Data Protection Using Hierarchical and Dynamic Elliptic Curve Cryptosystem in Wireless Sensor Network

[1]O. Sheela, [2]T. Samraj Lawrence, [3]D. C. Joy Winnie Wise

Department of CSE, Francis Xavier Engineering College, Tirunelveli, Tamilnadu, India

Abstract- In Wireless Sensor Networks (WSN), because of the absence of physical protection, the wireless connections are prone to different type of attacks. Therefore, security is a measure concern in WSN. Hence to provide security, Hierarchical and Dynamic Elliptic curve cryptosystem (HiDE) scheme is proposed. To serve a large amount of sensors, HiDE provides a hierarchical cluster-based framework consisting of a Backbone Network and several Area Clusters. Many Gateways connected together to form a Backbone Network. Sensor Nodes in the WSN are group together based on area to form an Area Cluster (AC). Area Cluster consists of Cluster Head (CH), Sensor Nodes and the Gateway. For energy efficient data transmission, Low Energy Adaptive Clustering Hierarchy (LEACH) is used to select the Cluster Head dynamically. The Cluster Head collects the data from the Source Node and transmit it to the Destination through the Gateway (GW) in the Backbone Network. However, limited by the coverage of Gateway, Source Gateway may not be directly linked with the Destination Gateway in a single hop, so needs to hop through other Gateways to reach the Destination Area Cluster. Data encryption using Elliptic Curve Cryptography (ECC) provides high security with small key size than RSA. Key management includes key computation, key exchanges, and data encryption and decryption. Cluster-based cryptographic mechanism provides efficient energy utilization of sensor nodes along with security and low message overhead. Thus, HiDE can protect the confidentiality of sensitive data with low computation overhead, and keep appropriate network performance for Wireless Sensor Network.

Keywords - Elliptic Curve Cryptography, Low Energy Adaptive Cluster Hierarchy, Wireless Sensor Network, Hierarchical Cluster, Data Protection.

I. INTRODUCTION

Wireless sensor networks (WSNs) comprise a large number of spatially distributed small autonomous devices (called sensor nodes) cooperatively monitoring environmental conditions and sending the collected data to a command center using wireless channels [15]. Because of the size and cost of sensor nodes there is a constraint on energy, memory, computation speed and bandwidth. Most of the applications of WSN needs secure communication. Because of the absence of the physical protection and the unattended deployment wireless communication and sensor nodes are prone to different type of attacks such as: impersonation, masquerading, spoofing and interception etc. Hence, a security mechanism in WSN is an important concern. Different security mechanisms in WSN are described in [16] and [17]. For implementing key management in WSN, it is important to select appropriate cryptographic methods. Cryptographic methods should meet the constraints of sensor nodes in WSNs. These cryptographic methods could be evaluated by code size, data size, processing time, and power consumption. Security mechanisms can be implemented by using public key cryptography or symmetric key cryptography. Most important public key algorithms include RSA, and Elliptic Curve Cryptography (ECC). In RSA to implement security operations thousands of multiplication instructions are performed, which is time consuming. It was found that encryption and decryption operations in RSA usually take on the order of tens of seconds [18]. Recent studies have shown that it is feasible to apply public key cryptography to sensor networks by selecting proper algorithms and associated parameters. Most of the literatures gives emphasis on RSA and ECC algorithms. Researchers are more attracted towards ECC, because it provides same level of security with much smaller key size. For example, RSA with 1024 bit key provides an accepted level of security whereas ECC with 160 bit key provides same level of security. The RSA private key operation limits its use in sensor nodes. ECC has no such problem because both the public key and private key operation use the same point multiplication operations.

II. RELATED WORKS

In [4], Haythem Hayouni, Mohamed Hamdi, Tai-Hoon Kim discussed about Encryption Schemes in Wireless Sensor Networks. As Wireless Sensor Networks (WSN) continues to grow, so does the need for effective security mechanisms. Enhancing the efficiency of these networks requires more security to provide integrity, authenticity and confidentiality of the data flowing through the network. Encryption is one of the most common tools used to provide security services for WSNs. There has been an enormous research potential in the field of encryption algorithms in WSNs. Algorithms, protocols, and implementation consist the main aspects the security specialist should consider to assess the efficiency of the protection approaches. It reviews the most significant approaches that have been proposed to provide encryption-based security services for WSNs. It also emphasize on the weaknesses of the approaches.

The Rivest-Shamir-Adleman (RSA)-based public key solution is also used to protect data privacy [14]. However, few works can provide solutions for strong data confidentiality and low message overhead simultaneously.

In [7], Kristin Lauter discussed about the advantages of Elliptic curve cryptography for Wireless security. It provides an overview of elliptic curves and their use in cryptography. The focus is on the performance advantages to be obtained in the wireless environment by using elliptic curve cryptography instead of a traditional cryptosystem like RSA. Specific applications to secure messaging and identity-based encryption are discussed.

In [5], Kamlesh Gupta, Sanjay Silakari discusses about ECC over RSA for Asymmetric Encryption. Cryptography is used to transmit the data securely in open network. ECC is a when compared to RSA and discrete logarithm systems, is a better option for the future. For this reason ECC is such an excellent choice for doing asymmetric cryptography in portable devices right now. The smaller ECC keys it turn makes the cryptographic operations that must be performed by the communicating devices to be embedded into considerably smaller hardware, so that software applications may complete cryptographic operations with fewer processor cycles, and operations can be performed much faster, while still retaining equivalent security. This means, in turn, reduced power consumption, less space consumed on the printed circuit board, and software applications that run more rapidly make lower memory demands. In brief, for communication using smaller devices and asymmetric cryptosystem, ECC is needed.

In [9], Ramesh K and Somasundaram K discussed about cluster head Selection algorithms in Wireless Sensor Network sensor nodes. In Wireless Sensor Network, life time is the most critical parameter. Many researches on these lifetime extension are motivated by LEACH scheme, which by allowing rotation of cluster head role among the sensor nodes tries to distribute the energy consumption over all nodes in the network. Selection of cluster head for such rotation greatly affects the energy efficiency of the network.

The existing system is the security of the data communication is provided through RSA. RSA is a public key cryptography. The data is encrypted using the public key and it is decrypted using the private key. It uses 1024bit key. Data are directly sent and received through the Gateway. Each data element is encrypted and only the users with the appropriate decryption keys can decrypt the data. It is a centralized architecture. The main disadvantage of the existing system is message overhead occurred due to centralized architecture. Since RSA uses 1024 bit key, it needs high energy for computation.

III. HIERARCHICAL ARCHITECTURE FOR DATA PROTECTION

In the proposed system, Hierarchical and Dynamic Elliptic Curve Cryptosystem is used. To overcome message overhead, Hierarchical structure is proposed. To serve a large amount of sensors, Hierarchical and Dynamic Elliptic Curve Cryptosystem (HiDE) provides a hierarchical cluster-based framework consisting of a Backbone Network and several Area Clusters. Many Gateways connected together to form a Backbone Network. Sensor Nodes in the WSN are group together based on area to form an Area Cluster (AC). Area Cluster consists of Cluster Head (CH), Sensor Nodes and the Gateway. For energy efficient data transmission, Low Energy Adaptive Clustering Hierarchy (LEACH) is used to select the Cluster Head dynamically.

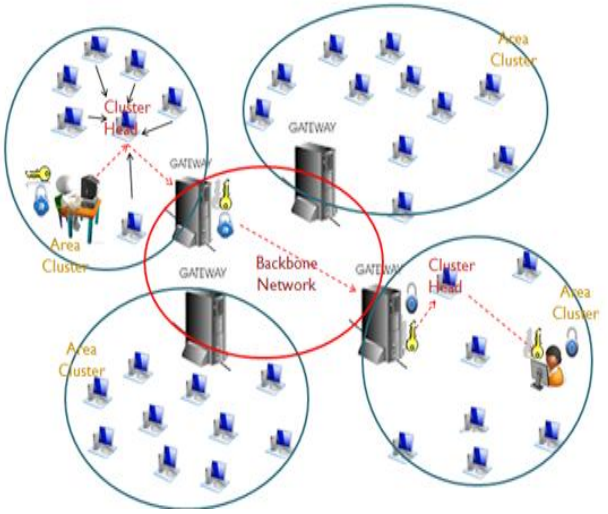

Figure 1 System Architecture

The Cluster Head collects the data from the Source Node and transmit it to the Destination through the Gateway (GW) in the Backbone Network Key management includes key computation, key exchanges, and data encryption and decryption. Cluster-based cryptographic mechanism provides efficient energy utilization of sensor nodes along with security and low message overhead. Thus, HiDE can protect the confidentiality of sensitive data with low computation overhead, and keep appropriate network performance for wireless sensor networks. The system architecture is shown in Figure 1.

The system implementation is done in three processes: Cluster Head Selection, Encryption Process, and Decryption Process.

A. Cluster Head Selection

In this module Cluster Head for both Source and Destination Area Cluster is selected by using the Low Energy Adaptive Clustering Hierarchy (LEACH) mechanism. By using LEACH, Cluster Head is selected dynamically. Sometimes the Source Node or the Destination Node itself acts as the Cluster Head.

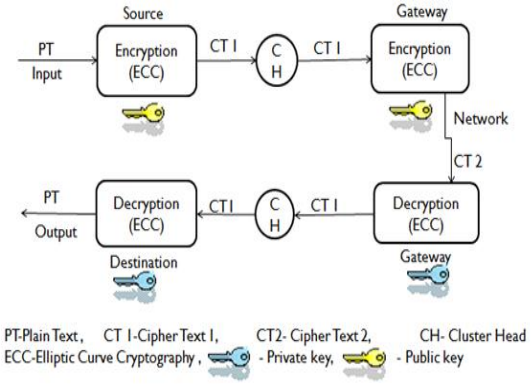

Figure 2 Encryption/Decryption Process

B. Encryption Process

The data is first encrypted in the source using the public key of the sender using Elliptic Curve Cryptography. Cluster Head (CH) collects the encrypted data from the source and transmits to the Gateway. In Gateway (GW) again the encrypted data is encrypted with the public key of the Gateway.

C. Decryption Process

The Gateway of the destination decrypts the data with the private key of the Gateway. Then Cluster Head gather the data from the Gateway. Cluster Head transmits the encrypted data to the destination. In destination, the encrypted data is decrypted using the receiver private key. The Cluster Head is automatically changed during the data transmission. Figure 2 shows the encryption and decryption process of the data using Elliptic Curve Cryptography. And the Cluster Head selection is done using LEACH dynamically.

Elliptical Curve Cryptography (ECC)

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. One of the main benefits in comparison with non-ECC cryptography (with plain Galois fields as a basis) is the same level of security provided by keys of smaller size. Elliptic curves are applicable for encryption, digital signatures, pseudo-random generators and other tasks. The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key. Elliptic Curve Cryptography (ECC) is a public-key cryptosystem just like RSA, Rabin, and El Gamal. Every user has a public and a private key. Public key is used for encryption/signature verification. Private Key is used for decryption/signature generation. Elliptic curves are used as an extension to other current cryptosystems. The equation of an elliptic curve is given as

$$y^2 = x^3 + ax + b$$

Key Generation

Key generation is an important part where generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key. Now, select a number 'd' within the range of 'n'. Using the following equation generate the public key

$$\mathbf{Q = d * P}$$

'd' is the random number that have selected within the range of (1 to n-1). 'P' is the point on the curve. 'Q' is the public key and'd' is the private key.

Encryption

Let 'M' be the message that are sending. It is necessary to represent this message on the curve. All the advance research on ECC is done by a company called Certicom. Randomly select 'k' from [1 – (n-1)]. Two cipher texts will be generated let it be C1 and C2.

$$\mathbf{C1 = k*P}$$

$$\mathbf{C2 = M + k*Q}$$

C1 and C2 will send.

Decryption

To get back the message 'M' that was send,

$$\mathbf{M = C2 – d * C1}$$

M is the original message that has sent.

Proof

To get back the message,

M = C2 – d * C1

'M' can be represented as 'C2–d*C1′

C2–d *C1 = (M + k * Q) – d * (k * P) (C2 = M + k * Q and C1 = k * P)

= M + k * d * P – d * k *P (canceling out k * d * P)

= M (Original Message)

The primary benefit promised by ECC is a smaller key size, reducing storage and transmission requirements, i.e. that an elliptic curve group could provide the same level of security afforded by an RSA-based system with a large modulus and correspondingly larger key: for example, a 256-bit ECC public key should provide comparable security to a 3072-bit RSA public key.

Low Energy Adaptive Clustering Hierarchy (LEACH)

Sensor nodes typically use irreplaceable power with the limited capacity, the node's capacity of computing, communicating, and storage is very limited, which requires WSN protocols need to conserve energy as the main objective of maximizing the network lifetime. An energy-efficient communication protocol LEACH, employs a hierarchical clustering done based on information received by the BS. The BS periodically

changes both the cluster membership and the cluster-head (CH) to conserve energy.

The threshold function is defined as

$$T(n) = \begin{cases} \dfrac{p}{1-p\left(r \bmod \left(\frac{1}{p}\right)\right)} & if\, n \in G \\ 0 & otherwise \end{cases}$$

Where n is the given node, P is the a priori probability of a node being elected as a Cluster Head, r is the current round number and G is the set of nodes that have not been elected as Cluster Heads in the last 1/P rounds. Each node during Cluster Head selection will generate a random number between 0 and 1. If the number is less than the threshold (T (n)), the node will become a Cluster Head.

IV. RESULTS

The data send by the sender is first encrypted using ECC. Then it can be collected by the Cluster Head in the Area Cluster. It can be send to the Gateway (GW). The data is again encrypted in GW using ECC for the second time as shown in Figure 3.

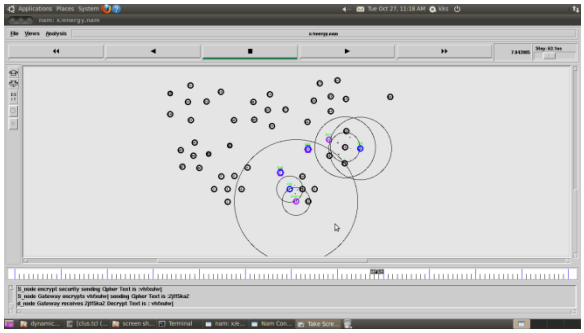

Figure 3 Data Encryption using ECC

The Cluster Head is altered dynamically during data transmission as shown in Figure 4.

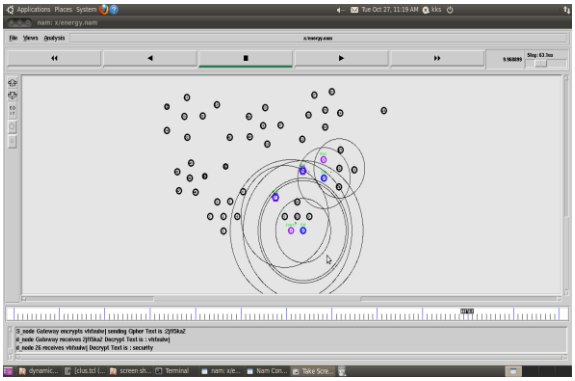

Figure 4 Alterations in Cluster Head

The Destination Area Cluster receives data through the Gateway which is connected to the Backbone Network. The dynamically selected Cluster Head receives the data from the Gateway and transmit it to the receiver. The data get decrypted using ECC is received by the receiver as shown in the figure 5.

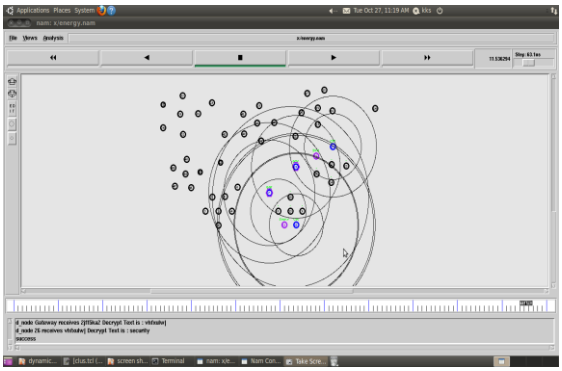

Figure 5 Data Decryption using ECC

The packet delivery ratio of the data encryption using both the existing RSA and the proposed ECC is shown in the Figure 6. It shows that the packet delivery rate of data is more in ECC than the RSA.

In Figure 7, the comparison of the throughput of both RSA and ECC algorithm

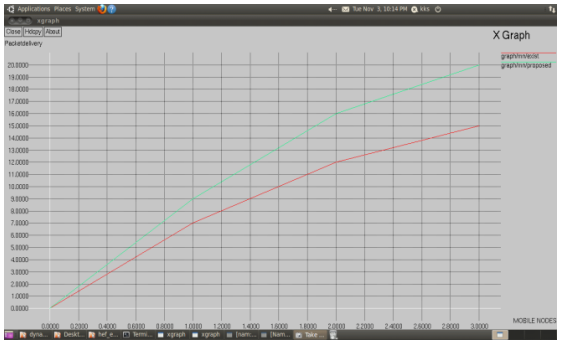

Figure 6 Comparison of Packet Delivery

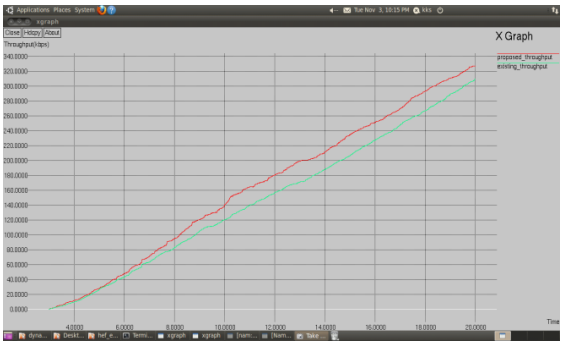

Figure 7 Comparison of Throughput Graph

is shown as graph. It shows that the throughput is high for ECC than the RSA algorithm used for encryption and decryption of data.

V CONCLUSION AND FEATUREWORK

In the proposed system, security for the data transmission is provided using Elliptic Curve Cryptography (ECC) which provides high security than the traditional RSA with smaller key size. Computation is also less because the use of the ECC with smaller key size. Energy need for computation is also less, which lead to low energy consumption in sensor nodes. Simulation results shows that the proposed system

provide high security, low computational complexity than the existing RSA. Thus, the Cluster based Cryptographic mechanism; Hierarchical and Dynamic Elliptic Curve Cryptosystem provide high security for data transmission and it is also highly energy efficient.

The future plan is to develop a trust and reputation management system to monitor the behavior of nodes and identify security attacks in advance. Also implement the protocol for data and key encryption. Moreover, it is plan to implement it in large scale sensor networks to evaluate overall message throughput and latency. It can protect the confidentiality of sensitive data with low computation overhead, and keep appropriate network performance for wireless sensor networks. Also doing the same process to do at only time for encrypt and decrypt, it will help to minimization of time and delay. Also the data will be sending secure.

REFERENCES

[1] Babu Karuppiah A. and Rajaram S. (2012), 'Energy Efficient Encryption Algorithm for Wireless Sensor Network', International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 3.

[2] Banta Singh Jangra and Vijeta Kumawat (2012), 'A Survey On Security Mechanisms and Attacks in Wireless Sensor Networks', International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 3.

[3] Chin yang Henry Tseng, Shiau-Huey Wang, and Woei-Jiunn Tsaur (2015), 'Hierarchical and Dynamic Elliptic Curve Cryptosystem Based Self-Certified Public Key Scheme for Medical Data Protection', IEEE Transactions on Reliability, Vol. 64, No. 3.

[4] Haythem Hayouni, Mohamed Hamdi and Tai-Hoon Kim (2014), 'A Survey on Encryption Schemes inWireless Sensor Networks' 7th International Conference on Advanced Software Engineering & Its Applications.

[5] Kamlesh Gupta and Sanjay Silakari (2011), 'ECC over RSA for Asymmetric Encryption: A Review', IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 3, No. 2.

[6] Khalid Hussain, Abdul Hanan Abdullah, Khalid M. Awan, Faraz Ahsan and Akhtab Hussain (2013), 'Cluster Head Election Schemes for WSN and MANET', World Applied Sciences Journal 23 (5): 611-620.

[7] Lauter K (2004), 'The advantages of elliptic curve cryptography for wireless security', IEEE Wireless Commun., Vol. 11, No. 1, pp. 62–67.

[8] Miodrag, Irina, Dragan and Ranko (2012), 'Energy efficient security architecture for Wireless Sensor Networks', 20th Telecommunications forum TELFOR.

[9] Ramesh K. and Somasundaram K.(2011), 'A comparative study of clusterhead selection algorithms in wireless sensor networks', International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4.

[10] Seema Bandyopadhyay and Edward J. Coyle (2003), 'An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks', IEEE INFOCOM.

[11] Shucheng Yu, Kui Ren, Wenjing Lou (2011), 'FDAC: Toward fine-grained distributed data access control in wireless sensor networks', IEEE Trans. Parallel Distrib. Syst., Vol. 22, No. 4, pp. 673–686.

[12] Shyr-Kuen Chen, Tsair Kao, Chia-Tai Chan, Chih-Ning Huang, Chih-Yen Chiang, Chin-Yu Lai, Tse-Hua Tung, and Pi-Chung Wang (2012), 'Reliable Transmission Protocol for ZigBee-Based Wireless Patient Monitoring', IEEE Trans. Inf. Technol. Biomed., Vol.16, No.1, pp.6-16.

[13] Suman Bala, Gaurav Sharma and Anil K. Verma (2012), 'Optimized Elliptic Curve Cryptography for Wireless Sensor Networks', 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[14] Soufiene Ben Othman, Abdelbasset Trad and Habib Youssef (2012), 'Performance Evaluation Of Encryption Algorithm For Wireless Sensor Networks', International Conference on Information Technology and e-Services.

[15] Junqi Zhang,Vijay Varadharajan(2010), "Wireless sensor network key management survey and taxonomy"; Journal of Network and Computer Applications, vol. 33, pp.63-75.

[16] X Chen, K Makki, K Yen and N Pissinou; "Sensor Network Security: A Survey";IEEE communication survey and tutorials, vol. 11, pp. 52-73, 2009.

[17] Yong Wang, Garhan Attebury, Byrav Ramamurthy; "A Survey of Security Issues In Wireless Sensor Networks", IEEE Communications Surveys and Tutorials, volume 8, pp. 2-23, 2nd quarter 2006.

[18] D. W. Carman, P. S. Kruus, and B. J. Matt, "Constraints and Approaches for Distributed Sensor Network Security", NAI Labs, Tech. Report 00-010, 2000.