A Priority and Trust Value Scheme to Inhibit the Flooding Attack in Ad Hoc Networks

Yi-Hsing Lin
Department of Computer Science,
Tunghai University, Taiwan
g95290007@thu.edu.tw

Chu-Hsing Lin
Department of Computer Science,
Tunghai University, Taiwan
chlin@thu.edu.tw

***Abstract*—Mobile ad hoc networks often deployed in many kinds of environments and the nodes in the network are unattended and have weak physical protection against attacks. Mobile ad hoc networks are particularly vulnerable to Denial of Service attacks. Flooding denial of service attacks are new and powerful attacks against on-demand Ad Hoc routing protocols. At present, the single scheme proposed to resist such attack is Flooding Attack Prevention proposed in 2005. And another new scheme to resist this kind of attacks be proposed in 2006 is Avoid Mistaken Transmission Table. In this paper, 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 packages for them, in this way flooding attacks can be defended. Through analysis, we show that our scheme can inhibit flooding attacks at less cost and is more efficient.**

***Index Terms*— Flooding attack, FAP, AMTT, Trust and Priority Value, NNLT, RREQ threshold, DATA threshold, upgrade and downgrade.**

I. 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 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. The routing of the Mobile Ad Hoc is always the focus of attention. Several mature and widely-used routing protocols include OLSR[1], DSR[2], TBRPF[3], AODV[4] and so on. Meanwhile, with the appearances of many kinds of attacks, many secure routing protocols for Ad Hoc networks are proposed [5][6][7][8].

In wire-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 a new 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.[9] 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. is called the Avoiding Mistaken Transmission Table (AMTT)[10].

We present Priority and Trust Value (PTV) scheme to mend the weakness of FAP and AMTT. 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 RREQ. And so nodes can effectively distinguish attacks and refuse to forward packages for them. By this way, flooding attacks are defended.

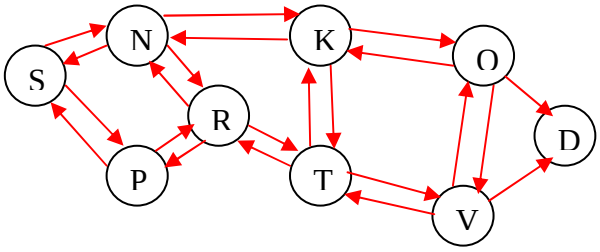
Our main contribution is to control RREQ and DATA packets according PTV scheme at nodes without changing the original AODV protocol. PTV is based on the numbers and frequency of receiving packets. We also design an upgrade and downgrade scheme for each node priority and trust value for the normal nodes which act like abnormal nodes. It is a recovery scheme for any node that is normal but acts like an attacker.

II. Related Work

A. Overview of ADOV protocol

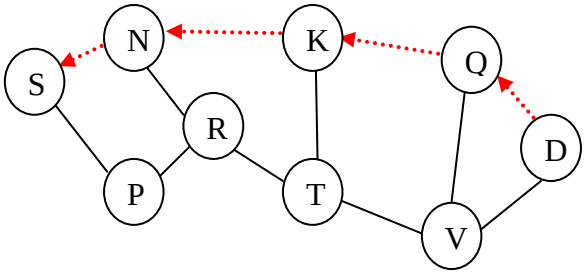
The Ad Hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an Ad hoc network [11]. Path discovery is entirely on-demand in AODV. It allows mobile nodes to obtain routes quickly for new destinations 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. 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 Fig.1. 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.

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 Fig.2



The RREQ packets go through

Fig.1 The forwarding route of RREQ.



The reverse path created by RREP

Fig. 2 The setup of routing path by RREP.

B. Flooding attack in Mobile Ad hoc network

Two typical kinds of flooding attack is the RREQ flooding attack and the DATA flooding attack. In RREQ flooding attacks, the attacker 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 [12]. 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.

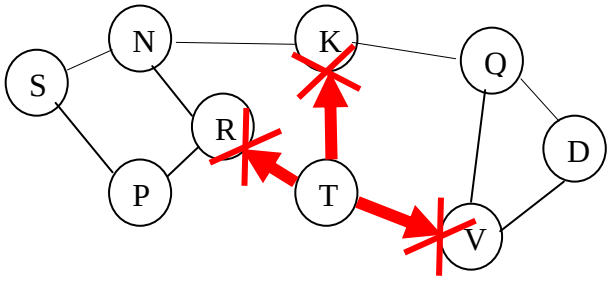
The excessive data packets in the network clog the network and deplete the available network bandwidth for communication among nodes in the network [12].

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 network will be broken out quickly.

C. Overview of FAP and AMTT scheme

- FAP (Flooding Attack Prevention)

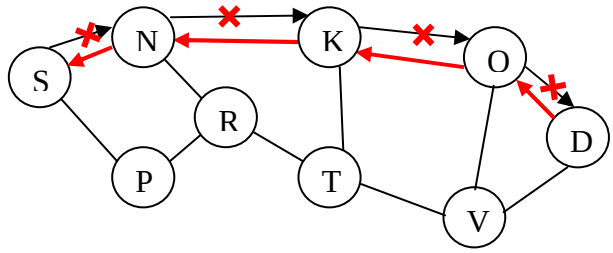
Flooding Attack Prevention (FAP) is a generic defense against the Ad Hoc Flooding Attack in mobile ad hoc networks developed by Ping Yi et al. at 2005.[10] FAP using two methods to stop the Ad Hoc Flooding Attack. Neighbor suppression is used to prevent the RREQ flooding attack and Path Cutoff is used 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 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.3.



✕Block the RREQ broadcasting by 1/Freq

Fig.3 Neighbor suppression of FAP

When the attacker activates the DATA Flooding Attack, the neighbor nodes are difficult to identify it because the neighbor nodes can not judge whether a DATA packets is useless in the network layer. The destination node can easily make a decision 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 continuing Flooding Attack from the attacker. The victim node originates the RRER message back to the attacker. The RRER message indicates IP address of victim node unreachable. The intermediate nodes which the RRER passes through will delete the route from the attack to the victim node. The RRER 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. In order to avoid attacker rebuild routes to other nodes, only the destination node can respond RREQ packets.



Routing path is cutoff

RRER packet forwarding

Fig.4 Path cutoff of FAP

- AMTT (Avoiding Mistaken Transmission Table)

In the AMTT 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.

Table1. 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 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. 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 packages.

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. 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.

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. In this way, whenever sending a data package, midway nodes set the corresponding Communication Record in their AMTTs to 1. 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.

III. Analysis of FAP and AMTT

1) Most nodes in Ad hoc networks have few calculating ability because of their limited hardware designs. And 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. Each node must make record for every RREQ it receives and 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.

2) 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 packages simultaneously, to implement this scheme will cost a lot, and easily leads to overwhelming consequences.

3) If two or more attacking nodes cooperate in the network, and set up links to send massive useless data packages, they will cause data flooding in the Ad Hoc network. If both sender and receiver are illegal nodes, the RRER packets will never appear and the legal nodes cannot sense it and so Path Cutoff can not work. So such attacks cannot be defended by the FAP scheme.

4) Because of the limit of hardware, nodes in Ad Hoc networks have few storage spaces. Each node has AMTT record to distinguish attacks. If there are many nodes and each node needs to communicate with each other, the AMTT record should cost a lot of storage spaces. Although AMMT has a mechanism to delete the AMTT record periodically to avoid broken links because that their nodes are removed away or by other reasons. According AMTT rules, every link record will be deleted when the source node send RNAC back. If any intermediate node holds the RNAC or keeps increasing value maliciously, the routes information will be kept in node and the storage will be consumed.

5) The AMTT can distinguish attacks according to the RREP packet 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 RREQ received numbers from

all nodes in the networks. Each node computes the average RREQ received number of each source node as the RREQ threshold. If a node receives the RREQ number over the threshold and Vald Indic value is 0, the node sent RREQ packets will be treated as the attacker and packets forwarded by it will be refused. But in the Ad Hoc network, it is difficult to collect information from all nodes in the networks. And if the destination node cooperated with attack node also sends legal RREP packets back, the midway nodes can not differentiate this kind of RREP packets. And so the flooding attack can slip into the networks.

IV. Our Scheme

There are obvious factors of flooding attacks in Ad Hoc networks. First, the attackers broadcast mass RREQ packets ignoring the rule of RREQ_RATELIMIT. Second, the attackers select mass fake addresses which are not in this network. Third, 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 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 inhibit flooding attacks at the first hop node and the whole networks can maintain well.

A. Priority and Trust Value Scheme

In the PTV scheme, each node establishes 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 behaviors. When attacked nodes are damaged or normal nodes are hacked, those neighbor nodes still can use the PTV scheme to reinstate transmission or inhibit the attacks.

Table2. 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 PTV of DATA 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 PTV will be set as 0 and the connection is blocked, else it will be set as 1 and the transmission is continued.

Table3. 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 package Numbers;
PT Value: Priority and Trust Value, 0 means this node is an attacker, 1 means this node is normal;

B. 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 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.

Table4. 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;

C. 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 (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. [11]

D. The definition of DATA packages Threshold

We define the Max DATA package threshold according to the default MTU of 802.11 by [13]. We define DATA threshold for node as (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 802.11x, and the 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.

E. 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 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.

F. The procedure of PTV scheme

At the beginning of Ad Hoc networks, nodes exchange "Hello" packets and write the status of neighbor nodes into NNLT. But now the value of PTV is null.

The node receives RREQ packets broadcast from the neighbor nodes. The node will compare the source address at RREQ with NNLT. If the source node address is already in NNLT, the node will process the next procedure or drop RREQ packet if the source node address is fake.

The node will write the status of received RREQ packets into PTV when its source node address is in NNLT. But if the source node status is already in PTV, the node will forward or drop it according to the value of Priority and Trust Value. The first record of the source node in PTV is set as 2 (normal).

If the received frequency of RREQ is over the Max Threshold, 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 received frequency of RREQ is over Min Threshold but not over Max Threshold, the node will forward RREQ packets and wait for any RREP packets sending back in two of Round Trip Time (RRT). If no RREP is sent back, the node will downgrade Priority and Trust Value as 1(low), or maintain the original value. If after another two of RRT, there are still no RREP sending back, the node will downgrade Priority and Trust Value as 0(lowest) and block this connection with this source node, else it will keep PTV as 1.

If the received frequency of RREQ is not over the Min Threshold, the node will set the Priority and Trust Value as 2(normal) and forward RREQ packets directly. All the nodes will run this procedure to inhibit RREQ flooding attacks.

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

If in periodically time such as 1 second, the received frequency of DATA packages coming from the same source address is over the DATA Threshold, the node will hold this connection and wait. If the node receives any RRER packets for this source address, then the node will set PTV as 0, else it will queue and forward DATA packages obeying the DATA Threshold by FIFO. It does not mean that no DATA flooding attack occurs if no RRER packets are sent back. This kind of situation could happen when the source and destination nodes are cooperated or any midway nodes keep the RRER packets. In order to avoid the DATA flooding attacks from occurring, the nodes control the DATA packages forwarding rate for situation that the node does not receive any RRER packets but the received DATA packages numbers is over DATA Threshold.

The node can reduce the mass DATA packets flooding into the network and stop the DATA flooding attacks in advance. By this mechanism, the node can detect and inhibit DATA flooding attacks.

V. Analysis

Our PTV scheme uses NNLT and PTV for nodes in Ad Hoc networks to detect and inhibit the flooding attack. The nodes which are hacked or infected by the hacker or virus can work after being repaired through the upgrade and downgrade function. The NNLT, RREQ PTV and DATA PTV of nodes only record the status of its neighbor nodes. Our scheme is better than FAP because PTV scheme do not need to calculate the sending frequency of nodes and set the priority of node according the inverse proportion to this frequency. So it costs a few storage spaces and calculation processes, and it inhibits flooding attack rapidly. Another way, our PTV scheme do not like AMMT needs to wait the RREP sent back to ensure the attack behavior or not. The attacks are detected and stopped immediately, and so that the whole network works as if no attacks occurred.

The figure and table can be displayed in the article or attach in the end of reference. The figure and table should be closed to the mention position if they are shown in the article. A large figure and table can cross two columns. The caption of figure and table should be described in the bottom and top of themselves respectively.

VI. Conclusion

In this paper, the PTV scheme is proposed to inhibit flooding attacks on the responsive routing. This scheme is simple and can defend flooding attacks at very little cost. Compared with the FAP and AMTT scheme, this scheme needs little calculation and is more suitable to be used in LANs in which the traffic of each node is almost equal. Especially, the PTV scheme stops the attack at the first node neighboring the attacker and do not change any protocol structure.

This paper only considers how neighbor nodes 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. So all nodes can prevent the attack at the beginning by virtue of the exchange of PTV.

REFERENCE

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

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

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

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

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

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

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

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

[9] 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

[10] 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

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

[12] 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

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