IDMA: Improving the Defense Against Malicious Attack for Mobile Ad Hoc Networks Based on the ARIP Protocol

Chaorong Peng[1] Chang Wen Chen[2]
[1]Dept. of Electrical and Computer Engineering, Florida Institute of Technology, Melbourne, FL 32901
[2]Dept. of Computer Science and Engineering, State University of New York at Buffalo, Buffalo, NY 14260
Email: cpeng@fit.edu; chencw@buffalo.edu

ABSTRACT

Malicious nodes are mounting increasingly sophisticated attacking operations on the Mobile Ad Hoc Networks (MANETs). This is mainly because the IP-based MANETs are vulnerable to attacks by various malicious nodes. However, the defense against malicious attack can be improved when a new layer of network architecture can be developed to separate true IP address from disclosing to the malicious nodes. In this paper, we propose a new algorithm to improve the defense against malicious attack (IDMA) that is based on a recently developed Assignment Router Identify Protocol (ARIP) for the clustering-based MANET management. In the ARIP protocol, we design the ARIP architecture based on the new Identity instead of the vulnerable IP addresses to provide the required security that is embedded seamlessly into the overall network architecture. We make full use of ARIP's special property to monitor gateway forward packets by Reply Request Route Packets (RREP) without additional intrusion detection layer. We name this new algorithm IDMA because of its inherent capability to improve the defense against malicious attacks. Through IDMA, a watching algorithm can be established so as to counterattack the malicious node in the routing path when it unusually drops up packets.

We provide analysis examples for IDMA for the defense against a malicious node that disrupts the route discovery by impersonating the destination, or by responding with state of corrupted routing information, or by disseminating forged control traffic. The IDMA algorithm is able to counterattack the malicious node in the cases when the node lunch DoS attack by broadcast a large number of route requests, or make Target traffic congestion by delivering huge mount of data; or spoof the IP addresses and send forge packets with a fake ID to the same Target causing traffic congestion at that destination. We have implemented IDMA algorism using the GloMoSim simulator and have demonstrated its performance under a variety of operational conditions.

Keywords: MANET, DoS, Assignment Router Identify Protocol, Clustering, Security Attack

1. INTRODUCTION

Current Mobile Ad Hoc Networks (MANETs) are seriously vulnerable to a variety of attacks from malicious nodes since MANETs has been assumed to rely on the protocols that use nodes as routers and to set up traffic with control messages which can be easily compromised by malicious nodes in the un-trusted network environment. For MANETs, it is obvious that the malicious attacks will cause energy consumption to grow and overhead will increase significantly for each node. This will in turn cause possible violation of maximum delay communication specifications. Furthermore, as overhead grow indefinitely, the energy consumption at some nodes may be exhausted. When this happens, some of the packets arriving at these nodes will have to be discarded and need retransmission, thereby wasting scarce communication resources. As a result, a phenomenon similar to a black hole in the traffic may occur and the network throughout will be reduced because of excessive packet delay.

Here, we list some of the critical networking performance parameters that are affected by Malicious Attacks with respect to mobile nodes:

- **Packets delay:** as Malicious Attacks continues, it will affect other normal nodes routing discovery operation and cause packets drop. As the result, it is a significant increase in the measurement of packets delay for nodes in MANETs.

- **Packets loss rate:** as Malicious Attacks continues, buffer space at some nodes may be exhausted. Packets arriving at these nodes will have to be discarded. As a result, it is a significant increase in the measurement of packets loss rate for nodes in MANETs.

Mobile Multimedia/Image Processing, Security, and Applications 2008
edited by Sos S. Agaian, Sabah A. Jassim, Proc. of SPIE Vol. 6982
698208, (2008) · 0277-786X/08/$18 · doi: 10.1117/12.783063

- **Collision rate:** as Malicious Attacks continues, nodes are obliged to accept unusual amount of messages. As a result, it is a significant increase in the measurement of the collision rate in MANETs.

- **Energy consumption:** as Malicious Attacks continues, nodes operate on unusual amount messages. As a result, it is a significant consumption of overload battery power of mobile nodes in MANETs.

A number of conventional schemes for the defense against a variety of Malicious Attacks in ad hoc network are based on adapting the basic on-demand routing protocol design for use in mobile wireless ad hoc networks. We present in this paper the design and evaluation of a new defense scheme against a variety of Malicious Attacks based on the ARIP routing protocol [2].The ad hoc wireless network is based on one source node and one destination node architecture. The source node needs to discover routing path based on either on-demand routing protocol (i.e. AODV [3]) or hybrid routing protocol (i.e. ZRP [4], DHMRP [1] and ARIP [2]).

In ARIP, Intelligent ClusterHead Agencies (ICHAs) establish multi routing path based on hierarchical clustering. ICHAs exchange routing information via gateway which rely on the reply path. This gateway node between ICHAs can obstruct proper routing by modifying routing information in network which is called impersonal attack [10]. And if a router who is actually a malicious node can drop up data packet or transmit data packets with lower power to next route on the routing path which is called warm attack. The Route Request Messages (RREQ) must be used to set up communication traffic in the ad hoc wireless network. This will give the attacker the opportunity to have control messages attack which is called Flooding Attack in the absence of any additional conditions and risks. Warm and Flooding Attacks in ad hoc network are very difficult to detect and defense, because malicious nodes look like performing normal nodes operation routing protocol. Another attack called Data attack [7] is dangerous, because other nodes in network will become an accomplice that will not only hurt the victim node, but also hurt its own. This type of attack is very hard to combat because any malicious node can send legitimate flood control packets and transmit of useless data to the victim node.

In this research, we will take advantage of the Intelligent ClusterHead Agencies (ICHAs) that are usefully able to establish multi routing path and control multi routes in ARIP routing protocol for ad hoc wireless network. The key design feature in the proposed IDMA Protocol includes ConfirmRG protocol, Watch Algorithm, Perimeter Protocol and Refuse Protocol, which are applied to counterattack malicious nodes from carrying on frenzied wrecking activities in a variety of attack in ad hoc wireless network. In ConfirmRG protocol, the idea is to determine routing path of source ICHA with a reply to confirm route gateway information (confirmRG) to its destination ICHA via routing path without gateway acknowledgment between source ICHA and destination ICHA. The destination ICHA will receive ConfirmRG packets to identify impersonal attack. In watch algorithm, ICHA watches the average date packets flow from a route located within its clustering to identify whether it has warm attack in its cluster. In Perimeter Protocol, a designated ClusterHead, instead of the source node, will originate RREQ packets so as to restrict malicious node's operation in network and use Perimeter Id to identify flooding attacks if the attacks come from malicious nodes. In Refuse Protocol, delegated destination node has the authority to make decisions so that the destination node operates network from passive to active to resist data flooding attack without damage normal nodes operation. The IDMA Protocol takes full advantage of the characteristics in ARIP to improve defenses against the malicious attack with interrupting normal network operations. We will present the analysis of the security flaws in ARIP and describe the IDMA Protocol with simulation results to show that it offers significant relief for flooding attack from the malicious nodes control packet and is capable of eliminating data flooding attacks in ad hoc wireless network.

The rest of the paper is organized as follows: In Section 2, we discuss some related work in the improving defense against the malicious attacks, In Section 3, we provide an overview of ARIP protocol which is the bases for IDMA design. In Section 4, we analyze a variety of malicious attacks and describe the IDMA Protocol to defend against the attacks in ARIP routing protocol. In Section 5, we implement IADM protocol using the GloMoSim simulator and demonstrate its efficiency under a variety of operational conditions. In Section 6; we conclude this paper with a summary.

2. RELATED WORKS

To prevent malicious attack in ad hoc wireless network, various solutions have been proposed. In [5], the authors presented an intrusion detection model and the response mechanism for block malicious node in wireless ad hoc networks; In [9], the authors proposed the Digital signature solution to provide security about data of packets in network and to detect impersonation attack. In [6], the authors proposed a random assessment delay technique to evaluate the

number of RREQ packets to mitigating control packets flooding attack. In [11], the authors proposed an intrusion detection to monitor network packets and to analyze packets for identifying patterns of attack. In [7], the authors proposed a Flooding Attack prevention based on AODV routing protocol. In this case, nodes process RREQ packets with the lower priority. By counting the number of RREQ packets that exceed a threshold values, these packets will be drown up to resist flooding attack. In [8], the authors proposed a filter technique with rate of RREQ packets per second to detect misbehaving node. When a rate of RREQ packets exceeds the threshold values, then this node is put in the black list.

In our previous study designed to combat main malicious nodes attacking, we show that conventional security measures cannot be used in ARIP routing protocol. For example, in Flooding Attack, they assume that individual nodes always have the same opportunely to count the number of RREQ packets which will be compared with threshold value to determinate malicious nodes in network. In ARIP routing protocol, only Gateway Nodes (GN) and ClusterHead (CH) rebroadcast RREQ messages if target is not available in neighbor of shooter or shooter's CH. The receivers RREQ of Cluster Nodes (CNs) delete RREQ messages. Hence, the uneven distributions of RREQ packets are in network. Also GN or CH coming from CN must need to count the number of RREQ packets. But it is not really accurate according to the number of RREQ packets from shooter's CH. It may occur in nodes who refuse to relay RREQ packets because the number of RREQ packets exceeds the threshold value. However, some GN or CH still rebroadcast RREQ packets, it just looks like overland flooding which still can be destructive. The defined level of nodes and flooding attack can also occur in a hole producing affects similar to flooding attack. In [7], the design of cutting off path scheme cannot be used in ARIP routing protocol because it disrupt no relative routing path but also interrupted shortest routing path algorithm in reactive routing protocol of ARIP.

3. OVERVIEW OF ARIP ROUTING PROTOCOL

In this section, we will first present an overview of ARIP. We will then illustrate the major principle of ARIP with an example application to explain the details.

3.1 Overview of ARIP

The ARIP [2] has been developed based on DHMRP [1], a dynamic hybrid multi routing protocol for ad hoc wireless networks based on clustering. The different between DHMRP and ARIP is that the router /hosts deliver packets with Route Identity (RI) to hide actual IP address of nodes to defend against hacker IP address attack.

ARIP is a clustering based protocol with intra-reactive and inter-proactive, dynamical multi routing protocol designed for routing in mobile ad hoc networks with large number of nodes. In ARIP, the entire network is divided into one hop away clusters. Each cluster consists of ClusterNode (CN), ClusterHead (CH), and Gateway Nodes (GN). A node has bi-direction links to all its neighbors and lowest Identity (i.e., IP address) node is assumed to be ClusterHead within a cluster. We also assume that each ClusterHead is a trust node in the network and each node maintains its neighbor information with IP address.

In ARIP, ClusterHeads are assumed to discover Target, to determine multi routing path, and to obtain reply path at sometime to deliver extract information between ClusterHeads. These ClusterHeads are called Intelligent ClusterHead Agents (ICHAs) in ARIP.

3.2 An Example of ARIP

An example of ARIP is shown in Fig 1. In this scenario, a "Shooter node" node_13 wants to send some data to a "Target node" node_9 without predefined routing information. Initially the shooter_13 sends Ask message to its CH_1 (is called shooter's CH). The Shooter's ClusterHead_1 broadcasts Router Request Information (RREQ) to its adjacent neighbor. ClusterHead_2 receives the RREQ message and rebroadcasts it via Gateway_4 which rebroadcasts RREQ until the Target's ClusterHead_3 discovers the Target_9 in its own cluster. Then, Target's ClusterHead_3 determines multi routes (9 and 10) and determines Route Identity Pool (RIP) from minRI and maxRI in dominating clustering and the reply message includes router gateway information (i.e., 8 and 11) and maxRI to its source ClusterHead_2 via reply path and also it is to be Target's ICHA_3.

Similarly, the ClusterHead_2 determined multi routers (i.e., 7, 8, 12 and 11) and RIP (minRI ~maxRI) in order to reply message of ICHA_3 and then reply route gateway information (i.e., 6, and 13) and maxRI to shooter's ClusterHead_1. It then becomes ICHA_2. The Shooter's ClusterHead_1 determined multi routers (i.e., 13 and 6) and RIP (minRI ~maxRI) in order to reply to the message of ICHA_2. Finally, each ICHA maintains Inter Route Table that includes routers with

RIs which come from RIP corresponding to actual IP address in its dominating clustering, and sends neighbor routers with RI information to a node which is selected as a router. Each route will maintain Router Catch which includes two neighbor routes with RI information. Then, RI in received data packet matches with RI in its Route Catch to gain next router information with RI. The router then takes itself RI in header of data packets which will be delivered to next router with RI.

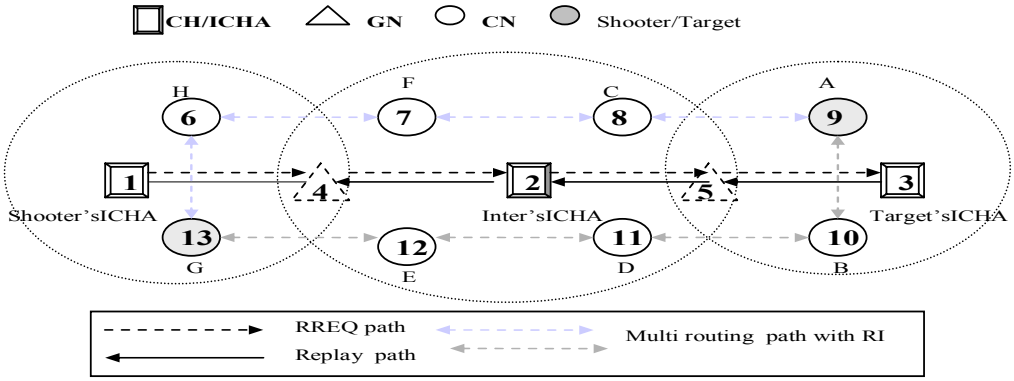

Fig 1: An example to show the formation of multi routing path with RI, One of the paths includes routers (actual IP:13, 12, 11, 10 and 9; corresponding to RI:G,E,D,B ,A) and another path includes routers (actual IP: 13, 6, 7, 8, and 9 ; corresponding to RI:G,H,F,C,A).

4. IDMA PROTOCOL: DEFENDING A VARIETY OF MALICIOUS ATTACK IN ARIP

The ARIP routing protocol has its own characteristics in reducing Malicious Attack since multi routing path and reply path exist in parallel in network. However, there are still opportunities for malicious node to attack network in ARIP routing protocol. In this section, we describe in detail a suite of schemes: ConfirmRG protocol, Watch algorithm, Perimeter Protocol and Refuse Protocol in IDMA protocol. Each protocol or algorithm will be utilized to defend against malicious nodes' attack with different type of attacks in ARIP.

4.1 ConfirmRG Protocol:

In ARIP, each ClusterHead (CH) obtains its neighbor clustering information provided by its Gateway Nodes (GN). Hence, each CH maintains its neighbor clustering information in its neighbor table. As a reactive routing protocol, ICHAs communicate with each other via gateway nodes. In this case, Gateway nodes could be malicious node to obstruct proper routing by modifying routing information in network. It can cause huge damage to the network by this type of impersonal attack.

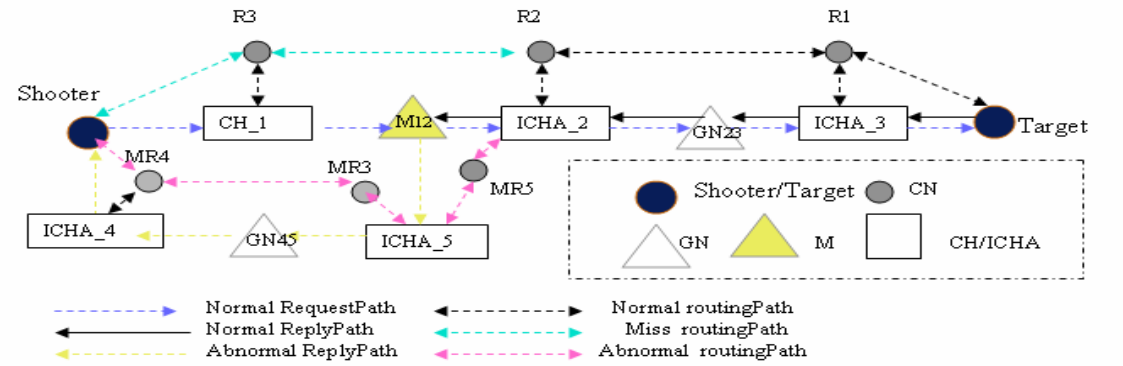

Fig 2: Impersonal Attack example: ICHA_2 wants to send replyRREP to CH_1 via Gateway Node (M12 is malicious node). However, M12 modifies routing information of replyRREP packets of ICHA_2 and relay replyRREP packets to ICHA_5, not to CH_1.

For Impersonal Attack example shows in Figure 2: The Target's ICHA_3 determines inter routing path (i.e., R1-R2) and sends ReplyRREP appending R2 to reviser CH (i.e.ICHA_2) via reviser GN23. Similarly, ICHA_2 determines its

inter routing path (i.e.R2 –R3) according to ReplyRREP of ICHA_3. Then ICHA_2 sends ReplyRREP appending R3 to reviser CH (i.e., CH_1) via reviser GN (i.e., M12). Because M12 is a malicious node, it modifies source ICHA IP address (i.e., CH1 was changed to ICHA_5), deletes R3 information from ReplyRREP of ICHA_2, and finally sends modified ReplyRREP packets to ICHA_5 without ICHA_2 acknowledgement. Therefore, the miss routing path (i.e., MR5-MR3-MR4) is established from ICHA_2 to ICHA_4. However, this is not the shortest routing path and therefore it is a successful impersonal attack for malicious nodes in network.

In ARIP, to defend against such impersonal attack, the reviser CH(i.e., ICHA_5) sends back a ConfirmRG packets via route gateway (i.e., MR5) to its destination ICHA (i.e., ICHA_2). If destination ICHA (i.e., ICHA_2) did not receive ConfirmRG packets from its source ICHA (i.e., CH_1) or received wrong ConfirmRG packets, then it identifies that this is an impersonal attack and will originate Black message including malicious nodes IP address (i.e., M12) in network. Therefore, the malicious nodes (i.e., M12) will be isolated in network.

4.2 Watching protocol:

In ARIP, each router monitors its neighbor routers according to neighbor table information. A router who is malicious router can adjust power when it transmits data packet. In order words, when the malicious router broadcasts Hello messages with normal power, its neighbor routers identify this router's existence in their neighbor table. However, when malicious router transmits data packets with lower power, then next router could not receive data packets but it thinks the neighbor router is normal behaviors according to its neighbor table information. This is a successful warm attack for malicious nodes in network.

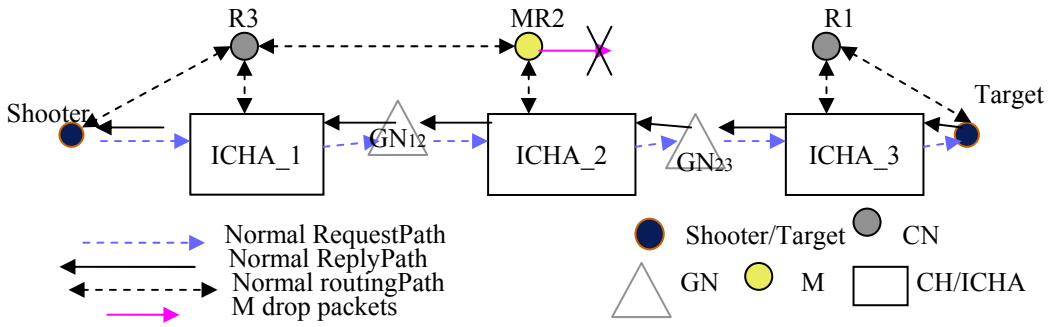

Fig 3: Warm attack example: Malicious router MR2 received packets from route R3. However, it transmits data with lower power so that the data packets could not reach to next Router R1.

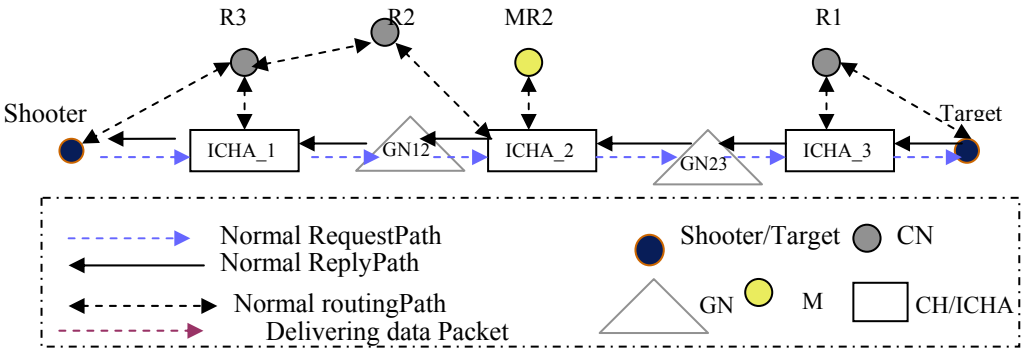

Fig4: Defending against warm attack example: R1 sends total number of miss packets to ICHA_3, receiver miss packets of ICHA_3 sends replyRREP appending to suspect router MR2 to ICHA_2. Receiver replyRREP packets of ICHA_2 determines new inter routing path R3-R2. The reply path from ICHA_2 to ICHA_3 will be responsive to deliver data .

For warm attack example shows in Figure 3, the MR2 is a router and also malicious node on the routing path. The MR2 originates its Hello messages with normal power so that the neighbor routes R1 and R3 can maintain MR2 in their neighbor tables. However, MR2 receives data packets from route R3 and transmits data packets with lower power to next route R1. Therefore, the MR2 action just looks like normal nodes behaviors. It is hard to detect this warm attack.

We assume that Sequence Numbers (SN) is provided. The source inserts sequence numbers within the data packet. In addition, we assume that the link layer supports reliable delivery by means of Ack (acknowledgement) packets. This provides critical evidence that a neighbor router has in fact received packets that were sent to it. When the router count the miss packets number exceed the threshold value, it identifies that its neighbor router has misbehaviors and sends missSN packets appending to total miss packets number and the suspect router to its ICHA. For the example shown in Fig 4, the ICHA_3 receives missSN packets from the routerR1 and sends replyRREP appending MR2 address to source ICHA_2 which determines new inter routing path (i.e., R3-R2) so that the MR2 will be isolated from routing path.

4.3 Some Definitions

To design effective protocol to identify and prevent the situation from deteriorating due to flood attack, it is required to provide some definition for shooter. In this section, we design perimeter protocol with these definitions.

(a) **Selection of new shooter's CH**: If shooter's CH moves out from the neighbor table of the shooter, then shooter can select a new shooter's CH. Or, if shooter received routing information from an ICHA, it must select this ICHA to be new shooter's CH.
(b) **Broadcast RREQ:** Shooter can not directly broadcasts RREQ messages.
(c) **Perimeter Identity:** Receiver Ask message of CH who is allowed to broadcast RREQ messages for query routing information of shooter is called Perimeter Identity (PerimId).
(d) **Canceling message:** If shooter obtains routing information, it must send canceling message to shooter's CH.

4.4 Perimeter Protocol

In ARIP, hybrid routing protocol employs proactive and reactive routing protocol. To discover routing path, we implement proactive protocol not only for shooter's CH, but also for shooter, because all nodes in network has own neighbors information in their neighbor table. In this section we will discuss the flood attack model in ARIP and utilizes Perimeter Protocol to defend against a variety of flooding attacks in ARIP routing protocol.

Shooter searches target with proactive routing protocol: When a shooter wants to send data packets to the target without routing information, it will search for its first consideration of neighbor table in two-hop away based on proactive routing protocol. Therefore, if the target is available in its neighbor table, it can directly deliver data packets to target without broadcast any RREQ packets.

For the first proactive routing protocol example shows in Fig 5, Shooter_1 directly transmits data packets to Target, as this target is in its neighbors table.

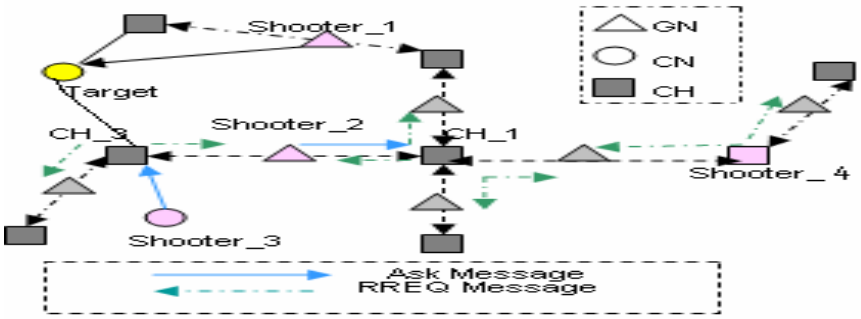

Fig 5: Example for proactive and reactive routing protocol.

If shooter scans neighbor table and finds no information about target. Shooter has the need to implement reactive discovery routing protocol to reach target. Shooter must ask its CH (is called Shooter's CH) to help discover target in the network. When Shooter's CH receives Ask messages from shooter; it must first implement proactive routing protocol to scan its neighbor tables in two-hop away range to search for target. If the search results indicate that the target exists, then, shooter's CHs will determinate routing path from shooter to target. For second proactive routing protocol example

shows in Fig 5, shooter_3 sends Ask messages to its CH (e.g., CH_3). Shooter's CH_3 determines Target to shooter routing path without originating RREQ packets.

Shooter's CH searches target with reactive routing protocol: If the target is not in clustering of shooter's CH, then reactive routing protocol is used to originate RREQ packets by shooter's CH. In ARIP, only when the shooter's role is a CH, can it direct broadcast RREQ packets. However, this role may be changed frequently due to the fact that entire network is divided into clusters. Each node plays different roles by the time pass as their role can change from one to another as the network topology changes frequently.

Therefore, shooter might not be a CH. For reactive routing protocol example shows in Fig 5, shooter_3 is a CN and shooter_2 is a GN. In order to use ARIP routing protocol, they need to select a CH to be shooter's CH in their neighbor table and send Ask messages to shooter's CH (e.g., CH_3 and CH_1 separately). Shooter's CHs originate RREQ packets in order to use reactive routing protocol to make enquiries routing path information for shooter. In this case, it naturally restrict the Flooding attacks since attacker cannot directly originate RREQ packets if shooter is a attacker in ARIP. However, with special property of ARIP, some Flooding attacks models are different from conventional routing protocol.

Forge Target Address Attack: The attacker can scope Target Address which might not be in the network. Then, there will be no reply messages returning to attacker's CH. Therefore, this is a successfully realization of flooding attack..

In ARIP, All nodes have the opportunity to generate forge target address attack. For Forge Target address attack example shown in Fig 6, attacker who is a GN sends Ask Message with forge Target IP address to attacker's CH. then attacker's CH originates RREQ packets under blinding.

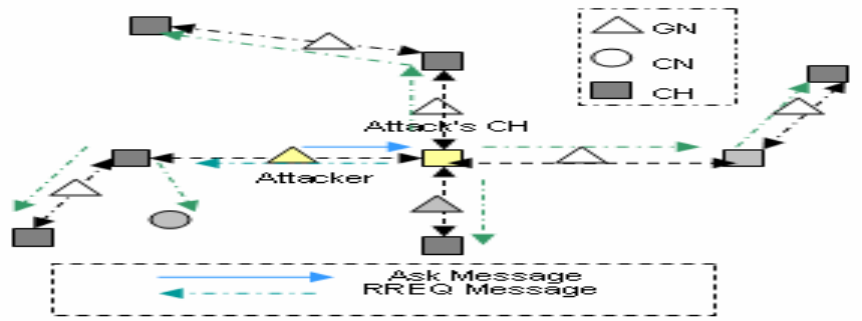

Fig 6: Example for Forge Target Address Attack

Abuse Ask Message Attack: if attacker is a GN, it can choose more than one CHs to be attacker's CH, therefore, more than two CHs would originate RREQ packets with different broadcast Id in network, as a result, there will be overflow large RREQ packets in network. For Abuse Ask Message Attack example shown in Fig 7, the attacker sends Ask_1 message to attacker's CH_1 and also sends Ask_2 messages to Attack's CH_2. The RREQ_1 and RREQ_2 packets with different Broadcast Id will be originated by attacker's CHs separately. The mass of RREQ packets will flood the network.

Abuse Shooter's CH Attack: attacker designates attacker's CH the use RREQ packets to help it enquire routing path information if attacker is not CH. The routing information provided to the attacker may not be attacker's CH since an ICHA may determine inter multi routing path from attacker to target/router gateway of routing path within its cluster. It is this ICHA that provides routing information to the attacker. Therefore, the attacker obtained routing information without attacker's CH acknowledgment. As a result, the attacker's CH unconsciously help attacker to successfully achieve flooding attack purpose in the network as it still continues to originate RREQ packets under blinding.

For abuse shooter's CH attack Example shown in Fig 8, attacker sends Ask message to attacker's CH. ICHA_j receives RREQ packets to discover target in its clustering and reply RREP appending to route gateway CN_a to ICHA_i. Then, ICHA_i scans shooter in its clustering, so that it determines routing path from CN_a to attacker, and sends routing information to attacker without acknowledgment of attacker's CH. If the attacker did not send canceling message to attacker's CH, then the attacker's CH will continue to originate RREQ packets under blinding.

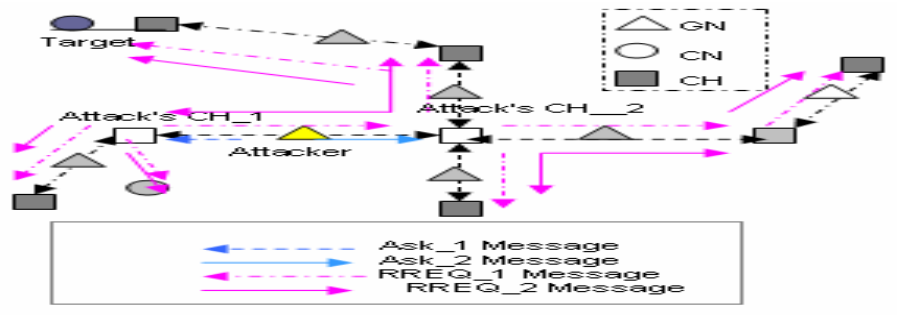

Fig 7: Example for Abuse Ask Message Attack

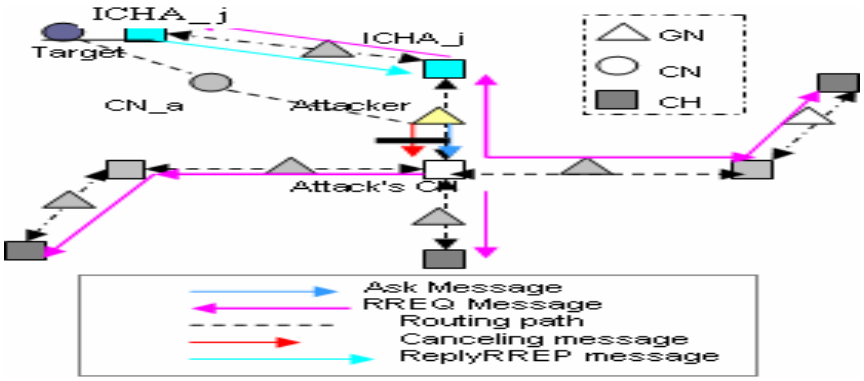

Fig 8: Example for Abuse attacker's CH Messages Attacker and Garbage Data Attack

Garbage Data Attack: After attacker obtains route information from ICHAs, it can transmit garbage data to target. By the data security rules, only the target can judge whether data is Garbage in application layer since there is no additional instruction mechanism in ARIP routing protocol. Therefore, excessive Garbage Data congest the network and depletes the available network bandwidth for the communication among the other nodes in network. The target will be busy for receiving the excessive useless packets from the attacker and lose normal work. As a result, this is a successful realization of flooding attack in network.

According to definition (a) and (b), shooter needs to designate a CH to be shooter's CH. After that, according to definition (c), the shooter sends Ask Message appending to PerimId.

A Perimeter List (PerimList) will be used to maintain PerimId information for each node in network. The PerimList includes as follow: <shooterAddr; targetAddr; PerimId, Nrreq>,, where these attributes are defined as:

PerimId: The receiver Ask Messages of CH checks whether the PermList is maintained. If not, it must maintains PermList and then it scans its neighbor table to discover target. If the results indicate that the target is not available in the neighbor table of shooter's CH, then shooter's CH begin routing discovery process in order to launch reactive routing protocol of ARIP.

To make sure that PerimId is maintained in each node, the PerimId will be appended into RREQ message for distribution in the network. Thereby, we have modification protocol in ARIP. When nodes (e.g., CN, GN, and CH) receive RREQ messages, it checks whether the PerimList exist. If not, it maintains PerimList, otherwise it updates PerimList. If shooter's CH finds out the shooter is not available in its neighbor table, it stops sending originate RREQ packets. If the time for Ask messages expires, based on definition (a), shooter does not obtain routing information. Then, shooter checks whether the PerimId is still in its neighbor table. If yes, then shooter resends Ask messages with PerimId to shooter's CH. Otherwise, it needs to select another CH within its neighbor to be shooter's CH and the PerimId is now new shooter's CH IP address

To avoid more than one shooter's CHs are designated by shooter at the same time, the shooter needs to provide old PerimId to new shooter's CH to make sure that this is not the initial shooter's CH

Nrreq: This is defined to avoid miscount in the number of RREQ messages. For example, a node might not count RREQ packets, if it is (i) overloaded; (ii) collision; (iii) it did not received route request, or (iv) if its role is CN in ARIP. Therefore, Shooter's CH must be responsible for recording Nrreq which is the number of RREQ packets. As a result, each node receives RREQ packets to flash its PerimId and Nrreq in its PerimList, even if it might not receive RREQ packets in the interval time. However, it still obtains the final Nrreq number of RREQ packets. Hence, when new shooter's CH receives Ask messages from shooter; it continues to take charge of the recording Nrreq.

For example: shooter's CHi broadcasts N^i_{rreq} number of RREQ packets at time Ti. Then shooter's CH stops sending originate RREQ packets because shooter moves out of its neighbor table. New shooter's CHj continue to originate RREQ packets N^j_{rreq} at time Tj, then total number of RREQ packets which was originated $N_{rreq} = N^i_{rreq} + N^j_{rreq}$ by both shooter's CH at different time Ti and Tj. The nodes in network receive RREQ to check whether old PerimId is in it PerimList, if yes, it use new PerimId instead of old PerimList and also flash Nrreq the number of RREQ. Therefore, PerimList which will be maintained at each node shown below :<shooterAddr, targetAddr, PerimId = Shooter's CHj; Nrreq>

After shooter's CH originated RREQ packets in network at time T, the shooter obtains routing information. Based on definition (a) and (d), the shooter MUST send canceling message to shooter's CH. And the ICHA which provided routing formation to shooter is to be new shooter's CH and responsible for originating RREQ packets if the shooter still needs to communication with target.

The PerimId will be set as an activated statue, which means that the target is in existing in network. After that the Nrreq number of RREQ could not be recorded by shooter's CH.

Each node will delete Nrreq value from its PerimList and maintain PerimId activated statue. Therefore, PerimList which will be maintained at each node is shown below :< shooterAddr, targetAddr, PerimId= Shooter's CHj; activated>

Defending Against Forge Target Address Attack: The attacker scoop forge IP address to be target and sends Ask packets with forge IP address to attacker's CH. As a result, no reply message with respect to target IP address will be responded. The RREQ packets will be flooding the network since attacker's CH continues to originate RREQ packets.

In order to implement Perimeter Protocol, the shooter's CH originates RREQ packets and takes charge for recording Nrreq, the number of RREQ packets. Once the Nrreq, the number of packets exceed a threshold value, it identifies that forge target IP address attack has occurred. The shooter's CH will stop originating RREQ packets and will broadcast Black list with shooter IP address. As results, the RREQ packets will be eliminated.

Defending Against Abuse Ask Message Attack: The attacker may send Ask message to more then one CH. Therefore, at same time, two or more attacker's CH will originate RREQ packets with different Broadcast Id. The mass of RREQ packets will flood in network.

Based on the Premier Protocol, each node in the network receives RREQ packets to check whether or not only one PerimId is in the packets, which means that these RREQ packets are originated by initial shooter's CH. Then, the node uses the PerimId in RREQ packets to compare with PerimId in PerimList to see if the PerimList exist. Otherwise, it just maintains PerimId and Nrreq in PerimList. If the comparison results shown that the PerimId does not match, then it identifies that this is abuse Ask messages attack. Then, the nodes will delete RREQ packets to resist flooding RREQ packets in network. The attacker's CH will broadcast BlackList message to isolate attacker in network.

Defending Agianst Abuse Shooter's CH Attack: The attacker may send Ask message to attacker's CH. Then, the attacker obtains routing information from a ICHA. However, it does not send canceling message to attacker's CH. Hence, the attacker's CH continues to originate RREQ packets under blinding. As a result, the RREQ packets will cause Flooding in the network.

Based on the Perimeter Protocol, ICHA must be the new PerimId for next attacker's CH. ICHA receives RREQ packets to check PerimId in RREQ. If PerimId in RREQ packets is not an ICHA IP address, then, it identifies that this is an abuse shooter's CH attack. The ICHA sends drop data packets information to its routes and broadcast blacklist messages including attacker address, the data packets from attacker will be dropped by routes and also the attacker will be isolated in the network.

4.5 Refuse Protocol:

In this section, we take full advantage of ARIP to design a target that has adequate power to make a decision for communication with the shooter. The conventional routing protocols do not consider such issue.

To avoid communication with unfriendly shooter, target can maintain a Refuse List (RefList) which includes unfriendly shooter IP address. Once a CH discovered the target is available in its clustering and became Target's ICHA, then Target's CH sends unique RREQ packets to inquire information about whether target likes to communication with shooter. If the shooter is available in RefList of target, then a Refuse message will be sent to Target's ICHA from target. Also, the target has enough power to judge whether a data packet is useful. Then, it sends Refuse message to Target's ICHA if target judges the data to be Garbage data. Target's ICHA will maintain a RefList that includes shooter Address, and target address.

In ARIP, the multi routing path and reply path are parallel in network, the reply packets are delivered via reply path and data packets are delivered via multi routing paths.

Based on the characteristics of ARIP, the Target's ICHA can send a reply RREP appended to RefList to its source ICHA all the way to the shooter's ICHA. Shooter's ICHA maintains the RefList and will refuse to originate RREQ messages.

Defending Against Garbage Data Attack In this case, the attacker wants to send garbage data to the victim node after it has obtained the routing information.

The best way to defend against the garbage data attack is to do that before the routing path establishment because ICHAs do not need to consume energy and network bandwidth for establishing the routing path.

Based on the Refuse Protocol, an example for defending against the garbage data attack is shown in Fig 8. In this case, ICHA_j discovers Target in its clustering and sends unique RREQ message to the target. The Target scans its RefList. If the results indicate that shooter is in the RefList that identities that this is Garbage data attack, the Target sends Refuse Message to ICHA_j, then ICHA_j reply with Refuse Message to ICHA_i via reply path.

In the second case, if the attacker is not in RefList in target, then the target will send agree packets to ICHA_j so that the ICHA_j determines routing path and sends ReplyRREP packets appended to the route gateway CN_a to ICHA_i.

ICHA_i checks the attacker in its clustering, then it determines routing path from CN_a to attacker and sends routing information to attacker. The attacker obtains routing information and sends data to target. When the target received data and determines that this is garbage data attack, then, it sends Refuse Message to ICHA_j. ICHA_j also sends drop data message to CN_a and sends Refuse Message to ICHA_i via reply path. ICHA_i search shooter in its clustering and sends Refuse messages to attacker to stop transmitting data by the attacker. If attacker wants to re-obtain routing information, it may resend Ask message. However, if ICHAs received RREQ packets to check if the attacker is in RefList, then they will broadcast BlackList including attacker address to resist the Garbage Data Attack.

5. SIMULATION RESULTS

In this section, we will report our study on the practical impacts of the attacks on the performance of ad hoc networks through simulation. Three attacks on ARIP are considered: impersonal attack, warm attack and Flooding attack. Except for warm attack, the attacker will discard data packets passing through it. Except for the impersonal attack, the attacker will modify reply RREP packets passing through it. Except for flood attack, the attacker is CH and broadcast RREQ message until end simulation time. Only one shooter and one target is assumed throughout simulations.

The simulation of attack on ARIP is deployed using GloMoSim [12]. The channel capacity of mobile is set to 2 Mbps and the transmission range is set to 250 meters. A free space propagation model with a threshold cutoff is used as the channel model. We use the Distributed Coordination Function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol.

In the simulation, 100 mobile nodes move in a 2000 x 2000 meter squire region. The mobility model is random waypoint model. The minimal speed is 0 m/s, and the maximal speed is 30 m/s. One shooter-target pair is selected randomly to generate Constant Bit Rate (CBR) traffic as the background traffic. The interval time for data transmission is 1.2 second. The size of all data packets is set to 1460 bytes. Each node broadcast periodic Hello message in 300 ms. we set three types attack in the simulation at same time. The attackers are chose from 100 nodes. We use different pause time (30s, 50s, 100s, 150s, and 200s) to represent 4 different mobility scenarios. The seeds are set to 1. The simulation time is 600s.

We measure end to end delay; throughput and total number of bytes received at target node under three different conditions:

1: The shooter transmits data packets without malicious nodes attack. This is called normal ARIP.

2: The shooter transmits data packets with different types attack from malicious nodes. This is called attack ARIP.

3: The shooter transmits data packets with different types attack from malicious nodes and IDMA protocol is adopted to defend against the attack in simulation. This is called defense Attack.

The plots in Figs 9, 10 and 11 show that normal attack, defense attack and attack delivered packet from shooter to target in ARIP. The results indicate that, utilizing IDMA protocol, the end to end delay, throughput, and Total number of bytes received, are approximately the same as the normal ARIP results. Moreover, the delay has been significantly reduced comparing with the case of attack. Therefore, the IDMA protocol is able to successfully defend the three types of attack.

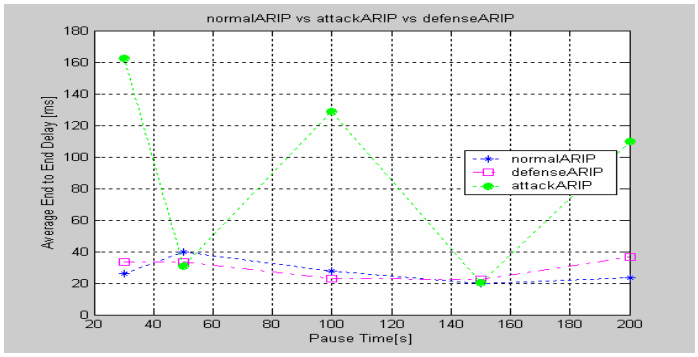

Fig 9: Performance on Average End To End delay

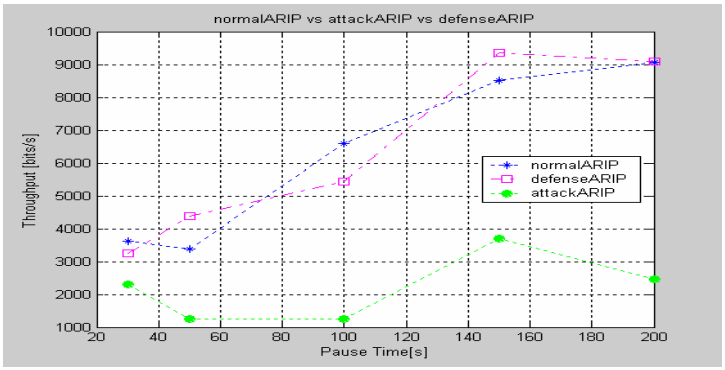

Fig 10: Performance on Throughput

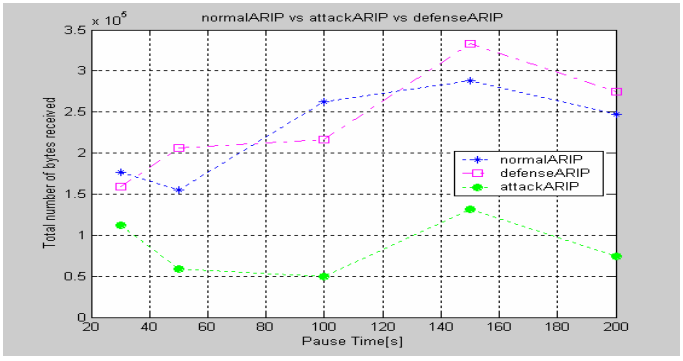

Fig 11: Performance on Total number of bytes received

6. CONCLUSION

We have proposed an IDMA protocol designed to improve the defense against various malicious attacks in ad hoc wireless networks. This protocol is aimed to minimize the costs of network monitoring and provide a degree of defense against malicious nodes attack without any instruction detection or authority key information exchange. In this research, we analyzed a variety of possible attacking models and provided a quantification of the damage the attacks may inflict. IDMA Protocol is developed to defend against the attacks and isolate malicious nodes in the ad hoc network. The Target has the authority to judge shooter misbehaviors at any time. In this scheme, we show that it can successfully counter the attacks coming from malicious nodes and reduce the compromised nodes in the ad hoc network. In the future, we plan to develop an enhanced protocol can be adopted to defend against more variety of possible attacks.

REFERENCES

[1] C. Peng, and C. W. Chen, "Dynamic Hybrid Multi Routing Protocol For Ad Hoc Wireless Network" The 2006 IEEE International Workshop on Wireless Ad Hoc and Sensor Networks conference.

[2] Peng, Chaorong; Chen, Chang Wen; "A New Network Layer for Mobile Ad Hoc Wireless Networks Based on Assignment Router Identity Protocol" International Conference on Computer Communications and Networks, 2007. ICCCN 2007.

[3] S. Das, C. Perkins, E. Royer, "Ad hoc on demand distance vector (AODV) routing", Internet Draft, draft-ietf-manet-aodv11.txt, work in progress, 2002.

[4] Z. J. Hass, R. Pearlman, "Zone routing protocol for ad-hoc networks", Internet Draft, draft-ietf-manet-zrp-02.txt, works in progress, 1999.

[5] Bhargava, S.; Agrawal, D.P, "Security Enhancements in AODV protocol for Wireless Ad Hoc Networks" Vehicular Technology Conference, 2001. VTC 2001 fall. IEEE VTS 54th

[6] Desilva, S.; Boppana, R.V.; "Mitigating Malicious Control Packet Floods in Ad Hoc Networks" Wireless Communications and Networking Conference, 2005 IEEE

[7] Ping Yi; Zhoulin Dai; Yiping Zhong; Shiyong Zhang; "Resisting Flooding Attacks in Ad Hoc Networks" Information Technology: Coding and Computing, 2005. ITCC 2005. International Conference

[8] Jian-Hua Song; Fan Hong; Yu Zhang; "Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks" Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT '06.

[9] Dijiang Huang; Sinha, A.; Medhi, D."A double authentication scheme to detect impersonation attack in link state routing protocols" Communications, 2003. ICC apos;03. IEEE International Conference

[10] Adm Burg, "Ad hoc network specific attacks", seminar on Ad hoc networking: concepts, applications, and security , technische university at munched, 2003.

[11] Oleg K, Ratan G.: "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks"

[12] Glomosim Home Page: http://www.pcl.cs.ucla.edu/projects/glomosim.