International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:5, No:5, 2011

Attack Defense of DAD in MANET

Sehyun Cho, Heasook Park

***Abstract*—**These days MANET is attracting much attention as they are expected to gratefully influence communication between wireless nodes. Along with this great strength, there is much more chance of leave and being attacked by a malicious node. Due to this reason much attention is given to the security and the private issue in MANET. A lot of research in MANET has been doing. In this paper we present the overview of MANET, the security issues of MANET, IP configuration in MANET, the solution to puzzle out the security issues and the simulation of the proposal idea. We add the method to figure out the malicious nodes so that we can prevent the attack from them. Nodes exchange the information about nodes to prevent DAD attack. We can get 30% better performance than the previous MANETConf .

***Keywords*—**MANETConf, DAD, Attacker, DDOS

I. Introduction

THE high expectation to use internet and telecommunication by people leads the rapid growth of the information technology. Also people want to use the internet with any limitation of the area or time. The tragedy of JAPAN in 2011 invokes the interest of MANET(Mobile Ad Hoc Network). It doesn't need any fixed infrastructure or centralized administration to make a network. Nodes communicate each other by a wireless media. Nodes could be a mobile phone, a lap top or any mobile device. There are several reasons why people put the interest into MANET. They can move and configure so fast. It is really good for cases like the war, the emergency situation, or the nature disaster[Fig 1]. They also operate separately. They are not subordinate to other nodes. They can communicate heterogeneous systems unlike the mobile phone. It is really cost-efficient comparing to other mobile communication. Like other network it is not almighty. It is less stable than the wired-network. It moves all around. There are limitations such as interference, data transmission distance and fading. Even though these disadvantages, the mobility is really an outstanding feature so that the research have been conducted. There are several working group studying on MANET such as Mobile Mesh Network, MANET, Multi-casting, Radio technology, Energy efficiency, Security and so on. One of the features of MANET is that they make the network by themselves. It needs an efficient self-configuration in case of vital environment. We firstly take a look on the part of several method of auto-configuration in MANET in section 2. Then we will discover the problem of MANETConf for auto-configuration in section 3. We will propose the proposed reinforced MANETconf method in section 4. The simulation result will be put in section 5. Finally we will conclude with brief explanation in section 6.

F. A. Author. Sehyun Cho, is with Broadcast Network department, Omniflow System Researching Team, ETRI, University of Science and Technology, Daejun, Republic of Korea (phone: 042-860-1805; fax: 303-555-5555; e-mail: csh@ etri.re.kr).

S. B. Author, Heasook Park, received the Ph.D. degree in Computer Science from the Department of Computer Engineering, ChungNam National University, Korea in 2005. From 1994, she has been a senior member of research engineering staff of ETRI(Electronics and Telecommunications research Institute). She has currently developed about flow based gateway and router in Network Research Department.

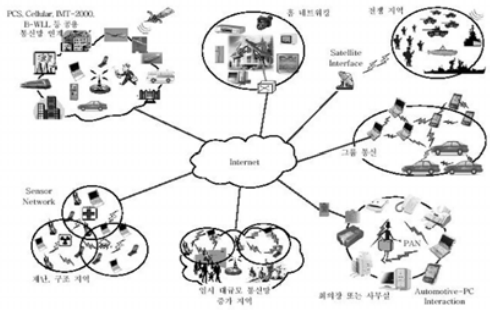

Fig. 1 The usage of MANET

II. Auto-configuration for MANET[1]

There are several reasons why we need to have a self-configuration in MANET. We need the information when we want to forward the packet. In order to do that, we need to know the configuration of current network. Also we need to trace the node which belonged to the network just before. So far there are two kinds of self-configuration. One is a stateful method and another is stateless method. The stateful method is similar to the current DHCP(Dynamic Host Configuration Protocol) method. There is a server to manage the IP Address in the pool and allocate the IP address whenever the nodes request. But it is kind of hard to set this method in MANET. As we said, nodes in MANET are mobile. We don't know where they are moving. Moreover, it is hard to notice that nodes are now staying or have left. Second method is stateless. The main difference between stateless and stateful method is the dependency of configuration. The stateless method doesn't need DHCP sever. Each node independently makes IP address for itself. It needs the duplication check. It causes time consumption for IP address configuration in order to check the DAD(Duplicated Address Detection). Despite of several defect in stateless method, it is more suitable than stateful method[2]. We take a look on a stateless method more deeply. There are several ways to support stateless method.

1) *IPv6 SAA(Stateless Address Auto-Configuration)[2]*

IPv6 SAA is one of stateless method. This was used in the wired network. It doesn't need the specific server like DHCP or node to configure the network. If the node in the SAA notices that it have moved into new area, it makes the IP address based

on link-local address then broadcasts it for DAD. The reason why it does DAD is that it verifies the uniqueness of IP address. It uses the NS(Neighbor Solicitation) and NA(Neighbor Advertisement) to verify. It waits timeout after the node broadcast for DAD using NS If the neighbor notices that the received IP in NS is duplicated, it sends NA using multicast. The sender using NS notices the duplication of IP after it receives NA. It is how to operate. Let's suppose that there is a node which frequently moves around. Is it possible to trace or notice that the node is moving around or move out to other MANET? The answer is no. It is hard to trace the node is moving or has moved out. Also it is so hard to measure the scale of MANET. It could be burden for nodes which are exchange the NS or NA frequently. It is hard for MANET to adapt this method. There are two reinforcement of IPv6 SAA method for MANET. It is Strong DAD and Weak DAD method. Strong DAD method uses reactive routing protocol as AODV(Ad hoc On-demand Distance Vector). When the node enters new area, it creates a new temporary address. It broadcasts its new address in AREQ(Address Request) message. If a reply arrives before the timeout, the node thinks the IP address duplicates. The time consumption of IP Setting is related to DAD failures. But it has one problem. It doesn't consider the merger[Fig.2]. After Strong DAD is conducted, it doesn't check the duplication of Address check again. Let's see the picture. Two MANET merge. After checking DAD, Strong DAD doesn't conduct any DAD check even if two MANET merge. So E-e(Node name-Node IP address) node wants send some data to a, the node a which is A-a and J-a receive the data at the same time. At the first time, it was not considered. So Weak DAD has a solution to solve this problem. Weak DAD has one more identifier to notice the node. It uses the key value which could be the link layer address or physical address. Before sending the data, the sender put the link layer address additionally in Hello message or Route Discovery message. When one node in the same MANET receive the packet which is addressed to it, it checks the key value again to make it sure that it is headed to it or not. The problem of duplicated situation in merging network could be solved by Weak DAD.

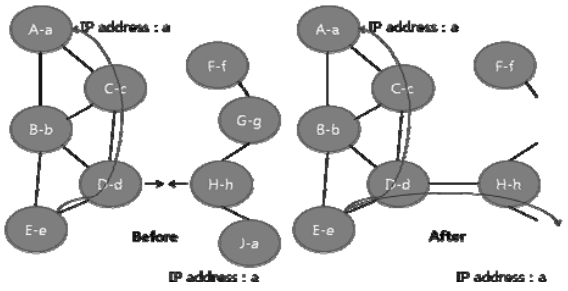

Fig. 2 The problem of Strong DAD

2) *MANETconf [3]*

MANETconf uses the nearest node t choose the new node's address in MANET. It has two possible cases to make the MANET. One is that the initial node become the leader in the MANET and another is that initial node belongs to the any topology. The first case is that there are no near nodes nearby. The second case is that there is MANET nearby and the leader node. Let take a look deeply.

(1) *A initial Node becomes the leader of MANET[Fig.3]*

When the node moves into new area, it broadcasts neighbor request with timer. If there is no node to reply, it assumes that there is no node nearby so that it becomes the leader node to try to make the MANET.

Fig. 3 MANETconf

(2) *A Node moves into near MANET*

Let's suppose that Node i enters into near MANET and there is the leader node named Node j. At first when i node broadcasts Neighbor Request with Timer. Node j replies when j node receives Neighbor Request. Node i checks the reply from Node j and checks the timer. Node i notices it moves into new MANET before the timer expires. Node i sends Requester Request to get the IP address. Node j allocates one IP address after this IP for Node i is duplicated or not. This is how to operate.

3) *Passive DAD method[4]*

This reason to suggest is for the merger of two MANET in Strong DAD like Weak DAD. As we mentioned above, there is a possibility to send packets to several node at the same time. In order to solve this problem, it uses sequence number in routing control message. It doesn't increase any burden like Weak DAD. It compares the routing control message when the packet is headed. By this way it can check the duplication of IP address.

III. The Problem of IP Auto-configuration[5]

In order to make a network in MANET, first thing to do is to allocate the IP address. Unlike other MANETconf, it performed better than other IP auto-configuration. But there are three possible attacks to prevent normal auto configuration procedure. Firstly [Fig.4] demonstrates that a malicious node acts as an initiator. A new node enters into new zone so that it

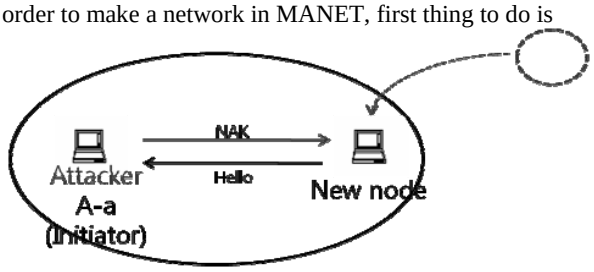

Fig. 4 Case 1

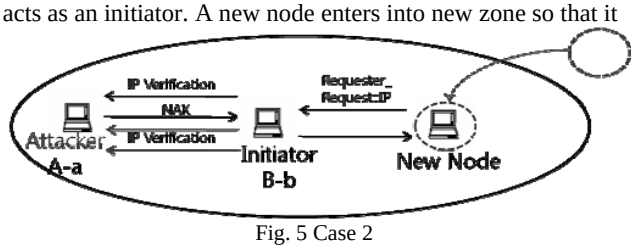

Fig. 5 Case 2

sends Requester_request to get IP address in half of itself. But Attacker named A-a(Node name-Node IP address) ignores or sends a garbage message to the new node. It is impossible for nodes to make the network so that they can not make MANET. Secondly [Fig. 5] demonstrates a malicious node acts as a requester and send address request message to the initiator. An attacker enters into node A's area and node A is an initiator. An attacker sends the request_request to get IP address continuously to make the initiator unavailable. Node A-a is so busy to process this messages. It causes a lot of available bandwidth for DAD. The service for the normal could not be conducted. A final case in [Fig. 6] is that a malicious node in the network could claim that the candidate IP address is already in use whenever it receives a message from an initiator for DAD check. The new node enters into node B's area and B is an initiator. B node chooses IP to verify for a new node. But node A-a continuously sends NAK for IPs from node B-b. That's why new node can't get any IP address. It is the three possible attack when MANET is configured using MANETconf. The previous method could not solve these problems so that we propose the reinforced MANETConf in the next chapter.

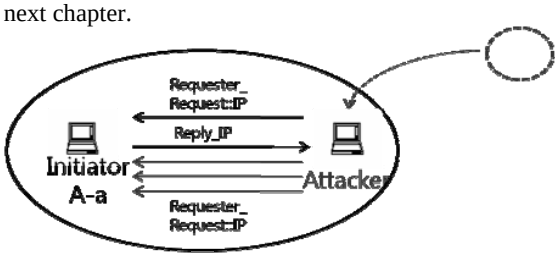

Fig. 6 Case 3

IV. The Reinforced MANETconf

We need to suppose this concept that it is adaptable when there are least two normal nodes. If there are two attackers among three nodes, it could not be possible to solve the problem like the previous MANETconf.

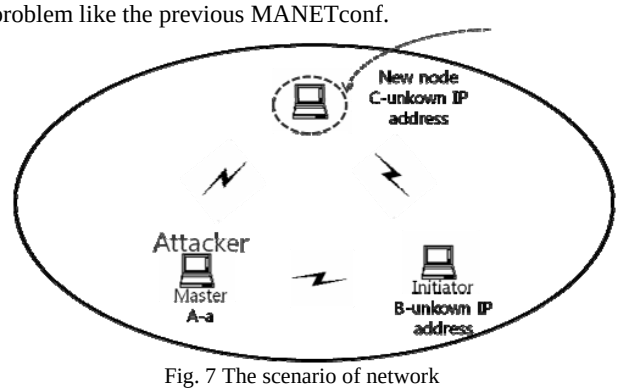

Fig. 7 The scenario of network

4.1 *Operation of the reinforced MANETconf*

Like [Fig. 7]. There are three nodes which one node is new, another is attacker, and the other is initiator. They try to make topology to send Hello to each other. But the master named A-a try to send NAK to them so that B and new node can't get any IP. Whenever they send the packet, they keep its record into table. We will take a look deeply and get to know the operation of the reinforced MANETconf with procedures. New node enters into new zone. In this zone, Master node is A-a to allocate IP address and is an attacker. Node B-b also has tried several times to get IP address by Requester_request message. But master doesn't reply with the right IP address. Also it tries to get IP address when the new node sends Requester_request message. When it broadcasts, the node C-unknown IP receives the B-unknown IP 's reply. The B-unknown IP node is too.

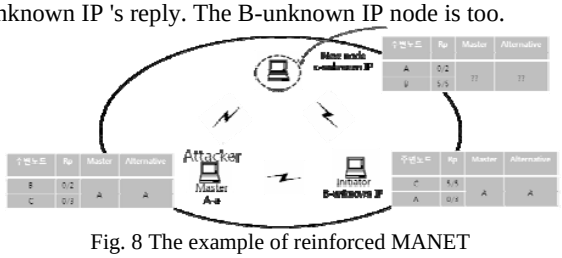

Fig. 8 The example of reinforced MANET

C-unknown IP and B-unknown IP nodes exchange RR messages. So they can create the table like below[Fig .8]. In the case of Requester B-unknown IP, it has received any messages from A when it tried to send Reqeuster_request five times. So Rp is 0. We jot down the procedure in Fig. 9. Following 20 step is how to operate by MANETConf .

```
Start
Step 01 : A requester (New Joining node) selects an
          initiator unicast Hello(RR) to the initiator
Step 02 :  n=0; (Set retry(n)=0)
Step 03 :  n++
Step 04 : The initiator broadcasts a TU(IQ) to all the
          nodes of the MANET group with the address of
          the requestor
Step 05 : if (all MANET nodes receive
               the IU(IQ) == TRUE)
Step 06 :      Recipient nodes reply with an affirmative or
                 a negative response to the initiator
Step 07 :  if (all MANET nodes compare that IU(IQ)
                 in their reliability check table == TRUE)
Step 08 :       if (Reliability check == 0)
                      goto END
Step 09 : else
Step 10 :    goto Step4
Step 11 : if(the initiator receives affirmative
                 TU(IR) messages from all nodes ==TRUE)
Step 12 :      The initiator assigned the IP address
                 to the requestor
Step 13 :  The initiator broadcasts a TU(AO) messages
             to tell recipient nodes of the MANET group,
                goto END
Step 14 : else
Step 15 :  if(The value in the reliability table from initiator is 0 )
                goto END
Step 16 :  The initiator selects another IP address
Step 17 :  if(retry count <=n)
Step 18 :      The initiator sends a TU(AB) message
                 to the requestor,
                 goto END
Step 19 :  else
Step 20 :  goto Step 3;
End
```

Fig. 9 The Pseudo code of reinforced MANETConf

4.2 Table for the reachable check

Each node saves the four things. They are the near node, Rp, Master node, Alternative node. The near node is the node to

exchange the hello message. Rp is the value for the reachable probability. The value is from 0 to 1. If a value is 0, it fails whenever it tries to send Hello. The value is 1, it succeed to send packet perfectly that there is no possibility for the near node to be an attacker. The master node is kind of a leader in MANET to be responsible for IP generation. Alternative node could be inactive for being responsible for IP generation but is possible to be the master node in the future in case the master node leaves. It makes the MANET work continuously

Rp is 0 <= Rp <= 1
Rp(ratio) = Reachablity / total trial

V. The Result of Simulation

5.1 *The simulation setup*

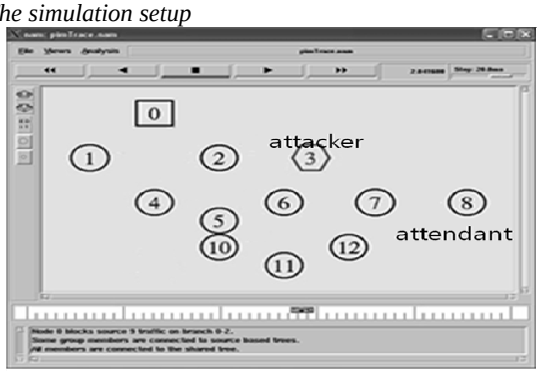

Fig .9 The configuration of Node

In this paper, we measure the result of DAD in MANET of Fig. 9. We use NS2 to conduct the simulation. We focus on the time how long it takes to do DAD and check the message overhead. Nodes are moving by the random waypoint mobility model[6]. Nodes moves around by the uniformed distribution method. The maximum speed of nodes is 5m/s. We set 20,40,60,80,100 nodes to take the test for this simulation. Nodes are set up like Fig. 9 to move around in 500 m X 500m. In the case of 20,40,60,80 and 100 nodes 15,30,45,60 pre-configured node are required to set up the network. And 2,4,6,8,10 attacker are set for DAD disturbance. The table below[Table 1] summarizes the configuration of the simulation.

TABLE I
THE SIMULATION SETUP

Parameter	Value
Simulation Time	20000 sec
The number of Nodes	20,40,60,80,100
Pre-configured Node	15,30,45,60,75
Malicious Nodes	2,4,6,8,10
Area	500 m X 500 m
Movement Model	Random Way Point

5.2 *The result of simulation*

In the Fig.10, it shows the result of the simulation. When there are few nodes in the MANET, the success rate of DAD is almost same. In the other hands, the performance is decreasing as nodes are getting more in MANETConf. It is really significant when we are willing to transfer some data.

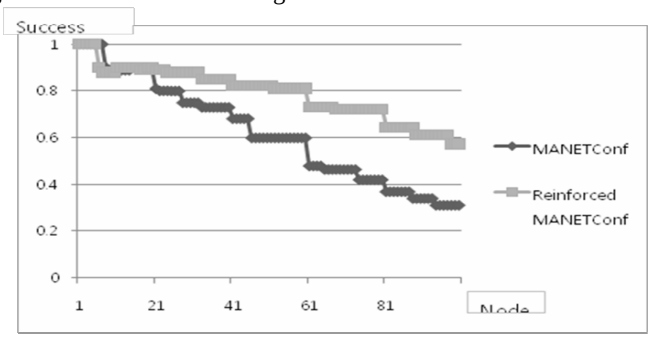

Fig. 10 The result of success message in DAD

As we can see, Reinforced MANETConf has better performance. It is approximately 30% better performance. However there is a side effect as well. Like Fig.11, we can see the significant increase of number of messages. We can not ignore this fact. When there are 100 nodes in the MANET, messages in reinforced MANETConf are 20% more than messages in the previous MANETConf. We should meet the line which is more important between the performance and success. It is pretty sure that it makes sure for the node to be bound with other nodes before sending the data.

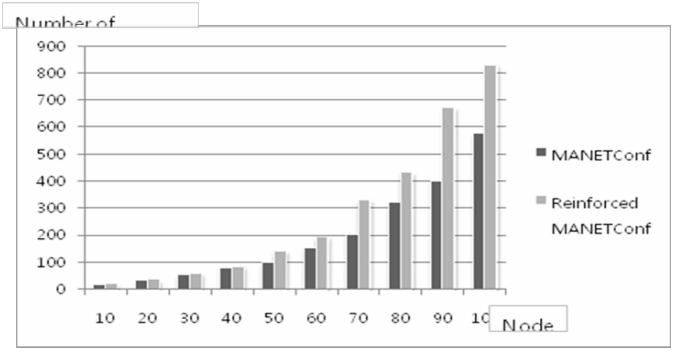

Fig. 11 The result of success message in DAD

VI. Conclusion

Even though there are a lot of researches going on to solve the issue of Auto-configuration in IETF and other researching groups, it is hard to meet the perfect what we want and need. DAD attack is one of the needs to be solved for IP address re-use, network configuration and network management. In this paper we proposed the reinforced MANETConf in the cases of DAD attacks. It can solve the problem of current MANETConf in the cases of DAD attacks. We conduct the simulation to check the performance when such the cases occur in NS2. We checked the success rate of message exchanges when previous MANETConf is conducted and reinforced MANETConf is conducted. The overhead in order to increase the nodes is checked as well. It is sure that reinforced MANETConf has more accuracy and more faithfulness than previous

MANETConf. But it is a significant burden for nodes before biding with other nodes. But reinforced MANETConf is recommended in the view of security.

REFERENCES

[1] C.E. Perkins, J.T. Malinen, R. Wakikawa, E.M. Belding-Royer, and Y.Sun, "IP Address Autoconfiguration for Ad Hoc Networks, draft-ietf-manet-autoconf-01.txt," Internet Engineering Task Force, MANET Working Group, June 2001.

[2] S. Thonmson and T. Narten, "IPv6 Stateless Address Autoconfiguration," RFC 2462, Dec. 1998

[3] Sanket Nesargi and Ravi Prakash, "MANETConf: Configuration of Hosts in a Mobile Ad hoc Network," In Proceedings of INFOCOM,2002

[4] H. Xhou, L. M. No,and M. W. Mutka, "Passive Address Allocation for MANET," Ad Hoc Networks Journal, vol. 1, issues 4 : pp.424-423, Nov. 2003.

[5] P. Nikander, "Denial-of-Service, Address Ownership, and Early authentication in the IPv6 world," presented at Cambridge Security Protocols Workshop 2001, April 2001.

[6] Josh Broch, David A. Malltz, David B. Jothnson, Yih-Chun Hu, and Jorjeta Jetcheva, "A Performance Comparision of Multi-Hop Wireless Ad Hoc Routing Protocols," Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking, pp.85-97 Oct. 1998.