A Lightweight Cryptosystem for Wireless Sensor Networks using ECC

Anisha Mahato[1], Dr. M. Pushpalatha[2]

[1] *M.tech Scholar, Dept. of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur Campus, Chennai , India*

[2] *Professor , Dept. of Computer Science and Engineering , SRM Institute of Science and Technology, Kattankulathur Campus ,Chennai , India*

Abstract *Wireless sensor networks consists of tiny devices known as sensor nodes. These sensors monitor the physical conditions of the environment and the information gathered is processed to get relevant outcomes. The data can be collected, compressed and performed required functionalities in it. Security of the sensed information in this wireless connection is the major concern. Security is required in any field where there is exchange of information especially sensitive data like personal details, transactions etc. This can be overcomed with the help of robust cryptographic algorithms. Identification of a suitable cryptographic algorithm is a major challenge due to the resource constraints in computational capability and storage resources WSN.*

In this paper the various lightweight cryptographic algorithms are discussed which are applied in the sensor nodes. Among the well known asymmetric cryptographic algorithms Elliptic Curve Cryptography (ECC) has the smallest key size for the same level of security. Field inversions used in ECC is a costly process. This can be reduced by the introduction of Montgomery Multiplication and projective coordinate system in the algorithm.

Keywords — *Elliptic Curve Cryptography(ECC), Elliptic Curve Discrete Logarithmic Problem (ECDLP), Montgomery multiplication, Wireless Sensor Networks(WSN)*

I. INTRODUCTION

Wireless Sensor Network (WSN) is a network of sensor nodes. Wireless Sensor Networks consists of dynamically spread tiny devices which is used to monitor a particular network. These sensor nodes are used to record and analyse various environmental conditions such as humidity , rainfall , temperature , light and sound. Each sensor node is autonomous. Each have its own operating system. The processing capabilities of the nodes are less due to less computational power and memory space. There is a central base station to which the nodes send their sensed data for further processing. It is also known as the sink node. The sink node is rich in storage resources and computing power than the other sensor nodes in a particular network. Since the sensed information is highly sensitive , it must be sent to the destination node through a secure channel.

In section II of this paper the hardware architecture of the sensor node is discussed followed by its characteristics in section III. The security challenges in WSN and the applications of sensor networks are discussed in section IV and V respectively The various attacks are discussed in section VI .In section VII ECC algorithm is discussed. In section VIII the key Distribution in WSN is being analyzed. The security goals of the lightweight cryptosystems is discussed in section IX. Section X contains the Proposed System followed by the Result and Analysis is section XI. And finally the conclusion in section XII.

II. HARDWARE ARCHITECTURE OF SENSOR NODE

Sensing Unit – The sensing unit senses various environmental conditions such as sound , light , humidity, pressure and pollution. There are two types of sensing units one is active sensors and the other is passive sensors. It contains a analog to digital unit (ADC) which has the property of converting the analog signals to digital and then sends it to the processing unit for further processing.

Transceiver Unit - Transmitting and receiving of messages over the wireless networks is done with the help of transceiver unit. The communication is through radio waves.

Processing Unit –The processing Unit has the task of processing the sensed information and to take appropriate action for the same such as validation of the message, the sensor to be triggered next etc.

Power Unit – The generation of power is done through this unit which helps it to live and function properly.

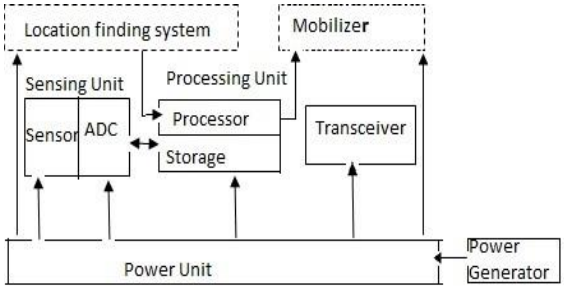


Fig-1: Hardware architecture of a sensor node

In Fig. 1. The hardware architecture of a typical sensor node is shown and the arrow heads gives the flow of information.

III. CHARACTERISTICS OF SENSOR NODE

Comparison and understaning the characteristics of two very popular sensor nodes which are MICA2 and MICAz in this section. A comparative study is performed based on the Processor, RAM , ROM, EEPROM , Data Rate and Power Supply as shown in Table 1. It can thus be seen that the operations in sensor nodes are performed with very less computing power, less power and with less programmable memory. Hence it is very important to consider the resource constraints of the sensor nodes while designing security mechanisms.

	MICA2	*MICAz*
Processor	8bit Atmega 128	8bit Atmega 128
RAM	4K bytes	4K bytes
ROM	128K bytes	128K bytes
Data Rate	38.4k baud	250k baud
Power Supply	2A A batteries	2A A batteries

Table -I: Comparison study of characteristics of sensor nodes [1] [7]

IV. CHALLENGES FOR SECURITY IN WIRELESS SENSOR NETWORKS

Limited resources - Sensor nodes have resource constraints on memory and computational power. They are very low. It proves as a hindrance for performing memory intensive operations.

Limited Communication Capabilities – The sensor nodes uses short ranged radio waves to transmit the sensed information to the neighbouring node or the base station. It works on less bandwidth which makes it difficult to transfer large information at once. Hence the security algorithms need to have short transmission range and less computation power.

Synchronization between nodes – There must be synchronization between the nodes in timestamps so that the key distribution process can be properly carried out during the encryption and decryption process.

Applying any encryption scheme in the sensor nodes require transmission of some extra bits , hence requiring extra memory.

The dynamics of the sensor networks change over time. It can be based on the topology or even the membership of the nodes.

V. APPLICATIONS

WSN has various outcomes in military and border security forces , smart homes, agricultural applications, health care applications, remote diagnosis etc. The sensor nodes are being deployed in unattended environment so it is necessary to have proper encryption and decryption methods for secure transmission. A hacker can intercept the messages being sent or even modify them before they reach the sink node. Security is a primary concern in WSN. Due to the resource constraints of the WSN most of the security protocols do not work.
In the following section some of the major WSN applications are discussed where security is necessary.

Military/ Border Surveillance – The geographical borders or battle fields can be risky for the soldiers to be present physically. To monitor any suspicious activity sensor nodes can deployed in those areas. It can be done through drones or military trucks. This is a very effective way of analysing the surroundings. It senses any kind of military movement, missile trajectory and if there is any violation of the country laws.
Once the information is sensed it must be sent to the base station for further processing in a secure manner. Upon receiving of messages appropriate decisions are being taken.

Healthcare Applications[4] – Wireless Sensor Networks in healthcare is an emerging technology. The patients body can be fitted with bio sensors to monitor the blood pressure level , haemoglobin , temperature, heart rate , oxygen etc [6]. The information received can then be sent to the doctor who can be present in any remote location. It reduces the cost and is also efficient for the patient to not travel to the hospital and get his/her result being present at home. Continuous follow ups can be maintained.

Smart Homes- The use of sensors in homes have increased rapidly since the last few years.
From remote control of television to having control of geysers, air conditioners , turning on/off of lights etc. Even if there is any sign of brokerage or theft in the house the owners can be easily notified on their cell phones to take necessary actions.

VI. ATTACKS ON WIRELESS SENSOR NETWORKS

- **Impersonation Attack –** In this attack the intruder tries to convince the sender that he is the actual receiver of the information. In WSN, the intruder can behave as a sink node or a sensor node or even a legitimate user. Here the attacker is successful in behaving identical to one of above.

- **Denial of Service Attack** – This causes flooding of the network so that there is no avaibility of resources and services. DOS attack can be done for the information so that the information is not available or the sensor nodes so that the nodes as well as the information in the nodes cannot be retrieved or denial of access to communication so that there is no communication within the network. This can be caused by jamming the network with excessive traffic.

- **Sensor node Capture Attack** – It occurs due to the placement of the sensor nodes in adverse situations . It is when a node is being compromised . The information stored in the sensor are being intervened by the unintended users. This can occur in Military border areas where the sensors can be captured by the other organizations. The information retrieved can be destroyed or can be used for fraudulent purposes.

- **Replay attack** – In this the attacker captures the information from one of the sensor nodes and tries to resend the packets to the destined party. In this way the attacker establishes communication with the recipient behaving as the sender.

- **Man in the middle attack** – Here the malicious user come in between two communicating parties. The attacker can modify the message to be sent to receiver or even form other messages to be sent. Mutual authentication should be done to overcome this.

- **Blackhole/Sinkhole attack** – Here a malicious node attracts all the traffic in a particular network. It acts like a blackhole. Here the attacker has the capability to listen to the requests and reply a forged message that the shortest path to the station is through them. This may even lead to the collapse of the entire network.

- **Hello flood attack** – It uses the technique of sending HELLO packets to the sensor nodes present in the network[3]. It tries to convince to be their neighbour. Once the sensors are convinced that it is their neighbour, it becomes the victims of the attacker and the information sent can be compromised and used for illegal purposes.

- **Wormhole attack** –In this tunnelling of bits of information is being done by the attacker node to send the packets to an alternate destination. The attacker can decide whether to send the whole message or a part of the message. This kind of attack is dangerous as it could be done during the initial phase of communication when the nodes starts to discover neighbouring information.

VII. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography (ECC) : It has been one of the most researched domains for security in the Wireless Sensor Networks due to its smaller key size and high level of security. It is a public key cryptosystem. It uses the concept of discrete logarithmic problem Let us take two points P and Q on the elliptic curve which in consideration. Suppose it satisfies the equation Q=kP, then determining the value of k [11] , with P and Q is known the discrete logarithmic problem. The infeasibility of the calculation of K using computational resources is the basis of ECDLP. A right elliptical curve should be selected in order to make ECDLP completely inflexible and a Q such that the number of points on the elliptic curve over the prime Q is divisible by a large prime number or such that Q is a huge prime number on its own. Implementation of ECC on Mica2 mote and the use of the computational resources is shown in Table II. Modifications can be performed in the ECC algorithm to reduce the number of field inversions with the help of Montgomery Multiplication and projective coordinates.

	Private Key Generation	Public Key Generation
Total CPU Utilization	1.690 x $10^{6\ \text{cycles}}$	2.512 x 10^8 cycles
Total Energy	0.00549 Joules	0.816 Joules

Table II: Computational resources for ECC on MICA2 [13]

VIII. KEY DISTRIBUTION

Scalability - It should be able to support large network and flexibility in increase or decrease of its size.

Efficiency – It should take into consideration the storage, processing and the communications limitations of the nodes in WSN.

- Storage Complexity – It states the amount of memory required to store the encryption algorithm and its credentials.

- Processing Complexity – It states the number of memory cycles required for key generation.

- Communication Complexity – the number of messages which are to be exchanged during the generation of the key.

Resilience – It states the resistance of the sensor nodes against node capture.

IX. SECURITY GOALS IN WIRELESS SENSOR NETWORKS

Integrity – Any kind of modification of the sent message before it arrives to the receiver is a loss of integrity[8]. There are two ways to check for integrity-one is the preventive mechanism and the other is the detective mechanism. In preventive mechanism let any modification of the message is not permitted whereas in detective mechanism it is checked if there is any change in the message and further it could be discarded.

Avaibility[8]- It states that the information is always available to the intended users when they need it. A sensor node present in the network must be able to make use of the resources and send the message to the neighbouring node. This ensure that the services of WSN are not hampered by internal or external attacks or by resource starvation due to the presence of complex operations. For example the security mechanism must have protection DOS attack where the attacker tries to load huge traffic in the network such that the sensor nodes are not able to communicate the simple request – response signal. This also effects the limited battery power of the sensors.

Confidentiality – In WSN confidentiality ensures that the message sent is being received only by the intended user in the network. It is one of the most important aspects of security as highly sensitive information are being exchanged in between the nodes.

Data Freshness – It states that the message once sent should be sent again. Hence replay of the old message is not allowed. This is really necessary for shared key cryptographic techniques as they need to be changed over time. A timestamp or a periodic counter in the algorithm can be used to decide the freshness of the message.

Time Synchronization – Collaborative operations are being performed in the WSN by synchronizing the clock of the nodes present. It becomes an important factor to protect against replay attacks or any other attacks where timestamp value is necessary.

Secure Localization – At times the sensors are being misplaced after being deployed in a particular environment. WSN will only be useful when the sensor nodes are places at the exact location where the information needs to be sensed and analysed.

X. PROPOSED SYSTEM

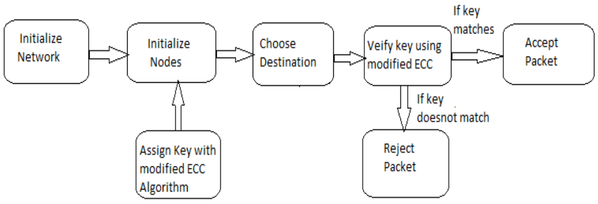


Fig-2: Block Diagram of Proposed System

1. Network Design:

Initialization of the nodes in the network is done using TCL coding. The process of sending packets is done through simulator.

2. Encryption using Modified ECC

The modification is done on the 'Point Multiplication' process of the ECC algorithm i.e., Q = K * P. It is made up of two process, Point Addition and Point Doubling.

Point Addition [15] - If P and Q are two points on the elliptic curve and P is not equal to –Q we draw a line through these two points P and Q which intersects the elliptic curve at exactly one more point –R. The reflection of the point –R with respect to the x-axis gives us the point R , which is the result of the addition of the points P and Q. Thus on the elliptic curve it is, P + Q = R

Point Doubling [15] - In this , a tangent is being drawn through the point P to the curve and wherever it intersects the curve it is been marked as R.The reflection of the point –Q with respect to the x-axis gives us the point Q, which being the result of point doubling of P. Thus on the elliptic curve it is, 2P = Q

The formula for point addition and point doubling are represented as follows:

$$x_3 = \begin{cases} (\frac{y_1+y_2}{x_1+x_2})^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a & , P \neq Q \\ x_1^2 + \frac{b}{x_1^2} \ , & P = Q. \end{cases}$$

$$y_3 = \begin{cases} (\frac{y_1+y_2}{x_1+x_2})(x_1+x_3) + x_3 + y_1 & , P \neq Q \\ x_1^2 + (x_1 + \frac{y_1}{x_1})x_3 + x_3 \ , & P = Q. \end{cases}$$

Montgomery multiplication process is used and Jacobian coordinates to make the algorithm lightweight. The x-coordinate of the resultant point was seen to be an expression of the resultant x-coordinates of P and Q. This made the algorithm more efficient for the sensor nodes. After the authentication is successful the packet is received at the destination node otherwise it gets rejected as shown in block diagram in Fig-2 . It can withstand most of the known attacks which are discussed in section X.

The formula for point addition and point doubling using Montgomery multiplication is represented as follows:

$$x_3 = \begin{cases} x + (\frac{x_1}{x_1+x_2})^2 + \frac{x_1}{x_1+x_2} & , P_1 \neq P_2 \\ x_1^2 + \frac{b}{x_1^2} \ , & P_1 = P_2. \end{cases}$$

$$y_1 = (x_1 + x)\{(x_1 + x)(x_2 + x) + x^2 + y\}/x + y$$

XI. RESULT AND ANALYSIS

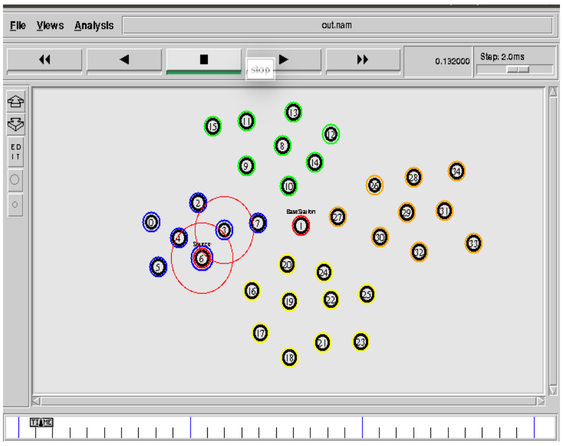
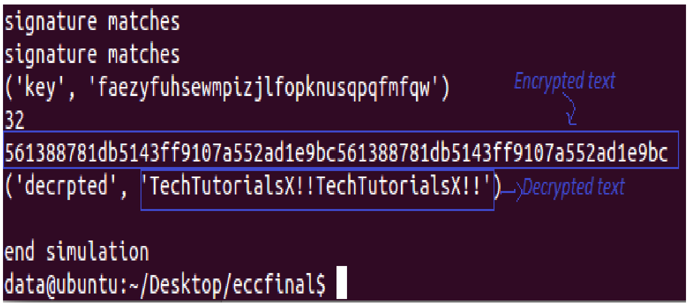


Fig- 3: Simulation of packets from source node to destination node



```
signature matches
signature matches
('key', 'faezyfuhsewmpizjlfopknusqpqfmfqw')
32
561388781db5143ff9107a552ad1e9bc561388781db5143ff9107a552ad1e9bc
('decrpted', 'TechTutorialsX!!TechTutorialsX!!')

end simulation
data@ubuntu:~/Desktop/eccfinal$
```

Fig-4: Encryption and decryption of sensed packets

The packets are being sent from the source to the destination node which is shown in Fig.- 3. When the information is sent from the source node, it is being encrypted. Once the signature matches ,then it is being decrypted by the destination node. The encryption and the decryption result is being shown in Fig-4 .Hence the information remains secret during packet transfer.

	Conventional ECC	**Proposed ECC**
Expected Execution Time (Message length-16 bits)	12 seconds	5 seconds
Number of Multiplication	2	1
Code Space	4 KB [14]	3.7 KB

Table III- Comparison of expected execution time between conventional ECC and proposed ECC.

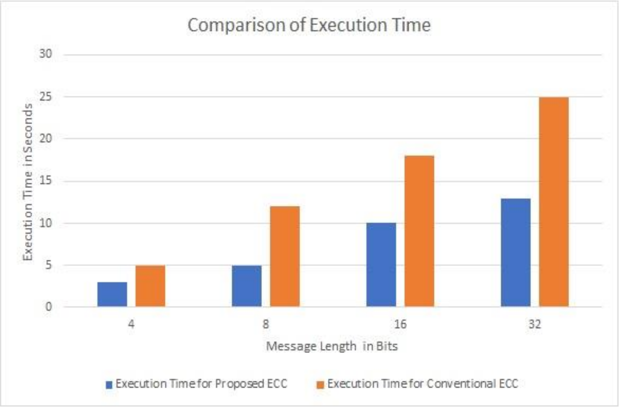


Fig-5: A bar graph showing the comparison of execution time difference between the Proposed ECC and the Conventional ECC

The modified ECC algorithm would be much lighter than the original ECC algorithm and the other asymmetric key cryptosystems. In Table –III, the execution time results which clearly states that the need for computational resources would be less in the proposed ECC which is the major limiting factor in sensor nodes. The number of multiplications would be reduced to one in this algorithm making the algorithm faster whereas the memory required to store the code remains same. In Fig. -5 ,the graph shows that when there is a change in the length of the message there is difference in execution time in both the proposed ECC and the Conventional ECC. The proposed ECC performs much better than the conventional ECC. The key validation in ECC would help to overcome side channel attacks, impersonation attacks, replay attacks and others. Thus can be successfully implemented in wireless sensor networks to provide security during transfer of packets.

XII. CONCLUSION

Providing secure routing of sensed information is one of the most important but difficult task in wireless sensor networks. Designing a lightweight public cryptosystem is the major goal. ECC is the best known public key encryption technique to be used in the wireless networks. This paper highlights the limitations of the security nodes and its security requirements would help the researches to work in this field.

REFERENCES

[1] Anil Kumar Sutrala, Ashok Kumar Das, Neeraj Kumar, Alavalapti Goutham Reddy, Athanasios V. Vasilakos, and Joel J. P. C. Rodrigues (2017)."*The Design of Secure User Authenticated Key Management Scheme for Multi-Gateway Based Wireless Sensor Networks using ECC".* Journal of Communication Systems (Wiley), Vol. 31, No. 8, pp. 1-31, 2018. (2017 SCI Impact Factor: 1.717)

[2] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu (2010). "*An Enhanced Two-Factor User Authentication Scheme in Wireless Sensor Networks."* Ad Hoc & Sensor Wireless Networks, 10(4):361{371,2010}

[3] Anitha S.Sastry, Shazia Sulthana and Dr.S Vagdevi, "*Security Threats in Wireless Sensor Networks in Each Layer*", International Journal of Advanced Networking and Applications, Vol. 04 Issue 04, pp. 1657-1661, 2013.

[4] Ashok Kumar Das, Anil Kumar Sutrala, Vanga Odelu, and Adrijit Goswami (2017). " *A Secure Smartcard-based Anonymous User Authentication Scheme for Healthcare Applications using Wireless Medical Sensor Networks,*" Wireless Personal Communications (Springer), Vol. 94, No. 3, pp. 1899-1933, 2017. (2017 SCI Impact Factor: 1.200)

[5] N. Khalil, M. R. Abid, D. Benhaddou, and M. Gerndt (2014) , "*Wireless sensors networks for Internet of Things".*IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), pages 1{6, Singapore, 2014.

[6] Minaie, A. Sanati-Mehrizy, P. Sanati-Mehrizy, and R. Sanati-Mehrizy(2013). "*Application of Wireless Sensor Networks in Health Care System*".American Society for Engineering Education, volume 3, pages 21{24, Atlanta, Georgia, 2013.}

[7] Woo Kwon Koo, Hwaseong Lee, Yong Ho Kim, Dong Hoon Lee (2008). "*Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks*".International Conference on Information Security and Assurance

[8] W. Stallings.(2004)" *Cryptography and Network Security: Principles and Practices*." Pearson Education, India, 3rd edition.

[9] S. Zhu, S. Setia, and S. Jajodia.(2006) *"LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks*." ACM Transactions on Sensor Networks

[10] B. Lai, S. Kim, and I. Verbauwhede.(2002)" *Scalable session key construction protocol for wireless sensor networks*."IEEE Workshop on Large Scale RealTime and Embedded Systems(LARTES), pages 1{6, Austin, Texas, 2002.

[11] Xu Huang, Pritam Shah, and Dharmendra (2010), SharmaFast *Algorithm in ECC for Wireless Sensor Netwok*",Proceedings of the International Multi-Conference of Engineers and Computer Scientists, Vol II, IMECS 2010

[12] Anil Kumar Sutrala (2018)," *Design and Analysis of Three-Factor User Authentication Schemes for Wireless Sensor Networks*", International Institute of Information Technology, Hyderabad

[13] Pyrgelis Apostolos,"*Cryptography and Security in Wireless Sensor Networks*", FRONTS 2nd Winterschool Braunschweig, Germany

[14] Nils Gura, Arun Patel, Arvinderpal Wander, Hans Eberle, and Sheueling Chang Shantz, "*Comparing Elliptic Curve Cryptography and RSA on 8-Bit CPUs*", Sun Microsystems Laboratories

[15] Guide to Elliptic Curve Cryptography, D Hankerson, AJ Menezes, S Vanstone, (Springer Professional Computing)