Elliptic Curve Cryptography based Secure Data Communication and Enhance sensor Reliability in Wireless Sensor Network

Uma Maheswari P, Ganeshbabu TR, P.Subramaninan

***Abstract:** Wireless Sensor Network (WSN) extends the advantages of small price, quick employment, and shared transaction medium, although it induces a lot of security and secrecy challenges. In this paper, the Elliptic Curve Cryptography based Secure Data Communication and Enhance sensor Reliability (SDER) in WSN. In this scheme, an Elliptic Curve Cryptography (ECC) Weierstrass function is used to verify the sensor reliability, and ECC cryptography technique is useful for providing the data security in the network. The simulation result demonstrates that the SDER reduces both the packet loss rate and the network delay.*

***Keywords:** data security, Elliptic Curve Cryptography, reliability, Weierstrass function, Wireless Sensor network.*

I. INTRODUCTION

A WSN contains tiny size sensor nodes that are capable of low energy and are proficient of data communications. As a WSN is distributed in a sensing area, these sensor nodes will be in charge to supervise abnormal events, for example, a forest fire or for gathering the sensed data of the surrounding [1]. In the type of a sensor node observing an unnatural occurrence or being set to inform the sensed data regularly, it will send the information to a Base Station (BS) [12].

The major persistent technologies are mostly working for key applications, for instance, industry mechanization [3] and home [2]. Every industrialised network is displayed to security terrors [4]. In exacting, WSN is showing to listening, hardware fiddling, as well as fake information. Thus, the defence of honesty, precision, as well as isolation of WSNs needs efficient protection schemes. Numerous WSNs employ symmetric cryptography that needs two neighboring nodes distributes a general key utilized to encode and decode the information or to validate them. The validation of the symmetrical keys among pairs of nodes in a WSN is known as a key direction [5], [6]. This chore is self-governing of the characteristic of the working encryption method that robustly involves the stage of safety and network routine.

Revised Manuscript Received on January 31, 2020.
P Uma Maheswari*, Electronics & communication engineering, PERI Institute of Technology, Chennai, Tamilnadu, India.
Email: umamaheswari.phd6@gmail.com
TR Ganeshbabu, Electronics & communication engineering, Muthayammal Engineering College, Rasipuram, Tamilnadu, India.
Email:ganeshbabutr@gmail.com
P Subramaninan, professor, Sri Indu College of Engineering & Technology, Hyderabad, India. Email: 69subbu@gmail.com

II. RELATED WORKS

Lightweight System employs a hash-chain key modifying scheme as well as proxy- saved key signature to reach capable, secure communication as well as fine-grained information admission control. Furthermore, this system is used to rearward privacy and reliable protection [7]. The dynamic secret key is useful to intend an encryption method for tidy grid communication. Among deuce parties of transaction, the earlier packets are implicit as transmitting succession here conveyed packet is noticeable as one, another is noticeable as zero. Throughout the transmission, the retransmission is yielded at dual positions to inform the active encoding key. Any mistaking retransmission should avoid the opponent of accomplishing the keys [8]. A secure secret key agreement protocol (SSKA) is applied to a helpful network utilizing standard modulation. Passive attacks from a listener gathered with the relay are measured. However, this scheme cannot provide data security in the system [9]. Hop to hop authentication scheme using ECC. The altering middle node authentication method permits node to communicate an limitless amount of messages lacking tolerating the threshold trouble in the network. Also, this method provides message source privacy [10]. A cross layer frame work is introduced to better data distribution and elastic traffic in multi hop wireless network [13-14]. Key Management introduces a novel key management method is known as random source allocation with a transient captain identity that follows the arbitary sharing of secret objects and a temporary captain identity utilized to produce pairwise keys [11].

III. ELLIPTIC CURVE CRYPTOGRAPHY BASED SECURE DATA COMMUNICATION AND ENHANCE SENSOR RELIABILITY (SDER)

In this scheme, we propose an ECC based Secure Data Transmission and Enhance sensor Reliability (SDER) in WSNs. WSN engage amount of sensors in a wide area and the BS far away from the Sensor nodes. These sensors sporadically examine the surrounding and transfer message to the BS. In SDER, dividing the complete network into a number of clusters should reduce the consumption of energy for data communication. Here, the clusters formed based on the sensor nodes distance and the CH is elected by the sensor residual energy.

A. Unreliable Sensor Detection

At supervising time, all nodes transfer the sensing information

to their CHs, which in turn obtain the data from sensor nodes rather than the CHs check the sensor reliability by ECC commutative property. Here, the ECC algorithm utilizing the Weierstrass Elliptic functions. Assume the coordinate details of the sensor and the CH node be l and m correspondingly; there is another point n which makes a straight line as instanced in figure 1.

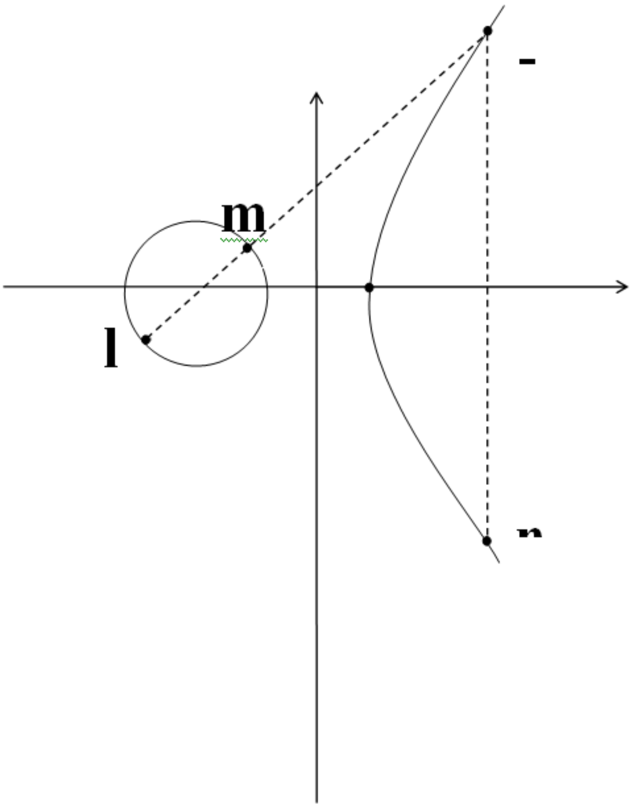

Fig. 1.lliptic Curve acting Sensor and CH Co-ordinates l and m

The Weierstrass Elliptic function is defined in (9),

$$y^2 = x^3 + cx + d \qquad (1)$$

$$l + m = n \text{ where } l \neq m \text{ and } \forall l, m \in E \qquad (2)$$

Where (x_1, y_1) and (x_m, y_m) (x_n, y_n) are the coordinates of the l, m and n points making an elliptic curve E. Thus the coordinates (x_n, y_n) can be found from the next equations.

$$x_n = \gamma^2 - x_1 - x_m \qquad (3)$$

$$y_n = \gamma(x_{1-x_n}) - y_1 \qquad (4)$$

Where, $$\lambda = \frac{y_m - y_1}{x_m - x_1} \qquad (5)$$

The commutative property of this work says that,

$$l + m = m + n \qquad (6)$$

$$Forward_{KEY} = l + m \qquad (7)$$

$$\mathrm{Re}\,verse_{KEY} = m + n \qquad (8)$$

The sensor generates the forward key, and CH generate the reverse key is equal, then the CH accepts the sensor message. Otherwise, CH rejects the sensor message and sends a notification to the network.

B. Secure Data Communication

Throughout path finding, the sensor assures the path node reliability. Although, the listener nodes right to use the information from reliable sensor, to determine this trouble utilizing ECC method. Each node obtains the ECC private as well as public key on the Database. Hence, the listener node does not listen the node information. The sender encode the original information by ECC public key, as well as the BS obtained the real information then it decoded by ECC private key as well as received real information from the sensor nodes.

The message m_s a indicate on EC EC_m next chooses an appropriate curve tip *P* as well as an elliptic Group *G(a,b)* as attributes. The node private key is PR_k as well as computes the public key PU_k is specified in formula (5).

$$PU_k = PR_k * P \qquad (9)$$

The sensor picks a arbitrary key $RK_s \in$ positive integer, the sender encode the message EC_m is certain in equation (6).

$$C_m = RK_s P * EC_m + RK_s PR_k \qquad (10)$$

The BS obtains the C_m message and decrypt

$$D = EC_m + RK_s(PU_k P) - K_{pu}(RK_s P) \qquad (11)$$

At last, the BS decode the message as well as gets the real message from the sensor.

IV. RESULTS AND DISCUSSION

This section reports an execution estimation of the SDER protocol implemented by Network Simulator 2 (NS2). In this section, figure 2, figure 3, figure 4 is a comparison between the SDER and existing method SSKA in WSNs.

The performance of the proposed method SDER regarding data received rate against the simulation time is compared with the existing method SSKA, as revealed in fig.2. The SDER outperforms better data received when compared to the SSKA due to the SDER transmit the data via trusted route and provide data security.

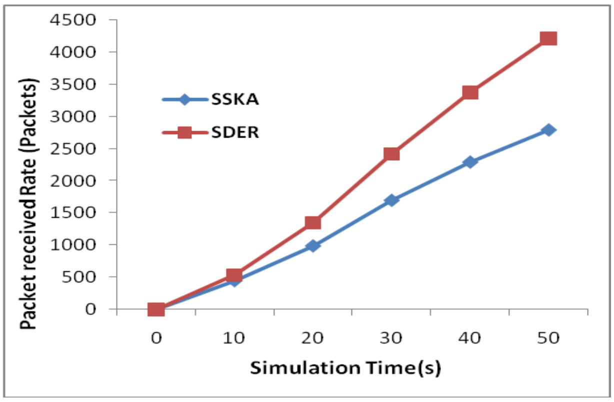

Fig. 2.Packet Received Rate of SDER and SSKA

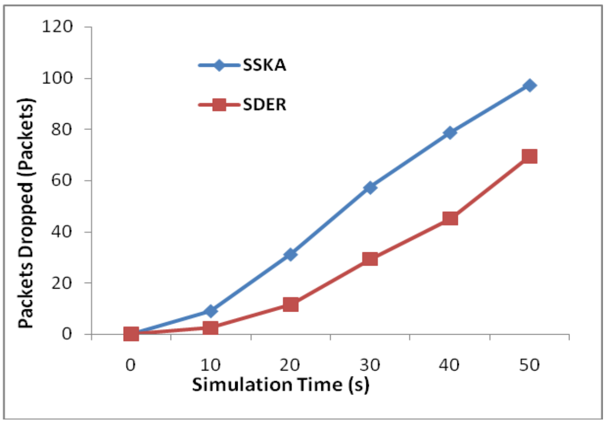

Fig. 3.Data Loss Rate of SDER and SSKA

Figure. 3. demonstrates that the data loss rate of SDER and SSKA. The SDER scheme used the ECC verification method; therefore; unauthenticated node does not loss the packets. Thus the loss rate is very low when compared to the SSKA.

Fig.4. indicate the delay rate of SDER and SSKA. The authenticated node transmits the data to the destination immediately. Therefore, the proposed scheme SDER delay time is very less when compared to the existing method SSKA.

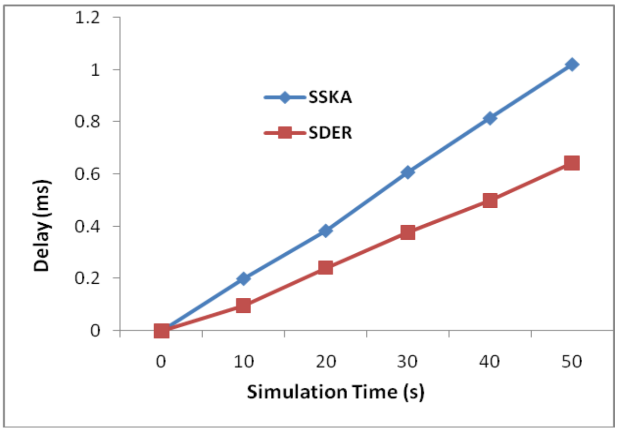

Fig. 4.Average Delay of SDER and SSKA

V. CONCLUSION

In this paper, an Elliptic Curve Cryptography based Secure Data Communication and Enhance sensor Reliability (SDER) in WSN. In this scheme, Elliptic Curve Cryptography (ECC) Weierstrass function is used to verify the sensor reliability, and ECC cryptography technique is to provide the data security in the network. The simulation result proves that enhances the packet received rate and reduces the delay in the network.

REFERENCES

1. C.F. Wang, J. D. Shih, B. H. Pan, and T. Y. Wu, "A network lifetime enhancement method for sink relocation and its analysis in wireless sensor networks", IEEE sensors journal, Vol. 14, No. 6, 2014, pp. 1932-1943.
2. J. C. Wang, C. H. Lin, E. Siahaan, B. W. Chen, and H. L. Chuang, "Mixed sound event verification on wireless sensor network for home automation", IEEE Transactions on Industrial Informatics, Vol. 10, No. 1, 2013, pp. 803-812.
3. P. Gaj, J. Jasperneite, and M. Felser, "Computer communication within industrial distributed environment—A survey", IEEE Transactions on Industrial Informatics, Vol. 9, No. 1, 2012, pp. 182-189
4. M. Cheminod, L. Durante, and A. Valenzano, "Review of security issues in industrial networks", IEEE Transactions on Industrial Informatics, Vol. 9, No. 1, 2012, pp. 277-293
5. J. C. Lee, V. C. Leung, K. H. Wong, J. Cao, and H. C. Chan, "Key management issues in wireless sensor networks: current proposals and future developments", IEEE Wireless Communications, Vol. 14, No. 5, 2007, pp. 76-84.
6. J. Zhang, and V. Varadharajan, "Wireless sensor network key management survey and taxonomy", Journal of network and computer applications, Vol. 33, No. 2, 2010, pp. 63-75.
7. D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks", IEEE journal of biomedical and health informatics, Vol. 18, No. 1, 2013, pp. 316-326.
8. T. Liu, Y. Liu, Y. Mao, Y. Sun, X. Guan, W. Gong, and S. Xiao, "A dynamic secret-based encryption scheme for smart grid wireless communication", IEEE Transactions on Smart Grid, Vol. 5, No. 3, 2013, pp. 1175-1182.
9. N. Wang, N. Zhang, and T. A. Gulliver, "Cooperative key agreement for wireless networking: Key rates and practical protocol design", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 2, 2013, pp. 272-284.
10. J. Li, Y. Li, J. Ren, and J. Wu, "Hop-by-hop message authentication and source privacy in wirelesssensor networks", IEEE transactions on parallel and distributed systems, Vol. 25, No. 5, 2013, pp. 1223-1232.
11. F. Gandino, B. Montrucchio, and M. Rebaudengo, "Key management for static wireless sensor networks with node adding" IEEE Transactions on Industrial Informatics, Vol. 10, No. 2, 2013, pp. 1133-1143.
12. K. Balaji, "Design and Analysis of Increasing throughput and minimising gross layer operations in IEEE 802.11 WLAN", International Research Journal of Engineering and Technology,2016.
13. K. Balaji, "A frame work for integrated routing, scheduling and Traffic Management in MANET" International Research Journal of Engineering and Technology, 2015.
14. T. A., Shanmugasundaram, V. Vijayabaskar, "A novel approach for energy efficient clustering in heterogeneous w ireless sensor networks" , ARPN Journal of Engineering and Applied Sciences, Vol. 10, No. 5, 2015, pp. 2172-2176

AUTHORS PROFILE

P. Uma Maheswari *, received the BE degree in Electronics and Communication Engineering from Bharathidasan University, Tiruchirappalli, Tamilnadu, India in 2003, and the ME degree in Communication Systems from Anna University, Chennai , Tamilnadu, India in 2008 respectively. She is currently an Assistant professor in the Electronics and Communication Engineering Department at PERI Institute of Technology, Chennai, Tamilnadu, India and working towards the PhD degree in the faculty of Information and Communication Engineering at Anna University, Chennai, Tamilnadu, India. Her research interests include wireless networks, routing protocols, applications and security issues in wireless sensor networks.

T. R. Ganeshbabu, received the DECE degree in Electronics and Communication Engineering from Swami Abedhanandha Polytechnic, Tamilnadu, India in 1988, the AMIE in Electronics and Communication Engineering from the Institute of Engineers, India in 1993, the ME degree in Applied Electronics from Bharathiyar University, Tamilnadu, India in 2001 and PhD in Medical Electronics from Anna University, Chennai, Tamilnadu, India in 2014 respectively. He is currently a Professor in the Electronics and Communication Engineering Department at Muthayammal Engineering College, Rasipuram, Tamilnadu, India. His research interests include signal processing, Image processing, Networks and Antennas.

Dr.P.Subramanian, received his MCA degree from Bharathidasan University, Trichy, India in 2002 and M.Tech with Computer Science and Engineering from SRM University, Chennai, India in 2007. He received the Ph.D, degree from St. Peter's University, Chennai, India in 2016. From 2003 to 2008, he worked with Valliammai Polytechnic College as a Lecturer. From 2008 to 2016 he worked with Shri Andal Alagar College of Engineering as Associate Professor during the time of relieving. From 2016 to 2018 he worked with Guru Nanak Institute of Technology, Hyderabad as Professor and Head for IT Department. Since 2018 he has been with Sri Indu College of Engineering & Technology, Hyderabad as Professor.