
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2020 SCPE. Volume 21, Issue 1, pp. 85–92, DOI 10.12694:/scpe.v21i1.1624

LONG AND STRONG SECURITY USING REPUTATION AND ECC FOR CLOUD ASSISTED WIRELESS SENSOR NETWORKS

ANTONY JOSEPH RAJAN D *AND NAGANATHAN E R †

Abstract. Wireless sensor network plays a significant role in the construction of smart cities, and the social network includes the Internet of Things, etc. In general, networks are most vulnerable of all the wireless devices due to the massive damage caused by disrupting these networks. Hence the nodes present in the network should get validated for its reputation. Therefore a Long and Strong Security mechanism with two-level checks is proposed here. Level 1 check includes verifying node reputation value and level 2 check includes Elliptical curve cryptography (ECC). Each sensor node sends the public master key to the cloud and secretly stored in the sensor node. Before data transmission, every node checks the master key, and if the master key is a match, then it transmits the data to the next hop. This process is continued until the source reaches the destination in the network.

Key words: Node Reputation, Grade Factor, Elliptical Curve Cryptography, Wireless Sensor Network.

AMS subject classifications. 94C12

1. Introduction. Many ways are available for implementing security measures, and among them, the most commonly used technique is cryptography. The cryptographic methods usually have three operations to be carried out for providing security. The activities include conversion of simple passage to cipher (secret code) text, identifying the value of secret key used and processing the algorithm of an understandable or straightforward transcript [17].

From the key variations, bi-cryptosystem are generated, namely symmetric key cryptosystem (private) and asymmetric key cryptosystem (public). If a similar key is used for both decrypting and encrypting the text or communication, then it is said to symmetric key cryptosystem. If a pair of keys such as private and public key utilized for decrypting and encrypting process, then this process is said to be asymmetric key cryptosystem. There were several scheme and algorithms projected to public-key cryptography as its initiation. Some example techniques for public-key cryptography are Diffie Hellman, Secured hash algorithm, RSA, ECC, etc. Prime numbers are used to generate keys for securely transferring data [2]. The public key is utilized for encrypting simple transcript or to confirm a digital mark, and the private key is utilized for decrypting secret code transcript or to generate a digital mark. Prime based ECC key generation is implemented for providing security measures and Further sections of this paper are organized in the following way. Section 2 gives a detailed description of existing security algorithms. CC based Secure Data Encryption scheme analysis is explained in detail. In section 4 the results are analyzed based on the presentation projected and conventional systems. In the final section, the conclusion of the work is included with the applications.

2. Related Works. Most of the works have been carried out for providing security in the field of wireless communication using symmetric and asymmetric key cryptosystems. The security issues are reduced in maximum by using the existing security mechanisms. Some of the secured mechanisms are discussed here in detail as follows;

The packets are forwarded to the node which is located away from and attack other nodes that are present in the network. This attacker node itself present in the network to attack the other nodes by assuming itself as a node that is present in the shortest path. To protect the network from malicious nodes i.e. node replication attack the secured transmission and communication approach [3] was proposed.

*Research Scholar, SCSVMV University, Enathur, Kanchipuram, India, Email: antonyjosephjmj@gmail.com
†Professor, Symbiosis Institute of Computer Studies and Research, Symbiosis International (Deemed University), Pune, India. Email: ernindia@gmail.com

Localized Encryption and Authentication Protocol [5] is a Key organization protocol in which four various keys are generated such as personal key, pair-wise key, cluster key and set, each key was created for a different type of purposes. The keys are established and updated in a timely manner among each other so that the involvement of base station reduced, in turn, energy consumption got reduced.

Elliptic Curve based asymmetric cryptosystem was implemented [4] by Muhammad Hammad Ahmed et al., in which ECC is used for its smaller key size. This greatly reduces the computational cost. The elliptic curve field was defined over the prime number, so that complexity in mathematical computations gets diminished. The maximum key length used for ECC is 384 for providing security. The double-and-add algorithm is used for point multiplication, and computation delays were compensated using 32 block size. A secure node authentication scheme [6] was implemented for protecting the data from unsecured routing. The sensor nodes collect data and shares over the communication link that shared data should be accessed only when the nodes are authenticated. The BS programs the signatures with a certificate authority, and once the nodes are verified that they are legitimate nodes, then the nodes can pass the information. Symmetric calculations offer secrecy, whereas satisfying the supremacy and memory requirements of sensor networks [7]. Here each sensor nodes uses a single key for encrypting and decrypting process and hence, it is challenging to provide authenticity, and there are no appropriate key switch mechanisms. The utilization of a single key in every hub of a system is a security hazard as one traded off hub can take a chance with the security of the entire system.

Prime Field Arithmetic for ECC [8] was proposed for high-level security mechanism using Optimal Prime Fields (OPF). The OPF is the general form of prime designed in the form of p= u.2K+v. Primes with low hamming weight are considered for reducing the execution time in consideration of hybrid technique Montgomery multiplication. Combinatorial Design of key distribution mechanisms [9] was proposed to fix the key size and which keys to be used for secured nodes and to create secured wireless links among them. This combinatorial approach uses two factors such as Balanced Deficient Block Devise (BDBD) and Global Quadrangles (GQ) are mapped for obtaining efficient keys for distribution among the network. However, the length of the key path gets varied according to the size of the network. Trajectory privacy-preserving framework was proposed [10] to analyze the threat models with various background information as well as to calculate the efficiency of the trajectory privacy. By considering the time factor, the theoretical mix-zone model is applied to preserving data by defining a data-sensitive area. Public key cryptography mechanism is used in the Secured Data Discovery and Dissemination based Hash (SDDDH) scheme [11]. Here one-way hash cryptographic function was applied for data security process. The base station generates a signature packet in each round of data distribution, and every sensor nodes receive a signature packet for node verification. Trickle algorithm is applied for packet verification, and puzzle keys are added for encryption of messages. However, this Merkley hash tree algorithm consumes more energy for packet encryption and verification. Secure communication for Industrial Internet of Things [12, 13] was proposed by applying a user validation protocol along with seclusion fortification for Industrial IoT was proposed. Security of the proposed scheme is proved under a random oracle model is used to prove the security of the IoT system and other security measures of the protocol. The mechanism [14] provides cryptanalysis of system based on ECC, the cryptanalysis consequence guides to intend a resolution to overcome the issues. It provides a robust hash based conditional P2 authentication and probabilistic key swap protocol that results lightweight and computes low overheads during the entities involved. Anonymous ECC-based self-certified two-factor key management scheme [15] was proposed that offers the required security features. This mechanism has the ability to produce a secure channel during the communication of secure sensors (cluster members) and access point (cluster head) [16].

3. Proposed Method – Long and Strong Security (L&SS) using two-level checks. The node undergoes two levels of security check during the transmission of information to the other node. Level 1 Node Reputation Check (L1-NRC) check includes the elimination of malicious node from the communication process by assigning a duplicate address for the routing nodes in the system. Level 2 Elliptic Curve Cryptography (L2-ECC) check adds the illegitimacy of the node for completely eliminating the node from the communication process.

3.1. Level 1-NRC. The nodes present in the network are categorized into malevolent and customary class. Malevolent nodes are selfish behaviour nodes, and customary nodes perform routine operations. These nodes are classified on behalf of reputation values of each node that is determined based on the grade calculation.

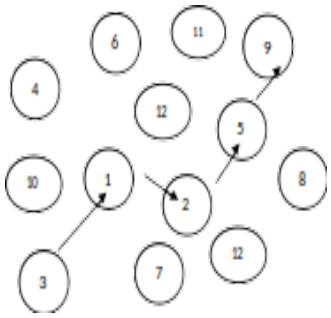

FIG. 3.1. *Dummy CGA Creation for nodes*

The grade factor (Gf) calculation of nodes includes their energy level and the energy threshold level. GH nodes fall under Normal Set Nodes (NSN), and GL nodes fall under Malevolent Set Nodes (MSN). The grade factor calculation is done based on the total number of processed control messages as per required data transmissions.

$$Gf_n = \frac{\text{No. of RREQ processed}_{(n)}}{\text{No. of RREP processed}_{(n)}} \tag{3.1}$$

$$(GL < 35 < GH)$$

The nodes are fallen under the category of secured nodes present in the routing path provided with a private key and certificate. To establish trust between the normal set of nodes and malignant nodes, a signed certificate is provided by a certificate authority. Using a Hash function, fake Cryptographically Generated Addresses (CGA) is created for each node. Here, CGA uses a hash extension method, which has security parameter 'sec' that linearly scales the number of bits used in the hash extension by imposing 16xsec many bits to zero in the hash value denoted by a hashing algorithm.

Dummy address is created for each node present in the route starts from source to destination. The dummy address is created for all the nodes such as source node, relay node and the destined node. This dummy address significantly reduces the passive attacks and also provides more security to the system. Besides, the dummy address generation ensures that the malicious observer cannot identify the original identity of the nodes.

Dummy CGA Generation: Address generation for legitimate nodes are not expected to exceed 2S. Besides T the time required to generate address is considered. Therefore the cost of address generation is G_T. The time value T is set constant for

$$G_T = 2^x + T \tag{3.2}$$

The source hub 3 generates dummy address by using G_T formulae (23+1), and the temporary node address of 3 is 9. The same procedure is done for all the intermediate nodes present in the route until it reaches to destination. Then the private key is assigned for all the intermediate nodes. If the key matches then the nodes processed for L2 ECC check. This process makes the node reputation value stronger.

Algorithm for L1-NRC:
Begin Procedure
Set Src & Dest node
While Src not in range of Dest do
Compute Gf(n)
Select NSN nodes
Assign CGA for all nodes
Checks for M_N in the routes
If M_N present in route nodes do

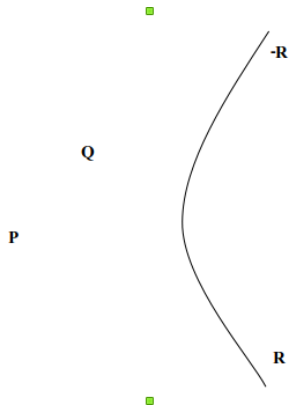

FIG. 3.2. *Nodes Representation with Elliptic Curve*

Create dummy CGA for all nodes
Assign private key for all the routing nodes
If key matches process L2 check
Else label the node as M_N
End Procedure

3.2. Level 2- ECC. Elliptical curve cryptography is a well-known process for providing security in wireless networks. Each sensor node sends the public master key to the cloud and secretly stored in the sensor node once the NRC is done. Before data transmission, every node checks the master key, and if the master key is a match, then it transmits the data to the next hop. This process is continued until the set of transmission between source and destination is done in the network.

The corroboration action of this level-2 check is to bring out that the directing node is malevolent to all other nodes present in the routing so that the node can be excluded from the communication process. It comes beneath level 2 (L2) action of the proposed mechanism. To incorporate this, there is a need to confirm that a node is illegitimate before broadcasting its label 'malicious' to all nodes. Therefore, the node that fails the NRC test is further examined using the elliptical curve cryptography technique using the Weierstrass Elliptic function. Consider the coordinate points of the initiator node or source and the Next node Ni are P and Q, respectively; there is another point R that creates a straight line as demonstrated in figure 3.2.

The Weierstrass Elliptic Curve function is defined in 3.3,

$$x^2 = y^3 + by + c \tag{3.3}$$

$$P + Q = R \quad where \quad P \neq Q \quad \forall P, Q \in E \tag{3.4}$$

where (x_P, y_P) and (x_Q, y_Q), (x_R, y_R) are the coordinates of points P, Q and R that forms an elliptic curve. Consequently, the coordinates can be attained through the subsequent expressions,

$$x_R = \alpha^2 - x_P - x_Q \tag{3.5}$$

$$y_R = \alpha(x_P - x_R) - y_P \tag{3.6}$$

with $(y_Q - y_P)/(x_Q - x_P)$.

The commutative property of this function states that,

$$P + Q = Q + P \tag{3.7}$$

TABLE 4.1
Simulation Parameters

Parameter	Value
Simulation Area	1000m x 1000m
Number of Nodes	100
Channel	WirelessPhy
MAC	802.15.4
Radio Propogation Type	Two Ray-Ground Type
Antenna Type	Omni Directional
Traffic Models	CBR
CBR Interval	1.0 ms
Simulation Time	50 sec
Node Communication Range	100m

The algorithm shows that the node estimates the reputation value and sends it for L2 verification. Meanwhile, the forward secret FS_KEY is calculated using equation 3.8 at the source end. The next node replies to the $L3_REQ$ with R_KEY using the equation 3.9.

$$FS_KEY = P + Q \tag{3.8}$$

$$BS_KEY = Q + P \tag{3.9}$$

The source node S compares its FSKEY with the BSKEY to conclude that the directing node Ni to the destination is a malignant node (MN). Therefore the computed FSKEY is not equivalent as BSKEY then the node is published as malicious to all other nodes and the next nearest node is considered for communication. The algorithm 2 is a part of the main algorithm 1 and is described below.

Algorithm 2
1: **Level-2_ECC_Check()**
2: S sends $L2_REQ$ to check directing nodes Ni
3: S calculates FS_KEY <- P+Q;
4: D replies with BS_KEY <- Q+P;
5: **If** (BS_KEY !=FS_KEY)
6: Remove M_N from the neighbour list
7: Label N as M_N & Broadcast to all nodes
8: Return 1
9: **Else**
10: Set node as Normal node
11: Return 0
12: **end if**
13: end

4. Results and Discussions. The proposed work of L&SS is examined with the Network Simulator (NS2). The imitation of the L&SS method has 100 nodes arrange in the simulation area 1000 × 1000 as revealed in Table 4.1. Every node accepts the signal from all direction through using the Omnidirectional antenna. By using a Constant Bit Rate (CBR) traffic model, the traffic is handled. The parameters used for analyzing the performance of the proposed and existing schemes are packet loss rate, packet received rate, average delay, leftover energy, and throughput.

5. Parameter Analysis. WSN implementation of many security schemes affects the QoS of the system. The metrics considered for the system evaluation are delivery rates, throughput, delay and detection rate. There is a tradeoff between QoS and security in this scheme.

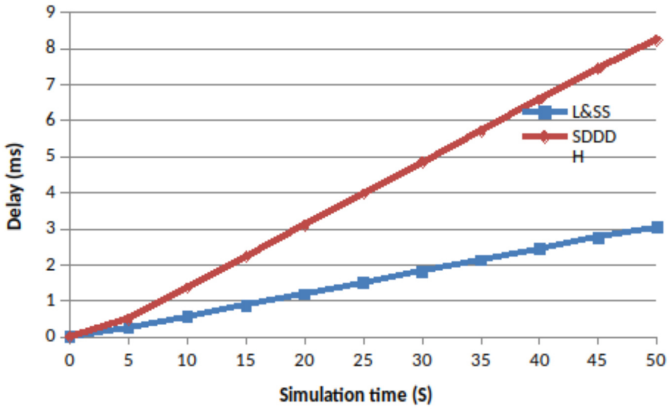

FIG. 5.1. *Packet Received Rate*

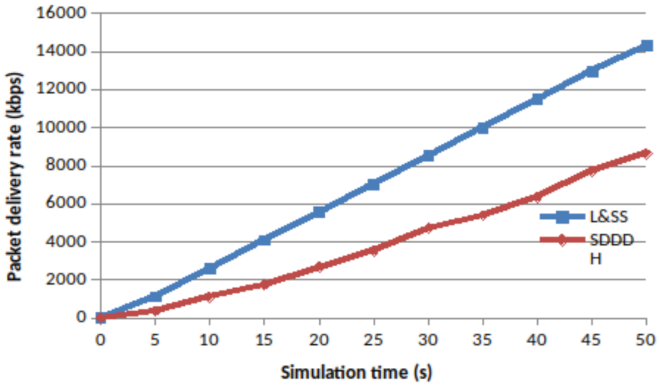

FIG. 5.2. *Average Delay*

5.1. Delivery Rate. The delivery rate of data from the source point to the destination point is identified to determine the total amount of packets received effectively by the destination point. DR is estimated by using equation 5.1

$$PDR = \frac{Total\ number\ of\ packets\ received\ successfully}{Total\ number\ of\ packets\ sent} \tag{5.1}$$

Figure 5.1 illustrates the delivery rate of packets for the proposed L&SS and the conventional method such as SDDDH. The L&SS method achieves greater PDR compared to other existing mechanisms since the node ID verification process prevents the intermediate nodes from malicious attacks.

Delay

Average delay is estimated by analyzing the time difference of sent packets and received packets. The delay estimation includes nodal processing and queuing time evaluation during transmission and reception of data, and the calculation is given in next equation:

$$\text{Delay} = \frac{\text{Packets received time-Packets sent time}}{\text{Total time}} \tag{5.2}$$

Delays of proposed (PDly.tr) and existing (Dly.tr) schemes are measured and plotted in figure 5.2. It can be observed that the delay of the proposed method is bare minimum since the route is filtered and the intermediate nodes are verified. The decrease in delay reflects the efficiency of network routing.

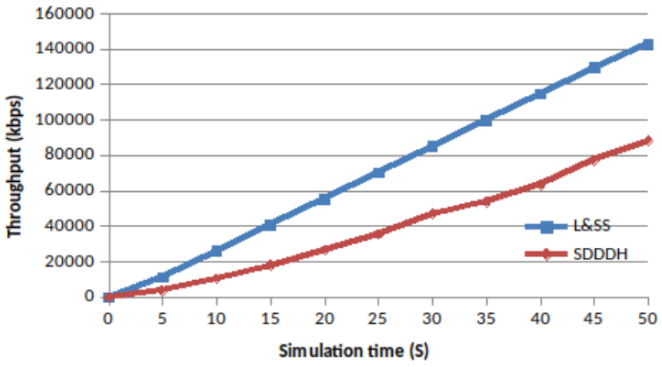

FIG. 5.3. *Throughput*

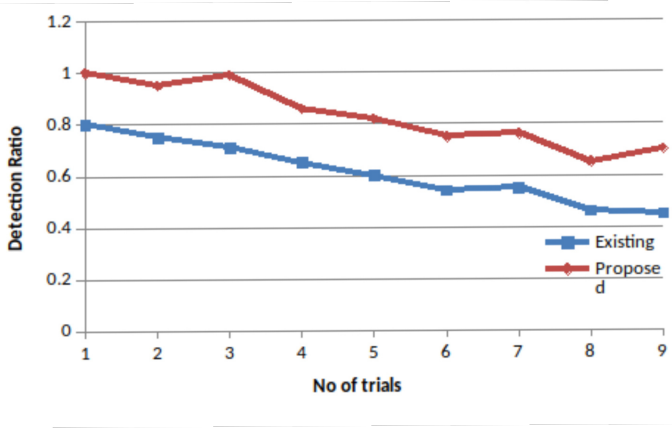

FIG. 5.4. *Detection Rate*

Throughput

Throughput is commonly evaluated for analyzing the overall network performance, and it is defined as the rate of successful delivery of packets to the destination over a preferred set of connections. Throughput calculation is given in the equation

$$\text{ThroughPut= Total Pkts Received} \times \text{Pkts Size} \times 100 \tag{5.3}$$

The simulation analysis proves that L&SS method has higher throughput compared to the SDDDH mechanism.

Detection

The detection rate for both proposed and existing routing protocols are examined. Figure 6 shows that the detection rate for both conventional and proposed schemes.

$$\text{Detection Rate} = \frac{D_{mn}}{T_{mn}} \tag{5.4}$$

where $D_{mn}$is the number of malicious nodes detected by one or more normal nodes, T_{mn} is the total number of malicious nodes.

6. Conclusion. Long and Strong Security mechanism with two-level checks is proposed here. Grade factor keys are generated for determining node reputation values as well as for node verification process. Besides, dummy address creation actions are performed to improve security measures. The proposed L&SS

simultaneously reduces energy consumption among nodes, and the routes are undetectable by malicious nodes since it uses dummy CGA for the transmission process. The data transmitted over the route are strongly encrypted with the help of public-key cryptosystems. Level 1 check includes verifying node reputation value and level 2 check includes Elliptical curve cryptography (ECC). Each sensor node sends a public master key to the cloud and secretly stored in the sensor node. Before data transmission, every node checks the master key, and if the master key is a match, then it transmits the data to the next hop. However, the computational cost makes the system quite complicated but offers strong security, and the number of packets outcome at the receiver is quite high. The performance of the network is analyzed and the proposed system has 35.7% greater efficiency compared to the conventional in terms of data delivery rate.

REFERENCES

[1] Stallings W. Cryptography and Network Security: Principles and Practice (5th edn). Pearson Education, 2013. DOI: 10.5772/2651.

[2] Ribenboim P. The New Book of Prime Number Records, Springer-Verlag, 1995; 22–25. DOI: 10.1007/978-1-4612-0759-7.

[3] Shimpi B, Shrivastava S. A modified algorithm and protocol for Replication attack and prevention for wireless sensor networks. In ICT in Business Industry & Government (ICTBIG), International Conference on IEEE, 2016; 1-5.

[4] Ahmed MH, Alam SW, Qureshi N, Baig I. Security for WSN based on elliptic curve cryptography. In Computer Networks and Information, 2011; 75-79. DOI: 10.1109/ICCNIT.2011.6020911.

[5] Zhu S, Setia S, Jajodia S. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Transactions on Sensor Networks (TOSN), 2006; 2(4): 500-528. DOI: 10.1145/1218556.1218559.

[6] Eschenauer L, Gligor VD. A Key-Management Scheme for Distributed Sensor Networks, Proc. Ninth ACM Conf. Computer and Comm. Security, 2002; 41-47. DOI: 10.1145/586110.586117.

[7] Rivest RL, Shamir A, Adleman LA. Method for obtaining digital signatures and public-key cryptosystems. Communication ACM, 1978; 21(2): 120–126. DOI: 10.1145/359340.359342.

[8] Rasheed A, Mahapatra RN. The three-tier security scheme in wireless sensor networks with mobile sinks. IEEE Transactions on Parallel and Distributed Systems, 2010; 958-965. DOI: 10.1109/TPDS.2010.185.

[9] Zhang Y, Grosssch'adl J., Efficient prime-field arithmetic for Elliptic Curve Cryptography on wireless sensor nodes. In Computer science and network technology (ICCSNT), 2011 international conference on IEEE, 2011; 1459-466. DOI: 10.1109/ICCSNT.2011.6181997.

[10] Çamtepe SA, Yener B., Combinatorial design of key distribution mechanisms for wireless sensor networks. IEEE/ACM Transactions on networking, 2007; 346-358. DOI: 10.1007/978-3-540-30108-0-18.

[11] He D, Chan S, Tang S, Guizani M., Secure data discovery and dissemination based on hash tree for wireless sensor networks. IEEE Transactions on wireless communications, 2013; 4638-4646 DOI: 10.1109/ TWC.2013.090413.130072.

[12] Li J, Li Y, Ren J, Wu J., Hop-by-Hop Message Authentication and Source Privacy in Wireless Sensor Networks. IEEE transactions on parallel and distributed systems, 2013; 1223-1232. DOI: 10.1109/TPDS.2013.119.

[13] Li Xiong, Jianwei Niu, Md Zakirul Alam Bhuiyan, Fan Wu, Marimuthu Karuppiah and Saru Kumari, "A robust ECC-based provable secure authentication protocol with privacy preserving for industrial Internet of Things." IEEE Transactions on Industrial Informatics 14, no. 8 (2017): 3599-3609 DOI:10.1109/TII.2017.2773666.

[14] Paliwal, Swapnil. "Hash-Based Conditional Privacy Preserving Authentication and Key Exchange Protocol Suitable for Industrial Internet of Things." IEEE Access 7 (2019): 136073-136093. DOI: 10.1109/ACCESS.2019.2941701

[15] Abbasinezhad-Mood, Dariush, and Morteza Nikooghadam. "Efficient design of a novel ECC-based public key scheme for medical data protection by utilization of NanoPi fire." IEEE Transactions on Reliability 67, no. 3 (2018): 1328-1339. DOI: 10.1109/TR.2018.2850966

[16] Jayarajan, P., Kanagachidambaresan, G. R., Sundararajan, T. V. P., Sakthipandi, K., Maheswar, R., Karthikeyan, A., "An energy-aware buffer management (EABM) routing protocol for WSN". The Journal of Supercomputing. (2018). doi:10.1007/s11227-018-2582-4

[17] E. Kayalvizhi, A. Karthikeyan, J. Arunarasi, "An Optimal Energy Management System for Electric Vehicles using Firefly Optimization Algorithm based Dynamic EDF Scheduling", International Journal of Engineering and Technology, vol. 7, no. 4, Aug-Sep 2015.

Edited by: Swaminathan JN
Received: Oct 29, 2019
Accepted: Jan 28, 2020