PUZZLE BASED APPROACH TO NETWORK SECURITY WITH AN EFFECTIVE ADDRESS ASSIGNMENT PROTOCOAL

LIMMA MARY RODRIGUEZ,
PG Scholar, Department of CSE,
Dhanalakshmi Srinivasan College of Engineering,
Coimbatore- 641 105

Abstract— In MANET all nodes will moving from time to time. For communication in MANET, there is no domain power to control it. The process of giving IP address to each node is a big deal. So it is harder to take off a collision less transmission. The process of giving IP value to each node is harder .Node in the sense each system in network .In this paper I propose an efficacious protocol for successful communication of system in network and also provide a defense mechanisam using game theory in network. The protocol will find where the communication failed ,it will trace out the IP of failed connection and provide successful connection with valid IP address. It is the effective remedy to the data loss in network and high rate of traffic in network. I put forward network security to MANET by giving the essence of game theory to propose a no: of puzzle based defense against attack. It will find the source, IP address, host number etc to the attackers .The result shows that my paper provide secure, successful data transmission and communication between network

***Index Terms*—MANET, IP address, game theory, puzzle based defense, attacker, defender, address assignment**

I .INTRODUCTION

A mobile ad-hoc nerwork is a continuously self arrangement, less purposefull network of mobile devices connected without wires. Ad-hoc is latin and means “for this wantage”. Every node in a MANET will move from time to time. The main problem in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such network may operate by themselves or may be connected to larger internet. They may contain more than one and different transievers between nodes .MANET nodes are equipped with wireless transmitter and reciever using antenna. A scenario of MANET in fig 1.1

The MANET has a major problem of address assignment. The node in ad-hoc network often changes its partition in the network and need a unique address to communicate with a new partition. The address assignment to the new node should be collision free one. Most of the system which are previously implemented suffer a lot to assign the collision free address assignment. The proposed system attempts to solve this collision free address problem. Due to the dynamic topology of MANET, auto assignment protocol faced with various problem in guaranteeing the various uniquiness of IP address.

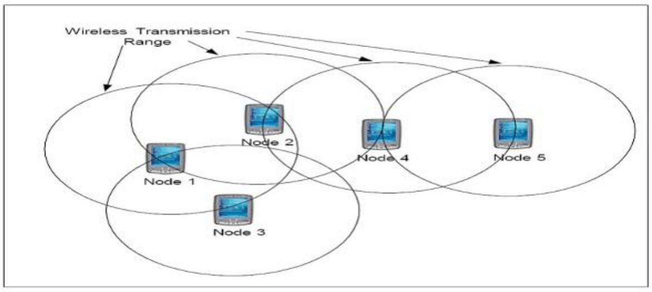


Fig 1.1 A MANET scenario

Network security becomes a challenging topic and new network attack cause vast loss to network resourses. Game theoritic approaches have been introduced as auseful weapon to handle those clever network attacks. It shows the interaction between the attacker who launches flooding attackes and defender who counters the attacks using puzzle based defense. This system attemps to find source of attacker,IP address, host number etc within the time period of interaction between attacker and defender. So we can avoid unauthorized access and also it will provide a secure data transmission.

II. RELATED WORK

There will be more researches and implementation were done in the MANET field. Most of the concepts were much efficient and there will be also have some drawbacks in there related area. In [1] they propose a protocol that arrange MANET nodes based on a clustered address database stored in filter that reduce control load and put forward a remedy to packet miss and network division. In [2] they point out network security. They review the existing gane theory based solution for network security problem and classify their application scenarios. In [3] a active scheme for automatic allocation of IP address in MANET introduced. In [4] they propose a new IP address allocation algorithm called prophet allocation. In [5] they propose a filter based addressing protocol for auto configuration of MANET and it is efficient to the packet miss. In [6] they present a distributed automatic host protocol proposed to configure node in a MANET.

In [7] feasibility of DAD approach is investigated, The detection of duplicate address is passive way, only by monitoring routing protocol traffic, three concepts of passive DAD is proposed. An approach [8] to IPV6 address auto configuration in ad-hoc networks. It apply stateless address auto configure protocol and neighbour discover protocol to context of ad-hoc networks. Mean field game theory provides a mathematical tool for problem with a large no: of players, their proposed scheme [9] can enable an individual node in MANET to make security defense decision without centralized administration. In networking computing systems [10] propose a new approach to automated response called the RRE. The engine employs a game theoritic response against adversaries modelled or opponent in a 2 player stochastic game.

SIFTER ADDRESS PROTOCOL

The sifter address protocol(SAP) aims dynamically auto configure network address,resolve collision with low control load, even in entering and exiting event. To obtain all these objectives SAP uses a spreaded compact sifter to represent the current set of allocated addresses. This sifter is present at every node to simplify frequent node entering event and reduce the control overhead required to solve address collisions inherent in random assignments, afterall i propose the sifter signature, which is hash of address sifter as a division picker. The sifter signature is an important feature for easily detecting network. Clubing event in which address conflicts may occur. I propose the use of two sifter which based on hash function and succession sifter which compress data based on address progression

A. TINGE SIFTER

The tinge sifter is a data structure used for SAP. There will be m bit representation from (0,1,2……n). The elements are inserted with SAP function , h1,h2,h3…… hk. After insertion of elements check whether it is in position. Then it will insert the 2 m bit insertion.

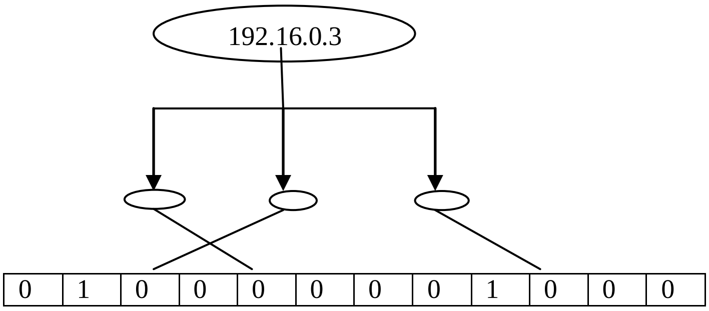


Fig 3.1 insertion of address elements in SAP

B.SUCCESSION SIFTER

The succession sifter will stores the addresses on the basis of sequence of address. The sequence of address inserted will be concatenated.The sifter size increases the no: of node participated also increases. The bit size also increases.

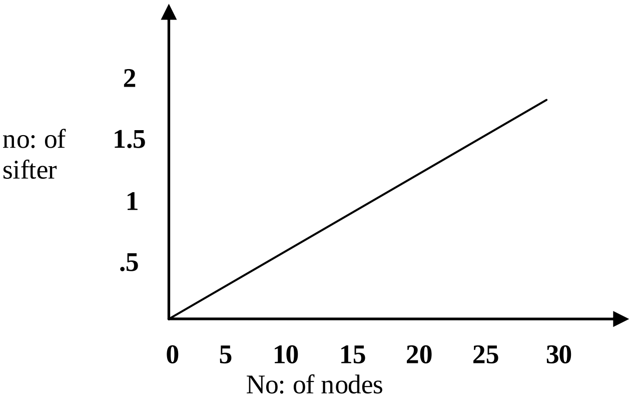


Fig 3.2 succession sifter graph

SAP PROCEDURES

The architecture of protocol shows different procedures like entering node management, exiting node management, network division clubbing, head selection management. it will be shown in fig 3.3. The existing system which is already in network. When a new node comes to join the network it becomes entering node ,it asks for head node to send address sifter and head node send it to entering node. The entering node chooses the available address and then it send to head node and it update the address sifter. In division clubbing event already there is two network, they want to join, so the head of both network exchange address sifter and check for collision,if it is free from collision, it will club. The existing node inform head and leave the network.

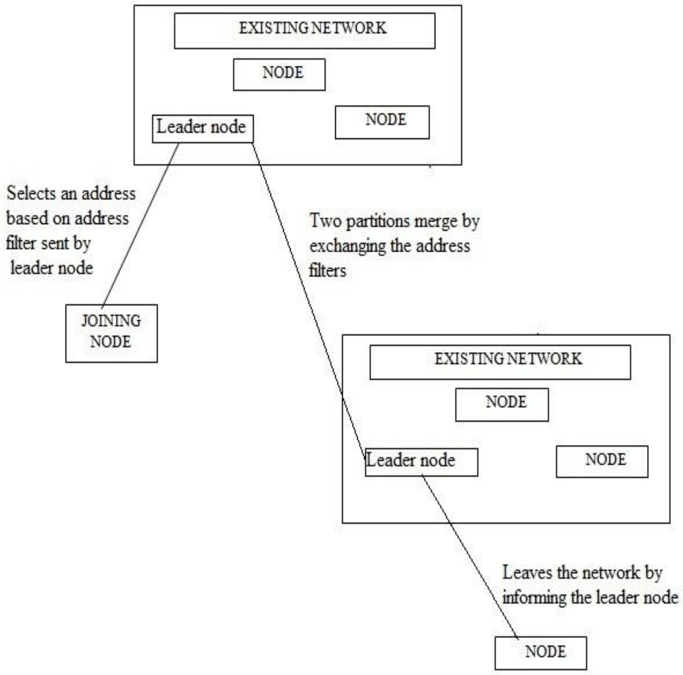

EXISTING NETWORK
NODE
Leader node
NODE
Selects an address based on address filter sent by leader node
JOINING NODE
Two partitions merge by exchanging the address filters
EXISTING NETWORK
NODE
Leader node
NODE
Leaves the network by informing the leader node
NODE

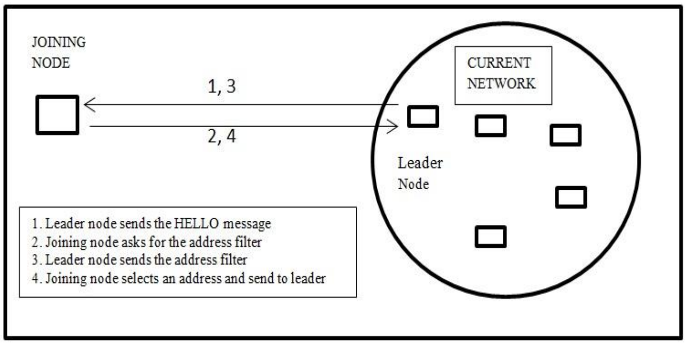
Fig 3.3 SAP Procedures

SYSTEM MODEL

This is the initialization stage of MANET. There are two situations which happen during a MANET initialization: slow and quick initialization. Each node join the network one by one with some delay between them. In quick initialization the node comes to join the network at same moment without any delay. Sifter based protocol is matching for both slow and quick initialization. The SAP method uses two messages namely HELLO and AREQ. (address request)

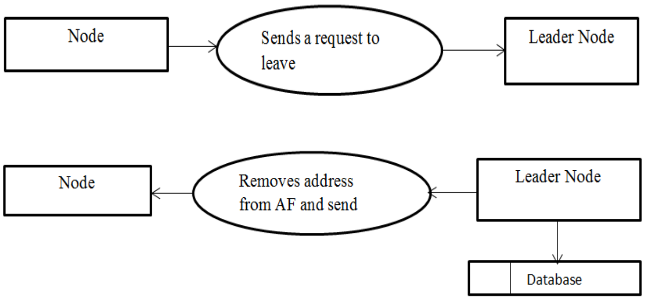
ENTERING NODE MANAGEMENT

It is the process of welcoming new node into the network. Here the new IP address will given to the entered node. Here after initialization phase the head node broadcast HELLO message. When node get message, it can identify the event is division clubbing or not. The message received by entering node. The node can join into the network.


JOINING NODE
1, 3
2, 4
CURRENT NETWORK
Leader Node
1. Leader node sends the HELLO message
2. Joining node asks for the address filter
3. Leader node sends the address filter
4. Joining node selects an address and send to leader

EXITING NODE MANAGEMENT

The communication takes place in the network with valid IP address. Here the communication is taking place successfully will be checked, if the connection is not successfully established find the faild node and its IP and leave that node. When a node leave the network its address should be detached from sifter, so its address can be used by other node in network future if not it leads to address scarcity when node exit from the network it should inform the head node to remove the address from address sifter

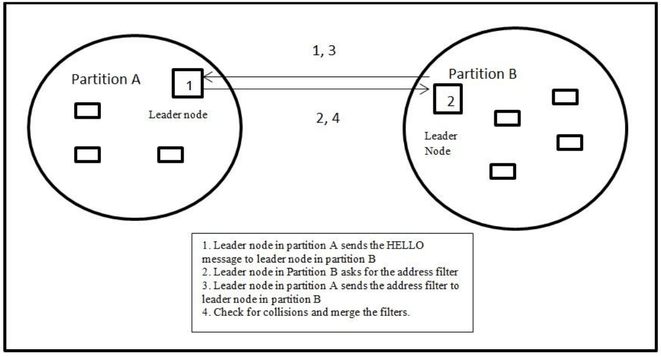


NETWORK DIVISION/CLUBBING

A MANET may split into two or more division and it will be connected together. Here the address sifter find address from database, give it to the successful node and make connection possible. The head node will detect the division clubbing event, The two division will have two set of address it some times have collision.So

when receiving the Hello message the leader node in the other partition will request for the address filter to the leader node in the other partition. Then the other leader node will sent the address filter to the requested leader node. The requested leader node then stores this received address filter and sends its address filter to the other leader. Then both the leader nodes in the two partitions will flood the network with the partition message.

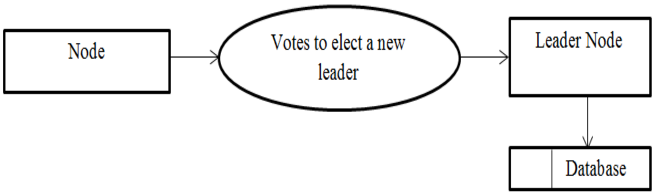
After getting the partition message the leader nodes will check the M bit, where the M bit denotes the lowest priority partition. Then the lowest priority partition will check whether there occurred any address collisions while joining the two address filters. If there occurred any address collision in case, then the lowest priority partition will take a new address and floods the network with an AREQ message to the other leader node. Later the two address filters are merged and thus creating a new address filter and the partition identifier of the address filter is updated.



1. Leader node in partition A sends the HELLO message to leader node in partition B
2. Leader node in Partition B asks for the address filter
3. Leader node in partition A sends the address filter to leader node in partition B
4. Check for collisions and merge the filters.

HEAD SELECTION MANAGEMENT

In this phase new head node is selected every node can vote to a node whome want to be head. A node can vote other node in same pattern. Finally vote counted and maximam no: of vote is made as head node. The head node stores the address sifter of partition and head node will send alone the HELLO message to other node.



IMPLEMENTATION OF GAME THEORY TO THE NETWORK SECURITY IN MANET

In recent years, a number of puzzle based defense mechanism has been proposed against flooding DOS attacks in network, these mechanism has not been designed through formal approaches and some design issues such as effectiveness and optimality have remained unresolved. This paper utilizes game theory to propose a series of optimal puzzle based defense stratergies for handling increasingly sophisticated attacks. It cumulates a stratergy for distributed attacks for unknown no: of sourses.

DEFENDER

The defender takes his part in the solution as an optimum defense against rational attackers. The defender treats incoming requests similarly and need not differentiate between the attack and legitimate requests. Upon receiving a request, the defender produces a puzzle and sends it to the requester. If it is answered by a correct solution, the corresponding resources are then allocated. As solving a puzzle is resource consuming, the attacker who intends to use up the defender’s resources by this time defender locates the attacker location and ip-address.

PUZZLE BASED APPROACH

A number of puzzle-based defense mechanisms have been proposed against flooding denial-of-service (DoS) attacks in networks. Here defender gave new user a puzzle of misplaced image to play with limited time period. If the user succeed in the game then only registration form is provided to the new user. Once a user succeed and enter in to the network once he will became legitimate user of that network and he doesn’t want to play the game there after entering the network.

ATTACKER

There are two principal classes of these attacks: flooding attacks and logic attacks. A flooding attack sends an overwhelming number of requests for a service offered by the victim. These requests deplete some key resources at the victim so that the legitimate users’ requests for the same are denied. A resource may be the capacity of a buffer, CPU time to process requests, the available bandwidth of a communication channel, etc.

REQUESTED COUNT

In the client-puzzle approach, the defender engages two types of resources, one for producing puzzles and verifying solutions, and the other for providing the requested service. The puzzle game is given to the new user who was not to be registered yet.it was identified by the ip- address of the system used by the user. If he was already registered he was no need to be registered.

DATA ACCESS

In this module is available only to the legitimate user of the network. Once a user successfully completed puzzle registration and login process he can use resource from the network. This resource section mainly consists of six sub modules Puzzle approach, Data security, Data Transfer, System blocking, Mailing, program blocking, User details. The puzzle approach module consist of a game puzzle such as Sudoku.in the game a picture is divided in to several parts and defender ask the user to play the game. User want to find solution of the problem with in a limited time. In this time defender got details of the user such as ip address, host number and its location.

Defender analyzes the ip address and accept/block it according to the result. Data security module is used to securely transfer a data or information from server to client or vice versa. Here the information to be sending was encrypted by any of the public key encryption methodsuch as RSA or RC4.The intruder once entered the network cannot view the original message due to the reason that message was encrypted.

Data transfer modules is used to send a data from server to client admin can view the data transferring path to the client. If admin saw anything anonymous in any of the router included in the path he can block that router and go for another safe path.Program blocking module is used to block a program running in server. Once the program was blocked it cannot be used by any of the client system in the network. Admin also can able to block the application of the client system

Mailing module is used to send and receive mails to multiple clients at a time. User details moduleis used to view all the clients in the networks. Admin can view the ip-address, host number, location of the user clients in the network.System blocking is used to block the system in the network. Admin can control the system blocking function.in this module the admin lock the system by using a username and password. Once the system is locked any of the user cannot be open the system without that username and password

DEFENDER TRUMP CARD ALGORITHM

1. Classful network total bits is 8**.** So Total bits = T_b =8.
   Sub-net mask be 0, 128, 192, 224, 240, 248, 252, 254,255
   Number of bits used for subnetting = n = 3

2. Number of bits left for host(m) = T_b - n as total bits is the summation,
   Number bits left for host i.e. T_b = m+n.
   Number of bits left for host = m = T_b - n = 8 - 3 = 5
   calculate number of subnets = 2^n

   Value of last bit used for subnet masking(Δ) = 2^m**.**
   Number of host per subnet = 2^m - 2.
   Number of subnets = $2^n = 2^3 = 8$,
   Value of last bit used for subnet masking Δ = $2^m = 2^5 = 32$

3. Find previously calculated number of subnets by separating subnets each having value of last bit used for subnet masking or Δ addresses.

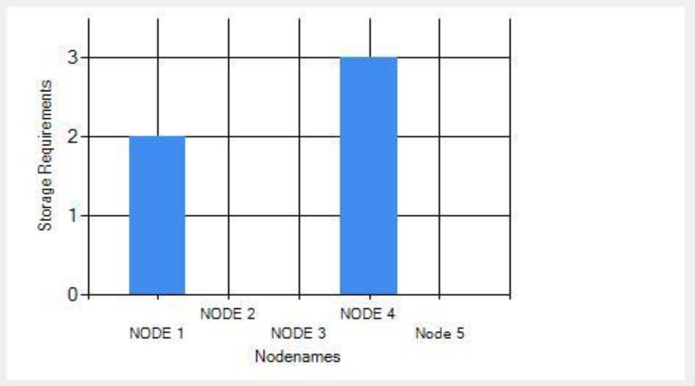
4. Find IP address is in which subnet, that subnet's first address is network address and last address is broadcast address.

PERFORMAN .CE EVALUATION

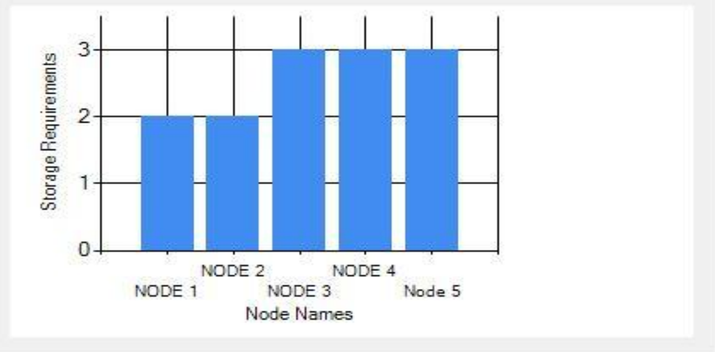
Here the graph was plotted based on the storage requirements needed by the leader based method and the SAP method. The graph results showed that the sap method has less storage requirements. In other case every node has to store the address filter. But in sap leader stores the address filter. Network performance refers to measures of service quality of a telecommunications product as seen by the customer. There are many different ways to measure the performance of a network, as each network is different in nature and design. Performance can also be modeled instead of measured. The chances of address collisions is less in this sap method. Since the leader is storing the address filter. A leader node can easily check whether an address is already assigned or not. When a joining node receives a Hello message it asks for the address filter to the leader node. Then the leader node sends the address filter to the joining node. And the joining node checks all the addresses already allocated in that network. And the joining node selects an address based on the addresses in the address filter in such a way that there is no address collision. And this address will be sent to the leader node and leader node once again checks this address for any collisions.

The graphs below show the comparison between the storage requirements needed for sap and the previous DAD method

Node Names	Storage in DAD	Storage in SAP
Node 1	2	2
Node 2	2	0
Node 3	3	0
Node 4	3	3
Node 5	3	0



Storage requirements needed in SAP



Storage requirements needed in DAD

V CONCLUSION

In this paper I propose a efficacious protocol for successful communication of system or node in MANET, along with that provide network security using game theory. Unlike the existing system a sifter based addressing protocol is used. It will avoid collision and find failed communication of IP address and provide successfull communication with IP address and provide secure via game theory. A puzzle based approach towards the attacker by defender. Giving game to the defender find attackers IP address, host number, location. The paper will provide a new phase to the existing security.

REFERENCES

1. Fernandes N.C, Moreira M.D and Duarte M.B, “An efficient and robust addressing protocol for node autoconfiguration in ad hoc networks”, in IEEE/ACM transactions, vol. 21,issue 3, 2012 July
2. Xiannuan,Yang xiao, “Game theory for network security”, in IEEE Communications Surveys & Tutorials, vol. 15, No. 1,First quarter 2013
3. C. E. Perkins, E. M. Royers, and S. R. Das, “IP address autoconfiguration for ad hoc networks”, Internet draft, 2000.
4. H. Zhou, L. Ni, and M. Mutka, “Prophet address allocation for large scale MANETs”, in Proc. 22nd Annu. IEEE INFOCOM, Mar. 2003, vol. 2, pp. 1304–1311.
5. N. C. Fernandes , M. D. Moreira and O. C. M. B. Duarte "An efficient filter-based addressing protocol for autoconfiguration of ad hoc networks", Proc. 28th IEEE INFOCOM, pages: 2464 -2472 2009.
6. N. H. Vaidya, “Weak duplicate address detection in mobile ad hoc networks”, in Proc. 3rd ACM MobiHoc, 2002, pages: 206–216.
7. S. Nesargi and R. Prakash, “MANETconf: Configuration of hosts in a mobile ad hoc network”, in Proc. 21st Annu. IEEE INFOCOM, Jun. 2002, vol. 2, pages: 1059–1068.
8. Z. Fan and S. Subramani, “An address autoconfiguration protocol for IPv6 hosts in a mobile ad hoc network”, Computer Communication, vol. 28, no. 4, pages: 339–350, Mar. 2005.
9. Yang wiev wang, Richard” A mean field game theoretic approach for security enhancement in MANET” in IEEE transactions for wirelesss communication, vol. 13,issue 3, 2014 march
10. Saman, Himanshue, William.”A game theoric intrusion –RRE” IEEE transactions , vol. 25,issue 2, 2014 february

Limma mary Rodriguez received B-Tech degree in computer science and engineering from kerala university in 2012 and ME degree from Anna university in 2015. Her major research interests in Networy security, privacy and future internet.