ISSN: 2321-7782 (Online)
Volume 3, Issue 5, May 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Secure and Self-Managed Node Configuration Addressing Protocol in MANET

Shaheena T P[1]
Computer Science Department
MEA Engineering College
Calicut University, India

Jemsheer Ahmed P[2]
Computer Science Department
MEA Engineering College
Calicut University, India

Abstract: ***In mobile adhoc network, the node moves from one network to another. The mobility of the node makes network partitions frequently. Then the node needs new and unique address to communicate to another node which will not collide with the other address in that network. So the address allocation is the key challenge in mobile adhoc network. Network initialization is another challenging issue because of the lack of centralized mechanism in the mobile network. To avoid address collisions in a dynamic network with fading channels, frequent network partitions, partition merging and joining or leaving nodes, it requires a distributed and self-managed mechanism. Most of the subsisting protocols are generally relegated on the substructure of the address management less on security issue. Here concentrate on Filter based Addressing Protocol and to propose a solution that safer against malicious host activities and reduces IP collision while joining and merging process is occur.***

Keywords: MANET, Address auto-configuration protocol, Address allocation, partition and merging, collision detection.

I. INTRODUCTION

Mobile Adhoc Networks (MANETs) are infrastructure less, flexible self-organizing network. This network is created by mobile nodes without any existing infrastructure. In MANET, the mobile nodes needs to identified mutually before communicate with each other. Then the node needs new and unique address to communicate to another node which will not collide with the other address in that network. The mobility of nodes makes network partitions frequently. Consequently, the node moves from one partition to another. Then the nodes need to create new address to avoid address collision in that partition.

The address allocation and routing are the most important processes that performed by the nodes in the mobile adhoc network. This characteristic increases the configuring speed of initialization of network with minimum infrastructure. Faster configuration of this network enhances the use of situations like military application and other emergency situations where high mobility is necessary.

Due to the lack of infrastructure, various challenges are encountered, i.e. network partition and merging partition, abrupt initialization and leaving node, simultaneous address request etc. The main issue is network partitioning due to the mobility of nodes. The Dynamic Host Configuration Protocol (DHCP) [1] and Network Address Translation (NAT) [2] are conventional protocols cannot be used to handle the dynamic nature of nodes in this network and difficult to assigning address to joining nodes. The address allocation is the key challenge in mobile adhoc network due to the above reasons.

The implementation of auto-configuration of node is more difficult in MANET than a wired network such as local area network. Because, due to the flexibility of mobile nodes, lack of infrastructure and open system etc. For this network, a distributed mechanism is more desirable to mobility of nodes and dynamic topology.

In MANET, there may be address conflict at the time of merging of different network partition. The auto configuration of node brings some issues that change the IP address during communication. Consequently, some of the nodes need to change the

duplicate addresses in the network otherwise it will interrupt ongoing communication. So, a protocol is needed to perform the network configuration task dynamically. In this literature, there exists variety of auto configuration protocols. All these protocols are generally classified on the basis of the address management.

Main Contribution of this paper is to detect malicious nodes after configuring nodes. For detecting malicious node here using the Bloom filter of particular node to identify their position based on the neighbors. The proposed solution uses neighboring node IPs instead of location information in order to detect malicious IPs. Neighboring node IPs are presented with a constant size using BFO (Bloom Filter Output). This output as a proof. Furthermore, the overall overheads in communication can be minimized by implementing this FAP protocol over the existing system.

The remainder of this paper is organized as follows. In Section II, we explain motivation of the auto-configuration protocol. In Section III, we describe the analysis of related work and compare the performance with Filter base addressing protocol. In section IV, described the identified problem in FAP. In Sections V, described the proposed work i.e. detecting the imitating node (i.e. processing against malicious attack) and their detection scenario using the Bloom filter technique and section VI, describe the simulation environment and the performance analyses, respectively. Finally, we conclude this paper in Section VII.

II. MOTIVATION

Nowadays the uses of mobile devices are increasing in high order. Due to this reason the address allocation is one of most important network parameter for the mobile nodes. Lack of a valid unique IP address, a mobile node cannot communicate in a unicast system but it can receive and send broadcast messages. The most existing addressing protocols focus on efficiency and correctness but not on security issues. The Filter based Addressing Protocol (FAP)[3] identifying and solving address collisions with a low control load and reduce communication latency. Here proposed system also works on detecting malicious nodes.

III. RELATED WORK

Zhong Fan and Siva Subhramani [4] proposed a stateless method to IPv6 address auto-configuration in ad hoc networks. An incipient node joins the network, then obtaining a non link local prefix and a device number which form an IPv6 address and sending with Address Request (AREQ) message. After sending AREQ, waiting a period for any response on the network. It will not receive any AREP, the node act as first node in that network. Otherwise it precedes Duplicate Address detection (DAD) [5] procedure. This initialization node also chooses a unique identifier (its MAC address) for this network. This identifiers act as partition identifier for the detection of partitioning and merging. Hello messages utilized by a node to advertise the network status to neighbors periodically. It includes chosen IP address and partition identifier. A joining node configured itself with an IP address and selecting partition identifier from the receiving hello message. When a node receives a hello message with a different partition identifier, it will detect that two partitions are merging and DAD procedure is triggered. All nodes in the merged network accede on an incipient prevalent partition identifier. So, the incipient network ID = ID1 +ID2. The first node detecting the merging of two partitions it includes incipient ID in the AREQ messages and it send to all other nodes in that network.

Sadique Bugti, Xia Chunhe, Li Wie, Ejaz Hussain [6] proposed a method cluster based addressing scheme in VANET (CANVET) that used for auto node configuration in VANET. There are different category nodes used for the formation of cluster.

- Undecided Vehicle (UV): The vehicle, which starts to find existing network.
- Non clustering Vehicle (Non CV): The vehicle which is not connected to any network.
- Member Vehicle (MV): The vehicle which is after joining a cluster.
- Cluster Head (CH): The vehicle which is the backbone of a cluster. It keeps two tables one for member vehicles and other for neighbouring cluster heads and the unique IP address assignment remains the duty of cluster head.

» Clusters Gateway (CGW): The vehicle which maintains its position between two CHs in order to keep cluster heads connected with the other.

The cluster heads maintain two tables; the member table is used to maintain updated information about MV such as assigned IP addresses, location, position, speed, status and role of the member vehicle in cluster. The neighbour cluster head (NCH) table is used to maintain updated information about the neighbouring CHs. The Joining Vehicle (JV) sends request for an IP address to the cluster. If the address request directly received by cluster head then cluster head allocates IP address for JV. If the address request (AR) received by any member vehicle then the member vehicle forward the request to cluster head and cluster head allocate address replay through member vehicle. This address request reply packet contains cluster head ID (CHID) plus allocated new Member Vehicle ID (CHID+MV). After receiving AR Replay the JV send AckMsg to CH, and joins the cluster and changes its status to MV. The AR is received by The CGW which forwards the AR to CH and reply back to JV with AR Replay. After receiving reply back from CGW, the JV and sent AckMsg to CH.

Amit Munjal, Yatindra Singh, AKrishna Phaneendra, Amitabha Roy [7] proposed a method Scalable Hierarchical Distributive Auto-Configuration Protocol (SHDAP) makes use of IPv6 local unicast address. This address has 128 bits. In this format consists prefix (7 bits), Global ID (41 bits), partition ID (16 bits) used instead of subnet ID in IPv6 and interface ID into two parts i.e. cluster ID (48 bits) and node ID (16 bits). There are different category nodes used for the formation of cluster. i.e. cluster head, configured node and requester node. When a new node joins in the network, it broadcast the network neighbour query message (NQ). After sending network neighbour query message, waiting a period of time for any network reply message (NP) on the network. It will not receive any reply message, the node itself act as cluster head in that network. Then cluster head randomly selected random partition ID, random cluster ID and assign itself with the node ID 1. The cluster head allocates addresses to other joining nodes and starting the node ID from 2 onwards. When a new node enters the existing network it broadcast a NQ message. All existing node respond with NR message to requester after receiving NQ message. The NR message consists hop distance of its cluster head and partition ID. If the requester receives more than one NR message from neighbour nodes, it only selects the neighbour node with least hop distance from its cluster head node. The network partition occurs when the node moves out of range from the existing partition or parent partition to form a small child partition. Nodes broadcast the hello message periodically to verify whether that node alive in that network. Here partition ID of each node will not change on any partition will occur, because the partition ID of each node is defined as a part of IP address only. It reduces the control overhead. In the merging process, there is no need for exchanging partition ID only exchanges their routing table. The main idea of this protocol is to logically divide the address space in to three fields and making ideal solutions for large scale MANET.

Natalia Fernandes, Marcelo Donato Moreira, and Otto Muniz Bandeira Duarte [4] proposed a Filter based Address Protocol (FAP) that based on distributed address database stored in filters. This filter reduces the control over head and packet loss in the MANET. There are two filters, bloom filter and sequence filter. The partition identifier defined by hash of the filter providing the detection of network partition. The bloom filter is a data structure for address distributed application. The sequence filter is also a data structure it stores and compresses the address based on the sequence of addresses.

When a new node joins in the network, it listens to the medium for a particular period. If the node does not receive any hello message in that network, it acts as initiator node itself. An initiator node chooses an address randomly, and it creates an empty filter to starts the network initialization. An initiator node broadcast the AREQ message N_f times in to the network. If more than one initiator node is there to broadcast the AREQ message, increase the reception of AREQ message by all nodes present in the network. Therefore the node leave in the initialization state and received address insert into the address filter. And then the node starts to send the Hello messages with filter signature which is the hash value of the address filter. If the initiator node receives the same address with different identifier then node finds there is the address collision. In this situation the node wait for particular time and choose another available address.

Merging events are also detected based on Hello and AF messages Nodes in different partitions choose their address based only on the set of addresses of their partition. Hence, nodes in different partitions can select the same address, which may cause collisions after the partitions merged. When a node receives a hello message with a different address filter in hello message, it will detect that two partitions are merging. A node chooses the addresses in their own partition. Therefore, nodes in different partitions can select the same address, which may cause collisions after the partitions merged. In this situation, both node exchange filter of its two partitions, each node on the lowest-priority partition must check whether its address is on the other partition filter to detect collisions. If there is a collision, the node randomly chooses an available address in both filters and broadcast the network with an AREQ to allocate the new address. The utilization of the hash of the filter instead of an arbitrary number as the partition identifier creates a better representation of the set of nodes. Hence, a transmutation in the set of nodes is automatically reflected in the partition identifier.

It presents more minute delays in the joining node procedure and on network partition merging events than the other proposals. This proposed protocol is more suitable for very dynamic environments with frequent partition merging and node joining events. FAP is an effective in handling network partitioning and merging using a simple data structure such as bloom filter and sequence filter. It is also able to prevent duplication of address and less communication control overhead.

In FAP, here uses two different filters depending on the scenarios. The sequence filter is a structure to store the address based on sequence of address and the Bloom filter is explains later.

Sequence Filter:

The sequence filter is a data structure to store and compact the addresses based on address sequence. The structure of the sequence filter is shown in Fig.1. The sequence filter created with a range of constant bits followed by the network address. In this filter, suffix of each address represented by one bit. Initially it set to zero. Each suffix of address set the correct position of that sequence filter. The first address of network used as network address. So this address doesn't assign to any other node in that network. The next address in that address sequence set in first bit of the sequence filter. Consequently, the address 192.168.100.4 is set in third bit position in corresponding filter.

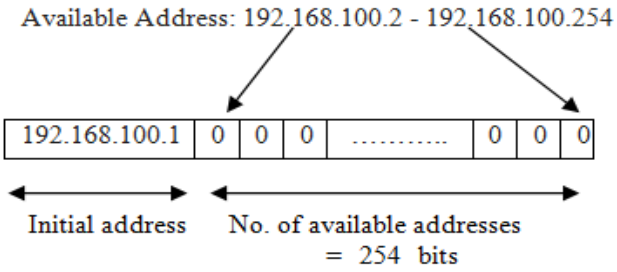

Fig.1. Sequence Filter

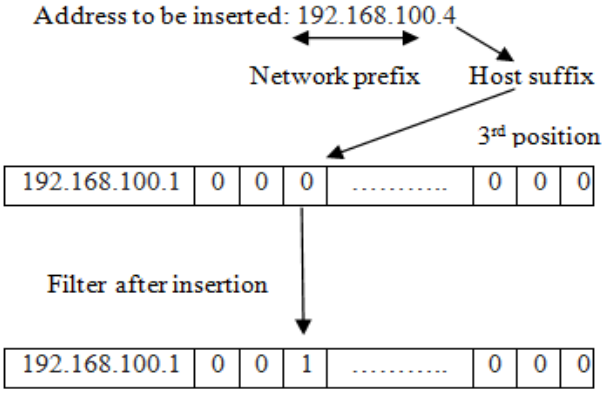

Fig. 2. Insertion of elements in the Sequence Filter

a) Observation Analysis

TABLE I shows several protocols share some common characteristics. However, they also differ in a wide range of issues. Here using parameters such as control overhead and communication latency that can be used to analyze the performance of an auto-configuration protocol for mobile adhoc networks.

The time between the points that when a node initiates auto configuration and when it is assigned a free IP address is referred as latency. Communication overheads during the auto configuration process and the increase in overhead due to resolving address conflict were additionally evaluated.

The filter based addressing protocol is the stateless configuration; it reduces control overhead and latency of address allocation because of their less control statements. It presents more minute delays in the joining node procedure and on network partition merging events than the other proposals. FAP is an effective in handling network partitioning and merging using a simple data structure such as bloom filter and sequence filter. It is also able to prevent duplication of address and less communication control overhead.

TABLE 1: Comparison of existing auto-configuration protocols

Methods	Techniques Used	Control Overhead	Address Allocation Latency
Fan and Subhramani's maethod *[3]*	Using NDP and DAD, stateless configuration, IPv6 address format.	High	High
CANVET *[7]*	Using clustering, stateful configuration, IPv6 addressing format.	High	High

SHDAP *[8]*	Using Clustering, stateless configuration, and IPv6address format.	Medium	High
FAP *[4]*	Using Bloom and sequence filter, stateless, IPv4 address format.	Less than Other protocols	Reasonable, based on control message(here less control messages are used)

IV. Problem Statement

The auto-configuration protocol FAP mainly focused to reduce control overhead and detecting the collision while partition merging is occur. The FAP is also focused to reduce the communication latency in order to reducing the control load. Namely, FAP only concentrate on effectiveness of auto-configuring the node in MANET. Sometime after configuring, some nodes in MANET operate maliciously i.e. nodes change their IP address into existing address in that network partition. It may cause to IP collision and hijack the information of other nodes in network.

V. Proposed Work

This work is introduces a method of detecting duplicate IP addresses and to avoid IP collision and malicious activities. The main idea of the work is to use neighbouring node IPs of a newly inserted node to create a bloom filter keeps the information of location of that node in that networks. The neighbouring node IPs are compressed and encoded by a Bloom filter sequentially, and used as a proof to detect malicious node. Subsequently, the validity of the proof is verified by comparing two Bloom filter outputs for the same node IP among the receiving messages from the neighbours.

a) Working Diagram

Each node create the bloom filter after finding their neighbors and broadcast to other nodes in that partition. Then each node checks whether duplicate address among their neighbor nodes. Here using Bloom Filter to collecting IP address of neighbor nodes of each node and output of this filter provide the location information of each node. This message proof floods to the network for the identification. Here some nodes act as malicious node can freely choose IP address of any configured node in that network. Consequently, some nodes receive same IP in this authentication message from different nodes. These nodes (victim node) check the bloom filter of each node and detect the malicious node according to their BFO.

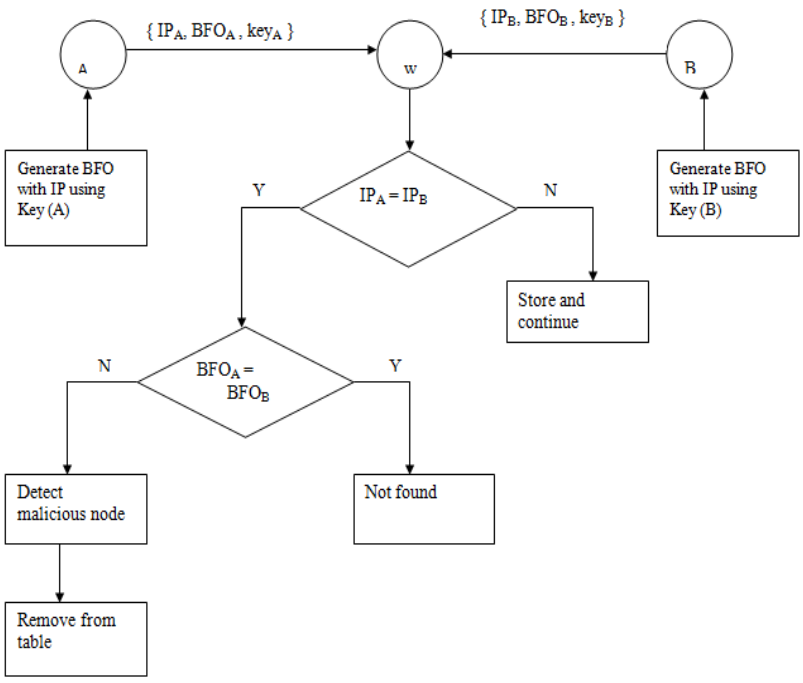

Fig. 3: Working Diagram of proposed work

b) Working Description

In this work, creating a proof for identifying malicious while malicious is created and updated in a newly added node, which may be malicious. For this, here define a bloom filter creating k independent hash functions and Bloom Filter Output (BFO) consists of m bits. Each node requests IP from each neighboring node. During this request, all nodes receive a reply message (IP and key) from their neighboring node. Consequently all nodes create and update their BFO (authentication message) and broadcast it frequently. Fig.3 shows a diagram that a node checks whether neighboring node IPs registered to a proof (BFO) or detecting the duplicated IPs are malicious or not. If there is a node received same IP from different neighboring node it checks their BFO. If the BFO is different, the node is identified as malicious.

1. Bloom Filter

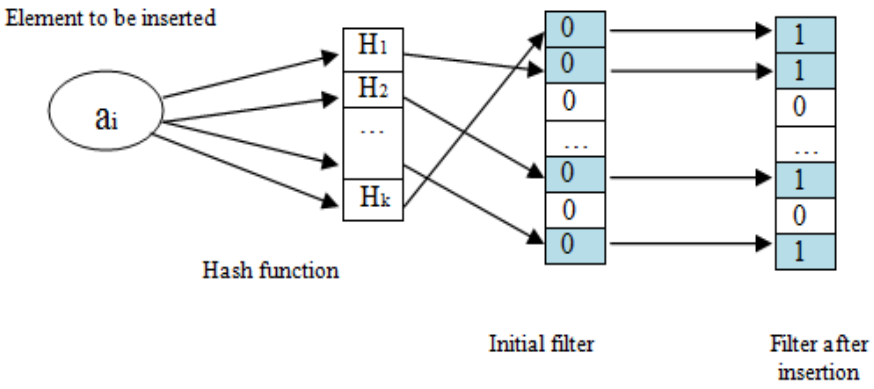

Fig.4. Insertion of element to the bloom filter

The Bloom filter is a compact data structure used on many applications, IP trace back and web cache. BF is an m bits vector representing a set A= {a1, a2, a3…an} composed of n elements. The elements are inserted into the filter through set of independent hash functions (H1, H2, H3… Hk) which outputs are uniformly distributed on m bits filter. Initially all bits are set to zero. Then, each element ai ϵ A is hashed by each of the k hash functions, which result provide a position set as 1 on m bit vector.

Here, each new node is handled by a Bloom filter which are compressed and encoded by neighbouring node IPs and to create a proof to detect malicious node. Each elements in the above set represent the neighbouring node IPs and set a position in m bit vector.

VI. Simulation Result

Here implement the simulation experiment using tool network simulator-2 (version 2.34). The evaluations are mainly focused on control overhead, collision overhead, address allocation latency and collision rate between existing protocol and proposed work.

a) Simulation Setup

The network maximum 35 nodes are simulated and the simulation area is 1000m × 1000m. It considers the two- ray ground model for the simulation ratio propagation and NS-2 IEEE 802.11 model for the Medium Access Control. The transmission range of the node was set to 250m and using bandwidth is 10 Mbits/sec. Traffic source have been chosen to be CBR (Constant Bit Rate) and the packet size is 512 bytes. The underlying routing protocol used for routing the packets was AODV (Ad hoc On-demand Distance Vector Routing Protocol).

b) Result Analysis

In this simulation, the procedure of this addressing protocol includes network initialization, joining node, partition merging and leaving a node in that network. In existing addressing protocols are generate number of control messages for the above

procedures. Consequently, reduces the available bandwidth and increase the address allocation latency. So that using some time parameters based on this simulation to increase the performance of protocol. The number of receptive control messages are depends on the time parameter used for this simulation. Therefore, to reduce control messages between the nodes for their address configuration. Shown in Fig.4.

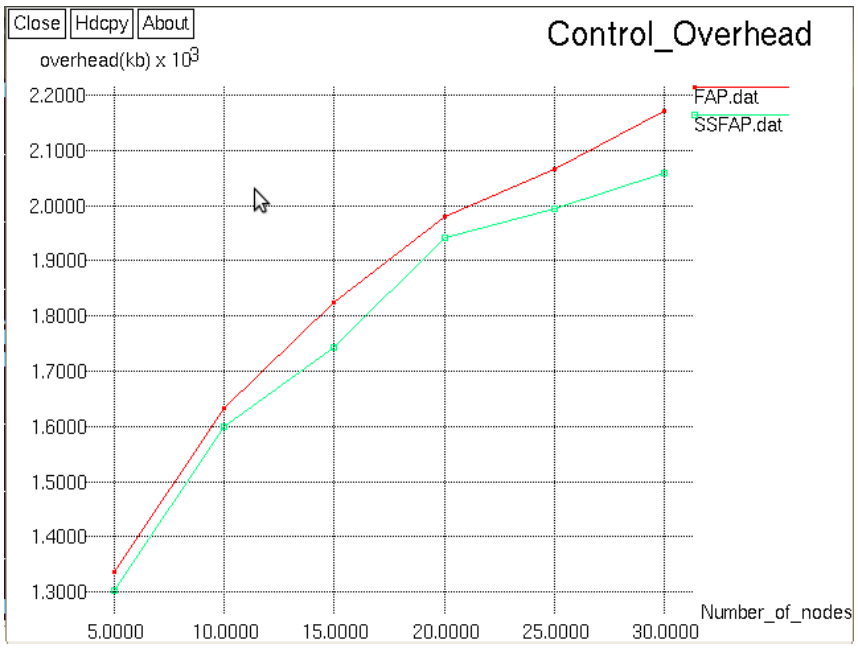

Fig.4. Control Overhead

Address conflict is a major problem in node auto-configuration process. Because, the process of the network initialization, merging network partition and attack of malicious nodes. In the network initialization, the abrupt nodes are randomly selected addresses may similar. Similarly, IP collision may detect while partition merging is occur. Sometimes some node act as malicious node, they imitate the existing node IP address. For the above reasons, in the enhanced work using a Bloom filter as a proof to detect the IP collision or malicious node and deleting the entire node in the table. Therefore reduce the control message while the IP collision is occurring. The xgraph is shown in Fig .5.

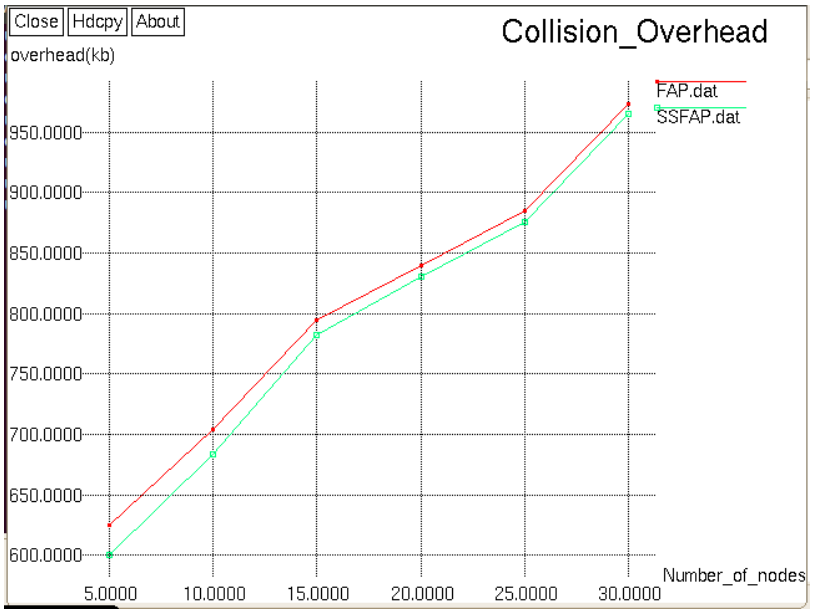

Fig.5. Collision overhead

In this proposed work, improve the performance of reducing the IP collision due to the BF technique. Shown in Fig. 6.

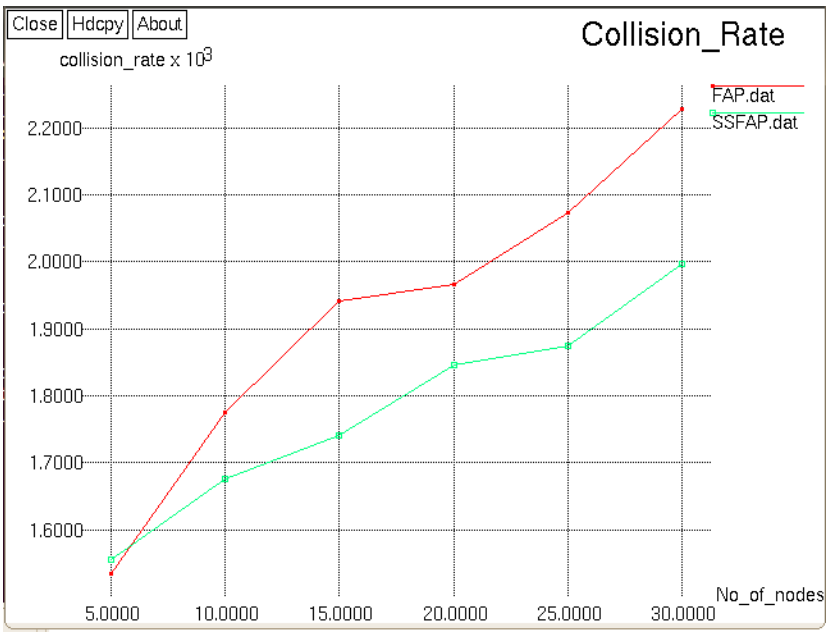

Fig.6. Collision Rate

The address allocation latency is the time taken by a node to get self configured in that network without any IP collision. The average configuration delay between the different transmissions ranges (different no of nodes) of proposed work is shown in Fig. 7. The latency of auto-configuring node is reduces due to the less control messages.

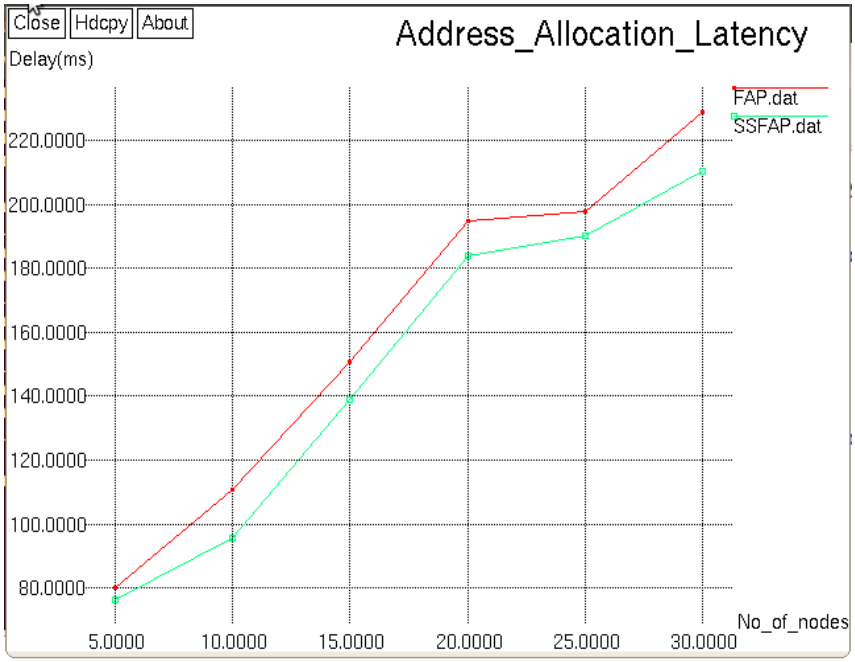

Fig.7. Address Allocation Latency

VII. CONCLUSION

This paper presented the critical analysis of different distributed and auto configuration protocol which aims at handling the challenge of address allocation in mobile ad hoc network. Due to the dynamic topology of mobile adhoc networks auto-configuration protocols face many problems with assuring the uniqueness of IP addresses. An efficient protocol, Filter based Addressing Protocol (FAP) definitely has an edge over others. This protocol enables MANET nodes to configure the network parameters of incipient nodes entering the network. These protocols designates the solutions to reduces address collision in the different situation such as addressing nodes, joining and leaving the network, network partition and merge. FAP reduces control overhead and communication latency of address allocation because of their less control statements. It presents more minute

delays in the joining node procedure and on network partition merging events than the other proposals. FAP is an effective in handling network partitioning and merging using a simple data structure such as bloom filter and sequence filter. It is also able to prevent duplication of address and less communication control overhead.

Here, a solution has been proposed for encountering security issues in the Filter base Addressing Protocol. The enhancement work is safer against the attack of malicious nodes (using same IP address) and to become reduces the IP collision. In the proposed system each node is handled by a Bloom filter. The main idea of the work is to use neighbouring node IPs which are compressed and encoded by a Bloom filter sequentially, and used as a proof to detect malicious node. Subsequently, the validity of the proof is verified by comparing two Bloom filter outputs for the same node IP among the receiving messages from the neighbours.

In this simulation, verified the protocol Secure and Self-managed Addressing Protocol (SSFAP) and achieved better results when compared to the Filter-based Addressing Protocol (FAP). By using SSFAP it provide better address allocation latency and less control overhead. It also provides better collision detection efficiency and address spoofing attack (malicious node). Because every node checks its IP address and location information with its received Bloom filter authentication method. In future, this filter technique can be improved to detect the false address conflict attacks and negative reply attacks in this self configurable network.

ACKNOWLEDGEMENT

We take this opportunity to express our gratitude to all who encouraged us to complete this work. We would like to express our deep sense of gratitude to MEA engineering college, Perinthalmanna to support our work. And also wish to express heartfelt thanks to the anonymous reviewers for their all contribution to improving the quality of this paper

References

1. R. Droms, “Stateless dynamic host configuration protocol (dhcp) service for ipv6,” 2004.
2. P. Srisuresh and K. Egevang, “Traditional ip network address translator (traditional nat),” 2001.
3. N. C. Fernandez, M. D. D. Moreira, and O. C. M. B. Duarte, “An efficient and robust addressing protocol for node autoconfiguration in ad hoc networks,” IEEE/ACM Transactions on Networking (TON), vol. 21, no. 3, pp. 845–856, 2013.
4. Z. Fan and S. Subramani, “An address autoconfiguration protocol for ipv6 hosts in a mobile ad hoc network,” Computer Communications, vol. 28, no. 4, pp. 339–350, 2005.
5. Y. Sun and E. M. Belding-Royer, “A study of dynamic addressing techniques in mobile ad hoc networks,” Wireless Communications and Mobile Computing, vol. 4, no. 3, pp. 315–329, 2004.
6. A. Bugti, X. Chunhe, L. Wie, and E. Hussain, “Cluster based addressing scheme in vanet (canvet stateful addressing approach),” in Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on. IEEE, 2011, pp. 450–454.
7. A. Munjal, Y. N. Singh, A. Phaneendra, and A. Roy, “Scalable hierarchical distributive auto-configuration protocol for manets,” in Signal-Image Technology & Internet-Based Systems (SITIS), 2013 International Conference on. IEEE, 2013, pp. 699–705.
8. Cho, Kwantae, Byung-Gil Lee, and Dong Hoon Lee. "Low-Priced and Energy-Efficient Detection of Replicas for Wireless Sensor Networks." Dependable and Secure Computing, IEEE Transactions on 11.5 (2014): 454-466.

AUTHOR(S) PROFILE

Shaheena T P is PG Scholar, currently pursuing her M.Tech in Computer Science and Engineering at MEA Engineering College, Perinthalmanna, Malppuram, Kerala. She has completed her B.tech from University Engineering College, Kariavattom, Thiruvananthapuram, kerala.

Jemsheer Ahmed P is currently working as an Assistant Professor in Computer Science and Engineering Department, MEA Engineering College, Perinthalmanna, Malppuram, Kerala. With 5 years of rich experience in the field of System Administration, Server Management and Virtualization held the post of System Analyst and Software Architect for R&D wing of MEA Engineering College. He is a Post Graduate in Software Engineering and Graduate in Computer Science and Engineering. Software quality management, project management and software testing are the major areas of specialization.