ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

An Overview of Node Auto-configuration Protocols in Mobile Ad hoc Network

Pathe Kiran E[1], Dhage J. S[2]

M.Tech Scholar, Department of Computer Science and Technology, Maharashtra Institute of Tech., Aurangabad, India [1]

Assistant Professor, Department of Computer Science and Technology, Maharashtra Institute of Technology, Aurangabad, India [2]

Abstract: Mobile Ad hoc Network (MANET) is a self organizing network in which mobile devices communicates with each other via wireless links. For unicast communication each node must have a unique IP Address. But In MANET, there is no any fixed infrastructure unlike in wired network. Mobile devices are free to join or leave the network. There is no any central server to assign unique IP Address to each node. Therefore, a protocol is needed which will assign unique IP Address to each node in a dynamic way. In this paper we will discuss different Node Auto-configuration protocols which will assign unique IP Address to each node.

Keywords: Mobile Ad hoc network, MANET, Rabin Cryptosystem, Node Auto-configuration, FAP, MANETConf, Authenticated Dynamic IP Configuration Scheme.

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a network in which set of mobile nodes communicates with each other through wireless links. Unlike wired network, MANET does not need any fixed infrastructure and it can be establish anywhere. The topology of such networks changes dynamically as node joins or leaves the network. Some scenarios where an ad hoc network can be used are business associates sharing information during a meeting, emergency disaster relief personnel coordinating efforts after a natural disaster such as a hurricane, earthquake, or flooding, and military personnel relaying tactical and other types of information in a battlefield [1].

In this type of network, a route between any two hosts may consist of multiple hops through one or more nodes. So mobile nodes are acts as router which forwards the packets to the correct destination node. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic [2].

II. NODE AUTO-CONFIGURATION IN MOBILE AD HOC NETWORK

To interchange messages with each other, each node must have a unique IP address. As discussed above nodes in this type of network joins or leaves the network dynamically. It means there is no fixed infrastructure in mobile ad hoc network. So there should be a mechanism which will assign unique IP address to each node in a network dynamically. A node auto-configuration protocol assigns a unique IP Address to each node.

Due to the dynamic topology of mobile ad hoc networks, auto-configuration protocols are faced with various problems in guaranteeing the uniqueness of IP addresses and in allowing network partitioning and merging [3].

The protocols must achieve the following objectives for correct functioning of the network:

- Assign unique IP Address to every node of the network.
- If a node leaves the network then that IP Address should be available to another node.
- If there is any loss of messages or node failure then protocol should operate to prevent two or more nodes from having same IP Address.
- If any node of the network is having free IP Address then it should assign or give it to the requesting node.
- It should minimize the overhead of additional packet traffic in the network.
- It must be flexible to partitioning and merging of mobile ad hoc network.
- As the topology changes dynamically, so the protocol must conduct synchronization to ensure the configuration of the network is as up to date as possible.

The node auto-configuration protocols can be classified according to address management.

A. Stateful

In this mode, every node maintains the network state. Each node keeps updated copy of tables with IP Address of the nodes.

B. Stateless

In this, every node assigns a random IP Address to itself and then performs duplicate IP address detection to check their uniqueness.

C. Hybrid

This is mixed type of mechanism of above two.

III. PROTOCOLS FOR NODE AUTO-CONFIGURATION IN MANET

A. FAP Protocol

FAP Protocol proposed in [4] is a lightweight protocol that configures mobile ad hoc nodes based on a distributed address database stored in filters that reduces the control

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

load and makes the proposal robust to packet losses and network partitions. Their protocol resolves all address collisions and also reduces the control traffic.
This protocol maintains a distributed database which contains all currently allocated IP addresses in compact fashion. This database is stored in filters. For that purpose they have used two types of filters. One is "Bloom filter" which is based on hash function. And another one is "Sequence filter" which compresses data based on address sequence. These filters assure both the univocal address configurations of the nodes joining the network and the detection of address collisions after merging partitions. They have used hash of these filters as partition identifier for an easy detection of network partitions.
Out of these two filters, the best filter is selected for FAP is based on network characteristics like estimated number of nodes in the network and available addresses.
There are four steps in FAP as follows.

Network initialization: It has two types of initializations. One of them is "Gradual Initialization" in which joining of nodes arrive one after other has long interval time. Another one is "Abrupt Initialization" in which all nodes arrive at same time. FAP is suitable for both of them by using HELLO messages and AREQ messages. Initial node selects the partition identifier and the rest of the nodes are managed by first node. The node uses HELLO messages to show its current status and partition identifier. AREQ message is used to differentiate other nodes generated AREQ messages but with same address.

Node joining: The node which wants to join a network will listens to a medium for some time. If it does not receive any response from the network nodes then it is concluded that there is no network exists and it starts the network. If it receives the response as HELLO message then node joins the network.

Assignment of address: The node which wants to join a network selects an address randomly by using the address range and creates an empty address filter and starts a network initialization phase. In this, it floods the network with AREQ messages to make sure that all initiator nodes have received AREQ messages. Then node sends HELLO messages that are hash of filter. If the initiator node receiver AREQ message with selected address and different identified number then there is address collision. Then node has to wait for some period and have to select a different available address and has to send a different AREQ message.

Network merging: To detect merging, the neighbour nodes in the network is checked if the signature in the message is same as its own, after receiving of HELLO message. Then joining node will ask for that host node to send the address filter of network using Address Filter (AF) message. After the host node receives the AF, it will check the bit I. If I=1 then it shows that the message has originated from the joining node. After that host node replies to the request with AF with R bit set as 1, suggesting that AF is in reply to a previous filter request. If joining node receives an AF reply message then address filter is stored and random available address is selected and then network is flooded with an AREQ message to allocate the latest address which then updates filter messages of other nodes.

B. MANETConf

MANETConf protocol proposed in [5] is based on common distributed database which contains the list of all assigned IP Addresses in MANET. If any new node wants to join a network will broadcast joining request to the nodes and waits for the response. Whoever firstly response to that message will be selected as an initiator node which is responsible to provide a unique IP Address. An initiator node selects a free IP address from his address table and assigns it to the requestor node after receiving the permission from rest of the network nodes. Because it may possible that other node may have chosen same address and his table is not totally synchronized because of message delays or it may possible that two nodes to simultaneously choose same IP address to assign it to different arriving nodes[6]. If it receives positive response from other nodes then that IP address is assigned to that requestor node. And it will broadcast this action to other nodes that keep their tables updated. If one or many nodes reply negatively then initiator concludes that the address is already assigned to a node and it then repeats the same procedure. If there is any node which does not reply then that node put in direct contact with it and then initiator waits for his reply to continue his configuration process. If that concerned node has left the network or does not replying from long time, initiator concludes that concerned node has left the network and it floods this information to all other nodes about his departure.
When two or more networks meet each other then their differentiation is done using Network ID which is a 2-tuple i.e. Lowest IP address used in the network and unique identifier of that node. When a network gets partitioned, one partition will save its network ID and other will detect the partitioning with the first IP assignment then only it will know the new node with lowest ID that will generates the new network ID and floods it within the network. When two or more nodes comes in communication range then they exchange their network identities, if received network identity is different than nodes network identity then network is merged [6].

The main advantage of this protocol is that it guarantees unique assignment of address and each node has ability to assign a new address.

C. Rabin cryptosystem

Rabin cryptosystem proposed in [7] proposes a model for secure IP Auto-configuration using public key cryptography. This model assigns a unique address and secure public key distribution when any new node joins MANET. Security is provided using Rabin cryptosystem which uses asymmetric key encryption.
To assign an IP Address dynamically, they have considered an autonomous ad hoc network which has no gateway or any connection to the external world. The

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

nodes are categorized according to their protocol as follows:

- Allocator: It is a node which maintains all currently allocated lists of addresses. It will allocate a new address to a joining node.
- Initiator: It is an intermediate node between allocators and requestor node that communicates messages between them.
- Requestor: It is a node who wants to join a network and which request for an IP Address.
- Normal: All other nodes are come into this category.

In this protocol MAC address of a requester node is used as nonce. Working of their protocol is shown by following pictorial presentation:

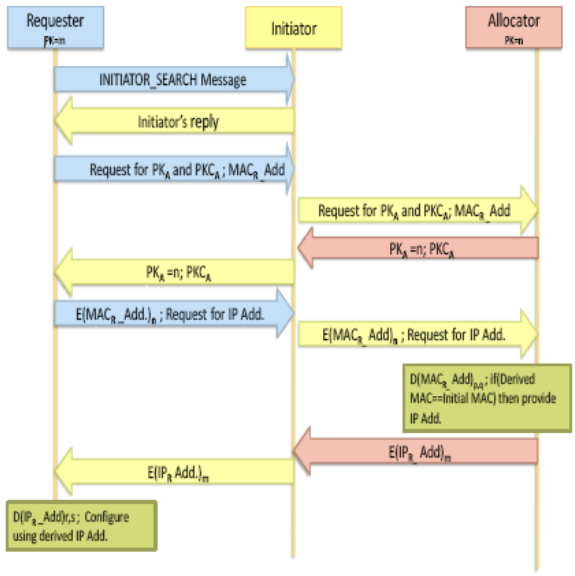

Fig. 1 Pictorial representation of Rabin cryptosystem [7].

In this, a requester node enters in a network and it broadcasts an INITIATOR_SEARCH message to find an initiator node. After receiving response, it will send his MAC address MAC_ADD to initiator and asks for allocator's public key PKA and certificate PKCA. Then receiver forwards this message to allocator node which sends his own public key PKA=n and certificate PKCA to initiator. Requestor sends his own encrypted MAC address E(MACR_ADD)n to initiator node and requests for unique IP Address. This message is forwarded to allocator which decrypts MAC address by using his private keys tuple (p,q) as D(MACR_ADD)p,q. If (Derived MACR_ADD==initial MACR_ADD) then allocator assigns free address to MACR_ADD as IPR_ADD. Then allocator encrypts assigned IP address using requestor's public key PKR=m as E(IPR_ADD)m and send it to initiator. It forwarded to requestor which decrypts it using his private key tuple (r,s) as D(IPR_ADD)r,s. At last Requestor configures itself using that given unique IP address IPR_ADD.

D. ADIP Algorithm

Authenticated Dynamic IP (ADIP) Algorithm proposed in [8] provides authentication based dynamic IP configuration scheme. This configuration scheme securely allocates IP address to authenticated nodes for MANET without broadcasting messages over the network. Each host has capability to generate a new unique IP address from its own IP address to new authenticated host. During IP address allocation process every host uses two distinct secret keys to authenticate the host. Their scheme has capability to handle security threats associated with dynamic address configuration such as address spoofing, address exhaustion, false address conflict, false deny message. Out of these security threats Address spoofing is a common problem occurs during address allocation which means spoofing of IP address by a malicious host to hijack the network traffic. Their proposed scheme has solved the problem of network partitions and mergers along with arrival and departure of a host efficiently [8].

IV. CONCLUSION

In this paper, we have reviewed node auto-configuration classification and their objectives. We have presented a survey report on various node auto-configuration protocols and their working.

ACKNOWLEDGMENT

I am genuinely thankful to Prof. Mr. Dhage J. S., who directed me in right way for penning above work, of Computer Science and Technology Department, MIT, Aurangabad.

REFERENCES

[1] Wiley Series on Parallel and Distributed Computing, Albert Zamya,Series Editor "Algorithms and Protocols for Wireless Mobile Ad hoc networks" Edited by AZZEDINE BOUKERCHE.
[2] http://en.wikipedia.org/wiki/Mobile_ad_network.
[3] L. Villalba, J.G. Martinez, A. Orozeo and J. Diaz, "Auto-configuration Protocols in Mobile ad hoc networks", Sensors, pp 3652-3666, 2011.
[4] Natalia Castro Fernandes, Marcelo duffles Donato Moreira, and Otto Carlos Muniz Bandeira Duarte, " An Efficient and Robust Addressing Protocol for Node Auto configuration in Ad Hoc Networks", IEEE transactions on networking vol. 21, no. 3, pp 845-856, June 2013.
[5] S. Nesargi, R. Prakash, "MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network" – IEEE INFOCOM, 2002 – ieeexplore.ieee.org.
[6] Bachar Wehbi "Address Autoconfiguration in Ad Hoc Networks" Institute National des Telecommunications-INT-Department Logiciels Reseaux –LOR-Internal Report , May 2005
[7] Jagrati Nagdiya, Shweta Yadav, "Secure Autoconfiguration in Mobile Ad hoc networks using Rabin cryptosystem", ISSN 2250-2459, ISO 9001:2008 Certified Journal, vol. 4, Issue 4, April 2014 www.ijetae.com.
[8] Uttam Ghosh and Raja Datta, "An Authenticated Dynamic IP Configuration Scheme for Mobile Ad Hoc Networks", IEEE, 2009.