A novel security algorithm ECC-L for wireless sensor network

Notom Ajaykumar | Mrinal Sarvagya | Parag Parandkar

School of ECE, Reva University, Bangalore, India

Correspondence
Notom Ajaykumar, School of ECE, Reva University, Bangalore, India.
Email: ajaykumarnotom@gmail.com

Wireless communication has poised to become one of the most predominant area of research in the field of communication engineering. Wireless Sensor Network also plays a significant role in shaping and linking IoT and communication era. The proposed work considers the two most influential parameters, the power consumption and security, for accessing the performance of Wireless Sensor Network. A novel security algorithm Rabin based Elliptic Curve Cryptosystem - Linear (ECC-L) has been designed, implemented and compared with existing ECC algorithm. The proposed algorithm uses double binding hash code technique. It supports sensor nodes with bio hash code for identification of authorization network to share the data. The impact of increase in number of nodes to the key performance metrics of WSN like, energy, packet loss, delay, throughput etc., is measured on ECC and proposed ECC-L by performing simulations. Qualitatively, the metrics show peak performance and significant performance improvement compared to ECC algorithm in terms of reduction in the packet loss, obtaining maximum throughput, avoidance of retransmissions and enhancement of energy efficiency in wireless sensor network. Quantitatively, the simulation results show that the proposed Rabin ECC-L algorithm perform enhanced better than the existing ECC algorithm for the impact of increase in number of nodes on reduction of control overheads by 21%, reduction in energy consumption by 27%, decrease in packet losses by 13%, increase in throughput by 32% and decrease in average delay by 32%.

KEYWORDS
bio hash coding, elliptic curve cryptosystem - linear (ECC-L), quality of service (QoS), wireless sensor network (WSN)

1 | INTRODUCTION

Wireless Sensor Networks (WSNs) improves in key parameters including energy efficiency, reduction of packet loss, throughput and security. In wireless domain, various algorithms have been used for getting the optimal solutions. Higher rate of packet loss amounts to greater energy consumption, affecting system performance detrimentally. Thus, lowering loss of packets helps the system to perform better. Another popular measure emphasized by various authors to improve the efficiency of the WSN functions is Quality of Service (QoS). The robust nature of ECC cryptosystem can be demonstrated based on the intricacy of the Elliptic Curve Discrete Logarithm Problem (ECDLP). QoS employs routing methods via optimization factors, enhancing routing protocol and security levels, which together gave cumulative effect of limiting the energy.1-4

To strengthen and enhance the security measure, many cryptosystems such as RSA, AES and ECC, were developed a robin based ECC to avoid computation challenges in terms of greater energy requirement. Considering secret key generation models working on inter node and intra nodes, the network also obviates the problem of key pre-distribution inherent to many existing cryptographic approaches.5-11

The security connected problems and challenges in WSNs were examined in4 and the security threats recognized. It also discusses the obstructions and the necessities in the sensor security and categorization of attacks. In,12 authors concentrated on the impact of the usual network attacks on the network to reduce the energy and discussed the issue of unnecessary addition of new nodes, thus resulting in poor deployment. The author proposed a Trust Sensing-based Secure Routing Mechanism (TSSRM) with the lightweight features and the capability to oppose lot of usual attacks simultaneously. All together the security route selection algorithm was also optimized, considering trust degree and QoS metrics.

Authors in13 proposed compressive security framework that give security services for the entire services of sensor network. They also incorporated an additional element, Intelligent Security Agent (ISA) to evaluate level of security and cross layer communications. Similarly, the security issues restrict design and deployment features. The necessity of security measure for designing a secure sensor network.10 The analysis recognized attacks at different layers and a few counter gauges, opposite to those attacks. At last, a few defensive gauges were discussed concentrating on the key management, link layer and routing security.10 Furthermore, Diro et al recommended lightweight cryptographic model such as Elliptic Curve Cryptosystem (ECC).14

In ECC, the key size is 1024, causes computational challenges, in this paper discussed Rabin ECC with 128 bit key size, changes randomly with respect to time and nodes.
2 | RELATED WORK

To accomplish less computation complexity, Kirsal Ever et al.\(^{15}\) proposed a scheme using improved Elliptic Curve Cryptography (ECC). This technique is considered as one of the most popular security measures in WSN.\(^{16}\) ECC generates private key to be distributed to neighbor nodes of the same network to establish secure transmission. It deploys variety of key sizes to enhance the safety of the cluster network. ECC signed digital envelop model in WSN permits less computation. ECC parameters are set for various security aspects. It avoids key issue of public key distribution by developing an approach involving division of clusters in WSN. This approach follows the same public key in entire network, which can ease the intrusion detection and add the threat of attacks by malicious nodes.

ECC is competent technique in terms of its feasibility in constrained devices like sensor nodes. It is used as a general crypto algorithm to encrypt and decrypt with minimum prime key field. The number of bits gives a comparison of key sizes of some eligible crypto systems for low computation devices for achieving different security levels. Also, the ECC system uses smaller key sizes compared to RSA for the same security level.

The performance comparison of ECC technique with Rivest-Shamir-Adleman (RSA) public key cryptosystem is depicted in Table 1. The result clearly indicates that the ECC technique uses comparatively lesser key length, thus deemed more efficient to implement in the cluster nodes of group of networks compared to RSA.\(^{17}\)

| Key length of RSA | Key length of ECC | Ratio |
|-------------------|-------------------|-------|
| 512               | 106               | 5:1   |
| 768               | 132               | 6:1   |
| 1024              | 160               | 7:1   |
| 2048              | 210               | 10:1  |

The rest of the manuscript is divided into four sections. Section II discusses related work incorporating the existing techniques. Section III elaborates the proposed Elliptic Curve Cryptosystem over finite field with doubling multiplier protocol. Section IV depicts the optimal simulation results, by showing the superiority of the proposed algorithm compared to the peer ones. Section V concludes the paper by highlighting the better efficiency achieved by proposed algorithm considering given set of parameters.

3 | PROPOSED WORK

In the general ECC technique, the computation process continuous with the variable public keys, shared by all the nodes in the network, including malicious node, that make the unauthorized nodes to possibly corrupt the data. To overcome this, digital signature is posed as the probable solution. The digital signature used with ECC provides the additional security in WSN. But at the same time, it will also share the same sign with the malicious nodes thus offering many chances of attack. To overcome this problem, Rabin Elliptic Curve Cryptosystem with linearity (Rabin ECC-L) is proposed in this paper.

Rabin ECC-L is enhanced version of ECC algorithm. One of the important features of Rabin ECC-L algorithm is that it avoids malicious nodes by incorporating random variation of private keys, while transmitting packets from the source node to sink node. Rabin technique generates the random key with variation in bit ranges for different packet transmissions.

In addition to that, Rabin ECC-L is used to generate the primary key which will vary randomly with respect to time, to avoid the formation of malicious nodes, that helps to reduce the retransmissions. It also masks the encrypted code to double the encryption standard by adding bio hash key. With this, a highly robust and efficient Symmetrical Elliptic Curve Cryptosystem with Rabin Technique for WSN routing protocol has been developed. This transmission model imbibes ECC-L assisted Rabin Technique, Un-linear Hashing and Soft Computing based multi constraints authentication.

Rabin ECC-L uses a random public key that can authorize the same ID nodes (Ni, i is 0 to n) of same network depicted in Equation (1).

\[
Ni = IDi,
\]

where node encodes the data with the element of EC using finite Galois field (G) \(G = 0,1,2, \ldots n.\)
### Table 2  Simulation environment

| Parameter                              | Value                   |
|----------------------------------------|-------------------------|
| MAC                                    | IEEE 802.15.4           |
| PHY                                    | 802.15.4PHY             |
| Antenna                                | Omni-directional        |
| Radio range                            | 200                     |
| Sensor nodes                           | 50                      |
| Efficiency of RF power amplifier       | 0.47                    |
| Link margin                            | 40 dB                   |
| Gain factor                            | 30 dB                   |
| Power density of AWGN channel          | $-134$ dBm/Hz           |
| Noise figure (Receiver)                | 10 dB                   |
| Path loss (db)                         | 3–5                     |
| Carrier frequency                      | 2.5 GHz                 |
| Bandwidth                              | 20 KHz                  |
| BER performance                        | $10^{-3}$               |
| Transmitter circuit power consumption  | 98.2 mw                 |
| Receiver circuit power consumption     | 112.6 mw                |
| Antenna gain of transceiver            | 5 dB                    |
| Routing table update (exchange) period for each round | 5                      |
| Routing table size                     | 100                     |
| Transmission rate                      | 2-10 kb/s               |
| Packet size                            | 2 kbits                 |
| Transmission probability of each node  | 0.8                     |
| Routing protocol                       |                         |
| - With proposed multifactor authentication and key management policy | |
| - Native AODV                          |                         |

A point, or group element, on the EC, consisting of two elements of the field $FP$ points $x$ and $y$, can only be created by the EC instance itself, as there has to be elements of the group generated by the EC. This curve is defined over the finite field (Galois field) $F_p$ and generates finite points, encrypted with node id to find the authorized network. The Equation (2) depicts encryption with node id.

$$y = Ni + GP(x, y)' .$$  \hspace{1cm} (2)

Elliptic Curve over a finite field of order $P$ is given by Equation (3)

$$y^2 = x^3 + a.x + b \pmod p.$$  \hspace{1cm} (3)

The implementation is simple, and it uses normal machine integers for its calculations. No special “big integer” manipulation is supported, so anything big will not work. However, it is a complete finite field ECC implementation which can be used to learn and understand the behavior of these curves and to experiment with them for their use in cryptography. Equations (4) and (5) uses different $p$ for enhancing the security.

$$y.a^3 + x.b^2 \neq 0 \pmod p$$  \hspace{1cm} (4)

$$y.G^2 = x.G^2 + a.x.G + b \pmod p.$$  \hspace{1cm} (5)

### 3.1 Doubling multiplier algorithm

In the Double multiplier algorithm, the curve point parameters of Field Point ($FP$) are multiples of constant values. The template parameter $P$ is the order of the finite field $F_p$ over which this curve of the doubling multiplier algorithm will act. Multiple packets depicted by “m” will occur in the form of series shown by Equation (6).

$$K = a^2.$$  \hspace{1cm} (6)

The Rabin ECC-L doubling multiplier multiplies “a” with “k” by expanding in multiples of 2, “a” is also an accumulator that stores the intermediate result between the “1s” of the binary form of the input scalar “k.”

$$a = 2.(x-y) \oplus a.$$  \hspace{1cm} (7)

Adding two points on the curve, special cases involving the additive identity access “x” component and “y” component as element of “Fp” are evident.

$$y = x.a + k.(\mod p)' .$$  \hspace{1cm} (8)
3.2 | Elliptic curve implementation

In Rabin ECC-L implementation process, the constant parameter of “x” and “y” components relates the input and output of the particular node. The curve pointed by polynomial in Equation (9) is used to initialize Elliptic Curve (EC).

\[ y = x^3 + a.x + b. \]  

(9)

After calculation of all the points (group elements) for this EC, if the order of this curve is large, it might take more time for computation.

\[ x_n = (n^*nsq + a.n + b) \pmod{P} \]  

(10)

\[ y_n = nsq \pmod{P}. \]  

(11)

To get a point (group element) on the curve with number of elements in this group, size is constant. The degree “P” belongs to this EC, parameter “x_n” is an element of “F_p,” the parameter “y_n” is also an element of “F_p.”

3.3 | Hash code binding

The elements of the EC curve of variable “X” point with finite field “P” generates Mod, calculates the remainder of “x” divided by “p.”

\[ x = x \pmod{p} \]  

(12)

Then, calculation and formation of the table for sliding out bytes is performed. The byte to slide out is used as the index for the table, the value contains the following:

\[ \text{out_table}[b] = \text{Hash}(b \parallel 0 \parallel … \parallel 0). \]  

(13)

Equation (13) represents encrypted output of initial stage having window size of 1 associated with zero bytes. Slide out byte “b_0” for window size “w” with known hash, is shown in Equation (14)

\[ H = H(b_0 \parallel … \parallel b_w). \]  

(14)

The first order of the output with respect to window size of b_w is expressed as.

\[ \text{out_table}[b_0] = H(b_0 \parallel … \parallel b_w) + H(b_0 \parallel 0 \parallel … \parallel 0) \]

After performing the above operation, following results are obtained

\[ H \left( (b_0 + b_0 \parallel b_1 + 0 \parallel … \parallel b_w + 0 \right) \) and \( H \left( b_0 \parallel b_1 \parallel … \parallel b_w \right) \).\]

Afterwards repetitions will continue k times with a new byte of data resulting in reduction mod Polynomial given by

\[ k = (h^*\text{polynomial}). \]  

(15)

The polynomial varies with 256-bit sequences, resulting in the mod table.

\[ [b] = A \parallel B, \] where \( A = b(x)^*x^k \pmod{\text{polynomial}} \) and \( B = b.x^k \).

The future course of action is determined by a polynomial having degree more than 8. These bits are used as a lookup to this table. The value is split in two parts: Part A contains the result of the modulus operation, part B is used to cancel out the 8 top bits, so that one XOR operation is enough to reduce modulo Polynomial.

\[ \text{FIGURE 1} \] 50 node network model contaminated with malicious nodes

\[ \text{FIGURE 2} \] Rabin ECC-L vs ECC compared for impact of increase in number of nodes on Control overhead
RESULTS AND DISCUSSION

In the proposed work, Rabin ECC-L node network is designed with various number of nodes like 50, 100, 150, 200, with addition of some malicious nodes in the network to check out various parameters of QoS in WSN. Some of the key network parameters and their respective values are given in Table 2.

In this model three malicious nodes are added keeping total number of nodes as 50 to observe the performance of WSN. Figure 1 shows the deployment of nodes contaminated with malicious nodes. The simulated results are generated by Network Simulator, NS version 2.35.

Figure 2 shows the simulation result of ECC and Rabin ECC-L packet overhead with number of nodes. It clearly shows that, packet overheads decreases compare to ECC with increase nodes. The control overhead using proposed algorithm is lesser than ECC by 21%.

Figure 3 compares ECC and Rabin ECC-L for the impact of increase in number of nodes on the energy efficiency in WSN. Rabin ECC-L is shows lower energy consumption compared to ECC by 27%.

Figure 4 shows the impact of increase in number of nodes on packet loss (in %). The graph clearly indicates that after increase in number of nodes, the packet loss decreases significantly by 13% for the proposed algorithm.

Figure 5 compares ECC and Rabin ECC-L for the impact of increase in number of nodes on the average throughput in kbps. The graph clearly indicates that after increase in number of nodes, the average throughput (in kbps) increases significantly by 32% for the proposed algorithm compared to ECC algorithm.

Figure 6 compares ECC and Rabin ECC-L for the impact of increase in number of nodes on the average delay in milliseconds. The graph clearly indicates that after increase in number of nodes, even in the presence of malicious nodes, the average delay (in ms) decreased significantly by 32% for the proposed algorithm compared to ECC algorithm.

CONCLUSION

The Rabin ECC-L Systematic layer security algorithm generates random key and transfers the key to the neighbor nodes to decrypt the information before hashing the code using hash binding finger print technique. In comparison with that, a highly robust and efficient Symmetrical Elliptic Curve Cryptosystem with Rabin Technique is developed for WSN routing protocol. The proposed transmission model incorporates ECC-L assisted Rabin Technique, Uni-linear Hashing and Soft Computing based multi constraints authentication. The efficacy of proposed cryptosystem is better than the previous algorithms because it is taking initially fixed key sizes and later varying it randomly, thus ensuring better energy efficiency and enhanced security. The simulation results show that the proposed Rabin ECC-L algorithm performs optimally better than the existing ECC algorithm for the impact of increase in number of nodes on reduction of control overheads by 21%, reduction in energy consumption by 27%, decrease in packet losses by 13%, increase in throughput by 32% and decrease in average delay by 32%.

ORCID

Notom Ajaykumar  https://orcid.org/0000-0002-5220-8650
REFERENCES

1. Dhote K, Asutkar GM. Optimization of routing techniques in wireless sensor network using queue management. Paper presented at: 2017 Devices for Integrated Circuit (DevIC); March 23-24, 2017; Kalyani India; pp. 500-504.

2. Kalnoor G, Agarkhed J. QoS based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks. Paper presented at: 2016 International Conference on Circuit, Power and Computing Technologies (ICCPPCT); March 18-19, 2016; Nagercoil, India; pp. 1-6.

3. Rachedi A, and Hasnaoui A. Security with quality-of-services optimization in wireless sensor networks. Paper presented at: 2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC); July 1-5, 2013; Sardinia, Italy; pp. 1319-1324.

4. Qin D, Yang S, Jia S, Zhang Y, Ma J, Ding Q. Research on trust sensing based secure routing mechanism for wireless sensor network. IEEE Access. 2017;5:9599-9609.

5. Sayeed A, Perrig A. Secure wireless communications: secret keys through multipath. Paper presented at: 2008 IEEE International Conference on Acoustics, Speech and Signal Processing; March 31-April 4, 2008; Las Vegas, NV; pp. 3013-3017.

6. Shi Q, Li Z. A secure QoS routing algorithm based on ACO for wireless sensor network. Paper presented at: 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing; November 13-15, 2013; Zhangjiajie, China; pp. 1241-1245.

7. Malathi M, Jayashri S. Design and performance of dynamic trust management for secure routing protocol. Paper presented at: 2016 IEEE International Conference on Advances in Computer Applications (ICACA); October 24-24, 2016; Coimbatore, India; pp. 121-124.

8. Levendovszky J, Thai HN. Quality-of-service routing protocol for wireless sensor networks. J Inf Technol Softw Eng. 2015;4:2.

9. Wenjun G, Dutta N, Chellappan S, Bai X. Providing end-to-end secure communications in wireless sensor networks. IEEE Trans. Netw. Serv. Manage. 2011;8:1-14.

10. Rehana J. Security of wireless sensor network. Paper presented at: TTK T-110.5190 Seminar on Internetworking; April 27, 2009.

11. Nair B, Mala C. Analysis of ECC for application specific WSN security. Paper presented at: 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCI); December 10-12, 2015; Madurai, India.

12. Rooopak M, Bharadwaj T, Soni S, Batra G. Review of threats in wireless sensor networks. Int J Comput Sci Inf Technol. 2014;5(1):25-31.

13. Sharma K, Ghouse MK, Kuldeep. Complete security framework for wireless sensor networks. Int J Comput Sci Inf Technol. 2009;3(1):0122-0129.

14. Diro AA, Chilamkurti N, Kumar N. Lightweight cybersecurity schemes using elliptic curve cryptography in publish-subscribe fog computing. Mobile Network Appl. 2017;22(5):848-858.

15. Kirsal EY. Secure-anonymous user authentication scheme for e- healthcare application using wireless medical sensor networks. IEEE Syst J. 2019;13(1):456-467.

16. Kodali RK. Elliptic curve based digital envelope in WSN. Paper presented at: 2013 International Conference on Advanced Electronic Systems (ICAES); September 21-23, 2013; Pilani, India; pp. 292-296.

17. Saqib N, Iqbal U. Security in wireless sensor networks using ECC. Paper presented at: 2015 9th International Conference on Advances in Computer Applications (ICACA); October 24-24, 2016; Coimbatore, India; pp. 270-274.

18. Le KH, Lee S, Butoin I, et al. An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography. J Commun. Networks. 2009;11(6):599-606.

19. Alagheband MR, Aref MR. Dynamic and secure key management model for hierarchical heterogeneous sensor networks. IET Inf. Secur. 2012;6(4):271-280.

20. Lee S, Kim K. Key renewal scheme with sensor authentication under clustered wireless sensor networks. Electron. Lett. 2015;51(4):368-369.

21. Chen W-H, Chen Y-J. A bootstrapping scheme for inter-sensor authentication within sensor networks. IEEE Commun. Lett. 2005;9(10):945-947.

22. Jokhio I, Jokhio A, Kemp AH. Light-weight framework for security-sensitive wireless sensor networks applications. IET Wireless Sens. Syst. 2013;3(4):298-306.

23. Choi J, Bang J, Kim L, Ahn M, Kwon T. Location-based key management strong against insider threats in wireless sensor networks. IEEE Syst J. 2017;11(2):494-502.

24. Gardino F, Ferrero R, Montrucchio B, Rebadengo M. Fast hierarchical key management scheme with transitory master key for wireless sensor networks. IEEE Internet Things J. 2016;3(6):1334-1345.

25. Jiang Z, Yang F. Reconfigurable sensing antennas integrated with thermal switches for wireless temperature monitoring. IEEE Antennas Wirel. Propag. Lett. 2013;12:914-917.

26. Petriu EM, Whalen TE, Abielmona R, Stewart A. Robotic sensor agents: a new generation of intelligent agents for complex environment monitoring. IEEE Instrum Meas Mag. 2004;7(3):46-51.

27. Alothi AI. An enhanced symmetric cryptosystem and biometric-based anonymous user authentication and session key establishment scheme for WSN. IEEE Access. 2018;6:70072-70087.

28. Baldini G, Giuliani R, Gentile C, Steri G. Measures to address the lack of portability of the RF fingerprints for radiometric identification. Paper presented at: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS); February 26-28, 2018; Paris, France; pp. 1-5.

29. Zhang L, Yang H, Yu Y, Peng F. A three-dimensional node security localization method for WSN based on Improved RSSI-LSSVR algorithm. Paper presented at: 2018 10th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA); February 10-11, 2018; Changsha, China; pp. 182-186.

30. Ahmed A, Ashraf U, Tunio F, Abu Bakar K, AL-Zahrani MS. Stealth jamming attack in WSNs: effects and countermeasure. IEEE Sens J. 2018;18(17):7106-7113.

31. Wu X, Huang J, Ling J, Shu L. BLTM: beta and LQI based trust model for wireless sensor networks. IEEE Access. 2019;7:43679-43690.