Detection of IP Address Space Exhaustion Attack to Address Allocation Schemes in MANET

Kinnari Vaishnav, Mohit Sati

***Abstract*—Mobile Adhoc Network (MANET) is a network without any infrastructure and no central authority. Absence of central authority makes MANET more vulnerable to various security attacks. MANET uses one of the address allocation schemes for configuration of new node. Address allocation schemes have several threats e.g. Address space exhaustion attack, IP spoofing, Address conflict threat, Address spoofing threat, etc. This paper suggests a novel approach that uses routing table based solution to detect address space exhaustion attack. Our solution uses three fields of routing table: destination address, hop count, hop limit. An ensuring mechanism is suggested in this paper to ensure detection of address space exhaustion in the network.**

***Keywords*—MANET, Address space exhaustion attack, malicious node.**

I. Introduction

Mobile adhoc network (MANET) is a category of wireless network where communicating nodes are moving. MANET utilizes multi-hop radio replaying and capable of operating without any fixed infrastructure. MANET is capable of performing autonomous operation without base station infrastructure and centralized administration. Nodes within the wireless range of each other communicate directly. Nodes outside the range of each other communicate using a multi-hop route through other nodes in the network. This multi-hop route changes with the network topology. Several routing protocols like DSR, ZRP, DSDV, AODV, etc. have been proposed for MANETs [1].

A. *IP Address Allocation Schemes in MANET*

A newly joined node cannot participate in unicast-communication with other node in the network until it has obtained a unique IP address. One of the ways to assign IP address is to pre-assign the IP Address and other related information of a node. Static IP address assignment for MANET nodes is not feasible as it needs to be done manually and requires prior knowledge of MANET's network configuration. This IP-related information includes an IP address, a net-mask, and a default gateway [2]. In wired networks, nodes are configured by a centralized DHCP server. However, this mechanism of assignment of IP address cannot be applied for the MANET, because of the dynamic nature of the network. Nodes can enter, move and leave dynamically. This makes difficult for any single node to maintain all of the information of nodes. MANETs may not have such dedicated servers. Hence, traditional centralized protocols cannot be used to configure nodes in MANETs. The nodes should be capable of being dynamically configured through self-configuration when they enter into the wireless networks. A scheme is required which self-organizes autonomous networks and having less number of control messages [2].

Researchers in the field of MANET have work on address allocation strategies. Researchers have suggested several address allocation schemes especially for MANET till now. Address allocation schemes can be classified as centralized, distributed, and centralized-distributed (Hybrid). Centralized address allocation schemes take help of central node for controlling address allocation process. Central node maintains information about allocated and free IP addresses. Distributed address allocation schemes involve all the nodes in the address allocation process. No central node assigned controlling responsibility of address allocation process. Centralized-Distributed address allocation schemes are those which uses central node for storing IP address information for whole network and some distributed nodes also contribute in address allocation processes. In this paper we have considered one address allocation scheme each of this type. In this paper, we reference a centralized scheme under the title, IPv6 Stateless Address Auto-configuration in Mobile Ad Hoc Network [3] suggested by Dongkeun Lee, Jaepil Yoo, Keecheon Kim, and Kyunglim Kang, a distributed address allocation scheme under the title, MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network [4] suggested by Nesargi and Prakash, and a centralized-distributed address allocation scheme under the title, A Distributed IP Address Assignment Scheme for Ad Hoc Networks [2] by Jang-Ping, Shin-Chih and Li-Hsiang.

B. *Attacks possible to IP address allocation scheme*

MANET is a dynamic, infrastructure less communication network so, chief researches have been proposed till now include routing protocol and auto-configuration. MANET in absence of central authority and due to shared communication medium more exposed to security attacks. This paper considers attacks possible to destabilize, interrupt address allocation process. A. L. Sandoval Orozco, J. García Matesanz, L. J. García Villalba, J. D. Márquez Díaz and T.-H. Kim [5] summarizes various security attacks to address allocation scheme in their paper. This summarization defines various attacks including IP address spoofing attack, address space exhaustion attack, address conflict attack, false address conflict attack, negative reply attack, multiple identity attack, denial of service attack, etc.

Kinnari Vaishnav, Mohit Sati
Gujarat Technological University
India

This paper [5] reviews schemes to detect attacks listed above. Attacks addressed by this paper are described as below:

- Address Space Exhaustion Attack: A malicious node can ask and maintain as many IP addresses as possible until exhausting the address space. Aim of malicious node is to free IP addresses by assigning addresses to fake node. This activity results in prevention of new node from being configured and entering into the MANET.
- Address Spoofing Attack: A malicious node assigns free IP address to itself to participate in the network; its aim is to gather important information necessary to execute active attacks.
- Denial of Service Attack: A malicious node keeps on taking many IP addresses generates large traffic, congestion and overhead in the network. This results in denial of service attacks.

Multiple Identity Attack: A node illegally claims multiple identities. A node demands or assigns itself many IP addresses and participates with different identities in communication.

Rest of this paper is organized as follows. Section II presents the way address space exhaustion attacks can be implemented in various address allocation schemes. Section III presents a scheme to detect address space exhaustion attack. Section IV finally draws a conclusion and future work.

II. Implementation of Address Space Exhaustion attack in address allocation schemes

In this section we present implementation of address allocation space attack in centralized, distributed and centralized-distributed address allocation schemes.

A. *Implementation of Address Space Exhaustion Attack in Centralized Address Allocation Scheme*

A paper titled "IPv6 Stateless Address Auto-configuration in Mobile Ad Hoc Network" [3] describes a centralized address allocation scheme. New node performs two steps procedure to get global IP address: 1) link-local DAD to ensure unique link-local address assignment by new node, 2) T-DAD to ensure unique Global address assignment by node.

Link-Local DAD [3]:

1. A new node chooses random local-link address and broadcast Neighbour Solicitation message to its 1-hop neighbour nodes. It sets DAD_TIME.
2. A new node waits to receive Neighbour Advertisement.
3. If Neighbour Advertisement is not within a time out period the node retries sending the Neighbour Solicitation message up to SENDING_RETRIES.

   Else

   On receiving Neighbour Advertisement new node chooses another local-link address an sends Neighbour Solicitation message again.
4. After all retries no Neighbour Advertisement is still received the address is not in use and that address is taken as its own.

Tunnel-DAD [3]:

1. After assigning link local address, a new node makes tentative global address.
2. A new node selects its neighbouring node that has global address and sends a Neighbour Solicitation message to selected node and sets DAD_TIME.
3. Selected neighbour node establishes a tunnel between itself and Internet Gateway and performs T-DAD on behalf of the new node.
4. Neighbour node passes Neighbour solicitation to Internet Gateway.
5. Internet Gateway receives Neighbour Solicitation and checks uniqueness of the global address by scanning MANET_DAD table.
6. If duplication in global address Internet Gateway sends Neighbour Advertisement to selected neighbour node, selected neighbour node sends this Neighbour Advertisement to new node.

   Else

   Internet Gateway makes entry of global address into MANET_DAD and do not send any message.
7. In case a new node does not receive Neighbour Advertisement within a time out period the node retries sending the Neighbour Solicitation message up to SENDING_RETRIES. After all retries no Neighbour Advertisement received that node assigns tentative address as its own global IP address.
8. In case new node receives Neighbour Advertisement, it chooses new tentative address and repeat T-DAD process again.

IP address space exhaustion attacks can be implemented one of following ways in this scheme.

- Malicious node enters in the network. Randomly picks link-local address and performs link-local DAD then it forms tentative global address and performs T-DAD. After assignment of global address, malicious node again picks new link-local address and performs whole address allocation scheme again and assigned with another IP address. Malicious node keeps on taking new IP addresses and internet gateway keep on doing entries for these IP addresses in MANET_DAD table.
- Malicious node acts like some new node's neighbour and issues T-DAD process again and again for some randomly chosen global address. Actually no new nodes are there around that neighbour and no new node has chosen malicious node as neighbour node to establish connection with internet gateway. Malicious node acting as neighbour node keeps on taking IP addresses and internet gateway keeps on doing entries for these IP addresses in MANET_DAD table.

B. *Implementation of Address Space Exhaustion Attack in Distributed Address Allocation Scheme*

A paper titled "MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network" [4] assigns an IP address to new node in mutually exclusive manner. This scheme works on cooperation of all network nodes. Address allocation process in that scheme [4] can be briefly described as follows:

1. New node chooses random IP address and sends Neighbour_query messages to its neighbours.
2. All neighbour reply by Neighbour_query_reply. A new node will select one of its neighbours and will act as an initiator.
3. Every node maintains a table having allocated, allocate pending and free IP address best of its knowledge. Initiator node checks its table for confliction in allocated or pending allocation entries to find confliction. If no confliction is detected, it enters IP address to pending_allocation list and broadcasts Initiator_request message for new node in the network.
4. On receiving Initiator_request every nodes check requested IP address in allocated or pending_allocaiton lists of table. If there is no confliction in IP address, that node sends affirmative reply to initiator.
5. Upon receiving all affirmative messages initiator updates its table by entering this IP address in to allocated list and removing this IP address from pending_allocaiton list and notifies new node. New node assigns this IP address to itself. Initiator also floods table update message with new node's IP address.

IP address space exhaustion attacks can be implemented one of following ways in this scheme.

- Malicious node enters network chooses a random IP address and a neighbour as an initiator. Initiator node broadcasts request on behalf of malicious node. On receiving all affirmative replies initiator notifies malicious node about uniqueness of IP address and floods table update message. Now malicious node again chooses some IP address chooses a neighbour node and follows the same procedure. Malicious node keeps on taking IP address, following detection procedure and assigning IP address.
- Malicious node may act as an initiator and keep on issuing detection procedure and assigning more and more IP addresses to itself.

Address space exhaustion attack in MANETConf scheme also generates broadcast storm [6] problem in the network.

C. *Implementation of Address Space Exhaustion Attack in Centralized-Distributed Address Allocation Scheme*

A paper titled "A Distributed IP Address Assignment Scheme for Ad Hoc Networks" [2] proposed a centralized-distributed IP address allocation scheme. A central coordinator C-root maintains current status about IP address pool in the network. This scheme [2] uses distributed approach for the process of address allocation. All Coordinators distributed across the network perform address allocation process to new node. Coordinators have set of IP addresses. Coordinators assign an unused IP address from its set to new node. Coordinator allocates half of its IP address pool to new coordinator. Each coordinator periodically reports its IP address pool status to central coordinator i.e. C-root using special message called "back_up". C-root handles common node and coordinator departure conditions. Nodes in the network periodically exchanges hello messages contains information about their closest coordinators. New node obtains IP address from its closest coordinator.
Address allocation process in that [2] scheme can be briefly described as follows:

1. New node enters in the range of established MANET
2. Listens hello packets (containing nearest coordinator information) of its neighbours
3. New node selects nearest coordinator and requests for IP address
4. Coordinator assigns single unused IP address to new node if it is two or less than 2 hops away. It assigns half of its unused IP address pool to node and makes it coordinator if new node is more than 2 hops away from it.

IP address space exhaustion attacks can be implemented one of following ways in this scheme.

- A malicious node joins a network and requests IP address from nearest coordinator. A malicious node assigned with an IP address by coordinator. Malicious node with the intention of IP address space exhaustion attack again issues request to its nearest coordinator and obtains second IP address. This node keeps on asking IP addresses from coordinator.
- A coordinator acts maliciously and implements address space exhaustion attack. Coordinator uses all the IP addresses of its IP address pool and demands more IP addresses from its nearest coordinator.

III. Detection of IP Address Space Exhaustion Attack

This paper assumes that malicious node is not mobile. Our solution does not use any cryptographic algorithms or keys

but, provide routing table based solution to detect address space exhaustion attack. Several routing protocols such as OLSR, DSDV, DSR, AODV, ZRP, etc. have been proposed in MANET. Routing protocol can be classified as proactive, reactive and hybrid. Depending on the routing schemes used nodes maintain different information in routing table. All routing protocols irrespective of their types and routing mechanism, at least maintain following three values for each route entry in the routing table: Destination Address, Next Hop, Hop Count. Destination Address is an address of destination node, Next Hop is the address of the node next to the source node on the path to destination node, Hop Count is hop distance from source node to destination node.

A. *Pre-detection Phase*

Our proposed scheme uses above mentioned three fields of routing table to detect address space exhaustion attack. Malicious node who implements the attack maintains more than one IP addresses. Routing table formed at each node will contain route entries for these all IP addresses. From routing table it can be seen that MANET growing, expanding one side more rapidly than other sides. Routing table entries for one side grows very quick.

If we elaborate an idea to detect address space exhaustion attack, a node part of the MANET can see a particular pattern in routing table. A pattern is, for set of IP addresses (Destination addresses), Next Hop entry and Hop count is same. This pattern in the routing table shows possibility of address space exhaustion attack but, this pattern does not give surety of the attack and malicious activity. Consider an application where some area of the MANET is dense and keeps on growing rapidly, this application also grows routing table entries of one side of the network more rapidly than others.

Any node detects such pattern in its routing table sends a message to upstream node of the set of IP addresses. After detection of pattern in routing table, this node sends a special message to the upstream node of the set of IP addresses. Upstream node of the set of IP addresses also experience possibility of attacks from routing table only. Neighbor nodes of malicious node also find that network is growing rapidly nearby (around).

B. *Detection Phase*

As explained above, routing pattern does not guarantee IP address space exhaustion attack. An upstream node of set of IP addresses performs ensuring mechanism. Fig.1 shows pictorial representation of this mechanism. MANET scenario is shown in the figure, containing genuine nodes with a malicious node. Malicious node has assigned number of IP addresses A, B, C, D, E…. The fig.1 shows an upstream nod performing ensuring mechanism as explain below:

- The upstream node does link local broadcast asking for IP addresses of its neighbour nodes. Sets broadcast_reply timer and waits for replies.

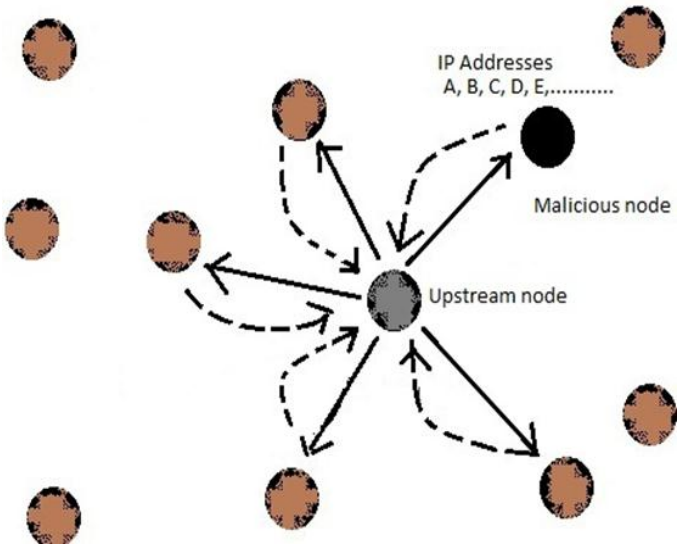

Figure 1. Procedure to detect IP Address Space Exhaustion Attack

- The malicious node cannot process more than one reply before broadcast_reply timeout. It can reply for one of the assigned IP addresses.
- After broadcast_reply timer expires, upstream node checks whether replies from all nodes are received or not. If it did not receive replies from set of IP addresses then it broadcasts a special message again and set broadcast_reply timer.
- The Upstream node repeats this procedure either number of time until threshold is reached or all replies received.
- Upstream node detects address space exhaustion attack around it if it has reached to threshold of retrying. Upstream node releases all IP addresses from which it did not receive replies.

C. *Post-Detection Phase*

The upstream node of a malicious node plays a vital role in detection of IP address space exhaustion attack. The upstream node uses link local broadcasts and replies to verify whether group of IP addresses are assigned by single node or multiple nodes exist. The upstream node frees fake IP addresses at the end of ensuring procedure explained above. Reclamation of IP addresses is performed depending on address allocation schemes as described below:

In a centralized scheme considered in section II-A the upstream node sends list of fake IP addresses to internet gateway. Internet gateway will update MANET_DAD table by removing these IP addresses.

In a distributed scheme considered in section II-B the upstream node broadcasts list of fake IP addresses in the network. All nodes receiving message will remove entries for fake IP addresses from allocated list.

In a centralized-distributed scheme considered in section II-C the upstream node sends list of fake IP addresses to its

nearest coordinator. Nearest coordinator sets status of these IP addresses free and will send this information to the C-Root in the next back_up message.

IV. Conclusion & Future Works

In this paper we presented an innovative scheme for detecting IP address space exhaustion attack in MANET. We have considered initially three different address allocation schemes but, it can be applicable to all address allocation schemes suggested till the day with no or little change. This scheme can be applicable to open network where key infrastructure is not provided. As this scheme is not using key encryption mechanism it avoids key maintenance overhead. In future we will optimize this scheme by preventing collision in the replies by the neighboring nodes of the detecting node and to define threshold value to start the detection phase.

Acknowledgment

The authors appreciate the anonymous reviewers for their valuable comments.

References

[1] M. Thoppian and R. Prakash, "A distributed protocol for dynamic address assignment in mobile ad hoc networks", IEEE Transactions on Mobile Computing, Vol.5, Issue 1, pp. 4-19, 2006.

[2] J. Sheu, S. Tu, L. Chan, "A distributed IP address assignment scheme for ad hoc networks", ICPADS'05, 2005.

[3] D. Lee, J. Yoo, K. Kim, K. Kang, "IPv6 Stateless Address Auto-configuration in Mobile Ad Hoc Network", LNCS 3842, pp. 360 – 367, 2006.

[4] S. Nesargi, R. Prakash, "MANETconf: Configuration of hosts in a mobile ad hoc network", INFOCOM,vol.2, pp.1059 - 1068 , 2002.

[5] A. L. Sandoval Orozco, J. García Matesanz, L. J. G, Villalb, J. Márquez Díaz and T. H. Kim, "Review article security issues in mobile ad hoc network", International Journal of Distributed Sensor Networks, 2012.

[6] S. Ni, Y. Tseng, Y. Chen, J. Sheu, "The broadcast storm problem in a mobile ad hoc network", MobiCom '99, pp.151-162, 1999.