Supervisory Host Model: A New Paradigm to Enhance the Security and Power Management for Mobile Grid Environment

H.PARVEEN BEGAM[1], M.A.MALUK MOHAMED[2]
Software System Group
M.A.M College of Engineering
INDIA
ssg_parveen@mamce.org, ssg_malukmd@mamce.org

Abstract: - 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 paper 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. Existing projects use RSA (Rivest-Shamir-Adelman) algorithm for encrypting the message which has a key size of 1024 bits, but in ECDSA the key size is 168 bits which is far less when compare to RSA algorithm. The main advantages of ECDSA are greater security for a given key size, effective and compact implementation for cryptographic operations requiring smaller chips, which results in less heat generation and less power consumption, suitable for machines having low bandwidth, low computing power, less memory and easy hardware implementations. So the combination of SH and ECDSA algorithm helps to improve the trust level in organizations.

Key-Words: - Mobile Grid Computing, Authentication, Secure Communication, Secure Service Certificate(SSC), Certificate generation and encryption, Digital Signature, ECDSA.

1 Introduction

1.1 About Certificate Authority

Several cryptographic protocols require digital certificates (in effect, electronic credentials) issued by an independent trusted third party (the CA) to authenticate the transaction. A digital certificate, which is electronic document containing information about an individual and his or her public key, is the answer. This document is digitally signed by a trusted organization referred to as a Certification Authority (CA). The basic premise is that the CA is vouching for the link between an individual's identity and his or her public key. For a relying party to determine whether the certificate was issued by a legitimate CA, the relying party must verify the issuing CA's signature on the certificate. CA's signature using the CA's public key to determine whether the certificate was issues by a trusted CA. Many businesses rely on digital certificates for banking procedures. 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 financial and technological drawbacks.

(i) Certificate authorities typically require a subscription to their service, which requires monthly payments to continue the relationship which is financial disadvantage.

i) In addition, multiple certificates for different sites or purposes can become a costly endeavor.

ii) 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.

iii) 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.

iv) Maintenance of CA in two or more levels requires more cost and time for authentication.

v) 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.

vi) The subject, not the relying party, purchases certificates. The subject will often utilize the cheapest issuer, so quality is not being paid for in the competing market.

vii) Certification authorities deny almost all warranties to the user (including subject or even relying parties).

viii) The expiration date should be used to limit the time the key strength is deemed sufficient. This parameter is abused by certification authorities to charge the client an extension fee. This places an unnecessary burden on the user with key roll-over.

ix) Users use an undefined certification request protocol to obtain a certificate which is published in an unclear location in a nonexistent directory with no real means to revoke it.

Like all businesses, CAs are subject to the legal jurisdiction(s) of their site(s) of operation, and may be legally compelled to compromise the interests of their customers and their users. Intelligence agencies have also made use of false certificates issued through extralegal compromise of CAs, such as DigiNotar, to carry out man-in-the-middle attacks.

Debiao et al. [40] proposes ID-based remote mutual authentication with key agreement scheme on ECC which helps to provide not only mutual authentication but also supports a session key agreement between the user and the server. The scheme also provides the known session key security, the perfect forward secrecy, the no key-compromise impersonation, the no unknown key-share and the no key control.

Li Depeng et al. [39] proposes an efficient and robust approach to authenticate data aggregation in smart grid via deploying signature aggregation, batch verification and signature amortization schemes to less communication overhead, reduce numbers of signing and verification operations, and provide fault tolerance. Corresponding fault diagnosis algorithms are contributed to pinpoint forged or error signatures. Mobile cloud computing is gaining popularity among mobile users.

1.2 Distributed CA (DCA)

A 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. There are two types of DCA; PDCA (Partially Distributed CA) and FDCA (Fully Distributed DCA).

Some of the issues may happen while using distributed CA also. To site a few i) Availability issues - Like the normal user nodes, the DCA shareholding nodes may move to the other places and be inaccessible to the user nodes. In this condition, a user node may not find the required k DCA server node; ii)Security issues -No important system secret must be allocated to a single node and DCA key pairs must be generated in a distributed way. Also, a key refresh protocol is required to ensure that the lifetime of critical keys are restricted. In addition, intra DCA data must be secured with encryption or digital signatures; iii) Reliability issues - DCA system should avoid relying solely on the underlying communication network, since channels or nodes may be compromised. Wherever possible, measures should be taken to improve the system's robustness. Use of encryption and digital signature for inter DCA node communication can improve DCA's security; iv) Lesser efficiency - Mobile nodes are power and bandwidth limited and communication is relatively slow and unreliable, so protocols should attempt to minimize the amount of transmitted data between nodes; v) Fault tolerance issues; vi) Managing user node mobility; vii) Self initialization; viii)

Scalability issues – For a few numbers of nodes, this technique is suitable. But for larger counts this method is not suitable due to various factors; ix) Integration issues - It must cooperate with the other security components and should be easily integrated with the other systems such as registration authorities or user applications; x) Certificate revocation and validation issues- Independency creates many problems; xi) Limited storage overhead - A PKI system requires large amount of storage for storing its certificate, keys, and other data structures.

2 Motivation

Mobile Grid Computing is an environment that allows sharing and co-ordinate use of diverse resources in dynamic, heterogeneous and distributed environment using different types of electronic portable devices which rely on two fundamental functions: communication and resource sharing. Since the Internet is not security-oriented by design, there exist various attacks, in particular malicious internal and external users. The combination of Grid environment with mobile devices leads to many security issues. A Mobile Grid has the following issues: Data Management, Resource Management, Information Management, Power management and Security Management. The focus is on security and power management.

Security is a very important factor in Mobile Grid Computing and is also difficult to achieve owing to the open nature of wireless networks and heterogeneous and distributed environments. In a distributed job execution environment the potential risks rise for the both integrity of the application and the resource provider. 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.

The combination of mobile and grid may lead to lot of security issues like authentication of 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 complexity of authenticity and security. Particularly in mobile grid environment, some of the risks like integrity of the processing the results is compromised by malicious mobile node, unnecessarily the MN performs free ride without contributing the resources which in turn reduces the system utility, spoiling the data confidentiality, destroying the files and applications and a malicious MN pretending to act as a owner are the issues to be solved. So providing countermeasures for the security issues assumes significant process.

3 Related Work

A few researchers have addressed some of the mobile grid issues. Thomas et al. integrated the mobile wireless consumer devices into the Grid which may cause limitations like reduced CPU performance, lesser secondary storage, heightened battery consumption sensitivity, and unreliable low-bandwidth communication. Given that the benefits of combining the resources of mobile devices with the computational grid are potentially enormous, one must compensate for the inherent limitations of these devices in order to successfully utilize them in the Grid. Proxy-based, clustered system architecture [1] proposes with favourable deployment, interoperability, scalability, adaptively and fault-tolerance characteristics as well as an economic model. Konstantinos et. al proposed the scheduling, performance and security related issues [2] in various networking contexts of mobile Grid computing. There may be limitations in usage of many proxy-based nodes which may lead to cost effectiveness. The utilization of baseline devices is easy to solve; but hard to motivate the user to contribute the baseline resources to the grid.

Sanjay P.Ahuja et al. proposed the conventional authenticated session key exchange protocol [7] which is based on certificates. The authentication protocol based on the public-key certificate eliminates the need for contacting the mobile user's home network as long as the certificate has a valid expiration date, even though that user is being serviced in the visiting network operated by

another service provider. The drawback of the authentication protocols based on certificates discussed here use RSA algorithm which is computationally heavy to perform encryption.

Universally trusted, certificate authority (CA) is a trusted third party that takes responsibility to generate public and private keys to provide authentication service to several service providers. Session key exchange protocol is done using digital certificates. A public key authentication called RSA is used for encryption and authentication. Certificate authority is a universally trusted third party. CA generates and maintains both public and private keys for each mobile node securely. The authentication protocol is based on public key method called RSA. In some schemes such as [25], certificates have limited lifetime and after expiration time they are revoked. Thus, compromised keys cannot be used anymore. The duration of this expiration time will be a trade-off between security and performance. Chaddoud et al. [24] proposed a DCA for near-term digital radio (NTDR) cluster-based ad hoc networks. The DCA is distributed among the cluster heads (CHs) which become the shareholding DCA nodes. Thus, no single CH knows the DCA private key and when a new CH joins the backbone it needs to be issued with a share of the DCA's private key.

Rao and Xie [26] present another distributed certification authority scheme based on clustering scheme. They classify MANET nodes into clients, repositories, and server nodes. The client nodes are organized into clusters. In each cluster, some nodes are elected to be a repository which stores the certificates of the nodes and servers within the cluster. Elhdhili et al. [27] propose a totally distributed cluster-based key management for ad hoc networks and use a (K,N) threshold scheme to distribute an RSA signing key to the set of CHs, Furthermore, they use proactive and verifiable secret sharing to protect the secret from various attacks. They also assume that the system contains three types of nodes. The first one is an administrator that will exist only when the initialization step can leave the network. The second nodes are a set of CHs and the third ones are regular nodes. In addition, the administrator and CHs have directories to save the certificates.

Dong et al. [28] have designed another cluster-based PDCA for MANET and propose optimization for DCA's nodes operations. First, when a user needs PDCA services, he must locate enough PDCA server nodes. To solve this problem, they shift the responsibility of CA discovery from user nodes to the CHs. Thus, a CH must maintain the required information to locate the CA nodes in or out of its cluster. Therefore, each CH maintains a CA information table (CIT), which contains a list of the CA nodes in its local cluster, and probably the CA information in other clusters. Lee and Jeong [29] proposed a partially distributed certificate management system that can handle mobility of nodes. It minimizes routing loads and enhances expandability of network by allowing participating nodes to authenticate each other without being interrupted by joining the cluster.

Zouridaki et al. [30] designed an elliptic curve-based DCA system. Elliptic curve is used because of its shorter key length and lower computational overhead. Their scheme uses a three-tiered logical view of DCA architecture. At the lowest tier, individual nodes are organized into clusters. The next tier consists of one or more certificate repositories in each cluster that broadcast the certificates of new nodes and the top tier consists of DCA servers that periodically inform the cluster about issued or the updated CRL.

In DCA, CA jobs are distributed among all the nodes which spoil the security. The frequency of communication between sender and the receiver gets increased. If any node CA compromises then the overall architecture will be spoiled. Scalability is another big issue in DCA. If the number of nodes increases, the DCA creates lot of confusions while generating the certificates and storing the certificates. Each node will store their certificates, which will be overloaded to all the individual nodes. So we need a system which satisfies all the security requirements and provides certificate storage.

Zissis et al. [36] proposes introducing a Trusted Third Party, tasked with assuring specific security characteristics within a cloud environment. The proposed solution calls upon

cryptography, specifically Public Key Infrastructure operating in concert with SSO and LDAP, to ensure the authentication, integrity and confidentiality of involved data and communications. The solution, presents a horizontal level of service, available to all implicated entities, that realizes a security mesh, within which essential trust is maintained.

Alcaraz et al. [34] explains about the model which is based on a set of current technologies such as the wireless sensor networks, the ISA100.11a standard and cloud-computing together with a set of high-level functional services. 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.

Tornos et al. [32] proposes a secure eVoting protocol based on ring signatures. The implementation details and the different modules of a voting platform included in the voting protocol. During the signature process a parameter called 'linking tag' is generated, that is able to identify the different votes sent by a single voter during a voting process. This characteristic makes it interesting in e-Cognocracy and Quality of experience evaluation scenarios.

4 Supervisory Host Model

4.1 Architectural view

The countermeasures under investigation include the authentication, confidentiality, secure communication, access control and so on. In each situation, our aim is to balance between functionality, performance and security while achieving any solutions and that will not impose any restrictions (e.g. increased power consumption) on the personal use of a mobile device. In order to provide security and power management in a holistic manner, A new paradigm for mobile grid environment with the help of Secure Service Certificates (SSC) and Supervisory host (SH) is presented. Figure 1 shows the mobile grid environment as cluster of clusters. Each cluster can be viewed as 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). SH manages all the resources and services which is within their cluster. Depending on MSS load conditions, MSS and SH may be configured on to the same host or on to different host. SH coordinates among the other neighbouring SHs in a peer-to-peer fashion. Supervisory Host (SH) in each cluster will take care of certificate generation and distribution. Traditional CA (Certificate Authority) cannot directly used in mobile grid environment due to the following reasons:

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. So a trusted model for each cluster is needed. Because of individual requirements and processing styles of each cluster, SH is very much useful for 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. The main responsibilities of SH is Certificate generation, Certificate distribution, Provision of repository of certificates and maintenance of confidentiality and authentication between mobile hosts. 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.

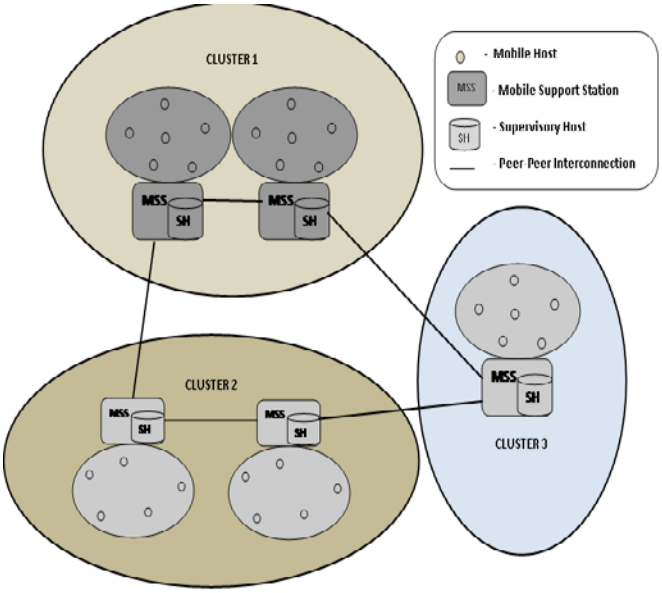

Fig 1. Clustered Mobile Grid architecture with Supervisory Host

Roles and responsibilities of Supervisory Host are Certificate generation using digital signature algorithm (ECDSA), providing repository of certificates to maintain confidentiality and Authentication between mobile hosts. In the proposed architecture, the authentication process can be improved with the help of ECDSA algorithm instead of RSA. Existing projects use RSA algorithm for encrypting the message which has a key size of 1024 bits, but in Elliptic Curve Cryptography with Digital Signature Algorithm (ECDSA) the key size is 168 bits which is far less when compare to RSA (Rivest-Shamir-Adelman) algorithm. The main advantages of ECDSA are greater security for a given key size, effective and compact implementation for cryptographic operations requiring smaller chips that generates less heat and less power consumption, suitable for machines having low bandwidth, low computing power, less memory and easy hardware implementations. Instead of trusting a third party, SH can be used to improve the trust level. Small organizations/ small projects where work needs to be completed quickly and where much time is not spent for certificate generation and authentication process. Business organizations, corporate, colleges and governments that use applications will expect security but doesn't like to depend on a third party. So the combination of SH and ECDSA algorithm helps to improve the trust level in organizations.

The supervisory host model for mobile grid systems defines an architecture that helps for generating the certificates 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 existing methods mobile hosts depends on Certificate Authority (CA) for generation of certificates using various certificate generation methods. Issues arise when the CA becomes malicious and also consumes more battery power. Our focus is to provide security and power management. This includes (i) Authentication of a mobile node: achieved by providing certificates with digital signature using ECDSA which has 168 bit key size which is far less when compared to RSA algorithm. (ii) Saving the battery power: achieved by introducing a Supervisory Host (SH) which is a static node located at Mobile Support Station (MSS) of each Mobile Grid Network (MGN) and it takes care of certificate generation and signing. The introduction of SH will enhance the security, anonymity and power consumption.

4.2 Certificate Generation using ECDSA

The supervisory host model for mobile grid systems defines an architecture that helps for generating the certificates and digital signatures for mobile hosts to provide 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 existing methods mobile hosts depends on Certificate Authority (CA) for generation of certificates using various certificate generation methods. Issues arise when the CA become malicious and also consumes more battery power. The focus is to provide security and power management. This includes (i) Generation of certificates using ECDSA, (ii) Repository of certificates in Supervisory Host, (iii) Authentication using Diffie-Hellman Key

Exchange Algorithm, (iv)Effective routing using Chord Distributed Hash Table (DHT). In the proposed architecture, the authentication process can be improved with the help of ECDSA algorithm instead of RSA.

4.2.1 Certificate Generation Process

Figure 2 shows the structure of Secure Service Certificate model. The Mobile Host issues the necessary components to SH in an encrypted format. After receiving the contents, SH starts generating the certificate along with digital signature with the help of public key of sender and receiver. The components of the certificate are: serial number, certificate identifier algorithm, issuer's unique ID, validity period, subject ID, subject public key, algorithm identifier, TTL and Nonce. ($ID_s||TTL||K_{pu(s)}||ID_d||N_1$). Certificate identifier algorithm helps to identify the encryption algorithm in which the certificate has been encrypted. Issuer's unique ID is identity of the supervisory host. Validity period is the time for which the certificate is valid. Subject ID is the identity of the receiver. Subject public key is receiver's public key. The sender node communicates with the receiver using this public key. Algorithm identifier is a type of algorithm where the data is encrypted. Finally, SH makes a copy of the SSC (Secure Service Certificate) and sends it to the corresponding mobile node. X.509 certificate has some limitations like revocation of root certificates, delegation issues, federation issues, ambiguous status report and aggregation issues. Moreover it uses RSA algorithm as certificate signature algorithm which has the key size as 1024 bits. The number of computations is more in RSA which increases computation time and is not suitable for mobile devices. Though mobile devices are battery powered, the RSA algorithm would not be suitable for mobile environment. The solution is to make use of 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.

Fig 2. Secure Service Certificate (SSC)

4.2.2 Digital Signature Algorithm

Digital signature schemes can be used to provide the following basic cryptographic services: data integrity (the assurance that data has not been altered by unauthorized or unknown means) data origin authentication (the assurance that the source of data is as claimed) non-repudiation (the assurance that an entity cannot deny previous actions or commitments). The ECDSA have a smaller key size, which leads to faster computation time and reduction in processing power, storage space and bandwidth. This makes the ECDSA ideal for constrained devices such as pagers, cellular phones and smart cards. ECDSA has three phases, key generation, signature generation, and signature verification.

Advantages of ECDSA:

The ECDSA offers remarkable advantages over other cryptographic system.

- 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.

ECDSA Key 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). E is an elliptic curve defined over Fq , and P is a point of prime

order n in E(Fq), q is a prime. Each entity A does the following:
1. Select a random integer d in the interval [1, n- 1].
2. Compute Q = dP.
3. A's public key is Q, A's private key is d.

ECDSA Signature Generation:

To sign a message m, an entity A with domain parameters D= (q,FR, a, b, G, n, h) does the following:
1. Select a random or pseudorandom integer k in the interval [1,n-1].
2. Compute kP =x1, y1 and 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.
3. Compute k-1mod n.
4. Compute s= k-1 {h (m)+ dr} mod n, where h is the Secure Hash Algorithm (SHA-1). If s = 0, then go back to step 1.
5. The signature for the message m is the pair of integers (r, s).

ECDSA Signature Verification:

To 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 public key Q and does the following
1. Verify that r and s are integers in the interval [1, n-1].
2. Compute
w = s-1mod n and h (m)
3. Compute
u1 = h(m)w mod n and u2 = rw mod n.
4. Compute
u1P + u2Q =(x0, y0) and v= x0 mod n.
5. 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
$k=s^{-1}(e+dr)=s^{-1}e+s^{-1}rd=we+wrd=u_1+u_2$ d (mod n)
Thus $u_1G+u_2Q=(u_1+u_2d)G=kG$, and v=r as required.

4.3 Repository for SSC

After generating the certificate, it is very necessary to store the certificate in a secure place such that no intruder can access the certificate. To achieve this each mobile node stores the SSC in its Supervisory Host. SH acts as a distributed database, so as to manage all the resources and services which is within their cluster. A major objective of SH is to provide ease of access to data for users at many different locations. To meet this objective, the SH system must provide location transparency, which means that a user (or user program) using data for querying or updating need not know the location of the data which also helps to maintain security of the system. Here, the repository of SSC is done using the concept of hash table. The reasons for using horizontal partitioning are efficiency, speed, security and ease of querying.

Each MH is maintained with a hash table that contains- 1)key value, 2)location, and 3)identifier. Likewise, each SH maintains a hash table which is automatically updated whenever a MH enters or leaves a MSS. When a MH enters a cell it sends a control signal to the corresponding MSS, which consists of the address of the MSS from where the mobile node is entering. In case when the old MSS address is null it indicates that the node had entered the system for the first time and thus creates an entry in its SH. When a MH wants to participate in a mobile grid, it registers itself with an MSS. The MSS assigns a unique identification for the MH namely, the Mobile Host Identifier (MHID) and passes the information to the corresponding SH, which checks the authentication and stores its information in its database. To store a certificate in SH, the mobile node sends the request message to Supervisory Host. SH will check the authentication of the mobile node that belongs to its cluster and then stores the certificates. Each cluster has a collection of mobile hosts and one SH is maintained for each cluster.

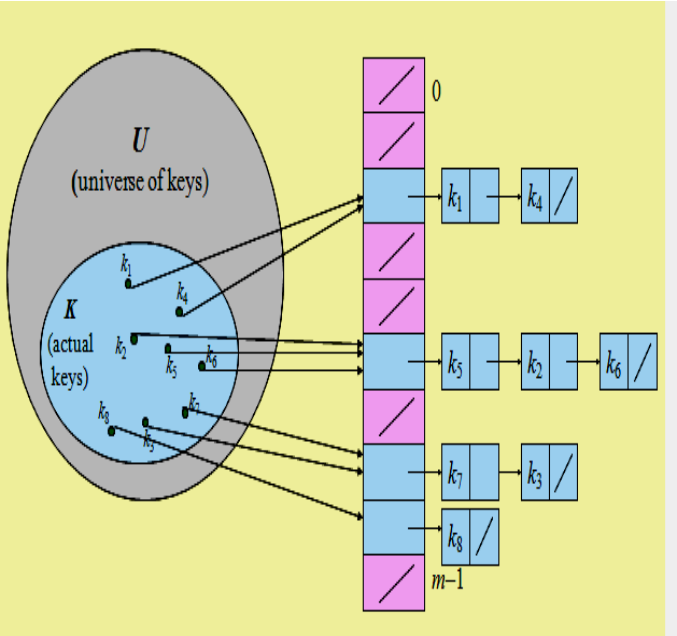

Fig 3. Certificate Index storage process in a hash table

```
Hash-Insert (F, 1)
 j -> 0
  repeat i -> h(k, i)
          if F[i] = NIL
             then F[i] -> 1
                  return j
             else j -> j + 1
    until j = m
  error "hash table full"
\\ Search data memory
Hash-Search (F, 1)
  j -> 0
  repeat i -> h(1, i)
          if F[i] = 1
             then return i
          j -> j + 1
  until F[1] = NIL or j = m
  return NIL
```

Fig 4. Hash Table entry process algorithm

4.4 Authentication using Diffe-Hellman Key Exchange Algorithm

Any mobile node (MH_i) may enter into Mobile Grid Network (MGN_i) and performs Diffe-Hellman process for authentication. If the node (say MH_s) from one grid and wants to communicate with another node (MH_d) in other grid, it must notify the receiver that it is an authenticated mobile node. To do that, the Secure Service Certificate (SSC) is used. The MH_s (sender mobile node) which wants to communicate with MH_d (receiver node), first sends its identification information to SH. Supervisory Host will check the details. If it ensures authentication, SH will send signed certificate with key pair. Same process is followed in the other side too. If two communicating nodes ensure its authentication, then content request is sent from MH_s to MH_d. MH_d will send signed certificate with public key to MH_s. After receiving the certificates at both sides communication starts between the mobile hosts.

The Diffie-Hellman key exchange is vulnerable to attacks in which the intruder intercepts messages between the sender and receiver, and assumes the identity of the other party (often known as the man in the middle attack). Consequently, the Diffie-Hellman algorithm should be used with a form of authentication, has a certificate to ensure that the symmetric keys are established between legitimate parties.

Communication is the medium for sending and receiving the data between two parties i.e. Sender and receiver but communication needs security from unauthorized people. Security covers a variety of computer networks that are used every day. It secures the network, as glowing as protecting and management operations being done. For more security, use Diffie –Hellman algorithm. Diffie–Hellman key exchange is a specific technique of exchanging cryptographic keys. 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.

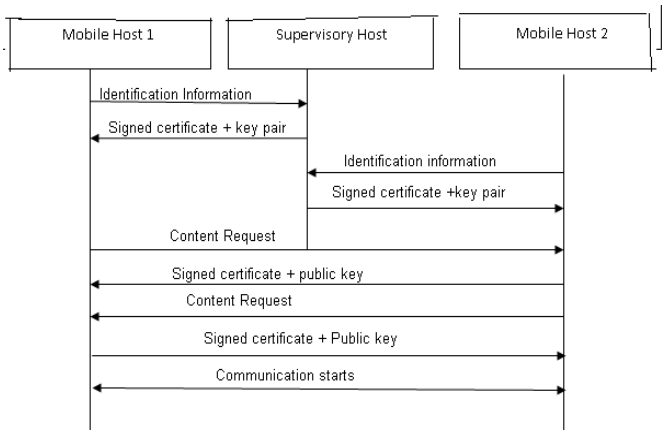

Fig 5. Authentication process using Supervisory Host

The Diffie - Hellman key exchange exploits arithmetical properties to produce a common computational result between two parties wishing to exchange information, without any of them providing all the necessary variables. By agreeing on two variables and providing each other with a computed public key, the resulting secret key will be identical throughout the exchange. The D-H protocol can be a powerful component in many a security measure. The Diffie-Hellman key exchange algorithm has proven to be one of the most interesting key distribution schemes in use today. 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-Hellman algorithm should be complemented with an authentication mechanism.

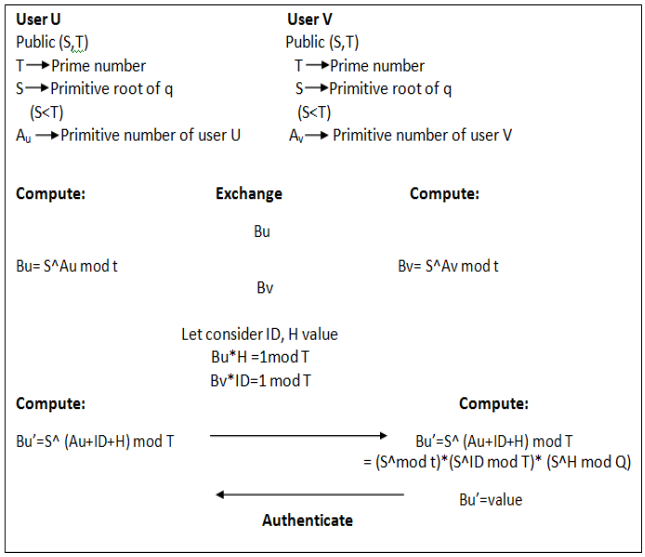

Fig 6. Diffie-Hellman Key exchange algorithm for any cluster

4.5 Routing using Chord Distributed Hash Table (DHT)

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 Distributed Hash Table (DHT) is being used. A Distributed Hash Table (DHT) 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 DHT, and any participating node can efficiently retrieve the value associated with a given key. The advantages of using DHT are Automatic load balancing, fully distributed, scalable in terms of state per node, bandwidth, and lookup time. 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 DHT to scale to extremely large numbers of nodes and to handle continual node arrivals, departures, and failures.

DHTs form an infrastructure that can be used to build more complex services, such as anycast, cooperative Web caching, distributed file systems, domain name services, instant messaging, multicast, and also peer-to-peer file sharing. One example DHT that tackles some of these problems is a logical ring of n nodes, each taking responsibility for 1/n of the keyspace. 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.

```
// 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 7. Secure Routing algorithm using chord DHT

5 Performance Analysis

To study the performance of the proposed model, the average power consumption, end-to-end delay, packet delivery ratio, the overall network lifetime as the function of number of nodes, varying network lifetime with respect to network size and storage capacity for mobile information explained and were 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. Throughout this section, the CA model is referred to as the old model and the Supervisory Host model is termed as the new model.

5.1 Power Consumption

The power consumption in mobile node is mainly due to transmission and reception of data packets. Whenever a node remains active, it consumes power. Even when the node is sleepy and participating in network, but is in the idle mode waiting for the packets, the battery keeps discharging. The battery power consumption refers to the power spent in calculations that take place in the nodes for routing and other processes. The number of nodes in the network versus average consumed battery power is considered as a metric. Figure 8 shows the comparison of the average consumed power for both the old and new models. The average consumed power is plotted against the number of nodes travelled in the network for different simulation time intervals. As the number of nodes increases, the battery power also increases. More the number of nodes more is the power consumed. The average consumed power by the mobile nodes is less in new model compared with the old model.

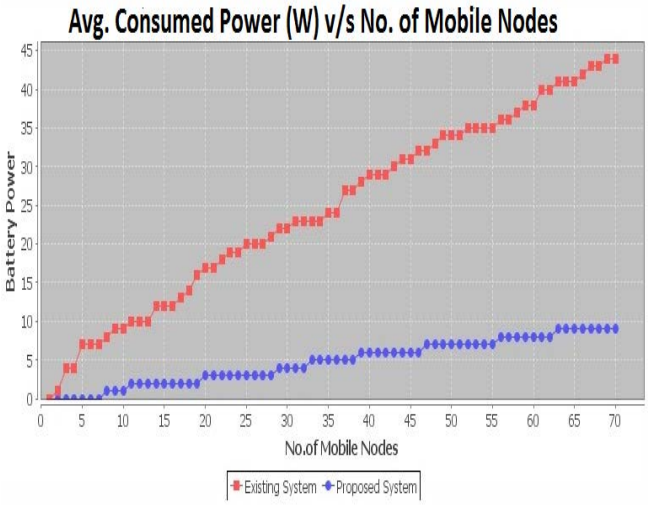

Fig 8. Comparison of average consumed power with increasing number of mobile nodes

5.2 End-to-End delay

Figure 9 shows the comparison of the end-to-end delay with moving speed of mobile nodes for both old and new models. The end-to-end delay is plotted against the number of nodes travelled in the network for different simulation time intervals. End-to-end delay refers in the direction of the time taken for a packet to be transmitted across a network from source to destination. Delay increases as the moving speed of the nodes increases.

Fig 9. Comparison of end-to-end delay with moving speed of mobile nodes

5.3 Network lifetime

Figure 10 shows the comparison of the network life time in both old and new models. The network life time is plotted against the number of nodes travelled in the network for different simulation time intervals.It is the time span from the deployment to the instant when the network is considered non-functional. It can be, for example, the instant when the first mobile node dies, a percentage of mobile nodes die, the network partitions, or the loss of coverage occurs. It affects on the whole network performance. As the number of nodes increases, automatically the network lifetime decreases. This degradation of the lifetime of the nodes is much lesser in the proposed system than the existing system.

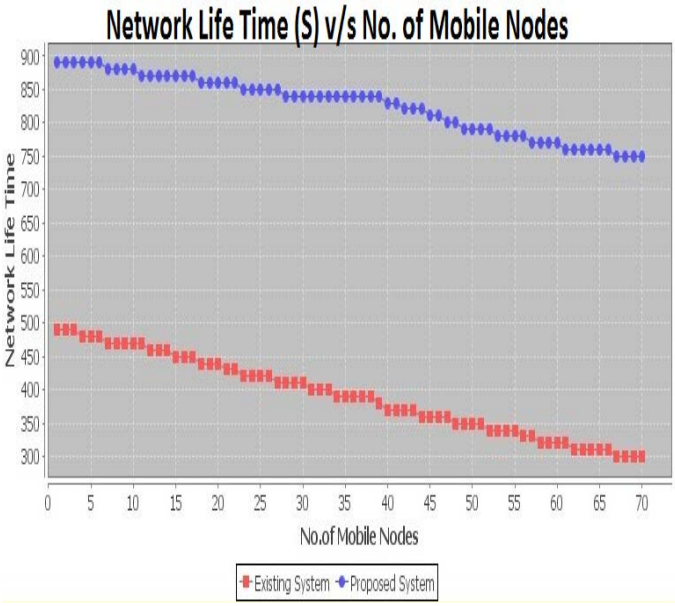

Fig 10. Comparison of network life time with increasing number of mobile nodes

5.4 Packet delivery ratio (PDR)

The packet delivery ratio is plotted against the number of nodes travelled in the network for different simulation time intervals shown in the following figure 11 shows the ratio of packets are successfully delivered to a destination compared to the number of packets that have been sent out by the sender. The number of packets delivered in the new model is greater than the old model.

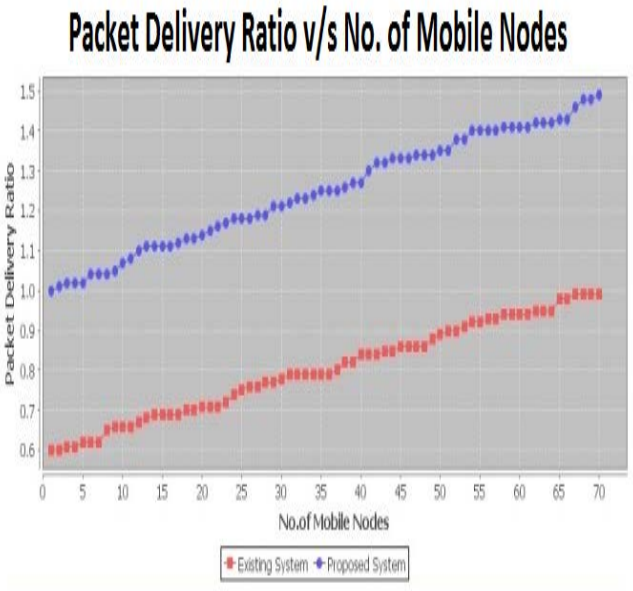

Fig 11. Comparison of packet delivery ratio with increasing number of mobile nodes

5.5 Throughput

Throughput is the total size of data packets properly received by a destination node each second. Throughput is the average rate of successful message delivery over a communication channel. These data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot. Figure 12 shows that the network lifetime is varying with respect to network size along with increasing number of mobile nodes.

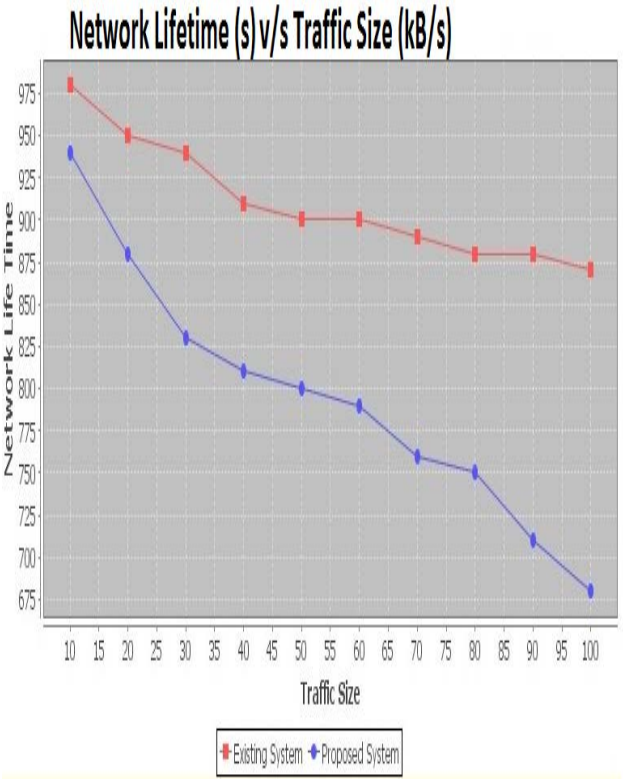

Fig 12. Comparison of network lifetime is varying with respect to network size

Table 1: Results for CA & SH model with tasks submitted based on capability of Mobile Host

	Certificate Authority Model			Supervisory Host Model			
#MH	Send Power (W)	Rec. Power (W)	Energy (kB/s)	Send Power (W)	Rec. Power (W)	Energy (kB/s)	Life Time (S)
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
49	0.1	0.05	5.0	0.4	0.2	20.0	400.0
57	0.3	0.15	15.0	0.1	0.05	5.0	100.0
66	0.3	0.15	15.0	0.2	0.1	10.0	200.0

Each MH has a client and a daemon. The clients are used to submit tasks to the MHs for distributed processing. The daemons are the computing entities at the MHs that execute a part of the submitted task concurrently with other daemons. The amount of computation and data for each participating MHs was given based on the capability of each MH. Table 1 shows the sending power, receiving power, energy and lifetime attained using the grid with various combinations of MHs participating. The speedup was calculated taking the average of the time taken when executed with single MH. The experimentation was done in Certificate Authority model and Supervisory host model with dynamic mobility of all the 69 participating node (including the node which initialized the application).

6 Conclusion

The paper highlights a new concept called Supervisory Host (SH) which is a static node that takes care of certificate generation and distribution. The main advantages and disadvantages of the proposed system and compared with the certificate authority model (ID based cryptography). The main advantages of Supervisory Host paradigm are simple registration process, reduced level of key exchange process and improved authentication process between two parties. 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. Existing projects use RSA algorithm for encrypting the message which has a key size of 1024 bits, but in Elliptic Curve Cryptography Digital Signature Algorithm (ECDSA) the key size is 168 bits which is far less when compared to RSA. Due to advancement in performance and speed of miniature devices and wireless networks, and increasing trend towards anytime, anywhere computing paradigm this field has got considerable attention.

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. The subject, not the relying party, purchases certificates. The subject will often use the cheapest issuer, so the quality is not being paid for in the competing market. Certification authorities deny almost all warranties to the user (including subject or even relying parties).The expiration date should be used to limit the time the key strength is deemed sufficient. This parameter is abused by certification authorities to charge the client an extension fee. This places an unnecessary burden on the user with key roll-over. Like all businesses, CA is subject to the legal jurisdiction(s) of their site(s) of operation, and may be legally compelled to compromise the interests of their customers and their users. Intelligence agencies have also made use of false certificates issued through extralegal compromise of CA, such as DigiNotar, to carry out man-in-the-middle attacks.

Maintaining the SH in each cluster takes some delay to have a secure communication. The limitation of the proposed framework is transmission delay in communication between supervisory host and the mobile node. Maintaining the delay and security is the state-of-the-art in mobile grid environment. As a future work, the proposed mobile grid can be extended to integrate the Supervisory Host into wireless sensor networks which will be useful to maintain security in military applications.

References:

[1] Phan, Thomas, Lloyd Huang, and Chris Dulan. "Challenge: integrating mobile wireless devices into the computational grid." *Proceedings of the 8th annual international conference on Mobile computing and networking*. ACM, 2002.

[2] Katsaros, Konstantinos, and George C. Polyzos. "Towards the realization of a mobile grid." *Proceedings of the 2007 ACM CoNEXT conference*. ACM, 2007.

[3] Mohamed, MA Maluk, D. Janakiram, and Mohit Chakraborty. "Surrogate Object Model: A New Paradigm for Distributed Mo-bile Systems." *ISTA*. 2005.

[4] A. Chakrabarti et al., "Grid computing security: a taxonomy", IEEE Security and Privacy 6 (1) (2008) 44–51.

[5] R. Kolonay, M. Sobolewski, "Grid interactive service-oriented programming environment, in: Proceedings of Concurrent Engineering" The Worldwide Engineering Grid, Press and Springer-Verlag, 2004, pp. 97–102.

[6] Park, Chang-Seop. "On certificate-based security protocols for wireless mobile communication systems." *Network, IEEE* 11.5 (1997): 50-55.

[7] Gupta, Vipul, et al. "Performance analysis of elliptic curve cryptography for SSL" *Proceedings of the 1st ACM workshop on Wireless security*. ACM, 2002.

[8] Lam, Kwok-Yan, et al. "Enhancing Grid security infrastructure to support mobile computing nodes." *Information Security Applications*. Springer Berlin Heidelberg, 2004. 42-54.

[9] Yan, Fei, et al. "An improved wireless grid security infrastructure based on trusted computing technology." *Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006. International Conference on*. IEEE, 2006.

[10] Butler, Randy, et al. "A national-scale authentication infrastructure." *Computer* 33.12 (2000): 60-66.

[11] Ahuja, Sanjay P., and Jack R. Myers. "A survey on wireless grid computing." *The Journal of Supercomputing* 37.1 (2006): 3-21.

[12] Lashkari, Arash Habibi, Mir Mohammad Seyed Danesh, and Behrang Samadi. "A survey on wireless security protocols (WEP, WPA and WPA2/802.11 i)." *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*. IEEE, 2009.

[13] Zheng, Yuliang. "An authentication and security protocol for mobile computing." *Mobile Communications*. Springer US, 1996. 249-257.

[14] Zou, X., Dai, Y. S., & Ran, X. (2007). "Dual-Level Key Management for secure grid communication in dynamic and hierarchical groups", *Future Generation Computer Systems*, *23*(6), 776-786.

[15] Holz, Ralph, et al. "The SSL landscape: a thorough analysis of the x. 509 PKI using active and passive measurements." *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 2011.

[16] Bruneo, Dario, et al. "Communication paradigms for mobile grid users." *Cluster Computing and the Grid, 2003. Proceedings. CCGrid 2003. 3rd IEEE/ACM International Symposium on*. IEEE, 2003.

[17] K Vedder, "Security Aspects orMObile Communication," Computer Security and fndustrrol Crypfography-State of the Art and Evolution, Springer-verloa. May. 1991, DD. 193-210.

[18] Anastasi, Giuseppe, Alberto Bartoli, and Francesco Spadoni. "A reliable multicast protocol for distributed mobile systems: Design and evaluation." *Parallel and Distributed Systems, IEEE Transactions on* 12.10 (2001): 1009-1022.

[19] Lin, Yue-Hsun, et al. "Spate: Small-group pki-less authenticated trust establishment." *Proceedings of the 7th international conference on Mobile systems, applications, and services*. ACM, 2009.

[20] Dai, Weiqi, et al. "Enhancing data trustworthiness via assured digital signing." (2012): 1-1.

[21] Zhou, Yun, Xiaoyan Zhu, and Yuguang Fang. "MABS: Multicast authentication based on batch signature." *Mobile Computing, IEEE Transactions on* 9.7 (2010): 982-993.

[22] Lam, Kwok-Yan, et al. "Enhancing Grid security infrastructure to support mobile computing nodes." *Information Security Applications*. Springer Berlin Heidelberg, 2004. 42-54.

[23] Patel, Vasant. "Key Sizes Selection in Cryptography and Security Comparison between ECC and RSA." (2000).

[24] G Chaddoud, K Martin, "Distributed certificate authority in cluster-based ad hoc networks", Wireless Communications and Networking Conference **2**, 682–688 (2006).

[25] D Dhillon, TS Randhawa, M Wang, L Lamont, "Implementing a fully distributed certificate authority in an OLSR MANET", Wireless Communications and Networking Conference **2**, 682–688 (2004).

[26] W Rao, SH Xie, "Merging clustering scheme in distributed certificate authority for ad hoc network", IET International Conference on Wireless, Mobile and Multimedia Networks, 1–4 (2006).

[27] ME Elhdhili, LB Azzouz, F Kamoun, "A totally distributed cluster based key management model for ad hoc networks", Third Annual Mediterranean Ad Hoc Networking Workshop (2004).

[28] Y Dong, AF Sui, SM Yiu, VOK Li, LCK Hui, "Providing distributed certificate authority service in cluster-based mobile ad hoc networks", Computer Communications **30**, 2442–2452 (2007).

[29] DY Lee, HC Jeong, "An efficient certificate management for mobile ad-hoc network", 5th International Conference on Mobile and Wireless Networks, 355–364 (2006).

[30] C Zouridaki, BL Mark, K Gaj, RK Thomas, “Distributed CA-based PKI for mobile ad hoc networks using elliptic curve cryptography”, First European PKI Workshop: Research and Applications EuroPKI, 232–245 (2004).

[31] Liu, Yunhao, et al. "Special Issue on Cyber-Physical Systems (CPS)—Part II."IEEE Transactions on Emerging Topics in Computing 1.2 (2013): 203-206.

[32] Tornos, Jose Luis, Jose Luis Salazar, Joan Josep Piles, Jose Saldana, Luis Casadesus, Jose Ruiz-Mas, and Julian Fernandez-Navajas. "An eVoting System Based on Ring Signatures." Network Protocols and Algorithms 6, no. 2 (2014): 38-54.

[33] Deka, Ganesh Chandra, ed. Handbook of Research on Securing Cloud-Based Databases with Biometric Applications. IGI Global, 2014.

[34] Alcaraz, Cristina, and Javier Lopez. "WASAM: A dynamic wide-area situational awareness model for critical domains in Smart Grids." Future Generation Computer Systems 30 (2014): 146-154

[35] Chu, Cheng-Kang, Sherman SM Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng. "Key-aggregate cryptosystem for scalable data sharing in cloud storage." Parallel and Distributed Systems, IEEE Transactions on 25, no. 2 (2014): 468-477.

[36] Zissis, Dimitrios, and Dimitrios Lekkas. "Addressing cloud computing security issues." Future Generation computer systems 28, no.3(2012):583-592.

[37] Yan, Ye, Yi Qian, Hamid Sharif, and David Tipper. "A survey on cyber security for smart grid communications." Communications Surveys & Tutorials, IEEE14, no. 4 (2012): 998-1010.

[38] Khan, Abdul Nasir, ML Mat Kiah, Samee U. Khan, and Sajjad A. Madani. "Towards secure mobile cloud computing: A survey." Future Generation Computer Systems 29, no. 5 (2013): 1278-1299.

[39] Li, Depeng, Zeyar Aung, John R. Williams, and Abel Sanchez. "Efficient authentication scheme for data aggregation in smart grid with fault tolerance and fault diagnosis." In Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES, pp. 1-8. IEEE, 2012.

[40] Debiao, He, Chen Jianhua, and Hu Jin. "An ID-based client authentication with key agreement protocol for mobile client–server environment on ECC with provable security." Information Fusion 13, no. 3 (2012): 223-230.