IOSR Journal of VLSI and Signal Processing (IOSR-JVSP)
Volume 5, Issue 2, Ver. I (Mar. - Apr. 2015), PP 52-59
e-ISSN: 2319 – 4200, p-ISSN No. : 2319 – 4197
www.iosrjournals.org

Integrity and Confidentiality for Skypilot Port Communication

Majel Monisha.B[1], Jose Anand[2]
[1,2,] *(ECE, KCG College of Technology/ Anna University, India)*

Abstract: *Wireless communication offers the benefits of low cost, rapid deployment, shared communication medium, and mobility, while at the same time has many security and privacy challenges. Dynamic Encryption Scheme, when used between two parties of communication, the former packets are coded as retransmission sequence, where as the retransmitted packet is marked as "1" and the other is marked as "0." During communication, the retransmission sequence is generated at both sides to update the dynamic encryption key. If retransmission sequence is missed or misjudged it would prevent the adversary from achieving the keys. The basic idea of dynamic secret is that the legitimate users dynamically generate a shared symmetric secret key utilizing the inevitable transmission errors and other random factors in wireless communication. At Chennai Port Trust the confidential information such as trading, banking transaction are communicated using wireless medium which utilizes unlicensed frequency, thus demanding for the secure transfer of data .The current scheme does not give appreciable performance thus demanding for a better secure and integrated communication. The problem with data transmission is mitigated by using Elliptic Curve Cryptography (ECC) algorithm which is being used for encryption and decryption. No node in between can read or views the data. Any node in between, which tries to read this information will not be able to do so because, the information will be encrypted using ECC. Therefore communication is secured as the data cannot be viewed while it passes through the intermediate nodes. Hence by this scheme secure communication is assured for the SkyPilot Port Communication.*

Index Terms: *Elliptic Curve Cryptography*.

I. Introduction

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them. In a network environment, authorized users may access data and information stored on other computers on the network. The capability of providing access to data and information on shared storage devices is an important feature of many networks. In a networked environment, each computer on a network may access and use resources provided by devices on the network, such as printing a document on a shared network printer. Routing is the process of selecting paths in a network along which to send network traffic. A routing protocol specifies how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network the choice of the route being done is by routing algorithms. Secure routing algorithm reduces the loss or tampering of confidential data and it comes handy for the organizations whose data are to be kept from prying eyes. Secure routing algorithm reduces the loss or tampering of confidential data and it comes handy for the organizations whose data are to be kept from prying eyes. The proposed system is used where it need quick response to link breakage in active routes, loop-free routes maintained by use of destination sequence numbers and which is scalable to large populations of nodes.

The existing system uses AES for routing. The Advanced Encryption standard (AES) is a specification for the encryption of electronic data. Key size of 128, 192 or 256-bit long can be chosen for encryption and decryption. One of the drawbacks to public key encryption systems is that it needs relatively complicated mathematics to work, making it very computationally intensive. Encrypting and decrypting symmetric key data is relatively easy to do. In fact, many solid state drives, which are typically extremely fast, use symmetric key encryption internally to store data and are still faster than unencrypted traditional hard drives. The major disadvantage of AES is sharing of key; the biggest problem with symmetric key encryption is that way to get the key to the party with whom the data is being shared. Symmetric key encryption is particularly useful when encrypting own information as opposed to when sharing encrypted information. Another disadvantage is that more damage if compromised.When someone gets their hands on a symmetric key, they can decrypt everything encrypted with that key. When using symmetric encryption for two-way communications, this means that both sides of the conversation get compromised.

II. Related Works

The survey focused on various encryption schemes and dynamic key distribution strategies that could provide a secure communication between the nodes. In similar interest, various security attacks and key distribution schemes were analysed for various Adhoc network scenarios. The various symmetric and asymmetric encryption schemes in different wireless environment were under gone and the performance of these schemes are analyzed with various network parameters. Dynamic Key encryption scheme with ECC encryption algorithm is seen as suitable to provide secure and integrated communication in the Port Trust Scenario.

The Optimal Probabilistic Encryption [1] is the optimal solution for the cipher matrices which is obtained in order to maximize performance criterion J-divergence for Ally fusion centre (AFC), whereas ensuring that it is zero for the Eavesdropping fusion centre (EFC).This scheme has no communication overhead and minimal processing requirements making it suitable for sensors with limited resources. An innovative key management scheme [2] called random seed distribution with transitory master key (RSDTMK), which adopts the random distribution of secret material and a transitory master key used to generate pairwise keys. The main novelty of RSDTMK is the generation of pairwise keys based on randomly predistributed seeds, which are turned by a permutation function, and then are transformed in a key by a pseudorandom function, which employs a master key, deleted after a time-out period. The two identity-based secure distributed data storage (IBSDDS) schemes[3]. The file owner can decide the access permission independently without the help of the private key generator (PKG); For one query, a receiver can only access one file, instead of all files of the owner; Scheme is secure against the collusion attacks, namely even if the receiver can compromise the proxy servers, cannot obtain the owner's secret key. Two new IBSDDS schemes are proposed in standard model where, for one query, the receiver can only access one file, instead of all files. Bad Data Injection attack [4]is defined as a cyber-physical attack which is a combination of two aspects on the cyber side, modern attack techniques are exploited to intrude and inject bad data into the information system; On the physical side, attackers construct the bad data to bypass the traditional error detection in power systems. For cyber defense, the inherent properties of electrical parameter have not been concerned and for physical defense, the integrity and validity of power grid data cannot be ensured. The cyber-physical fusion is a better solution, which combines the features of cyber network and the physical models of power system. The public key infrastructure (PKI) solution [5] supports the trusted computing elements, including device attestation. Primary issue is the need for a cohesive set of requirements and standards for smart grid security. A secure data retrieval scheme [6] using Cipher text-policy attribute-based encryption (CP-ABE) for decentralized Disruption-tolerant network (DTN) where multiple key authorities manage their attributes independently. The inherent key escrow problem is resolved such that the confidentiality of the stored data is guaranteed even under the hostile environment where key authorities might be compromised or not fully trusted. The ordered bucketization (OB) [7] as a cryptographic object. In OB, plaintext space is divided into p disjoint buckets, numbered from 1 to p, based on the order of the coverage ranges. OB is quite useful in that a range query can be performed over encrypted data without the need to decrypt by attaching a bucket number to each ciphertext. The concept of dynamic secret [8] is applied to design an encryption scheme for smart grid wireless communication. Between two parties of communication, the previous packets are coded as retransmission sequence, where retransmitted packet is marked as "1" and the other is marked as "0." During the communication, the retransmission sequence is generated at both sides to update the dynamic encryption key. Any missing or misjudging in retransmission sequence would prevent the adversary from achieving the keys. This scheme can protect the users against eavesdropping by updating the dynamic encryption key with retransmission sequence in communication, even the attackers know the details of scheme and obtain the encryption key at some time; it is a light-weight encryption method with only simple operations , self-contained, that is, it is dynamically generated during the normal communication without additional traffic and control command.

III. Sky Pilot Communication

The flexible and scalable SkyPilot network technology can support concurrent data, voice, and video applications, mixed-use networks, and multiple tiers of service. Using a unique synchronous protocol and advanced beam switching antenna arrays, Active SkyPilot nodes automatically detect the presence of new neighbouring mesh nodes and fixed-wireless customer premise equipment (CPE). SkyPilot solutions enable unmatched scalability and performance for all broadband wireless applications by their various features such as Mesh Architecture, Automatic Link Discovery, Mesh Route optimization, Traffic Management, Bandwidth Scheduling, Transmission Coordination, Advanced Antenna Array, High Gain, Transmit Power, Sectorization & Adaptive Modulation and Embedded Security Features.

The SkyPilot wireless mesh architecture is specifically designed to maximize packet throughput, enable Quality of Service (QoS), and deliver high scalability while preserving the resiliency and flexibility of wireless mesh communications. Based on an innovative and unique protocol, the SkyPilot wireless mesh architecture

automatically manages multiple wireless mesh operations that would otherwise require specialized personnel or complex management systems.

The SkyPilot wireless mesh network is a low-latency, high-bandwidth radio system operating in the 5 GHz bands as a self-forming, self-balancing, and self-healing wireless mesh network. The intelligent, self-forming SkyPilot mesh technology manages traffic across the mesh network to mitigate interference, maximize available bandwidth, and support the prioritization of voice and data for improved Quality of Service performance. The SkyPilot network provides a range of services for fixed broadband access subscribers, roaming Wi-Fi users, public safety professionals, mobile municipal staff, and public works agencies. Each SkyPilot Gateway controls a subnetwork of associated SkyPilot Extenders and Connectors to provide coverage and capacity as needed. By deploying additional SkyPilot Gateways, a service provider can "inject" capacity into the network, extend network coverage, and enhance network reliability. Unlike a conventional point-to-multipoint base station, the SkyPilot Gateway is the foundation of a true mesh topology that delivers multi-hop versatility, dynamic re-routing in the event of node failure, and outstanding scalability. SkyPilot Extender products are elements of the SkyPilot network that act as a relay node of the SkyPilot network and provides Ethernet connectivity for client devices. SkyPilot Gateways and Extenders are also available in DualBand models. These models are available with integrated access points that allow for simultaneous wireless access to the SkyPilot wireless mesh network, using the 2.4 GHz band for public Wi-Fi connectivity. The SkyPilot Element Management System (EMS) provides SNMP-based network element management capabilities. The SkyPilot EMS manages SkyPilot network devices, providing control and monitoring capabilities over the network's physical and logical connectivity, implementing a Fault, Configuration, Performance, and Security (FCPS) network management administration model for the SkyPilot wireless mesh network.

IV. Project Description

In order to overcome the disadvantages of Advanced Encryption standard (AES) algorithm in the existing system, Elliptic Curve Cryptography (ECC) algorithm is being used for encryption and decryption in the proposed system. Therefore communication is secured as the data cannot be viewed while it passes through the intermediate nodes. In this system AODV routing protocol is used for transmission of data. It is a reactive protocol that requests the route only when it needs. It does not require nodes to maintain routes to the destination that are not communicating. First, a route request is sent and a table is maintained for each node, in which all the route replies are stored. Then the AODV algorithm chooses a path in random from the table and transmits the data. Therefore communication is secured as the data cannot be viewed while it passes through the intermediate nodes.

1. Architecture

The direct communication between Skypilot gateway node to client node is entertained or the communication between gateway through the Skypilot extender node to client is allowed but the communication between two client nodes is denied. The Fig 1 shows the overall architecture of the SkyPilot Communication.

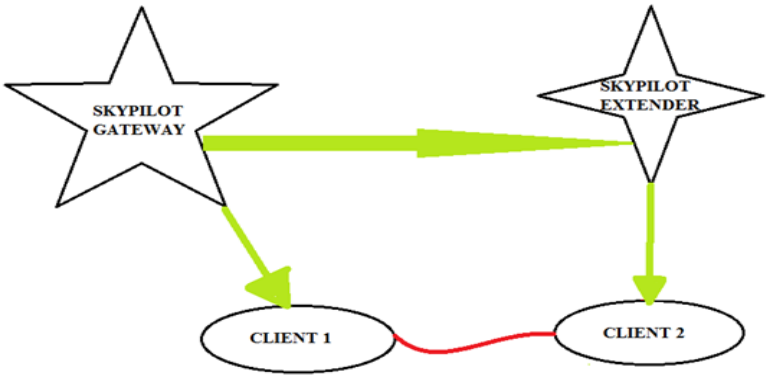

Figure 1 Skypilot Architecture Diagram

2. Flow of cryptographic scheme

The work flow of Elliptical Curve Cryptography has three major work are Compress, Encrypt, and Hide the message. User can perform all three works simultaneously or individually. For encryption of data user has to enter private key and that key will accessed by Algorithm to make any Plain Text to Cipher Text. If message should hide Click on encrypt check box , If file should encrypt ,Click on compress check box. Select master file and output file. If file should compress the same time User can retrieve the Cipher Text to Plain Text by entering the same key.

The Fig 2 illustrates detailed design of encryption and decryption process. The nodes hold the source, destination, sequence number and next hop details being stacked in it. The source node undergoes the route discovery process which includes the request packet broadcasting, reply packet forwarding, random path selection and route maintenance. The ECC implementation includes the encryption and decryption of the data packet between the intended nodes.

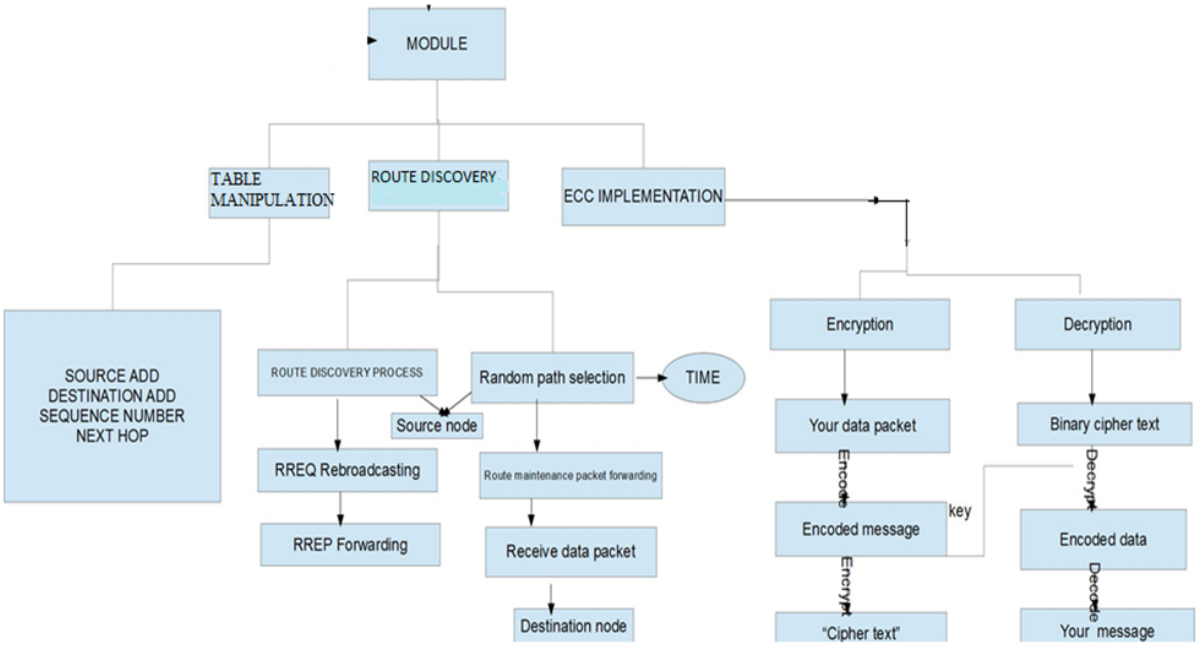

Figure 2 Detailed design diagram

3. Sequential flow of the cryptography process

The sender initiates the route discovery process by sending the request packets in the network, once the request packet reaches the intended destination it sends back reply packet through same path. The path is selected by randomization process and the data is encrypted using the ECC algorithm and send over the network. This encrypted holds the data with key. If the send cipher key matches with the private key then the data is decrypted successfully.

4. Algorithm

The algorithms used for the proposed system are

- ECC Algorithm
- Randomization Process

4.1 ECC Algorithm

Elliptic Curve Cryptography algorithm is used for secure data transmission which uses key generation technique. The sender will encrypt the message with receiver's public key and the receiver will decrypt its private key:

$$Q = d * P$$

generates the public key ,Where d = The random number that is selected within the range of (1 to n-1).P is the point on the curve. Q is the public key , d is the private key

Encryption

Let 'm' be the message that we are sending

Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 - (n-1)].

Two cipher texts will be generated let it be C1 and C2:

$$C1 = k*P$$

$$C2 = M + k*Q$$

C1 and C2 will be sent.

Decryption

To get back the message 'm' that was sent :

$$M = C2 – d * C1$$

M is the original message that was send.

Work Done

$$M = C2 – d * C1$$

'M' can be represented as 'C2 – d * C1′

$$M=C2 – d * C1$$
$$=(M + k * Q) – d * (k * P)$$
$$(C2 = M + k * Q \text{ and } C1 = k * P)$$
$$= (M + k * (d * P)) – d * k *P$$
$$= M+(k*d*P)-(d*k*p)$$
$$(Q=d*P)(\text{Cancelling out } k * d * P)$$
$$= M (\text{Original Message})$$

4.2 Randomization Process

Randomization algorithm is used to select a random path. Random path is selected from the various available paths in the route table. Use of randomization algorithm prevents attackers from easily predicting the path. Let Ni denotes node in a network, t be Destination node, W^{Ni} be an estimated minimal cost to send a packet to t. Nexthop be the next node along the Minimal cost path to the destination node . C_t^{Ni} be a set of node candidates for the next hop. H_t^{Ni} be a set of tuples, records the history of packets from Ni to t.

V. Result And Analysis

The Fig 3 shows the Log In window of RADWIN manager software. The logging process is done with the aid of particular and unique IP address assigned to each gateway, repeater and sink SkyPilot nodes and the specific password assigned to each operator in the sophisticated environment to make sure that authorized persons are logging in the RADWIN manager.

Figure 3 Log In Process

The Specific Class C addressing is utilised for the assignment of IP address to each node connected in this SkyPilot environment, the changes to be made in the tool can be carried out by the installer part only not by the operator and observer criteria processes.The Fig 4 shows the sharing of link password for the secure transaction process. During the establishment of secure communication the exchange of passwords is demanded. When accessing a service, the user and the service provider have a common interest in making sure that the user, the subscription, or the device accessing the service is a genuine one, and that the transaction performed cannot be denied. Authentication is a means to achieve such trust and a secure protocol is then used for functions such as authorization and reporting of usage statistics.

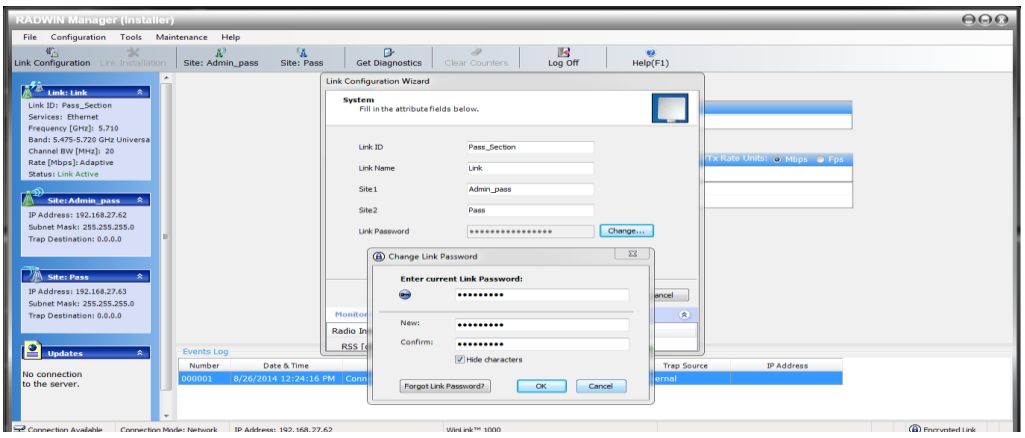

Figure 4 Sharing Of Password

The Fig 5 shows the window indicating Link ID, Link name, Site positions and password to ensure secure communication. When Port sender send personal information to their customers or to another port gate via digital exchanges, they may need to secure this exchange with a specific secret, which will allow only the targeted person to be able to actually read the information. Features such as control session login/logout, derivation of keys from sessions, a simplified data protection function, multiple key containers, key import/export, a common method for accessing and defining properties of keys, and the lifecycle control of credentials such enrollment, selection, and revocation of credentials with a focus enabling the selection of certificates for signing and encryption.

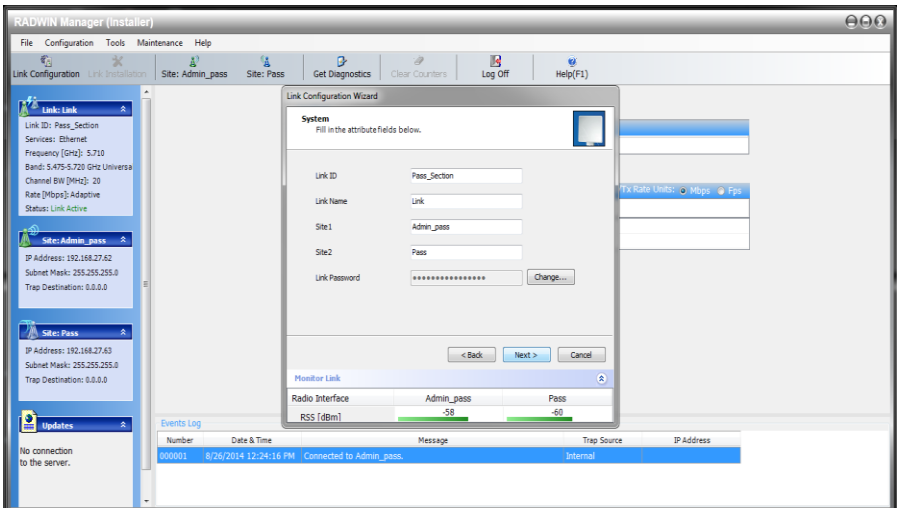

Figure 5 Secure Link Password

The Fig 6 shows the Receiver Signal Strength , throughput and the active E1 ports. The transmission and reception rate of the particular node is observed to get the information about their speed and analyse whether any packet dropping is done and also to ensure that data is transferred between the intended nodes in an encrypted link.

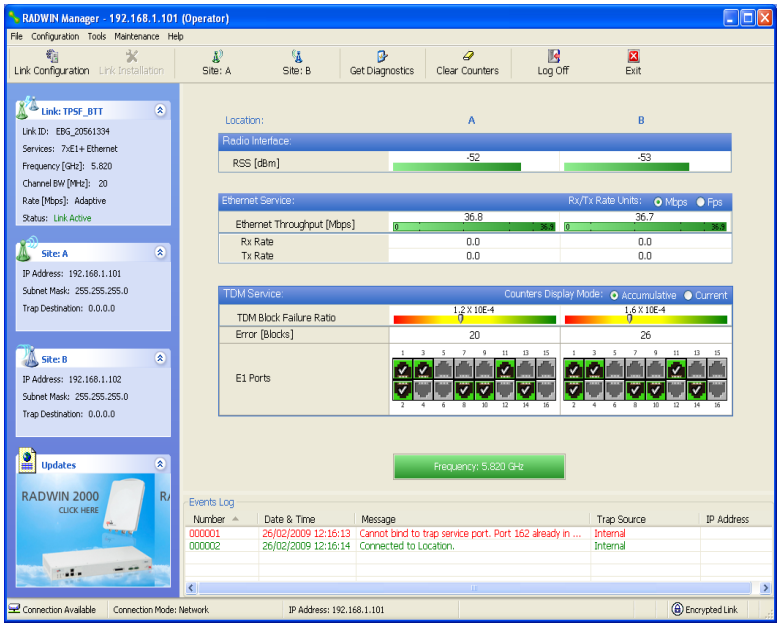

Figure 6 E1 Port Manager Window

The Fig 7 shows the window for changing Link password after attaining the threshold value under dynamic scheme. Given a key pair, data encrypted with the public-key can only be decrypted with its private key; conversely, data encrypted with the private-key can only be decrypted with its public key. This characteristic is used to implement encryption and digital signature in the network. Digital signature is a mechanism by which a message is authenticated i.e. proving that a message is effectively coming from the intended sender to ensure that secure communication is carried out.

Figure 7 Password Changing Window

The Fig 8 shows the alternate link password window which is supplied with the product and the encrypted link at bottom right corner shows the secure link being established. The one time symmetric-key has been used to encrypt the message. This key has been encrypted using the recipient's public-key. Only recipient can decrypt Symmetric Key and use it to decrypt the message.

Figure 8 Secure Link

VI. Conclusion And Future Work

Elliptical Curve Cryptography (ECC) is a public encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. The main problem of conventional public key cryptography systems is that the key size has to be sufficient large in order to meet the high-level security requirement, which results in lower speed and consumption of more bandwidth, the solution is Elliptic Curve Cryptography system. It is mainly used in the resource constrained environments, such as ad-hoc wireless networks and mobile networks.

There is a trend that conventional public key cryptographic systems are gradually replaced with ECC systems. As computational power evolves, the key size of the conventional systems is required to be increased dramatically .The mathematic background of ECC is more complex than other cryptographic systems such as Geometry, abstract algebra, number theory. ECC provides greater security and more efficient performance than the first generation public key techniques in Mobile systems and Systems required high security level. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers.

For elliptic-curve-based protocols, it is assumed that finding the discrete logarithm of a random elliptic curve element with respect to a publicly-known base point is infeasible. The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an RSA-based system with a large modulus can be achieved with a much smaller elliptic curve group.

Using a small group reduces storage and transmission requirements. ECC algorithm is proposed and implemented using RADWIN. The performance of AES and ECC algorithms is evaluated. From the presented result it is evident that ECC offers better performance than AES algorithm. ECC has advantage over the AES in terms of speed and key size. In future the work may be extended by including the schemes and techniques over different types of data such as sound and image.

References

[1]. Komninos,E. Philippou and A. Pitsillides, Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures, IEEE Communications Surveys & Tutorials,2013.

[2]. Filippo Gandino, Bartolomeo Montrucchio, and Maurizio Rebaudengo ,Key Management for Static Wireless Sensor Networks With Node Adding,IEEE Transactions On Industrial Informatics, Vol. 10, No. 2, May 2014, pp 1133 – 1143.

[3]. Jinguang Han, Willy Susilo, and Yi Mu, Identity-Based Secure Distributed Data Storage Schemes, IEEE Transactions On Computers, Vol. 63, No. 4, April 2014, pp 941 - 953.

[4]. Dai Wang, Xiaohong Guan, Ting Liu, Yun Gu, Yanan Sun, Yang Liu ,A Survey on Bad Data Injection Attack in Smart Grid, Ministry of Education Key Lab for Intelligent Networks and Network Security, School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, Shaanxi, China, IEEE 2013.

[5]. Anthony R. Metke and Randy L. Ekl, Security Technology for Smart Grid Networks, IEEE Transactions On Smart Grid, Vol. 1, No. 1, June 2010, pp 99 – 107.

[6]. Reza Soosahabi, Mort Naraghi-Pour,Dmitri Perkins, and Magd A Bayoumi,Optimal Probabilistic Encryption for Secure Detection in Wireless Sensor Network,IEEE Transactions On Information Forensics And Security, Vol. 9, No. 3, March 2014, pp 375 – 384.

[7]. Younho Lee, Secure Ordered Bucketization, IEEE Transactions On Dependable And Secure Computing, Vol. 11,No. 3, May-June 2014, pp 292 – 303.

[8]. Ting Liu, YangLiu, YashanMao, Yao Sun, Xiaohong Guan, Weibo Gong, and Sheng Xiao , A Dynamic Secret-Based Encryption Scheme for Smart Grid Wireless Communication, IEEE Transactions On Smart Grid, Vol. 5, No. 3, May 2014, pp 1175 – 1182.

[9]. Xudong Wang, and Ping Yi, Security Framework for Wireless Communications in Smart Distribution Grid, IEEE Transactions On Smart Grid, Vol. 2, No. 4, December 2011, pp 809 – 817.

[10]. JunbeomHur and KyungtaeKang ,Secure Data Retrieval for Decentralized Disruption-Tolerant Military Networks, IEEE/ACM Transactions On Networking, Vol. 22, No. 1, February 2014, pp 16 – 26.

[11]. WeixiaoMeng , Ruofei Ma and Hsiao-Hwa Chen , A Survey on Smart Grid Neighbourhood Area Networks ,IEEE Network, Vol. 25, No. 5, Feburary 2014 pp. 24 – 32.

[12]. Ye Yan, Yi Qian, Hamid Sharif and David Tipper , A Survey on Cyber Security for Smart Grid Communications, IEEE Communications Surveys & Tutorials, Vol. 14, No.4, Fourth Quarter 2012, pp 998 – 1009.