Intelligent Automation & Soft Computing
DOI: 10.32604/iasc.2022.026483
Article

Tech Science Press

Security Protocol Function Using Quantum Elliptic Curve Cryptography Algorithm

K. Sudharson[1,*] and S. Arun[2]

[1]Department of Information and Communication Engineering, Anna University, Chennai, 600025, India.
[2]Department of ECE, Prathyusha Engineering College, Thiruvallur, 602025, India.
*Corresponding Author: K. Sudharson. Email: susankumar@gmail.com
Received: 28 December 2021; Accepted: 10 February 2022

Abstract: Quantum Computing (QC). The content of node or sink nodes is processed using the fundamental principles of quantum mechanics. However, cryptography techniques face several other issues, such as availability, integrity, and vulnerability, to name a few. The researchers have overcome many obstacles, yet security remains a crucial concern in QC. However, experimenters recently discovered that the QC has a lot more data hacking than static networks. Moreover, the bitwise error is still present in implementing the Quantum Computing Cryptography Protocol (QCCP). Because all nodes are mobile and dynamic topology occurs, the proposed research uses the Quantum Elliptical Curve Cryptography (QECC) protocol. To provide the appropriate key generation and key sharing mechanism to convert the fool node to a brawny node and avoid packet loss and energy consumption in the network. By turning the fool node into a vital node, the QECC lowers the network's error rate. The experiment uses Network Simulator 2 to achieve successful outcomes such as decreased packet loss, reduced error rate with increased energy consumption, increased pair key generation for additional nodes, and increased packet size.

Keywords: Quantum computing; elliptic curves; mobile ad hoc networks; cryptography; wireless sensor networks

1 Introduction

The secure delivery of content is a crucial task and emerging trend in Mobile Adhoc Network (MANET) that works parallel towards the design. In MANET, nodes are auto-configuring and do not need any infrastructure used to share the information in the network. For example, the node might be a sensor node used to sense the structure of the environment, and the physical behavior of the area needs to share from time to time with other nodes frequently [1]. Nowadays, mobile networks use automatic network provisions, easy to deploy, and are less expensive. The nodes are linked base station to base station or any centralized unit system [2]. However, the node's capabilities are restricted resources like bandwidth, storage volume, transmission speed, and battery existence are all factors to consider—the numerous issues owing to the construction of nodes that baits several kinds of attacks [3].

Furthermore, MANET is vulnerable to a range of privacy concerns due to its numerous updates and constraints. Providing an improved strategy for security challenges requires building the best protocol and algorithm in cryptography to protect MANET transmission [4]. Unfortunately, it is extremely tough to create or find a better replacement of protocol and algorithm in MANET. A broadcasting message to another node without trust, energy utilization, and memory management lead to high risks like vulnerable activities and coercions and disparate security attacks like malicious, blackhole attacks, and wormhole threats [5]. Also, in MANET, cryptography is a growing field that focuses on the application-oriented like in military operation legitimate user sharing the information that is kept private, which was hijacked by the hacker owing to a malicious node [6]. By using the key based on pairs, the real message is encoded to transmit the content in the network. The receiver node needs to identify the correct key to decipher the message; otherwise, the node will stamp as a malicious node [7].

Cryptography has applications like Broadcasting, telecommunication technologies, and digital payments such as the online platform, email, and cellular telephones [8]. Several conventional cryptographic techniques are linked to particular mathematical operations and utilize various mathematical strategies to prevent snoopers from finding the essence of protected transmissions. Therefore, owing to the tremendous capability of quantum processing, this security feature may be insecure [9]. Furthermore, the conservative cryptographic algorithm cannot guarantee fundamental security [10]. In the MANET, the communication of the nodes can be forged together or separated on the operation management. Creating a routing infrastructure is quite challenging to imply the authenticated transmissions of data in dynamic network topology, owing to infrastructure-less communication. Meanwhile, secure key management also plays an integral part in the MANET to provide the best result for the network protection in various services like trust model, cryptosystem, production, storage, and distribution of keys.

They were using Network security to preserve raw data in telecommunication. It comprises policy and practices for preventing and tracking illegal access, misuse, modification, or denial of web access. An admin is in charge of the node, and they are entitled to share or obtain data across the network. The user requires a user account or authorization to communicate over a network. Cryptography aims to safeguard the content and the network resource by assigning a unique secret key to the proper understanding.

2 Related Works

Safari et al. [11] suggested a free-space Quantum Key Distribution (QKD) method with a grounded relay-assisted approach in light of the BB84 framework standard. They examined the functioning of passive relays to send quantum bits (qubits) to another relay node devoid of completing any evaluation or detection action. They used a near-field study to put an upper limit on the qubits of the relay-assisted QKD Bit Error Rate (QBER). Furthermore, trial analysis indicates that perhaps the relay-assisted approach outperformed direct transmission at longer connection ranges where disturbance effects are most damaging.

Gao et al. [9] have examined the trustworthiness of a 2–3 party Quantum Key Distribution Protocol (QKDP). These protocols standards tended to be more susceptible to sparse-coding attacks. For example, Eve gained the session key by sending Alice scrambled qubits as a fake signal and then paired evaluation after Alice's encoding. The attack procedure was eerily comparable to Eve and Alice's closely packed conversation. Furthermore, this assault did not suffer any flaws in the data transmission; both Alice and Bob were unaware of it. Finally, their analysis addressed the origin of the ambiguity and a feasible strategy to construct these standards.

Gao [12] has discussed the cryptographic framework of a 4-party quantum key distribution mechanism that uses cumulative snooping. In the 4-party Quantum Secret Sharing (QSS) method, only one superior,

Alice, intends to do bell condition measure. At the same time, another agent must perform a single qubit operation without introducing any error on Alice's hidden content.

Hwang et al. [13] have suggested integrating the implicit with the explicit quantum key distribution protocol. Establishing a dedicated secure network may evade man-in-the-middle exploits, snooping threats, and replay attacks. Their technique has cut down the number of communication cycles. In addition, the parties involved have been regularly using and exchanging a long-term secret key. The use of a combination of traditional and quantum cryptography can identify the actuality of malicious activities like eavesdropping.

Abushgra et al. [14] suggest a Quantum authenticated key distribution mechanism to carry out key allotment. It was also supposed to ensure that the communication groups ha both intuitively and formally. The participants rely on a third party for the authentication part of their protocol. As a result, the proposed approach is suitable in network systems that manage sensitive data, such as those used by the army, healthcare providers, and research institutes. They used polarised photons in juxtaposition levels for genuineness and secure key distribution, which provide a high level of protection against various threats.

Lu et al. [15] A (t, n) threshold quantum cryptosystem (or (t, n)-QSS) suggest exchanging combined conventional content and quantum states relying on monolithic phase shift function on mono qubit in conjunction with Shamir's (t, n) secure communication. Ensuring authenticity, It has secret restructuring. The framework uses fake photons and the confidential value in Shamir's approach as the hidden value to minimize eavesdropping. As a result, it is robust to intercept-and-resend threats, entangle-and-measure threats, and contestant threats such as entangled swapping attacks, according to tests.

Yeh et al. [16] suggest an elliptic curve cryptography device authentication that helps resolve several privacy challenges in ad hoc networks. Internal cyber attacks, forging attacks, masquerading attacks, replay attacks, and prediction attacks are all protected by the suggested method, including a standard form of authenticating, a guarded secret key change, and renewal. The recommended approach enhances verification while providing excellent privacy in mobile ad hoc networks.

Wang et al. [17] tried to match genetic algorithms to Quantum Genetic Algorithms (QGA), which ran 25 times and repeated many times for 500 iterations. QGA's universal difficulty seems to be on the O(N) measure, in which N denotes the overall population. On the other hand, the hardness of a GA has been on the scale of O(N2). As a result, the complexities reduce to a linear state.

Chen et al. [18] To detect the security challenge of vehicle identity verification, offer a quantum Vehicular Ad-hoc Networks (VANETs) defensive mechanism. It works on quantum mechanics and the BB84 quantum secure-key exchange technique. Additionally, the unique quantum system can defend against most VANET-targeted attacks. Furthermore, Using interconnect vehicles to all since the suggested quantum approach solves the dependability and security concerns. Furthermore, their suggested system provides unique benefits such as distant identity verification, identity revocation, and irreversibility by cleverly leveraging quantum physics features.

Miri et al. [19] abridged the Symmetric Key Cryptography (SKC) method for the safety requirement based on IEEE 802.15.4 standard. Then, they introduced a few different vulnerabilities and failures present. Indeed, Public Key Cryptography (PKC) provides superior-key access control and cyber safety results SKC. They demonstrated that the Certificate-Less Public Key Cryptography (CL-PKC) approach is an appropriate Asymmetric Key Management methodology for ad hoc Impulse Radio Ultra-Wideband (IR-UWB) systems.

Gautam et al. [20] examine how the characteristics of various trust management, verification, and secret-key management systems can be made available to the specific application in this article. In addition, they explain the techniques, benefits, and limits of a proposed initially key management, verification, and

reputation strategy in Wireless Sensor Network (WSN), relying on this study. The purpose of this in-depth investigation is to assess and discover the best protection system that solves the user's needs.

Qazi et al. [21] this study focused on security challenges in WSNs. As a result, adding security and data encryption in a novel approach for node-to-node transmission was necessary. Also, with the assistance of the Elliptic Curve Digital Signature (ECDSA) cryptographic algorithm, the suggested algorithm not only ensures protection for the multi-hop routing network but also multitudes storage space on endpoints by providing a suitable method for assessing "key" generation period, a total of hello packets, and packet size.

3 Problem Statements

MANET comprised of nodes is scattered in a particular area to monitor the physical phenomenon. The node's channel capacity is restricted, and battery power with a limited resource can transmit the sensed or received data. The mobile node operates with the tiny Operating System (OS) used to schedule all the aspects present in the network [22]. In recent years the MANET has emerged from current events in the network world. The majority of the study focuses on resolving network problems with node security. The MANET is very complicated to design the protocol compared to the wireless sensor network, and the routing protocol is creating a novel form of energy-saving for mobile security.

The main problem in MANET is finding the acceptable route from source to sink node. The many things in MANET are to identify the routing protocol to discover the secure pathway in the set of connections. Finding a trusted path among the group of nodes in the network is challenging due to the mix of good nodes and fool nodes. The nodes are working independently with limited battery power, which operates the "key" sharing mechanism and finds the malicious attack in the network. Quantum Key Sharing (QKS) is a field of quantum cryptography that is very significant. This system combines quantum physics and classical encryption. In this research work, we utilize efficient cryptographic techniques to provide a solution to various attacks and identify the fool nodes from the network to find the trusted path. Also, multiple parameters like error rate, energy consumption, and key generation rate are greatly improved [23].

4 Quantum Elliptic Curve Cryptography (QECC)

The suggested algorithm divides each node into two categories. The complete network nodes are brawny, whereas fool nodes are the weakest. During data transmission, this split of nodes creates a conformist storage operation. A further study describes QECC's incorporation and integration with Algorithm for Wireless Secure Communication (ASWC).

4.1 QECC Implementation in MANET

AWSC used the asymmetric technique to generate keys in the system's robust and reliable architecture to avoid cyber attacks during end node-to-end node connection. In 3 distinct instances, the two categories of nodes interact. Furthermore, the stages of QECC are separated because then paired keys are produced in the system for transmission initially and instead exchanged across endpoints over an information exchange connection.

MANET contains scattered gadgets that are self-contained throughout the system. These network elements use sensor nodes to analyze "key" physical and environmental parameters. The devices are routers or terminal nodes that work along with the entry point to form a conventional MANET. Amongst the most challenging aspects of deploying an overlay network is maintaining topology organization and interconnection throughout communication networks. In a MANET, the channel's connectivity influencing by various elements' topology [24].

The network communication topology is an essential and relevant component to examine since it can impact various factors in the connection, including data latency, energy efficiency, network temporal, network scalability, time synchronization, communicative stability, and so forth. The mesh network model was employed for the nodes to disseminate the content with each other's help. Routes tables, which instruct each node about interacting with the open network, are typically used in meshes systems. Mesh topology has many advantages, including moving massive volumes of information across the infrastructure using much less energy and being called an energy-efficient technique. QECC creates various paired keys for every network node, with each key generated dynamically through the cryptographic approach [25].

Furthermore, the created keys are asymmetric, meaning that any arbitrary node can make them and exchange them with all the other nodes. Each node has a private and public key and a unique identification value, thanks to the non-symmetric key. In addition, every node includes an identity table containing node ID and bitmask and the calculated hash to validate by using authentication tokens.

Tab. 1 shows the following is an example of an authentication table: In the QECC model, the authenticating method utilizes a BitMask and hashes to verify node interaction. Each node's secret key is preserved in an authentication table, with j+m bits across each record to ensure the data capturing in the authentication table.

Table 1: Sample authentication

Node ID	Bit_Mask
1	010101
2	000111
3	110011
4	010101
5	010101

The Diffe–Hellman technique sends pairs of keys between terminals and the endpoints, then communicates using an asymmetric cryptographic procedure; this establishes a secure and authenticated connection between the nodes. As a result, the quantity of foolish nodes in the cluster is higher, while the amount of brawny nodes is lower than fool nodes; each node contains an authenticity table and its data.

The data recorded by the foolish nodes in the network is just for the brawny nodes, but the data stored by the brawny nodes is for both the foolish nodes and another brawny node in the network. Furthermore, Brawny nodes can communicate with foolish nodes given a sufficient handshake method. For example, for foolish node1, Tab. 2 shows a sample authentication field. For saving bandwidth, the Foolish node stores The NodeID and hash code of the brawny node1, and it will also get the NodeIDs of other brawny nodes in the network.

To record Several nodes in the network by all of the terminal nodes over the link, including masking bits and hashing algorithms. As an example, the connectivity used for QECC has five nodes, including four foolish nodes, two brawny nodes, and one sink or relay node. Each of the four and two foolish nodes contains information about other nodes; in this scenario, each node contains information about the other six network nodes. Nodes receive data to build cryptographically secure transmission between them. The network's foolish nodes enlist the support of brawny nodes to build communication with the other foolish nodes; The three-way handshake technique for accomplishing this divides the nodes as weak and robust

nodes to avoid insecure data transmission. The QECC function has three fields, key, node ID, and bit_mask ID is created for the solution.

Table 2: Sample authentication for fool node

Node ID	Bit_Mask
Brawny node 1	0110
Fool node 1	–
Fool node 5	–
Fool node 3	–
Fool node 4	–

4.2 QECC with AWSC

The Elliptic Curve Cryptography (ECC) key size is smaller than other non-ECC cryptographic methods, and this is because the standard symmetric approach uses a lot of bits, which is not feasible. In an earlier state, the ECC works perfectly by using a 160 bits size [26]. According to QECC, two phases are there, and it computes the pair-wise keys for the channel's nodes. Then, a using cryptographic mechanism to exchange this pair of keys with other paired nodes. Because QECC employs an asymmetric-key cryptography method, To distribute the asymmetric key in the following manner:

a) Each node has a pair of keys (public and private keys), as well as a Node ID.
b) Each node has an authenticity table that contains the node's ID number, bitmask, and by generating hash code.

The authenticity database on nodes keeps track of the network's actual public keys, including their mobile NodeID, bitmask, and hash code. For storing the authentication table in the memory location of the foolish and brawny nodes. The foolish nodes exclusively hold information from brawny nodes, while the brawny nodes, as the channel's most robust nodes, store content from both sorts of nodes, foolish and brawny nodes. The mechanism of electronic certificates (digital sign) on a secret that is only accessible by the source node in this transmission; the source node is also referred to as the signatory since it stamps the information with the sender's secret or personal key. The goal of employing electronic documents in the suggested method is to have privilege escalation, i.e., a signing is only genuine if it could be verified. AWSC, one of three types of device signatures, would be developed using an elliptic curve cryptographic technique.

4.3 Proposed Model of QECC

ECC is a new cryptographic hash function that offers excellent throughput, fast signs, and a little hash value, making it a practical option for programmers. This inter-channel stage involves tinier keys only when the key has used the encryption as a public key, and even the private key used to decode information as a public key. ECC is the premise of solid and functional elliptic curves above the contained environment. ECC comprises three steps: (1) key-creation, (2) signature method and (3) verifying process.

In Fig. 1, the communication sharing mechanism categorizing into two types of a node in QECC. Based on the communication, the nodes must first validate using data stored as the initial phase. Secondly, in the QECC technique, the node is clustered into two different types fool around node and brawny nodes.

Finally, the data exchange method exists between the nodes to identify the fool node and eliminate it from the route.

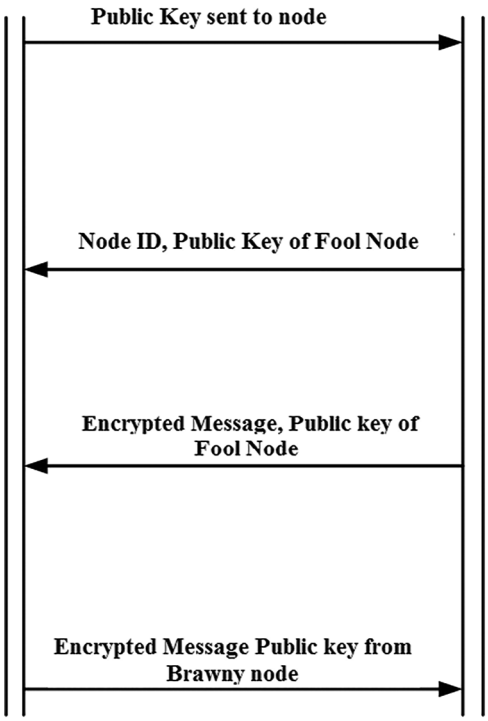

Figure 1: QECC key sharing mechanism

5 Network Model

The nodes have been set up randomly in MANET; the suggested method is designed based on the network topology. Furthermore, to configure the nodes independently, their network mobility is limited. The networking model's suggested activity splits into 2 phases: first, generate the pair-wise for node in the network after the key sharing proposes completed, and secondly, find the weak node in the network and convert the node into a powerful node; otherwise, eliminate from the network. These difficulties enable predictable routing to be ambiguous. They were anticipating a quantum-based key sharing mechanism, Addressing the unpredictability issues that are creating problems, finding the strong-node and fool node to find the acceptable route to share the content.

The node needs to communicate with the other node first, and then it needs to send and broadcast the encrypted key to all the neighbor/forwarders nodes. If a node does not even share the key/message in the network, consider that it will be a malicious node [27]. Once the node found has a weak node tried to change or recover the node too strong to take place in the routing scheme, the node will automatically eliminate over the content transmission and from the routing table. The QECC is a protocol that allows each sensor node to authenticate by exchanging their public keys. When a node transmits a message encrypted with the private key to another node, the node requests the public key. Then, it decodes the message using symmetric and asymmetric algorithms, comparing the message digest and declaring the node authorized and legitimate if the digest is the same.

Fig. 2 shows that the projected work's structural design follows how the nodes communicate between them and share the secure-key information in the networks. In Fig. 3, the security model has proposed an

algorithm to cluster the node into two sets already mentioned in the previous section. Finally, the MANET needs to create the proposed security algorithm to better the routing mechanism and secure the network from attackers.

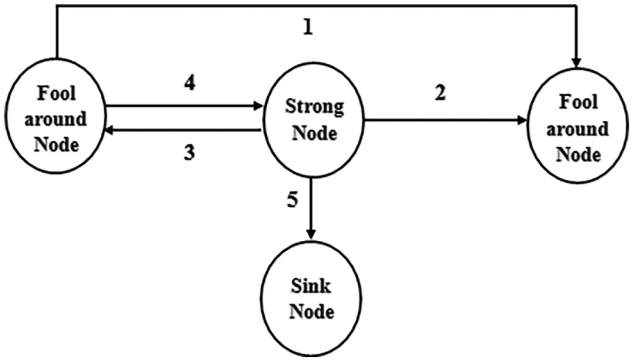

Figure 2: Communication model of strong node and fool around node

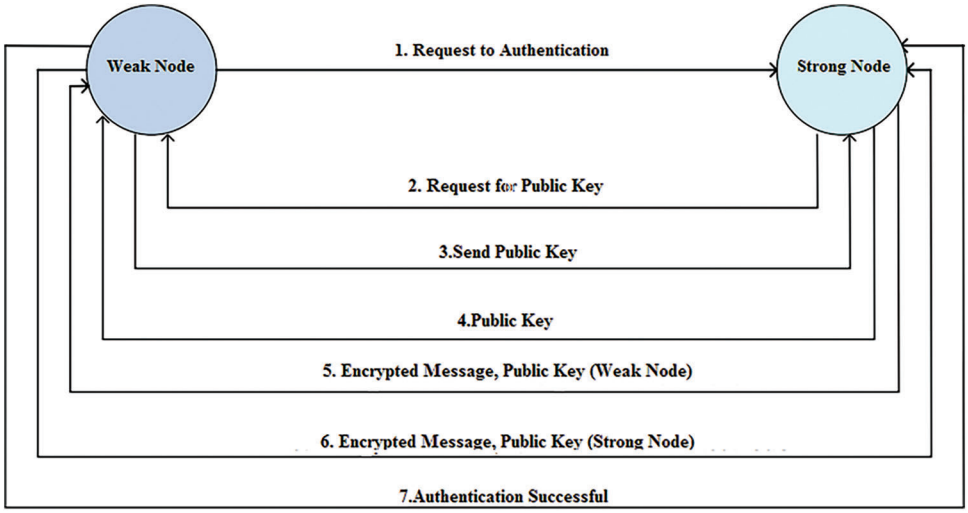

Figure 3: Security model for QECC

The exchange of content in AWSC splits into two types, i.e., exchange of content between a similar set of nodes and exchange of content among different nodes. Owing to the handshake mechanism, the interaction between 2 nodes of a similar type will produce latency. The robust endpoints are accountable for handshakes and initiating connectivity across n nodes in the identical type of node interactions; thus, the hop size is vital for the identical set of nodes will be incremented by 1.

Connectivity amongst two kinds of nodes, and from the other extreme, demands straightforward authentication and hence does not demand a solid node to build a communication channel. As a result, the number of input streams is lower throughout transmission. Tab. 3 shows the number of nodes and the overall sum of keys exchanged throughout both means of communication. It is to mention here that; the packets sent and received among the network size in MANET will grow as the number of nodes increases.

Table 3: Duration to generate pair-wise keys

No of node	Time (ms)	Key establishment
10	35	1
20	60	3
30	115	6
40	168	10
50	208	16
60	245	22
70	329	29
80	414	36
90	518	45
100	694	58

5.1 Duration to Generate Pair-wise Keys

The secret-key establishment time of creating every paired key during transmission in MANET using the QECC algorithm would be the first component upon evaluating the efficiency of QECC. The first situation involves a communication session between 2 weak nodes attempting to interact through a powerful node's handshake method. Tab. 3 demonstrates that the secure-key establishment period for interaction among two nodes of a similar kind is longer.

5.2 Count of 'Hello' Messages

The information was acquired while monitoring FN1 (weak node1) and FN2 (weak node2) interact. FN1 sends a "hello" indication to FN2, indicating that count is the amount of "hello" signals passed (Haidari et al.) [24]. Similarly, the number of "hello" signals required to handshake among two mobile nodes of a similar type through a single powerful node would be nine. The frequency for "hello" signals for various nodes includes the fact that once the number of active nodes reaches even, the frequency is lower, and when the network size is odd, the count is higher. A visual depiction of the count for "hello" signals is for a varying number of nodes. The inquiry emerges about why the amount of "hello" signals is lower for even network nodes than with odd network nodes; the explanation for this is when an approximately equal number of sensor nodes interact with one another, the quantity of "hello" messages is lower. This is because of establishing numerous pairings in the network. If an odd number of sensor nodes connect, exchange a few unnecessary "hello" statements.

5.3 Total Quantity of Bits/Data Packet

The total amount of frames sent during the interaction between two nodes of the same kind, when FN1 and FN2 wish to interact, they must rely on BN1 for assistance; additional packets can be sent for this purpose while authorizing the nodes and generating paired keys for transit between nodes. The proposed protocol's security is assessed using the capture and resend attack by using the elliptic algorithm is used to create the intercept and resend attack. The experimental results reveal that the suggested system outperforms the AWSC-based QECC method regarding "key" computation performance and safe information transfer between parties.

6 Performance Analysis

The Quantum Elliptic Curve Cryptography (QECC) is simulated in the NS2 and used to perform the routing protocol. One hundred nodes setting up in various depths, and the transmission range is 1000 m × 1000 m with a random point. Analyzing the performances of the different data packets, and calculated throughput, and examining the error rates to attain the result such as energy savings, packet delivery ratio, and trust level.

Based on Tab. 4, the number of nodes, routing protocol, data transmission, and simulation test the network performance with the help QECC algorithm. In all the aspects, by taking the simulation testing result. Analyzing the outcomes among the existing protocol is explained in the upcoming topic.

Table 4: Parameters and simulation setup

Channel used	Wireless channel
Propagation	Two ray propagation
MAC	MAC
No. of sensor node deployed	100 to 1000
Speed of the node in water	0.5 m
Nodes	Mobility nodes
Coverage	1000 × 1000 m^2
Node range	200 to 250 m
Data size	50 bytes
Start-up energy	5 J
Transmitting power	2 W
Reception power	0.75 W
Idle power	0.008 W
Filter	Gradient filter
Antenna	Omni antenna
Node position updates (interval time)	0.5 ms
Queuing length	50 m
Simulation duration	600 ms

6.1 Average Key Generation for QECC vs. AWSC

The number of nodes used in a different area the data transmission from source to destination.

Table 5: Average key generation for QECC *vs*. AWSC

Nodes	Average Key Generation (ms)	
	QECC	AWSC
10	60	45
20	158	126
30	310	289

(Continued)

Table 5 (continued).

Nodes	Average Key Generation (ms)	
	QECC	AWSC
40	468	398
50	580	545
60	631	622
70	765	740
80	777	756
90	823	798
100	876	836

Fig. 4 examined the performance of both QECC and AWSC. The basis performance of the With the use of the QECC method, Examining the "key" expansion time of creating each paired key for transmission in an ad hoc network. The system's initial method entails configuring interaction between the foolish and powerful nodes. The fool node cannot get the route information because it is considered a malicious node in the networks. The fool node is trying to communicate with each other, which help of handshaking process to the brawny node. The findings revealed that data transmission's "key" establishment time takes longer. The QECC has the most route discovery and next-hop possibilities to use the asymmetric method. When generating the pair-wise key, consider the modification of node and routing.

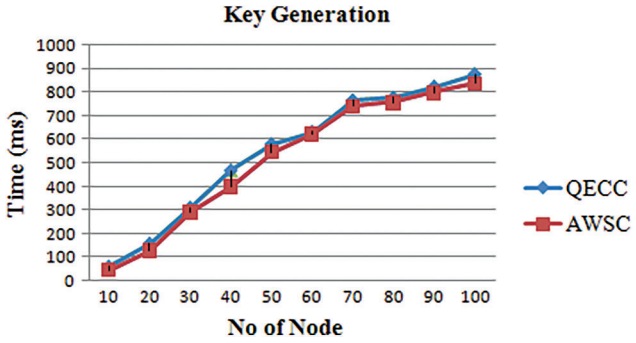

Figure 4: Average key generations

6.2 Variations of Average Count of "Hello Message" for QECC vs. AWSC

The result shows the number of hello messages to the sink node in secured communication between the forwarder nodes. The outcome is plotted based on the simulation test.

Tab. 6 shows the Average count of the hello message exchanged between the selected nodes. First, the virtual location of nodes in the network determines packet transmission between source and destination. Then, the malicious nodes select the fool node to retrieve the data. In this simulation, the node is secure and transmitted the data via the trusted path to reach the sink node, safely calculating the error rate and sending packets directly to a particular node called brawny node to sink node. So, the packet delivery ratio remains the same between source and destination, and improvement in the data security by using QECC compared to AWSC.

Table 6: Average count of "Hello" message for QECC *vs*. AWSC

Nodes	Average Count of "Hello Message"	
	QECC	AWSC
10	1	1
20	3	3
30	6	5
40	10	8
50	16	12
60	22	18
70	29	23
80	36	28
90	45	37
100	58	44

Fig. 5 depicts the information recorded between the source and sink nodes; in this case, the sender sends content to the mobile sink *via* forwarders. The node sends a 'hello' message to the sink, putting the number of 'hello' information exchanged here at one. Similarly, six 'hello' pulses would be necessary to communicate *via* a brawny node across two nodes of the same type. Tab. 6 indicates the quantity of 'hello' pulses for various nodes, as well as the fact that when the number of nodes is even, the count is minimal, and when the number of nodes is odd, the quantity is the largest. It also visually depicts the count of 'hello' signals to various node counts. The inquiry emerges about why the frequency of "hello" messages is lower for an even amount of nodes than with an odd amount of nodes; One explanation for this is because when actual sensor nodes connect, the number of "hello" messages is fewer as there are already numerous pairs in the network. While the odd number of nodes communicates with each other, there can be a few unnecessary "hello" signals during the conversation [28].

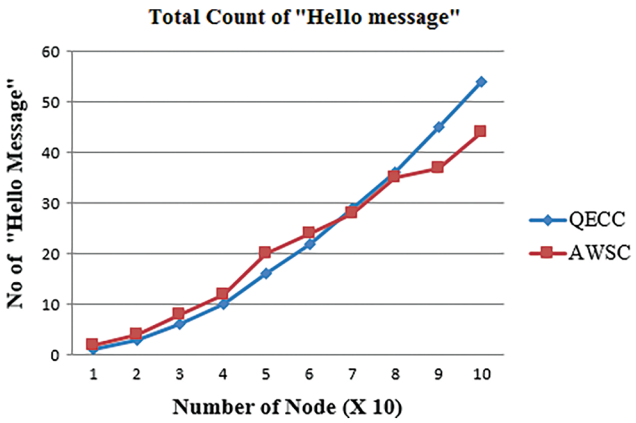

Figure 5: Average count of "Hello Message"

6.3 Variations of Average Error Rate for QECC vs.. AWSC

The simulation for changing the topology and node mobility from static to dynamic can reduce the error rate. Tab. 7 shows the average error rate.

Table 7: Average error rate for QECC *vs*. AWSC

Nodes	Average error rate (bits/s)	
	QECC	AWSC
10	5.00	8.00
20	6.20	9.12
30	8.04	10.71
40	8.31	12.71
50	9.85	13.01
60	10.19	14.06
70	11.21	13.11
80	10.92	12.90
90	9.65	12.33
100	9.32	12.34

Fig. 6 shows that the symmetric and asymmetric algorithm to discover a more reliable path raises the network size using the Euclidean function. As a result, the brawny node and source node are more likely to find the very next-hop address for the location precisely. Furthermore, by shifting the node travel from stable to the rapid evolution of architecture and transmission range, we simulated message quality, revealing that MANET is more likely to succeed than QECC. Furthermore, the symmetric and asymmetric functions rely on the fool node to turn into a powerful node then transmit messages to the sink.

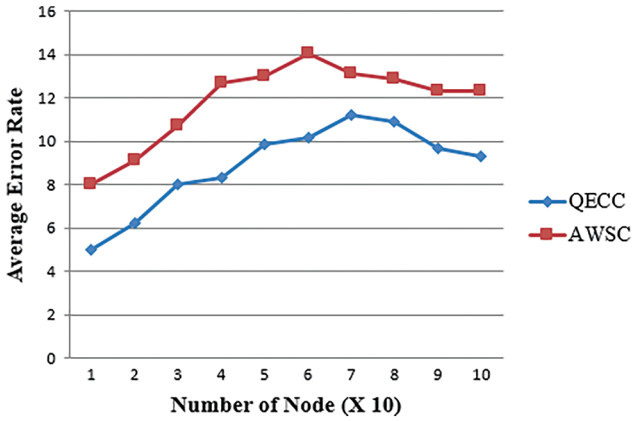

Figure 6: Average error rate

6.4 Variations of Average Trust Path for QECC Vs AWSC

We simulate the end-to-end node by altering the node mobility from fixed to dynamic network modification and locating the brawny node. Tab. 8 shows the average number of nodes present in the networks as forwarders based on that, and the calculation is to find the trust path.

Table 8: Average trust path for QECC *vs*. AWSC

Nodes	Average trust path	
	QECC	AWSC
10	0	1
20	1.2	1
30	1.5	1
40	3	1.1
50	4.2	1
60	4.7	1
70	6.2	1.1
80	7.5	1.2
90	7.9	2
100	10	2

Fig. 7 shows the data communication between the vital nodes the node sends is the 'hello message.' Similarly, the interaction between two comparable groups of nodes *via* one powerful node will result in a total of nine 'hello' signals. The quantity of 'hello' signaling for a different group of nodes, including the fact that if the number of sensor nodes would be even, the counting is lowest; however, if the number of sensor nodes is uneven, the counting for 'hello' messages is highest(Qazi et al.) [21]. The number of 'hello' signals sent by a certain amount of nodes. Also, the trusted path for QECC is at a higher rate than the previous protocol AWSC.

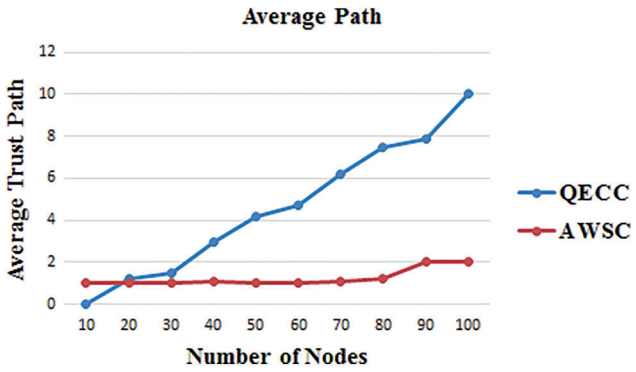

Figure 7: Average trusted path

6.5 Overall Percentage Comparison of Proposed QECC and AWSC

Table 9: Overall % comparison with all parameters

Quality parameter	QECC	AWSC
Key generation	54	52
Packet sent	68	58
Error rate	48	87
Trusted path	46	12
Trusted path	46	12

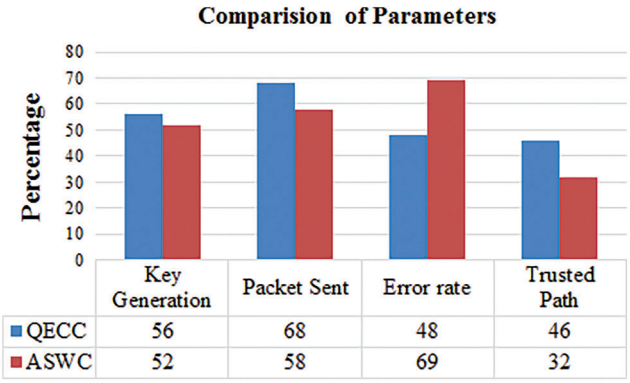

Figure 8: Overall % comparison with all parameter results

7 Conclusion and Future Work

Based on Tab. 9 and Fig. 8 the QECC's performance is simulated and analyzed using several metrics compared to the present AWSC protocol. Compared to AWSC, the average trustworthy path observed in QECC is approximately 46 percent higher, implying that a more significant number of nodes will be vulnerable to malicious attacks. In AWSC, a considerable packet loss happens due to the fool node. QECC improves the secured data packet supplied to the sink node by 68 percent and reduces packet loss. When reducing the mistake rate, the system's energy efficiency improves. Compared to the AWSC, the QECC has a 48 percent error rate reduction. The nodes may share the content in the network when using pair-wise "key" creation, which reduces the risk. As node energy improves, the network's life span improves as well. When compared to AWSC, QECC saves up to 60% of energy. The session key agreement, which includes authentication, privacy, untraceability, and resistance to various assaults, is used in the system as mentioned above for secure data transfer—our suggested method used in a range of real-world networks. In the future, data security implementation will help increase network performance by reducing the number of vulnerable assaults. In addition, as previously stated, the benefits of our QECC concept at various levels in MANET can be transferred to WSNs, allowing us to better our WSN strategy in future research like Biometric authentication, RFID, smart grid, E-health, and applications that require shared keys and cryptographic signature were all examined by QECC.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] K. N. Qureshi, S. Din, G. Jeon and F. Piccialli, "Link quality and energy utilization based preferable next hop selection routing for wireless body area networks," *Computer Communications*, vol. 149, pp. 382–392, 2020.

[2] K. N. Qureshi, A. H. Abdullah, F. Bashir, S. Iqbal and K. M. Awan, "Cluster-based data dissemination, cluster head formation under sparse, and dense traffic conditions for vehicular ad hoc networks," *International Journal of Communication Systems*, vol. 31, no. 8, pp. e3533, 2018.

[3] P. B. Hari and S. N. Singh, "Security issues in wireless sensor networks: Current research and challenges," in *Int. Conf. on Advances in Computing, Communication, & Automation (ICACCA)*, Dehradun, India, pp. 1–6, 2016.

[4] A. Yasin and M. A. Zant, "Detecting and isolating black-hole attacks in manet using timer based baited technique," *Wireless Communications and Mobile Computing*, vol. 2018, no. 1, pp. 1–10, 2018.

[5] S. Sarika, A. Pravin, V. Aishwarya and K. Selvamani, "Security issues in mobile ad hoc networks," *Procedia Computer Science*, vol. 92, pp. 329–335, 2016.

[6] V. C. Venkaiah, A. T. Naidu and A. Singh, "A dynamic key management paradigm for secure wireless ad hoc network communications," *International Journal of Information and Computer Security*, vol. 14, no. 3/4, pp. 380–402, 2021.

[7] B. Zhao, X. Zha, Z. Chen, R. Shi, D. Wang *et al.,* "Performance analysis of quantum key distribution technology for power business," *Applied Sciences*, vol. 10, no. 8, pp. 2906, 2020.

[8] G. Aymen and A. Mostafa, "Integration of a quantum scheme for key distribution and authentication within EAP-TLS protocol," *International Journal of Information and Communication Technology*, vol. 14, pp. 380–402, 2019.

[9] F. Gao, S. Qin, F. Guo and Q. Wen, "Dense-coding attack on three-party quantum key distribution protocols," *IEEE Journal of Quantum Electronics*, vol. 47, no. 5, pp. 630–635, 2011.

[10] R. Sharma, "Quantum cryptography: a new approach to information security," *International Journal of Power System Operation and Energy Management*, vol. 1, pp. 11–13, 2012.

[11] M. Safari and M. Uysal, "Relay-assisted quantum-key distribution over long atmospheric channels," *Journal of Lightwave Technology*, vol. 27, no. 20, pp. 4508–4515, 2009.

[12] G. Gao, "Cryptanalysis of multiparty quantum secret sharing with collective eavesdropping-check," *Optics Communications*, vol. 283, no. 14, pp. 2997–3000, 2010.

[13] T. Hwang, K. Lee and C. Li, "Provably secure three-party authenticated quantum key distribution protocols," *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 1, pp. 71–80, 2007.

[14] A. A. Abushgra and K. M. Elleithy, "A shared secret key initiated by EPR authentication and qubit transmission channels," *IEEE Access*, vol. 5, pp. 17753–17763, 2017.

[15] C. Lu, F. Miao, K. Meng and Y. Yu, "Threshold quantum secret sharing based on single qubit," *Quantum Information Processing*, vol. 17, no. 3, pp. 1–13, 2018.

[16] H. L. Yeh, T. H. Chen, P. C. Liu, T. H. Kim and H. W. Wei, "A secured authentication protocol for wireless sensor networks using elliptic curves cryptography," *Sensors*, vol. 11, no. 5, pp. 4767–4779, 2011.

[17] H. Wang, J. Liu, J. Zhi and C. Fu, "The improvement of quantum genetic algorithm and its application on function optimization," *Mathematical Problems in Engineering*, vol. 2013, no. 5, pp. 1–10, 2013.

[18] Z. Chen, K. Zhou and Q. Liao, "Quantum identity authentication scheme of vehicular ad-hoc networks," *International Journal of Theoretical Physics*, vol. 58, no. 1, pp. 40–57, 2019.

[19] J. Miri, B. Nsiri and R. Bouallegue, "Certificateless based quantum cryptosystem for ad-hoc UWB-IR," *Wireless Personal Communication*, vol. 114, no. 2, pp. 1805–1823, 2020.

[20] A. K. Gautam and R. Kumar, "A comprehensive study on key management, authentication and trust management techniques in wireless sensor networks," *SN Applied Sciences*, vol. 3, no. 1, pp. 393, 2021.

[21] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal *et al.,* "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 547–566, 2021.

[22] H. Bodur and R. Kara, "A comparison on broadcast encryption schemes: A new broadcast encryption scheme," *Advances in Electrical and Computer Engineering*, vol. 20, pp. 69–80, 2020.

[23] M. H. Ozcanhan and H. Turksonmez, "A strong mutual authentication protocol for SHIELD," *Advances in Electrical and Computer Engineering*, vol. 20, pp. 81–90, 2020.

[24] M. J. Haidari, Z. Yetgin and A. Elewi, "Emergency-aware irresponsible message forwarding for vehicular communications," *Advances in Electrical and Computer Engineering*, vol. 20, pp. 61–68, 2020.

[25] G. Horvat, D. Zagar and G. Martinovic, "STFTP: Secure TFTP protocol for embedded multi-agent systems communication," *Advances in Electrical and Computer Engineering*, vol. 13, no. 2, pp. 23–32, 2013.

[26] B. LaMacchia, "The long road ahead to transition to post-quantum cryptography," *Communication ACM*, vol. 65, no. 1, pp. 28–30, 2022.

[27] C. Dai and Z. Xu, "A secure three-factor authentication scheme for multi-gateway wireless sensor networks based on elliptic curve cryptography," *Ad Hoc Networks*, vol. 127, no. 1, pp. 102768, 2022.

[28] N. Ajaykumar, M. Sarvagya and P. Parandkar, "A novel security algorithm ECC-L for wireless sensor network," *Internet Technology Letters*, vol. 3, no. 3, pp. e150, 2020.