“A Proposed Model for Service Discovery with Security in Wireless Adhoc Network”

Noor Mohd[1, 2], Quamar Danish[1]

[1] Graphic Era University, Dehradun, India

[2] Research Scholor Bhagwant University, Rajasthan India

noormohdcs@gmail.com; danishquamar@yahoo.com

ABSTRACT

Service discovery technologies are exploited to enable services to advertise their existence in a dynamic way, and can be discovered, configured and used by other devices with a minimum of manual efforts. Automatic service discovery will play essential role in future network scenarios. Especially, the development Mobile Ad Hoc Networks (MANETs).Due to the deployment of tiny operating system and small memory, individual node is not able to perform all of the computation assigned to it, but the computation can be achieved by the concept of distributed system. Application of such kind atmosphere is needed in the area of oceanography, transaction management and getting the information of disastrous environment or geographical information of a place where a person cannot reach. We have provided a Dynamic Service Model with Security in MANET (DSM-SMT). Which provides high degree of security with dynamic service deployment, a special type of node is used for transaction recovery and provides the log of services for QoS information, which is not included in the previous model and also there is no concept of security in previous models.

INTRODUCTION

MANETs (Mobile Ad hoc Networks) consist of wireless hosts that communicate with each other in the absence of a fixed infrastructure. To make greater utilization of resources in vicinity, it is important for nodes in MANET to be able to discover remote services seamlessly and carry out transactions with the service providers, while security is paramount to the success of the transaction. In MANET, each node can be a combination of service user, service provider and service directory, which caches the service providers in vicinity. Therefore a decentralized approach is required for maintaining service and information about service objects. The routing protocol DSDV[1], AODV[2], TORA[3], DSR[4] uses destination addresses to deliver the packets. In case of MANET the mobile nodes uses the service of other node in neighborhood for processing a transaction in distributed manner. So routing protocols are unable to provide the information about the service providers present in the MANET. The model for dynamic service providers are failed if a single malicious node inserts into the network. So there should be must have a security for preventing malicious node to get inside the network. The nature of ad hoc networks poses a great challenge to system security designers; the lack of Trusted Third Party adds the difficulty to deploy security mechanisms. In this paper, we proposed the related work in section II , Section III contains Problem Formulation, Section IV presents the proposed approach ,Section V gives the validation of proposed approach and Section VI concluded the paper and gives the future work directions .

RELATED WORK

In [5], Yuan Yuan, Ashok Agrawala, presented a secure service Discovery Protocol for MANET, which deals in finding the service provider in the mobile environment. But they have not given the concept of recovery mechanism and there is a lack of security issues. Computer networking community approaches the problem from a various perspective and proposes different architectures and protocols for service discovery, including JINI [6], UPnP [7], Salutation [8], SLP [9].In [9] The SLP defined by IETF protocol is a language-independent protocol for automatic service discovery on Internet Protocol (IP) based networks. SLP infrastructure consists of three agents: *User Agent (UA), Service Agent (SA), and Directory Agent (DA)*.In [6], A Jini system is a distributed system where the overall goal is to turn the network into a flexible, easily administered tool on which human and computational clients can find resources. In [7], UPnP uses Simple Service Discovery Protocol (SSDP) [9] for service discovery. This protocol is used for announcing a device’s presence to others as well as discovering other devices or services. In [10], captain assigned the task to node within the cluster, these nodes are called as players, and these players perform the assigned work and send the result to captain, captain collectivity find the result. For recovery purpose captain send the information about transaction to the DAA, but major problem in this work is security issues and DAA is just like a fixed node.

PROBLEM FORMULATION

In [5], support for dynamic service provider is good but in terms of security this model fails. As shown in figure1, if a malicious node get inside the network, it receives the service request message it can send a reply with a malicious message that can infect (node can also crash) and this malicious message will be saved in the service directory of node so other nodes get the reply about this service from the current node. In case of secured environment the malicious node can also send the request message of service user (node) to the other unwilling nodes.

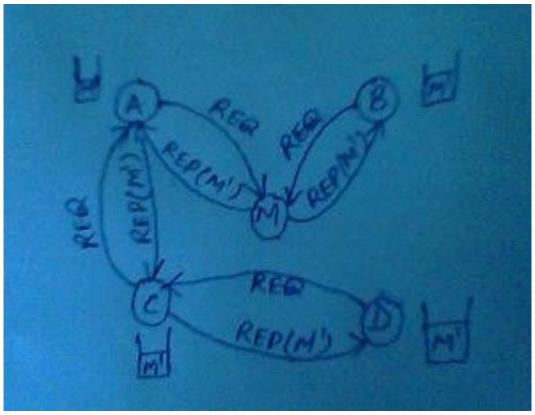

Figure: 1

For the case of recovery there is no mechanism to make the node stable with coherent data. For example if in a cluster there are five nodes. Node H is service user and node A, B, C, D are service provider. If node B leaves the cluster in between the reply of service. B can send some reply before leaving the cluster so, cache of H has some transient data after node B leaves out. The transient data from H should be removed because B will not commit. As shown in figure 2

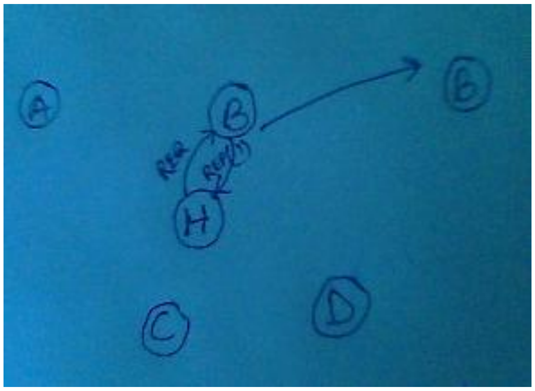

Figure: 2

PROPOSED APPROACH

SERVICE REQUEST

Each node which want the one or more services send a service request which contain following fields

[Source Address, Destination Address, Nonce, Route, HopCount, Service Description, Alive Time, Packet Type]

Source Address, is the address of sender;
Destinatin Address, is the address of destination node;
Nonce, increases per request (it reduces the chance of duplicacy)
HopCount, inform the node about the maximum node the packet can travel.
Service Description, this defines the type of Service.
Route, this field preserves the information of the route the packet has traveled (this information is used for reply purpose; the reply can be done by the method of piggyback).
Alive Time, If looping occurs within the network. This provides help in removing this problem.

DSM-CLUSTER HEAD

Each node in MANET perform as a router and head contain two cache memories (high speed memory) one is used to hold the type of services which are provided by its cluster, that means it contain the services provided by the node within the cluster. Second cache is used to store the information about the type of services that are provided by the neighboring cluster. Each node within the proposed approach contains a network key, which is gained by the new node (which wants to join the cluster) from Log Manager (LM) by passing primary authentication, and secondary authentication will be done by cluster head. Each message within the network is encrypted with this network key before sending the message. In the proposed approach there is no chance to leak the network key but if any case network key becomes un secure each head communicate with its LM to get a temporary group key. LM communicates with each other and decide one network key. Which is provided by LM to each cluster head which comes under it. And cluster head again provide the network key to its nodes.

LOG MANAGER (LM)

This is a special node which contains the log for recovery it gets the data about transaction from the cluster heads, and check the primary authentication for new node which want to join the cluster.
It store the information about transaction in the form of

[Client Id, Destination Id, Hop Count, QoS]

Hop Count, and QoS are used to determine the quality of service that provided by the destination node. For example, if QoS represent the time to reply the service

Client Id	**Desti.Id**	**Hop Count**	**QoS(in time unit)**
100	2	3	10
101	3	2	13
102	4	2	10
103	5	1	20

Table 1

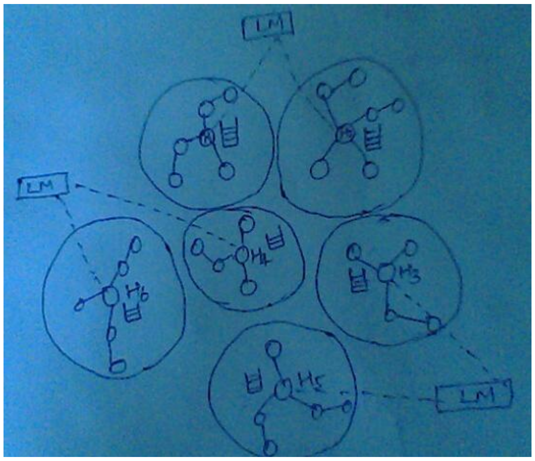

Figure: 3

Here in the above example these destinations (Id 2, 3, 4, 5) provide same service but it is efficient to choose the destination id 4 for providing the service

```
If (    client have more than one service provider for a particular service)
{
        Check the log history for that particular destination;
         Choose the Best one;
```

```
                send the information about transaction to LM;
        }
```

Whenever a node receives a service request, it performs the following steps;

```
If(HopCount == 0)
Discard the packet;
If ( Nonce are equal orDuplicated Request)
Discard the packet;
Else
Extract the Service-Description field;
If(has match in the its own first cache)

Generate Service-Reply packet (1);
Else
If(has match in second cache)
If( hops > HopCount)
Discard the packet;
Else
Generate Service-Reply packet (2);
Else
Forward the request packet (3)
```

<u>SECURITY MECHANISM</u>

A node wants to join a Cluster

Step1: When node want to join a cluster it sends a HELLO message to LM.

Step 2: LM receives the HELLO message and broadcasts its public key.

Step 3: The node which want to connect the cluster gets the public key.

Step 4: It sends an encrypted (by PU_{LM}) message with primary authentication information and its public key to LM that is required by LM to identify that this node is not a malicious node.

$\mathbf{E}_{PU}^{LM}(\,\mathbf{PU_N} \parallel \mathbf{Nonce} \parallel \mathbf{PAu}\,) \rightarrow \mathrm{LM}$

Step 5: LM receives the message and checks the authentication then sends Network key (P_G) and Cluster Head (CH) public key (PU_H) encrypted with the public key of the node.

LM : $\mathbf{E}_{PU}^{N}(\,\mathbf{P_G} \parallel \mathbf{PU_H} \parallel \mathbf{Nonce}) \rightarrow \mathrm{Node}$

Step 6: Node sends its Public key (PU_N), Nonce and Authentication Information encrypted with Network key(P_G), again encrypted the whole message with Cluster head public key(PU_H) to CH.

Node: $\mathbf{E}_{PU}^{H}(\,\mathbf{P_G}\,(\,\mathbf{PU_N} \parallel \mathbf{Nonce} \parallel \mathbf{Au}\,)) \rightarrow \mathrm{CH}$

Step 7: CH receives the message from Node.

Step 8: CH checks the authentication of requesting node by the Au message and locations of other neighboring nodes.

Step 9: CH reply the new node with public keys of neighboring nodes encrypted with Network key (P_G) then public key (P_N) of node.

CH: $\mathbf{E_P^N}$ ($\mathbf{P_G}$ (**Reply || Public Keys of the neighboring determined by location which is sent in authentication message**)) → Node
Step 10:The node receives the message and now it can connect.

CONCLUSION AND FUTURE WORK

In this paper we propose a highly secured service discovery with the use of cryptographic techniques. The problems which are created by the malicious nodes are fully removed. This paper also includes the recovery from the node crashes and leaving out of the node. The service user gets the service on behalf of QoS and hop count .Further work can include the implementation of this approach.

REFERENCES

[1] M.R. Pearlman and Z.J. Haas, "Determining the Optimal Configuration for the Zone Routing Protocol", IEEE Journal on Selected Areas in Communications, Special Issue Wireless Ad Hoc Networks, pp. 1395-1414, Aug 1999.

[2] D.b. Johnson and D. A. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", in Mobile Computing,edited by T. Imielinski and H. Korth, chapter 5, pp. 153-181, Kluwer Academic Publishers, 1996.

[3] V. Park and M.S. Corson, IETF MANET Internet Draft "draft-ietf-MANET-tora-spe03.txt", Novemmer 2000.

[4] C. E. Perkins and E.M. Royer, "Ad-hoc On Demand Distance Vector Routing", Second IEEE Workshop onMobile Computing Systems and Applications, pp. 90-100, February 1999.

[5] Yuan Yuan, Ashok Agrawala, A Secure Service Discovery Protocol for MANET, Computer Science Technical Report, CS-TR – 4498.

[6] Sun Microsystems,. Jini Community Resources: Jini Technology Architectural Overview. January 1999. http://www.sun.com/jini /whitepapers/architecture.html

[7] Microsoft Corporation,. Universal Plug and Play: Background, http://www.upnp.org/resources/UpnPbkgnd.htm

[8] Salutation Consortium,. Salutation Architecture Specification Version 2.0c. Part 1, The Salutation Consortium, June 1, 1999. http://www.salutation.org

[9] E. Guttman, C. Perkins, J. Veizades, M. Day," Service Location Protocol, Version 2", RFC 2608, IETF, Jun 1999

[10] Shalini Varshney, Implementation of collaborative Transaction Processing System on Manet ,M.Tech Thesis, IIT Kanpur,2002.