DOI: https://doi.org/10.46632/jeae/1/2/10

Journal on Electronic and Automation Engineering

Vol: 1(2), 2022

REST Publisher; ISSN: 2583-6951

Website: https://restpublisher.com/journals/jeae/

Enhanced Identity Based Encryption of Security for Wireless Sensor Network

[*]R. Venkadesh, R. Vijayarajeswari, N. Rajkumar, R. Sujitha

Mahendra Engineering College, Namakkal, Tamil Nadu, India.

[*]Corresponding author Email: venkadeshr@mahendra.info

Abstract: *Wireless Sensor Network (WSN) is defined as an ad hoc network setting that includes devices with limited resources for bandwidth, storage, computation time and energy. In the environment of WSN, security makes a substantial contribution to increased processing and energy in the nodes. Sensor nodes are used for remotely controlling network topology in dangerous environments. The secure data transmission over a network has garnered a lot of attention. The design of the key management scheme is required for future research because the mechanism of security management plays the vital role in WSN. Identity-based Encryption (IE) has experienced limited acceptance, owing to the complete confidence required of the private key generation utilizing Elliptic Curve Cryptography (ECC). The security in WSN has become a significant issue in the sensor network. The data get transformed from one node to another must be secured to avoid a data breach by any of the attackers. The link must be secured to ensure data efficiency and greater accuracy. This paper proposes the enhanced ECC algorithm for providing identity-based key encryption in cluster-based WSNs. A separate key generation concept has been proposed here for reducing the network complexity. The node-to-node has less number of key generations and the cluster head-to-sink node has a larger number of key generations. The outcome show that the suggested method holds well in minimizing the timing requirements for key generation, computation time is less, less energy consumption communication, and better packet-to-delivery ratio.*

Keywords: *Identity-based Encryption (IE), Elliptic Curve Cryptography, Wireless Sensor Network, cluster based, security management*

1. INTRODUCTION

WSNs generally contain wireless sensor with tens to thousand nodes that connect over wireless channels enabling data transfer as well as collaborative analysis [1]. It may be used on a global basis for tracking the environment and ecosystems in factories for maintenance based on circumstances whereas in building enabling infrastructural health monitor, in households to create smart homes, in individuals for patient tracking, etc. [2, 3]. WSN is made up of sensors, computers, connectivity, actuators, and energy sources [4]. These components are incorporated onto one or more panels. Sensor nodes are located in a specific region for tracking actual environmental or physical situations like pressure, sound, temperature, motion, location, etc. [5]. It's commonly employed in military applications. Typically, the surroundings is hostile or in a catastrophe zone. The existence of malicious nodes in the sensor network causes a variety of security issues [6]. Significant research concerns in WSN are energy, hardware and software issues, self-management, MAC layer issues, collecting and transmission of data, implementation, decentralized management, multi-media communication, synchronization, and real-time operations [7]. Because of the essential properties of sensor nodes, security is an essential and critical concern. This research concentrates on security attacks over WSN. The WSNs have a wide range of applications, including military, traffic control, smart healthcare, and smart homes [8]. As an instance in medical health, it has significantly improved the human race [9]. In an application procedure, data communication must be secure. When there is no encrypted transmission of data over network, an intruder can easily get sensitive data or potentially counterfeit certain data in order to compromise the network, casting the security and confidentiality of the data in the network is doubt. Key management allows for secure communication keys enabling data transfer among network nodes, ensuring message integrity, confidentiality, authentication, etc. Nodes from sensor network have limited storage capacity, less computing power as well as less reserves of energy. Because

of symmetric encryption algorithms both decryption and encryption processes require less energy which frequently employed for securing data transmission over the network [10]. Moreover, symmetric encryption techniques are unable to perform full digital signature authenticity. Conventional public key encryption methods, such as Ron Rivest, Adi Shamirh, and Len Adleman (RSA) are capable of offering security when the length of the key (a minimum of 1024 bits) is sufficient but the increase in key length has accumulate computing overhead. Existing method of public key encryption are deemed unsuitable for sensor network nodes due to their enormous storage space requirements, and high energy consumption, high computational complexity. Improvement of ECC algorithm while performing real-world tests on sensor nodes has demonstrated that ECC may be used to limited resources WSNs. An additional issue to take into account is that conventional public key infrastructure (PKI) generates a public key certification to each node for assisting to verify the authenticity of other public key parties. Therefore, the certificate generation, publishing, verification and storage demand is enormous quantity of resources from the network. It is admirable that the new IE scheme addresses this issue. Clustering is the course of action of grouping sensor nodes in an extensive sensor network that has been deployed extensively. The cluster head is picked from each node in the cluster's center. Local communication, also known as intra-cluster communication means communication that occurs inside a cluster. Inter-cluster communication means communication involving two separate clusters. The sensing region is determined and then geometrically split into N grids of equal size. Sensors are then cautiously placed in every grid box, each batch with an initialized CH node. To boost security, the updated protocol generates a new secret key for each identity by utilizing the master secret key. An encapsulation algorithm is also used to confound the attackers. The message is encrypted in the technique by utilizing the associated sender's ID, which yields the right ciphertext and the incorrect ciphertext. The right and incorrect ciphertexts are then wrapped with the appropriate author's encapsulated key and sent to the recipient. Receivers would make sure whether an encapsulated key matches the novel encapsulated key and obtain suitable communication during the decapsulation process. Inadequate security procedures can lead to the loss of valuable, personal, and sensitive data from many sensor systems. It's also leading customers and users to lose faith in WSN. In the worst-case situation, selection and data destruction or alteration might result in unrecoverable consequences. Other negative consequences of weak security precautions include excessive network congestion and overburdened servers, user distrust, and costly recovery costs. There are several concerns and obstacles in designing and proposing a reliable method for WSN. Some of the most promising issues and challenges for security in WSN are, Deployment and maintenance methods, wireless connectivity, power outage, malware, and numerous security assaults all affect reliability.

2. LITERATURE REVIEW

Tyagi and Kumar have illustrated the user authentication with multi-factor as well as key agreement scheme in WSNs by Chinese remainder theorem [11]. Similarly, Darbandeh and Safkhani have introduced a secured authentication protocol to WSNs with respect to RFID tags [12]. Khah et al. have proposed a key management with dynamic and multi-level in WSNs [13]. Chen et al. have created a verifiable-secured protocol with authenticated key agreement to monitor system for the remote patients [14]. Li et al. have suggested an undetectable authentication as well as key agreement technique for smart homes. To ensure the private transfer of highly sensitive data, the approach employs just extremely low-cost bit-wise operations as well as hashing techniques. For encryption of a confidential parameter, the technique considers timestamps as random strings, as well as a user's identity also serves to be a random number [15]. In this section, researchers demonstrate that the approach suffers from certain design flaws, namely the sensor node anonymity loss, the loss of user anonymity as well as untraceability, insecurity towards offline password guessing attacks, and insecurity towards impersonation intruders. To the best of our ability, these analysis methodologies to authentication as well as key agreement procedures have not previously been developed. Wormhole detection by mobile beacon-based is being considered in WSNs. Attackers are precisely targeted and exterminated. If the mobile communication properties as well as static beacon have been violated, the junction point of the chords' perpendicular bisector becomes known [16]. The wormhole attacker is positioned at the middle of the communication disk. Mobile beacons travel throughout the network to communicate with static beacons. The authors provided compromise-tolerant security technique with a location-based that detects wormholes using location-based keys. Each node consists of unique private key that get associated with its location and it’s ID. The node-to-node authentication protocol is also get explained and execute completely with respect to location-specific keys [17]. It is an effective wormhole preventative measure. When the node falls into communication range as well as has location-based keys, it can be identified as a legitimate neighbor. When the node is not in communication range, the process of authentication is refused. The authors developed wormhole mitigation in mobile multi-hop wireless networks utilizing a secure

localization as well as key distribution mechanism [18]. Each sensor node stores communication keys. If two sensor nodes are in communication range of one another, they can exchange the communication key. When the nodes fail to stay in communication range, they are unable to exchange a communication key. The node fails to process a message that arrives from a neighbor connection by means of tunnel due to it lacks of shared key required for decryption. The authors provided a secure range-independent localization technique to wormhole detection whereas the locators send the beacon data [19]. Each sensor node determines its precise position using the beacon data. This approach is range-independent as well as distributed. Wormholes are found when the transmission range violations as well as sector uniqueness properties have been met. Daniela and Giovanni [20] simplified the use of AES in WSN by proposing a seven-round encryption scheme and combining these with the tabular lookup approach to optimize every round of activity. (Simulated test results indicate that such a technique has considerably increased operational efficiencies, including a performance that is 13 times faster than a popular AES algorithm that requires just lesser than 1 KB of storage capacity. Even though the security is less than that of the typical AES encryption technique, it is still appropriate for low-energy WSNs. Resist the node replication attack. Replication attack occurs when an intruder acquires a node and duplicates it in various geographic areas in order to create an illicit communication link with a genuine node. There are certain approaches to prevent node replication attacks [21]. In this design, the BS pre-allocates data regarding each node's communication neighbors inside the network. Simultaneously, they employ the neighbor node authentication process, as well as the legal node that declines the request for the replica node's data, preventing it from passing the authentication and establishing an encrypted communication channel. As a result, the method has proved successful against node replication attacks. Moreover, network weak point protection is based on location data for relay nodes is protected. Similar to the need for safeguarding certain vital private information in daily lives, it must prevent certain significant data from becoming accessible [22].

3. RESEARCH METHODOLOGY

This section describes the proposed work and it's working. The nodes are randomly deployed in the sensing field and can interact with each other within their communication range. The nodes are static and sense the sensing field in a TDMA manner. The nodes are homogeneous and clusters are formed. The cluster has Cluster Head (CH) and all other intermediate nodes. All the nodes in the cluster will communicate with the CH and send their data promptly. During the transmission of data, the intermediate nodes being utilized are located between the source node and the CH. To restrict the access of data by the unauthorized nodes/computers the link has been encrypted to ensure that the data should not be breached at any point of time during its movement from node to node or node to CH. The enhanced ECC encryption technique has been utilized which is made of two phases. The low-level key generation has been applied for the node to node communication within the cluster that generates less number of keys for encryption and decryption and high-level key generation is applied between CH to CN communication. The system architecture is shown in figure 2. Authors assume the network under investigation to be a WSN throughout this study. Sensor nodes in this scenario are resource-constrained sensors with similar operations and capacities. BS, on the other hand, is often presumed to be secure and honest and has been responsible for customizing the nodes before the network's installations. Moreover, each node is randomly dispersed. We believe that an intruder is either active or passive throughout this study. Both nodes and BS were fixed. The tier-1 encryption has been provided between a node to node and also node to CH. The tier-2 encryption has been enabled between CH to SN which generates more keys for better security than the tier-1. The CH selection is energy efficient to improve the overall network lifetime. The CH is selected based on the energy criteria, distance to SN, and available residual energy. Multi-hop communication is adapted for the transmission of information from a source node to CH. During the transmission, the link has been secured for restricting unauthorized access by any of third party. The following are the key goals of this paper, (1) Utilizing elliptic curve cryptographic approach and digital signatures, create a cryptography-based mechanism to encrypt information sharing across WSNs, (2) To ensure that every node in the transmission path maintains its validity and authenticity and (3) To compare the proposed method to other mechanisms currently in use. The information to be forwarded towards other nodes is signed using Elliptic Curve Cryptography (ECC). Every node would be given an ID as well as other information to sign and validate communications at first. Messages are usually signed with the sender's private key as well as other properties, whereby the recipient can verify. Aggregate-verify is indeed envisioned, which aids in the certification of multiple messages at once following aggregation. Elliptical Curve Cryptography is a type of cryptography that works with groups of points on an elliptic curve. The security is based on the elliptic curve discrete logarithmic problem ECDLP's difficulty. The exponential technique is the most well-known solution for finding ECDLP. This means as compromising ECC is much harder than compromising RSA. With a

lower-key size, ECC may provide having a similar degree of security to RSA, for example, 128 Bit ECC can give equivalent security to the traditional 1024-bit RSA. Shorter key sizes frequently result in faster throughput and bandwidth, storage, and energy savings. As a result, ECC is more suitable for devices with limited resources, such as WSN. There are several weaknesses with ECC, including side-channel attacks and twist-security risks. Both types attempt to breach the ECC's private key security. Side-channel attacks like differential power attacks, fault diagnosis, regular power attacks, and fundamental scheduling attacks are all too frequent. There are simple countermeasures for all types of side-channel attacks. The fundamental signing and verification procedure of digital signatures utilizing an elliptic curve cryptographic technique is shown in Figures 3 & 4.

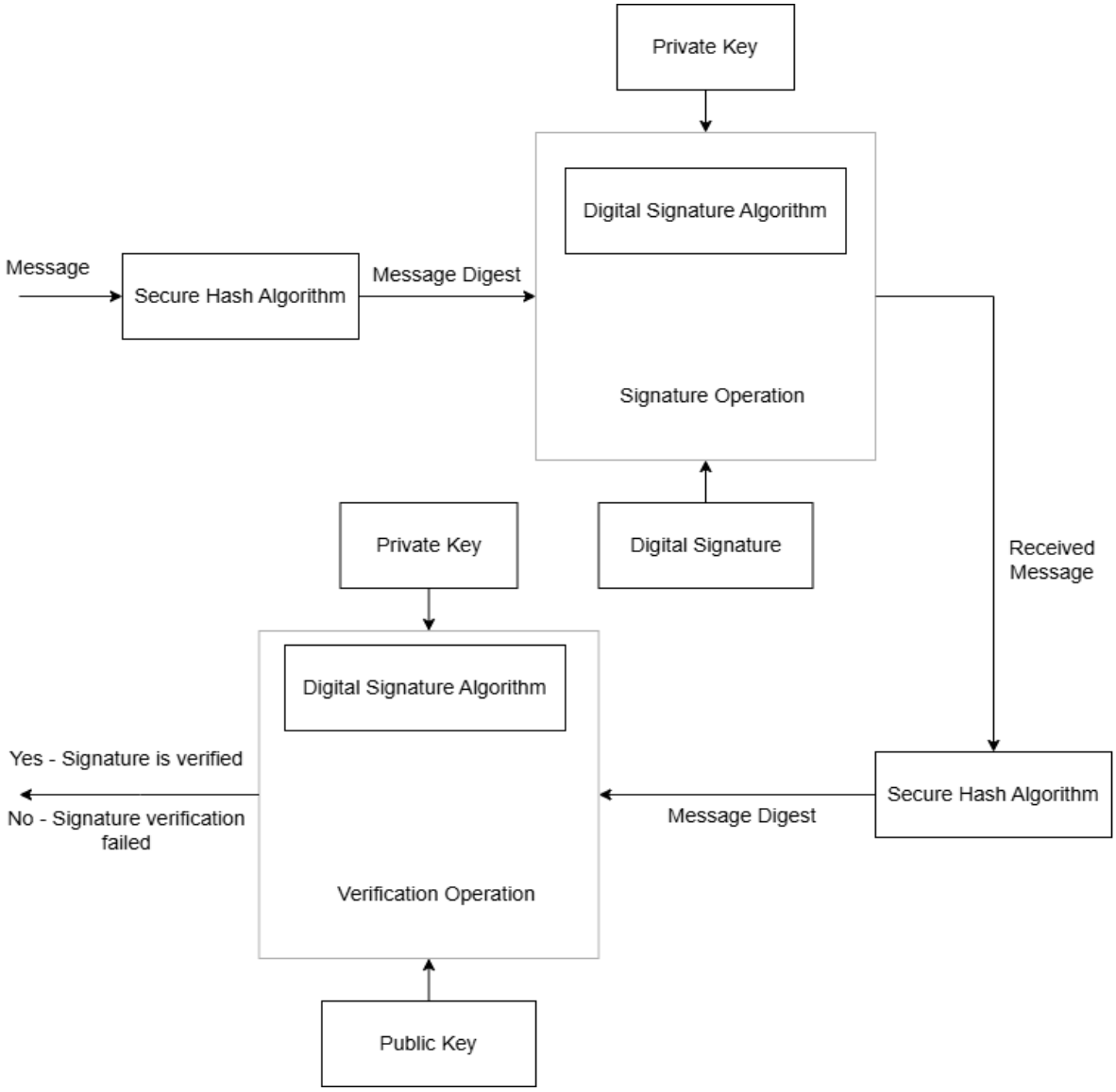

FIGURE 1. Proposed framework for ECC-IE

Elliptic curves may be found in a wide range of mathematical fields, from mathematicians to cryptographic. Elliptic curves have been used in security since the invention of ECC that is gaining prominence in public key cryptography. ECC is built on mathematical notions involving elliptic curves in Galois Fields. Such regions can be binary (GF(2n)) or prime fields G F(P). ECC-based cryptographic techniques depend on the difficulties of computing the discrete logarithm of an elliptic curve. Scalar multiplier is the act of adding P to its own x times to produce point $Q = xP \in$

Fp provided an integer x and a point $P \in Fp$. The discrete logarithm of point Q to base P, given by $k = logPQ$, is indeed the value x. Scalar multiplying in elliptic curve points can be effectively calculated by combining the adding rules with the double-and-add method along with its variations.
ECC is comprised of three stages: key creation, signature method, and verification method.

Key Mechanism: The sender (signer) is the only one who has access to the private key in AWSC, which is used to produce signatures. The public key, on the other hand, is disseminated to everyone communicating parties and may be validated by any trustworthy person.

Key Generation: In ECC, the sender chooses the private key at randomized and uses formulae to calculate the public key. Where'd' is the caller's private key and 'A' is the elliptic curve's coordinates.

$B= d.A$

Key Sharing Mechanism: The transmitter has access to the private key, while the recipient has access to the public key through a security gateway such as Diffie– Hellman key distribution or another key agreement method.
Signing Mechanism: The pre-computation of the hash or digestion of the information to be signed utilizing a secured hash algorithm would be the first step in the signing process. Step 2 is to use a random generator to generate a random number, which will serve as the basis for something like the elliptic curve computations. After then, the information is signed, and the transmitter transmits a random number to the recipient including a signed message.

Verifying Mechanism: The next method is known as the verifying mechanism. Whenever a signed message reaches the receiving side, the authentication of the message may be checked utilizing the public key of the authentication system, in this instance the transmitter. The hash is produced on the receiver section, together with the public key and the variables of digital signatures, using the same hash technique that was used for signing the data. Those hashes are therefore checked, and the signatures were verified if they agree; else, the confirmation might fail.

Communication Mechanism: For data communication execution, two types of nodes are classified. The first stage requires the nodes to verify it using previously saved data.

One must produce both a public and a private key as part of the key creation process. The communication would be encrypted with the user's public key and decrypted with the recipient's private key. They must now choose a number‘d’ from the set of 'n'. Utilizing equation 1 illustrate the obtained public key.

$$B = d.A \quad (1)$$

‘A’ is the point on the curve, ‘B’ is the public key and‘d’ is the private key. Where n= (n-1)/2 for communication between node to HN and n= (n-1) for communication between HN to SN.

Encryption

Let's make 'm' the message we're conveying. This message must be represented on the curve. Consider 'm' as the 'M' on the 'E' curve. Choose 'k' at random from the range $[1 - (n - 1)]$. Following encryption, cipher texts (C1 and C2) would be created is expressed in equation 2.

$C1 = k * A$

$$C2 = M + k * B \quad (2)$$

Decryption

The transmitted message 'M' is expressed as the expression in equation 3

$$M = C2 - d * C1 \quad (3)$$

4. RESULT AND DISCUSSION

This section shows the results of the proposed enhanced ECC algorithm for key generation for providing identity-based security in WSN. On the Sensor Network, we employed the ECC technique with minimal modifications. The success of the ECC method is determined by the complexity of processing discrete logarithms that raises the method's

efficacy. The results of the proposed work have been depicted using four parameters, namely key generation time, energy consumption, and packet delivery ratio.

Packet Delivery Ratio (PDR)

The packet delivery ratio (PDR) is the ratio of the total of packets sent through the number of packets received as a percentage of the total number of packets sent. The formulae is expressed in equation 4

$$PDR = (No.of\ packets\ received\ /\ No.of\ packets\ sent) * 100 \quad (4)$$

Figure 2 illustrate the PDR for proposed ECC-IE method and it is compared with traditional ECC and Data Encryption Standard (DES) method. The PDR ratio is increasing with the increase in the number of nodes. Based on the involvement of two key generation proposals, the PDR is high and better for the ECC-IE while compared with traditional ECC and DES.

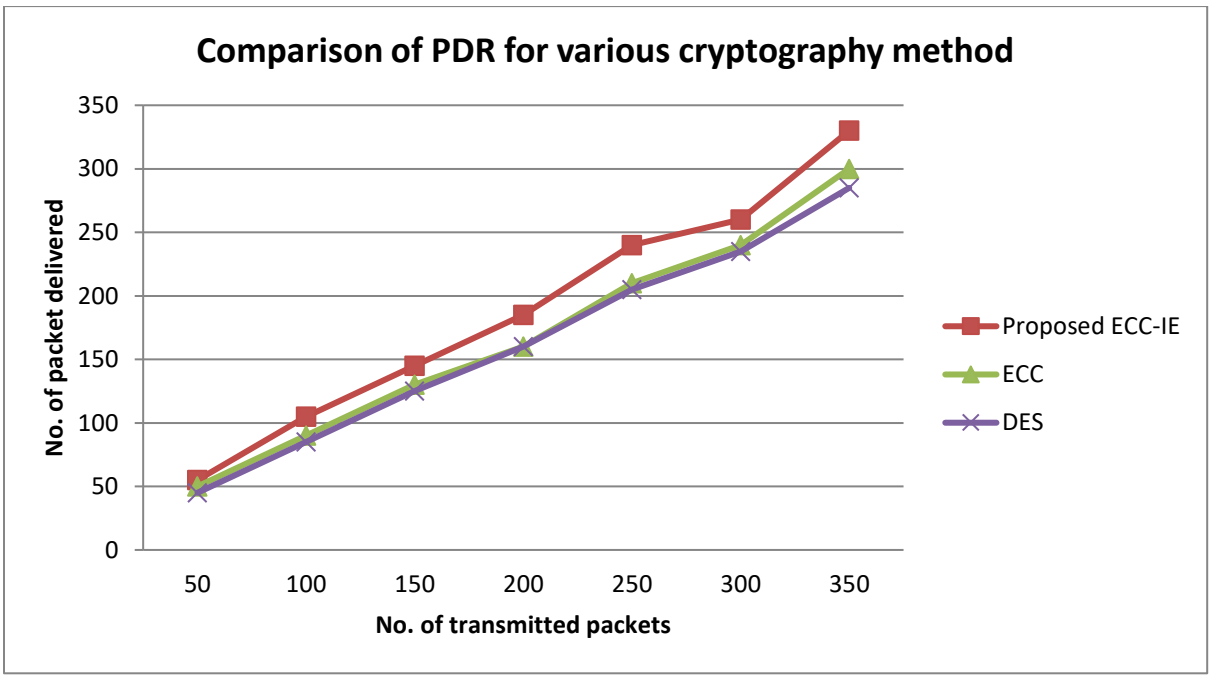

FIGURE 2. Comparison of PDR for various cryptography methods

Key generation time

The key generation time by the proposed work requires very less as the proposed ECC-IE defined two types (2 tiers) of key generation techniques. Figure 3 illustrates the key generation time of the proposed work has been compared with the traditional ECC and DES method and it has been observed that the timing requirement for the ECC is more compared with ECC-IE but lesser than DES. Moreover, the time consumed for key generation is very high in DES method. The key generation time is as shown in figure 8.

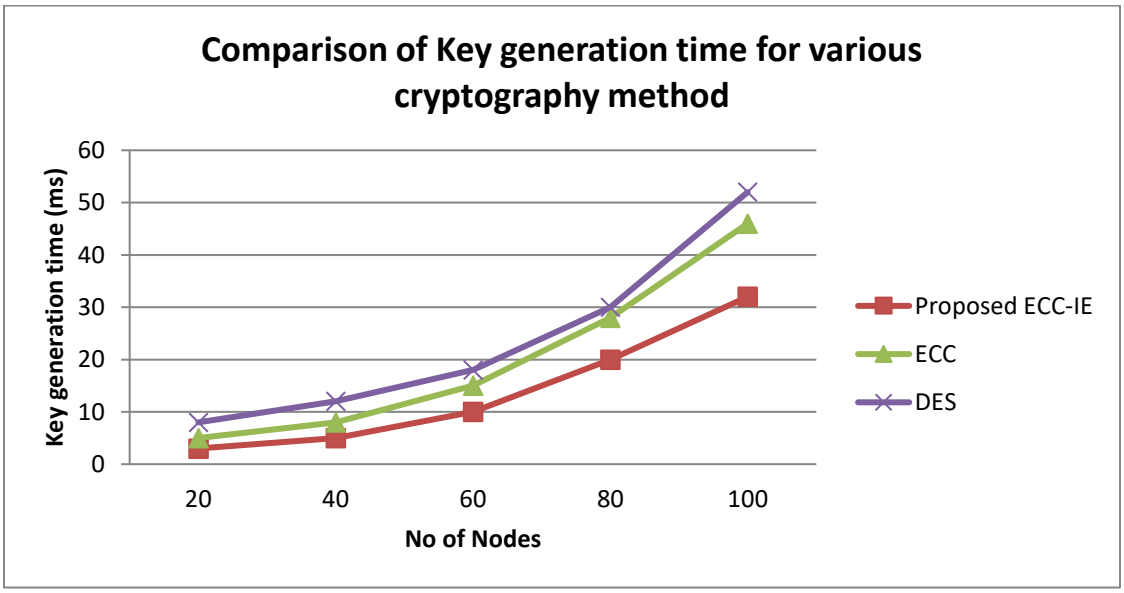

FIGURE 3. Comparison of key generation time for various cryptography methods

Energy Consumption

Energy consumption has defined to be an overall energy consumed for transmission, reception, sensing, aggregation, encryption, decryption, and key generation. The proposed utilizes the multipath routing technique to send the sensed data to HN and HN to SN. The energy required for key generation and encryption is also less whenever there is a transmission between node and HN. Overall the energy consumption is less in the proposed ECC-IE compared to the other two traditional ECC and DES method. The energy consumption is more as the data transaction requires more energy and there is no proper key management scheme. Figure 4 illustrate the consumption of energy is very low in proposed ECC-IE while compared with other traditional ECC and DES method.

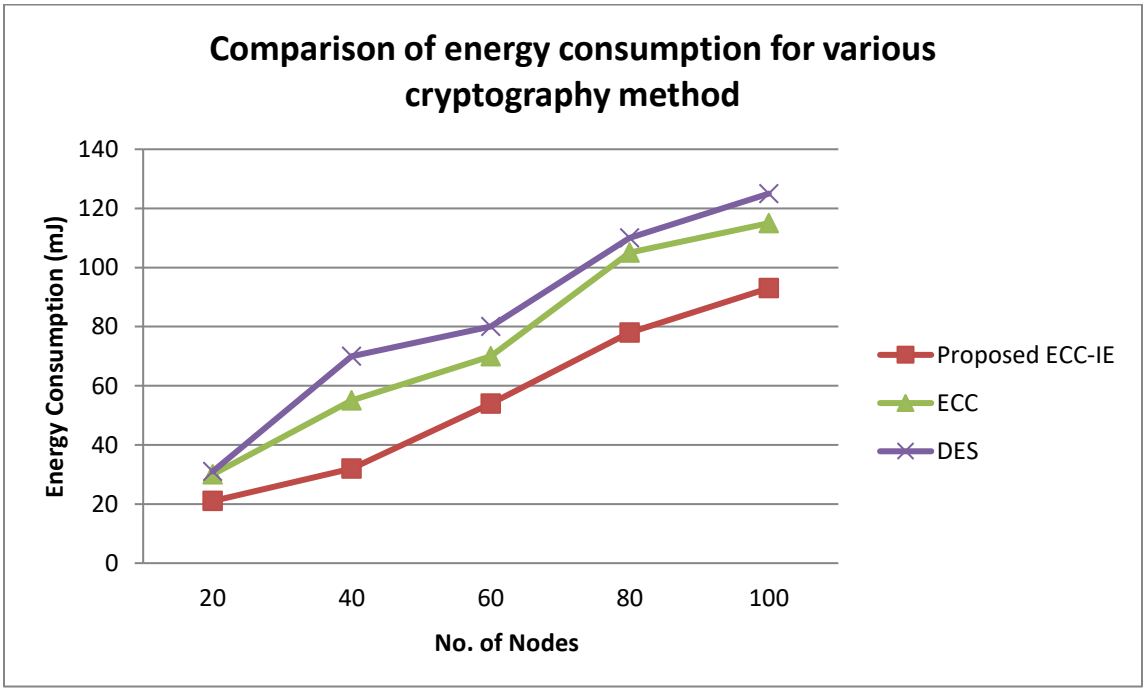

FIGURE 4. Comparison of energy consumption for various cryptography methods

5. CONCLUSION

This paper gives a comprehensive security analysis of a proposed construction for reducing trust in an IE system's PKG. In specifically, the analysis encompasses all of the different sorts of entities in the environment, models the assaulting entities as either honest-but-curious or malicious, and takes into account collaborations between all groupings of hostile entities. The security analysis demonstrates that a great deal of attacks that acquire a user's plaintext may be avoided by selecting suitable system parameters, implementing security mechanisms beyond the scope of IE, like identity authentication and the open-world setting benefits, as well as require the multiple randomly participation of selected entities in particular assignments. It determines the processes necessary for the sensor in the architecture. The proposed work defines two-tier keys while transmitting data from the source node to SN via HN. Identity-based key generation is proposed here with the use of an ECC-IE method for reducing the complexity and minimizing the overall time. The proposed work result gets compared with conventional ECC and DES method. It is found that the proposed work works far better than the other two protocols considering the parameters like energy efficiency, PDR and key generation time.

REFERENCES

[1]. P. Roy, A. K. Tripathy, S. Singh, and K. C. Li. Recent advancements in privacy-aware protocols of source location privacy in wireless sensor networks: A survey. Comput. Sci. Inf. Syst., 19(2):857{886, 2022.

[2]. C. M. Chen, L. Chen, Y. Huang, S. Kumar, and J. M. T. Wu. Lightweight authentication protocol in edge-based smart grid environment. EURASIP J. Wirel. Commun. Netw.,, 2021(1):68, 2021.

[3]. T. Sampradeepraj, V. A. Devi, and S. P. Raja. Secure multicasting in wireless sensor networks using identity based cryptography. Concurr. Comput. Pract. Exp.,, 35(1), 2023.

[4]. M. L. Chiang, H. C. Hsieh, T. L. Lin, T. P. Chang, and H. W. Chen. Dynamic weight-based connectivity recovery in wireless sensor and actor networks. J. Supercomput., 80(1):734-760, 2024.

[5]. Cao, C., Tang, Y., Huang, D., Gan, W., & Zhang, C. (2021). IIBE: an improved identity-based encryption algorithm for WSN security. Security and Communication Networks, 2021.

[6]. Singh, S., & Saini, H. S. (2021). Learning-based security technique for selective forwarding attack in clustered WSN. Wireless Personal Communications, 118(1), 789-814.

[7]. Qichen, W. (2022, April). Research progress on wireless sensor network (WSN) security technology. In Journal of Physics: Conference Series (Vol. 2256, No. 1, p. 012043). IOP Publishing.

[8]. Kandris, D.; Nakas, C.; Vomvas, D.; Koulouras, G. Applications ofWireless Sensor Networks: An Up-to-Date Survey. Appl. Syst. Innov. **2020**, 3, 14.

[9]. Yang, Y.; Liu, X.; Deng, R.H.; Li, Y. Lightweight Sharable and Traceable Secure Mobile Health System. IEEE Trans. Dependable Secur. Comput. **2020**, 17, 78–91.

[10]. Cheng, S.; Wang, L.; Ao, N.; Han, Q. A Selective Video Encryption Scheme Based on Coding Characteristics. Symmetry **2020**, 12, 332.

[11]. G. Tyagi and R. Kumar. Multi-factor user authentication and key agreement scheme for wireless sensor networks using Chinese remainder theorem. Peer Peer Netw. Appl.,, 16(1):260{276, 2023.

[12]. F. G. Darbandeh and M. Safkhani. SAPWSN: a secure authentication protocol for wireless sensor networks. Comput. Networks,, 220:109469, 2023.

[13]. S. A. Khah, A. Barati, and H. Barati. A dynamic and multi-level key management method in wireless sensor networks (WSNs). Comput. Networks,, 236:109997, 2023.

[14]. C. M. Chen, S. Liu, X. Li, SK H. Islam, and A. K. Das. A provably-secure authenticated key agreement protocol for remote patient monitoring iomt. J. Syst. Archit.,, 136:102831, 2023.

[15]. F. Li, X. Yu, Y. Cui, S. Yu, Y. Sun, Y. Wang, and H. Zhou. An anonymous authentication and key agreement protocol in smart living. Comput. Commun.,, 186:110{120, 2022.

[16]. Butt, T. M., Riaz, R., Chakraborty, C., Rizvi, S. S., & Paul, A. (2021). Cogent and energy efficient authentication protocol for wsn in iot. Comput. Mater. Contin, 68, 1877-1898.

[17]. Rhim, H., Tamine, K., Abassi, R., Sauveron, D., & Guemara, S. (2021, March). Enhancing security using digital signature in an efficient Network Coding-enabled WSN. In 2021 18th International Multi-Conference on Systems, Signals & Devices (SSD) (pp. 70-78). IEEE.

[18]. Gulganwa, P., & Jain, S. (2022). EES-WCA: energy efficient and secure weighted clustering for WSN using machine learning approach. International Journal of Information Technology, 14(1), 135-144.

[19]. Bakshi, G., & Sahu, H. WSN Security: Intrusion Detection Approaches Using Machine Learning. In Computational Intelligence for Wireless Sensor Networks (pp. 151-174). Chapman and Hall/CRC.
[20]. De Venuto, Daniela, and Giovanni Mezzina. 2018. "Spatio-Temporal Optimization of Perishable Goods' Shelf Life by a Pro-Active WSN-Based Architecture" Sensors 18, no. 7: 2126. https://doi.org/10.3390/s18072126
[21]. Li, L.; Xu, G.; Jiao, L.; Li, X.; Wang, H.; Hu, J.; Xian, H.; Lian, W.; Gao, H. A Secure Random Key Distribution Scheme Against Node Replication Attacks in IndustrialWireless Sensor Systems. IEEE Trans. Ind. Inform. 2020, 16, 2091–2101.
[22]. Du, A.; Wang, L.; Cheng, S.; Ao, N. A Privacy-Protected Image Retrieval Scheme for Fast and Secure Image Search. Symmetry 2020, 12, 282.