ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

Accomplished Self-Curative Key Dispersion in Mobile Ad-hoc Networks

M.Venkata rao[1], P.Sriknth[2], M.Srinivasa Rao[3], Ramakrishna[4]

Assistant Professor, Department of CSE, Holy Mary Institute of Technology & Science, Hyderabad, India[1,2,3,4]

ABSTRACT - **This Paper is to extract the underlying concepts Self-CURATIVE key DISPERSION schemes are particularly useful when there is no network infrastructure or such infrastructure has been destroyed. A self-CURATIVE mechanism can allow group users to recover lost session keys and is therefore quite suitable for establishing group keys over an unreliable network, especially for infrastructure less wireless networks, where broadcast messages loss may occur frequently In this project, we will propose an ACCOMPLISHED self-CURATIVE key DISPERSION scheme with sponsorization capability. The main contribution of this project is highlighted by the following properties: The distance between two broadcasts which are used to recover the lost one can be set according to the underlying wireless networks. Working in this way facilitates a shorter length of the broadcast messages. More users of the group can sponsor a new user to join the group for subsequent sessions without any interaction with the group manager. The storage overhead of personal keys at each group user is a polynomial, which will not increase with the number of sessions. This project presents an analysis of security and efficiency. Findings performed here suggest that the proposed scheme outperforms other self-CURATIVE key DISPERSION schemes in term of the length of broadcasts, sponsorization, and storage overhead.This proposed project is implemented using the Java Microedition package which has the ability to code for the mobile devices. We also use the Sun java wireless toolkit to simulate the running of the project before deploying in the real world environment.**

Keywords: Cryptography, concept factorization, WN : Wireless Network, HC: Hash Chain,QC: Quantum Cryptography, GM : Group Manager, K : Key,UML: Unified Modelling Language, J2ME: Java Micro Edition, key-agreement protocol.

I.INTRODUCTION

An ACCOMPLISHED threshold self-CURATIVE key DISPERSION scheme with favorable properties is proposed in this project. Firstly, the distance between two broadcasts used to recover the lost one is alterable according to network conditions. This alterable property can be used to shorten the length of the broadcast messages. Secondly, any more than threshold-value users can sponsor a new user to join the group for the subsequent sessions without any interaction with the group manager. Thirdly, the storage overhead of the self CURATIVE key DISPERSION at each group user is a polynomial over a finite field, which will not increase with the number of sessions. In addition, if a smaller group of users up to a threshold-value were revoked, the personal keys for non-revoked users can be reused.

Objective:

In this project, we will propose an ACCOMPLISHED self-CURATIVE key DISPERSION scheme with sponsorization capability. The main contribution of this project is highlighted by the following properties: The distance between two broadcasts which are used to recover the lost one can be set according to the underlying wireless networks. Working in this way facilitates a shorter length of the broadcast messages. More users of the group can sponsor a new user to join the group for subsequent sessions without any interaction with the group manager. The storage overhead of personal keys at each group user is a polynomial, which will not increase with the number of sessions

Limitations of Project:

An infrastructure less network offers a means of addressing the needs for a more flexible, durable and cost ACCOMPLISHED network system than conventional centralized hierarchical fixed infrastructure systems does. Infrastructure less wireless networks, especially mobile wireless ad hoc networks, are ideal candidates for communications in applications such as rescue missions, scientific explorations and even military operations. These potential applications highlight concerns regarding security issues. Theoretically, all key DISPERSION schemes developed for reliable networks can be used in wireless networks with minor alternation. However, mobility changes the topology of networks frequently. Due to mobility of nodes, traditional security models designed for fixed-network topologies may not be fully applicable in infrastructure less

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

wireless networks. To better design an ACCOMPLISHED and secure key DISPERSION scheme, the designers should consider many factors such as application requirements, network topologies, and packet loss characteristics of the underlying wireless networks.

II.SYSTEM OVERVIEW

Existing System

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.

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.

Mobile ad-hoc networks became a popular subject for research as laptops and 802.11/Wi-Fi wireless networking became widespread in the mid to late 1990s. Many of the academic papers evaluate protocols and abilities assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other, and usually with nodes sending data at a constant rate. Different protocols are then evaluated based on the packet drop rate, the overhead introduced by the routing protocol, and other measures.

Peer networking involves the passing of messages between computing systems that operate as "peers." When a message is posted to a peer network, the message is propagated through the peer network by the peers. Computers operating as peers within the peer network are sometimes referred to as "nodes." In a typical peer networking configuration, at least some of the nodes operate as both a client and a server. For example, a node acts as a client when it receives a message from another node. That same node also acts as a server when it passes that message to another node. In this way, messages are communicated within the peer network.

Peer networks are sometimes constrained from communication outside of a particular group, location, company, or domain. This restriction operates as a boundary to peer network communication, such that a message posted on the peer network will not be delivered to a node separated from the peer network by the boundary. Moreover, if two peer networks are separated by a boundary, a message sent on one peer network is not delivered to the other network.

Diffie–Hellman key exchange (D–H) is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Although Diffie–Hellman key agreement itself is an anonymous (non-authenticated) key-agreement protocol, it provides the basis for a variety of authenticated protocols, and is used to provide perfect forward secrecy in Transport Layer Security's ephemeral modes.

Diffie–Hellman establishes a shared secret that can be used for secret communications by exchanging data over a public network.

An Intrusion Detection System (IDS) is a defense system, which detects malicious activities in a network. One feature of intrusion detection systems is their ability to detect or provide a view of malicious activities and issues by notifying or block a assumed connection. IDS tools are capable of distinguishing between attacks coming from own employees or customers and attacks posed by hackers. An intrusion Detection Systems has its core element a sensor (an analysis engine) that is responsible for detecting intrusions. It has decision making mechanisms is called sensor that receive raw data from knowledge base, system log and audit trail sources. The role of sensor is to filter information and discard any irrelevant data obtained from the event set associated with the protected system. Intrusion detection systems can be arranged as centralized or distributed. A distributed IDS consists of multiple Intrusion Detection Systems (IDS) over a large network, which communicate with each other. This survey report discusses the security issues at cluster based security management. In node level security management each node is responsible for securing itself. MANET routing protocols can be divided into proactive and imprudent categories. Both proactive and reactive protocols can suffer from control packet floods caused by malicious nodes.

Mobile Ah-hoc Networks (MANETs) are networks that are made of mobile and power controlled nodes infrastructure less self organizing, all the nodes share the same functions with respect to the network operation, (i.e. there is no node that is in charge for authentication or security services). It is vulnerable to security attacks due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring, management point, and lack of

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

a clear line of defense.Wireless Mesh Networks (WMN) is slightly more delicate. It exploits the nodes redundancy of nodes and the self-organizing network prototype to overcome some problems that are inherent to wireless networks (tradeoff between distance and transfer rates) or to networks in general (congestion, configuration and installation costs). Applying the above definition of WMN, you may find that both MANETs and WMN are "self-organizing", but you could also argue that MANETs can be seen as a subset of WMN. The most interesting application of WMN, tough is probably the use of wireless nodes (either mobile or fixed) to convey traffic from mobile users that have a wireless device to the wired internet.

A Wireless Sensor Network (WSN) consists of distributed autonomous devices using sensors to cooperatively scrutinize physical or environmental circumstances, such as high temperature, echo, shuddering, pressure, motion or pollutants, at different locations. They were originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and locale monitoring, healthcare applications, home computerization, and traffic management.

There are mainly two approaches to securing a MANET: proactive and reactive. The proactive approach attempts to prevent security threats in the first place, typically through various cryptographic techniques. The reactive approach seeks to detect threats a posteriori and react accordingly. Both approaches have own merits and is suitable for addressing different issues in MANET. For example, most secure routing protocols adopt the proactive approach in order to secure routing messages exchanged between mobile nodes, while the reactive approach is widely used to protect packet forwarding operations. Due to the absence of a clear line of defense, a complete security solution for MANETs should integrate both proactive and reactive approaches, and encompass all three components: prevention, detection, and reaction. The prevention component deters the attacker by significantly increasing the difficulty of penetrating the system. Ad hoc wireless internet extends the service of the internet to the end users over an ad hoc wireless network; some of the applications of the ad hoc internet ate wireless mesh networks.

In Sensor networks security manage by a centralized control called base stations. A base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface. They can be used as a nexus to disseminate control information into the network or extract data from it. The sensor nodes establish a routing forest, with a base station at the root of every tree. Base stations are many orders of magnitude more powerful than sensor nodes. Typically, base stations have enough battery power to surpass the lifetime of all sensor nodes, sufficient memory to store cryptographic keys, stronger processors, and means for communicating with outside networks.

No matter how carefully the prevention mechanisms are designed a completely intrusion-free system is infeasible. In MANETs, detecting and reacting components that discover the irregular intrusions and take reactions to avoid persistent adverse effects are indispensable for the security solutions are called Intrusion Detection Systems (IDS). They explore issues associated with deviations from normal system or user behavior which are concerned with the detection of hostile actions.

To classify the intrusion detection systems there is a family of tools that use information derived from a single host based IDS (HIDS) and those IDSs that exploit information obtained from a whole segment of a local network (network based IDS). The HIDS reside on a particular computer and provide protection for a specific system. They are not only equipped with system monitoring facilities but also include other modules of a typical IDS. Two primary types of HIDS can be distinguished:

a. Real Secure Agent, and Port Sentry System monitors incoming connection attempts. These examine host-based incoming and outgoing network connections. These are particularly related to the unauthorized connection attempts to TCP or UDP ports and can also detect incoming port scans.

b. Systems which examine network traffic (packets) that attempts to access the host. These systems protect the host by intercepting suspicious packets and looking for aberrant payloads.

Security attacks decreases highly available communication processes during detecting faults and intrusion in mobile ad hoc networks. LITON (Lightweight Intrusion-Tolerant Overlay Network) architecture [12] aims at providing highly available communication in spite of faults and intrusions in the mobile ad hoc network. It is the first overlay network that is able to tolerate intrusions that shows how routing schemes originally developed for mobile ad hoc networks (MANETs) can be used in overlay networks, and introducing a smart route caching strategy that allows for quick recovery when faults are detected. In LITON Lightweight Intrusion-Tolerant Overlay Network every overlay node is an Internet host residing in an autonomous system (AS). Autonomous systems may be connected via public or private (not globally advertised) links. Overlay node placement is arbitrary; however, since LITON is explicitly designed to overcome limitations of Internet inter-domain routing, spreading nodes across different ASs may significantly improve network availability.

MANETs are typically dynamic peer networks (DPNs). The specific security requirements of DPNs (in particular, key management) are still considered to be open research challenges. Recently, several key agreement protocols for DPNs were proposed. In the key agreement protocols were obtained by extending the well-known Diffie–Hellman (DH)

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

key exchange scheme to groups of n parties. In two key agreement protocols were proposed based on the threshold cryptography using the Lagrange interpolation theorem. A hierarchical structure is adapted by many key management schemes. The basic rekeying algorithm of a hierarchical structure divides the key management domain into smaller administrative groups. In addition, public key infrastructure (PKI), secure multicast, and logical tree-based algorithms are adapted by intra-group rekeying systems. Mobility impacts performance only when members cross groups. For instance, when two partners provide broadcast services for users in two overlapping groups, users moving within each group are managed by their local group key distributors (GKDs) and without any coordination between their broadcasts. On the other hand, when a user crosses from one group to another, security should be transferred between partners. The proposed a scheme called CLIQUES, which applies a key agreement rather than a key tree. CLIQUES is a logical linear structure which passes key information sequentially. The last group member will obtain the information of all the nodes. The proposed a safe communication scheme for MANETs. This communication is based on cluster structure and applies in wireless infrastructure. In this construction, the transmission range of nodes is 1-hop and one node with the largest weight value to be selected as multicast router (MR). The multicast router is a center to build the group. After group construction, MR will generate group key for encryption and decryption during data transmission. According to this scheme, we can manage keys ACCOMPLISHEDly and reduce the amount of rekeying.

Disadvantage of Existing System:

An infrastructure less network offers a means of addressing the needs for a more flexible, durable and cost ACCOMPLISHED network system than conventional centralized hierarchical fixed infrastructure systems does. Infrastructure less wireless networks, especially mobile wireless ad hoc networks, are ideal candidates for communications in applications such as rescue missions, scientific explorations and even military operations. These potential applications highlight concerns regarding security issues. Theoretically, all key DISPERSION schemes developed for reliable networks can be used in wireless networks with minor alternation. However, mobility changes the topology of networks frequently. Due to mobility of nodes, traditional security models designed for fixed-network topologies may not be fully applicable in infrastructure less wireless networks. To better design an ACCOMPLISHED and secure key DISPERSION scheme, the designers should consider many factors such as application requirements, network topologies, and packet loss characteristics of the underlying wireless networks.

Proposed System

In this project, we will propose an ACCOMPLISHED self-CURATIVE key DISPERSION scheme with sponsorization capability. The main contribution of this project is highlighted by the following properties: The distance between two broadcasts which are used to recover the lost one can be set according to the underlying wireless networks. Working in this way facilitates a shorter length of the broadcast messages. More users of the group can sponsor a new user to join the group for subsequent sessions without any interaction with the group manager. The storage overhead of personal keys at each group user is a polynomial, which will not increase with the number of sessions. This project presents an analysis of security and efficiency. Findings performed here suggest that the proposed scheme outperforms other self-CURATIVE key DISPERSION schemes in term of the length of broadcasts, sponsorization, and storage overhead.

III.THE WORKING PRINCIPLE

Wireless Mesh Networks (WMN) is slightly more delicate. It exploits the nodes redundancy of nodes and the self-organizing network prototype to overcome some problems that are inherent to wireless networks (tradeoff between distance and transfer rates) or to networks in general (congestion, configuration and installation costs). Applying the above definition of WMN, you may find that both MANETs and WMN are "self-organizing", but you could also argue that MANETs can be seen as a subset of WMN. The most interesting application of WMN, tough is probably the use of wireless nodes (either mobile or fixed) to convey traffic from mobile users that have a wireless device to the wired internet.

A Wireless Sensor Network (WSN) consists of distributed autonomous devices using sensors to cooperatively scrutinize physical or environmental circumstances, such as high temperature, echo, shuddering, pressure, motion or pollutants, at different locations. They were originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and locale monitoring, healthcare applications, home computerization, and traffic management.

There are mainly two approaches to securing a MANET: proactive and reactive. The proactive approach attempts to prevent security threats in the first place, typically through various cryptographic techniques. The reactive approach seeks to detect threats a posteriori and react accordingly. Both approaches have own merits and is suitable for addressing different issues in MANET. For example, most secure routing protocols adopt the proactive approach in order to secure routing messages exchanged between mobile nodes, while the reactive approach is widely used to protect packet forwarding operations. Due to the absence of a clear line of defense, a complete security solution for MANETs should integrate both proactive and reactive approaches, and encompass all three

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

components: prevention, detection, and reaction. The prevention component deters the attacker by significantly increasing the difficulty of penetrating the system. Ad hoc wireless internet extends the service of the internet to the end users over an ad hoc wireless network; some of the applications of the ad hoc internet ate wireless mesh networks.

In Sensor networks security manage by a centralized control called base stations. A base station is typically a gateway to another network, a powerful data processing or storage center, or an access point for human interface. They can be used as a nexus to disseminate control information into the network or extract data from it. The sensor nodes establish a routing forest, with a base station at the root of every tree. Base stations are many orders of magnitude more powerful than sensor nodes. Typically, base stations have enough battery power to surpass the lifetime of all sensor nodes, sufficient memory to store cryptographic keys, stronger processors, and means for communicating with outside networks.

No matter how carefully the prevention mechanisms are designed a completely intrusion-free system is infeasible. In MANETs, detecting and reacting components that discover the irregular intrusions and take reactions to avoid persistent adverse effects are indispensable for the security solutions are called Intrusion Detection Systems (IDS). They explore issues associated with deviations from normal system or user behavior which are concerned with the detection of hostile actions.

To classify the intrusion detection systems there is a family of tools that use information derived from a single host based IDS (HIDS) and those IDSs that exploit information obtained from a whole segment of a local network (network based IDS). The HIDS reside on a particular computer and provide protection for a specific system. They are not only equipped with system monitoring facilities but also include other modules of a typical IDS. Two primary types of HIDS can be distinguished:

a. Real Secure Agent, and Port Sentry System monitors incoming connection attempts. These examine host-based incoming and outgoing network connections. These are particularly related to the unauthorized connection attempts to TCP or UDP ports and can also detect incoming port scans.

b. Systems which examine network traffic (packets) that attempts to access the host. These systems protect the host by intercepting suspicious packets and looking for aberrant payloads.

c. Login Activity Monitoring Systems monitors the networking layer of their protected host (Host Sentry). Their role is to monitor log-in and log-out attempts, looking for unusual activity on a system occurring at unexpected times, particular network locations or detecting multiple login attempts. The network-based type of IDS (NIDS) produces data about local network usage. The NIDS reassemble and analyze all network packets that reach the network interface card operating in promiscuous mode.

In Mobile ad hoc network security attacks on routing information [1], exhausting nodes resources, maliciously manipulating data traffic is caused by lack of network infrastructure. AIS (Artificial Immune System) architecture protects and reacts against known and unknown dys-functions and attacks in a Mobile Ad Hoc Network. It is designed as two systems, primary IDS and secondary IDS. These components communicate across the network. The primary IDS are centralized and responsible the packager component was originally missing from selection. In order to adapt to new attacks, a process through which components of successful detectors are recombined using the evolutionary process to make new detectors. The secondary IDS are distributed and are responsible for data gathering, data reduction, detection, and response. It also forwards successful detections to the primary IDS. The architecture of AISANIDS contains two major components. The secondary IDS consist of four components, the sensors, the packager, the detector, and the response. The primary IDS consist of only an analysis component. The sensors collect audit information and convert it to a common event format. The packager performs data reduction by grouping the events into sessions. The analysis component uses these sessions to create detectors. The detector component matches current sessions to its detectors. Finally, the response component automatically responds to attacks. Ideally, once the secondary IDS had a set of detectors, it could continue to function even if the primary IDS failed. Further recommend combining both detection methods to maximize the effectiveness of IDS.

Real time intrusion in service oriented and user centric intrusion detection system [2] decreases ubiquitous computing for the user short term and long term behavior. SUIDS (Service-oriented and User-centric Intrusion Detection System) with Chi-Square Statistic Test increases ubiquitous computing for the user short term and long term behavior. In this way, the observation reflects the 'most recent past' characteristics of variables in an online fashion. Along with a chi-square statistic test, SUIDS (Service-oriented and User-centric Intrusion Detection System) can measure not only the mean and variance of variables, but also their probability attributions and occurrence patterns. It handles the heterogeneity issue of pervasive network by classifying network nodes into three major categories (head nodes, service nodes, and user nodes) and integrating intrusion detection with service specific knowledge. Security-related factors and subtle scenarios will be considered and tested regarding the system detection effectiveness. A resource-ACCOMPLISHED detection algorithm will be investigated to further improve the performance of SUIDS.

Poor connectivity and limited bandwidth makes network vulnerable to security attacks at node level communication in

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

mobile ad hoc networks. Mobile Agent Based Intrusion Detection System (MABIDS) [3] runs on each node intrusion detection system locally and equally cooperates with other intrusion detection systems running on other nodes. It derived from a MANET requirement analysis. The mobility and autonomy associated with MAs to provide an ACCOMPLISHED and flexible s olution to poor connectivity and limited bandwidth in M ANET context. In architecture of intrusion detection is based on collection and analysis of system and network audit data. Upon detection, intrusions report to security management. Architecture of MABIDS contains the System Administrator (SA) is in charge of harmonizing all the activities among the modules, such as Sensor management (SM), Event Manager (EM), Response Agent (RA), IDS Agents Framework, and PMADE. The sensor management is composed of Data classifier and Data formatting. Data classifier collects raw data from system audit and local route. The data that comes out of the Data classifier divided into three groups: system-level data, user-level data and packet- level data. Data formatting processes the group-data with the data formats rules of local IDS and outputs event data. Communication overhead can more reduce by dividing load into the IDS cluster nodes.

Lack of central authority in self organized mobile ad hoc network increases security threats. Self-organizing mechanism [4] manages security on node-level decreases security threats from mobile ad hoc networks attackers. It based on the assumptions where individual nodes are themselves responsible for their own security level. Self-organized mobile ad hoc network a node that is responsible for its own security should carry out. The management of security becomes easier if suitable metrics can be developed to offer evidence of the security level or performance of the network. Intrusion detection and prevention (IDS/IPS) techniques can be applied for this purpose. A security monitoring system continuously estimating the actual security level can be attached to the individual nodes of a self-organized mobile ad hoc network. Exploring component metric area and identify dependencies between them.

Due to lack of network central infrastructure and central authority for authentication malicious node attacks for authentication and authorization. It protects and reacts against known and unknown dys-functions or attacks in a mobile ad hoc networks [5]. It was designed as two systems, primary IDS and secondary IDS. These components communicate across the network. The primary IDS is centralized the packager components was originally missing from selection. The secondary IDS is responsible for data gathering, data reduction, detection and response. It also forward successful detection to primary IDS. The immune based system may miss some obvious attacks and raise alters when exposed to rare but permissible activities.

IV.IMPLEMENTATION OF SYSTEM

In this section of the documentation we describe the important part of the coding techniques which are being used in the proposed project. The complete code is not included in the report, only the sections which are most important and critical are included in this section of the report

A.Pseudo for Explanation of Key functions:

```
public QuantumA()
  {
        basixpublic = new char[2][2];
        basix = new char[17];
        dataArray = new int[17];
        statesArray = new char[17];
        basixpublic[0][0] = '-';
        basixpublic[0][0] = '|';
        basixpublic[0][0] = '\\';
        basixpublic[0][0] = '/';
        dataFinal = new int[17];
        dfi=0;
   }  public void generateBasix()
  {
     r1 = new Random();
        for(int i=1;i<=16;i++)
        {
        int ii = Math.abs(r1.nextInt()) %2;
              if(ii==0)
                    basix[i] = '*';
              if(ii==1)
                    basix[i] = '+';
        }
  }

 public void generatedataArray()
  {
     r2 = new Random();
        for(int i=1;i<=16;i++)
        {
              int ii = Math.abs(r2.nextInt())%2;
              dataArray[i] = ii;
        }  }
          public void generatestatesArray()
  {
        for(int i=1;i<=16;i++)
        {
if(basix[i]=='*' && dataArray[i] == 0)

        statesArray[i] = '\\';
```

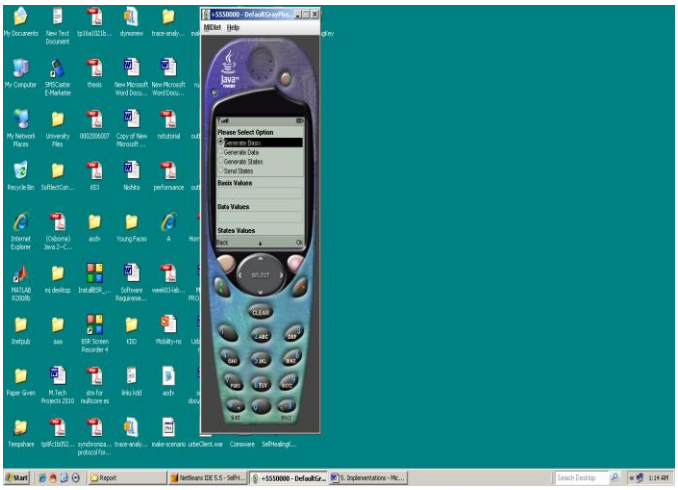
ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

```
                if(basix[i]=='*' && dataArray[i] ==
1)
                        statesArray[i] = '/';
                if(basix[i]=='+' && dataArray[i] ==
0)
                        statesArray[i] = '-';
                if(basix[i]=='+' && dataArray[i] ==
1)
                        statesArray[i] = '|';
  }

public String displayBasix()
  {
        String str="";
        for(int i=1;i<=16;i++)
        {
                str += basix[i];
                str += " ";
        }
        return str;
  }

public String displaydataArray()

  {
        String str="";
        for(int i=1;i<=16;i++)
        {
                str += dataArray[i];
                str +=" ";
        }

        return str;

  }

public String displaystatesArray()
  {
        String str="";
        for(int i=1;i<=16;i++)
        {
                str += statesArray[i];
                str += " ";
        }

        return str;

  }

}
```

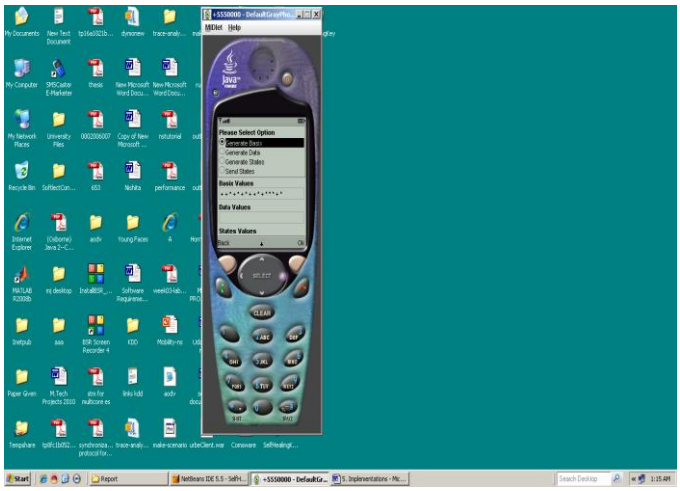
V.EXPERIMENTAL RESULTS

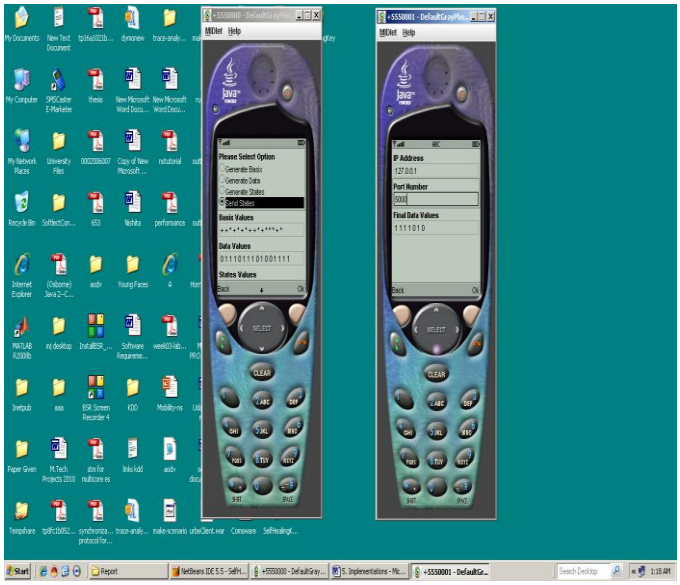
The concept of this paper is implemented and different results are shown below.



ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013





In this section of the documentation we have describe the important part of the coding techniques which are being used in the proposed project. The forms as well as the output screens are also provided which shows the communication between different form of the Mobile code.

VI.CONCLUSION

In this project a new self-CURATIVE key DISPERSION scheme. The proposed scheme has sponsorization capability and enables a large and dynamic group of users to establish a session key for secure communications over an unreliable wireless network. In order to shorten the length of broadcast messages, the distance between two broadcasts used to recover the lost one is adjustable in our scheme. The scheme also enables a user to recover, from a single broadcast message, T keys associated with the sessions in which she/he belongs to the group. The storage overhead of personal keys is a polynomial over Fp, which will not increase with the number of sessions. The proposed scheme has been comprehensively analyzed in an appropriate security model to prove that it is secure and self-CURATIVE and also achieves both forward security and backward security.

In terms of storage overhead, our scheme requires that each user stores a personal key of certain size in each session. In future work we can form the procedure of Setup and after receiving the session key DISPERSION broadcast. In the procedure of Setup, each user stores the initial session identifier and a polynomial as his personal key. After receiving the session key DISPERSION broadcast, each user stores the session identifier. Moreover, in future the maximum number of session's m is no longer needed to be determined in the procedure.

.

REFERENCES

[1] Y. Zhou and Y. Fang, "A two-layer key establishment scheme for wireless sensor networks," IEEE Trans. Mob. Comp., vol. 6, no. 9, pp. 1009-1020, Sept. 2007.

[2] W. Du, J. Deng, Y. Han, and P. Varshney, "A pairwise key preDISPERSION scheme for wireless sensor networks," in Proc. 10th ACM Conf. Computer Commun. Security CCS '03, 2003.

[3] J. Hwang and Y. Kim, "Revisiting random key pre-DISPERSION for sensor networks," in Proc. ACM Workshop Security Ad Hoc Sensor Networks (SASN '04), pp. 43-52, 2004.

[4] K. Hwang and C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," IEEE Trans. Wireless Commun., vol. 2, no. 2, pp. 400-407, Mar. 2003.

[5] J. Staddon, S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, "Self-CURATIVE key DISPERSION with revocation," in Proc. IEEE Symposium Security Privacy, pp. 224-240, 2002.

[6] D. Liu, P. Ning, and K. Sun, "ACCOMPLISHED self-CURATIVE key DISPERSION with revocation capability," in Proc. 10th ACM, 2003.

[7] C. Blundo, P. D'Arco, A. Santis, and M. Listo, "Design of self-CURATIVE key DISPERSION schemes," Design Codes Cryptography, no. 32, pp. 15- 44, 2004.

[8] G. Sáez, "On threshold self-CURATIVE key DISPERSION schemes," Cryptography
Coding, LNCS, vol. 3796, pp. 340-354, 2005.

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 2, February 2013

[9] R. Dutta and S. Mukhopadhyay, "Improved self-CURATIVE key DISPERSION with revocation in wireless sensor network," in Proc. Wireless Commun. Networking Conf., pp. 2963-2968, 2007.
[10] T. M. Cover and J. A. Thomas, "An ACCOMPLISHED key DISPERSION scheme with self-CURATIVE properties," IEEE Commun. Lett., vol. 9, pp. 759-761, 2005.
[11] M. J. Bohio and A. Miri, "Self-CURATIVE group key DISPERSION," International J. Network Security, vol. 1, no. 2, pp. 110-117, 2005.
[12] Y. Jiang, C. Lin, X. Shen, and M. Shi, "Mutual authentication and key exchange protocols for roaming services in wireless mobile networks," IEEE Trans. Wireless Commun., vol. 5, no. 9, pp. 2569-2577, Sept. 2006.

Biography

Mr.M.Venkata Rao B.Tech In ASR Engineering College-Tanuku, And Is M.Tech In Holy Mary Institute Of Technology & Science (Hits-Jntuh), R.R.Dist, A.P, India. He Is Working Presently As Assistant.Professor In Department Of Computer Science & Engineering In Holy Mary Institute Of Technology & Science (HITS). His Research Interests Include Mobile Networks And Information Security.

Mr.Punugoti Srikanth Is An Assistant Professor In Computer Science And Engineering At The Holy Mary Institute Of Technology And Science(HITS).He Received The Master Of Technology Degree In Information Technology From The Sathyabama University,Chennai In 2012.He Received The Bachelor Of Technology Degree In Information Technology Vaageswari College Of Engineering Applied To JNTU Niversity,Hyderbad In 2010. 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 Associate.Professor In Department Of Computer Science & Engineering In Holy Mary Institute Of Technology & Science (HITS), R.R.Dist, A.P, India. His Research Interests Include Data Warehousing & Data Mining And Cloud Computing.

Mr.K.Ramakrishna,Graduated Information Technology and Engineering From Kakatiya University, Warangal, Andhra Pradesh, India , 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 Holy Mary Institute Of Technology & Science (HITS),R.R.District ,A.P,India.He Has 3 Years Experience, His Research Interests Include Mobile Computing And Networking.