ISSN : 2278 – 1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 1, Issue V, July 2012

Secure Path with Time-Space Cryptography for Mobile Ad-hoc Networks

K.Ramakrishna[1], M.Srinivasa Rao[2], Y.Rokesh kumar[3], *U.Rakesh*[4]

M.Tech (SE), Computer Science Department, Hyderabad-72, India[1],

M.Tech (CSE), Computer Science Department, Hyderabad -83, India[2],

M.Tech (SE), Computer Science Department, Nellore, Hyderabad, A.P[3],

M.Tech (SE) Computer Science Department[4],

ramakrishnamtech08@gmail.com[1], sree.mandalapu.sree@gmail.com[2], rokeshy1@gmail.com[3], rakesh.upalla99@gmail.com[4]

ABSTRACT - This Paper describes the design and performance of a secure path with time-space cryptography for mobile ad-hoc networks. It works in the time domain for key distribution between source and destination as well as in the space domain for intrusion detection along the route between them. Even if public key encryption is more powerful and superior in distributing keys, our scheme relies on symmetric key encryption because it is highly efficient and simple to implement. Thus, each node does not require any powerful hardware, thereby leading to a small and light device. The symmetric key cryptography shares a common secret key between source and destination.

Keywords: Cryptography,SecuredRouting,Ad-hoc Networks

I. INTRODUCTION

In recent years, mobile wireless networks have become increasingly important for users of computing systems. There are currently two types of mobile wireless networks, Infrastructure Network and Ad-Hoc Network. The first type refers to a network with any type of infrastructure by installing base stations in cellular networks or access points in wireless local area networks. On the other hand, the second type of mobile wireless networks does not rely on any fixed infrastructure, forming a network in ad-hoc fashion with mobile nodes. While mobile nodes that are far apart depend on others to relay data as routers, those that are within each other's radio range communicate through direct wireless links. In this paper, we focus on design and performance evaluation of our secure routing protocol for mobile ad-hoc networks. In these systems we implement the key concept of the time-space cryptography to provide secure routing against malicious attacks that mobile ad-hoc networks might face. This paper presents our time-space cryptography to provide secure routing against malicious attacks that mobile ad-hoc networks might face. The proposed scheme is named in that it works in the time domain for key distribution between source and destination as well as in the space domain for intrusion detection along the route between them. Even if public key encryption is more powerful and superior in distributing keys, our scheme relies on symmetric key encryption because it is highly efficient and simple to implement. Thus, each node does not require any powerful hardware, thereby leading to a small and light device. Sometimes, limiting the size and weight is very important in terms of portability, especially when a battery is used and it is not easy to replenish as in the battlefield environment.

A)Vehicular Ad Hoc Networks: Vehicular Ad Hoc Networks (VANET) are a form of MANETs used for communication among vehicles and between vehicles and roadside equipment. Intelligent vehicular ad hoc network (InVANET) is a kind of Intelligence in Vehicle(s) which provide multiple autonomic intelligent solutions to make automotive vehicles to behave in intelligent manner during vehicle-to-vehicle collisions, accidents, drunken driving etc. InVANET uses WiFi IEEE 802.11 b/802.11g/802.11p and WiMAX IEEE 802.16 for providing easy, accurate, effective communication between multiple vehicles on dynamic mobility. Effective measures to track the automotive vehicles, media download /upload, conference between vehicles are also preferred. InVANET can also be applied for artillery vehicles during warfare, battlefield, and peace-time operations. Mesh networking in mobile applications has been demonstrated in multiple military scenarios.

B) Computer Network: A computer network is a group of interconnected computers. Networks may be classified according to a wide variety of characteristics. This article provides a general overview of some types and categories and presents the basic components of a network.A network is a collection of computers connected to each other. The network allows computers to communicate with each other and share resources and information. The Advance Research Projects Agency (ARPA) designed "Advanced Research Projects Agency Network" (ARPANET) for the United States Department of Defense. It was the first computer network in the world in late 1960's and early 1970's.C)Network Classification: The following list presents categories used for classifying networks.*Scale: Based on their scale, networks can be classified as Local Area Network (LAN), Wide Area Network (WAN),* Metropolitan Area Network (MAN), Personal Area Network (PAN), etc.

D)Connection method: Computer networks can also be classified according to the hardware and software technology that is used to interconnect the individual devices in the network, such as Optical fiber, Ethernet, Wireless LAN, HomePNA, or Power line communication.Ethernet uses physical wiring to connect devices. Frequently deployed devices include hubs, switches, bridges and/or routers.Wireless LAN technology is designed to connect devices without wiring.

These devices use radio waves or infrared signals as a transmission medium.Functional relationship (Network Architectures): Computer networks may be classified according to the functional relationships which exist among the elements of the network, e.g., Active Networking, Client-server and Peer-to-peer (workgroup) architecture.

E)Network topology: Computer networks may be classified according to the network topology upon which the network is based, such as Bus network, Star network, Ring network, Mesh network, Star-bus network, Tree or Hierarchical topology network,Network Topology signifies the way in which devices in the network see their logical relations to one another. The use of the term "logical" here is significant. That is, network topology is independent of the "physical" layout of the network. Even if networked computers are physically placed in a linear arrangement, if they are connected via a hub, the network has a Star topology, rather than a Bus Topology. In this regard the visual and operational characteristics of a network are distinct; the logical network topology is not necessarily the same as the physical layout.[3]

II.SYSTEM OVERVIEW

Types of networks:

Below is a list of the most common types of computer networks in order of scale.

a)Personal Area Network (PAN):
A personal area network (PAN) is a computer network used for communication among computer devices close to one person. Some examples of devices that are used in a PAN are printers, fax machines, telephones, PDAs and scanners. The reach of a PAN is typically about 20-30 feet (approximately 6-9 meters), but this is expected to increase with technology improvements.Personal area networks may be wired with computer buses such as USB and FireWire. A wireless personal area network (WPAN) can also be made possible with network technologies such as IrDA and Bluetooth.

b) Local Area Network (LAN):
This is a network covering a small geographic area, like a home, office, or building. Current LANs are most likely to be based on Ethernet technology. For example, a library may have a wired or wireless LAN for users to interconnect local devices (e.g., printers and servers) and to connect to the internet. On a wired LAN, PCs in the library are typically connected by category 5 (Cat5) cable, running the IEEE 802.3 protocol through a system of interconnected devices and eventually connect to the Internet. The cables to the servers are typically on Cat 5e enhanced cable, which will support IEEE 802.3 at 1 Gbit/s. A wireless LAN may exist using a different IEEE protocol, 802.11b, 802.11g or possibly 802.11n. The staff computers (bright green in the figure) can get to the color printer, checkout records, and the academic network and the Internet. All user computers can get to the Internet and the card catalog. Each workgroup can get to its local printer. Note that the printers are not accessible from outside their workgroup. Typical library network, in a branching tree topology and controlled access to resources[3].All interconnected devices must understand the network layer (layer 3), because they are handling multiple subnets (the different colors). Those inside the library, which have only 10/100 Mbit/s Ethernet connections to the user device and a Gigabit Ethernet

connection to the central router, could be called "layer 3 switches" because they only have Ethernet interfaces and must understand IP. It would be more correct to call them access routers, where the router at the top is a distribution router that connects to the Internet and academic networks' customer access routers.The defining characteristics of LANs, in contrast to WANs (wide area networks), include their higher data transfer rates, smaller geographic range, and lack of a need for leased telecommunication lines. Current Ethernet or other IEEE 802.3 LAN technologies operate at speeds up to 10 Gbit/s. This is the data transfer rate. IEEE has projects investigating the standardization of 100 Gbit/s, and possibly 40 Gbit/s.[3]

c) Campus Area Network (CAN):
This is a network that connects two or more LANs but that is limited to a specific and contiguous geographical area such as a college campus, industrial complex, office building, or a military base. A CAN may be considered a type of MAN (metropolitan area network), but is generally limited to a smaller area than a typical MAN. This term is most often used to discuss the implementation of networks for a contiguous area. This should not be confused with a Controller Area Network. A LAN connects network devices over a relatively short distance. A networked office building, school, or home usually contains a single LAN, though sometimes one building will contain a few small LANs (perhaps one per room), and occasionally a LAN will span a group of nearby buildings. In TCP/IP networking, a LAN is often but not always implemented as a single IP subnet.
d) Metropolitan Area Network (MAN):
A Metropolitan Area Network is a network that connects two or more Local Area Networks or Campus Area Networks together but does not extend beyond the boundaries of the immediate town/city. Routers, switches and hubs are connected to create a Metropolitan Area Network.

e) Wide Area Network (WAN)
A WAN is a data communications network that covers a relatively broad geographic area (i.e. one city to another and one country to another country) and that often uses transmission facilities provided by common carriers, such as telephone companies. WAN technologies generally function at the lower three layers of the OSI reference model: the physical layer, the data link layer, and the network layer.

f) Global Area Network (GAN)
Global Area networks (GAN) specifications are in development by several groups, and there is no common definition. In general, however, a GAN is a model for supporting mobile communications across an arbitrary number of wireless LANs, satellite coverage areas, etc. The key challenge in mobile communications is "handing off" the user communications from one local coverage area to the next. In IEEE Project 802, this involves a succession of terrestrial Wireless local area networks (WLAN).

Internetwork
Two or more networks or network segments connected using devices that operate at layer 3 (the 'network' layer) of the OSI Basic Reference Model, such as a router. Any interconnection among or between public, private, commercial, industrial, or governmental networks may also be defined as an internetwork.In modern practice, the interconnected networks use the Internet Protocol. There are at least three variants of internetwork, depending on who administers and who participates in them:

- Intranet
- Extranet
- Internet

Intranets and extranets may or may not have connections to the Internet. If connected to the Internet, the intranet or extranet is normally protected from being accessed from the Internet without proper authorization. The Internet is not considered to be a part of the intranet or extranet, although it may serve as a portal for access to portions of an extranet.

a) Intranet
An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer applications, that is under the control of a single administrative entity. That administrative entity closes the intranet to all but specific, authorized users. Most commonly, an intranet is the internal network of an organization. A large intranet will typically have at least one web server to provide users with organizational information.

b) Extranet
An extranet is a network or internetwork that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities (e.g. a company's customers may be given access to some part of its intranet creating in this way an extranet, while at the same time the customers may not be considered 'trusted' from a security standpoint). Technically, an extranet may also be categorized as a CAN, MAN, WAN, or other type of network, although, by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

c) Internet:

The Internet is a specific internetwork. It consists of a worldwide interconnection of governmental, academic, public, and private networks based upon the networking technologies of the Internet Protocol Suite. It is the successor of the Advanced Research Projects Agency Network (ARPANET) developed by DARPA of the U.S. Department of Defense. The Internet is also the communications backbone underlying the World Wide Web (WWW). The 'Internet' is most commonly spelled with a capital 'I' as a proper noun, for historical reasons and to distinguish it from other generic internetworks.[3]

Participants in the Internet use a diverse array of methods of several hundred documented, and often standardized, protocols compatible with the Internet Protocol Suite and an addressing system (IP Addresses) administered by the Internet Assigned Numbers Authority and address registries. Service providers and large enterprises exchange information about the reachability of their address spaces through the Border Gateway Protocol (BGP), forming a redundant worldwide mesh of transmission paths.

Basic Hardware Components

All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers. In addition, some method of connecting these building blocks is required, usually in the form of galvanic cable (most commonly Category 5 cable). Less common are microwave links (as in IEEE 802.11) or optical cable ("optical fiber").

Network Interface Cards:

A network card, network adapter or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses. It allows users to connect to each other either by using cables or wirelessly.

Repeaters:

A repeater is an electronic device that receives a signal and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair ethernet configurations, repeaters are required for cable runs longer than 100 meters away from the computer.

Hubs:

A hub contains multiple ports. When a packet arrives at one port, it is copied to all the ports of the hub for transmission. When the packets are copied, the destination address in the frame does not change to a broadcast address. It does this in a rudimentary way: It simply copies the data to all of the Nodes connected to the hub.

Bridges:

A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports. Once the bridge associates a port and an address, it will send traffic for that address only to that port. Bridges do send broadcasts to all ports except the one on which the broadcast was received.Bridges learn the association of ports and addresses by examining the source address of frames that it sees on various ports. Once a frame arrives through a port, its source address is stored and the bridge assumes that MAC address is associated with that port. The first time that a previously unknown destination address is seen, the bridge will forward the frame to all ports other than the one on which the frame arrived.

Bridges come in three basic types:

1. Local bridges: Directly connect local area networks (LANs)
2. Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced by routers.
3. Wireless bridges: Can be used to join LANs or connect remote stations to LANs.

Switches:

A switch is a device that performs switching. Specifically, it forwards and filters OSI layer 2 datagrams (chunk of data communication) between ports (connected cables) based on the MAC addresses in the packets. This is distinct from a hub in that it only forwards the datagrams to the ports involved in the communications rather than all ports connected. Strictly speaking, a switch is not capable of routing traffic based on IP address (layer 3) which is necessary for communicating between network segments or within a large or complex LAN. Some switches are capable of routing based on IP addresses but are still called switches as a marketing term. A switch normally has numerous ports, with the intention being that most or all of the network is connected directly to the switch, or another switch that is in turn connected to a switch.[3]

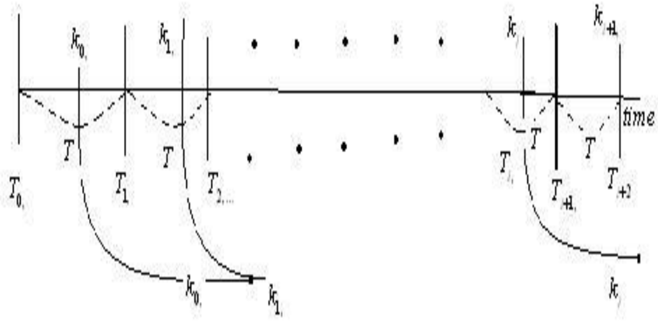
Switch is a marketing term that encompasses routers and bridges, as well as devices that may distribute traffic on load or by application content (e.g., a Web URL identifier). Switches may operate at one or more OSI model layers, including physical, data link, network, or transport (i.e., end-to-end). A device that operates simultaneously at more than one of these layers is called a multilayer switch.Overemphasizing the

ill-defined term "switch" often leads to confusion when first trying to understand networking. Many experienced
from key timenetwork designers and operators recommend starting with the logic of devices dealing with only one protocol level, not all of which are covered by OSI. Multilayer device selection is an advanced topic that may lead to selecting particular implementations, but multilayer switching is simply not a real-world design concept.

III.THE WORKING PRINCIPLE

1. **Time-Space Cryptography:**

This section presents our time-space cryptography to provide secure routing against malicious attacks that mobile ad-hoc networks might face. The proposed scheme is named in that it works in the time domain for key distribution between source and destination as well as in the space domain for intrusion detection along the route between them. Even if public key encryption is more powerful and superior in distributing keys, our scheme relies on symmetric key encryption because it is highly efficient and simple to implement.



Key Assignment And Disclosure

2. Secure Routing Protocol:

Mobile ad-hoc networks consist of mobile nodes (each node conceptually consisting of a router, a radio port and one or more host computers). To communicate with mobile nodes that are not within the transmission range, a routing protocol is required for each node. Recently, many routing protocols have been proposed for mobile ad-hoc networks. In general, they can be divided into two main categories: proactive and reactive protocols. In a proactive routing protocol, nodes periodically exchange routing information with other nodes to maintain all the routes on the network beforehand, while in a reactive approach each node attempts to discover a route on demand only when it has a packet to send. Although there is no single standard routing protocol yet for mobile ad-hoc networks, reactive routing protocols are known to perform better than proactive routing protocols in terms of lower overheads.

In most routing protocols, routers exchange information on the network topology in order to establish and maintain routes between nodes. Such routing information can be tampered by malicious adversaries who intend to bring the network down. They could be external attackers or compromised nodes inside. Certainly, actual data traffic should be also protected in this relay situation. Hence implementation of secure routing protocol is one of the key security areas in mobile ad-hoc networks. Normally, cryptographic schemes such as digital signature are used to protect both routing information and data traffic.

These schemes assume the use of key management by a central trusted entity called Certificate Authority (CA) or KDC (Key Distribution Center), which is responsible for key distribution to nodes and establishment of mutual trust relationships between nodes. Introducing any central entity into mobile ad-hoc networks is problematic. That is, if it is tampered, then the entire network can be easily compromised.

An ad-hoc network is a local area network or other small network, especially one with wireless or temporary plug-in connections, in which some of the network devices are part of the network only for the duration of a communications session or, in the case of mobile or portable devices, while in some close proximity to the rest of the network. In Latin, ad hoc literally means "for this," further meaning "for this purpose only," and thus usually temporary. The term has been applied to future office or home networks in which new devices can be quickly added, using, for example, the proposed Bluetooth technology in which devices communicate with the computer and perhaps other devices using wireless transmission. Each user has a unique network address that is immediately recognized as part of the network. The technology would also include remote users and hybrid wireless/wire connections.

3.Mobile ad-hoc network**:** A mobile ad-hoc network (MANET) is a kind of wireless ad-hoc network, and is a self-configuring network of mobile routers (and associated hosts) connected by wireless links – the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet.

Computer Network: A computer network is a group of interconnected computers. Networks may be classified according to a wide variety of characteristics. This article provides a general overview of some types and categories and presents the basic components of a network. A network is a collection of computers connected to each other. The network allows computers to communicate with each other and share resources and information.

Application

The decentralized nature of wireless ad hoc networks makes them suitable for a variety of applications where central nodes can't be relied on, and may improve the scalability of wireless ad hoc networks compared to wireless managed networks, though theoretica and practical limits to the overall capacity of such networks have been identified.Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of a dynamic and adaptive routing protocol will enable ad hoc networks to be formed quickly.Wireless ad hoc networks can be further classified by their application:

- mobile ad hoc networks (MANETs)
- wireless mesh networks
- wireless sensor networks.

An important part of wireless connectivity is mobility. Mobile computers must be able to move between adjacent cells or across multiple network domains without disturbing the application level process. Mobile users and mobile protocols must not make any changes to the existing TCP/IP Internet protocol to insure connectivity and usability of the Internet as it exists today.

A mobile host is the Internet Mobile Host Protocol (IMHP) entity that roams through the Internet. Each mobile host has a home agent on its home network. Each home agent maintains a list known as a home list. The home list is a list of mobile hosts that the home network will serve and it also maintains the location of each mobile host as the network becomes aware of their locations. As mobile hosts roam from one network to the next, they have to register with foreign agents on new subnets as they try to connect to that network.

Foreign agents are much like a home agent except they interact with visiting home agents from other networks. Each foreign agent maintains a list known as the visitor list, which identifies the mobile hosts that are currently registered with it. The combination of the foreign agents address for a particular home agent (care-of-address) along with its home address is known as a binding. A binding defines where to send packets for a particular home agent at any given time. [7]

0(bits) 8 24 31

type	reserved	Hop count
Time interval index		
Originator ip address		
Key value		

KDIS Packet format

IV.IMPLEMENTATION OF SYSTEM

A.Pseudo for Secure Single Hop:

```
public InputStream is;
public OutputStream os;
    public SocketConnection sc;
    public ServerSocketConnection scn;
     int isel = choiceGroup1.getSelectedIndex();
                    if(isel==0)
                {
                    Thread t = new Thread(this,"T1");
                    flag =1;
                    t.start();
                }
                     if(isel==1)
                {
                    getDisplay().setCurrent(get_SendForm());
                }
                if(isel==2)
                {
                getDisplay().setCurrent(get_ReceivePortForm());
                }
```

B.Pseudo for Secure Multiple Hop:

```
if(flag==1)
        {
            try
            {
                ServerCall sc = new ServerCall();
            String key =
sc.sendRequest("http://localhost:9090/CentralAuthority/Central
Auth?message="+textField1.getString());
            System.out.println(key);
            }
            catch (Exception ex)
            {
                ex.printStackTrace();
            }
        }
```

C.Pseudo for Security Analysis:

```
     scn =      (ServerSocketConnection)Connector.open
("socket://:"+t    extField7.getString());
            System.out.println(scn.toString());
```

ISSN : 2278 – 1021

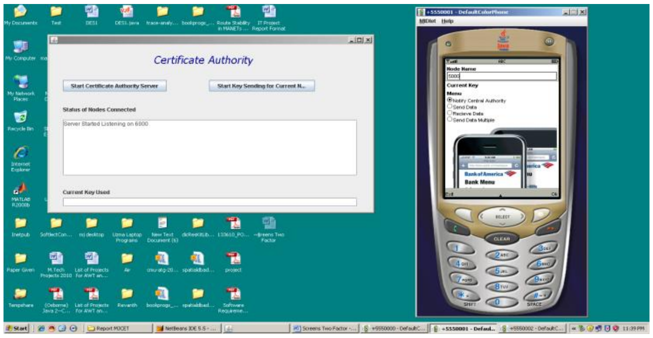
```
            System.out.println("Waiting for Connection ");
            sc = (SocketConnection)scn.acceptAndOpen();
            System.out.println("Connection Accepted ");
            is = sc.openInputStream();
            os = sc.openOutputStream();
            StringBuffer sb;
            String str = "";
            int c=0;
            while (((c = is.read()) != -1))
                str += (char)c;
            System.out.println("Hello");
            textField5.setString(str);
            DES d2 = new DES();
                        d2.initialize();
                        String plain = d2.decrypt(cipher);
String plain = d2.decrypt(str);
System.out.println(plain);
 textField6.setString(plain);
 System.out.println(str);
```

D.Pseudo for Reputation Mechanism:

```
Socket Connection sc1 =
(SocketConnection)Connector.open("socket://localhost:"+textF
ield3.getString());
            System.out.println("Connected ");
            InputStream is1 = sc1.openInputStream();
            OutputStream os1  = sc1.openOutputStream();
            DES d1 = new DES();
 d1.initialize();
String cipher = d1.encrypt(textField4.getString());
System.out.println(cipher);
          os1.write(d1.hexcipher.getBytes());
            os1.flush();
            os1.close();
            sc1.close();
```

V.EXPERIMENTAL RESULTS

The concept of this paper is implemented and different results are shown below.



Certificate Authority

Start Certificate Authority Server | Start Key Sending for Current N...

Status of Nodes Connected

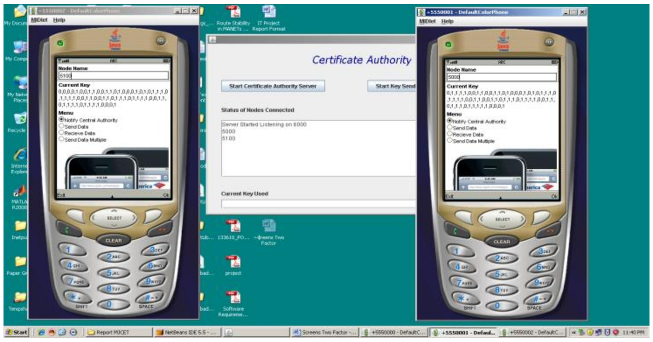
Server Started Listening on 6000

Current Key Used

Node Name: 5000

Current Key

Menu
● Notify Central Authority
○ Send Data
○ Recieve Data
○ Send Data Multiple



Certificate Authority

Start Certificate Authority Server | Start Key Send

Status of Nodes Connected

Server Started Listening on 6000
5000
5100

Current Key Used

Node Name: 5100

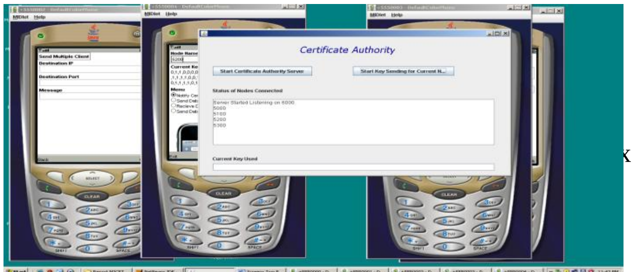
Current Key
0,0,0,0,1,0,0,1,1,0,0,1,1,0,1,0,0,0,1,0,1,0,1,1,1,0,1,1,1,1,0,0,1,1,0,0,1,1,0,1,1,1,0,1,1,1,1,0,0,1,1,0,1,1,1,1,0,1,1,1,1,1,0,0,0,1

Menu
● Notify Central Authority
○ Send Data
○ Recieve Data
○ Send Data Multiple

Node Name: 5000

Current Key
0,1,1,1,1,0,0,1,1,0,0,1,1,0,1,0,0,0,1,0,1,0,1,1,1,0,1,1,1,1,0,0,1,1,0,0,1,1,0,1,1,1,0,1,1,1,1,0,0,1,1,0,1,1,1,1,0,1,1,1,1,1,0,0,0,1

Menu
● Notify Central Authority
○ Send Data
○ Recieve Data
○ Send Data Multiple



Certificate Authority

Start Certificate Authority Server | Start Key Sending for Current N...

Status of Nodes Connected

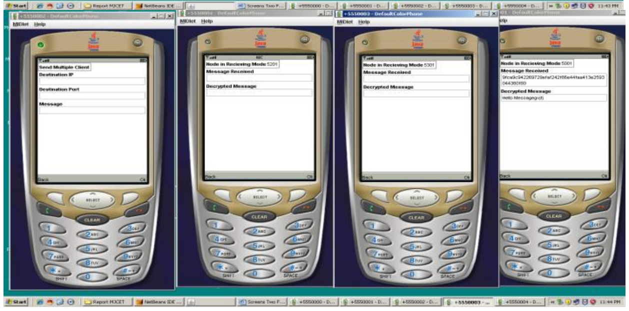
Server Started Listening on 6000
5000
5100
5200
5300

Current Key Used

Send Multiple Client
Destination IP
Destination Port
Message

Node Name: 5200

xcipher);



Send Multiple Client
Destination IP
Destination Port
Message

Node in Recieving Mode 5201
Message Received
Decrypted Message

Node in Recieving Mode 5301
Message Received
Decrypted Message

Node in Recieving Mode 5001
Message Received
9fca9c94226972efaf242f66e44faa413e2593044380f80
Decrypted Message
Hello Messagegvdj

5. Performance Analysis

The proposed paper is implemented in Java and J2ME technology on a Pentium-III PC with 20 GB hard-disk and 256

MB RAM. The propose paper's concepts shows efficient results and has been efficiently tested on different systems.

VI.CONCLUSION

In this paper we implemented the design and performance of a secure routing protocol with time-space cryptography for mobile ad-hoc networks. The key idea in the proposed time-space scheme is that it works in the time domain for key distribution between source and destination as well as in the space domain for intrusion detection along the route between them. Our secure routing protocol is based on routing to provide security for mobile ad-hoc networks using the time-space cryptography. For data authentication, the symmetric key encryption is used due to its high efficiency and a secret key is distributed using a time difference from the source to the destination.

VII. FUTURE ENHANCEMENTS

In this paper we implemented the design and performance of a secure routing protocol with time-space cryptography for mobile ad-hoc networks. The key idea in the proposed time-space scheme is that it works in the time domain for key distribution between source and destination as well as in the space domain for intrusion detection along the route between them. Our secure routing protocol is based on routing to provide security for mobile ad-hoc networks using the time-space cryptography. For data authentication, the symmetric key encryption is used due to its high efficiency and a secret key is distributed using a time difference from the source to the destination.

REFERENCES

[1] Y. Hu, A. Perrig, and D.B. Johnson, *"Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,"* Proceedings of ACM MobiCom, pp. 12-23, September 2002.
[2] H. Krawczyk, M. Bellare, and R. Canetti, "*HMAC: Keyed-Hashing for Message Authentication*," IETF RFC 2104, February 1997.
[3] L. Zhou and Z.J. Haas, "*Securing Ad Hoc Networks*," IEEE Network Magazine, Vol. 13, No. 6, pp. 24-30, November/December 1999.
[4] A. Perrig, R. Canetti, J.D. Tygar, and D. Song, "*The TESLA Broadcast Authentication Protocol,"* Cryptobytes, Vol. 5, No. 2, pp. 2-13, Summer/Fall 2002
[5] Y. Hu, D.B. Johnson, A. Perrig, "*SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks*," Proceedings of IEEE Workshop on Mobile Computing Systems & Applications, pp. 3-13, June 2002.
[6] S. Lee and C. Toh, "*A Simulation Study of Table- Driven and On-Demand Routing Protocols for Mobile Ad Hoc Networks*," IEEE Network Magazine, Vol. 13, No. 4, pp. 48-54, July/August 1999.
[7] C. Perkins, E. Belding-Royer, and S. Das, "*Ad Hoc On-Demand Distance Vector (AODV) Routing*," IETF RFC 3561, July 2003.
[8] I. Joe, "*SCTP with an Improved Cookie Mechanism for Mobile Ad-Hoc Networks*,"
Proceedings of IEEE GLOBECOM, December 2003.

Biography

Mr.K.Ramakrishna, Graduated in Information Technology and Engineering from kakatiya University, Warangal, Andhra Pradesh, India , 2007,and is M.Tech In Software Engineering from Jawaharalal Nehru Technological University Hyderabad,A.P,India in 2010.He Is Working presently as Assistant Professor In Department of Computer Science And Engineering In Holy Marynstitute Of Technologyand Science(HITS),R.R.District ,A.P,INDIA.He has 3 Years experience, His Research Interests Include Mobile Computing And Networking.

Mr M.Srinivasa Rao Post Graduated in Computer Applications (MCA) From Acharya **Nagarjuna University, 2005 and post graduated in** Computer Science & Engineering (M.TECH) From JNTU Hyderabad, 2012. He is working presently as Asst.Professor in Department of Computer Science & Engineering in HOLY MARY INSTITUTE OF TECHNOLOGY & SCIENCE (HITS), R.R.Dist, and A.P, INDIA. His research interests include Data Warehousing & Data Mining and Cloud Computing.

Y.Rokesh kumar,B.Tech(CSE)from AVS College of engineering,&technology, and is M.Tech In Software Engineering from Jawaharalal Nehru Technological University Hyderabad,A.P,India in 2010.He Is Working presently as Assistant Professor In Department of Computer Science And engineering, in AVS college of engineering & technology,

Rakesh.U, B.Tech(CSIT) in SKTRM college of engineering,JNTUH, and is M.Tech In Software Engineering from Jawaharalal Nehru Technological University Hyderabad,A.P,India in 2010.He Is Working presently as Assistant Professor In Department of Computer Science And Engineering In MurthyInstituteOfTechnologyandScience,R.R.District ,A.P,INDIA.He has 2 Years experience