Secure Host IP Configuration Protocol for Mobile Ad Hoc Networks

Fathimabi Shaik and N. Rama krishnaiah
[1] M.Tech student, Computer Science and Engineering, Jawaharlal Nehru Technological University, Kakinada, India.

[2] Assistant Professor, Computer Science and Engineering, Jawaharlal Nehru Technological University, Kakinada, India

Abstract

Secure dynamic IP addressing is a prime requirement for unicast communication between authorized hosts in mobile ad hoc networks(MANETs). Recently, several approaches have been proposed for dynamic addressing scheme. However, most of the approaches rely on broadcasting for address solicitation and/or duplicate address detection. As a result, several types of security threats in dynamic IP configuration can be observed. In this paper, we present an ID based dynamic IP configuration scheme that can securely allocate IP addresses to the authorized hosts for a mobile ad hoc network without broadcasting over the entire network. Each host in the MANET can generate new unique IP address from its own IP address for a new host. The proposed scheme provides authentication for address configuration without the help of a trusted third party without compromising the security-threats associated with dynamic IP configuration. Performance analysis shows that our proposed addressing scheme has less addressing latency and control overhead compared to the similar existing schemes. The proposed scheme is using MAC address to generate ID so, it is providing more security. Moreover, the proposed scheme is able to solve the problem of network partitions and mergers along with the arrival and departure of a host efficiently and securely.

1. INTRODUCTION

Mobile Ad hoc Network (MANET) is a collection of two or more devices equipped with wireless communications and networking capability. The devices within the radio range can immediately communicate with each other. The nodes that are not within each others radio range can communicate with the help of intermediate nodes where the packets are relayed from source to destination. Each node should be configured with a unique identity to ensure the packets correctly routed with the help of routing protocol (e.g., AODV [1]) in the MANET. In this paper, we focus on the problem of secure unique address allocation in an independent MANET.

Traditionally, a user can either configure the address of a host manually or the host can acquire its IP address dynamically through certain dynamic methods, such as, Dynamic Host Configuration Protocol (DHCP) [2]. Manual address configuration in most cases is inapplicable to MANETs. DHCP requires the presence of a centralized DHCP server which maintains the configuration information of all hosts in the network. Since a MANET is devoid of any fixed infrastructure or centralized administration, this approach cannot be used.

Recently, a number of dynamic address configuration protocols ([4]–[7], [10]–[12]) have been proposed. However, most of the protocols either rely on passive duplicate address detection (DAD) mechanism [8] to resolve the address conflicts or lack a mechanism for authentication or rely on a trusted Mobile Ad hoc Networks (MANETs) are very attractive for either military or civilian applications in environments where fixed infrastructures are not available and rapid deployment is desired. Mobile Adhoc Network is a collection of two or more devices equipped with wireless communications and netwokring capability. In the last decade, large research efforts have been made to address challenges posed by MANETs. These challenges include mainly IP address auto-configuration, routing, security and QoS issues. In security context, the major part of research up to now was concentrated mainly on trust models and routing security problems. However, the lack of security in previously suggested auto-configuration schemes can lead to serious attacks in potentially hostile environments, mainly IP spoofing attack, sybil attack, traffic overload DoS attack, exhaustion address space attack, and conflict address attack. This problem was tackled by some few papers [1]-[5]. We have analyzed these proposals and pointed out their weaknesses and shortcomings in [13]; we have identified also the imperative security requirements related to this problem.

In the present paper, we propose a new ID based secure stateful IP address allocation protocol

for MANETs. The scheme relies on ID generation and verification and Message Authentication using RSA and SHA1. This proposed scheme explores improved solution to the problems which may arise due to host failures, message losses, mobility of hosts and network partitioning and merging. This scheme solves definitively the problem of some attacks such as IP spoofing and Sybil attacks, unsolved up to now by conventional mechanisms.

The remainder of the paper is organized as follows. In section II, we present our ID based auto-configuration Algorithm. Section III gives the performance comparison, which is followed by conclusions presented in Section IV.

II. The IDSA Algorithm

In this section we present our proposed algorithm for secure ID Based IP configuration where IP addresses are allocated to the network nodes dynamically. We call this proposed technique as IDSA , ID Based Secure IP Address Allocation Algorithm. As mentioned in section I, most of the existing address allocation schemes for MANET are not providing security. Here in this paper we propose a technique where every we are doing node authentication and message authentication.

Address Allocation Algorithm:

1 Set configured = false
2 Set begin = true
3 Generate publickey=KPN, PrivateKey=KSN
4 If begin= true then
5 Generate sign(KSN,RTJ);
6 (RTJ+SigN) message 1-hop broadcast;
7 Start RTJTimer ;
8 Begin=false
9 Else
10 Selfconfigure();
11 Configure=true;
12 End
13 If multiple (response(OfferIP)+Sigc) msgs from neighbours then
14 Select minimum IP from response(OfferIP) messages;
15 Generate node_idG = H(IP,KPP);
16 Generate SigG(KPP,Response(OfferIP));
17 If SigG==SigI and node_id G== Node_idI then
18 Generate node_idN=H(offerIP,KPN);
19 Generate SigN(KSN,Select(Node_idN));
20 Send (select(node_idN)+SigN) to selected initiator;
21 Stop ResponseTimer, start AckTimer
22 Else
23 Select next minimum IP From Resonse(OfferIp) messages;
24 Goto step 13
25 end
26 end
27 if(ACK+SigC) is received from selected Initiator then
28 Generate node_idG=H(IP,kPC)
29 generate SigG(KPP,ACK);
30 if SigG == SigC and node_idG== node_id C then
31 stop acktimer
32 configured =true
33 end
34 end
35 if(Timeout(ResponseTimer) then
36 begin =true
37 end
38 if(Timeout(ackTimer) then
39 begin=true
40 end

a) IP Address Allocation: When a new node Nn wants to join a MANET, it first randomly generates a public key and private key (KPN,KSN)pair. It then periodically issues a RTJ broadcast message along with signature SigN to its neighbours till it receives response messge. If no message received then the new node Nn configures itself and generates a unique network ID and also node identifier node_id. The RTJ messages contains MAC address as an identifier of the host Nn and 0.0.0.0 as the IP address. The neighbor nodes on receiving the signed RTJ message then they send response(OfferIP) messges to the new host. When the new node Nn receives the signed response(OfferIP) messages from its neighbors it chooses the smallest IP address that is offered to it. This smallest IP address is then unicast in a signed select message back to the initiator offering that IP address. The other Response(OfferIP) messages sent by neighbors are ignored by Nn. On receiving the signed select message, signed Ack message is sent to the new Node Nn. After receiving signed Ack message from the selected initiator, Nn performs a final check on the configuration parameters specified in the ACK message and configures itself.

It may be noted that if during the IDSA address allocation procedure some packets are lost (due to channel error, mobility etc), the initiator and the new node Nn may sometimes lost synchronization. In such a situation the IP address may get wasted or the IP may be assigned to some other nodes if proper steps are not taken. The proposed protocol solves this problem by using timer. The timer times out in case it does receive acknowledgement leading the concerned node to response a packet.

b) Authentication: In our scheme In our scheme, authentication of a new node *Nn* and a initiator is verified at the time of address allocation in the following way: the node *Nn* generates its node ID (*node idN*) using secure one-way hash function (*H*) in the following way:
node idN = *H*(*offerIP*,*KPN*), where *KPN* is the public key of the node *Nn* and *offerIP* is the offered IP address by a Initiator to it. The node *Nn* sends its *node idN* to the Initiator. The Initiator also generates node ID (*node idG*) same way for the node *Nn*. The node *Nn* is authenticated if and only if the received *node idN* and the generated *node idG* are same. Similarly, the node *Nn* can also verify the authentication of a Initiator. It generates *node idG* using the IP address and the public key (*KPP*) of the Initiator. The Initiator is authenticated to the node *Nn*, if and only if the received *node idI* and the *node idG* generated by the node *Nn* are same.
The scheme also uses signature for the message authentication. Node *Nn* generates a signature (*SigN*) using its private key (*KSN*) for each message and then sends the signed messages along with its public key (*KPN*) to the Initiator.
The Initiator also generates signature (*SigG*) on the received messages using the public key of the node *Nn*. If the received *SigN* and the computed *SigG* is same, the the Initiator is ensured that the messages are from the authenticated node.
Similarly, the Initiator node also generates signature using its private key (*KSP*) and sends the signed messages along with its public key (*KPP*) to the node *Nn*. The node *Nn* can also verify the authenticity of the received messages from the Initiator in the same way.
c) *Graceful Departure:* A node may join or leave a MANET at any time. If a node wants to depart gracefully, it sends signed RELEASE message with its *allocation status* to its parent node to avoid address leak problem. Every node maintains recycleLIST to record the *allocation status* for its departed children. After receiving the signed RELEASE message from its children, checks the authentication of the children as well as the signature of RELEASE message. If the authentication becomes successful, the parent node updates its recycleLIST and sends a signed OK message to the departing children. If the departing node receives a signed OK message from its parent node before the timer expires then the departing nodedeparts gracefully. If the root node wants to leave, it informs its greatest descendent to be the new root. The function for graceful departure of a node and the corresponding parent Initiator using pseudo code is given in function graceful departure and graceful departure children respectively.

Function graceful_departure
1 if *configured = true* then
2 Generate *SigN*(*KPN*,*RELEASE*);
3 send (*RELEASE* + *SigN*) message to parent;
4 start okTimer;
5 if (*OK* + *SigP*) *message is received from parent* then
6 Generate *SigG*(*KPP* ,*OK*),
node idG = *H*(*IP*,*KPP*);
7 if *SigG == SigC and node idG == node idC* then
8 stop okTimer;
9 if *switch-off* then
10 *configured* ← *false*; *counter* ← 1;
11 end
12 else
13 departure;
14 end
15 end
16 end
17 end
18 if *timeout(okTimer)* then
19 *counter* ← *counter* + 1;
20 end
Function graceful_departure_children
1 if (*RELEASE* + *SigN*) *message is received from children* then
2 Generate *SigG*(*KPN*,*RELEASE*);
3 Generate *node idG* = *H*(*IP*,*KPN*);
4 if *SigG == SigN and node idG == node idN* then
5 Generate *SigP* (*KSP* ,*OK*);
6 send (*OK* + *SigP*) message to requested children;
7 recycle the IP address into the recycleLIST;
8 else
9 drop the (*RELEASE* + *SigN*) message;
10 exit;
11 end
12 end

d*) Graceless Departure:* A node departure may be graceless due to several reasons. It may be due to packet loss or when two MANETs merge. It can also happen if a MANET splits into two or more MANETs. It is therefore necessary to detect the graceless departure of a node so that its IP address can be reused. In order to detect graceless departure every node scans IP addresses of its children. If the parent node discovers that a child node is missing, it then updates the recycleLIST for the missing child node to reuse the IP address later. Graceless departure or address leak problem can be detected by periodically broadcasting signed HELLO messages of AODV routing protocol. Thus, there will be no additional overhead to detect graceless departure of a node.
e*) Network Partitioning and Merging:* Due to its dynamic and unpredictable nature, a MANET can

partition and again merge at any instant of time. Network partitioning is detected when a node stops receiving HELLO messages from its neighbors. In such a case the node will become the new root and generate *Network ID* (NID) as a network identifier of the split MANET. This NID is then sent to the nodes willing to join the split MANET. In our proposed protocol, there will be no address conflicts in the event of network partitions. However, if the network is partitioned and again merged then there are chances of IP address conflicts. The proposed protocol solves this address conflict as follows: Todetect network partitioning and merging we have used unique ID as a network identifier. This identifier is contained in the periodic HELLO message of AODV routing protocol. HELLO messages are exchanged between neighbors. When the two partitions merge, the network ID of an alien node can be detected by a host through the HELLO messages it receives. In our proposed IDSA scheme, node is identified by a unique tuple *_node id, IPaddress_*. Though, there is a chance of IP address conflicts for a node, the probability of tuple conflict is significantly less. Moreover, the possibility of tuple uniqueness in the MANET can be detected using AODV routing protocol.

This can be done by sending a signed route request (RREQ) message with its own node id and IP address as the destination address as well as the source address. The tuples are in conflict if it still receives the signed route reply (RREP) message from the network. In case of tuple conflicts, the node having less number of neighbors with the same NID has to reset its configuration and call IDSA algorithm as a new node *Nn*.

Otherwise, the node has to change its ID with the NID of the other partition. It may be noted that in the initial state of address allocation, more than one node may configure themselves with the same IP address. Even then there is very less chance of tuple conflicts.

III. PERFORMANCE COMPARISON

Table I presents the comparison of our proposed IDSA scheme with the existing dynamic addressing approaches. We focus on qualitative evaluation of all the approaches. Let *n* be the number of mobile hosts in the network where the number of links is *l*, the average 1-hop latency is *t* and the network diameter is *d*. The existing DHCP [2] gives the guarantee of the uniqueness but can not be deployed in mobile ad hoc network. Further, DHCP needs to locate the server. Thus the latency is 4x *tx d* and communication overhead is *O(n2)*.

Another dynamic allocation scheme ANETconf [4] requires a positive acknowledgment from all known nodes indicating that the address is available for use.

TABLE 1

COMPARISION OF DYNAMIC ADDRESSING APPROACHES

Metrics	DHCP	ManetConf	ODACP	Prophet	Prime DHCP	IDSA
Uniqueness	Yes	Yes	Yes	No	Yes	Yes
Latency	O(4td)	O(2td)	O(2t)	O(2t)	O(2t)	O(2t+m)
Overhead	$O(n^2)$	$O(n^2)$	O(2l)	O(n/2)	O(n/2)	O(n/2)
Complexity	Low	High	Low	High	Low	Low
P.Msg	Yes	Yes	No	No	Yes	Yes
Security	No	NO	No	No	No	Yes

Duplicate address detection (DAD) [8] is also necessary for MANETconf. Thus, the latency of MANETconf is 2 x *t x d* and the communication overhead is *O(n2)*. In ODACP [3], every host need to register with an address authority to reduce the communication overhead from *O(n2)* to *O(2l)* and the latency from 4 x *t x d* to 2x*txd*. Prophet [5] is the only mechanism that can not guarantee the uniqueness of addresses. Both Prophet and Prime DHCP [6] send their request to neighbors for an IP address and therefore the latency is 2t. The communication overhead of and Prime is the average degree (*n*/2) of each node in the network. MANETconf and prophet are complex address allocation scheme. Most of the approaches including our proposed IDSA scheme use explicit mechanisms to detect network events such as partitions and merges except Prophet.

The detection is normally accomplished by utilizing a unique network identifier which is either broadcast throughout the network by a leader node, or is contained in periodic hello messages (refer to P.Msg in table I) exchanged between neighbors. Finally, none of them have considered MANET security except our proposed IDSA scheme.

In the proposed IDSA, every Initiator in the network generates an unique IP address from its own IP address for a new host. After the partition occurs, the split networks can grow independently. Now if the partitions are merged at any later stage, even there is a chance of IP address conflicts, the chance of tuple *_node id, IP address_* conflicts are very less. This shows that the IDSA scheme is robust and has no additional overhead to detect network events such as partitions, mergers or graceless departure of a node.

The IDSA host *Nn* sends request to neighbors only for an IP address, assuming that the address space is sufficient, the latency is 2*t* +*m* and the communication overhead is the average degree (*n*/2)

for each node of the network. Here *m* is the complexity of the public key *digital signature* (e.g., RSA) algorithm. Thus, both the latency and overhead are less for address allocation. The complexity is also low for address allocation as neither there is a need to maintain any block of addresses, nor there is a requirement to generate any complex function for an IP address. Also the IP addresses for new nodes are generated from a node acting as *Initiator* which reduces the complexity and memory requirement of our scheme even further.

Fig 1 . During Address Assignment Process

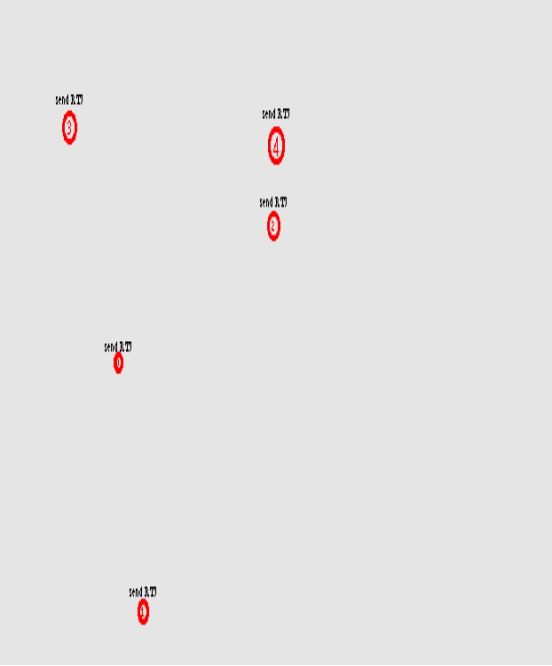
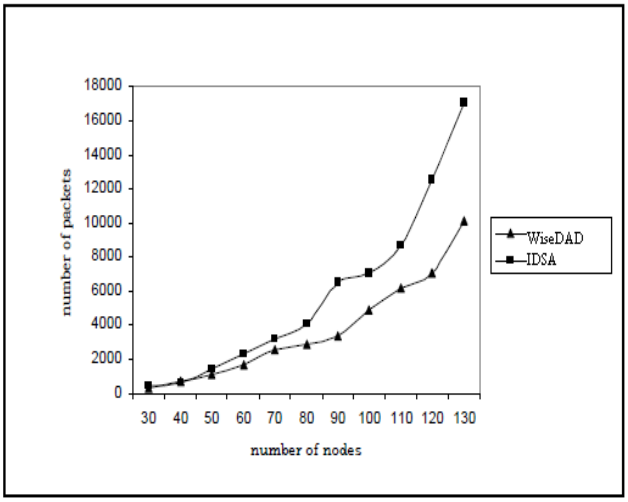


Fig 2. Effect of network size on communication overhead



Finally, in our proposed IDSA scheme, a node can verify authentication of another node. Also, all the IDSA messages are signed using private key of the sender and then transmitted. The receiver can verify the signature of the received messages and also the authenticity of the sender. Without any authentication, an attacker can spoof an IP address of a host in the MANET and may transmit false messages, such as, address conflicts, deny messages to a host during address allocation process. It also ensures that the attacker neither can generate signature for a message nor IP can be spoofed without knowing the private key.

IV. CONCLUSION

In this paper we proposed a secure dynamic IP address allocation algorithm for mobile ad hoc networks. In the algorithm every node in the network also acts as a Initiator and has the capability to assign IP addresses securely to authorized new hosts. The scheme also ensures that only authorized host will be configured in the MANET. The signaling messages for the address assignment need not be flooded all over the MANET, thereby saving considerable bandwidth. In addition to this, as each host can assign a unique IP address for a new host and the node is identified by a unique tuple *_node id, IP address_*,the DAD broadcasting is not required. The scheme can also handle network partitions and mergers efficiently and securely.

Further, it has low complexity, low verhead, is robust and more secure in comparison to the existing addressing schemes for the MANET.

REFERENCES

1) C. Perkins, E. Belding-Royer, and S. Das,“Ad hoc On-Demand Distance Vector (AODV) Routing,” draft-ietf-manet-aodv-11.txt, June 2002 (work in progress).
2) Applications, ACM Press, pp. 234-244, 1994.R. Droms, “Dynamic host configuration protocol”, RFC 2131, Mar. 1997.
3) Y. Sun and E. M. Belding-Royer, “A study of dynamic addressing techniques in mobile ad hoc networks”, *Wireless Communications and Mobile Computing*, April 2004.
4) S. Nesargi and R. Prakash, in MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network,” in *Proc. INFOCOM*, 2002, pp. 1059-1068.
5) H. Zhou, L. M. Ni, and M. W. Mutka, “Prophet address allocation for large scale MANETs”, in *Proc. INFOCOM*, 2003, pp. 1304-1311.
6) Y. Hsu and C. Tseng, “Prime DHCP: A Prime Numbering Address Allocation

Mechanism for MANETs", in *IEEE Communicatons*, August 2005.

7) M. Fazio, M. Villari, A. Puliafito, "AIPAC: Automatic IP address configuration in mobile ad hoc networks", in *Performance Evaluation of Wireless Networks and Communications*, Computer CommunicationsVolume 29, Issue 8, 15 May 2006, pp. 1189-1200.

8) K. Weniger., "Passive Duplicate Address Detection in Mobile Ad Hoc Networks", In *WCNC*, Florence, Italy, February 2003.

9) S. Ni, Y. Tseng, Y. Chen, and J. Sheu. "The broadcast storm problem in a mobile ad hoc network", In *Proceedings of the ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM)*, 1999 pp. 151-162.

10) Ana Cavalli, Jean-Marie Orset, "Secure hosts auto-configuration in mobile ad hoc networks", in *Data ommunication and Topology Control in Ad Hoc Networks*, Ad Hoc NetworksVolume 3, Issue 5, September 2005, pp. 656-667.

11) P. Wang, D.S. Reeves and P. Ning, "Secure Address Auto-Configuration for Mobile Ad Hoc Networks", in *Proceedings of 2nd Annual International Conference MobiQuitous 2005*, pp 519-522.

12) U. Ghosh and R. Datta, "An Authenticated Dynamic IP Configuration Scheme for Mobile Ad Hoc Networks", accepted in *Sixth International Conference on wireless and Optical communications networks (WOCN2009)*, Cairo, Egypt, april 2009.