ISSN: 2278-0181
Vol. 1 Issue 3, May - 2012

Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network

[#1]Asha Rani Mishra
asha1.mishra@gmail.com
[#2]Mahesh Singh
mahesh100nucs@gmail.com
#Advanced Institute of Technology & Management, Palwal

***Abstract* —This paper discusses different issues of Wireless Sensor Network (WSN) and the relevance of the Elliptic curve y cryptography. Security in WSN is a greater challenge in WSN due to the processing limitations of sensor nodes and nature of wireless links. Extensive use of WSNs is giving rise to different types of threats. To defend against the threats proper security schemes are required. Traditionally security is implemented through hardware or software and is generally achieved through cryptographic methods. Limited area, nature of links, limited processing, power and memory of WSNs leads to strict constraints on the selection of cryptographic techniques. Elliptic Curve Cryptography (ECC) is the best candidate due to its smaller key size. High security despite of smaller key size results in area and power efficient crypto systems.**

Keywords: Public Key Cryptography, ECC, WSN, Attacks

I. INTRODUCTION

Wireless sensor network consists of a large number of sensor nodes that are able to collect and disseminate data in areas where ordinary networks are unsuitable for environmental and/or strategic reasons. [1] They play an important role in a wide variety of applications covering critical military surveillance applications to forest fire monitoring and building security monitoring in the near future. In these networks, a large number of sensor nodes are deployed to monitor a vast field, where the operational conditions are most often harsh or even hostile. Since these networks are usually deployed in remote places and left unattended, they should be equipped with security mechanisms to defend against attacks such as node capture, physical tampering, eavesdropping, denial of service, etc. Unfortunately, traditional security mechanisms with high overhead are not feasible for resource constrained sensor nodes. The researchers in WSN security have proposed
various security schemes which are optimized for these networks with resource constraints.

Various components of a sensor node are shown in Figure 1. Each node has the capability to sense the data from the environment perform some computation and communicate with the other nodes in the network. Once a sensor node is deployed, the network can keep operating only until the battery power is sufficient.

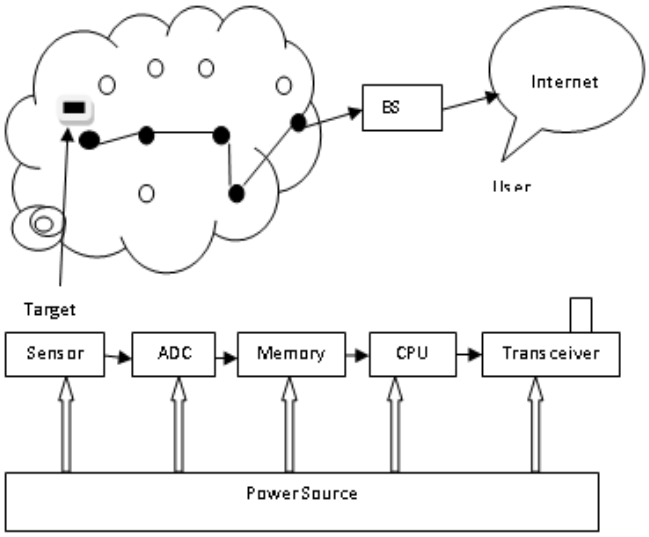

Figure 1. Component of the Sensor Node

Each sensor node is capable of only a limited amount of processing. But when coordinated with the information from a large number of other nodes, they have the ability to measure a given physical environment in great detail. Wireless sensor networks consists of high number of nodes, are deeply

deployed, has frequently changing topology due to failure or mobility and has no global identification on as contrast to adhoc networks[8].These differences takes a different approach while trying to achieve secure data transfer in WSN. Since Sensor devices are limited in terms of computation, storage and energy encryption techniques require more resources. Various new cryptographic methods both symmetric and asymmetric are being proposed that achieved more security taking into consideration the constrained capabilities of sensor network.

In wired data networks there is a centralized control which is used to help nodes to establish secure and reliable communication, but there is no trusted authority in WSN because of sensor node's limitations, that's why cryptographic algorithms must be selected properly Enabling security in WSNs is very scenario reliant in all its approaches.

The operations of sensor nodes are very sensible to potential attacks on various layers. A number of solutions that discussed this issue have been proposed so far. In next section we will discuss the WSN architecture and characteristics. Section III and IV deal with security requirements and key management issues in WSNs, respectively. Section V will present Elliptic Curve Cryptography. Section VI concludes the paper and proposes some future work. Section VI and VII discusses suitability of ECC in WSNs and key exchange mechanism using ECC.

II.ARCHITECTURE AND CONSTRAINTS OF WSN

A sensor network is composed of ten to thousands of the sensor nodes which are placed in the wide area. In the sensor network all the nodes are communicating with each other either directly or through the other nodes. In the sensor network one or more nodes among them are treated as sink. All the other nodes in the network send the sense data to the sink. Wireless sensor network architecture includes both a hardware platform and an operating system designed specifically to address the needs of wireless sensor networks.

Figure 2 shows the architecture of a Wireless Sensor Network (WSNs). Small circle shows the sensor nodes and a filled circle shows the gateway through which data is sent to the main system.

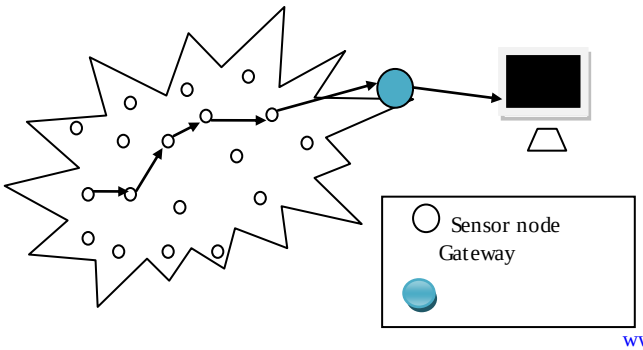

Figure 2: Architecture of Wireless Sensor Network

Various constraints of WSN are: Energy constraints, memory limitations, unreliable communication, and higher latency in communication.

III. SECURITY ISSUES AND CHALLENGES IN WSN

Security issues in wireless sensor network can be broadly classified into five categories: cryptography, key management, secure routing, secure data aggregation, and intrusion detection.

Key Management: Key is used for secure communication either in case of Symmetric key or asymmetric key algorithms. For the implementation of various security schemes. Key distribution is not typical in WSNs, but constraints such as small memory capacity make centralized keying techniques impossible. Straight pairwise key sharing between every two nodes in a network is not suitable for large growing networks. A security scheme in WSNs must use efficient and reliable key distribution for secure communication between all relevant nodes.

Secure Routing: These protocols are deals with how a node sends message to other nodes or a base station. A major challenge is to verify authentication of the communication broadcast by the base station. Existing methods often uses public key cryptography which has high computational overhead making them infeasible in WSNs. The goal of a secure routing protocol is to ensure the integrity, authentication, and availability of messages.

Data Aggregation: Data aggregation focus on removing duplicate data which can result while aggregating information this is very much essential for energy-constrained WSN. Aggregators are vulnerable to attack when it is comprised by injecting false data in the sensor network. Another possible attack is to compromise a sensor node and inject forged data through a sensor node. Without authentication, the attackers can fool the aggregators into reporting false data to the base station. Secure data aggregation requires authentication, confidentiality, and integrity. Moreover, secure data aggregation also requires the cooperation of sensor nodes to identify the compromised sensors.

IV. SECURITY REQUIREMENTS IN WSN

Security is a critical issue for a variety of sensor network applications. There exist a large number of Vulnerabilities in WSNs like intrusion, interception, modification and fabrication which leads to several threats to a WSN protocol [10]. Conceptually, the threats could be listed from different

perspectives. The previous research have listed threats according to how attacks are accomplished, on which layer of the communication stack they are realized, and finally whether the malicious node becomes a member of the network during the attack or not. Various Security issues in WSN can be broadly classified as: Cryptography, key management, secure routing, Data aggregation and Intrusion detection as shown in Figure 3.

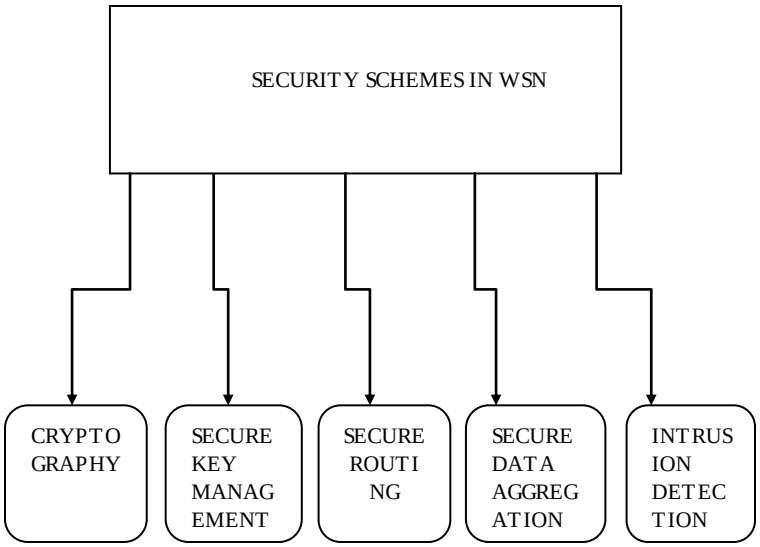

Figure 3: Various Security schemes in WSN

In order to secure WSNs, there are security objectives that provide security services, such as Confidentiality which confidential information should never be revealed, authenticity is needed in sensor network for each sensor node and base station to ensure that the data received was sent by a trusted entity. This type of authentication is needed during the clustering of sensor node in WSN and integrity of information should always assured so that information will not be altered in any unexpected manner,

Various cryptographic solutions have been proposed till now based on symmetric and asymmetric algorithms. Symmetric algorithms provide confidentiality while fulfilling the power, space and memory requirements of WSN. [7] However they fail to provides authenticity and proper key exchange mechanisms which is achieved through public key cryptography.

A. Security principles in WSN

Various security principles in WSN [3][4] can be categorized as:

- Data Confidentiality: This ensures that only authorized sensor nodes are able to access the contents of messages.
- Data Authentication: This confirms sender's identity i.e. data sent is from correct source.
- Data Integrity: Data is not changed in an authorized manner. It is achieved by digital signature and encryption.
- Data Freshness: This ensures that no old data is replayed. This security requirement is needed where key strategies in the network design. Keys needed to be changed time to time and there is a distribution delay for the keys.
- Data Availability: Make sure that services offered by WSN or by a single node must be available whenever necessary. Denial of Service attacks and sensor node capturing make weak availability of sensor network Also additional computation, communication consumes additional energy and if no more energy exists, the data will no longer be available. A single point failure will be introduced if using the central point scheme. This greatly threatens the availability of the network. The requirement of security not only Security issues in wireless sensor network can be broadly classified into five categories: cryptography, key management, secure routing, secure data aggregation, and intrusion detection. affects the operation of the network, but also is highly important in maintaining the availability of the whole network.
- Time Synchronization: Most sensor network applications depend on some structure of time synchronization. An individual sensor's radio in order to preserve power it may be turned off for periods of time. Also, sensors may want to compute the end to-end delay of a packet as it moves between two pairwise sensors. A more collaborative sensor network possibly will require group synchronization for tracking applications, etc.

- Secure Group management: Sensor nodes it should be flexible, resilient, self-organizing, adaptive and corrective in regards to security measures.

- Secure Localization: The exchange of the information about the precise location of the sensor nodes while communicating with the authenticated neighbors is critical in WSN to maintain the integrity of WSN Services.

V .VARIOUS THREATS AND ATTACKS IN WSN

Wireless environment is more susceptible to threats and attacks as compared to wired due to the susceptibility of

unguided medium. The architectural aspect of wireless sensor networks i.e. having centralized base station or sink makes easier employment of security measures as compare to wireless adhoc networks. [9] Attacks in WSN can be considered against security mechanism and routing mechanism.

A. Layered based attacks and security issues

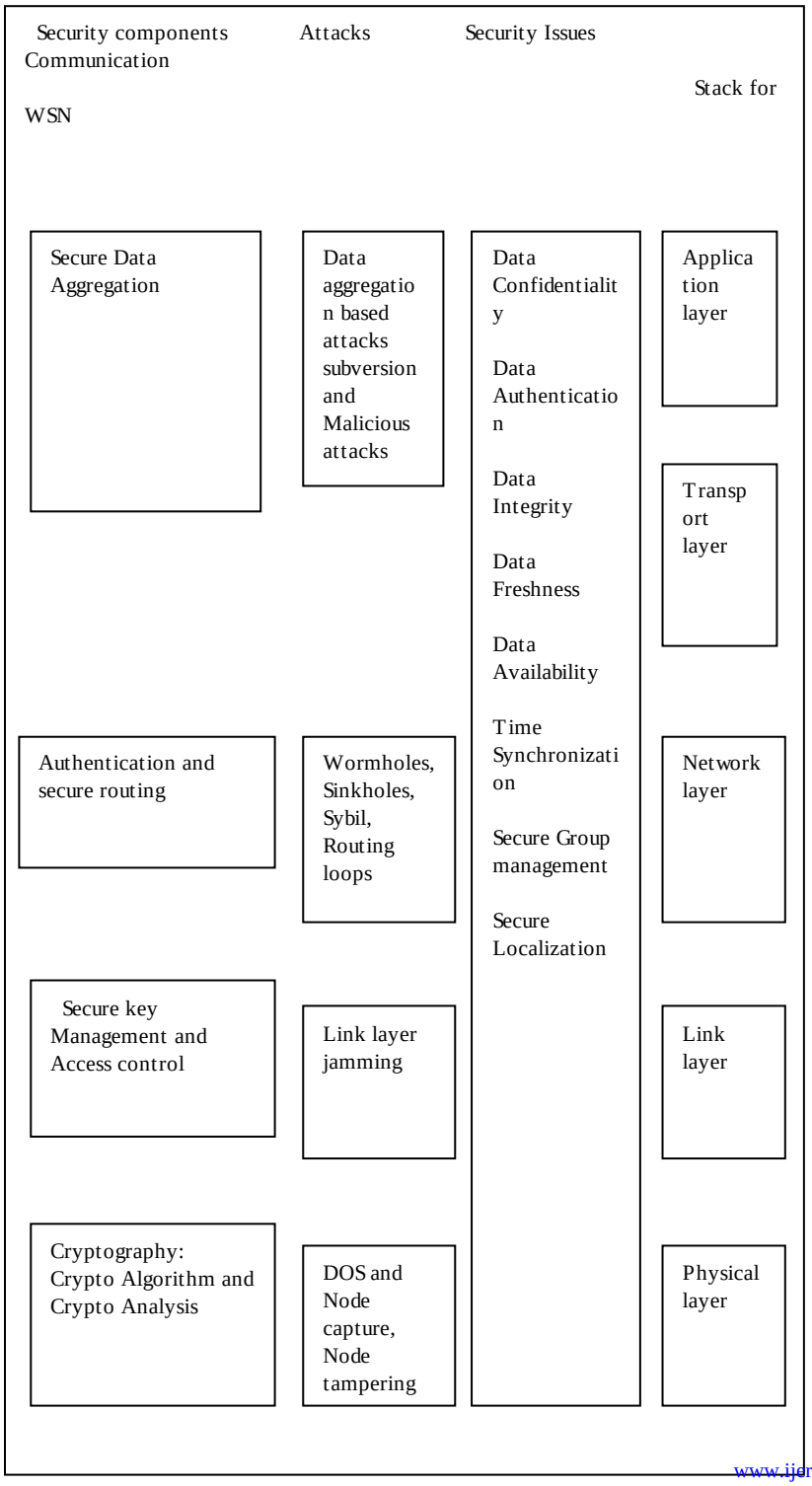

Figure 4: Architecture of WSN Security

VI. KEY MANAGEMENT AND KEY MANAGEMENT SCHEMES IN WSN

Key management and Key establishment is an important issue in wireless sensor networks [5].There are two approaches for it - Centralized and Distributed. In the previous approach there is prior assignment of a unique key to every node and uses the base station as central source of trust while in later approach each sensor node is able to authenticate its neighbors or a subset of them. Most of the traditional techniques in wireless sensor networks are unsuitable because of low power in fact that typical key exchange techniques use asymmetric cryptography, as well called public key cryptography. Usually, Diffie-Hellman which is one of public-key protocols is used to key establishment. In the public-key protocols, data is encrypted with the public key and decrypted only with the private key so it is necessary to maintain both public and private keys. In symmetric protocols data encrypt and decrypt with a single shared key so it has key exchange problem. Secure key distribution of keys securely to communicating hosts is significant problem since pre-distributing the keys is not always possible. Asymmetric cryptosystems were not considered as an option for constrained devices due to their extensive mathematical calculations. These calculations require large amount of space and power resources seen widespread use is also one of the most accessible illustrations of this principle in action.

An efficient key management scheme for WSN using ECC can be designed. A typical WSN can be assume as a combination of both large number of normal sensor nodes also known as cluster heads and small number of special nodes. Cluster nodes having more power computationally more capable than special nodes. Before the predistribution of the sensor nodes, key server based on ECDSA can be used to generate both public/private key pair.

V. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) is a public key cryptography. where each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user

knows the private key whereas the public key is distributed to all users taking part in the communication.

Public-Key cryptography (PKC) systems can be used to provide secure communications over insecure channels without exchanging a secret key. The most popular public-key cryptography systems nowadays are RSA and Elliptic Curve Cryptography (ECC). Elliptic curve cryptography (ECC) was proposed in 1985 by Neal Koblitz and Victor Miller.

The mathematical operations of ECC is defined over the elliptic curve $\mathbf{y2 = x^3 + ax + b}$, where $\mathbf{4a^3 + 27b^2 \neq 0}$. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number [6]. The public key is obtained by multiplying the private key with the generator point G in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. The security is based on the difficultly of a different problem, which is called the Elliptic Curve Discrete Logarithm Problem (ECDLP).

A. Elliptic Curve Discrete Logarithm Problem (ECDLP)

Let P and Q be two points on an elliptic curve such that k*P = Q, where k is a scalar. Given P and Q, it is computationally infeasible to obtain k, if k is sufficiently large. k is the discrete logarithm of Q to the base P. Hence the main operation involved in ECC is point multiplication. i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve. No sub exponential algorithm to solve ECDLP is known.

VI. ECC IN WIRELESS SENSOR NETWORK

Wireless sensor networks (WSNs) are rapidly growing in their importance and relevant to both the research community and the public at large. Security is critical for a variety of sensor network applications. There exist a large number of security vulnerabilities in WSNs, which cause many kinds of attacks. Wireless sensor networks (WSN) are representative networks using these tiny and low-power sensor devices. Two types of Communications occur in sensor networks: one is between end nodes, and the other is between end node and base station (BS). Since not only the resource restriction in conventional wireless networks but security critical applications, security functions are very important issues in WSN.

Main proposes of security in the WSN is not massage encryption but prevent from changing the contents of the massage or disguising sender. It is the most important mutual authentication in order to defend from disguise of sender. Because of limited energy, many researches have done in order to maximize a lifetime of networks

Implementations of symmetric key algorithms are ideal for resource constrained environments of WSN. But symmetric algorithms can only provide confidentiality. Public key cryptosystems are resource hungry but are able to provide a lot more than confidentiality. ECC got the attention of the researchers due to its smaller key size. It offers practical implementation possibilities in resource constrained devices. Previous work shows public key algorithms are a good choice for use in wireless sensor networking, and that the benefits of smaller ECC keys and certificates will be significant in improving energy conservation. ECC is used to achieve authentication and key management.

ECC and some related work about wireless communication that is based on elliptic curve cryptographic techniques. Presently, RSA algorithm demands a key length be not less than 1024 bits for long term security and we know that ECC with only a 160 bits modulus offers an the same level of security as RSA with 1024-bit modulus shown in Table1.Thus, using ECC in wireless communication system is extremely recommended. The key distribution and storage problems, which are typical in secret-key settings it is solved by the ECC cryptography conception.

ECC KEY SIZES (Bits)	DSA KEY SIZE (Bits)	RSA KEY SIZES (Bits)	KEYSIZE RATIO (Bits)	Comment
160	512	1024	1:6	Short period security
256	2048	3072	1:12	Medium period security
384	3072	7680	1:20	Long term security

Table1: Key size Comparison for ECC and RSA

VII. SECURITY MECHANISM USING ECC

Due to openness of wireless sensor networks, secure communication between nodes is necessary.

The Elliptic Curve Cryptography(ECC)] is based on algebraic concepts related with elliptic curves over finite fields Fp or F2m. Elliptic Curve encryption and decryption system requires appoint G and an elliptic group E_q (a, b)as a parameters.

Encryption using ECC

To encrypt and send a message Pm to B, A chooses a random positive integer k and produces the cipher text Cm as given by equation consisting of the pair of points.

$Cm = [k*G, Pm + k*P_B]$

Here A has used B's public key P_B.

Decryption using ECC

To decrypt the cipher text, B multiples the first point in the pair by B's private key n_B and subtracts the result from the second point as shown by equation.

$$Pm + k*P_B - n_B(k*G) = Pm + k(n_B*G) - n_B(k*G) = Pm$$

A key exchange between users A and B can be explained as following steps:-

- A select an integer $n_A < n$ as A's private key.
- A generates a public key $P_A = n_A * G$ which is a point in $E_q(a, b)$.
- B select an integer $n_B < n$ as B's private key.
- B generates a public key $P_B = n_B * G$ which is a point in $E_q(a, b)$.
- .Public keys are exchanged between A and B.A generates the secret key $K = n_A * P_B$ and B generates the secret key $K = n_B * P_A$

VI. CONCLUSION

And this, in the end, is the reason ECC is an appropriate choice to achieve security in Wireless sensor networks (WSN). ECC is an excellent choice for asymmetric cryptography in portable constrained devices. 1024-bit RSA key provides the same level of security as a160-bit elliptic curve key. The advantages can be achieved from smaller key sizes including storage, speed and efficient use of power and bandwidth. The use of shorter keys means lower space requirements for key storage and quicker arithmetic operations. These advantages are essential when public-key cryptography is applied in constrained devices, such as in mobile devices or RFID. In brief, ECC based algorithms can be easily included into existing protocols to get the same backward compatibility and security with smaller resources.

REFERENCES

[1] Guo Xiao Wang, Zhu Jianyong, Analysis and Design of Energy-oriented Security Protocols for Wireless Sensor Networks,"2011

[2] Hero Modares Rosli Salleh Amirhossein Moravejosharieh, Overview of security issues in Wireless Sensor Network,"2011

[3] E.Yoneki and J. Bacon ,"A survey of Wireless sensor Network technologies,"2005.

[4] J.P Walters, et al." Wireless Sensor network security: A survey, "2007

[5] Hero Modares Rosli, Salleh Amirhossein ,Moravejo sharieh, Wireless Network Security Using Elliptic Curve Cryptography," 2011

[6] Moncef Amara and Amar Siad," Elliptic curve Cryptography and its applications", 2011

[7] Guo Xiaowang, Zhu Jianyong, Research o"n Security Issues in Wireless sensor networks,"2011

[8] Yong Wang, Garhan Attebury, and Byrav Ramamurthy A Survey of security issues in wireless sensor networks, University of Nebraska-Lincoln

[9]Pathan,A-S.K.,Alam,M.,Manowar,M.,and Rabbi,F.,"An efficient Routing Protocol for Mobile Ad Hoc networks with Neighbour Awarness and Multicasting.,Proc IEEE E-Tech Karachi I,2004,PP.97-100

[10] C.P Fleeger,Security in Computing,3rd edition,prentice_Hall Inc.NJ.2003