IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Identity based key agreement for security in WSN using enhanced ECC technique

Vishal More[1], B. Suryakanth[2], Sangamesh J. Kalyane[1]

[1]Department of Computer Science and Engineering

[2]Department of Electronics and Communication Engineering

Bheemanna Khandre Institute of Technology, Bhalki and

Affiliated to Visvesvaraya Technological University, Belagavi, INDIA

ABSTRACT: Cluster-based Wireless Sensor Network information privacy is regarded as a difficult challenge for this sort of network. Because of the dynamic environment of WSNs and their deployment in open regions, they are subject to a variety of cyber-attacks that might disrupt their operations. Furthermore, due to the resource constraints of sensing devices, traditional security approaches in WSNs are impracticable due to the high cost of computing, communications, and memory capacity. The security in WSN has become a significant issue in the sensor network. The data which is transmitted 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 to reduce the complexity of the network. 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 results show that the proposed work holds good in minimizing the timing requirements for key generation, computation time is less, less energy consumption communication, and better packet-to-delivery ratio.

Keywords: WSN, Security, ECC, Cluster, Encryption Key

1. INTRODUCTION

Wireless Sensor Network (WSN) has been paid attention by several industry leaders and researchers in the past few years due to their potential applications in defense, control systems, and medical treatments. Cluster-based WSN (CWSN) is among the recommended strategy to reach networking expansion and energy efficiency in literary works. As illustrated in Figure 1, the CWSN network is separated into numerous clusters/sections. Every cluster has a Cluster Head (CH) who is in charge of gathering information across all nodes through its cluster and then forwarding this to the Base Station (BS) following an aggregation procedure. Although most sensors have been deployed in defenseless or even remote places, most WSN approaches involve high security to meet basic security standards and to render such applications resilient to various cyber-attacks, restricting an attacker from disrupting the network's positive function by seizing the power of sensors. Lighting, pressure, moisture, pollution levels, temperature, and vehicle speed are employed in a wide range of life-changing applications, including medicine, nuclear energy, electrical boilers, pollution monitoring, disaster response, military surveillance, and home automation systems in almost every section WSN are employed [1] [2]. The security of connections would be another key problem that impacts the use of CWSN. Wireless connections seem to be unsafe by definition, and an attacker can overhear and manipulate contents sent across nodes by exploiting these vulnerabilities. The basic WSN architecture is shown in figure 1.

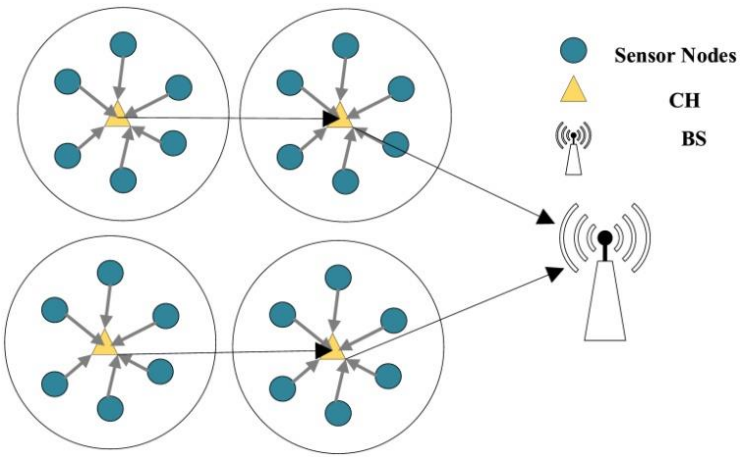

Figure 1: Wireless Sensor Network

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 [3]. 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.

The following are the basic security criteria regarding WSNs, (1) Information confidentiality: The safety criterion aims to keep delivered information hidden from unauthorized nodes, (2) data integrity, which guarantees the information supplied is retrieved without being tampered with by a suspicious node, (3) Authentication: The recipient may confirm the legitimacy of the message source's identification using this safety criterion, (4) information freshness, which refers to the fact that the information sent was sent recently and have not yet been repeated, (5) Availability, wherein network ought to be accessible although if cyber-attacks are present, (6) Non-repudiation refers to the concept that when a communication is transmitted, the transmitter never disputes that it was delivered. Cryptography is among the security strategies used to safeguard communications in public networks like WSN. Symmetric Key Cryptography (SKC) and Public Key Cryptography (PKC) are the two types of cryptographic methods that are often used. In terms of computing complexity and energy usage, SKC-based systems deliver good results. A key distribution, on the other hand, seems to be a more complex and sophisticated operation. PKC-based systems are often more versatile since they allow for simple key distribution and non-repudiation, although they are costly for sensor nodes with limited resources.

Some of the well-known security attacks are as follows [4] [5], in tampering, the sensors are designed to perform in a variety of weather conditions. As a result, it is extremely susceptible to serious attacks such as node capture. The intruder can seize the nodes and tamper with their cryptographic data, compromising the entire network. Blackhole: A node is deceiving the path finding process, and it may promote that a certain fictitious pathway is the most effective and quickest route for communications. As a result, it may draw all packets to one's own. Occasionally, it will drop all of the packets, making it impossible to retrieve them. DoS (denial-of-service) attacks: WSN is harmed by a DoS attack that reduces system throughput and blocks different services. Several key management techniques allow for the issuance of an individual node ID to each node. Node capturing attack: The nodes are assaulted directly and the information provided to them is taken. The intruder could get access to the node's data, including encryption keys, identification, and other confidential material.

In WSNs, key generation may be done via protocols that produce a secret key exchanged among two nodes using public-key cryptography. Networks have employed Public Key Cryptography (PKC) in conjunction with Symmetric Key Cryptography to achieve substantial security forces [6]. PKC-based key distribution systems give a network with durability, scale, and adaptability. The disadvantage is that they are costly, sluggish, and use a lot of energy. The prevailing tendency is to encrypt with Symmetric Keys and distribute keys via PKC. Owing to its resource constraints, WSN hasn't taken use of this benefit. While deploying numerous security services, PKC has failed to establish a firm footing in WSN. PKC activities are becoming a feasible alternative if used sparsely, following the successful execution of PKC in WSN utilizing ECC. One of the benefits of using PKC-based identity management is the ability to verify broadcasts. PKC is possible even on WSNs with limited resources due to ECC benefits [7] [8]. ECC is a perfect choice among different PKC choices in WSN because of its speedy execution, quick processing, and reduced key size signatures compared to certain other PKC methods including RSA. An ECC is a type of electronic communication certificate. For security similar to 1024-bit RSA, the protocol requires 160-bit keys. Other notable benefits of lower-key sizes include reduced memory use and quicker processing. The proposed work utilizes the ECC concept for key generation and providing security to WSN systems. With ECC, one can attain a similar degree of security with smaller keys. When compared to RSA, ECC delivers great protection with quicker, shorter keys in the future wherein mobile phones should carry out even further cryptography with less processing competence. This paper represents the identity-based key management for secure routing in WSN using an enhanced ECC algorithm which uses less number of keys for making a better secure link between nodes and to the SN.

1.1 Related Work

This section depicts the security approaches defined for the security in WSN along with their work contributions also their works pros and cons.

S. Sangeethapriya and R. Amutha [9] discussed that WSNs are a type of distributed system that is a part of the physical environment in which they operate. Sensor networks rely on the nodes existing inside the network, unlike most computers, which function largely with data acquired by humans. The energy spent for transmission must be as low as feasible to offer a dependable and efficient transmission utilizing a WSN. This is because the nodes are powered by batteries; thus the energy consumption must be low for the nodes' lifetime to be extended. Various transmission approaches for reducing energy usage in a WSN have been proposed.

SISO, MISO, and MEMO are the three most used approaches. One technique to reduce the amount of energy used by networking is to use cooperative communications. This uses a wide range of nodes (termed cooperative nodes) to convey relatively similar information to the receiver with the source node, reducing the overall energy needed for transmission as compared to traditional methods. The entire energy is made up of broadcast energy and cooperative transmitting (often known as long-haul communications). The number of collaborating nodes is critical in long-haul transmissions. The transmission energy can be reduced by determining the best E2E probability. The transmitting energy can be decreased by optimizing two parameters: (1) the number of cooperative nodes required for cooperative communication; and (2) the E2E probability value.

Due to H. Harb, A. Makhoul [10] explained that In wireless sensor networks, low battery capacity and high transmission energy consumption make in-network aggregation and forecast a difficult task for researchers. As contrasted to the reduced energy consumption of in-network operations, the utmost energy-intensive behavior is communication from sensors. The energy exchange among transportation and compute advantages applications while analyzing network information end instead of just transmitting sensor information. The study investigated a cluster-based strategy wherein information is routinely sent from sensor nodes to their respective CH. The proposed technique is separated into two phases: aggregation and adaptation, and it preserves energy savings in periodical sensing devices. To eliminate redundancy from original information and limit the number of information sets given to the CH, the aggregation stage is performed to find commonalities between information (metrics conducted for a period of duration p). Using the sets-similarity joins algorithms, the adaptation phase enables sensors to recognize replica data sets gathered between intervals. Experiments on real sensor data were undertaken to assess the performance of the suggested method. The proposed approach is beneficial in conditions of energy usage and data quality, according to the findings.

Y. D. Zhang and Shaohua Wan [11] discussed that by lowering the communication cost, data aggregation methods are commonly used to broaden the life span of sensor networks. Many applications were previously worried about tree-based prearranged techniques, which are an essential process for the sink to regularly gather information from each sensor. Because the data aggregation process normally takes several rounds, it's critical to collect this data effectively, lowering the energy cost of data transmission. When storing sensor routing tables in such systems, a tree is commonly used as the routing configuration to minimize computational overheads. We compared and examined an angular division routing method and query region division routing using LEACH to estimate the performance of the suggested method. In comparison to the models presented in the literature, theoretical and practical findings show that the inquiry province partition method based on an angle has a lesser energy outlay.

L. Xing Guo, W. Jun Feng [12] suggested that when using the LEACH approach to pick a cluster head, the remaining energy of nodes is ignored, and a node having low power might be chosen as a CH. As an outcome, the cluster generated through these low-energy nodes would die prematurely, squandering system resources. Throughout this study, researchers added an energy component to the process of selecting a CH, that can prohibit a node with really low power from becoming a CH. And in the meantime, they run simulations of the LEACH protocol to examine how it fared in addition to network durability, network connectivity, data gathering, and energy consumption. The results of simulations reveal that our enhanced method outperforms the LEACH approach in these areas.

Daniela and Giovanni [13] 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.

Most of the other approaches listed above provide flaws that prevent them from adequately meeting the requirements of WSNs in practice. To address the aforementioned issues, a better identity-based encryption scheme that operates on the theory of identity-based cryptography is suggested, that might significantly optimize the key generation process, minimize network traffic, and increase network safety.

The organization of the paper is as follows, section 2 explains the proposed work, section 3 depicts the results and discussion on the proposed work, finally, section 4 gives the conclusion of the presented work.

2. PROPOSED WORK

This section describes the proposed work and its 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.

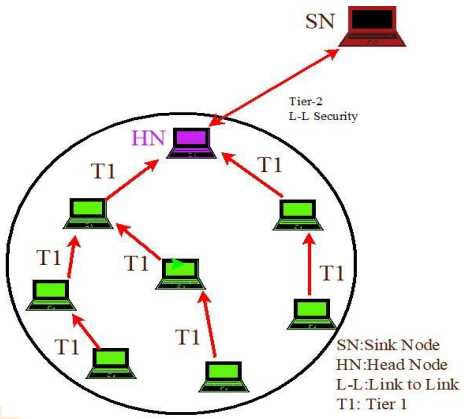

Figure 2: System Environment

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.

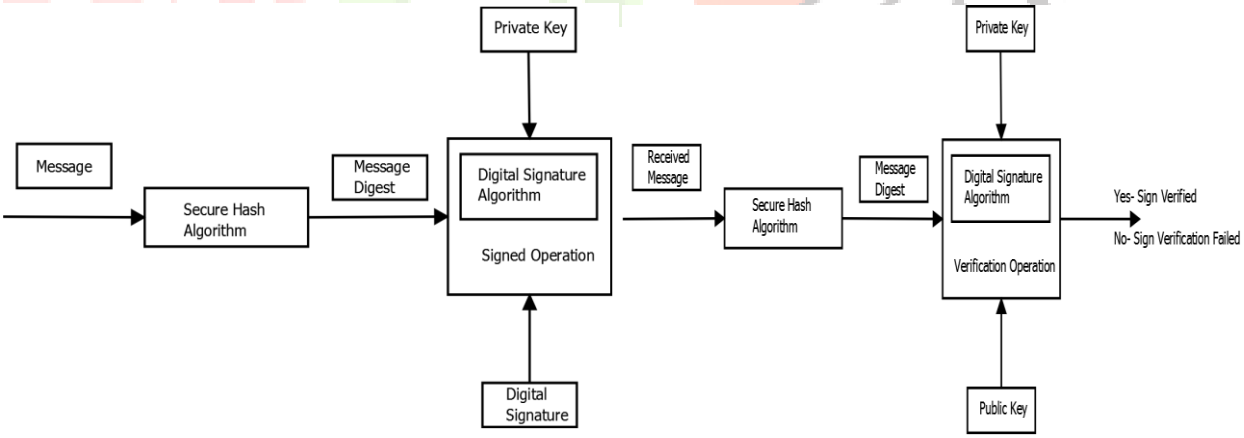

Figure 3: ECC signing mechanism

Figure 4: ECC verification mechanism

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∈Fp provided an integer x and a point P∈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.

Algorithm

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 below, one would obtain the public key.

$$B = d.A$$

‘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.

$$C1 = k * A$$
$$C2 = M + k * B$$

Decryption:

The transmitted message 'M' is expressed as the expression below.

$$M = C2 - d * C1$$

3. 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 computation analysis, key generation time, energy consumption, and packet delivery ratio.

Energy Consumption: Energy consumption is defined as the 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 work compared to the other two conventional protocols SPIN [14] and SLEACH [15]. The energy consumption is more as the data transception requires more energy and there is no proper key management scheme. The energy consumption graph is shown in figure 5.

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 method of calculating it is provided beneath.

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

The PDR of the proposed work is better when compared with SLEACH and SPIN protocol. The PDR ratio is increasing with the increase in the number of nodes. With the inclusion of two key generation proposals, the PDR is better for the proposed work and worst performance by the conventional SPIN protocol. The PDR has been described in figure 6.

Computation Analysis: Computation analysis is calculated by knowing the overall time required for the sender to sense the data and send the sensed data to HN and from HN to SN via encrypted links considering the key generation phase, encryption, and decryption. The computation analysis is calculated based on the timing factor in milli-seconds and due to the two-tier proposal, it is found that the time overall consumption is very less in the proposed work than compare both the conventional protocols. The SPIN protocol takes a very high computation time to compare to SLEACH and the proposed work. As the number of nodes varies the computation time changes yet the proposed work has a far higher difference when compared with both the protocols. The computation analysis has been described in figure 7.

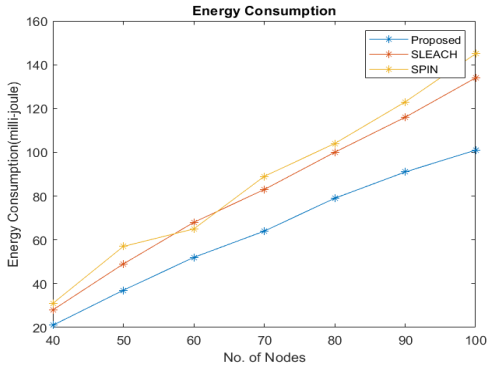

Figure 5: Energy Consumption

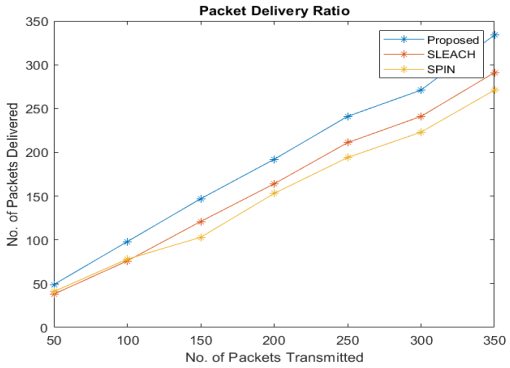

Figure 6: Packet Delivery Ratio

Key generation time: The key generation time by the proposed work requires very less as the proposed work has defined two types (2 tiers) of key generation techniques. The key generation time of the proposed work has been compared with the SLEACH protocol and it has been observed that the timing requirement for the SLEACH protocol is more as the number of nodes increases. The key generation time is as shown in figure 8.

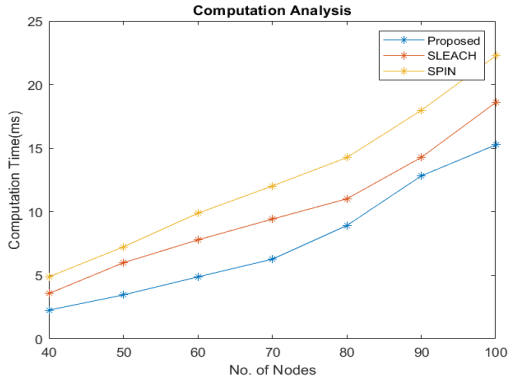

Figure 7: Computation Analysis

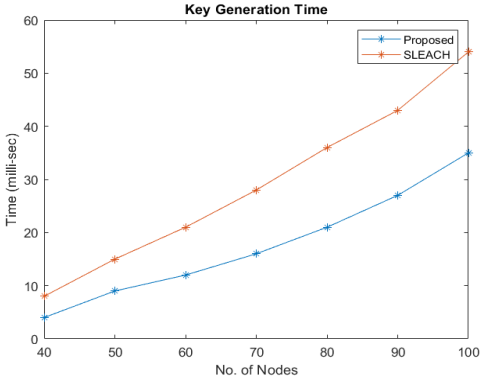

Figure 8: Key Generation Time

4. CONCLUSION

Wireless sensor networks are becoming increasingly used in a variety of applications. Several limits exist in the wireless sensor network, which includes data storage, computing systems, security, and restricted energy, to name a few. We have suggested a secure technique for wireless sensor networks in our scheme. We determine 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 enhanced ECC algorithm for reducing the complexity and minimizing the overall time. The result of the proposed work has been compared with conventional algorithms SLEACH and SPIN. It is found that the proposed work works far better than the other two protocols considering the parameters like energy efficiency, PDR, key generation time, and overall computation analysis.

REFERENCES

[1] Sohraby K, Minoli D, Znati, T, "Wireless sensor networks: technology, protocols, and applications". Wiley, pp 15–18, 2007. ISBN:978-0-471-74300-2

[2] Saleh Y, Yahya MS, Dalyop IA, Hussain R "Wireless sensor network (WSN) in insect monitoring: acoustic technique in insect monitoring a review/survey" *Int J Eng Technol* 7(3), pp.121–126, 2018, doi: 10.14419/ijet.v7i3.36.29091

[3] F. Mezrag, S. Bitam, and A. Mellouk, "Secure routing in cluster-based wireless sensor networks," *in GLOBECOM 2017 - 2017 IEEE Global Communications Conference*, Dec 2017, pp. 1–6, doi: 10.1109/GLOCOM.2017.8254138

[4] Khan, Shafiullah, Al-Sakib Khan Pathan, and Nabil Ali Alrajeh, eds. Wireless sensor networks: Current status and future trends. *CRC press*, 2016.

[5] M. Al-Rakhami and S. Almowuena, "Wireless Sensor Networks Security: State of the Art", ". *arXiv preprint*, 2018, doi: https://doi.org/10.48550/arXiv.1808.05272.

[6] Du, Wenliang; Wang, Ronghua; and Ning, Peng, "An efficient scheme for authenticating public keys in sensor networks" (2005). *Electrical Engineering and Computer Science*. 17. https://surface.syr.edu/eecs/17.

[7] Hankerson, Darrel, Alfred J. Menezes, and Scott Vanstone. Guide to elliptic curve cryptography. Springer Science & Business Media, 2006.

[8] K. Shim, "A Survey of Public-Key Cryptographic Primitives in Wireless Sensor Networks," in *IEEE Communications Surveys & Tutorials*, vol. 18, no. 1, pp. 577-601, First quarter 2016, doi: 10.1109/COMST.2015.2459691.

[9] S. Sangeethapriya and R. Amutha, "Reliable data transmission in wireless sensor networks," International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp. 1-6, doi: 10.1109/ICICES.2014.7034188.

[10] Harb, H., Makhoul, A., Tawil, R. and Jaber, A., "Energy-efficient data aggregation and transfer in periodic sensor networks", *IET Wirel. Sens. Syst.*, 4, pp. 149-158, 2014. https://doi.org/10.1049/iet-wss.2014.0068

[11]. S. Wan, Y. Zhang and J. Chen, "On the Construction of Data Aggregation Tree With Maximizing Lifetime in Large-Scale Wireless Sensor Networks," *in IEEE Sensors Journal*, vol. 16, no. 20, pp. 7433-7440, Oct.15, 2016, doi: 10.1109/JSEN.2016.2581491.

[12]. L. XingGuo, W. JunFeng and B. LinLin, "LEACH Protocol and Its Improved Algorithm in Wireless Sensor Network," *2016 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2016, pp. 418-422, doi: 10.1109/CyberC.2016.87.
[13] 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
[14] Bahae Abidi, Abdelillah Jilbab, Mohamed El Haziti, Chapter 1 - Routing protocols for wireless sensor networks: A survey, Editor(s): Amy Neustein, *In Advances in ubiquitous sensing applications for healthcare, Advances in Ubiquitous Computing*, Academic Press, 2020, Pp. 3-15, ISSN 25891014, ISBN 9780128168011, https://doi.org/10.1016/B978-0-12-816801-1.00001-3.
[15] Ouafaa, Ibrihich, Esghir Mustapha, and Krit Salah-Ddine. "Performance analysis of SLEACH, LEACH and DSDV protocols for wireless sensor networks (WSN)." Journal of Theoretical and Applied Information Technology, vol 94, no. 2, pp. 304, 2016, doi: 10.9790/2834-1402025156.

BIOGRAPHIES OF AUTHORS

	Vishal More DOB:22.10.1982. Completed B.E from SRTU Nanded in 2006, and M.tech from RVC Bangalore in 2009, currently working as a assistant professor in the department of CSE BKIT, Bhalki since from april 2009. Email:vishal.more1@gmail.com
	Dr. B. Suryakanth Chandrappa DOB:01.04.1965Experienced Professor with a demonstrated history of working in the higher education industry. Strong education professional with a Doctor of Philosophy - PhD focused in Microwave communication (Microstrip Antenna) . Working as Professor in ECE Department BKIT, Bhalki, affiliated to VTU, Belagavi. Email: bsuryakanth3413@gmail.com
	Dr. Sangamesh J.Kalyane DOB:30.05.1985. Completed BE from VTU Belagavi 2009, and M.tech from JNTU Hydrabad in 2011.Received the Decorate degree in Computer Science and Engineering from Visvesvaraya Technological University Belagavi, Karnataka 2020, from april 2012 to till date working as an Associate professor in the department of computer science and engineering at Bheemanna Khandre Institute of Technology Bhalki- Karnataka. Email: kalyanesangamesh@gmail.com