INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & MANAGEMENT

A SURVEY ON ARCHITECTURE FRAMEWORK FOR SECURE HYBRID MULTIPATH MANET

D.V.S.S.Subrahmanyam
Professor, Dept. Of CSE, Sreyas Institute of Engg. & Technology, Hyderabad, India
subrahmanyam.dvss@gmail.com

ABSTRACT

The present day people are very much enthusiastic towards internet with full speed. So everyone wants to have internet on their palms. This paper describes the connection of internet with manets, Gateways act as bridges for forwarding data packets between integrated mobile ad-hoc networks (MANETs) and the Internet. This study presents an adaptive gateway discovery scheme that balances efficiency and overhead by limiting the flooding scope of gateway advertisement messages In many applications, multipath routing scheme is favorable than single-path routing due to many advantages. Security issues in hybrid MANET, however, is still challenging task. In this paper, we present architecture framework for secure hybrid multipath MANET that can provide global connectivity. The main object of the paper is to reliable internet performance with in the low cost.

Keywords: Multipath manet.

INTRODUCTION

MANETs are a kind of Wireless ad hoc network that usually has a routable networking environment on top of a Link Layer ad hoc network. MANETs consist of a peer-to-peer,selfforming,self-healing network in contrast to a mesh network has a central controller.

MANETs circa 2000-2015 typically communicate at radio frequencies (30 MHz - 5 GHz).From the last few years mobile Adhoc networks has been a challenging task because of the limited range networks If we consider only a stand-alone MANET then it has limited applications, because the connectivity is limited to itself. In the integrated MANET-Internet communication, a connection could be disrupted either by attacks on the Internet connectivity or by attacks on the Adhoc routing protocols. Due to this reason, almost all possible attacks on the traditional Adhoc networks also exist in the integrated wired and mobile Adhoc networks.4G systems will integrate existing and new networks seamlessly, allowing mobile users to roam globally with no limit to underlying access technologies. One of the network types included in 4G systems is the Mobile Ad Hoc Network (MANET).In the integrated MANET-Internet communication, a connection could be disrupted either by attacks on the Internet connectivity or by attacks on the ad hoc routing protocols. Due to this reason, almost all possible attacks on the traditional ad hoc networks also exist in the integrated wired and mobile adhoc networks. whatever the attacks are, the attackers will exhibit their actions in the form of refusal to participate fully and correctly in routing protocol according to the principles of integrity, authentication, confidentiality and cooperation. Hence to design a robust framework for integrated MANET-Internet communication we have to minimize attacks on the internet connectivity and also on the adhoc routing protocols.

ARCHITECTURAL DESIGN OF MANET

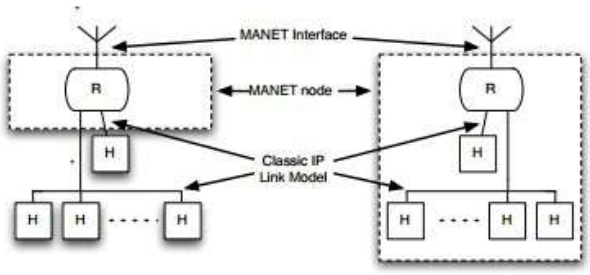

Figure.2. architecture of a manet

This architectural model considers MANET nodes as routers with hosts attached, as illustrated. These attached hosts may be" external" or" internal" – however the important observation to make is, that the links between these hosts and the router are classic IP links, behaving as described. This implies that, from the point of view of the hosts, and the applications running on these hosts, connectivity is via a classic IP link. Hosts, and their applications, are not exposed to the specific characteristics of the MANET interfaces and are connected to the MANET via a router, which has one or more MANET interfaces. This is symmetric with how hosts on an

Ethernet, such as illustrated in figure 1 are not exposed to the intricacies of what type of connectivity the router has beyond the Ethernet. Since the hosts are connected to a classic IP link, these hosts are configured and behave as hosts in any other network, and the links to which they are connected have properties identical to those of any other classic IP link.

Introduced in Mobile IP: MN (Mobile Node), FA (Foreign Agent) and HA (Home Agent). It is assumed that a MN has a unique Ipaddress associathree new functional entities wereted with its home network. HAs and FAs broadcast Agent Advertisements via one-hop link to advertise their presence. The MN checks these received Agent Advertisements to detect whether it is on its home network or has roamed to a foreign network. When the MN is away from its home network, it can obtain a Care-of Address (CoA) from a FA's Agent Advertisement and create a Registration Request to its HA. When HA receives the Registration Request, it creates a new entry containing the MN's CoA or updates the existing entry in its Binding List, and sends a Registration Reply to the FA. Upon receiving the Registration Reply, the FA records the MN's home address in a Visitor List, and relays the Registration Reply to the MN. After a successful registration, the HA maintains reach ability information for the MN in the foreign network where the CoA is allocated. All datagram's destined to the MN's home address will be tunnelled to the MN's CoA by the HA.Subsequently, the FA encapsulates the tunneled datagram's and delivers the datagram's to the visiting MN. Using Mobile IP, MNs are able to maintain their unique home IP addresses on the global Internet.

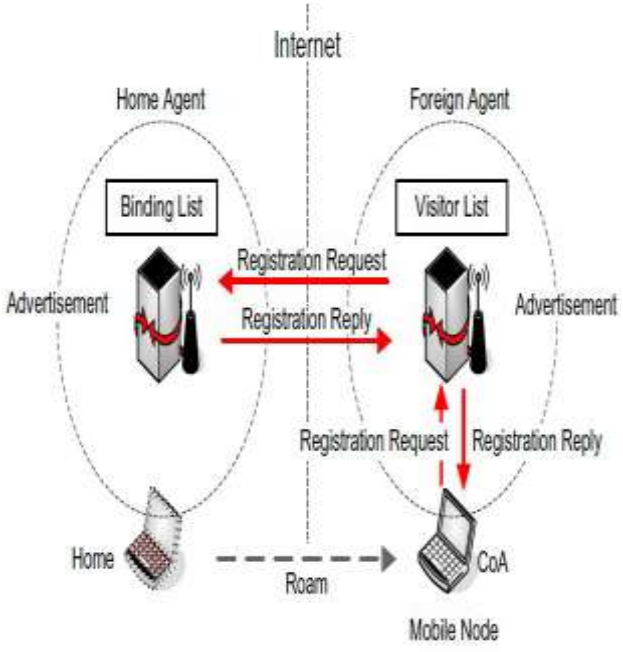

Fig. 2. Mobile IP agent discovery and registration operations.

Proacrive approach
Within the MANET, a modified Routing Information Protocol (RIP) plays the role of a proactive routing protocol. One foreign agent works as a default IP router for the entire MANET, and simultaneously participates in the ad hoc routing. The foreign agent advertises periodically; all ad hoc nodes are compelled to register with the foreign agent. The modified RIP is responsible for relaying Agent Advertisements and Registration messages between the ad hoc nodes and the foreign agent via multi-hop paths.

Reactive approach
Reactive ad hoc routing protocols have been developed to decrease the control overhead and preserve the bandwidth. Under reactive routing protocols, routing information is obtained only when needed, and two main phases are involved: Route Discovery and Route Maintenance.
Advantages:
The bandwidth between the manet and the router can be decreased in this route is maintained as no other traffic in gateways may not perform.
Disadvantages:
In maintaining the two phases the authentication may delay.

Generic ADHOC Routing:
Hoagent designed Manets using hierarchal mobile ip based mobility anchor point(MAP)manages the multiple access routers serving the manet. A mobile Node moving the within map can register with an AR, without necessity to update registration frequently with its home agent. In this way (AR) discovery can be implemented using reactive adhoc routing protocols. These protocols are crucial in challenging various nodes discovery procedures within the given protocol designed with the network interface in the mobile nodes that are proposed within the given network .the topology also plays a major role providing access to the given network by providing static and dynamic routing gateways and these gateways are to be proposed at various levels and to be maintained at different network topologies if the node indicated by the temporary ip address matches the requested address and different and the mapping between various global topologies provide bridge between various nodes connected over a network

GATEWAY DISCOVERY

The gateway discovery is a key component in providing Internet connectivity to the MANET. An ad hoc node must discover an Internet gateway prior to communicating with an Internet correspondent node. The gateway discovery approaches can be broadly divided into three categories: proactive approach, reactive approach, and hybrid approach. In the proactive approach, adhoc nodes passively hear periodic advertisements from Internet gateways. In the reactive approach, ad hoc nodes may actively solicit advertisements from gateways when necessary. The hybrid approach may combine the proactive approach and the reactive approach together.

MIP-MANET solution
(i) Sequence number: This number is copied from the Sequence Number field in the Agent Advertisement. This is used to determine (and drop) duplicate Advertisements.
(ii) FA lifetime: This is the lifetime of the foreign agent, which is three times the Advertising Interval. A mobile node considers that it has lost connectivity with the foreign agent if the FA lifetime field expires.
(iii) Registration lifetime: This indicates the period of valid registration for the mobile node at the foreign agent.

Gateway route expiry
(i) The mobile node has not received Agent Advertisement from its registered gateway for more than one Advertising Interval,
(ii) The route to the registered gateway has become invalid because of the route expiration or movement. If one of the above conditions is satisfied, the mobile node (initiator) will solicit a new gateway by originating a special RREQ, in which the destination is the All Mobility Agents Multicast Group.

ROUTING INTEROPERABILITY

Here we have designing of protocol interfaces.

Protocol interfaces
Between manet and the internet gateway is also an ip router connecting the heterogeneous networks so that have different Mac protocols. The protocol interface design sub standing concerns the packet processing algorithm activated when ip layer receives a packet from physical layer(or)from the higher layer

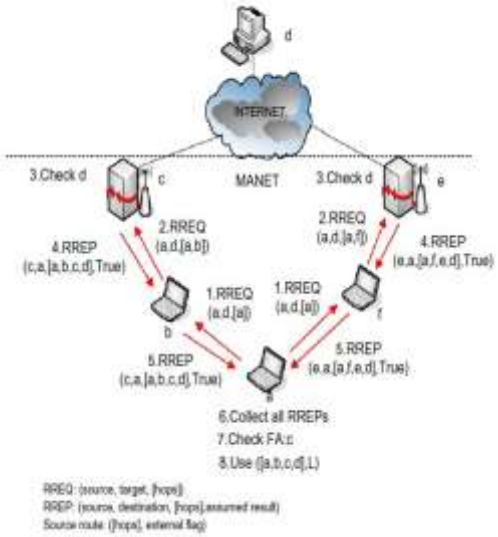

Figure.4.1. External route discovery

under reactive adhoc routing when a source node within the manet attempts to contact an unknown destination, it needs to discover the destination location. Inside or outside the manet and obtain a route to the destination by RREQ/RREP cycle most existing schemes assume that the manet is configured as an ip subnet so any destination with a different network prefix from the subnets prefix must belong to external network a gateway may send a proxy RREP indicating a route towards external destination.

SECURITY ISSUES

MANETs suffers from number of vulnerabilities owing to the fact that they depend on their constituent nodes to function effectively. Malicious nodes may interfere with the smooth functioning of the network through quite a few ways as described as below 1.Daniel of service: It is one of the well known attacks on the computer systems largely because it has on the smooth functionality of the network. This kind of attack is especially damaging to MANETs owing to the limited communication bandwidth and resources of nodes. In the AODV protocol for instance, a large number of RREQs,they flood the entire network leading to the consumption of all node battery power, along with network bandwidth and this could lead to Dos Black Hole Attack: The malicious node advertises its availability of new routes without checking its routing table. In this way routing availability is made to reply to the request and hence intercept the data packet.As,the result of the dropped packets the amount of retransmission is done with congestion. this is a more stable form of the attack wherein the attacker selectively forwards packets may be suppressed whenever necessary over the network.

Routing table/cache poisoning:

In this kind of attack, hostile nodes in the network sends fictitious routing updates or modify genuine route update packets are sent to the given uncompromised nodes within the given network each node cache contains information about specific routes that have been frequently used and an adversary may also poison the route cache to achieve similar objectives.

Colluding attacks:

This kind of threat is encountered when two or nodes collude in order to disrupt the smooth functioning of the network by modifying all packets addressed to them. it also causes a significant damage to the network over particular nodes.

Methods proposed to secure routing protocols:

Secure AODV:

This is an extension of the AODV protocol routing messages in the given network yields route requests and route replys are authenticated and guaranteed to the integrity and authenticity. This source node signs the routing message and makes the security with the private key and the recipient. nodes verify the nodes with the public key and its hash chain mechanism is used to prevent the hop count by hostile intermediate nodes. However this protocol suffers from the performance amount on the use of consumption of the given load on the network and this load can be reduced due to great performance ability distribution.

Secure routing protocol(srp):

Attempts to implement more nodes in generalized way can be able to reduce the load over the network when the intermediate node receives the node information in the given architecture and route discovery procedure along the given network and different protocols are being implemented to reduce the load and maintain proper routing over

the network. this prevents a few attacks such as spoofing and various methods vulnerable to the attacks that gives different protocols over a network.

PROBLEM STATEMENT

Problems in architecture

The design of protocol interfaces to achieve integration of adhoc routing protocols and mobile ip in the ip routing system of the internet architecture in this is cannot produce a new connection immediately after the failure of the old connection in architectures we use many many algorithm to overcome this problem but according to this paper in every architecture we have to integrate the manet with the network every time and establish a new connection. So by this problem the interface again starts from the first phase.

Problems in gateway

In the gateway discovery the manet has to send a request to the network to establish a new connection if the on port is already working with a manet it has to re request the network for a new gateway. If all the gateways are busy in connecting it has to wait until the connection established.

Problems in security issues

Developing a security mechanisms to protect manets from malicious attacks is essential. By having have single username and password the hacker can easily attack the Manet so the security level in this must be high. Even though here they used key management algorithm and identity based cryptography algorithm they have their own security issues.

PROPOSED SOLUTION

The mobile nodes move according to the improved version of the commonly used randomly way point model. It has been shown that the original random waypoint model can generate incorrect routing information. With the improved random way point model the mobile node reaches a steady state after a quick warm up period. Each mobile nodes begins the simulation by selecting a random destination in the defined network area and moves to the destination in a random speed. the random speed is distributed uniformly over a specific time interval. Upon reaching the node the mobile node waits for another node and selects various paths over the network. This is called as the mobility model of the given system.

Proposed solution to prevent hacking:

If the authentication of the network has done by having the username and password it can be easily hacked .So here we propose a private key is automatically generated with the user is connected through the gateway and a unique ip address is provided so that the user and data of the user can be prevented from hackers.

CONCLUSION

Efficient management of Mobile IP functionality supporting seamless data services in the Internet integrated MANETs where ad hoc nodes may change their association with the Internet gateways, is a major challenge. The inadequacy of existing Mobile IP schemes applicable toMANETsmotivated the search for more efficient gateway discovery/ handoff schemes. In this article, we presented one of our solutions to this challenge. Existing schemes mainly considered the Mobile IP authentications to enhance the securities in MANET-MIP networks. It would be of future research interest to configure more secure authentication protocols, such as Remote Authentication Dial-In User Service (RADIUS) protocol and Access Controller Access Control System Plus (ACACS+) protocol. On the other hand, developing security mechanisms to protect the MANETs from malicious attacks is essential. For future work, a robust framework that strengthens the securities both on the Mobile IP part and on the MANET part is highly desired.

REFERENCES

1. http://xanthippi.ceid.upatras.gr/courses/mobile/2005_06/int.pdf
2. http://hipercom.thomasclausen.net/resteam/data/publications/b
7f1ba5e862cd37af321ce71cacab179.pdf
3. http://www.cscjournals.org/library/manuscriptinfo.php?
mc=IJCSS-292
4. http://dl.acm.org/citation.cfm?id=1405269
5. http://www.ijcaonline.org/manets/number4/SPE89T.pdf