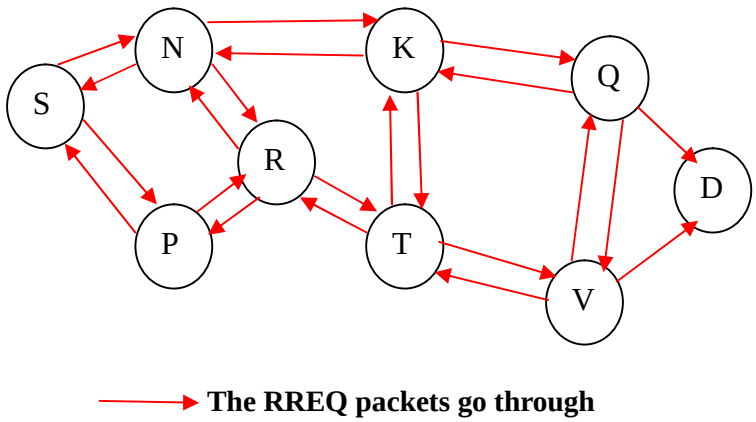
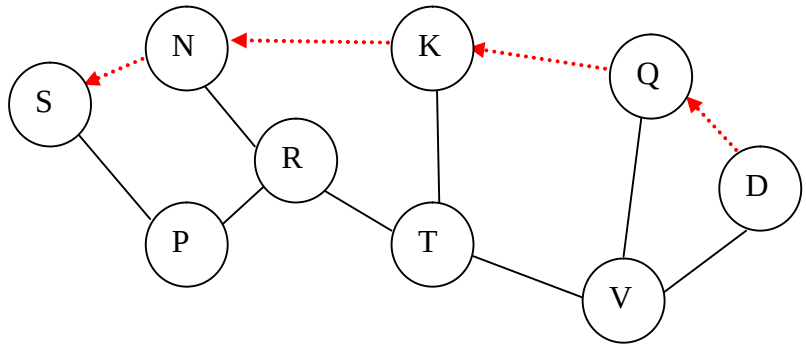


Figure 1.3 The forwarding route of RREQ.

Each node maintains a monotonically 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 receiving 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. 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, as shown in Figure 1.4



The reverse path created by RREP

Figure 1.4 The setup of routing path by RREP.

1.1.3 RREQ Packets Flooding Attack

Broadcasting RREQ packets into the whole network for discovering routing path will consume a lot of resource of network. In order to reduce the congestion in a network, the AODV protocol adopts some methods. A node can not originate RREQ messages per second more than RREQ_RATELIMIT. 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 the same node at route discovery for a single destination must utilize the binary exponential backoff algorithm. When the first time a source node broadcasts a RREQ packet, it waits roundtrip time for the reception of RREP packet which answers this RREQ. If any RREP packet is not received within that time, the source node sends a new RREQ packet. When calculating the time to wait for the RREP packet after sending the second RREQ packet, the source node must use a binary exponential backoff algorithm. Hence, the waiting time for the RREP packet corresponding to the second RREQ packet 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 RREQ 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 packet has been received, the flooded area is enlarged by increasing the TTL by a fixed value. This procedure is repeated until an RREP packet is received by the originator of the RREQ, i.e., the route has been found.

In RREQ flooding attack, the attacker who violates the above rules selects many IP addresses which do not exist in the networks as destination addresses. Then it successively originates mass 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 [10]. Figure 1.5 shows an example of RREQ Flooding Attack.

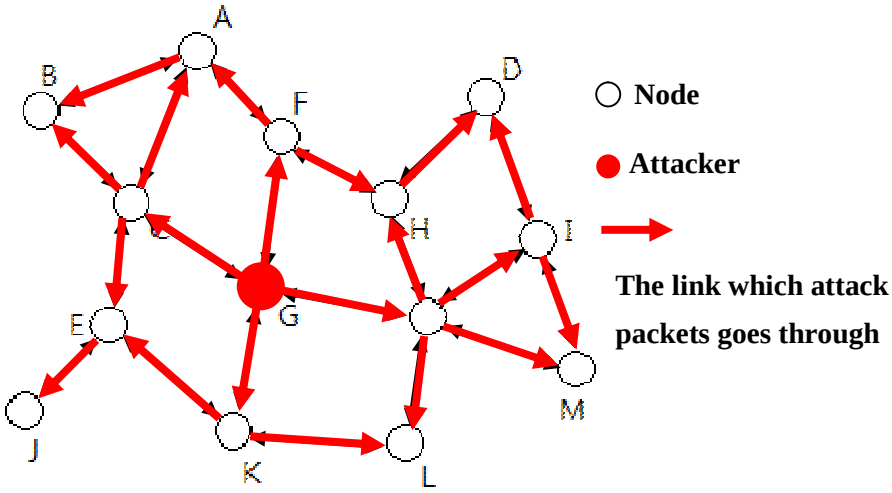


Figure 1.5 The RREQ flooding attack in Ad Hoc networks.

1.1.4 DATA Packets Flooding Attack

When nodes in MANET finish route discovery and build correct routing path to destination nodes, the source nodes send the DATA packets along these legal routing path. In DATA flooding attack, 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. Figure 1.6 shows an example of DATA flooding attack. The destination node will be busy for receiving the excessive packets from the attacker and can not work normally. The excessive data packets in the network also clog the network and deplete the available network bandwidth for communication among nodes in the network [10].

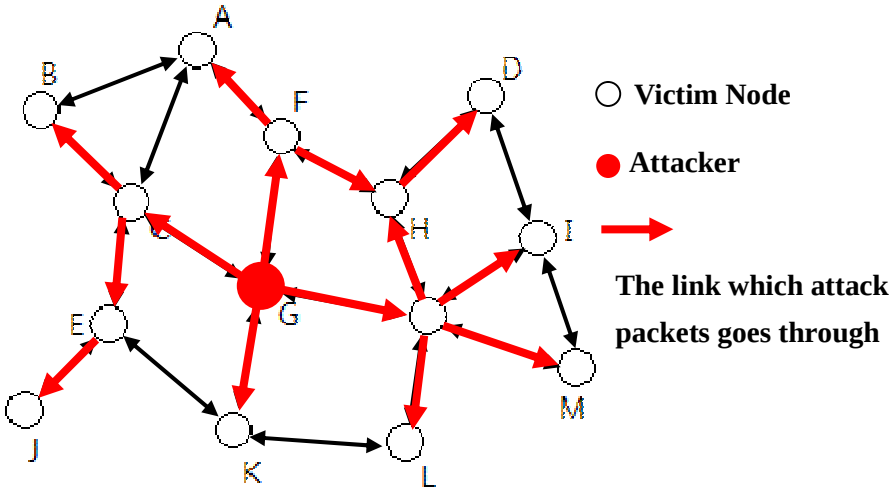


Figure 1.6 The DATA flooding attack in Ad Hoc networks.

1.2 Motivation

Recently, with the rapid growth of wireless network, more and more applications are based on Ad Hoc network. They are being deployed for a wide variety of applications, such as ad hoc meeting, military application, emergent operation and etc. When Ad Hoc network is deployed in a hostile environment, the security issue becomes extremely important. Because of the weak of hardware design for wireless devices, Ad hoc network is easily suffered attack malevolently. If these attacks are not found early enough, they will cause damages on hosts seriously.

In wired network, the attacks like Denial of Service (Dos) and Dynamic Denial of Service (DDoS) are powerful attacks. These attacks let many famous websites crash in a short time, and successfully paralyze the whole network. The flooding attacks in Ad Hoc network just like the DoS attack in wire network. Many secure routing protocols [5] [6] [7] [8] and intrusion detection mechanisms [11] [12] have been proposed to defense attacks and detect misbehaving nodes.

In 2005, Ping Yi et al. [13] first introduced this attack model and developed a Flooding Attack Prevention Scheme (FAP) to resist it. Then another scheme was proposed by Shaomei Li et al. in 2006 is called the Avoiding Mistaken Transmission Table (AMTT) [14].

Two of above schemes cost a lot of storage spaces and calculation processes, and that will be a large burden for mobile devices. For this reason, we would like to propose a new scheme to defense flooding attack caused by malicious nodes. We also want to reduce the storages and calculation in procedure of defense and inhibiting attacks effectively and quickly.

1.3 Organization of the Thesis

The rest of this thesis is organized as follows: Chapter 2 surveys the related defense schemes of flooding attack in Ad Hoc network. Chapter 3 presents the design of our proposed scheme base on priority and trust value. The analysis is shown in Chapter 4. Conclusions and future work are summarized in Chapter 5.

Chapter 2
Related Works

There are two main researches on the flooding attack in Ad Hoc network: Flooding Attack Prevention (FAP) which be proposed in 2005, Avoiding Mistaken Transmission Table (AMTT) which be proposed in 2006.

2.1 Overview of Flooding Attack Prevention

Flooding Attack Prevention is proposed firstly by Ping Yi et al. in 2005. This scheme provides two methods to defense the RREQ flooding attack and the DATA flooding attack. Neighbor suppression is used to defense the RREQ flooding attack, and Path Cutoff is used to defense the DATA flooding attack.

2.1.1 The Procedure of Neighbor Suppression

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 network. In this kind of situation, the node has been isolated from the network.

Figure 2.1.1 shows that a simple topology of mobile ad hoc network. The node T communicates with the other node through node R, K and V. If the neighbor node R, K and V refuse to receive packets from node T, node T can not send any packet to the other nodes.

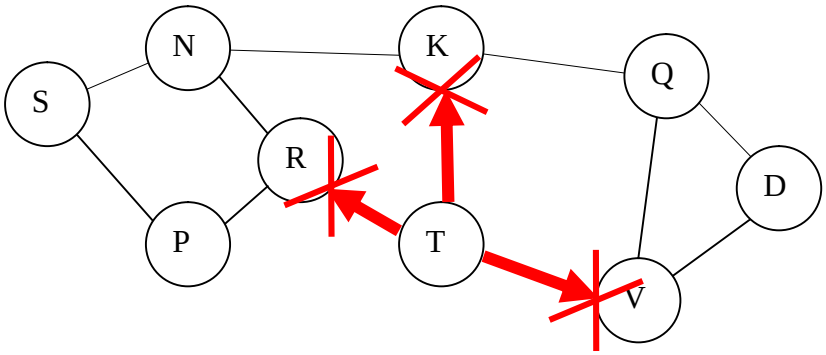


Fig.2.1.1 A simple topology of mobile ad hoc network

The method of neighbor suppression is designed according to the above feature of mobile ad hoc network. In AODV route protocol, the node disposes the RREQ packet according to the rule of “first-in, first-out” (FIFO). If the fore RREQ packets are not dealt with, the hind RREQ packets can not received. Just as this rule, the excessive RREQ packets which have arrived nodes ahead from the attacker will prevent the nodes from receiving later RREQ packets.

The method of neighbor suppression changes the rule of FIFO to the rule of priority. It uses the method of processing priority and threshold to prevent RREQ Flooding Attack. Each node in Ad Hoc network sets up the processing priority and threshold for its neighbor nodes. The priority of node is in inverse proportion to its frequency of originating RREQ packets. The threshold is the maximum of originating RREQ packets in a period time, such as 1 second. If the frequency of originating RREQ packets of the attacker exceeds the threshold, the node will not receive the RREQ packets from the attacker any more.

The method of neighbor suppression defines 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 indicated in 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.[17]

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

To clarify, we take node F and its neighbor node A, C, H, G for example in Figure 2.1.2. Node F sets up the processing priority for its neighbor A, C, H, and G. The initial values of the four priorities in node F are all set up to 1. After node A broadcasts two RREQ packets in 1 second, the processing priority of node A is changed to 1/2. If node C originates 5 RREQ packets in 1 second, the processing priority of node C is changed to 1/5. After this, if node A and node C broadcast RREQ packets at the same time, node F will firstly dispose the RREQ packet from Node A because the priority of node A is higher than that of node C. If node H broadcasts excessive RREQ packets in a period time, the priority of node H will fell very low. If the frequency 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 RREQ Flooding Attack is prevented by its neighbor nodes.

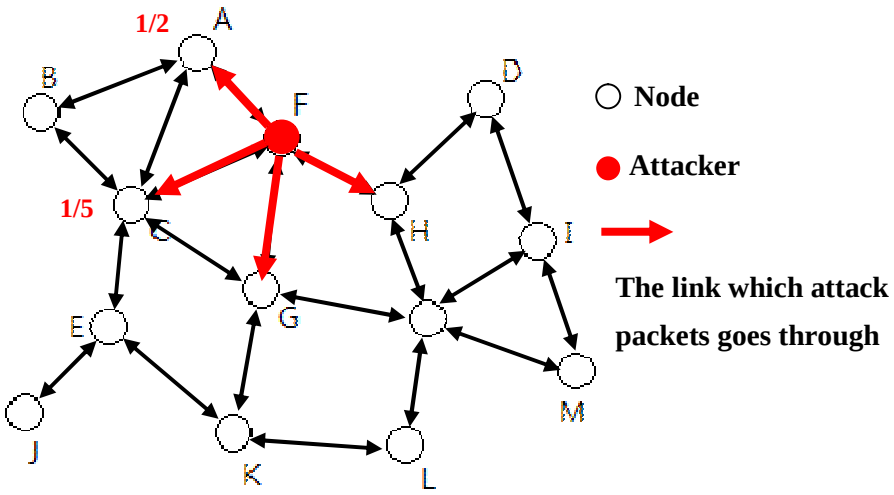


Figure 2.1.2 The procedure of Neighbor Suppression

2.1.2 The Procedure of Path Cutoff

When the attacker originates DATA Flooding Attack, the neighbor nodes is difficult to identify it for the neighbor node can not judge that a DATA packets is useless in network layer. The destination node can easily make a decision in application layer when it has received these useless DATA packets. The method of path cutoff is to prevent DATA Flooding Attack.

When the attacker originates DATA Flooding Attack, the attacker has set up a legal path from the attacker to victim node ahead. Then the attacker starts to send mass useless data packets to the victim nodes. When the victim node finds that these data packets are useless and it is the DATA Flooding Attack, he can cut off the path from the attacker in order to prevent the attacker from continuing Flooding Attack. The victim node originates RRER message to the attacker along the path which set up by the attacker. The RRER message indicates IP address of victim node unreachable. The intermediate nodes who the RRER passes through will delete the route from the

attack to victim.

The RRER message may cut off some paths which are not related with DATA Flooding Attack, and these paths may be repaired by the originate nodes hereafter. With the paths which the attacker carries out DATA Flooding Attack in virtue of are cut off gradually, the DATA Flooding Attack is terminated. Figure 2.1.3 shows the path cutoff form victim node to attacker. When these attack paths are ended, the attacker may originate RREQ in order to set up paths to the other nodes again. The other nodes can refuse to set up these routes by means of no answering RREP for these RREQ. In AODV protocol, the intermediate nodes can reply the RREQ instead of the terminal nodes if they have an active route to the destination. For this reason, the attacker can set up paths to victim through the victim node refuse to do it. To avoid this, the function which the intermediate nodes may reply the RREQ should be cancelled. Only the destination may respond to this RREQ.

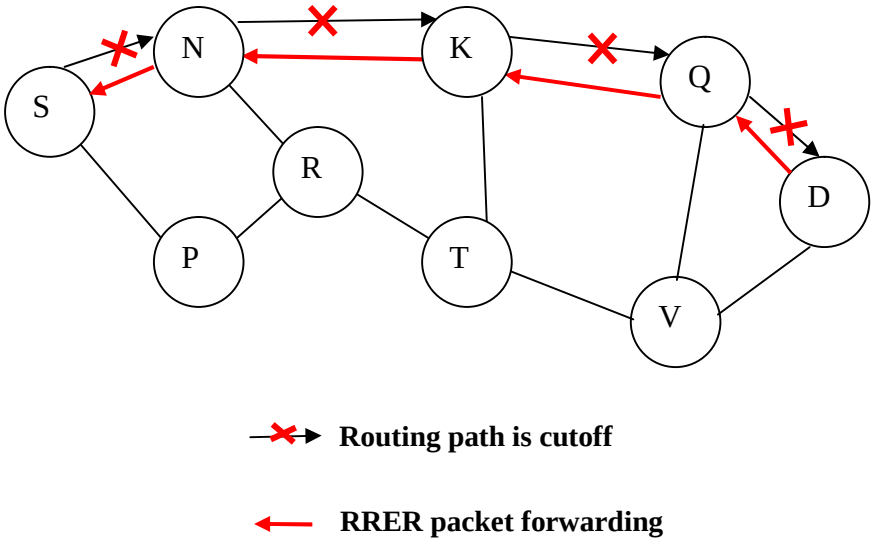


Fig.2.1.3 Path cutoff of Flooding Attack Prevention

2.2 Overview of Avoiding Mistaken Transmission Table

Avoiding Mistaken Transmission Table is proposed by Shaomei Li et al. in 2006. This scheme provides a simple and can defense the flooding attack at little cost.

2.2.1 The Format of Avoiding Mistaken Transmission Table

In AMTT scheme, each node establishes an avoiding mistaken transmission table. This table is used to record received RREQ packets and enroll existed legal communication routes.

Table 2 The Format of AMTT

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

S IP Addr: the Source IP Address;

D IP Addr: the Destination IP Address;

RREQ Num: Number of RREQ Packets;

Seq Num: Sequence Number of RREQ;

Vald Indic: Validity Indication, 1 indicates this route is legal, NULL indicates it is illegal;

Comm Rec: Number of Data Packets Passed Through;

2.2.2 The Procedure of Avoiding Mistaken Transmission Table

When node A wants to send packet to node B, it sends RREQ packet. Every node receiving this RREQ adds an item in its AMTT, fills the source IP address, destination IP address, sequence number according to the packet, and sets the RREQ Num as 1. 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 statistic to the received RREQ packets. For example, when the RREQ packet sent by node A passes through node T and node Q, these two nodes add an item in their own AMTT respectively, as in Table 3.

Table 3 RREQ Value

S IP Addr	D IP Addr	RREQ Num	Seq Num	Vald Indic	Comm Rec
A's IP	B's IP	1	s	NULL	NULL

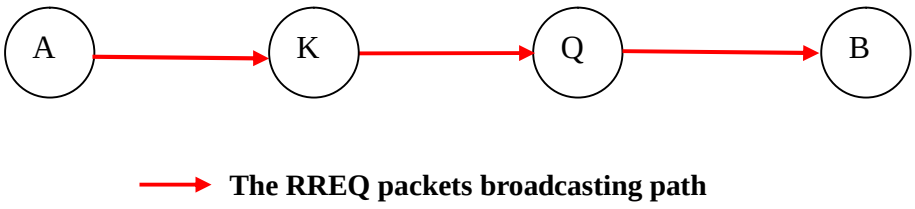


Fig 2.2.1 The nodes write the AMTT records from the RREQ passing through

After the destination node receives RREQ from the source node, it adds corresponding item in its AMTT, and then sends the RREP packet back to the source node along the routing path. 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, as in Table 4. Otherwise, they

discard this RREP packet and do not set the Validity Indication.

Table 4 Validity Indication

S IP Addr	D IP Addr	RREQ Num	Seq Num	Vald Indic	Comm Rec
A's IP	B's IP	1	s	1	NULL

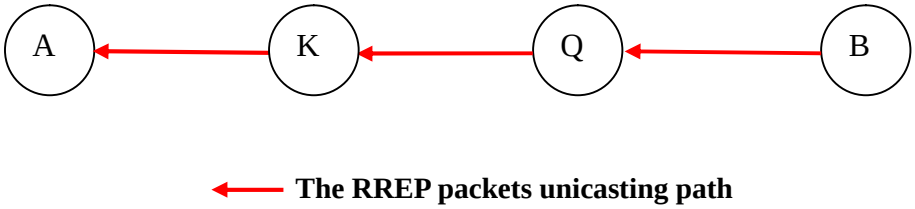


Fig 2.2.2 The nodes write the AMTT records from the RREP passing through

When a node forwards a data packet, it will set the Communication Record of the item whose source IP address and destination IP address in its AMTT to 1. In this way, whenever sending a data packet, midway nodes set the corresponding Communication Record in their AMTTs to 1, as in Table 5.

Table 5 Communication Record

S IP Addr	D IP Addr	RREQ Num	Seq Num	Vald Indic	Comm Rec
A's IP	B's IP	1	s	1	1

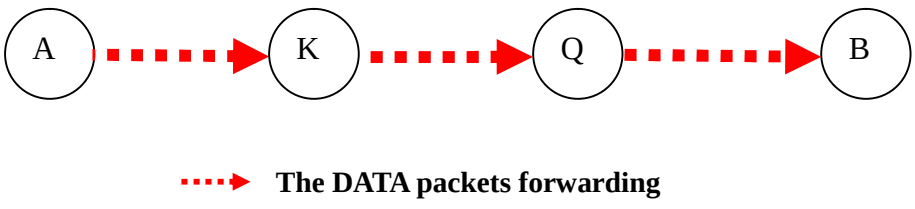


Fig 2.2.3 The midway nodes record the numbers of DATA packets passing through

Each node periodically (such as 4*(Round Trip Time)) does statistics 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. All the nodes receives RANC will delete corresponding items in their AMTTs.

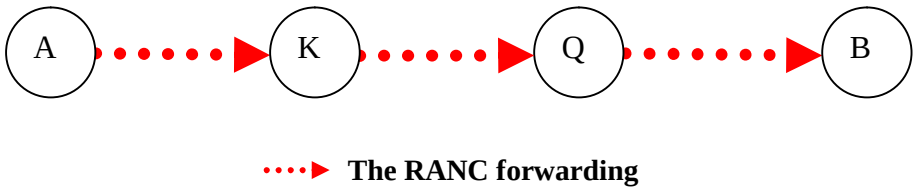


Fig 2.2.4 The nodes receive RANC and delete items of their AMTTs

Let's assume that one node T's AMTT has n items. Their Source IP Address, Destination IP Address and RREQ Num are respectively (S_i , D_i , RVQ_i) , here $0 \le i < n$. Node T periodically (such as average Round Trip Time) and ordinally statistics each source node's RVQ_{all} = (RVQ_0+ RVQ_1+ · · · +RVQ_i +RVQ_{n-1}), the RREQ number sending from S_i to all D_i (i = 0,1,.....,(n−1)). Then it will compare RVQ_{all} with its threshold, assume it is *threshold*. If RVQ_{all} overruns *threshold*, node T will search all the Validity Indication and Communication Record of the items whose Source IP Address is S_i. If all these items' Validity Indication and Communication Record are null, it can decide S_i as attacker, and refuses to forward packets from S_i 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
Priority and Trust Value Scheme

Here are three obvious characters of flooding attacks in Ad Hoc networks. The first is that the attackers broadcast mass RREQ packets ignoring the rule of RREQ_RATELIMIT. The second is that the attackers select mass fake addresses which are not in this network. The last is that the 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 cooperates with the Priority and Trust Value (PTV) and packets threshold of neighbor nodes to detect and inhibit the flooding attacks. We use “HELLO” packets to collect the status of neighbor nodes in the Neighbor Nodes List Table (NNLT) at the beginning of AODV. In order to avoid nodes faking the address or the value of hop counts, nodes also use the value of Hop Count in RREQ packet header to identify the source node address. So it is easy to inhibit flooding attacks at the first hop node and the whole networks can maintain well.

3.1 Priority and Trust Value Scheme

In Priority and Trust Value scheme, each node establishes a RREQ PTV table to record the RREQ packets passing through itself and set the Priority and Trust value (PT value) for each source node. The node can decide to forward packets or not by the Priority and Trust value. Table 6 shows the format of RREQ PTV table.

Priority and Trust value can be upgraded or downgraded according to the received packets behaviors. When attacked nodes are damaged or normal nodes are hacked, those neighbor nodes still can use the PTV scheme to reinstate the transmission or inhibit the attacks.

Table 6. Format of RREQ PTV

S IP Addr	RREQ Num	Time Stamp	RREP Num	PT Value

S IP Addr: Source IP Address;

RREQ Num: Received RREQ Numbers;

Time Stamp: Time Stamp; the time when first RREQ packet be received;

RREP Num: Received RREP Numbers;

PT Value: Priority and Trust Value;

The DATA PTV records the status of DATA packets passing through. It also records the numbers of DATA packets with the same source and destination addresses. The nodes can hold and queue DATA packets if the value of DATA Num is over the DATA threshold. And then the nodes will wait for the answers from the destination node. If the nodes receive any error message, the value of PTV will be set as 0 and block the connection. Else it will be set as 1 and the transmission is continued.

Table 7. Format of DATA PTV

S IP Addr	D IP Addr	DATA Num	PT Value

S IP Addr: Source IP Address;

D IP Addr: Destination IP Address;

DATA Num: DATA packet Numbers;

PT Value: Priority and Trust Value, 0 means this node is an attacker, 1 means this node is normal;

3.2 Neighbor Nodes List Table (NNLT)

The nodes in mobile Ad hoc network broadcast “HELLO” packets to find the neighbor nodes around themselves. 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.

According to the AODV protocol, the nodes also broadcast “HELLO” packets periodically to check if its neighbors are still available. In PTV scheme, the nodes record the neighbor’s IP address in the PTV table when they exchange “HELLO” packets. By this way, the nodes will delete the record when its neighbor node is dead (node remove away or do not answer the “HELLO” packet).

The nodes also can collect the same information when they receive RREQ packets. And by this way, the nodes can prevent the attacker from faking its address for cheating and reduce the storage space of the PTV table. Table 8 shows the format of Neighbor Node List Table (NNLT).

Table 8. Format of Neighbor Node List Table (NNLT)

N IP Addr	LOD	PT Value

N IP Addr: Neighbor node IP Address;

LOD: Live or Dead; 0 as Live, 1 as Dead;

PT Value: Priority and Trust Value from RREQ PTV;

For example, there are three nodes (node *x*, *y*, *z*) around node *k*. When the nodes exchange “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. NNLT also records those nodes LOD (Live or Dead) status. Node *k* can then delete PTV of nodes

since LOD value is 1. Figure 3.2.1 shows the procedure of NNLT and Table 9 shows the records in NNLT after the nodes exchange "HELLO" packets. And the PT Value will be written according the value of RREQ PTV table.

When a new node *m* adds, it will also obey the rule of protocol and exchange "HELLO" packets first. So the NNLT of node *k* will add a new record of node *m.* If node *m* do not obey this rule and start to send RREQ packets to node *k.* Node *k* will drop all RREQ packets from node *m*, because node m do not in its NNLT. And node *k* can stop flooding attack at the beginning of AODV protocol.

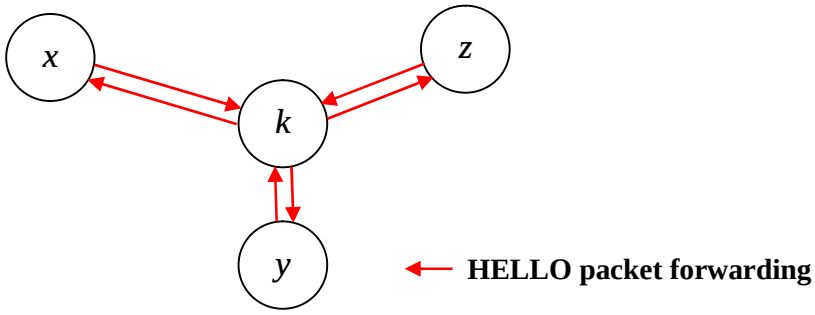


Fig.3.2.1 The procedure of Neighbor Nodes List Table

Table 9 The records in NNLT after the nodes exchange "HELLO" packets

N IP Addr	LOD	PT Value
x's IP address	0	
y's IP address	0	
z's IP address	0	

3.3 The Definition of RREQ Threshold

In the normal scenario (without any attacks), each node uses RREQ RATELIMIT to limit the frequency to broadcast RREQ packets. If the frequency of received RREQ packets is over this default limit, the node will stop forwarding RREQ packets to its neighbors. In order to exhaust all network resource, the attack node will ignore the rate limits and SEND MASS RREQ packets to its neighbors in the attack scenario.

We assume that the node has ***n*** neighbor nodes collecting from NNLT. And according to the definition of RFC 3561 [15], the default sending frequency of RREQ packets for each node must be RREQ_RATELIMIT. So we can get the max RREQ packets from its neighbor nodes at the same time is ***n****RREQ_RATELIMIT. By this, we define the Max and Min RREQ Threshold for each node as (1)(2).

Max Threshold = *nRREQ_RATELIMIT** (1)

Min Threshold = RREQ_RATELIMIT (2)

n are the numbers of neighbor nodes.

RREQ_RATELIMIT is defined by RFC 3561 and the default value is 10. [15]

3.4 The Definition of DATA Packets Threshold

We assume that there are no any traffic packets appearing in the whole network, and the complete link bandwidth between source node and destination node is only used for the transmission of data packets. So we decide the Max DATA packets threshold according to the default Maximum Transmission Unit (MTU) of 802.11 by [16]. And the DATA threshold for each node we defined is (3).

$$\textbf{DATA Threshold} = \frac{Bandwidth}{MTU} \Big/ n \qquad (3)$$

Bandwidth is the bandwidth of 802.11*x*, like 802.11b for 11Mbps.

MTU is the default maximum transmission unit of 802.11*x*, and the default value is 2272 bytes.

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. And this formula will cost very little computation for each node.

3.5 The Level of Priority and Trust Value

We define three levels of Priority and Trust Value. Level 0 is the lowest; it means that this node is trustless and it is an attacker. The nodes neighboring to this node should refuse forwarding any packets form it. Level 1 is low; it means that this node is not worthy to trust. The nodes neighboring to this node should hold RREQ packets and forward these RREQ by the rule of RREQ_RATELIMIT. Level 2 is the normal; it means that this node is normal and trustable. The nodes neighboring to this node would forward RREQ packets for it directly. Table 10 shows the three level of priority and trust value.

Table 10 The Three Level of Priority and Trust Value

Level	Status	Actions for this level
0	lowest	the node refuses forwarding any packets from it
1	low	the node hold packets and forward packets by the rule of RREQ_RATELIMIT
2	normal	the node forward packets directly

3.6 The Procedure of Priority and Trust Value Scheme

3.6.1 The Procedure to Inhibit the RREQ Flooding Attack

At the beginning of Ad Hoc networks, the nodes exchange “HELLO” packets and write the information of its neighbor nodes into Neighbor Nodes List Table (NNLT). But now the value of PTV is null.

When the nodes start to connect with each other, they broadcast RREQ packets firstly. Then the nodes will receive the RREQ packets which broadcasted from its neighbor nodes. After receiving RREQ packets, the node will compare the source address at the header of RREQ packets with NNLT. If the source node address is already in NNLT, the node will process the next procedure. Else the node will drop the RREQ packets because of the source node address is faked.

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 Priority and Trust Value. 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.

Fig 3.6.1 shows the workflow of the RREQ Priority and Trust Value

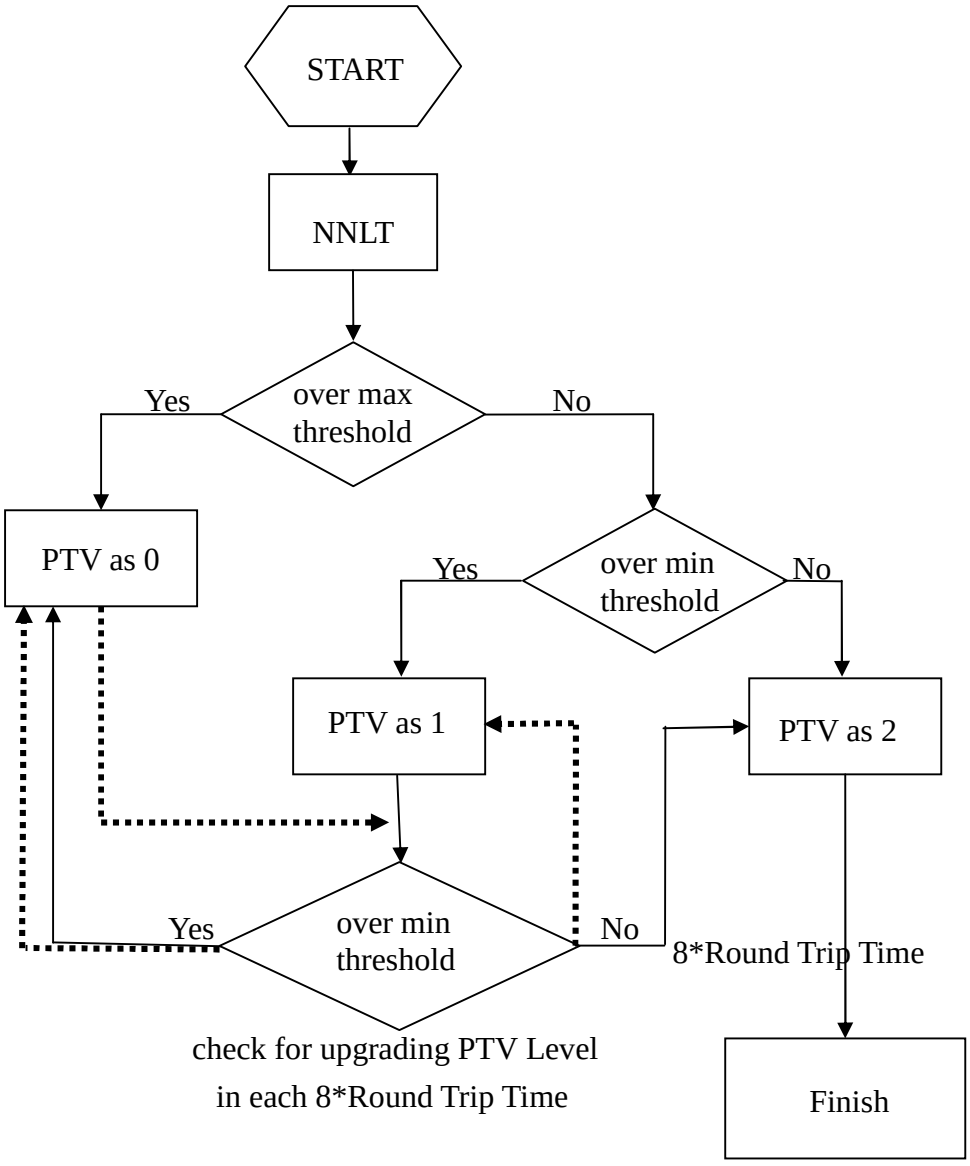


Fig 3.6.1 The Simple Workflow of the RREQ Priority and Trust Value

3.6.2 The Procedure to Inhibit 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 PT 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 RRER packets. If the node receives any RRER 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 RRER 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 RRER 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 RRER packets and the receiving DATA packets numbers is over DATA Threshold.

By this way, the node can reduce the mass DATA packets flooding into the network and stop the DATA flooding attacks in advance. And the node can detect and inhibit DATA flooding attacks by using this mechanism. Fig 3.6.2 shows the workflow of the DATA Priority and Trust Value

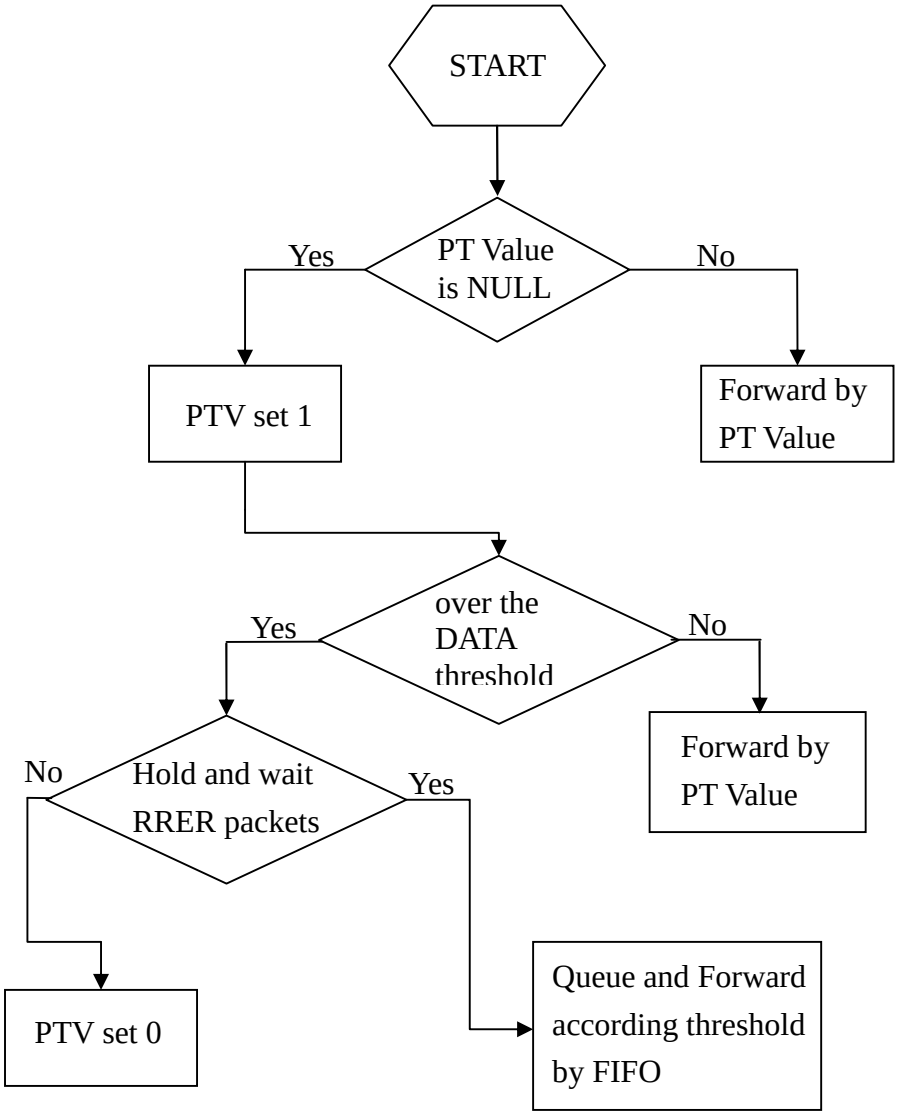


Fig 3.6.2 The Simple Workflow of the DATA Priority and Trust Value

Chapter 4
The Analysis

4.1 Comparison of FAP and AMTT

Most nodes in Ad hoc networks have little calculating ability because of their limited hardware designs. In FAP, to compare each RREQ's priority depended on its sender's frequency of sending RREQ to decide the forwarding order is only effective when the traffic in the network is heavy. In FAP each node must make records for every RREQ packet it receives and the reserve space to calculate sending frequency for its neighbor nodes. Calculating frequency is a complicate process, which will burden mobile nodes in Ad Hoc networks.

As to the data flooding attack, the FAP scheme employs passive defense. It works when the data flooding attack is happened and detected. If many attackers set up routes with many legal nodes and send large sums of useless data packets simultaneously, to implement this scheme will cost a lot, and easily leads to overwhelming consequences.

If two or more attack nodes cooperate with each other in the network and set up links to send massive useless data packets, they will cause data flooding in the Ad Hoc network. In this situation, the RRER packets will never appear and the legal nodes cannot sense the data flooding attack. And then the Path Cutoff can not work correctly. Such flooding attacks cannot be defended by the FAP scheme.

Because of the limits of hardware designs, the nodes in Ad Hoc networks have little storage spaces. In AMTT scheme, each node uses AMTT records to distinguish the flooding attacks. If there are many nodes in the networks and each node needs to communicate with each other, the AMTT records in each node should cost a lot of

storage spaces. Although the AMTT scheme has a mechanism to delete the AMTT records periodically in order to avoid broken links which nodes are removed away or by other reasons occupied the storage spaces. According AMTT rules, every link record will be deleted when it receives the RNAC sent by the source node. If there has any intermediate node holding the RNAC or keeps increasing the Communicate Record value maliciously, the route information will be kept in node for a long time and the storage in the node will be consumed.

The AMTT scheme can distinguish attacks according to the RREP packets sent back by the destination node. The midway nodes in the routing path will set Vald Indic value as 1 and identify the route as legal. It also collects the RREQ receiving numbers from all nodes in the networks. Each node computes the average RREQ received numbers of each source node as the RREQ threshold. If a node receives the RREQ numbers is over the threshold and Vald Indic value is NULL, the node send RREQ packets will be treated as the attacker and refuses forwarding packets for it.

In the Ad Hoc network, it is difficult to collect information from all nodes in the networks. And if the destination node cooperates with the attack node and also sends the legal RREP packets back, the midway nodes can not differentiate this kind of RREP packets. And the flooding attack can slip into the networks.

4.2 Analysis of Our Scheme

After comparing with FAP and AMTT, we find out that the AMTT scheme needs a lot storage spaces to record the collected information, and the FAP scheme needs a complex computation process. So we analysis both schemes and our propose scheme with two dimensions in the two flooding attack: the storages and the computation.

We assume that there has an ad hoc network with n nodes and each node has m nodes around itself, and $n > m$. In FAP, each node needs to record m records for the RREQ packets which pass through it and do the complex computation processes for the receiving frequency as node's RREQ priority.

In AMTT scheme, each node needs to create the AMTT for recording the RREQ and DATA packets passing through. If all nodes in the Ad Hoc networks need to communicate with each other, the each node needs to record $(n\text{-}1)^2$ records in its AMTT. That will cost large storage spaces for these AMTT records.

The AMTT scheme also needs to calculate the average received RREQ numbers from all nodes as threshold. This procedure also still cost a lot of computation processes, but it is better than the FAP scheme.

In our scheme, like the FAP scheme, the node only records the information neighboring itself. Each node only uses m records for the RREQ PTV. The DATA PTV needs $m*(n\text{-}1)$ records. But the records of DATA PTV can be simplified less than each four of Round Trip Time. The Max RREQ Threshold, Min RREQ Threshold and the DATA Threshold in our scheme are only using simple calculation formula than the other two schemes. So our scheme cost less computation than FAP and AMTT.

We compare three schemes with resisting RREQ flooding attack and DATA flooding attack. In FAP scheme, it uses m records and complex calculation to resist

the RREQ flooding attack. But the FAP scheme uses the weak judging function to resist the DATA flooding attack, and it can not resist flooding attacks especially when two attack nodes work together.

In the AMTT scheme, it uses $(n\text{-}1)^2$ records to resist the RREQ flooding attack. And the AMTT scheme also use a lot computation for deleting useless records and setting the threshold.

In our proposed scheme, it uses *m* records to inhibit the RREQ flooding attack and *m**(*n*-1) records to inhibit the DATA flooding attack. Our scheme also uses the simple calculating function to set the threshold. Table 11 and Table 12 show the comparison of FAP, AMTT and our proposition. After the analysis, our Priority and Trust Value Scheme is better than FAP and AMTT.

Table 11 The Comparison of FAP, AMTT and PTV in resisting RREQ flooding attack

	The used storage spaces	The quantity of calculation
FAP	*m*	complex
AMTT	$((n\text{-}1)^2)$	little
PTV	*m*	few

Table 12 The Comparison of FAP, AMTT and PTV in resisting DATA flooding attack

	The used storage spaces	The quantity of calculation
FAP	*None**	None*
AMTT	$((n\text{-}1)^2)$	little
PTV	*m*(n-1)*	few

Chapter 5

Conclusions and Future Work

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 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 costs more little storage spaces and little computation.

The major contributions of our scheme are described as follows:

1. Our scheme detects and stops the flooding attack from the first node which neighboring to the attack node. This let nodes inhibit flooding attack more quickly.
2. Our scheme can inhibit the flooding attack launched by two or more attack nodes working together.
3. Our scheme utilizes few storage spaces and little calculation. The nodes in Ad Hoc network only record N nodes information, where N is the number of nodes neighboring to itself. This is more suitable to be used in LANs in which the traffic of each node is almost equal.
4. Our scheme let nodes recovering from misbehavior still work normally by upgrade

and downgrade function.

5. Compared with FAP and AMTT, our scheme also does not change any protocol structure and the whole network works as normal when suffering the flooding attack.

This thesis considers how neighbor nodes can detect the misbehaviors of attackers by using PTV. Based on this, we will do research in the future to exchange PTV for nodes in Ad Hoc networks. And all nodes can prevent the flooding attack at the beginning by virtue of the exchange of PTV.

Bibliography

[1] C. Perkins, and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing for mobile computers", *Proceedings of the Symposium on Communication Architectures and Protocols*, pages: 234-244, August, 1993

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

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

[4] 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: 2007-9-30.

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

[10] David B. Johnson, David A. Maltz, Yih-Chun Hu, and Jorjeta G. Jetcheva, “The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR), “ Internet-Draft, draft-ietf-manet-dsr-07.txt, February , 2002, Work in progress.

[11] A. Hasswa, M. Zulkernine, and H. Hassanein, “Routeguard: An Intrusion Detection and Response System for Mobile Ad Hoc Networks,” *WiMob’2005, IEEE International Conference*, Volume 3, Pages: 336 – 343, August, 2005.

[12] L. Stamouli, P. G. Argyroudis, and H. Tewari, “Real-time intrusion detection for ad hoc networks,” *WoWMoM 2005 Sixth IEEE International Symposium*, Pages: 374 -380, June, 2005.

[13] Ping Yi, Zhoulin Dai, and Yiping Zhong, et.al, “Resisting flooding attacks in Ad Hoc networks,” In *proceedings of International Conference on Information Technology: Coding and Computing (ITCC'05)*, April, 2005.

[14] 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 Page(s):1 – 4.

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

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

[17] Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong, “A New Routing Attack in Mobile Ad Hoc Networks,” *International Journal of Information Technology 2003,* Pages: 83 -94, Vol. 11 No. 2.