# Improving Performance of Wireless Sensor Network By Using ECC

Ms. Shazia Islam (Associate professor), Deepshri Dewangan
Department Of Computer Science Engineering, RCET Kohka Bhilai

***Abstract* –In this paper we have presented a Public Key Infrastructure for wireless sensor networks. The scheme tries to solve the problem of security in WSN by the use of public key cryptography as a tool for ensuring the authenticity of the base station. In the proposed scheme, we tries to increase performance of the WSN by using ECC method which is based on the Discrete mathematics. ECC is more complex than other cryptographic systems and its performance is efficient than the first generation schemes. Our evaluations demonstrate that the proposed scheme is secure and requires less memory space than the public key cryptography based incentive schemes which improves efficiency.**

***Keywords- WSN, Cryptography, ECC, PKI, Random Oracle Model.***

## I. INTRODUCTION

A Wireless Sensor Network (WSN) are spatially distributed autonomous sensors to monitor physical or environmental.
The WSN is built of "nodes"- from a few to several hundreds or even thousands, where each and every node is connected to one or many sensors. Wireless sensor network (WSN) consist of sensor nodes which are tiny, low power, a microcontroller, a circuit and battery or an embedded form of energy harvesting. To provide security for WSN it is necessary to perform encryption and decryption between communicating nodes A lot of the schemes are very effective in terms of security, but it is very complex or difficult to apply in real world sensor network environment. Regarding the feature of sensor node, in this paper we propose a scheme Discrete logarithm cryptography (DLC) which is another part of cryptography which provide security by difficulty in solving logarithmic equations over large finite groups.

## II. LITERATURE SURVEY

In 2002 B. Lynn , proposed a method for integrating authentication with encryption in the Boneh-franklin IBE system. The modification were influence the performance, the authenticated encryption and decryption algorithms are faster than the corresponding non-authenticated versions because the proposed Authenticated-Encrypts faster than plain Encrypts because there is one less exponentiation and no point of multiplication.
In 2003 Sakai and Kasahara proposed a new ID-Based scheme for cryptosystem. In this paper, the author proposed the efficient method for a class of ID based cryptosystems with signature and the having multiple centres. This technique also provided the authentication along with the encryption scheme simultaneously. The proposed method in this paper is able to reduce the number of computations of the pairing for the verification of ID based signature.
In other related work Boneh and Boyen in 2004 gave two proficient Identity based encryption based technique of Public key Encryption that is provably selective identity secure without the random oracle model. Encryption does not require bilinear map computation and decryption requires at most two in both the systems. Without random oracle, this development extends to give an efficient selective identity secure Hierarchical IBE (HIBE). It is similar to the Gentry-Silverberg system, but able to prove security without using random oracles.
Another ID based encryption scheme is proposed by Yao. et.al. in 2004. Forward secrecy is the central idea of this algorithm in which the compromise of long-term keys does not compromise past session keys and therefore past communications. Throughout the life time of the system, secrete keys are updated at regular intervals in this model. This technique fulfils the following HIBE requirements:-

1. Dynamically User association: New user able to join the present available hierarchy and receive the secrete key at any time from their parents.
2. Joining-time-oblivious Encryption: The encryption is independent on the knowledge of the existing hierarchy history of ancestors. If the sender knows the current time and ID-tuple of the receiver along with the public parameters of the system can encrypt the message.
3. The scheme should be forward-secure key.
4. Autonomous refreshment of the secrete keys.

In 2005 a new IBE based encryption scheme is proposed by Boneh et.al. In this approach, the encryption is based on Identity based Encryption specifically encryption is based on hierarchal identity based encryption of constant size cipher text. In HIBE system, the Cipher texts are always just three group elements but in this system decryption requires only two bilinear map computations and illustrated that how private keys can be further compressed to sub-linear size and also describe an efficient mechanism for encrypting to the future.
In 2006 Jing-Shyang Hwu et. al. proposed an ID-based cryptosystem . This system provides security enhancements to the mobile applications as recipient used the mobile phone number as a public key then the system is sending an ID-based encrypted short

message and it is exactly same as sending a normal short message. It is the desired feature for mobile applications such as bank or stock transactions.

In 2008 Boldyreva et. al. in their paper explain the use of ID Based Encryption in broadcasting of messages. The proposed target system has goal of broadcast encryption such that, it is able to prevent revoked users from secrete information access during broadcasting process. The proposed the improvement of the previous available solution as a new way to moderate the limitation of IBE with regards to revocation. They build the system on already developed fuzzy IBE by Sahai and waters. on ID based key management in Mobile Ad Hoc Networks . In this Paper, they emphasis on the Mobile Ad hoc Networks i.e. MANET. How can we safe and secrete communication on MANET. They discussed the strengths, weaknesses of Different approaches and providing a comparison between their main features.

In 2009, Butler et. al. also used the ID-Based encryption in P2P Systems . Because of their efficiency, scalability and reliability the structured peer-to-peer (P2P) systems have grown very much. A unique identifier is assigned to each user and object by this system. However the proposed technique allow an adversary to carefully select user IDs and/or simultaneously obtain many pseudo identities—ultimately leading to an ability to disrupt the P2P system in very targeted and dangerous ways. In this paper, they proposed new ID assignment protocols based on identity-based cryptography. There three protocols can be described as:-

1. Protocol 1: A fully decentralized ID-based assignment scheme
2. Protocol 2: A centralized scheme in which a single host plays the role of both ID authority and bootstrap node.
3. Protocol 3: An approach that retains the separation of duties in a decentralized model at a low cost by using a hybrid of identity-based and symmetric key cryptography.

In 2009 YUGUANG FANG et.al, describe and developed another application for wireless network. In his article, they concentrated on the heterogeneous network and its services. They discussed a novel approach to addressing the issues of security and admitted the effectiveness of security in wireless networks by ID based cryptography system. The authors also proposed a novel security solution based on location. The basic idea of their location-based approach is, name a node with both an ID and its location and thus bind the ID and location together. With this scheme i.e. location based ID-PKC approach, this technique can defend against the aforementioned security attacks effectively.

In 2010 F. Richard Yu et. al. gave a hierarchical Identity Based Key Management Scheme in Tactical Mobile Ad Hoc Networks . The authors proposed the technique of key management in distributed hierarchal network in which the nodes of hierarchy can get their keys updated either from a threshold sibling or from their parents. The technique of dynamic node selection formulated as a stochastic problem and the proposed scheme can select the best nodes to be used as PKGs from all available ones considering their security conditions and energy states. The technique had objectives to simultaneously improve the security of network and maximizing the lifetime of network. Simulation results show that the proposed scheme can decrease network compromising we propose a distributed hierarchical key management scheme to select the best nodes to function as the PKG taking into account the nodes' security conditions and energy states. Therefore, the computation and implementation complexity of the proposed scheme are reduced dramatically.

Recently in 2012, Zhiguo Wan also apply the ID-Based encryption scheme in his article. They proposed a routing protocol for mobile ad-hoc network and called it USOR (Unobservable Secure On-Demand Routing Protocol). They propose an protocol USOR which is efficient for privacy preserving by employing group signature based anonymous key establishment. The unobservable routing protocol uses two phases to execute. First, an anonymous key establishment process is performed to construct secret session keys. After that an unobservable route discovery process is then executed to find a route to the destination. Then an unobservable route discovery routing protocol process is executed to find a route to the destination. The proposed USOR is the first unobservable routing protocol, more on USOR is that it is excellent and best routing protocol for ad hoc networks, which achieves stronger privacy protection over network communications.

In chen- huang WUuses Certificateless Public Key Cryptography (CLPKC)as a new paradigm was introduced by Al-Riyami and Paterson in Asiacrypt 2003, which set aside the use of certificate to ensure the authenticity of the user's public key in the public key cryptography and also overcomes the key escrow problem in the identity-based public key cryptography. They give the first precise definition and security notions for Self-Generated-Certificate Digital signature. The first concrete signature scheme which is provably secure under the CDH assumption. Although the efficiency of the proposed scheme is not very efficient, the first concrete scheme itself is of much interest.

## III. PROBLEM IDENTIFICATION

As a brief analysis of the existing scheme, It provide both secrecy and digital signatures and its security is based on the integer factorization problem. . Among them, the most largely use is public key infrastructure, which provides security services such as scalability, confidentiality, integrity, but they are not able to perform well, and complexity is high. It seems that it is not energy saving since a handshake between each pair of sensors is too cost consuming concerning the amount of exchanged data. The Existing system shows security and accuracy of the system is not sufficient now a day. The system uses a large number of keys for encryption and decryption of information after this the data requires a large amount of memory, which causes :Slow working, Wastage of memory, Easy to crack. To overcome with this problem by Implementation of ECC using projective coordinates which shows considerable improvement in efficiency compared to the affine coordinate implementation. This improvement in efficiency is achieved because the elimination of multiplicative inverse operation in point addition and doubling otherwise it cost considerable processor cycles. If the irreducible polynomials are either trinomial or pentanomial which causes reduction in binary

field to run much faster. The ECC (Elliptic Curve Cryptography) algorithm solve the memory problem because ECC works with the small size key. ECC is another field in cryptography. In public key cryptography each user taking part, in the communication generally have a pair of keys. Implementation of ECC using projective coordinates which shows considerable improvement in efficiency compared to the affine coordinate implementation.

## IV. METHODOLOGY

### 4.1 ECC (Elliptic Curve Cryptography)

Elliptic Curve Cryptography(ECC) is a subset of DLC, where the discrete logarithm solution over an equation (plane curve). Discrete logarithm cryptography (DLC) uses mathematical calculation where security is provided by difficulty in solving logarithmic equations over large finite groups. The elliptic curve equations can over finite groups on prime fields ( Fp ) or binary fields (p;m). For prime fields, where p is a large/odd prime> 3, curves are of the form

$$y2 = x3 + a * x + b. \quad \text{Eq. 4.1}$$

For binary fields, the order of the field is a power of 2, the curves are of the form

$$y2 + X * Y = x 3 + a * x2 + b \quad \text{Eq. 4.2}$$

ECC keys can be smaller than RSA keys, because it is believed that the solution to a discrete logarithm is fundamentally more complex than the factorization of large integers. In the proposed method we use ECC to improve the performance of WSN. The inherent security is in the difficulty of recovering this key via factorization of large integers. It is already proved that RSA keys should be a minimum of 1024 bits where ECC uses 160 bit as key.

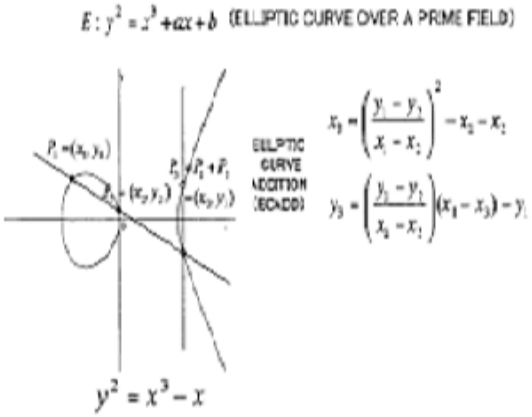


***Figure 4.3 Elliptic curve over a Prime Field***

### 4.2 Discrete Logarithm Problem

Given a prime *p*, generator *g*, and an element *y* in group G, find the integer *x*, such that

$$y=gx \pmod p \quad \text{Eq. 4.3}$$

The fastest algorithm known for solving discrete logarithm problem is still GNFS which has a subexponential running time.

#### 4.2.1 Discrete Logarithm

The logarithm function is the inverse of exponentiation. An analogous function exists for modular arithmetic. The logarithm of a number is defined to be the power to which some positive base (except 1) must be raised in order to equal the number. That is for base x and for a value y.

$$y=x^{\log_x(y)} \quad \text{Eq. 4.4}$$

The properties of the logarithms include:

$$\log_x(1)=0$$
$$\log_x(x)=1$$
$$\log_x(xy)= \log_x(y)+\log_x(z) \quad \text{Eq. 4.5}$$
$$\log_x(y^2)= r * \log_x(y) \quad \text{Eq. 4.6}$$

Consider a primitive root a for some prime number p (the argument can be developed for nonprimes as well). Then we know that the powers of a from 1 through (p-1) produce each integer from 1 through (p-1) exactly once. We also know that any integer b satisfies

$$b= r(\text{mod } p)$$

For some r, where 0<=r<=(p-1)

By the definition of modular arithmetic. It follows that for any integer b and a primitive root a of prime number p, we can find a unique exponent I such that

$$b=a^i(\text{mod } p)$$

where 0<=i<=(p-1)

This exponent i is referred to as the **discrete logarithm** of the number b for the base a(mod p).

This demonstrates discrete logarithm.

## V. Results

### 5.1 Network Simulator 2.35 (NS2)

Network Simulator is Discrete event and Packet level Simulator, where the advance of time depends on the timing of events which is maintained by a scheduler and an event is an object in the C++ hierarchy. In addition to this, an event with an unique ID, a scheduled time and the pointer to an object that handles the event. The Figure 5.1 shows Architecture of Network Simulator.

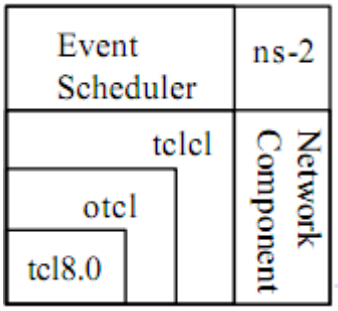


***Figure 5.1 NS2 Architecture***

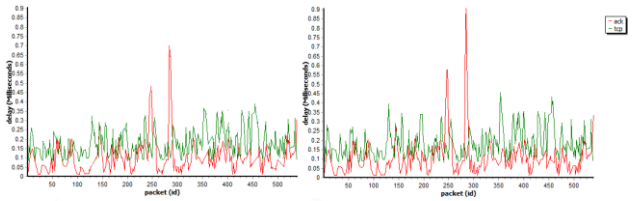

*Figure 5.7 Comparison graph of 30 node for RSA and ECC.*

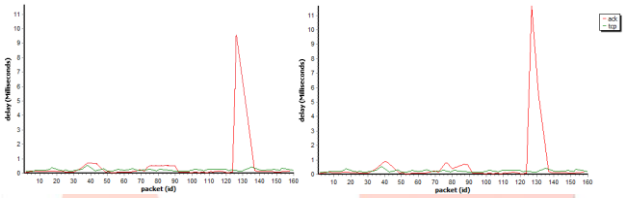

*Figure 5.8 Comparison graph of 40 node for RSA and ECC.*

*Table 5.1 Comparable Key Sizes in Terms of Computational Effort For Cryptanalysis*

| ECC -Based Scheme (*Size of n in bits*) | RSA (*modulus size in bits*) |
|---|---|
| 112 | 512 |
| 160 | 1024 |
| 224 | 2048 |
| 256 | 3072 |
| 384 | 7680 |
| 512 | 15360 |

## VI. CONCLUSION

The proposed scheme covers there keying property and considers nodes addition and revocation from the view point of secured key establishment. 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. The packet delay in RSA is less as compared to ECC but ECC improves efficiency of WSN using small key size. Using a small group reduces storage and transmission requirements. It can be enhanced to digital signature in our proposed scheme. Hence, we conclude that Digital Signature Algorithm scheme is more suitable to be implemented in WSN.

## VII. REFERENCES

[1] Hua guo,Xiyong zhangy,Yi Muz,zhoujun Li. *An efficient certificateless Encryption scheme* in the standard model ,IEEE 2009.
[2]Mohamed Hamdy Eldefrawy1,Muhammad Khurram Khan1,Khaled Alghathbar1.*A KEY Agreement Algorithm with Rekeying for Wireless Sensor Networks using public key cryptography*, IEEE 2010.
[3]Mohamed Elsalih,Mahmoud and Xuernin Shen. *Secure cooperation Incentive Scheme with limited use of public key cryptography for multi-hop wireless network*, IEEE 2010.
[4]Chen-huang,Fujian Putian. *Self Generated-certificate Digital signature*, IEEE 2010.
[5]Darpan Anand,Vineeta Khemchandani,Rajendra K. Sharma. *Identity-Based Cryptography Techniques and applications* , IEEE 2013.
[6]Zhang yu. *The sheme of public key Infrastructure for improving wireless sensor network security*, IEEE 2012.
[7] Md. Iftekhar Salam, Pardeep Kumar, HoonJae Lee. *An Efficient Key Pre-distribution Scheme for Wireless Sensor Network Using Public Key Cryptography* ,IEEE 2010.

[8] G. Swapna,P. Vasudeva Reddy,T. Gowri,Efficient. *Identity Based Multi-Proxy Multi-Signcryption Scheme Using Bilinear Pairings over Elliptic Curves*,IEEE 2013.
[9] Alexandra Boldyreva, Hideki Imai, *Life Fellow, IEEE*, and Kazukuni Kobara. *How to Strengthen the Security of RSA-OAEP*, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 56, NO. 11, NOVEMBER 2010.
[10] Mohamed Elsalih Mahmoud and Xuemin (Sherman) Shen .*Secure Cooperation Incentive Scheme with Limited Use of Public Key Cryptography for Multi-hop Wireless Network,* IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.
[11] Seung-Hyun Seo, Xiaoyu Ding and Elisa Bertino .*Encryption Key Management for Secure Communication in Smart Advanced Metering Infrastructures* ,IEEE 2013.
[12] Yevgeniy Dodis , Kristiyan Haralambiev Daniel Wichs, *Cryptography Against Continuous Memory Attacks*, 2010 IEEE 51st Annual Symposium on Foundations of Computer Science.
[13] Kuo-Yi Chen,Chin-Yang Lin,Ting-Wei Hou. *The low-cost secure sessions of access control model for distributed applications by public personal smart cards*, 2011 IEEE 17th International Conference on Parallel and Distributed Systems.
[14] Xin Zhou, Xiaofei Tang. *Research and Implementation of RSA Algorithm for Encryption and Decryption*, 2011 The 6th International Forum on Strategic Technology