Combining SDRAC & TARF technologies for addressing and communication in MANETs

Triveni[1], Dr.Mohamedh Rafi[2]
[1, 2] Department of CS&E
[1, 2] UBDT College of Engineering & Technology, Davanagere, Karnataka,india

Abstract- *In this paper new technology going to introduce for address allocation for group of wireless networks. This Schema is low-overhead identity based and can allocate the address as required. Since MANETs does not have infrastructure an antagonist use this to hurl various harmful attacks. To secure TARF routing framework is using for secured communication.*

Keywords- MANET, Address allocation

I. INTRODUCTION

Mobile Adhoc Network is self-designed stateless network. Hear movable systems are linked by wireless connections. Each

System in the network can move in any direction without any restriction therefore infrastructure of the network changes repeatedly. Systems that are within the range can to exchange message in a direct manner. Then nodes outside the range communicate with each other interposed nodes. These nodes transfer the packets from source to destination.

There are two types in mobile adhoc network 1) Pure, 2)Managed. Pure are constructed without any preparation any node can enter and exit the network whenever it is required it does not requires registration and something else. But in some serious application such as in military application it is not suitable so there required authorization of nodes. Those are allowed in the network. So In that situation Managed MANET's are helpful here every node in the network have the public key, private key, &session key so that the messages exchanged between the nodes are protected & cannot be hacked easily.

Since in wireless sensor network messages are exchanged between the source &destination through the multi-hop path. It will become the target of malicious assaults like selective forwarding, sink whole assault& syhil attack etc. An attacker node simply replays all the outgoing packets from a valid node by duplicating its identity or address.

Sink whole attacks are performed after stealing the valid nodes identity. Here a spit node will act as a real base station. Sometimes a valid node in the network also compromises to perform the attacks in the network.

Objectives:

To assign IP address to the nodes a IP addressing standard must have coming after accusatives:

- Shared IP skill Structure: Address which is going assigned to the every system of the network must be shared because MANETs does not have the Infrastructure.
- Unique or Different IP Address:
- The protocol should assign the different address for every system of the network.
- Robust: Network partitioning &merging is more in wireless networks so that it is strong enough to deal with the address conflicts.
- Should support Growth of the Network: Protocol should take same amount of time to assign IP address to the network Even if systems in the network Increases.
- Pledge against Attacks: It should provide the protection against Security threats that incurs during the address allocation Process.

II. RELATED WORK

Already there are two types of existing IP address allocation Schemas Stateless and State full. In Stateless IP Address Allocation schema the node enters to network simply chooses one IP address & send this address to every node in the system to check whether they having same address or what. If any node having same IP address the same process is repeated till it is different from others. But this process produce unwanted traffic in the network &collision between the packets occurs, this problem is called dispersed widely problem.

In state full assigning approach every system of the network stores the information about the already assigned address, available address & about network management. Here network partitioning &merging can be takes place with the help of DAD mechanism.

In Dynamic address configuration protocol scheme one node will maintain the address information of each of the node.

In buddy system technique available addresses are divided into blocks &these blocks will be maintained by nodes in the network. Node which wants address repeatedly sends requests .On accepting this message originator system separates the mass of available addresses into 2 portions.

Taghiloo proposed a virtual address space. In this schema initiator node assign address to new node by taking address from allocator node. Tajamolia, Taghiloo proposed another schema it uses secret key encryption technique for address allocation in order to solve the problems like security threats. It is light weight &secured schema for address allocation. We can allocate unique address to nodes by using mechanisms like prime DHCP, ADIP, IDDIP& IDSDDIP. DSDV routing protocol is implemented in DHCP to find network partition & merges. In ADIP authentication is done by a third party. The trusted third party may involve in security attacks. Self-authentication technique is used in IDDIP & IDSPDIP techniques.

A new technique is proposed that is filter based addressing protocol. Here filters contain already allocated addresses in dense fashion & it also stores the distributed database. Bloom filter used to assign the unique address. Sequence filters are used to find the address conflicts during the merging of networks.

But in all existing schema we have to use DAD mechanism to find the duplicate address because of this traffic in the network will become more.

III. WORKING PRINCIPLE

This proposed technique or algorithm is SD-RAC algorithm. It allocates the address to new nodes with low overhead. Already existing node act as a proxy to assign the address. Each of the Proxy node stores the information about the already assigned addresses, while assigning the address to new node it checks the stored information so that it can assign new unique address. DAD mechanism for address resolution also does not require. It saves Considerable amount bandwidth and energy of the network. After assigning the address secure communication takes Place with the help trust value assigned to the neighbors nodes, here two technologies are combined for address allocation & secure communication. SDRAC algorithm & TARF technologies are implemented for his purpose respectively.

System Model & Key distribution

Each of the authorized node in the network has set of IDs, these IDs are stored in a table called Tlist. The network starts with a single node grow up by adding other nodes. We pretend to possess that the first node from which network starts is trustable or non-malicious node. Each of the nodes in the network can move feely means it can enter & exit the network whenever it is required. And every node in the network has the public key & private key these shared among them using following technique: set of security parameters associated with each of the nodes are G1, G2, e, H1, H2, Q1, ppub. S is the master key of the network. It is distributed between the nodes by threshold manner (N,T+1) & ppub=sQ1. Public Key (Kpa) & Private key (Ksa) are computed as follows: Kpa=H1(IDa), Ksa=SKpa. Here H1 &H2 are cryptographic hash functions. Ida is the identifier of the node a it is also a hardware address.

Address allocation by SD-RAC algorithm:

Whenever the fresh node enters the network it dispatch Discover (IDNn, r3) errand to its neighbor nodes, If it is not gets any response from neighbor such as OFFER message or DENY message within specified time period. Then itself configures as route node with unique network ID & Digital certificate. If case any of the neighbor nodes received its discover message it sends OFFER message back to new node.

Format of this message is (OFFER(IPo, Idp, r4, DIG_CERTp)).

Where

IPo-> Offered IP address to the new node.

Idp -> Hardware address of proxy node.

r4 -> Random number generated using the hash function.

DIG_CERTp -> Digital certificate of sent node.

After getting this message new node will select the IP address from required neighbor & denies the offers from the other nodes. Selected IP address sends back to the node which offering it with message (select (IDNn) +∂n). Where ∂n is the authentication tag. After receiving this message proxy sends acknowledgement back to new node i.e., ACK (IDp, DIG_CERTNn) + ∂p. New node verifies it set the configuration parameters, these are nothing but the default mask for the network & gateway address if any.

SD-RAC algorithm uses the timers to solve the synchronization problem between proxy & new node. If

acknowledgement is not received within the specified period of time, timer triggers so that relevant nodes resend the packet.

Authentication:

In the MANET each of the nodes should be authorized. So authorization process takes place by two ways: 1) The signature schema, 2) Message authentication. First method is used for broadcast errand e.g., DISCOVER. In message verification new system Nn produces a signature (σ) by make use of its private key sends this to proxy along with its hardware address proxy verifies it using public key of new node. After verifying the signature proxy generates shared key kpn. Using its private key (Ksp), public key of new node & random numbers r3, r4. After that it generates authentication tag sends this to new node. That is also generates shared key to verifies this tag. New node also generates digital signature using assigned IPo address so that it can demonstrate that its IP address is given by the trust worthy node.

Different IP Address Procreation:

The algorithm which generated the unique IP address is unique ip generation. IPV6 address 8 classes of hexadecimal numbers distinct by colons. ex:- (EBFD:OCB7:8BA4:8A2E:0000:0001:OD7A:BFEA) first 4 groups represents network prefix, next 4 groups represents the host identifier. The address is depicted in dotted decimal format. Root proxy configures itself IP address p.q.r.s.t.u.v.w.0.0.0.0.0.0.0.1 & for host identifier it assign from 1.0.0.0.0.0.0.1 to 255.0.0.0.0.0.0.0.1. Each of the nodes maintains the count that stores the information about the already assigned address so that it checks this before allocating address. If case proxy node may not have IP address to allocate then it request parent node assign the address. It grows until to reach route node thus address can be allocated from a.b.c.d.e.f.g.h.0.0.0.0.0.0.0.1 to a.b.c.d.e.f.g.h. 255.255.255.255.255.255.255.254 with network prefix so each requested node get unique IP address.

Secure Communication between the nodes:

For secure communication between the nodes TARF technology is going to implemented. In this technique security against intruders is provided by evaluating trust value of neighbor node. These trust value is a decimal number [0, 1] are stored in a node. It represents the opinion the node about the neighboring node. Before starting the communication each of the nodes in the network generates a routing table this table contains the information about the paths from source to destination. There may be the multiple paths from source to destination. After that it will evaluate the trust value of each neighboring node from which it can reach to the destination. Sender sends the data to the destination by through the node which has highest trust value waiting for the acknowledgement from the neighboring node. If it gets positive acknowledgement from neighbor node then source node increases its trust value otherwise it decrease its trust value and selects another link path having second highest trust value.

IV. CONCLUSION

SD-RAC algorithm provides secure address allocation for MANETs. It is scalable, distributed and assigns address dynamically. Since existing node act as Proxy node to assign the address DAD mechanism is not required for address resolution it reduces the traffic and saves considerable bandwidth and energy. It can stand against network partitioning and merging. SD-RAC algorithm has poor addressing latency & fewer aloft than other algorithms. TARF technique is implemented for secure address communication between nodes.

REFERENCE

[1] N. C. Fernandes, M. D. D. Moreira, and O. C. M. B. Duarte, “Anefficient and robust addressing protocol for node autoconfiguration inad hoc networks,” IEEE/ACM Trans. Netw., vol. 21, no. 3, pp. 845–856,Jun. 2013.

[2] A. Pirzada, C. McDonald, and A. Datta, “Performance comparison oftrust-based reactive routing protocols,” IEEE Trans. Mobile Comput.,vol. 5, no. 6, pp. 695–710, Jun. 2006.

[3] K. Sanzgiri et al., “Authenticated routing for ad hoc networks,” IEEE J.Sel. Areas Commun., vol. 23, no. 3, pp. 598–610, Mar. 2005.