Asian Journal of Information Technology 15 (21): 4333-4354, 2016
ISSN: 1682-3915

Implementation of CDHT with ECDSA to Enhance Authentication and Secure Communication in Mobile Grid Environment

[1]H. Parveen Begam and [2]M.A. Maluk Mohamed
[1]Software System Group, M.A.M. College of Engineering, Tirchirappalli,
621105 Tamil Nadu, India
[2]Department of CSE, M.A.M. College of Engineering, Tirchirappalli
621105 Tamil Nadu, India

Abstract: Mobile grid is a class of distributed systems that autonomously engages sharing of resources and exchange of services to provide higher performance and utilization of the mobile device resources in a seamless, transparent, secure and efficient way. It allows sharing and co-ordinate use of diverse resources in dynamic, heterogeneous and distributed environment. Mobile grid focuses towards many issues like data management, resource management information management, power management and security management. Due to the combinationb of grid and mobile devices, it leads to many security issues like authentication, authorization, non-repudiation integrity, confidentiality and secure routing. Our main focus is to provide authentication and secure communication. In existing system, certificate authority is used for athrough digital certificates which is a trusted third party and has the responsibility of certificate generation and verification. If the CA is subverted, then the security of the entire system is lost. Normally RSA algorithm of 1024 bit key size is used which is computationally infeasible to perform the encryption which results in more power consumption and it is not suitable for mobile devices which are battery powered. In proposed system, a new architecture called Supervisory Host (SH) that helps in generating and distributing the Secure Service Certificates (SSC) is employed. Elliptic Curve Digital Signature Algorithm (ECDSA) of 168-bit, key size is used for generating digital signature which results in compact implementation and less heat generation. CHORD DHT (Distributed Hash Table) is used for secure and effective routing. Thus the combination of SH and ECDSA algorithm helps to improve the trust level in organizations.

Key words: Mobile grid computing, supervisory host, Secure Service Certificate (SSC), digital signature, ECDSA, CDHT

INTRODUCTION

Mobile grid: Grid computing can be defined as a set of parallel and distributed systems that enable the sharing of geographically distributed independent and heterogeneous resources like computers, software, etc., for effectively solving computationally intensive problems. Grid computing paradigm has become one of the most important techniques in the area of high performance computing. As the number of prospective users increases rapidly, the available resources can be supplemented with resources available from the mobile devices. Mobile computing is another computing paradigm of distributed systems, considering mobility, portability and wireless communications. The main motivation of combining the mobile and grid computing is to carry out the user's work while on the move. Due to various constraints with the wireless network, the environment and the user may rapidly change their environment from stationary to mobile and is location dependent. As the mobile devices in use are huge in number, even a small percentage of their resource utilization in a grid environment shall be highly advantageous and useful. Although, significant work is being done in the field of increasing the processing and power capabilities of mobile devices, its value is lesser than that of a wired device.

Mobile grid computing broadens the scope of grid computing by including a vast resource pool available in the form of mobile devices. As the number of mobile devices in use is bound to increase in coming years and with enhanced features, mobile grid computing will offer in the area of high performance computing. Mobile grid is a branch of grid where the infrastructure includes mobile

Corresponding Author: Parveen Begam, Software System Group, M.A.M. College of Engineering, Tirchirappalli, 621105 Tamil Nadu, India

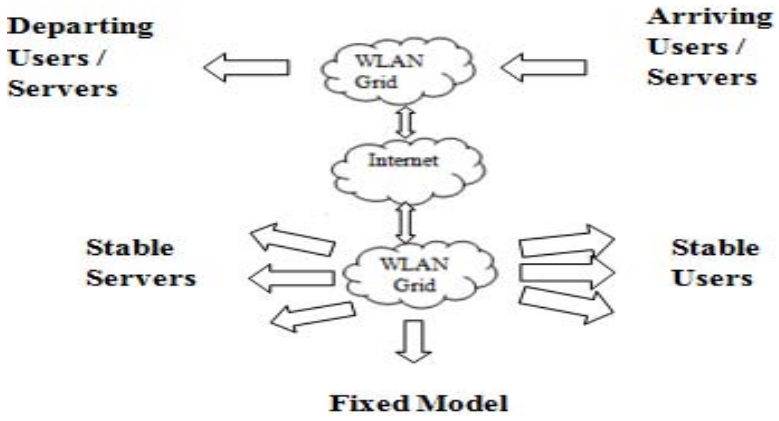

Fig.1: Mbileg grid

devices. The mobility of devices is not supported in most of the grids that are in operation today. This problem might seem trivial but with millions of mobile devices running today and their processing power remaining unutilized to the maximum, it seems a good idea to include these in the existing family of grids. Apart from utilizing resources on the mobile devices, the mobile grid can provide mobile devices with an opportunity to use the resources on the grid, there by saving their own resources considerably and overcoming the physical shortcoming of the device.

Mobile devices having access to the grid as users would thus be able to perform certain tasks on the run which otherwise would have been done only when the user could access a wired device. Certain situations could allow the mobile devices to contribute to the grid resource warehouse. The main factors that hinder the growth of this paradigm as compared to the grid computing paradigm are the issues related to mobility and the constraints of mobile computing are that mobile devices are poor in available resources as compared to wired systems; Mobile devices are more prone to security breaches; mobile connectivity is highly variable in performance and reliability; mobile devices rely on a finite energy source.

Figure 1 shows the model of mobile grid and provides a new technology for solving complex and compute intensive problems in mobile or nomadic environments. WLAN grid consists of stable servers and it also gets connected with the stable users to provide the better performance.

The following are the devices predominant in the grid and relative mobility of the service in the grid into four types:

- Fixed wireless grids
- Mobile or dynamic wireless grids
- Sensor network grids
- Ad hoc grids

Fixed wireless grids extend grid resources to wireless devices that are usually static. This type of grid has no difference with traditional wired grid except the communication medium is wireless. Mobile or dynamic wireless grids make services accessible through mobile devices such as PDA and smart phones. It is based on a wireless network in which each cell consists of a number of mobile devices. Mobile devices residing in a cell of wireless networks are coordinated by a central entity that resides at the access point/Base Station (BS) in order to perform a task. Mobile devices can be used as both resource consumers and resource providers.

Sensor network grid integrates wireless sensor networks and traditional grid computing technologies. These are formed from tiny devices that are generally dedicated to a single purpose. Based on wireless sensor network infrastructure, sensor grid adopts the technologies of data grids, computing grids and access grids to storing, processing, presenting and sharing the data collected from the sensors.

Mobile grid solutions further extend the business opportunities. Already existing mobile health telematics applications like telemonitoring and teleconsultation can be combined and enriched by back-end services. Making existing data and computation intensive services available to mobile users is the second possibility. So the spectrum of applications becoming available is extended, particularly those orchestrating services and resources across organizations and domains. The field of mobile grid computing is growing quickly; there are still a large number of challenges that these devices face which remain open problems to be resolved.

It may appear that the unification of mobile wireless consumer devices with high-performance grid computing might not be that simple. A mobile grid has the following issues:

- Data management
- Resource management
- Information management
- Power management
- Security management

The focus is on security and power management. The combination of mobile and grid may lead to a lot of security issues like authentication of the mobile node and mobile code, prevention of attacks in the base station, secure communication between two mobile nodes, communication cost of constructing the session keys and computing the complexity of authenticity and security. And as focused on mobile devices, the battery power is considered as the main factor.

As authentication is the main factor, Certificate Authority (CA) is used which is a trusted third party and by using CA the certificates are generated and there are also some issues which is mainly used for certificate generation and verification. To overcome the issues of CA the proposed system fully focused on Supervisory Host (SH) which is a static node which resides within the Mobile Support Station (MSS) and it coordinates the resources present within their own cluster. It communicates with the neighboring Supervisory Host (SH) in a peer-to-peer fashion. It is mainly used for certificate generation and verification in the proposed system. The SH model is used to have efficient security and power management for mobile grid systems.

Certificate authority: In cryptography, a transaction requires digital certificates which are issued by an independent trusted third party (the CA) to authenticate that transaction. A Certificate Authority (CA) is a trusted entity that issues electronic documents that verify a digital entity's identity on the internet. The electronic documents which are called digital certificates, are an essential part of secure communication and play an important part in the Public Key Infrastructure (PKI). ACA issues digital certificates that contain a public key and the identity of the owner. The matching private key is not made available publicly but kept secret by the end user who generated the key pair. The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person organization, server or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials so that users and relying parties can trust the information in the CA's certificates. CAs uses a variety of standards and tests to do so. In essence, the certificate authority is responsible for saying "yes, this person is who they say they are and the CA, certify the person.

Issues in certificate authority: The digital certificates are used in many applications especially in banking and other legal binding process; they have got financial and technological drawbacks.

- Service subscription is one of the main issues in Certificate authority. That is it requires monthly payments to continue the relationship which is a financial disadvantage
- It is most cost effective for the use of multiple certificates for different sites. Technological disadvantages like creating a platform that accepts all digital certificates is a difficult undertaking and human carelessness may compromise the safety of login credentials
- If the CA is subverted, then the security of the entire system is lost; resulting in a security breach of the entities that trust the compromised CA
- It is cost and time effective to maintain CA in two or more levels for authentication. Moreover, CA is a third party, so most of the business organizations, corporate, colleges and governments that use applications expect more security but doesn't like to depend on a third party
- Purchasing the certificate is an easier process but the quality matters. So if use the cheapest issuer, so quality is not being paid for in the competing market.
- Certification authorities deny almost all warranties to the user
- To limit the time, the expiration date should be used as the key strength.

Distributed certificate authority: 1A DCA is realized through the distribution of the CA's private key to a number of shareholding DCA nodes. However, the public key of the DCA will be known by all network's nodes and will be used to verify signatures of certificates issued by the DCA. When operations such as issuing or revoking certificates are required, a threshold of available shareholding DCA nodes should participate. It shows that although distribution increases reliability and availability, it decreases the security of the system. One of the main components of PKI infrastructure is a Certificate Authority (CA) it is a trusted third party used for issuing, revoking and managing of user certificates.

Unfortunately, the CA itself can be attacked and finally compromised in this case, the intruder can sign certificates using the CAs private key. In partially implemented DCA (PDCA), services of the CA are distributed to a set of specialized server nodes using secret sharing. Each of these nodes can generate partial certificates and a client can create a valid certificate by combining enough number of these partial certificates the special server nodes must have high energy and the heterogeneity of the nodes in the network is utilized to choose the candidates for CA nodes. However, if all the nodes in MANET re identical, the nodes of the distributed CA might be chosen randomly.

In Fully implemented DCA (FDCA) services of a CA are distributed to all nodes and using secret sharing, each of these nodes can generate partial certificates. FDCA reduces the communication delay and improves the availability because almost all the neighbors of a requesting node hold shares of the DCA's private signature key. However, it allows attackers to break the system more easily and when an intruder enters the network and compromises one or more nodes he becomes as good as a valid one. Based on their functions and their operational needs of the networks each type have different DCA proposals based on the above-mentioned DCA schemes which are classified mainly with regard to either PDCA or FDCA.

Literature review: In the existing resaerch, there are many studies that focus on the certificate authority to provide secured data transmission. There are also papers that deal with the digital signature and certificate generation by using various algorithms and papers based on smart grids and cluster based networks which help to develop a new model of supervisory host.

Alcaraz and Lopez (2014) proposed "WASAM; a dynamic wide-Area situational awareness model for critical domains in smart grids" in which this is the case of the smart grid and its domains which should be monitored through intelligent and dynamic mechanisms able to anticipate, detect and respond before disruptions arise within the system. Given this fact and its importance for social welfare and the economy, a model for wide-area situational awareness is proposed. These services include global and local support for prevention through a simple forecast scheme, detection of anomalies in the observation tasks, response to incidents, tests of accuracy and maintenance, as well as recovery of states and control in crisis situations.

Chaddoud and Martin (2006) proposed, "distributed certificate authority scheme with weighted secret sharing for mobile Ad-hoc Networks" (Li *et al*., 2008) and in this node authentication is an essential security service in Mobile Ad-hoc Networks (MANETs). To provide node authentication, they constructed a distributed certificate authority in MANETs. In this study, to solve the number of neighbor node problem in Fully Distributed Certificate Authority (FDCA) schemes, they proposed a distributed certificate authority scheme with weighted secret sharing. Each node share weight with current node degree information. Node's share weight has to be adjusted due to the mobility of nodes. Although, many DCA schemes were proposed but there still exists unsolved problems. to solve the number of neighbor node problem, they proposed a weighted threshold signature scheme using bivariate polynomial and apply it to the DCA scheme. In the weighted threshold signature scheme, each participant has his/her own share weight and a subset of participants can create a signature if the sum of their share weights is greater than or equal to the threshold. They analyzed the security of DCA scheme.

Abidi *et al.* (2014) proposed" implementation of Elliptic Curve Digital Signature Algorithm (ECDSA)" and in this architecture to implement the ECDSA in FPGAs circuit has been proposed. This architecture is planned to reach high performance running in FPGAs circuit. A digital signature or digital signature scheme is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender and that it was not altered in transit digital signature schemes can be used to provide the following basic cryptographic services: data integrity, authentication, non-repudiation. In cryptography, elliptic curves are used for asymmetric operations, such as key exchange over an insecure channel or asymmetric encryption. Consequently, it is considered that ECC provides an equivalent security level as EIGamal or RSA with much shorter keys. However that the estimates vary a little depending on the source. A security levels is achieved when they estimate that solving the instance will require more that 2n operations. Some benefits of having smaller key size include faster computation time and reduction in processing power and storage space. This makes ECDSA ideal for constrained environments such as pagers, PDAs, cellular phones and smart cards.

Hayouni and Hamdi (2015) proposed), "Energy Efficient Key menagement scheme for clustered hierarchical wireless sensor networks. In this they proposed a novel authentication protocol and secure key management scheme using elliptic curve cryptographic and diffie-hellman algorithm, conforms to the security requirements of mobile heterogeneous sensor networks. It provides a secure channel, between different

communication nodes, as a solution to improve the protection of WSNs. For this they proposed a dynamic method of preload of sensors which make sure that the deployed nodes initialize themselves and a key agreement protocol which make two nodes to establish a secure pair wise key. Security analysis and performance evaluation showed that the solution ensures an enhanced security level by reducing the communication overhead and energy consumption..

Woungang *et al.* (2015) proposed "MR-chord: mproved chord lookup performance in structured mobile P2P networks" (Woungang *et al.*, 2015). Peer-to-peer (P2P) is a distributed application architecture that partitions tasks or workloads between peers. MR-Chord used to maintain and update the finger table using a modified distributed hash table-based protocol. The lookup hop count generated by MR-chord is higher compared with that generated by the original chord. MR-Chord was designed to maintain and update the finger table using a modified distributed hash table-based protocol, so that the necessary lookup services in the network are provided. MR-Chord outperforms the original chord protocol in terms of lookup success rate, overlay consistency, lookup delay time, lookup hot count and total network load, chosen as performance metrics.

Muthukuru and Sathyanarayana (2013) proposed "A secure elliptic curve digital signature approach without inversion". The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). Elliptic curve based digital signatures are stronger and ideal for constrained environments like smart cards due to smaller bit size, thereby reducing processing overhead. Considering the security of data it is lacking regarding random number choosing or determination. This lacking leads to recovery of the private key in original elliptic curve digital signature scheme. There are three popular public-key algorithms which can provide digital signatures:

- Elliptic Curve Digital Signature Algorithm (ECDSA)
- RSA scheme
- ElGamal signature scheme

Among these ECDSA provides a faster alternative for public-key cryptography, much smaller key lengths are required to provide the desired level of security elliptic curve based digital signatures are stronger and ideal for constrained environments like smart cards due to smaller bit size, thereby reducing processing overhead.

ECDSA was implemented over Elliptic Curve (EC) P-192 and P-256 using VTM, FTM and TBM encryption methods and compared their performance. They also implemented ECDSA for various domain parameters, after observing the results when the key size increases then complexity increases and performance decreased. After comparing VTM, FTM and TBM based ECDSA methods, ECDSA using variable text message encryption is better when comparing with fixed length text message and text based encryption used ECDSA. The main reason is the speed of scalar multiplication which plays an important role in the efficiency of the whole system. In VTM based ECDSA method, the number of scalar multiplications are reduced, so this method is efficient when compared with FTM and TBM based methods.

Murthy *et al.* (2011) proposed "an elliptic curve based signature method to control fake research based certificates" (Sivagurunathan and Prathapchandran, 2014). Information confidentiality, authentication and integrity are desirable features for electronic transactions and these features are achieved by using a proper combination of symmetric and asymmetric cryptographic techniques. In order to ensure information authenticity, digital signatures are the equivalent part for normal signatures. It is well known that with the help of digital signature, forgery of digital information can be identified and it is widely used in e-commerce and banking applications. In this paper, a method is proposed that utilizes the combination of hashing and signing techniques to control fake university degree certificates. As the objective is strong signatures that occupy minimal space on the certificate, Elliptic curve digital signatures are considered for the proposed scheme. In this, the major disadvantage is that SHA-1 can be exploited by attackers to generate and install a fake certificate.

Li *et al.* (2008) explained" An Authenticated Encryption Mechanism for Secure Group Communication in Grid" . In grid computing, group communication is an important strategy to realize large-scale information resource sharing. They presented four algorithms including keys generating individual signature generating and verifying, group signature generating and encrypting, decrypting and group signature verifying which constitute the authenticated encryption mechanism for group communication in grid.

Johnson *et al.* (2001) proposed, "The elliptic curve digital signature algorithm". Unlike the ordinary discrete logarithm problem and the integer factorization problem, no sub exponential-time algorithm is known for the elliptic curve discrete logarithm problem. For this reason, the strength-per-key-bit is substantially greater in an algorithm that uses elliptic curves. This study describes the ANSI X9.62 ECDSA and discusses related security, implementation and interoperability issues.

Litke1 proposed "Mobile grid computing: changes and challenges of resource management in İobile grid environment". In this study, they This study provides a discussion on mobile grid definition, the basic motivation and benefits that can stem from this new technology, especially as far as it concerns collaborative engineering industry and the everyday life of the "mobile" citizen. In the sequel it presents a set of major technical topics that influence the traditionally basic Grid infrastructure services under the new grid environment involving mobile grids.

Burkhard Stiller proposed "Regulatory issues for mobile grid computing". Regulatory issues for communications and value-added services determine a key requirement of study to ensure that a competitive and fair commercial usage within a legal domain can be achieved. Therefore, this study pursues a comprehensive study identifying the key mobile grid regulations on a european level, while such grid services are considered to be of major importance for upcoming value-added services. The focus is put mainly on those regulatory determinations affecting areas neglected by the communications framework, namely the areas of value-added services in mobile grids and of determinations governing relations among service providers and between service consumers and service providers.

Bichhawat and Joshi (2010) "A Survey on Issues in mobile grid computing". Mobile grid computing broadens the scope of grid computing by including a vast resource pool available in the form of mobile devices. As the number of mobile devices in use is bound to increase in coming years and with enhanced features, mobile grid computing will have a lot to offer in the area of high performance computing. This study surveys the paradigm of mobile grid computing and the features it offers in the current computing environment and also discussed the role of mobile devices in the existing grid technology. We also discuss the various challenges the paradigm faces as a result of inclusion of the feature of mobility in the grid computing environment.

Chaddoud and Martin (2006) proposed, "Distributed certificate authority in cluster-based Ad hoc networks". They proposed a distributed certificate authority intended for deployment in an NTDR cluster-based architecture and also outlined the procedures for maintaining this distributed certificate authority amongst a highly dynamic membership of shareholding nodes.

Mohamed, proposed" ASAMO: Authentication and Secure communication using abstract monitoring objects for mobile grid computing". They discussed about a framework of dynamic secure routing protocol called Select Successive Hop Routing (SSHR) algorithm using Abstract Monitoring Objects (AMOs) Secure Service Certificates (SSC) and layer based encryption for each data transfers to improve the security level, anonymity and dynamicity of the data are proposed. This includes authentication of the mobile node security flow between mobile nodes saving battery power hand-over of authentication information. The proposed framework solves the issues like asymmetry in network connectivity, computing power and mobility.

Muthukuru and Sathyanarayana (2013) proposed, "Implementation of elliptic curve digital signature algorithm using variable text based message encryption" (Muthukuru and Sathyanarayana, 2013). Digital Signatures are considered as digital counterparts to handwritten signatures and they are the basis for validating the authenticity of a connection. It is well known that with the help of digital signature, forgery of digital information can be identified and it is widely used in e-commerce and banking applications. Elliptic Curve Digital Signatures (ECDSA) are stronger and ideal for constrained environments like smart cards due to smaller bit size, there by reducing processing overhead. They implemented ECDSA over Elliptic Curve (EC) P-192 and P-256 using various text message encryptions which are Variable size Text Message (VTM), Fixed size Text Message (FTM) and Text Based Message (TBM) encryption methods and compared their performance.

Mathur *et al.* (2015) proposed" solving security Issues in mobile computing using cryptography techniques-A survey "(Murthy *et al.*, 2015). They discussed about the security problems arising from the technological advances in mobile computing as well as their solution. Using cryptographic techniques information can be provided adequate security, over the air. Encryption of data takes place using symmetric or asymmetric cryptography algorithms depending on the area of application and level of security required. The paper presents a comparative survey on AES, DES, IDEA, RC2, BLOWFISH, RSA encrypting algorithms with their advantages and disadvantages over different parameters. Sivagurunathan and Prathapchandran (2014) proposed" Trust and cluster based authentication schemes in mobile ad hoc networks-A Review". Mobile Ad Hoc Network (MANET) is a distinct kind of network where the nodes are connected by way of wireless medium and without any infrastructure. Nodes in the network are fully dependent on other nodes so as to complete the mission successfully. In addition to this, nodes are moving freely and make dynamic topology. Moreover these types of networks can be easily constructed whenever and wherever required. It offers plenty of applications; it also

has its own weaknesses that are disturbing the network from a security perspective. In order to do the data transmission successfully, each node should trust other while forwarding node that is ensuring authentication with which it is communicating by the way of cooperating with each other. But achieving such cooperation in this distinct environment is too difficult. Moreover scalability is one of the considerable issues because number of nodes in the MANET can increase dramatically. Clustering is an idea to provide the scalability to the MANET.

Parmar *et al.* (2013) proposed, "Mobile grid computing: Facts or fantasy". They analyzed the challenges for harvesting this potential for grid computing. The inherent limitations of typical mobile devices, such as reduced CPU performance, small secondary storage, heightened battery consumption sensitivity and unreliable low-bandwidth communication are outraced by number of smart-phones sold annually, suggesting that the concept should not be prematurely dismissed. Given the enormous benefits of mobile grid computing, solutions to compensate for the inherent limitations of these devices must be developed in order to successfully utilize them in the grid.

Xiong *et al.* (2015) proposed, "EMC3: energy-efficient data transfer in mobile crowd sensing under full coverage constraint". They proposed a novel Mobile Crowd Sensing (MCS) framework called EMC3 which intends to reduce energy consumption of individual user as well as all participants in data transfer caused by task assignment and data collection of MCS tasks, considering the user privacy issue, minimal number of task assignment requirement and sensing area coverage constraint. Specifically, EMC3 incorporates novel pace control and decision making mechanisms for task assignment, leveraging participants' current call and historical call records as well as predicted future calls and mobility in order to ensure the expected number of participants to return sensed results and fully cover the target area with the objective of assigning a minimal number of tasks.

Begam and Mohamed (2014) proposed" Adaptive certificate-based mutual authentication protocol for mobile grid infrastructure" (Mathur *et al.*, 2015). Digital certificates and signatures provide protection in legally binding situations. Even though the digital certificates are used in banking and other legal binding process, they have got their own drawbacks which could be financial or technical. Financial being subscription for the service and technical being creation of platform that could accept all digital certificates and human errors. If the CA is subverted, then the security of the entire system is lost; resulting in a security breach of the entities that trust the compromised CA. Maintenance of CA in two or more levels requires more cost and time for authentication. Moreover CA is a third party, so most of the business organizations, corporate, colleges and governments that use applications expect more security but doesn't like to depend on a third party. This study proposes a new concept called Supervisory Host (SH) which is a static node that takes care of certificate generation and distribution. The advantages of supervisory host are simple registration process, reduced level of key exchange process and improved authentication process between two parties. SH is maintained independently for any particular application, the trust level is high and authentication process can be improved with the help of ECDSA (Elliptic Curve Cryptography Digital Signature Algorithm) algorithm.

Lashkari *et al.* (2009) proposed "A survey on wireless security protocols (WEP, WPA and WPA2/802.11i)" (Saputro *et al.*, 2012). They explained the structure of WEP and WPA as first and second wireless security protocols and discussed all their versions, problems and improvements and also try to explain WPA2 versions, problems and enhancements that have done solve the WPA major weakness. Finally we make a comparison among WEP and WPA and WPA2 as all wireless security protocols in Wi-Fi technology.

Saputro *et al.* (2012) proposed "A survey of routing protocols for smart grid communications" (Parveen Begam and Maluk Mohamed). With the recent initiatives to upgrade the existing power grid to the Smart Grid (SG), there has been a significant interest in the design and development of an efficient communications infrastructure for connecting different components of the SG. In this study, they focused on the routing issues in the SG communications infrastructure which consists of different network components, such as Home Area Networks (HANs), Neighborhood Area Networks (NANs) and Wide Area Networks (WANs). They provide a comprehensive survey of the existing routing research and analyze the advantages and disadvantages of the proposed protocols with respect to different applications areas.

Stoica *et al.* (2001) proposed the paper based on "Chord: A scalable peer to peer lookup service for internet applications" (Stoica *et al.*, 2001). A fundamental problem that confronts peer-to-peer applications is to efficiently locate the node that stores a particular data item. Chord provides support for just one operation: given a key, it maps the key onto a node. Data location can be easily implemented on top of Chord by associating a key with each data item and storing the key/data item pair at the node to which the key maps. Chord adapts efficiently as nodes join and leave the system and can answer queries even if the system is continuously changing. Chord's performance was measured through simulation and

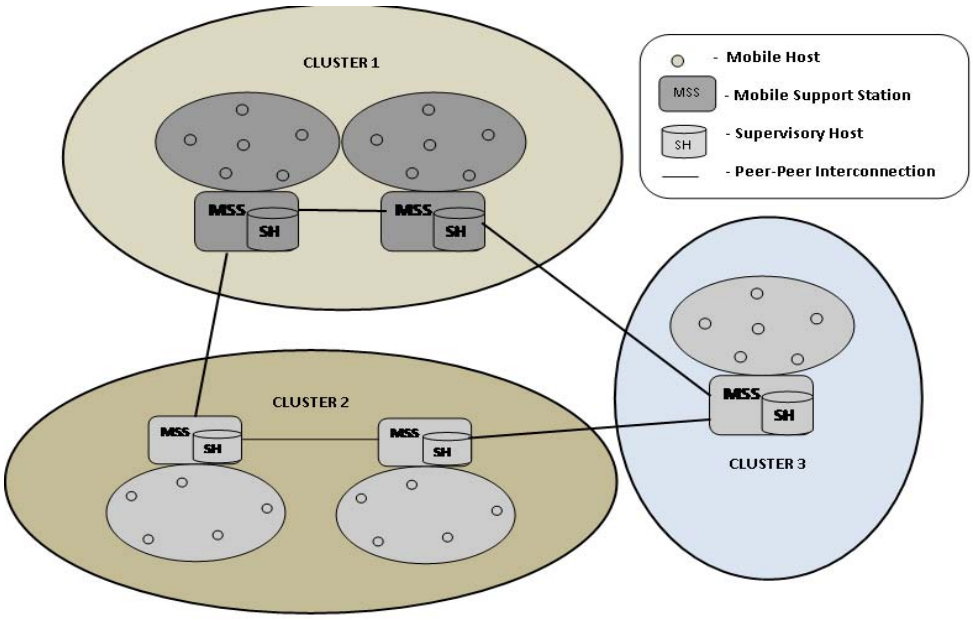

Fig. 2: Clustered mobile grid architecture with supervisory host

experimented and deployed. The chord software takes the form of a library to be linked with the client and server applications that use it.

Proposed work

Architectural view: The supervisory host model for mobile grid systems defines an architecture that helps in generating the Secure Service Certificates (SSC) and digital signatures for mobile hosts to have efficient security and power management. Some of the existing methods to generate digital signatures and certificates are symmetric or asymmetric algorithms, Identity based algorithms, biometric based algorithms. In the existing systems, mobile hosts depend on Certificate Authority (CA) for generation of certificates using various certificate generation methods. Issues arise when the CA becomes malicious and when it consumes more battery power.

The advantages of supervisory host are simple registration process, reduced level of key exchange process and improved authentication process between two parties. CA requires registration and shares challenges between the users. SH is maintained independently for any particular applications to achieve higher trust level. For this, a trusted model for each cluster is needed. Because of individual requirements and processing styles of each cluster, SH is very much useful for the authentication process, since the requirements and the processing styles of each cluster is different. The attacks are also reduced because the SH resides in the base station.

Figure 2 shows the mobile grid environment as a cluster of clusters. Each cluster can be viewed as a collection of MHs (mobile hosts) and SHs (Supervisory Hosts). The MHs are handled by the Mobile Support Station (MSS) of the traditional cellular system. Each cluster is coordinated with a designated static host called Supervisory Host (SH). The SH have so many responsibilities and they are briefly discussed below.

Figure 2 shows the cluster can be viewed as a collection of MHs (mobile hosts) and SHs (Supervisory Hosts). The MHs are handled by the Mobile Support Station (MSS) of the traditional cellular system. Each cluster is coordinated with a designated static host called Supervisory Host (SH). The focus is to balance between performance, power consumption and security because as use mobile devices it may increase the battery power consumption. In order to provide security and power management in mobile grid environment, the supervisory Host is used. SH is a new paradigm which mainly has the responsibility of managing all the resources and services within their cluster. The configuration of MSS and SH will vary based on the MSS load condition. Another important responsibility of SH is to coordinate the other neighboring SHs in a peer-to-peer fashion. The combination of SH and ECDSA algorithm helps to improve the trust level in organizations. The main advantages of Supervisory Host paradigm are simple

registration process, reduced level of key exchange process and improved authentication process between two parties.

Supervisory host: Supervisory host manages all the resources within their cluster. So it will have the main responsibility of handling mobile nodes and manages them in a better way. Coordinate the neighboring nodes in a peer to peer fashion that is supervisory host not only manage but also coordinate the nodes to perform the process in an organized manner. The main responsibility of SH is certificate generation. It generates the certificate with the help of ECDSA algorithm. The second important responsibility is to distribute the certificates. After generating and distributing the certificates the next step is to Store the Secure Service Certificate (SSC) in a repository which is useful to verify the certificates for future use.

Functions of supervisory host:

- Register with MSS-Mobile osts have to register with their corresponding Mobile Support Station present in their own cluster
- MSS assign Unique ID as MHID-The MSS assigns a unique ID to the registered mobile hosts.
- Pass that information to SH-The mobile host with the ID is passed to the SH which have the repository to store the data
- SH checks the information and stores in its database-The SH verifies the MH with ID and saves it in their database.
- Store the certificate in SH-for the respected MHID SH generates the certificate for the secure communication.

Certificate generation: In order to provide security and power management in mobile grid environment, proposed a new paradigm with the help of Secure Service Certificates (SSC) and Supervisory Host (SH). The Supervisory Host (SH) is used for faster Key generation and distribution when more number of mobile hosts is used simultaneously. After generating certificate, it stores it in a secure place so that no intruder can access and it can easily retrieve and distributes the certificate to the authenticated nodes for that reasons SH maintains repository. In proposed system mainly focused on authentication and power consumption so instead of RSA, Elliptic Curve Cryptography Digital Signature Algorithm (ECDSA) is used for signature generation and verification. By using ECDSA which have less key size compared to RSA, it can easily save the battery power and also it is very efficient in signature generation and verification.

In Existing models, Certificate Authority (CA) is used to generate public and private keys and takes the responsibility to provide authentication service to several service providers. Digital certificates are used for session key exchange. RSA is a public key authentication and it is used for encryption and authentication. The main responsibility of CA is to generate and maintains both public and private keys for each mobile node securely. There is another way of using DCA scheme which is based on clustering scheme. MANET nodes are classified into clients, repositories and server nodes. The client nodes are organized into clusters. In each cluster, they maintain the repository and for that node in that respective cluster are elected and they act as a repository for that respective cluster. In DCA, the jobs are distributed among all the nodes so it will become a major security issues in this scheme. The other common issues in CA and DCA are availability, scalability, Fault tolerance, user node mobility and etc. For these reasons SH is introduced which take care of all the responsibilities of CA and it plays an important role in certificate generation and distribution and it also contribute it service for repository too. The Proposed scheme which use ECDSA for certificate generation and the process is as follows.

Certificate generation process using ECDSA: In mobile grid systems, the SH is used for generating the certificates and digital signatures for mobile hosts to provide efficient security and power management. The existing methods use Symmetric or Asymmetric algorithms such as; Identity based algorithms, biometric-based algorithms to generate digital signatures and certificates. And in some other existing methods, the mobile host depends on Certificate Authority (CA) for generation of certificates using various certificate generation methods. The CA is trusted third party and it also has lot of issues. When the CA become malicious the entire system will lost and it also consumes more battery power. Our focus is to provide security and power management. This includes,

- Generation of certificates using ECDSA
- Repository of certificates in supervisory host

SH makes a copy of the SSC (Secure Service Certificate) and sends it to the corresponding mobile node. The Existing System of X.509 has some issues and it uses RSA algorithm which has the key size as 1024 bits. The computations of RSA are more complicated which increases computation time and it is not suitable for mobile devices which are battery powered. Figure 3 shows

Fig.3: Secure Service Certificate (SSC)

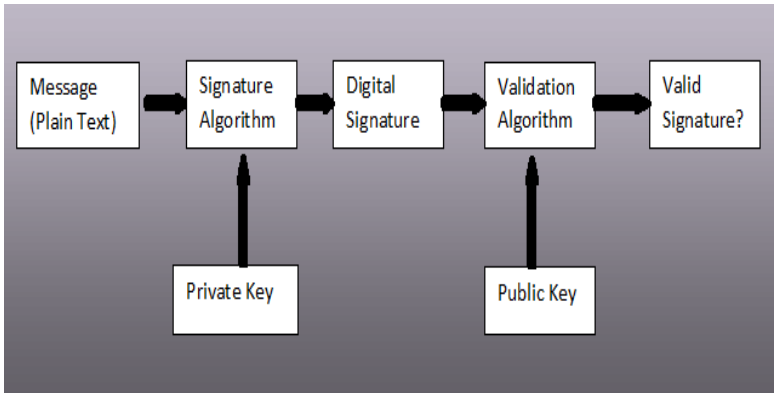

Fig. 4: Digital signature

the Secure Service Certificates (SSC) which consists of only necessary fields like certificate serial number, certificate identifier algorithm, issuer unique ID, Validity period, algorithm identifier, certificate signature algorithm and certificate signature.

For certificate generation, the mobile hthe necessary components to SH in an encrypted format the SH generates the certificate along with digital signature with the help of public key of sender and receiver. The SSC components: serial number, certificate identifier algorithm, issuer's unique ID, validity period, subject ID, subject public key, an algorithm identifier, TTL and Nonce. (Ids||TTL||Kpu(s)||IDd||N1) (Fig. 4).

- Certificate Identifier algorithm: to identify the encryption algorithm is used in which the certificate has been encrypted
- Issuer Unique ID: Identity of supervisory host
- Validity period: the time for which the certificate is valid
- Subject Unique ID: Identity of receiver
- Subject public key: Receiver's public key
- Algorithm Identifier: The type of algorithm where the data is encrypted

Elliptic curve digital signature algorithm: A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A Digital Signature Certificate (DSC) is a secure digital key that certifies the identity of the holder, issued by a Certifying Authority (CA). It typically contains user's identity (name, email, country, APNIC account name and your public key). Digital Certificates use Public key infrastructure meaning data that has been digitally signed or encrypted by a private key can only be decrypted by its corresponding public key. A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity).

The Elliptic Curve Digital Signature Algorithm (ECDSA) is the elliptic curve analogue of the Digital Signature Algorithm (DSA). It was accepted in 1999 as an ANSI standard and was accepted in 2000 as IEEE and NIST standards. It was also accepted in 1998 as an ISO standard and is under consideration for inclusion in some

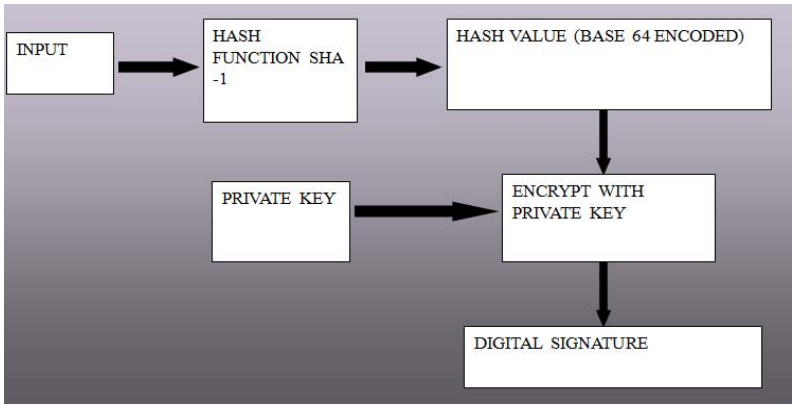

Fig. 5: Signature generation

other ISO standards. The ECDSA have the following features, a smaller key size which leads to faster computation time and reduction in processing power, storage space, bandwidth. This makes the ECDSA ideal for constrained devices such as pagers, cellular phones and smart cards.

The following are the some of the advantages of ECDSA. It provides greater security for a given key size. It provides effective and compact implementations for cryptographic operations requiring smaller chips. It produces less heat and consumes less power due to smaller chips. It is mostly suitable for machines having low bandwidth, low computing power, less memory. It has easier hardware implementations. There are 3 important Phases in ECDSA. They are as follows:

- Key pair generation
- Signature generation
- Signature verification

In ECDSA for key pair generation, domain parameters is needed which helps to generate the key pair. The domain parameters for ECDSA consists of a suitably chosen elliptic curve E defined over a finite field Fq of characteristic p and a base point G belongs to (Fq). Domain parameters may either be shared by a group of entities or specific to a single user. There are some restrictions which are placed on the followings for several reasons specifically for some specific attacks, Field size q and the representation used for the elements of Fq. The elliptic curve and the order of the base point.

Domain parameters of ECDSA

- A field size q, where q = p, an odd prime or q = 2 m
- An indication FR (field representation) of the representation used for the elements of Fq
- Two field elements a and b in Fq which define the equation of the elliptic curve E over Fq' (i.e., y2 = x3+ax+b in the case p>3 and y2+xy = x3+ax+b in the case p = 2)
- Two field elements xG and yG in Fq which define a finite point G = (xG, yG) of prime order in E (Fq)
- The order of the point G, with n>2^160 and n > 4vq and
- The cofactor h = #E (Fq)/n

Key pair generation: An entity A's key pair is associated with a particular set of EC domain parameters D= (q, FR, a, b, G, n, h).Each entity A does the following:

- Select a random integer d in the interval [1, n- 1]
- Compute Q = dP
- A's public key is Q, A's private key is d

Signature generation: To sign a message m, an entity A with domain parameters
D = (q, FR, a, b, G, n, h) and associated key pair(d,Q) does (Fig. 5):

- Select a random or pseudorandom integer k, [1<k<n-1]
- Compute KG = (x1, y1) and convert x1 to an integer x1
- Compute r = x1 mod n (where x1 is regarded as an integer between 0 and q-1). If r = 0 then go back to step 1

- Compute k^-1mod n
- Compute SHA-1(m) and convert this bit string to an integer e
- Compute s = k^-1 {e+ dr} mod n, If s = 0, then go back to step 1
- The signature for the message m is the pair of integers (r, s)

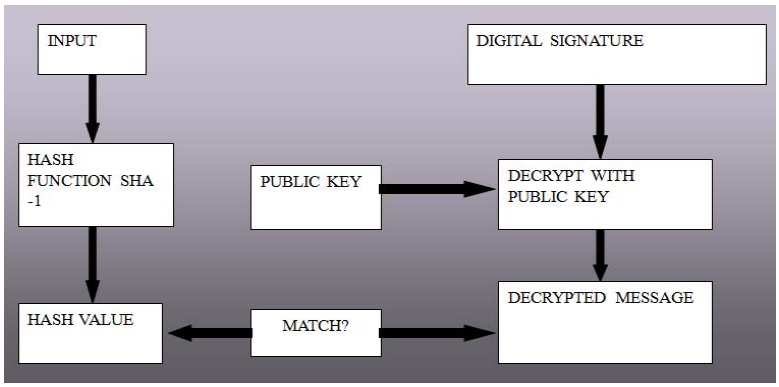

Fig. 6: Signature verification

Signature verification Verify A's signature (r, s) on m, B obtains an authenticated copy of A's domain parameters D = (q, FR, a, b, G, n, h) and associated public key Q and does the following: (Fig. 6).

- Verify that r and s are integers in the interval [1, n-1]
- Compute SHA-1(m) and convert this bit string to an integer e
- Compute w = s-1mod n
- Compute u1 = ew mod n and u2 = rw mod n
- Compute X = u1G+u2Q
- If X = O, then reject the signature. Otherwise convert the x-coordinate x1 of X to an integer x1 and compute v = x1 mod n
- Accept the signature if and only if v = r

If a signature (r,s) on a message m was indeed generated by A, then s = k-1 (e+dr) mod n. Rearranging gives,

k = s-1(e+dr) = s-1e+s-1rd = +wrd = u1+u2 d (mod n)

Thus:

u1G+u2Q = (u1+u2d) G = kG and v = r as required

Secure storage process of SSC: After generating the certificate, it is necessary to store the certificate in a secure place. The supervisory host acts as a repository and it stores the SSC from the mobile nodes. It helps to locate the data and also to maintain the security of the system. The repository of SSC is done by using the concept of a hash table.

Mobile host: It has hash table that contains key value, Location, Identifier. Supervisory host has hash table that is used for the purpose of, to automatically update whenever the mobile host enters or leaves from MSS (Mobile Support Station). Each cluster has a collection of mobile hosts and one SH is maintained for each cluster.

Hash functions transform the keys into numbers within a predetermined interval. These numbers are then used as indices in an array (table, hash table) to store the records (keys and pointers). If M is the size of the array, then the hash function h (key) can be computed in this way: h(key) = key% M. This will map all the keys into numbers within the interval [0, M-1]. If each character is represented with p bits, then the string can be treated as base-2 p number.

Once we have found the method of mapping keys to indexes, then we have to choose the size of the table (array) to store the records and we can perform the basic operations. Insert-use the hash function to generate an address for each value to be inserted. Search-for a key in the table: the same hash function is used. Delete-a record with a given key-

first we apply the search method and when the key is found we delete the record. The hash function maps keys into indices in a many-to-one fashion. Having a second key into a previously used slot is called a collision. Collision resolution deals with keys that are mapped to same addresses. There are various methods which help to reduce collision resolution. The Methods are as follows,

- Separate chaining
- Open addressing
- Linear probing
- Quadric probing
- Double hashing

Open addressing: If collision occurs, next probes are performed following the equation:

$$hi(x) = (hash(x) + f(i)) \bmod \text{table size}$$

Where:

hi(x) = An index in the table to insert x
hash(x) = The hash function
f(i) = The collision resolution function.
I = The current attempt to insert an element

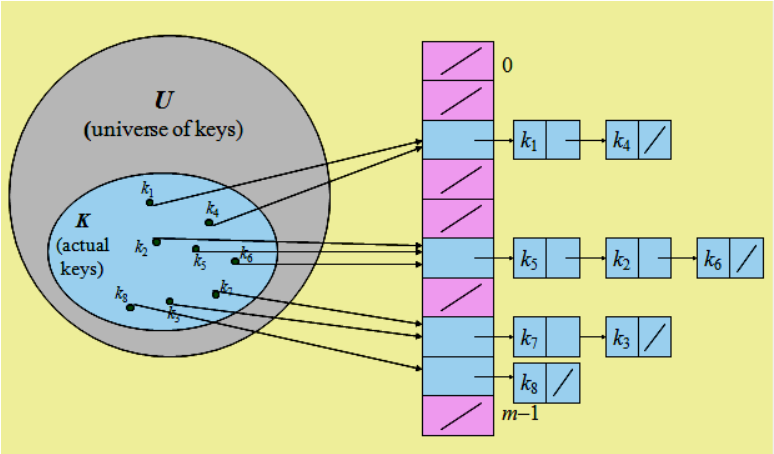

Fig. 7: Separate chaining

Separate chaining: Keys hashing to same address are kept in lists attached to that address. For each table address, a linked list of the records whose keys hash to that address is built. This method is useful for highly dynamic situations where the number of the search keys cannot be predicted in advance. The method is used in cases that we cannot predict the number of records in advance, thus the choice of M basically depends on other factors such as available memory.

M is chosen relatively small so as not to use up a large area of contiguous memory but enough large so that the lists are short for more efficient sequential search. Fig.7. shows the separate chaining process and in this. For each table address, a linked list of the records whose keys to that particular address, is built. This method is useful for highly dynamic situations where the number of the search keys cannot be predicted in advance. In this method of hashing, the lists should be maintained in order and it will be useful if there is much more searches than inserts. It represents the chains as binary search tree. Thus, it is easy to implement Fig. 7.

Authentication using Diffie-Hellmann (DH) key exchange algorithm: Figure 8 communication is the medium for sending and receiving the data between two parties i.e., sender and receiver. But the communication needs security. It's often required that a message be encrypted between two parties for secure communication. There are plenty of algorithms out there for encryption that are very secure but their weakness lies in transporting the encryption key. The diffie-hellmann key exchange protocol allows people to exchange keys in a manner that does not allow an eavesdropper to calculate the key in a fast manner. Diffie-hellmann algorithm is extremely simple in its idea and with it has a rather high level of cryptographic stability which is based on the supposed complexity of the discrete problem of taking the logarithm.

Mobile Grid Network (MGN_i) performs Diffie-Hellman process for authentication of the mobile nodes (MH_i) presents within the mobile grid network. The node from one grid wants to communicate with node in another grid it have to create the secret keys and shared between these two node which are present in separate grid is a difficult process. Consider, if the node (say MH_s) from one grid and wants to communicate with another node (MH_d) in other grid, the receiver have to verify that it is an authenticated mobile node. The process has the following steps Fig. 9 and Table 1.

- Mh_s (sender mobile node) which wants to communicate with MH_d (receiver node), first sends its identification information to Supervisory Host (SH)
- Supervisory Host (SH) will verify the information in the repository
- The communicating node exchanges their computed public keys to each other
- Then they start to compute the common shared secret key with the help of their own private keys
- After exchanging their common secret keys authentication will be ensured

Thus, the Diffie-Hellman key exchange method permits two parties that have no prior information of each other to establish a shared secret key over an insecure communications channel. Diffie-Hellman Key Exchange (DHKE) is one of the early public-key concepts. The diffie-hellmann protocol can be a powerful component for a security measure. The diffie-hellmann key exchange

```
HASH-INSERT (T, k)
i = 0
 repeat j --> h(k, i)
    if Y[j] = NIL
       then T[j] = k
         return j
       use i = i +1
  until i = m
error "table overflow"
\\Search
HASH-SEARCH (T, k)
i = 0
   repeat j --> h(k, i)
      if T[j] = k
         then return j
       i = i +1
   until T[j] = NIL or i = m
return NIL
```

Fig. 8: Algorithm for hash table entry

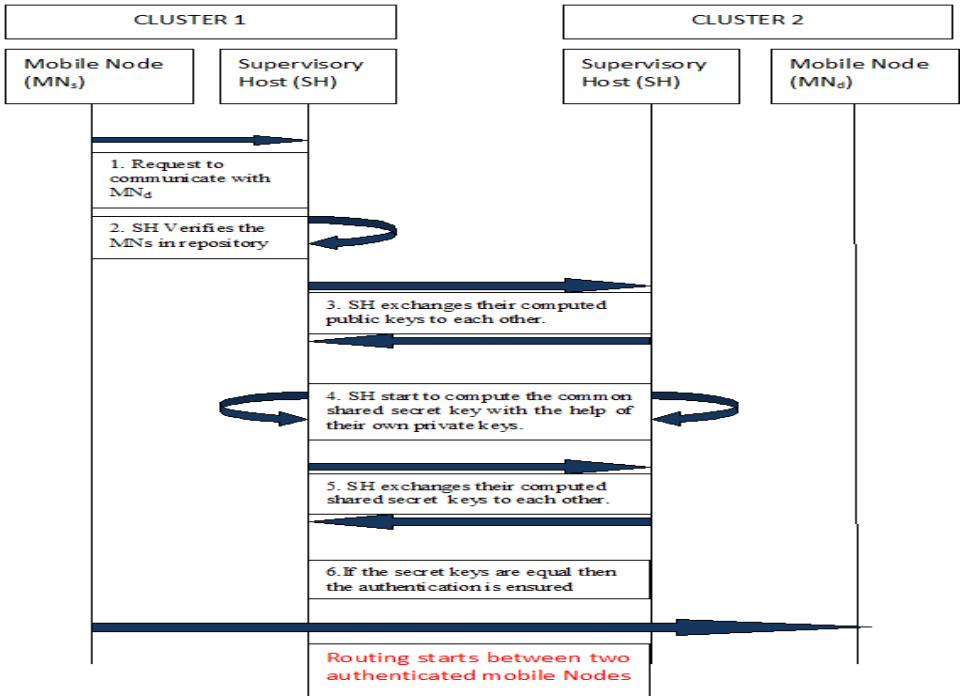

Fig. 9: Authentication process using supervisory host

Table 1: Results of CA and SH with tasks submitted based on capability of Mhs

CA Model				SH Model			
#MH	Send power (W)	Rec. Power (W)	Energy (kb sec^{-1})	Send power (W)	Rec. power (W)	energy (kb sec^{-1})	Lifetime (sec)
1	0.2	0.1	10.0	0.3	0.15	15.0	300.0
1	0.0	0.0	0.0	0.3	0.15	15.0	300.0
2	0.3	0.15	15.0	0.1	0.05	5.0	100.0
3	0.0	0.0	0.0	0.0	0.0	0.0	0.0
4	0.1	0.05	5.0	0.3	0.15	15.0	300.0
8	0.3	0.15	15.0	0.3	0.15	15.0	300.0
22	0.0	0.0	0.0	0.0	0.0	0.0	0.0
35	0.2	0.1	10.0	0.3	0.15	15.0	300.0
19	0.1	0.05	5.0	0.4	0.2	20.0	400.0

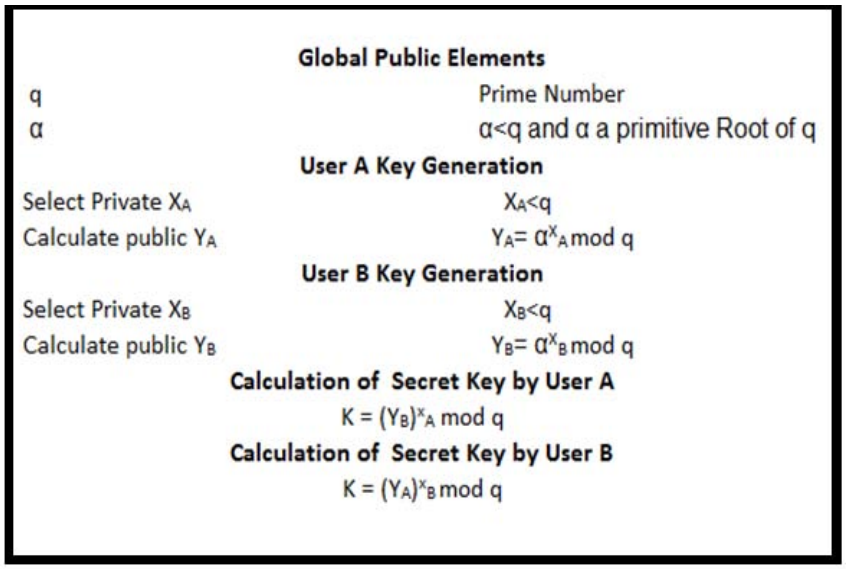

Fig. 10: Diffie-hellmann key exchange algorithm for any cluster

algorithm has proven to be one of the most interesting key distribution schemes in use today. It exploits arithmetical properties to produce a common computational result between two parties wishing to exchange information, however one must be aware of the fact that although the algorithm is safe against passive eavesdropping, it is not necessarily protected from active attacks (whereby an intruder impersonates one of the parties involved in the exchange). For this reason, the Diffie-Hellmann algorithm should be complemented with an authentication mechanism. Thus the diffie hellmann key exchange algorithm helps in mobile grid network for the secure communication between two mobile nodes in which one present in one cluster and the other node is in different cluster. For exchange, the supervisory host has to verify the authentication of the two mobile nodes and then only the communication will proceed by considering the secret keys which helps in secret communication (Fig. 10).

Routing using Chord Distributed Hash Table (CDHT): After the authentication process is over, distribution of the generated SSC has to be performed using an efficient routing method. For this purpose, a method called Chord Distributed Hash Table (CDHT) is being used. Chord provides support for just one operation: given a key, it maps the key onto a node. Data location can be easily implemented on top of Chord by associating a key with each data item and storing the key/data item pair at the node to which the key maps. There are 3 features that distinguish chord from many other peer-to-peer lookup protocols (Fig. 11). They are:

- Simplicity
- Provable correctness
- Provable performance

Domain name service provides a host name to IP address mapping. Chord can provide the same service

```
// ask node k to find id's nextnode
k.find-successor(id)
return k' = find-previousnode (id);  return k'.nextnode;
//ask node k to find id's previousnode
k.find-previousnode(id);  k'=k;
while (id  (k',n'.nextnode]))
k'=k'.closest-preceding-hash(id);  return k';
//return closest hash preceding id
n.closest-preceding-hash(id)
for k= downto 1
if(hash[j].node (k,id))
return hash[j].node;  return n;
define nextnode hash[1].node
//node k joins the network;
//k' is an arbitrary node in the network
k.join(k')
if(k)
init-hash-table(k'); update-others();
//move keys in (previousnode,k]from nextnode
Else //k is the only node in the network
For j=1 to n
Hash[j].node=k;  Nextnode = k;
//initialize table of local node; k' is an node already in network
k.int-hash-table (k')
hash[1].node = k'.find-nextnode(hash[1].start);
previousnode=nextnode.previousnode;
nextnode.previousnode=n;
```

```
for k=1 to n-1
if(hash[j+1].start [k,(hash[j].node))
hash[j+1].start [k,hash[k].node; else
hash[j+1].node=k'.find-nextnode(hash[j+1].start);
//update all nodes whose hash tables should refer to k
k.update-others ()
for j=1 to n
//find last node p whose jth hash might be k
P=find-previous node (k-2j-1); k.update-hash-table (k,j)
if(s [k,hash[j].node))  hash [i].node = s;
p = previous node; // get first node preceding k
P.update-hash-table(s,j);
// pseudo code for stabilization
k.join (k')
previousnode = nil; successor = k'.find-successor (k);
// verify k's immediate successor& tell the nextnode about k
k.stabilize (); x = nextnode.previousnode;
if(x (k,nextnode)) nextnode=x;
nextnode.notify(k);
// k' thinks it might be our nextnode
k.notify(k')
if(previousnode is nil or k' (previousnode,k))
previousnode = k';
// periodically refresh the hash table entry
k.fix-hashs(); k = random index > 1 into hash[];
hash [i].node = find-nextnode(hash[i].start);
```

Fig. 11: Secure routing algorithm using chord DHT

with the name representing the key and the associated IP address representing the value. Chord requires no special servers while DNS relies on a set of special root servers.

A CDHT is a class of a decentralized distributed system that provides a lookup service similar to a hash table; (key, value) pairs are stored in a CDHT. Any participating

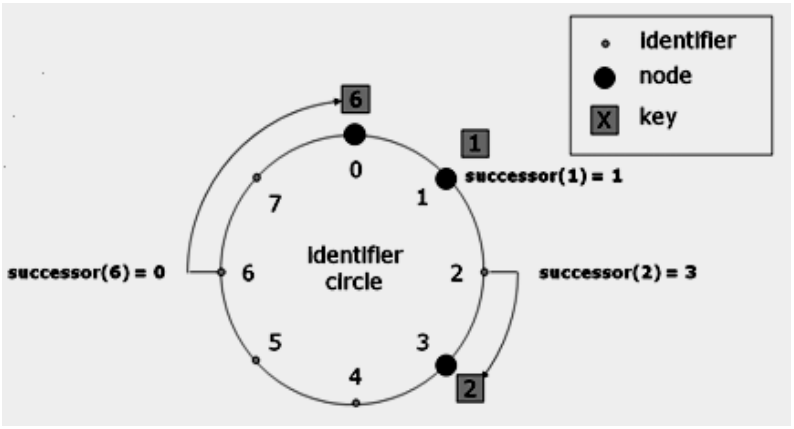

Fig. 12: An identifier circle consists of three nodes 0, 1and 3. In this example, key 1 is located at node 1, key 2 at node3 and key 6 at node 0

node can efficiently retrieve the value associated with a given key. Chord simplifies the design of peer-to-peer systems and applications based on it by addressing these difficult problems and they are considering as the advantages of CDHT. They are as follows

- Load balancing
- Decentralization
- Scalability
- Availability
- Flexible naming

The application using Chord is responsible for providing any desired authentication, caching, replication and user-friendly naming of data. Chord's flat key space eases the implementation of these features. Responsibility for maintaining the mapping from keys to values is distributed among the nodes in such a way that a change in the set of participants causes a minimal amount of disruption. This allows a CDHT to scale to extremely large numbers of nodes and to handle continual node arrivals, departures and failures. For example, an application could authenticate data by storing it under a chord key derived from a cryptographic hash of the data. Similarly, an application could replicate data by storing it under two distinct chord keys derived from the data's application level identifier. Co-operative mirroring and time-shared storage are the examples of applications for which chord would provide a good foundation for routing. CDHTs form an infrastructure that can be used to build more complex services, such as any cast, cooperative web caching, distributed file systems, domain name services instant messaging, multicast and also peer-to-peer file sharing.

An example of CDHT that tackles some of these problems is a logical ring of n nodes, each taking responsibility for 1/n of the key space. Once a node is added to the network, it finds a place on the ring to sit between two other nodes and takes responsibility for some of the keys in its sibling nodes. The beauty of this approach is that none of the other nodes in the ring are affected; only the two sibling nodes have to redistribute keys. When CDHT is compared to napster and its centralized servers, it avoids single points of control or failure by a decentralized technology. It is also compared with gnutella and its widespread use of broadcasts, avoids the lack of scalability through a small number of important information for routing.

The consistent hash function assigns each node a key, a bit identifier, using a base hash function such as SHA-1. A node's identifier is chosen by hashing the node's IP address, whereas a key identifier is produced by hashing the key. The term "key" refers to both the original key and its image under the hash function as the meaning will be clear from context. Similarly, the term "node" will refer to both the node and its identifier under the hash function. The identifier length must be large enough to make the probability of two nodes or keys hashing to the same identifier negligible. Consistent hashing assigns keys to nodes as follows.

Identifiers are ordered in an identifier circle modulo 2^m. Key is assigned to the first node whose identifier is equal to or follows (the identifier of) in the identifier space. This node is called the successor node of key, denoted by successor(k). If identifiers are represented as a circle of numbers from 0-2^m-1, then successor (k) is the first node clockwise from k (Fig. 12). Figure 8 shows an identifier circle with m = 3. Circle has three nodes: 0, 1 and 3. The

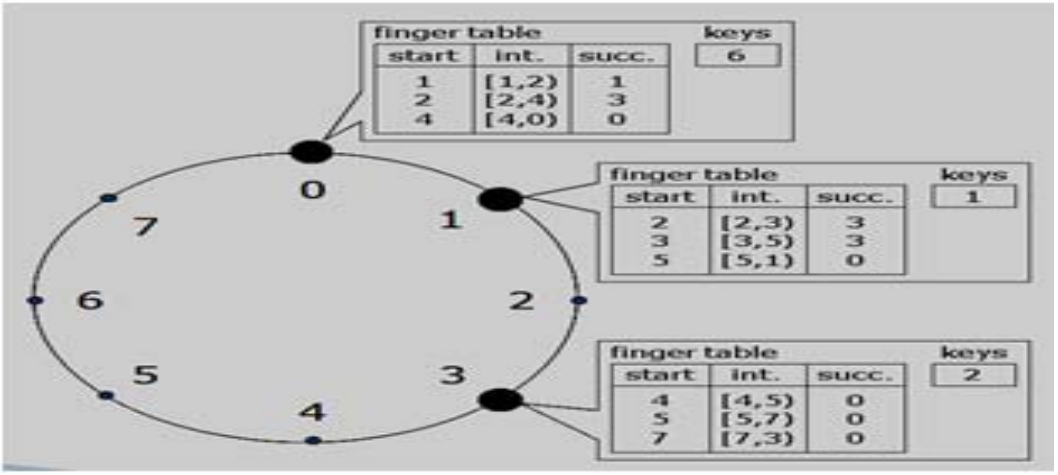

Fig. 13: Finger tables and key locations with nodes 0, 1 and 3 and keys 1, 2 and 6

successor of identifier 1 is node 1, so key 1 would be located at node 1. Similarly, key 2 would be located at node 3 and key 6 at node 0. Consistent hashing is designed to let nodes enter and leave the network with minimal disruption. To maintain the consistent hashing mapping when a node n joins the network, certain keys previously assigned to n's successor are now assigned to n. When node n leaves the network, all of its assigned keys are reassigned to n's successor. No other changes in assignment of keys to nodes need occur. In the example above, if a node were to join with identifier 7, it would capture the key with identifier 6 from the node with identifier 0. In this example, key 1 is located at node 1, key 2 at node 3 and key 6 at node 0

Lookups are accelerated by maintaining additional routing information. Each node maintains a routing table with (at most) m entries (where $N = 2^m$) called the finger table. The i^{th} entry in the table at node n contains the identity of the first node, *s* which succeeds n by at least 2^{i-1} on the identifier circle (Fig. 13):

- S = successor $(n + 2^{i-1})$ (all arithmetic mod 2)
- S is called the ith finger of node n, denoted by n. finger(i).node
- Chord must perform three tasks when a node n joins the network
- Initialize the predecessor and fingers of node n
- Update the fingers and predecessors of existing nodes to reflect the addition of n
- Notify the higher layer software so that it can transfer state
- When a node n fails, the nodes whose finger tables include n must find n's successor. In addition, the failure of n must not be allowed to disrupt queries that are in progress as the system is re-stabilizing. The key step in failure recovery is maintaining correct successor pointers, since in the worst case find predecessor can make progress using only successors. To help achieve this each chord node maintains a "successor-list" of r nearest successors on the Chord ring

RESULTS AND DISCUSSION

To study the performance of the proposed model, the certificate generation, the end-to-end delay, energy saving process, packet delivery report, data rate are explained and implemented over a simulated model of a Mobile grid network. The scenario was studied over both the Certificate Authority (CA) model and Supervisory Host (SH) model. In this process the CA with RSA model is referred to as the old model and the supervisory host with ECDSA model is termed as the proposed and new model (Fig. 14).

Certificate generation: Certificate generation is main responsibility of both supervisory host and certificate Authority. The graph shows the time taken to generate certificate between existing certificate authority which used RSA for certificate Generation and the proposed supervisory host will use ECDSA for certificate generation.

Packet delivery report: The time taken to deliver the packets between existing RSA and the proposed ECDSA.

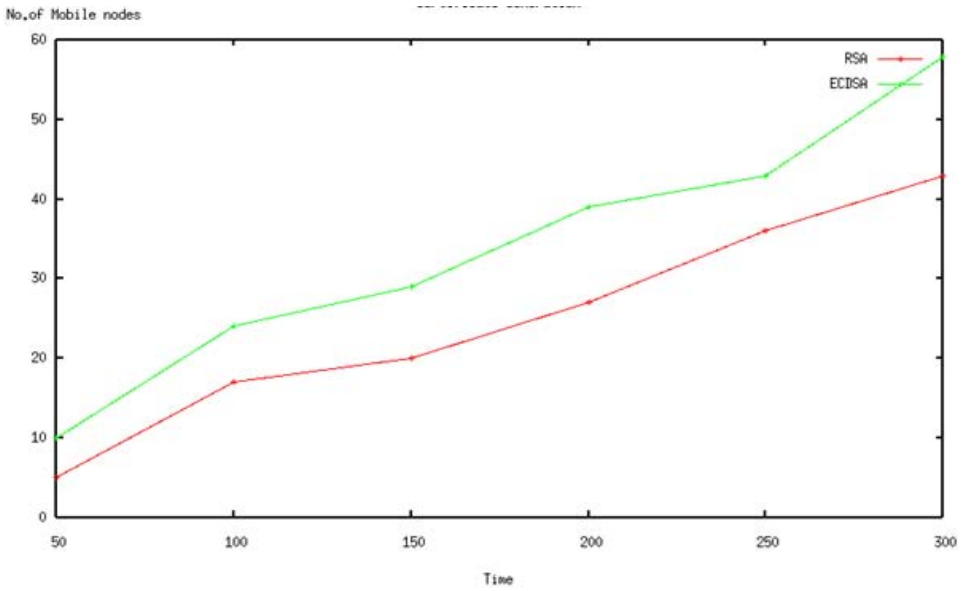

Fig. 14: Certificate generation

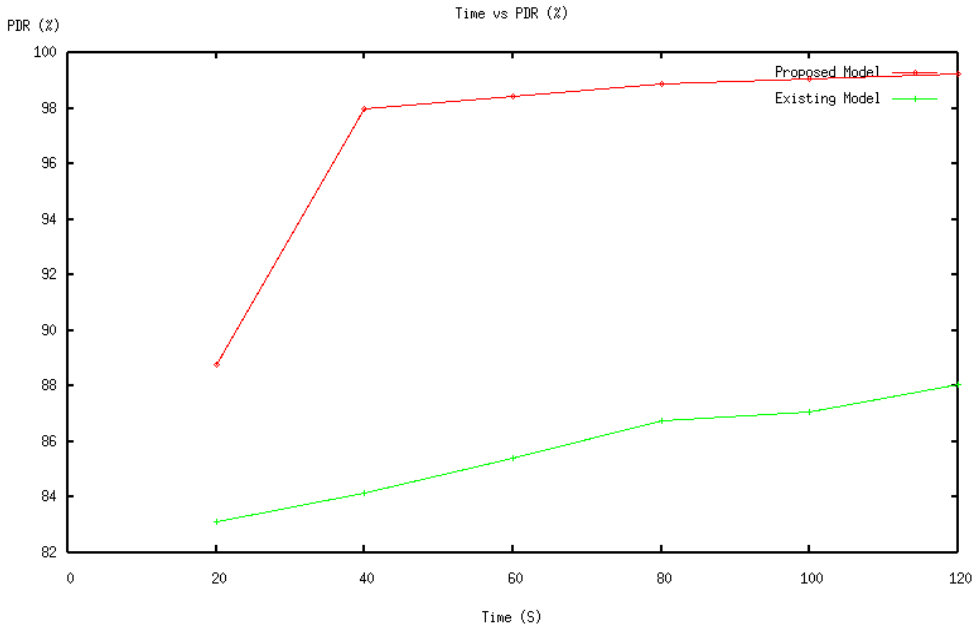

Fig. 15: Packet delivery ratio

Figure 15 shows packet delivery ratio with respect to time. In that the RSA has very less delivery ratio when compared to ECDSA.

End to end delay: The delay time for packet delivery between the Existing RSA and the proposed ECDSA varies with respect to time. Figure 16 discusses about the end to end delay difference with actual time for packet delivery between RSA and ECDSA.

Energy saving process: The mobile devices are battery powered and power consumption is one of the important factors. Figure 17 shows the comparison of the average consumed energy with time. As the time increases, the battery power is saved in proposed model.

Packet loss: Figure 18 Shows the comparison of time versus control packet overhead. The network life time is plotted against the packets travelled in the network.

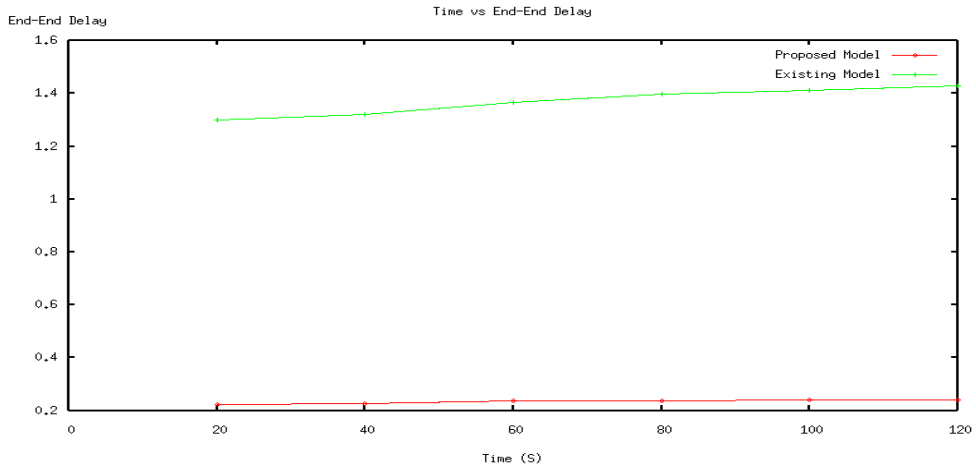

Fig. 16: End to end delay

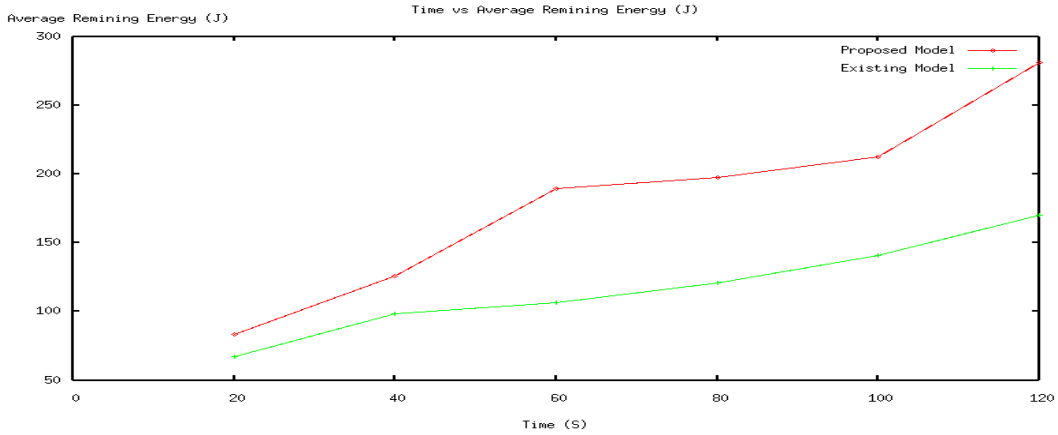

Fig. 17: Average remaining energy vs time

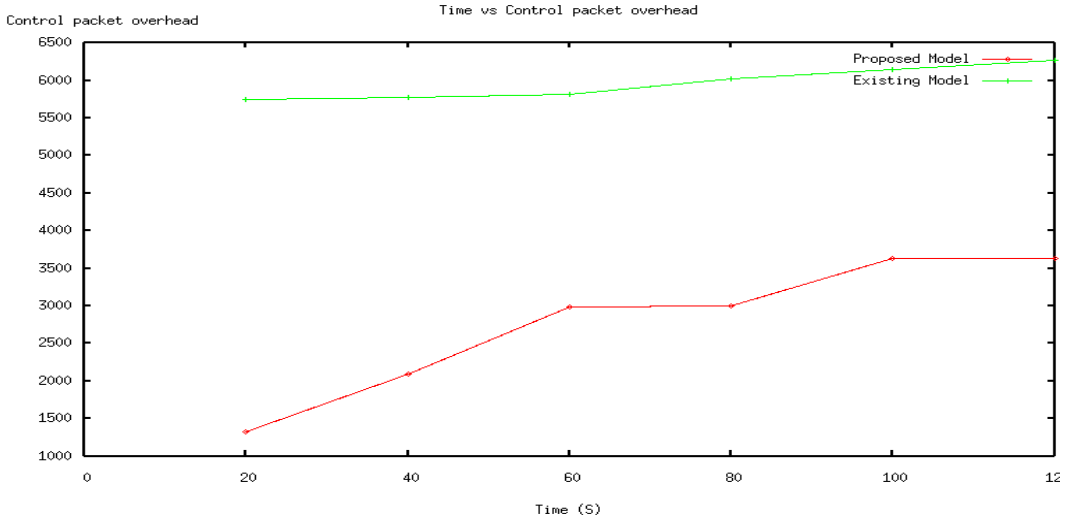

Fig. 18: Packet loss process

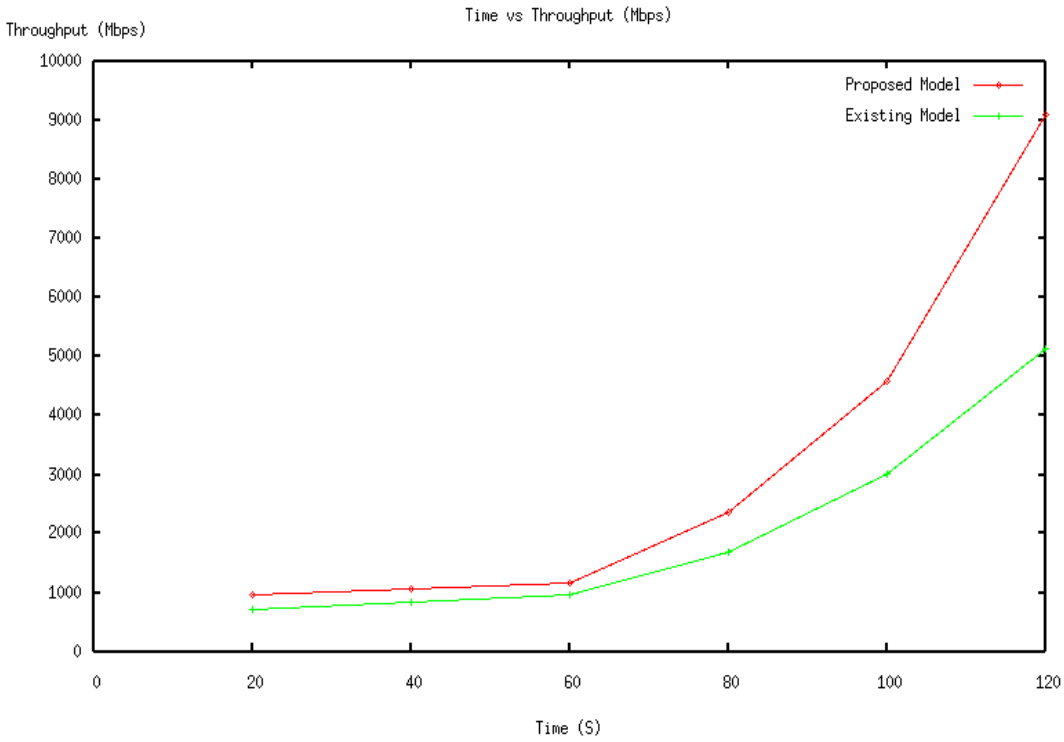

Fig. 19: Comparison of network lifetime is varying with respect to network size

As the time increases, automatically the control packet overhead is comparatively less in proposed model.

Data rate: Throughput is the total size of data packets properly received by a destination node each second. Figure 19 shows that the network lifetime is varying with respect to network size along with increasing number of mobile nodes.

CONCLUSION

In this study, a new concept is introduced called Supervisory Host (SH) which is a static node that takes care of certificate generation and distribution. The supervisory host also maintains a repository which helps to store the certificates for future use. The main advantage of SH is that it takes care of mobile host and their coordination between other nodes. The Registration Process in SH is very simple and it improves the authentication by reduced level of key exchange process. SH is maintained independently for any particular applications, the trust level is high and authentication process can be improved with the help of ECDSA algorithm which have key size of 168 bits which is far less when compared to RSA. SH is also used to store and retrieve certificates and the repository of SSC is done using the concept of hash table. Thus in order to provide security and power management in mobile grid environment, a new paradigm is proposed with the help of Secure Service Certificates (SSC) and Supervisory Host (SH). It is important that after storage the secure communication will be done between the authenticated nodes. Diffie-hellmann key exchange algorithm is used for authentication and chord DHT is used for secure Routing between the authenticated nodes. As a future work, the proposed system can be extended for secure routing of CHORD DHT Technique and can be compared with the other DHT Techniques of routing to get the clear performance implication between the Chord and other DHT techniques.

REFERENCES

Abidi, A., B. Bouallegue and F. Kahri, 2014. Implementation of Elliptic Curve Digital Signature Algorithm (ECDSA). Proceedings of the 2014 Global Summit Conference on Computer and Information Technology (GSCIT), June 14-16, 2014, IEEE, Monastir, Tunisia, ISBN:978-1-4799-5626-5, pp: 1-6.

Alcaraz, C. and J. Lopez, 2014. WASAM: A dynamic wide-area situational awareness model for critical domains in smart grids. Future Gener. Comput. Syst., 30: 146-154.

Begam, P. and M. Mohamed, 2014. ASAMO: Authentication and secure communication using abstract monitoring objects for mobile grid computing. Int. J. Comput. Sci. Appl., Vol. 3,

Bichhawat, A. and R.C. Joshi, 2010. A survey on issues in mobile grid computing. Int. J. Recent Trends Eng. Technol., 4: 15-19.

Chaddoud, G. and K. Martin, 2006. Distributed certificate authority in cluster-based ad hoc networks. Wirel. Commun. Netw. Conf., 2: 682-688.

Hayouni, H. and M. Hamdi, 2015. Energy efficient key menagement scheme for clustered hierarchical wireless sensor networks. Proceedings of the 2015 IEEE 12th International Conference on Networking, Sensing and Control (ICNSC), April 9-11, 2015, IEEE, Tunisia, ISBN:978-1-4799-8069-7, pp: 105-109.

Johnson, D., A. Menezes and S. Vanstone, 2001. The Elliptic Curve Digital Signature Algorithm (ECDSA). Int. J. Inform. Secur., 1: 36-63.

Lashkari, A.H., M.M.S. Danesh and B. Samadi, 2009. A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i). Proceedings of the 2nd IEEE International Conference on Computer Science and Information Technology ICCSIT 2009, August 8-11, 2009, IEEE, Kuala Lumpur, Malaysia, ISBN:978-1-4244-4519-6, pp: 48-52.

Li, Y., H. Jin, D. Zou, S. Liu and Z. Han, 2008. An authenticated encryption mechanism for secure group communication in grid. Proceedings od the 2008 International Conference on Internet Computing in Science and Engineering, January 28-29, 2008, IEEE, Wuhan, China, ISBN:978-0-7695-3112-0, pp: 298-305.

Mathur, R., S. Agarwal and V. Sharma, 2015. Solving security issues in mobile computing using cryptography techniques-A survey. Proceedings of the 2015 International Conference on Computing, Communication and Automation (ICCCA), May 15-16, 2015, IEEE, Uttar Pradesh, India, ISBN: 978-1-4799-8890-7, pp: 492-497.

Murthy, S.G.K., M.R. Murthy and A.C. Sarma, 2011. Elliptic curve based signature method to control fake paper based certificates. Proceedings of the World Congress on Engineering and Computer Science, October 19-21, 2011, WCECS, San Francisco, USA, ISBN:978-988-18210-9-6, pp: 1-3.

Muthukuru, J. and B. Sathyanarayana, 2013. A secure elliptic curve digital signature approach without inversion. Int. J. Eng. Adv. Technol., 3: 454-456.

Parmar, K.B., N.N. Jani, P.S. Shrivastav and M.H. Patel, 2013. Mobile grid computing: Facts or fantasy. Int. J. Multidiscip. Sci. Eng., 4: 26-33.

Saputro, N., K. Akkaya and S. Uludag, 2012. A survey of routing protocols for smart grid communications. Comput. Networks, 56: 2742-2771.

Sivagurunathan, S. and K. Prathapchandran, 2014. Trust and cluster based authentication schemes in mobile Ad Hoc networks-A review. Proceedings of the 2014 International Conference on Power Signals Control and Computations (EPSCICON), January 6-11, 2014, IEEE, Gandhigram, India, ISBN:978-1-4799-3612-0, pp: 1-5.

Stoica, I., R. Morris, D. Karger, M.F. Kaashoek and H. Balakrishnan, 2001. Chord: A scalable peer-to-peer lookup service for Internet applications. Comput. Commun. Rev., 31: 149-160.

Woungang, I., F.H. Tseng, Y.H. Lin, L.D. Chou and H.C. Chao et al., 2015. MR-Chord: Improved chord lookup performance in structured mobile P2P networks. IEEE. Syst. J., 9: 743-751.

Xiong, H., D. Zhang, L. Wang and H. Chaouchi, 2015. EMC 3: Energy-efficient data transfer in mobile crowdsensing under full coverage constraint. IEEE. Trans, Mob. Comput., 14: 1355-1368.