Asian Journal of Information Technology 15 (19): 3835-3845, 2016
ISSN: 1682-3915

ACPIP: A New Intrusion Prevention System for Manet Through Address Configuration

[1]A. Jahir Husain and [2]M.A. Maluk Mohamed
[1]M.A.M.College of Engineering, Tirchirappalli, 621105 Tamil Nadu, India
[2]Department of CSE, M.A.M.College of Engineering, Tirchirappalli, 621105 Tamil Nadu, India

Abstract: The salient characteristics of Mobile Ad hoc Networks (MANET) make it more vulnerable to various attacks. In this study we propose a novel dynamic IP configuration scheme that generates IP address for MANET nodes by using a simplified cryptographic hash function. The MAC addresses and the IP addresses are mapped with the Manufacturer Serial Number (MSN) of the nodes participating in the MANET. The proposed technique named as Auto Configuration Protocol with Intrusion Prevention (ACPIP) specially designed for MANET is capable of securing and organizing MANET as it develops from one node to many. A new Malicious Node Alert (MNA) technique is included to secure the MANET from Distributed Denial of Service (DDoS) attacks. We evaluate the performance of this solution through simulation experiments. The results demonstrate that it is possible to prevent the DDoS attacks by properly configuring IP address, in an efficient way.

Key words:MANET, auto-configuration, DDoS attacks, Intrusion Detection System (IDS), Distributed denial of Service (DdoS)

INTRODUCTION

Two indispensable issues of MANET are IP address auto configuration and Intrusion Detection Systems (IDS). The address auto-configuration can be defined as a task of assigning conflict less, unique IP address to every participating node in the MANET without any human involvement or by not using any centralized DHCP server. When a new node enters in a MANET, a unique conflict-free IP address must be assigned to it before it can actively participate in the network. The nodes in a MANET have to configure with link local addresses which are valid within the MANET to communicate themselves and the nodes may also need to configure global routing addresses to communicate with the external world. By nature in a MANET any node can enter and any node can exit at any point of time. In most of the existing auto configuration schemes a node will be given a new IP address when it rejoins. As the IP address gets changed every time when a node rejoins within the lifetime of the MANET, the processes of assigning unique IP address is very difficult. Apart from the auto-configuration, MANET nodes must have a mechanism for computing trust value of each other node to identify malicious and selfish nodes. Every node calculates the trust value of a specific node based on its direct experience and the information received from the other neighboring nodes. If this trust value happens to be lesser than a predefined threshold, then that specific node is considered as a selfish or malicious and hence marked as not to be trusted. Nodes must be assigned unique identities and these identities must be validated properly. In order to eliminate the misbehaving node, the auto-configuration scheme should work properly so that no node can get multiple identities. The auto-configuration system must be designed in such a way that no node can get more than one address. If a node can get more than one identities then it is easy for a malicious node to initiate Sybil or IP spoofing attacks. The attacker can use the identities one by one or simultaneously to falsify the trust estimation. There are chances created for the malicious nodes to alter the trust value of other genuine nodes and hence disrupting the routing system which depends on the trust value of nodes. Moreover, if the malicious node is sensed, then suddenly it may go offline and may try to rejoin with a newer set of identities to begin a new attack. Lack of centralized administration and the peer to peer nature of a MANET cause unique identification of nodes a challenging task. Only using an IP or MAC address as a credential does not provide any protection against Sybil

Corresponding Author: A Jahir Husain, M.A.M. College of Engineering, Tirchirappalli, 621105 Tamil Nadu, India

or IP spoofing attacks as both of these addresses can be spoofed easily. The existing mechanisms which properly guarantee that a single identity is attached to a single node, either involve a centralized trust module like a TTP (Trusted Third Party) or require human intervention. These requirements greatly diminish the MANET application scenarios. As a possible solution, we consider that some distinguishing non-modifiable characteristics of mobile device hardware can be used to fingerprint them. For example, 'Manufacturer Serial Number' of hard disk drive in a laptop is unique and it is burnt on the hard disk controller.

The PDAs have unique and unchangeable PDA serial number etc. (Hashmi and Brooke, 2008). In order to restrict the nodes, from spoofing IP or MAC addresses, these unchangeable, fixed characteristics of the hardware identification of the device can be utilized as strong credentials and IP or MAC address can be bound to them.

Literature review: Over the last decade, many research works have been done on MANET routing protocols. The essential requirement for all the routing protocols is that every node in the MANET must be assigned its own unique IP address to transmit data. The existing address allocation protocols for wired networks are not directly applicable for mobile networks. According to Weniger (2003), the present auto-configuration protocols can be organized into three categories. The best effort allocation scheme The Leader-based allocation scheme and The Decentralized allocation scheme The protocols in the first category do not guarantee the address uniqueness. In the Prophet scheme (Zhou *et al*., 2003) the address allocation is done by means of a series of random numbers generated by a function f(n). However, to resolve the address conflicts, prophet scheme requires some mechanism, similar to passive Duplicate Address Detection (DAD) (Weniger, 2003). Hence there are chances of creating broadcast storm problem, since the passive DAD uses the periodic link state routing information to notify the nodes about their neighbors. In the second category, nodes get valid IP addresses from a leader or server of the network like DHCP. In DHCP, a new node needs to broadcast the 'server discovery' message, then after getting the IP address it uses the DAD to verify the uniqueness of the IP address. In ODACP (Sun and Belding, 2004) the server broadcasts advertisement periodically, in order to lessen the broadcasting by new nodes. Hence, it is possible for a new node to directly register its IP addresses to the server. Since, the time interval between successive advertisements is high, the broadcasting overhead will be reduced but it also creates longer latencies for nodes to obtain addresses. In the third category, a node can get an IP address either by itself or from a neighbor node and then executes the DAD to guarantee the uniqueness of the address. In AAA, nodes arbitrarily select an address in the range of 169.254/16. In MANETconf (Nesargi and Prakash, 2002), each node keeps a list of all addresses used in the MANET and a new node acquires an address from one of its neighbors. The MANETConf protocol constructs a partition identity (ID) for the MANET and the same is flooded periodically over the whole network. If the partition ID control packets are not received by a node within a certain period of time, it assumes that the network is partitioned. Moreover such a periodical flooding will increase the network interruption. Furthermore, in this scheme network overhead and resource consumption are higher than the expected level. In MANETconf address assignment is based on a distributed mutual exclusion algorithm which considers the IP addresses as a shared resource. Complete synchronization is needed among all the nodes to avoid duplicate addresses.

Another decentralized address configuration protocol known as Prime DHCP (Hsu and Tseng, 2005) is proposed by Hsu and Tseng. Here a new node will be assigned an IP address without broadcasting it over the entire MANET. Prime DHCP considers every node as a DHCP proxy and it execute a Prime Numbering Address Allocation (PNAA) algorithm to compute unique addresses for every node. However, the drawback of this approach is that it does not consider the MANET security at the time of address allocation process. In weak DAD, (Vaidya, 2002), researchers proposed a scheme with an intention to handle network merger. It supports proactive routing protocols and needs slight alteration in the routing protocols. In SAAMAN the authors projected a scalable address configuration scheme for MANETs. (Hussain *et al*., 2011) In this method a new node configures itself with an address and its uniqueness is confirmed with Duplicate Address Detection Servers (DDS). A tree based topology oriented auto-configuration mechanism in a MANET, nodes are divided in to three types which are root node, leader node and normal node (Mistarihi *et al*., 2011). Every node has to play any one of these roles. The responsibility of the root node is very essential. It has to maintain the records of the leader nodes and their address information in its database and executes the tasks of network partitioning and merging. Leader nodes hold disjoint set of IP addresses to configure the new incoming nodes. Normal nodes do not have any special job in general however used for routing if the leader nodes are not present in a particular area.

In Filter-based Address Auto Configuration Protocol (FAACP) for duplicate address detection and recovery scheme, employs a sequence filtering technique for address space management (Reshmi and Murugan, 2015). The scheme proposes a grid like structure of MANET topology to handle network merging and partitioning. In quadratic residue based address allocation scheme for MANETs, the first node configures itself with an IP address (Chu *et al*., 2008). In addition, it produces the number of distinct cycles and length of each long cycle (address block). The MAC address and the IP address are mapped in MMIP (Ghosh and Datta, 2009). In this scheme every node in the network should act as proxies and binds the MAC address with the allocated IP address. MMIP asserts that, it allocates secured IP addresses to the nodes of a MANET as the MAC addresses of the individual nodes are associated with the allocated IP addresses. However, the drawback of this protocol is that MAC address is not unique and it can be duplicated by some means.

In ADIP scheme, MANET nodes are used as proxies. In this a proxy node can produce IP addresses for a new authenticated node from its own IP address. (Ghosh and Datta, 2011) A trusted third party is used for the authentication. The protocol is capable of managing the security threats associated with a general dynamic IP configuration. In general we can see that Duplicate Address Detection (DAD) mechanism is mostly utilized in the existing dynamic IP addressing schemes for MANET for conflict detection. Also except a few, most of the existing schemes are not considering the security aspect while allocating the dynamic addresses.

Problem definition: The proposed approach ACPIP is designed to tackle two important DoS attacks namely, Sleep Deprivation attack and Sybil attack. These two attacks are the result of inefficient address configuration. In this research work our aim is to propose a new IPS (Intrusion Prevention System) specially designed for MANETs. We propose a protocol which aims to prevent the attacks on MANET due to IP address conflicts by dynamically assigning unique IP address for every node in a MANET. Before getting in to the deep discussion, it is necessary to describe the attacks which are caused by inefficient address configuration.

- Sleep deprivation attack
- Sybil attack

Sleep deprivation attack: Sleep Deprivation (SD) is a Distributed Denial of Service (DdoS) attack. In this type of attack an intruder communicate with another node in a way that looks like a genuine node. However the aim of this communication is to make the target node out of its energy saving sleep mode. (Nadeem and Howarth, 2009, 2013). There are two types of malicious Route Request (RREQ) flooding, by which, an intruder makes SD of a node by the weakness of the route discovery process:

Malicious RREQ Type 1: An intruder broadcasts a RREQ packet to a destination node with IP address that is within the IP address range but the corresponding node does not actually present in the network. This forces all the nodes to forward this RREQ because no node will keep the route for this non existing destination IP address.

Malicious RREQ Type 2: After broadcasting a RREQ, an attacker will not wait for the ring traversal time; instead it carries on resending the RREQ for the same destination with higher TTL values. This is a considerable denial of service attack since energy constrained operations of MANETs are considered to be very important.

Sybil attack: Every node in a MANET which wants to take part in routing needs to have a unique IP address, through which nodes are identified. Since MANET lacks of central authority to assign or verify the IP address, an intruder illegitimately claim multiple addresses to send RREQ or RREP packets. A Sybil node can either construct a new identity or forge an identity from a genuine node. This is called as Sybil attack (Nadeem and Howarth, 2009, 2013). This is an imitation attack in which the attacker can use either random IP address or the IP address of any other node to make uncertainty in the routing progress and it also creates the base for some other severe attacks. In Sybil attack a malicious node mimics some non-exist nodes and it will look like a number of malicious nodes combine together. This attack affects auto-configuration as well. In order to prevent these attacks we must ensure that every node joining the MANET must be assigned “one and only one” IP address

Scheme description: In this study, we describe the ACPIP (Auto-Configuration Protocol with Intrusion Prevention) scheme in detail. ACPIP consists of four major parts namely MSN, IP_COMPUTE, allotment table and Malicious Node Alert (MNA) message. There are

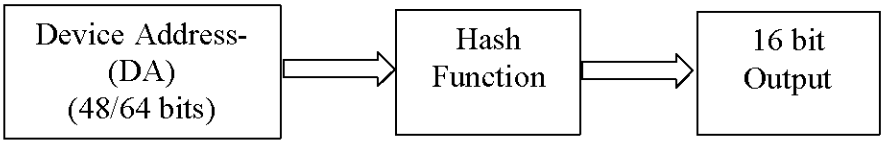

Fig. 1: Black diagram of the proposed algorithm

numerous auto configuration mechanisms already proposed in the literature. Even though most of the existing algorithms assume the secure MANET, the improper assignment of IP address for the MANET nodes causes the above said types of attacks. In this study we propose a protocol which dynamically assigns IP address to every node coming in to the network with a strategy that, "Every node must be given a one and only one IP address". We consider an independent ad hoc network functioning itself. Figure 1 shows the black diagram of the proposed protocol. Our protocol is based on a simplified cryptographic hash function which accepts a Device Address (DA) and produces output as 16 bit value. The input may be a 48 bit Ethernet MAC address, a Bluetooth address, UWB address or a 64 bit Zigbee address or any other unique identification of a node which wants to participate in the MANET. This value is processed by a hash function and it generates a 16 bit value.

MATERIALS AND METHODS

System model: We think of an independent ad hoc network which is not interconnected with any other network and has no gateway or connection to the outside world. The network is created from one node as origin and then the remaining nodes join the network one by one. The nodes are free to move everywhere and can join or leave the network at any point of time. Hence a dynamic topology will be created and we can't predict the size of the network. We can define the lifetime of the MANET as the period between the first node configures itself with an IP address and all the nodes have left out or switched off.

The ACPIP algorithm: In this section we present our proposed algorithm for dynamic IP configuration. A Device Address (DA) like Ethernet MAC address, Bluetooth Address or any other equivalent identification (Hardware address of Zigbee or UWB protocol) can be used to calculate the IP address of a MANET node by a simplified cryptographic hash function. We call this algorithm as Auto Configuration Protocol with Intrusion Prevention (ACPIP) algorithm. The technique proposed here makes every node as a provider to a new node N_{new}. Thus all the nodes are talented to calculate and assign IP addresses from the physical address of the new node N_{new} and so N_{new} can acquire an address just from its neighbors. Each provider computes a unique IP address for a new host N_{new} from the physical address given by N $_{new}$ Thus, broadcasting a request message for searching a server or for DAD is not required. There are three phases in our proposed ACPIP algorithm. In phase I the first node N_{first} of the MANET configures itself and becomes a provider. In phase II, a new node N_{new} makes a request for IP address and in phase III the provider node computes and offers a new IP address to N_{new}. Algorithms for the first two phases are given in Algorithm I and an algorithm for the third phase is given in Algorithm II respectively. respectively.

Algorithm i: configuration of nfirst and n new

```
Set configured ß false;
Set wait_timer ß 0.0;
Set iprep_timer ß0.0;
do while (configured = false)
{
      broadcast IPREQ message;
      start wait_timer;
      if timeout(wait_timer)
      {
                IP_COMPUTE (self MAC address)
                                                  // Refer IP_COMPUTE
function
                Set IP Address;
                Set Configured ß true;
                Exit;
      }
      else if MSNREQ message is received
      {
                Stop wait_timer;
                Read Manufacturer Serial Number(MSN);
                Send MSNREP message;
                Start iprep_timer;
      }
      If IPREP message is received
      {
                Stop iprep_timer;
                Set IP Address;
                Set configured ß true;
                Exit;
      }
      Else if timeout(iprep_timer)
      {
                Set configured ßfalse;
      }
}
```

Algorithm ii: provider node response

If ipreq message received

```
{
    Check allotment table for DA
    If DA available in allotment table
    {
    Reply with MSNREQ message
    If MSNREP message received
            {
            Check allotment table for MSN
            If new MSN
                        {
                        Confirm malicious node
                        Alert neighbours
                        Reply with DENY message
                        }
            Else
                        {
                        Reply with OLD IP address        //Rejoining of genuine node
                        }
            }
    }
    Else                                                 // new Device address
    {
    Reply with MSNREQ message
    If MSNREP message received
            {
                        Check allotment table for MSN
                        If new MSN          //new node joins MANET
                              {
                              IP_COMPUTE     (Device address)
                              Update allotment table      // store MSN, DA, and IP
                              Reply with IPREP message
                              }
                        Else                //MSN exists in allotment table
                              {
                              Mark as suspicious node
                              Reply with OLD IP address
                              }
            }
    }
}
```

Address allocation for the first node: When a new node N_{new} wants to join a MANET, the proposed ACPIP algorithm broadcasts an IPREQ (Request for IP address) message to its neighbors and it waits for a certain period of time to receive a reply from any one of its neighbor. The reply message will be a MSNREQ (Request for Manufacturer Serial Number) message. If no MSNREQ message is received, the new node N_{new} computes its IP address itself by calling the IP_COMPUTE function by supplying its own MAC address as a parameter of the function. The function IP_COMPUTE calculates and returns the host id portion (3rd and 4th octets) of the IP address. Now N_{new} configures itself to the link local IP address 169.254.x.x where x.x are replaced by the value x1 and x2 returned by the IP_COMPUTE function. In this case the node N_{new} becomes the first node of the MANET and it will be the IP provider for the next newly joining node.

Address configuration for the new node: Assume that a MANET already exists and a new node N_{new} wants to join the MANET and broadcasts IPREQ message. This message contains its Device Address (DA) as an identifier of the host N_{new}. Our ACPIP algorithm uses a cryptographic hash function IP_COMPUTE which accepts a Device Address of size 48/64 bits and it generates unique 16 bit value. This 16 bit value will be used in the place of x.x in the above said IP address. In order to overcome the fake DA issue such as duplicate MAC address problem, we need to have one more parameter which uniquely identifies a node in a network. In general any ARP and/or RARP packet contains only

....

MAC addresses of the source and destination hosts for unique identification. However there is a hidden parameter which exists in every node is its Manufacturer Serial Number (MSN) (Hashmi and Brooke, 2011) which is a unique number available in all types nodes. The MSN can be read through special commands in various operating systems. In our proposed algorithm we have used MSN combined with Device Address which ensures the unique identification of a node in the network. The conversation between N_{new} and the provider node will have the following steps:

- Node N_{new} broadcasts IPREQ message. (Contains its Device Address)
- Provider node will receive this message and ask for MSN of N_{new} (Sends the MSNRREQ message)
- N_{new} sends back the MSNREP message which contains the Manufacturer Serial Number (MSN) of its own
- Provider node accepts and checks whether an IP address is already assigned for this node.
- If already assigned then provider will send back the same IP address to the N_{new} without calling IP_COMPUTE function
- If not (a new MSN is found) then the provider calls the IP_COMPUTE function by supplying the MAC address of N_{new} as parameter to the function to generate the IP address and returns the same to N_{new}

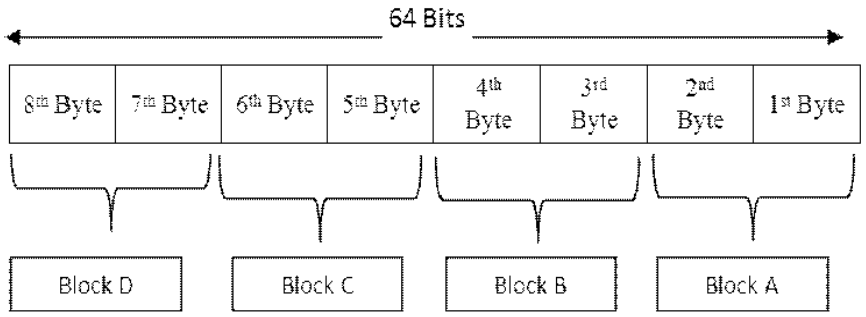

Fig. 2: Segmenting 64 bit MAC address into 4 blocks

- N_{new} will configure to the IP address and send back the confirmation message IPACK to the provider.

Now we describe the IP_COMPUTE function. It is a simplified form of a cryptographic hash function. The IP_COMPUTE function is designed as follows: MAC address of a mobile device which wants to participate in the MANET will be read and its length is calculated.

IP_COMPUTE (device address)

```
{
   Define constants:
      C1 = 1010101010101010
      C2 = 1111111100000000
      C3 = 1100110011001100
      C4 = 1111000011110000
      Read device address DA
      Convert to binary (digit by digit)
                 // divide the string in to three blocks
      If size <64 bits
      {
Append required numbers of 0's to the most significant bits to make the size
= 64 bits
      }
      Block A = first 2 bytes
      Block B = second 2 bytes
      Block C = third 2 bytes
      Block D = fourth 2 bytes
//perform simple binary addition in the
   following steps
      R1 = Middle 16 Bits(Block A* C1)
      R2 = Middle 16 Bits(Block B* C2)
      R3 = Middle 16 Bits(Block C* C3)
      R4 = Middle 16 Bits(Block D* C4)
      R= R1+R2+R3+R4
                  // Right most 16 bits of R
                                            // Discard the carry if any
      X1= 8 least significant bits of R
      X2= 8 most significant bits of R
      Return (169.254.x1.x2)

}
```

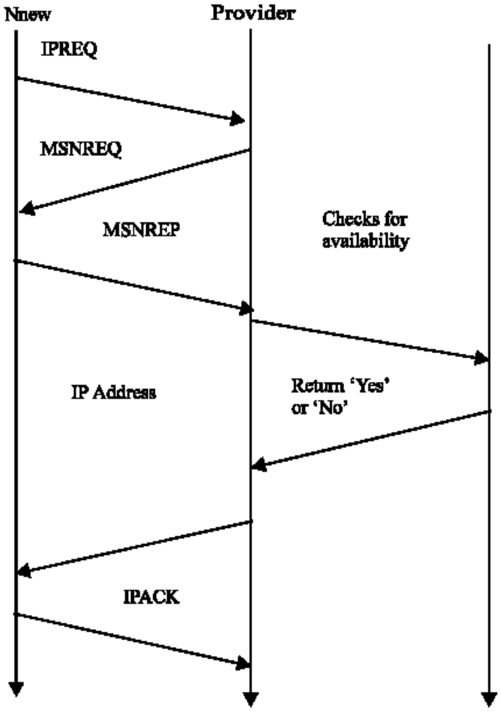

Fig. 3: IP address conversation process

In general the MAC address is 48 bits long in Ethernet, Bluetooth and UWB technologies whereas 64 bits long in zigbee protocol. Hence in this function 48 bit addresses are padded with 0's to make them to 64 bits long before further processing. We define four binary constants C1, C2, C3 and C4 which are used to avoid collisions while hashing. The entire string is broken up into 4 blocks namely A, B, C and D. This is shown in Fig. 2. This process will create a 16 bit binary string and is divided into two 8 bit words. These 8 bit words are used as node IDs in the proposed IP address. Fig. 3 illustrates the conversation between N_{new} and the provider. On receiving the IPACK message from the new node N_{new}, the provider node maps the MAC address and the MSN of N_{new} with the IP address and it is encapsulated in a MSN_MAC_IP message then broadcasted to all nodes within its radio range (including N_{new}). After receiving this message from the provider, N_{new} performs a final check on the configuration parameters.

The neighbors after receiving the MSN_MAC_IP message broadcasts it to its neighbors and so on such that the whole of the MANET receives it within a short time. The nodes then updates their allotment table by inserting the MSN, MAC address and the IP address of the new host N_{new} in the allotment table entry.

Partitioning and merging of network: In our proposed ACPIP address allocation mechanism, more than one node will/would not have the same IP address at any point of time. Due to the dynamic and unpredictable nature of the MANET, the network can partition and then again can remerge at any instant of time. However in our proposed ACPIP protocol there will not be any conflicts of address in the network even if the network partitions because of the use of MSN. Even if a node switches off or disconnected within the lifetime of the MANET, the IP address of the said node will not be assigned to any other host as described earlier. Therefore, there will be no address conflicts even if two divided networks join again as every node has the ability of producing unique IP addresses for a new node. Moreover, the following scenarios are also effectively handled in our proposed protocol:

- A node which is switched-off or discontinued (generally a malicious node) will be automatically identified if it tries to re-enter the network within its lifetime
- The MANET can partition and then the separated networks can merge later without any address conflict
- Two independently configured MANETs having different net IDs may join without any clashes of the IP addresses

RESULTS AND DISCUSSION

Constructing and updating allotment table: In our proposed ACPIP scheme, the allotment table plays a vital role and has to be updated whenever a new node joins the network. Allotment table is maintained by each node in the MANET, where the MSN, MAC address and the IP address of each node are stored. Allotment table is created for a new host N_{new}, after the IP address is generated from its provider. Each node acting as provider in the MANET updates their allotment table by inserting MSN, MAC address and IP address for the new host N_{new}.

MNA (Malicious Node Alert) message: The MNA scheme is designed to prevent malicious RREQ message from an attacker. A RREQ is initiated by a source node which has data packets to be sent to a destination. This route request is flooded throughout the MANET to find the route for the destination by its IP address. Each node, upon receiving a RREQ packet, rebroadcasts the packet to its neighbours until the destination is found. In our ACPIP scheme, every node keeps and updates the allotment table which contains all other nodes IP address which are genuine. Consider a scenario where a malicious node tries to flood a malicious RREQ packet which contains the destination that does not actually exist in the network. Every node receives this request finds that no such IP address exists in their allotment table and marks the sender as suspicious node. The RREQ will be refused. The node encounters a suspicious RREQ, initializes its mal_count (malicious node counter) with the IP address of the suspicious node. A MNA message is generated consisting of the suspicious IP address and the mal_count and the same is broadcasted to every other node in the radio range. All other nodes which receive the MNA message rebroadcast it to other nodes, in such a way that the entire network will be alerted in a short time. Suppose if the same malicious node leaves from the network and tries to rejoin later, it must seek for an IP address by providing its MAC address and the MSN. As per our ACPIP algorithm the same IP address will be provided to the node which rejoins. If the node once again tries to broadcast a similar malicious RREQ, it will be denied and the mal_count is incremented by one. If the mal_count reaches a threshold value, then the suspicious node will be confirmed as a malicious node and will not be allowed to enter the MANET once again. We set threshold as minimum as required. In this way the sleep deprivation attack can be effectively prevented.

Performance evaluation: We conducted experiments and analyzed the performance of our proposed idea using GLOMOSIM simulator. The experiments were focused at collecting the results of address allocation Latency, Communication overhead and the number/type of messages exchanged by our protocol, at the same time preventing the attacks due to improper IP address assignments. In this research we aimed to prevent two attacks namely .Sleep deprivation Attack and Sybil Attack. This is achieve by assigning unique IP address, in a different way. The ACPIP protocol was tested by using the following parameters:

- Random waypoint mobility model
- Network area is 1000 m×1000 m

Table 1: Performance comparison of ACPIP with other schemes

Metrics	MANETconf	Prophet	PrimeDHCP	SAAMAN	MMIP	FAACP	ACPIP
Complexity	High	Low	Medium	High	Medium	Medium	Low
Communication Overhead	High	Low	Medium	Medium	Low	Medium	Medium
Latency	High	Low	Low	High	Low	Low	Medium
Scalability	No	Yes	No	Yes	Yes	Yes	Yes
Uniqueness	Yes	No	No	Yes	Yes	Yes	Yes
Intrusion sybil		No	No	No	No	No	No
Prevention sleep	Yes						
Deprivation for attacks	Yes	No	No	No	No	No	No

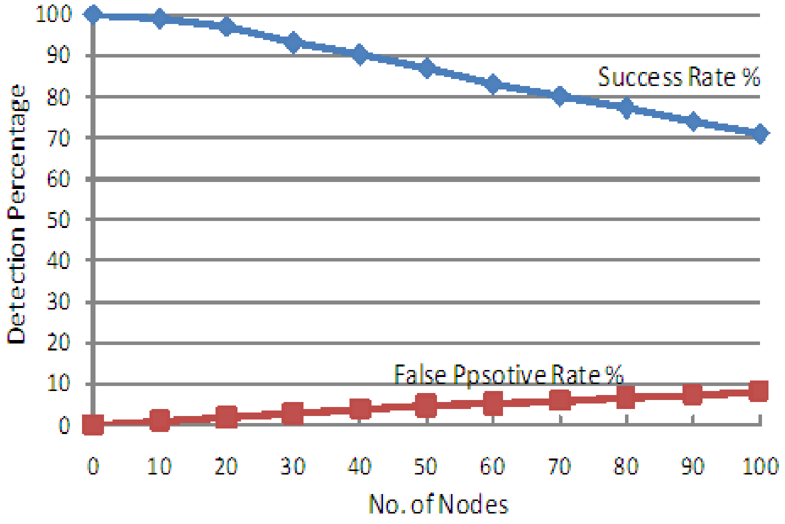

Fig. 4: Success and false positive rates of SD attack against the number of nodes

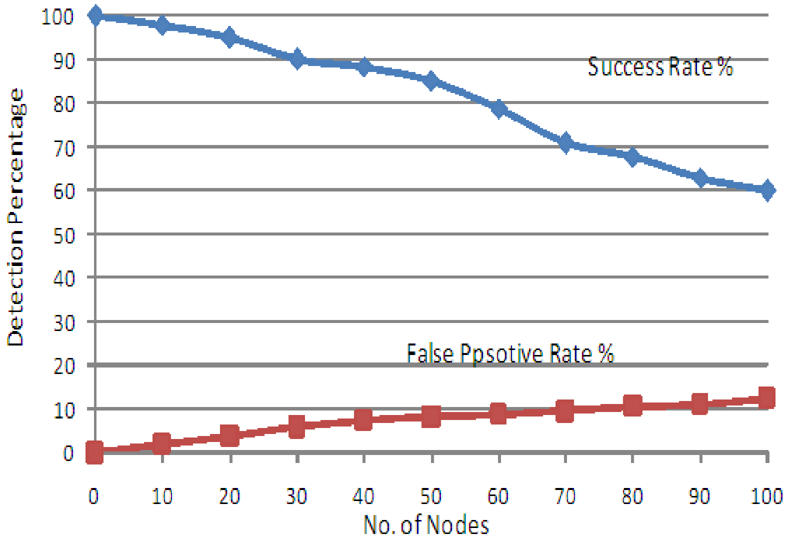

Fig. 5: Success and false positive rates of sybil attack against the number of nodes

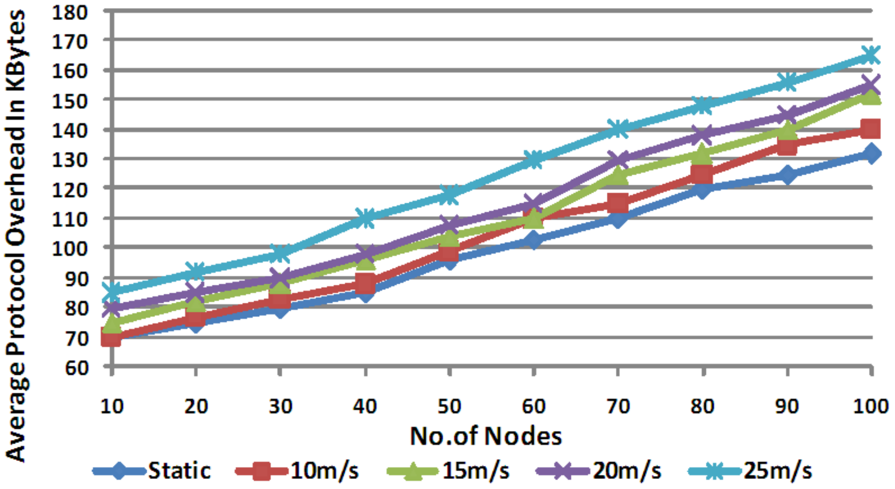

Fig. 6: Average address allocation latency in seconds

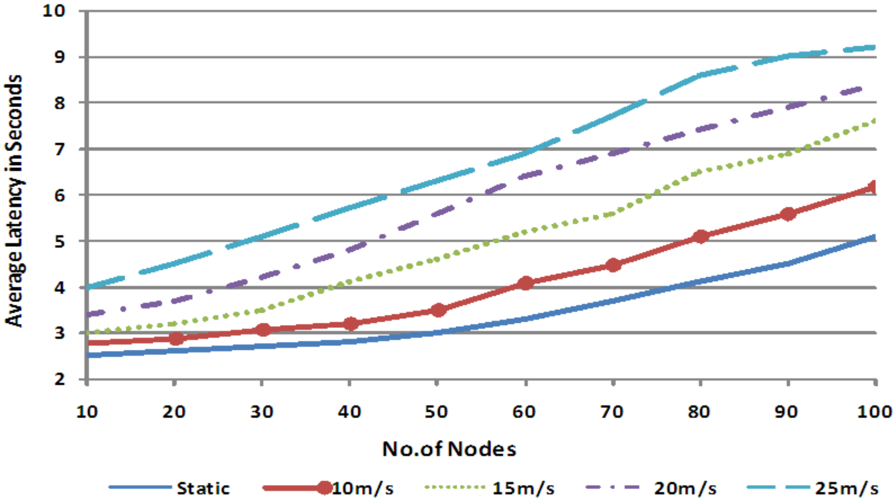

Fig. 7: Average protocol overhead

- Nodes move with a maximum speed of 25 meters/second
- The routing protocol used was the Ad hoc On demand Distance Vector (AODV)
- Transmission range of the node is 100 m
- Data link layer was IEEE 802.11 for all the nodes
- The number of nodes in the network is 100
- Routing Protocol: AODV

The proposed protocol was tested and compared with the other well-known protocols for address assignment and for Intrusion Detection. The metrics taken for evaluating the performance are: distributed process, complexity, communication overhead, uniformity, latency and scalability. Table 1 demonstrates the performance comparison of ACPIP with other schemes.

Experiment analysis: In this section, we present a case study with different attack setup and analyses were made to test the proposed ACPIP. We present the simulation results of these experiments and some significant conclusions from the investigation of the attacks. The first experiment was conducted to test the performance of ACPIP against sleep deprivation attack using Malicious RREQ flooding (MRF) attack. The chart in Fig. 6-8 shows the Success Rrate (SR) and False Positive Rate (FPR) of ACPIP by accounting the number of nodes in the

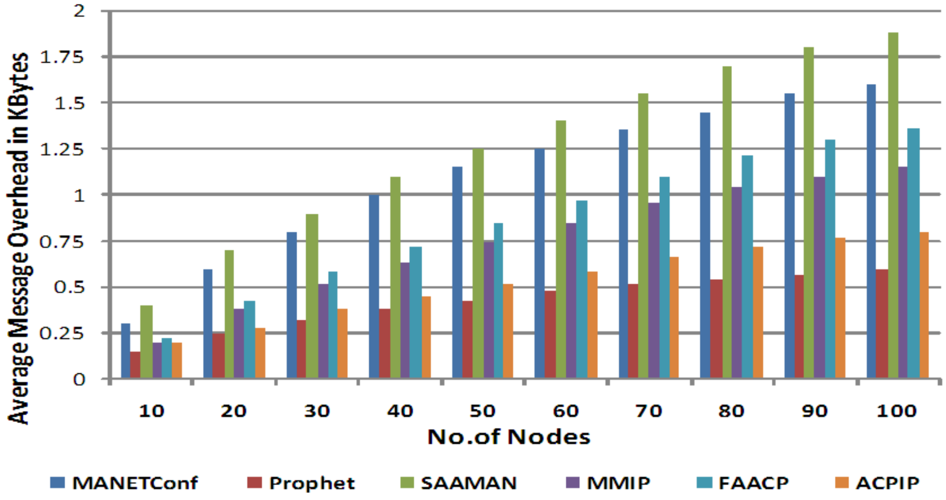

Fig. 8: Average message overhead

MANET with SD attack. SR here means the rate of correctly spotting the intrusion in the network, identifying the attack type and then pointing out the node which is triggering the attack. The False Positive Rate (FPR) means that a correctly behaving node has been wrongly identified and separated. The graph shows a better performance of ACPIP in terms of high SR and low FPR rates against the SD attack.

CONCLUSION

In this study we have presented an innovative dynamic Intrusion Prevention System (IPS) by means of allocating unique IP address for MANETs. In a MANET reassigning the unique address when a node rejoins is a major challenge. IP address duplication after rejoining of a node in a MANET make it vulnerable for DoS attacks. The solution provided here, addresses this issue and easily tolerate communication losses, splitting and reunion of MANET. The solution maps the Manufacturer Serial Number (MSN) of a node with the allocated IP address. It guarantees that a node in a MANET will not be able to alter its IP address within the lifetime of the MANET, even if the MAC address of the node is changed. This removes the periodic message exchange between neighbors. In the algorithm, every host in the network acts as the address provider having the ability to assign IP addresses to new hosts. The signaling message excluding the MNA message need not be flooded over the MANET saving considerable bandwidth. No signaling message other than the MNA message is flooded over the MANET which saves the considerable amount of bandwidth and battery power of nodes. The simulation experiments show that the proposed solution has reasonable latency, minimal communication overheads, uniqueness in providing IPv4 address and simultaneously preventing DoS attacks in a standalone MANET. In future we want to expand our solution for IPv6 which requires additional computation. Furthermore we will focus an Intrusion Prevention System which will secure MANET combined with Internet of Things (IoT).

REFERENCES

Chu, X., Y. Sun, K. Xu, Z. Sakander and J. Liu, 2008. Quadratic residue based address allocation for mobile ad hoc networks. Proceedings of the 2008 IEEE International Conference on Communications, May 19-23, 2008, IEEE, Hong Kong, ISBN:978-1-4244-2075-9, pp: 2343-2347.

Ghosh, U. and R. Datta, 2009. Adip: An improved authenticated dynamic ip configuration scheme for mobile ad hoc networks. Int. J. Ultra Wideband Commun. Syst., 1: 102-117.

Ghosh, U. and R. Datta, 2011. A secure dynamic IP configuration scheme for mobile ad hoc networks. Ad Hoc Netw., 9: 1327-1342.

Hashmi, S. and J. Brooke, 2008. Authentication mechanisms for mobile ad-hoc networks and resistance to Sybil attack. Proceedings of the 2nd International Conference on Emerging Security Information, Systems and Technologies, August 25-31, 2008, Cap Esterel, France, pp: 120-126.

Hsu, Y.Y. and C.C. Tseng, 2005. Prime DHCP: A prime numbering address allocation mechanism for MANETs. IEEE. Commun. Lett., 9: 712-714.

Hussain, S.R., S. Saha and A. Rahman, 2011. SAAMAN: Scalable address autoconfiguration in mobile ad hoc networks. J. Netw. Syst. Manage., 19: 394-426.

Mistarihi, A.M.F., A.M. Shurman and A. Qudaimat, 2011. Tree based dynamic address autoconfiguration in mobile ad hoc networks. Comput. Netw., 55: 1894-1908.

Nadeem, A. and M. Howarth, 2009. Adaptive intrusion detection and prevention of denial of service attacks in MANETs. Proceedings of the 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, June 21-24, 2009, ACM, Leipzig, Germany, ISBN:978-1-60558-569-7, pp: 926-930.

Nadeem, A. and M.P. Howarth, 2013. A survey of MANET intrusion detection and prevention approaches for network layer attacks. IEEE. Commun. Surv. Tutorials, 15: 2027-2045.

Nesargi, S. and R. Prakash, 2002. MANETconf: Configuration of hosts in a mobile ad hoc network. Proceedings of the IEEE Twenty-First Annual Joint Conference on Computer and Communications Societies, June 23-27, 2002, IEEE, Richardson, Texas, USA., ISBN: 0-7803-7476-2, pp: 1059-1068.

Reshmi, T.R. and K. Murugan, 2015. Filter-based address autoconfiguration protocol (FAACP) for duplicate address detection and recovery in MANETs. Comput., 97: 309-331.

Sun, Y. and R.E.M. Belding, 2004. A study of dynamic addressing techniques in mobile ad hoc networks. Wirel. Commun. Mob. Comput., 4: 315-329.

Vaidya, N.H., 2002. Weak duplicate address detection in mobile Ad hoc networks. Proceedings of the 3rd ACM International Symposium on Mobile Ad hoc Networking and Computing, Lausanne, Switzerland, June 9-11, 2002, ACM, New York, USA., pp: 206-216.

Weniger, K., 2003. Passive duplicate address detection in mobile ad hoc networks. Proceedings of the 2003 IEEE Conference on Wireless Communications and Networking WCNC-2003, March 16-20, 2003, IEEE, Germany, ISBN: 0-7803-7700-1, pp: 1504-1509.

Zhou, H., L.M. Ni and M.W. Mutka, 2003. Prophet address allocation for large scale MANETs. Ad Hoc Netw., 1: 423-434.