INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Providing Data Security in Healthcare centers using Digital Signatures based modified Elliptic Curve Cryptography (ECC) algorithm

[1] Er. Amandeep Kaur, [2] Er. Shushil Kumar

Research Scholar[1], Assistant Professor[2]
Department of Computer Science
SUSCET Tangori, Punjab, India

Abstract: *Recent technical enhancements in the field of sensors, low-power integrated circuits, and wireless communications has led to the design of low-cost, miniature, lightweight, and intelligent sensor nodes. These nodes are capable of sensing, processing, and transmitting one or more vital signs. These nodes can be seamlessly integrated into wireless body area networks for health monitoring. These networks will revolutionize health care systems by allowing cheap, non-invasive, regular, ambulatory health monitoring with almost real-time transmission of medical records via the Internet. Though a number of ongoing research efforts are going on in various technical, economic, and social issues, many technical problems still need to be resolved in order to have flexible, reliable, secure, and power-efficient WBANs suitable for medical applications. In the proposed work, ECC algorithm with Digital Signature has been implemented for providing secure Medical Data Transmission. Entire work has been simulated in NS-3. Results are compared on the basis of Throughput, Execution time, PDR and PLR.*

Keywords: *WSN, Medical Data Security, ECC Algorithm, Network security, Wireless Body area Network, Digital Signature.*

1. INTRODUCTION

Wireless sensor networks (WSNs) compose an immense number of small sensor nodes that send the collected information using the wireless channels. This sensor network is a amalgamate system combining insignificant sensors and actuate with figure out elements. Most sensor networks consist of thousands of low power, less- cost nodes expand to monitor and affect the environment. WSNs have many applications such as traffic control, health monitoring and environment monitoring etc. Most of the applications of WSNs require secure communication of information at both ends. Therefore security in WSNs is an analytical issue because sensor nodes have limited storage and energy for processing. When these sensor nodes are deployed in any environment, the problem of secured sharing of keys between sensor nodes becomes an issue of attention as sensor nodes are prone to various types of undesirable attacks. The rapidly requirements of ad hoc network technology has a wide range of applications, such as vehicular ad hoc network (VANET), wireless sensor network (WSN), emergency and military communications. Due to the features such as openness and dynamic topology, ad hoc networks suffer from various attacks in data plane. [1] WSN-based applications which induced a host of research activities in both academia and industry. Since most of the target WSN applications are very sensitive, security issue is one of the major challenges in the deployment of WSN.

2. SECURITY REQUIREMENTS FOR WSN

a) Message authentication: The message receiver should be able to verify whether a received message is sent by the node that is claimed or by a node in a particular group. In other words, the adversaries cannot pretend to be an innocent node and inject fake messages into the network without being detected.[2]

b) Message integrity: The message receiver should be able to verify whether the message has been modified en-route by the adversaries. In other words, the adversaries cannot modify the message content without being detected.[3]

c) Identity and location privacy: The adversaries cannot determine the message sender's ID and location by analyzing the message contents or the local traffic.[4]

d) Node compromise resilience. The scheme should be resilient to node compromise attacks. No matter how many nodes are compromised, the remaining nodes can still be secure.

e) Efficiency: The Security scheme should be efficient in terms of both computational and communication overhead.[5]

3. TYPES OF WIRELESS SENSOR NETWORK

Depending on the environment, the types of networks are decided so that those can be deployed underwater, underground, on land, and so on.[6]

a) Terrestrial WSNs: Terrestrial WSNs are reliable of communicating base stations efficiently, and consist of hundreds to thousands of wireless sensor nodes deployed either in disorganized (ad hoc) or structured (Preplanned) manner. In a disorganized mode, the sensor nodes are randomly spread within the target area that is discarded from a fixed plane. The preplanned or structured mode considers optimal placement, grid placement, and 2D, 3D placement models. In this WSN, the battery power is limited; however, battery is equipped with solar cells as an alternative power source.[7]

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

b) Underground WSNs: The underground wireless sensor networks are more costly than the terrestrial WSNs in terms of deployment and demand, maintenance, and equipment cost attentions and careful planning. The WSNs networks consist of a couple of sensor nodes that are not visible in the ground to monitor underground conditions. To broadcast information from the sensor nodes to the base station, extra sink nodes are located above the ground. The underground wireless sensor networks deployed divided into the ground are difficult to reactivate. The sensor battery nodes equipped with a limited battery power are difficult to recharge. In addition to this, the underground environment makes wireless communication a objection due to high level of attenuation and signal drop.[8,9]

c) Under Water WSNs: More than 70% of the earth is occupied with water. These networks consist of a number of sensor nodes and vehicles deployed under water. Self-governing underwater vehicles are used for gathering data from these sensor nodes. A challenge of underwater communication is a long propagation delay, and bandwidth and sensor failures. Under water WSNs are equipped with a limited battery that cannot be recharged or replaced. The issue of energy reservation for under water WSNs involves the development of underwater communication and networking technologies.

d) Multimedia WSNs: Multimedia wireless sensor networks have been proposed to enable tracking and monitoring of events in the form of multimedia, such as imaging, video, and audio. These networks consist of low-cost sensor nodes equipped with microphones and cameras. These nodes are linked with each other over a wireless connection for data compression, data retrieval and cooperation. The challenges with the multimedia WSN include high energy consumption, high bandwidth requirements, data processing and compressing techniques. In addition to this, multimedia contents require high bandwidth for the contents to be delivered properly and easily.[10]

e) Mobile WSNs: These networks consist of a collection of sensor nodes that can be moved on their own and can be interacted with the physical environment. The mobile nodes have the ability to compute sense and communicate. The mobile wireless sensor networks are much more versatile than the static sensor networks. The advantages of MWSN over the static wireless sensor networks include better and improved coverage, better energy efficiency.

4. EXISTING WORK

In the previous work, Elliptic Curve Cryptography (ECC) for secure key distribution and data exchange has been implemented. ECC provides same level of security by using lesser key size than RSA. Moreover, this scheme has mutual authentication of sink node by base station server and of base station server by sink node. It uses hash value of sink ID, registered random number and timestamp value for two-way authentication. Furthermore, proposed technique uses timestamp value to identify replay attack. Overall, it proves a better security mechanism in case of WSNs for healthcare devices. Previously, proposed approach has used ECC, but replay attack and mutual authentication was major concern in that approach. Medical data is very sensitive in nature which demands a very secure architecture. 2-way authentication and in just two steps has enhanced the overall security architecture of Wireless Sensor Networks for healthcare applications.

It has been observed and analyzed from the implementation of ECC algorithm and existing techniques that the existing problems of replay attack and mutual authentication have been resolved. Replay attack issue can be resolved using time stamp value. This value would enable receiver to identify the status of message. Real message would contain current time whereas replay attack message would contain old time. Apart from replay attack issue, mutual authentication is one of the most important requirements in WBANs due to the privacy and security concern of data. Previous technique describes that Sink node would authenticate the base station server before actual transmission of medical data and base station server would also authenticate the sink node before any actual reply. However, devices are having resource constraints, so large computations cannot be performed because they may slowdown the overall performance. Digital Signature could be used further for authentication in ECC algorithm to increase the performance.

5. PROPOSED ELLIPTIC CURVE DIGITAL SIGNATURE(ECDSA) ALGORITHM

Computations needed for ECDSA authentication are the generation of a key pair (private key, public key), the computation of a signature, and the verification of a signature.

A. KEY PAIR GENERATION

The public key is derived from the private key and the domain parameters. The key pair must reside in the authenticator's memory. As the name implies, the private key is not accessible from the outside world. The public key, in contrast, must be openly read accessible.

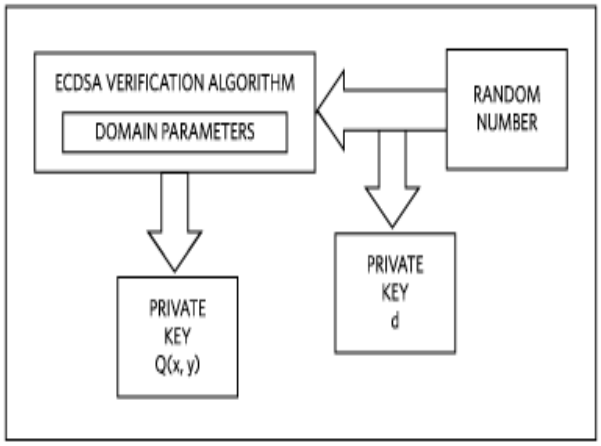

Figure 1: Key Generation Process

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Now, we have to consider a number'd' within the range of 'n'. Using the following equation we can calculate the public key
Q = d * P; d = the random number that we have chosen 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' has the point 'M' on the curve 'E'. Randomly select 'k' from [1 – (n-1)].
Two cipher texts will be calculated let it be C1 and C2.
C1 = k*P
C2 = M + k*Q
C1 and C2 will be sent.

DECRYPTION
We have to get back the text 'm' that was send to us,
M = C2 – d * C1
M is the original message that we have send.

PROOF
How do we get back the original message?
M = C2 – d * C1
'M' can be shown 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).

B. SIGNATURE COMPUTATION
A digital signature allows the recipient of a message to verify the message's authenticity using the authenticator's public key. First, the variable-length message is converted to a fixed-length message digest h(m) using a secure hash algorithm. After the message digest is computed, a random number generator is activated to provide a value k for the elliptic curve computations.

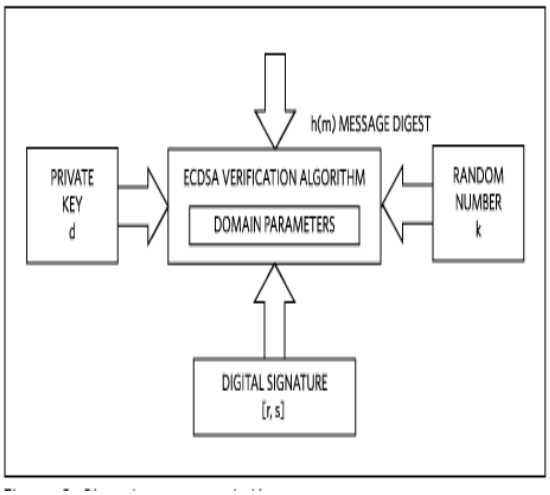

Figure 2: Signature Computation

C. SIGNATURE VERFIFICATION
The signature verification is the counterpart of the signature computation. Its purpose is to verify the message's authenticity using the authenticator's public key. Using the same secure hash algorithm as in the signature step, the message digest signed by the authenticator is computed which, together with the public key Q(x,y) and the digital signature components r and s, leads to the result.

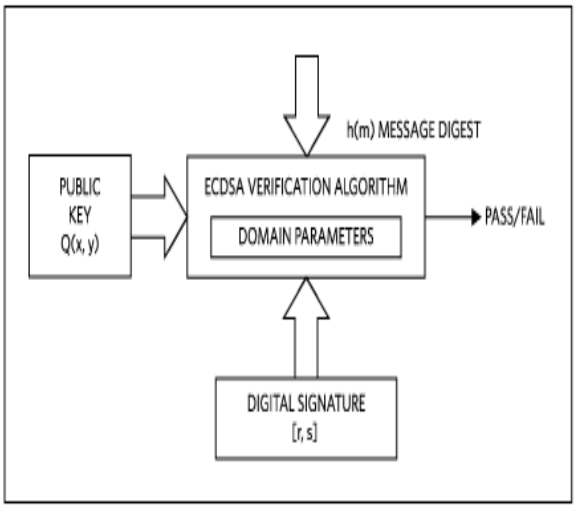

Figure 3: Signature Verification

6. OBJECTIVES
The major objectives of our research work are:
1. To study about symmetric and asymmetric security algorithms for wireless sensor networks.
2. To implement the entire work in Network Simulator version 3
3. To implement the concept of Digital Signature in Simple ECC algorithm and compare the results on the basis of various parameters.

7. RESULTS
In the proposed research work ECC algorithm and ECC algorithm with Digital Signature has been implemented. Parameters considered for result comparison are Packet Delivery Ratio, Packet Loss Ratio, Throughput and Execution Time.

Packet Delivery Ratio: The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.

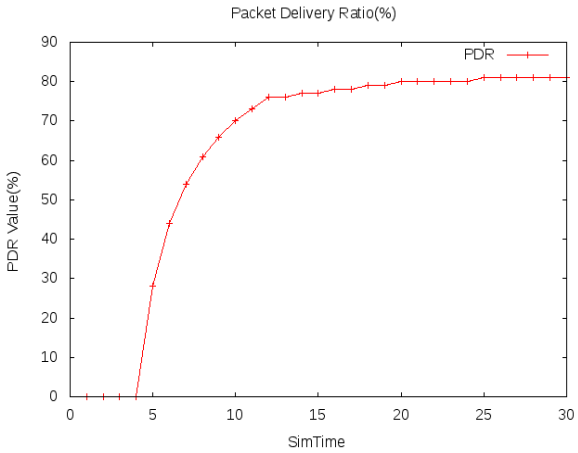

Figure 4: Packet Delivery Ratio of ECC Algorithm

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

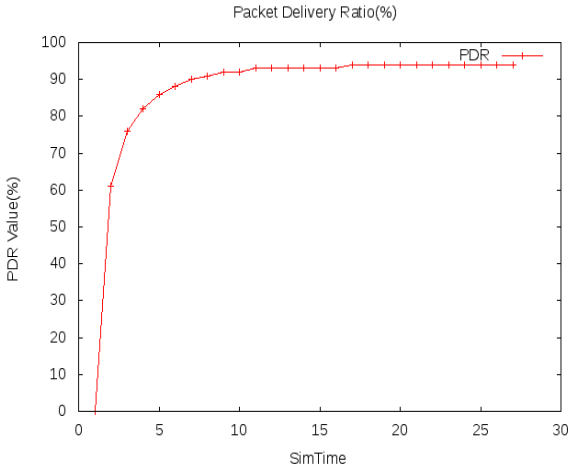

Figure 5: Packet Delivery Ratio of ECCDS Algorithm

Packet Loss Ratio: Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss is typically caused by network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent.

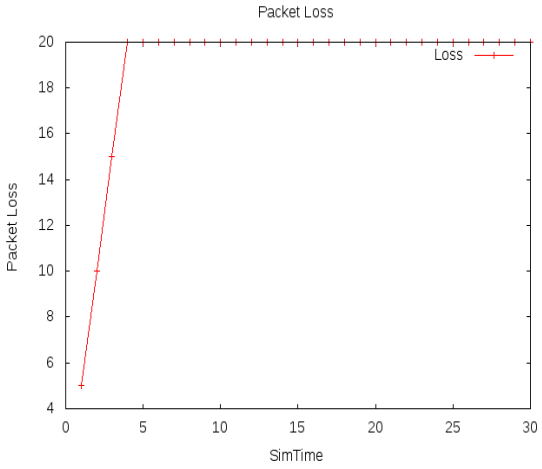

Figure 6: Packet Loss Ratio in ECC Algorithm

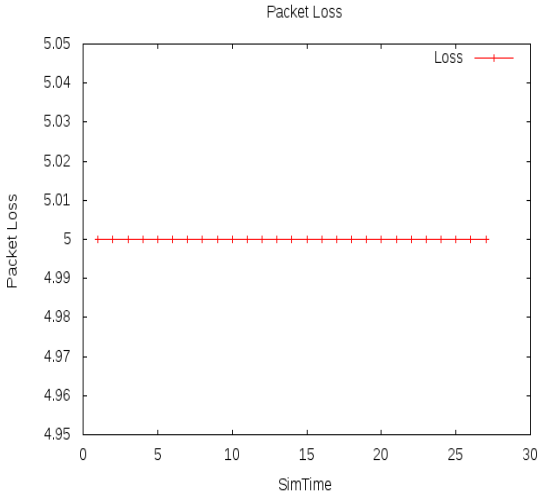

Figure 7: Packet Loss Ratio in ECCDS Algorithm

THROUGHPUT: It defines how much useful data can be transmitted per unit time. It is equal to the bandwidth if there is no protocol. However, in most practical cases the throughput is less than the bandwidth.

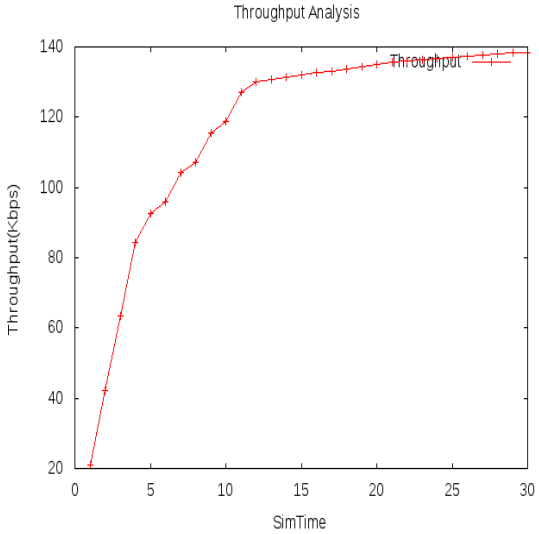

Figure 8: Throughput of ECC Algorithm

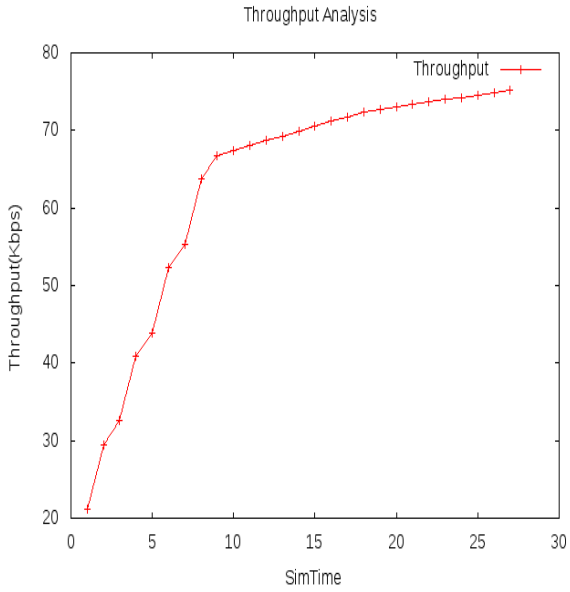

Figure 9: Throughput of ECCDS Algorithm

Execution Time: It is the time during which a program is running (executing), in contrast to other program lifecycle phases such as compile time, link time and load time.

Table 1: Execution Time

Execution Time (Seconds)	
ECC Algorithm	**ECC Algorithm with Digital Signature**
0.00019054	0.00019026

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

8. CONCLUSION AND FUTURE SCOPE

It is concluded that ECC algorithm with Digital Signature is performing better as compared to ECC algorithm. Simulation results are obtained using Network Simulator version 3. Parameters used for comparison are Throughput, Execution time, PDR and PLR. Moreover, ECC algorithm with Digital Signature is secured as compared to ECC algorithm in the sense it provides Authenticity and Confidentiality as well. It also resolves the existing problems of Replay attack and Mutual Authentication. ECC with Digital Signature has been proved as the best cryptographic technique for secure data transmission in a resource constrained environment.

In future new security mechanism can be implemented with better security and privacy. The implemented work can be tested on real time systems. Further security parameters should be considered for a better and improved security. These security algorithms are implemented on Health care systems while in future they can be tested on Universities and Colleges information management system where they can provide required security to the confidential data.

REFERENCES

[1] **Al-Sakib Khan Pathan, Hyung-Woo Lee and Choong Seon Hong (2006), "*Security in Wireless Sensor Networks: Issues and Challenges*" ICACT2006, ISBN 89-5519-129-4, pp 20-22.**

[2] **Mona Sharifnejad, Mohsen Sharifi, Mansoureh Ghiasabadi and Sareh Beheshti (2007), "*A Survey on Wireless Sensor Networks Security*", 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications", March 25-29, 2007.**

[3] **Zoran S. Bojkovic, Bojan M. Bakmaz, and Miodrag R. Bakmaz (2008), "*Security Issues in Wireless Sensor Networks*", International Journal of Communications, Issue 1, Volume 2, 2008.**

[4] **Hemanta Kumar Kalita1 and Avijit Kar (2009), "*Wireless Sensor Network Security Analysis*", International Journal of Next-Generation Networks (IJNGN), Vol.1, No.1, December 2009**

[5] **Gaurav Sharma, Suman Bala, A. K. Verma and Tej Singh (2010), "*Security in Wireless Sensor Networks using Frequency Hopping*", International Journal of Computer Applications (0975 – 8887), Volume 12– No.6, December 2010.**

[6] **Hemanta Kumar Kalita and Avijit Kar (2011), "*Key Management and Security Planning in Wireless Ad-Hoc Networks*", 2nd International Conference and workshop on Emerging Trends in Technology (ICWET) 2011.**

[7] **T. Lalitha and R. Umarani (2012), "*Cluster based Efficient Key Management and Authentication Technique for Wireless Sensor Networks*", International Journal of Computer Applications (0975 – 8887), Volume 39– No.16, February 2012.**

[8] **Jyoti Shukla and Babli Kumari (2013), "*Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview*", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 2, Issue 3, March 2013.**

[9] **P.Uthaya Bhanu1 and J. Saravanan (2014), "*Data Security in Wireless Sensor Network*", International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320-9801, Vol. 2, Issue 2, February 2014.**

[10] **Jian Li, Yun Li, Jian Ren and Jie Wu (2014), "*Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks*", IEEE transactions on parallel and distributed systems, vol. 25, no. 5, may 2014.**