QASEC: A Secured Data Communication Scheme for Mobile Ad-hoc Networks

Muhammad Usman[a], Mian Ahmad Jan[b,*], Xiangjian He[c,*], Priyadarsi Nanda[c]

[a] *Department of Computer Science and Software Engineering, Swinburne University of Technology, Australia*
[b] *Department of Computer Science, Abdul Wali Khan University Mardan, Pakistan*
[c] *Global Big Data Technologies Center, School of Electrical and Data Engineering, University of Technology Sydney, Australia*

Abstract

Mobile Adhoc NETworks (MANETs) are valuable for various applications due to an efficient, flexible, low-cost and dynamic infrastructure. In these networks, proper utilization of network resources is desirable to maintain Quality of Service (QoS). In multi-hop end-to-end communication, intermediate nodes may eavesdrop on data in transit. As a result, a secured and reliable data delivery from source to destination is required. In this paper, we propose a novel scheme, known as QASEC, to achieve better throughput by securing end-to-end communication in MANETs. The QoS is maintained through an optimal link selection from a queue of available transmission links. The end-to-end communication is secured by authentication. A simple secret-key based symmetric encryption is deployed for interacting nodes. Our proposed QASEC scheme prevents the malicious nodes from data exchange with legitimate intermediate nodes on any established path between the source and the destination. Experimental results show that QASEC performs better in terms of packet-loss rate, jitter and end-to-end delay. Furthermore, QASEC is efficient against various attacks and has a much better performance in terms of associated costs, such as key generation, encryption, and storage and communication.

Keywords:

[*] Corresponding author

Email addresses: mianjan@awkum.edu.pk (Mian Ahmad Jan), xiangjian.he@uts.edu.au (Xiangjian He)

MANET, QoS, Authentication, Optimal link, Symmetric Encryption.

1. Introduction

Among the wireless networks, Mobile Ad-hoc NETworks (MANETs) provide infrastructureless features and the devices in MANETs can easily move from one place to another. Unlike a Wi-Fi or a 4G-based transmission system where there is a proper communication infrastructure and centralized control, multi-hop MANETs pose design challenges in the faspects of proper bandwidth utilization, Quality of Service (QoS), power consumption and data confidentiality, due to their distributed and dynamic nature. The mobile nodes in a MANET can join or leave the network at any time, can set up new links and can affect the data rates of wireless links. The multi-hop communication also demands time coordination and communication overhead for distributed control and routing, and cannot ensure the confidentiality of transmitted data over wireless links.

To maintain the QoS, the available approaches in literature are usually classified into two major domains, i.e., bandwidth-reservation-based techniques and best-effort delivery techniques [1, 2]. In the bandwidth-reservation-based techniques, the bandwidth is reserved for specific applications requesting a high and constant bandwidth. On the other hand, best-effort techniques are suitable for applications where the demands for bandwidths vary from time to time. The elasticity in a bandwidth demand helps in increasing and in maintaining the QoS of an overall network. The best-effort techniques mostly use simple and distributed algorithms and are unable to deal with any applications that demands a constant bandwidth.

Due to highly dynamic nature of a MANET, malicious nodes can easily join and roam in the network. The malicious nodes can create three major impediments, i.e., misuse of transmission links, maliciously manipulating packet transmission and information stealing [3, 4, 5, 6]. With the first impediment, a malicious node prevents its neighbours from getting a fair share of the available bandwidth. Such type of problem can also be considered as a Denial-of-Service (DoS) attack, where the transmission bandwidth is flooded with the garbage data. With the second impediment, the transmission of data packets can be disturbed in many ways, such as dropping valid data packets, delaying of packet transmission, creating routing loops and spoofing. With the third impediment, the malicious node modifies the routing tables, directs traffic to unknown destinations, and can even lead to severe consequences, such as misuse of personal data.

In this paper, we consider a QoS-Aware Secured End-to-End data Communication (QASEC) in MANETs. The QoS is ensured by selecting an optimal transmission link to maintain a smooth data transmission between source and destination nodes. For a secured data delivery from the source to destination nodes, each node along the transmission link is authenticated. As a result, the malicious nodes are barred from communication along the transmission path. The main contributions of QASEC are as follows.

- We propose a simple and lightweight scheme to select the best link among the available transmission links from source toward the destination nodes, based on the current network status. The selection of an optimal transmission link helps in efficient utilization of available bandwidth and minimization of end-to-end delay. To improve QoS, end-to-end response time and available bandwidth are estimated to evaluate the consumption of available bandwidth by the sender nodes. This evaluation enables the sender nodes to adjust their data transmission rates.

- To ensure a secured transmission over an infrastructureless and unreliable MANET, a simple authentication handshake mechanism is proposed. The proposed mechanism relies on symmetric encryption using shared secret keys and identity of each device for authentication.

The rest of the paper is organized as follows. Relevant literature is summarized in Section II. The proposed QoS-aware end-to-end secured communication scheme is discussed in Section III. In Section IV, experimental setup and results are discussed. Finally, the paper is concluded in Section V.

2. Literature Review

In this section, the related works from MANET pertaining to QASEC are presented. First, we provide Quality of Service (QoS) related literature in Section 2.1 followed by security provisioning in Section 2.2.

2.1. Quality of Service

A survey on hybrid routing protocols for MANETs was presented in [7]. This survey explains the four categories, i.e., mesh, tree, zone and multi-path, of hybrid routing mechanisms along with their performances. Another similar survey for routing protocols based on link-stability for MANETs was presented in [8]. In their survey, the routing protocols are classified based on link stability and mobility support and are explained with examples. A survey on structured Peer-to-Peer (P2P) architecture over MANETs was presented in [9]. This survey identifies approaches in terms of P2P systems and MANET underlay systems, and summarizes their performances. In order to provide the QoS mechanism during the routing process, a feedback-based routing protocol was proposed to support scalable video streaming over MANETs [10]. The proposed protocol helped in reducing the congestion in MANETs and in maintaining a better quality of received videos. However, the feedback introduced a communication overhead with an increasing number of relay nodes. To maintain QoS in MANETs, both delay and network interference were considered to control the network topology [11]. This approach could help in improving the performance of delay-constrained MANETs but at the cost of reducing transmission range. A multi-cast routing protocol was combined with network coding to meet the bandwidth requirement in lossy MANETs [12]. This protocol reduced the total bandwidth consumption and guaranteed the bandwidth availability to a requested flow but at the cost of overhead of control packets. To support the VoIP transmission in MANETs, a distributed application and a network layer protocol was proposed in [13]. To maintain the QoS level for VoIP transmission, the protocol helped in selecting the best path between the source and the destination nodes. However, due to insufficient power of mobile devices, it could not support a long range communication. Cuckoo-search-based QoS routing for MANETs was proposed in [14]. The proposed scheme satisfied the QoS constraint with better routing metrics. However, heavy computational load made this scheme unsuitable for light processing mobile devices.

2.2. Security

Similar to other wireless networks, communication over MANETs is made via radio waves. As a result, an intruder or a malicious entity can eavesdrop on communication in transit. Communication among the nodes, outside the radio range of each other, is relayed by intermediate nodes, which may further expose the network to various types of attacks. Trust among the nodes in a MANET is achieved via a web of trust model [15]. In this model, the nodes create their own public and private keys and establish trust relationships among themselves, in a self-organizing fashion. This model can be classified into two types: certificate-based model and reputation-based model. In the former model, trust is established based on the observed behaviours of participant entities within a network [16]. The latter is a simple model in which trust among the nodes is based on a central Trusted Third Party (TTP), which is responsible for ensuring trust among the nodes within the same authority domain. In a Public Key Infrastructure (PKI), the TTP is responsible to act as a Certificate Authority (CA), a trusted entity responsible for issuing, verifying and revoking of digital certificates. In [17], the authors proposed a PKI-based approach for MANET. The proposed work is based on threshold cryptography for distributing the role of the CA among the communicating nodes. The secret key of the CA is distributed among all the nodes within the network for certificate signature. The proposed work is vulnerable to mobile adversary attacks when the number of malicious nodes exceed the threshold limit set by the cryptographic approach. In [18], an on-demand public key management protocol was proposed for the self-organized nodes within MANETs. Instead of certificates, the proposed protocol relies on public keys generated by the nodes. In the absence of the CA, the self-generated public keys are less trustworthy and they affect the reliability and authenticity of the proposed protocol. In MANETs, public key authentication can be achieved using certificates or an ID-based approach, which is not the case with the proposed protocol of [18]. An on-demand routing protocol was proposed by authors in [19]. To authenticate a particular node, a certificate chain was established towards it. Although, the proposed protocol reduced the storage requirements, it incurred a high communication overhead that increases exponentially with the number of hops towards the target node. In [20], the authors proposed a secured and efficient algorithm, based on Elliptic Curve Cryptography (ECC). Instead of using a trusted third party for certificate generation, the proposed approach was a self-certified ID-based public key approach for distributed MANETs. The proposed approach was efficient in terms of computational costs, communication and storage, involved during encryption.

3. QoS-Aware Secured End-to-End Data Communication

In this section, we define a data transmission model (i.e., QASEC) for MANETs. This model is divided into two sections, i.e., the sections describing a QoS model and an authentication framework for malicious nodes detection, respectively.

3.1. Quality of Service Model

In this section, few assumptions are first discussed. Then, a routing model is proposed and explained to ensure the QoS in end-to-end data communication in MANETs.

3.1.1. Assumptions

In the QoS model, we consider a MANET consisting of N nodes and L links. Each link represents a connection between two nodes within the transmission range of each other. The nodes are assumed to be synchronized for transmission, congestion control and packet scheduling. The transmission parameters help in determining a set of available transmission links and mode of transmission. The packet scheduling helps in selecting a suitable transmission link from the set of available links. Congestion control, on the other hand, calculates the rate of incoming data traffic. It is also assumed that, within a transmission range, a node can perform multiple transmissions or receptions from multiple nodes, simultaneously. Let us assume that each source node $s \in \{1, 2, \cdots, N\}$, maintains a set of its available transmission links and selects the best transmission link, also known as primary link, for data transmission to the destination node d, where $d \in \{1, 2 \cdots, N\}$. Each node has a unique ID and we assume that the nodes exchange identification messages with each other at regular time intervals. Each identification message contains the sender node ID and its location information. It is assumed that the data rate is never zero between the source and destination nodes when the source and destination nodes are different. The data rate is a time-dependent factor and is readjusted by the contention window of d from time to time. At time t, the maximum possible traffic on a transmission link to a specific destination d is denoted by $\overline{L}_{s,d}(t)$.

3.1.2. Routing Model

Geographical routing or position-based routing is commonly used in wireless networks. The position-based routing uses either face-based routing or greedy routing or a combination of these two routing algorithms [21]. Greedy routing utilizes the local information of the network to deliver data packets to the destination. This routing scheme, also known as table-driven routing, maintains the routing tables. Our routing model is also based on the table-driven routing principles. As the nodes are mobile, it is possible that they may be moving constantly from one geographical location to another. A source node s selects an available transmission link as a primary link, only if the link represents the minimum distance to the destination or to the next hop and offers maximum bandwidth. Remaining links from the set of available transmission links are considered as backup links. Due to mobility, current primary link may not be optimal to use for further transmissions, after certain time. In this case, a new transmission link from the backup links needs to be selected as the primary link. Furthermore, the mobility will bring new nodes within the transmission range of each other, and the set of available transmission links needs to be modified and updated, instantaneously. This modification procedure will eliminate the old transmission links and will add new available transmission links.

If a link is select as the primary link at time t, then the node s will get the maximum bandwidth and can transmit maximum amount of traffic, as shown in the following equation.

$$s \longleftarrow \bar{L}_{(s,d)}(t). \tag{1}$$

The capacity of a wireless link (i.e., ε) between the source and destination nodes in a multi-hop communication can be computed using Eq. 2.

$$\varepsilon = \sum_{z=1}^{Z} \varepsilon_z, \tag{2}$$

where, ε_z is the capacity of z-th consecutive transmission link from the source and destination nodes in a link consisting of Z-hops.

The available bandwidth of the z-th transmission link in an interval of time $(t-\lambda, t]$, can be estimated as follows.

$$B_z = (1 - \overline{\theta_z})\varepsilon_z, \tag{3}$$

$$\overline{\theta_z} = \frac{1}{\lambda} \int_{t-\lambda}^{t} \theta_z(t) dt. \tag{4}$$

Here, $\theta_z(t)$ represents the instantaneous utilization of the z-th transmission link at time t and λ is the time shift.

The end-to-end available bandwidth between the source and destination nodes at time t can be computed using Eq. 5.

$$B = \sum_{z=1}^{Z} B_z. \tag{5}$$

Eqs. 2- 3 and Eq. 5, can be used for a general representation of the link capacity and the available bandwidth but may not be compatible with different network conditions. In the case of MANETs, the transmission links are usually shared and unreliable. In that situation, we compute six parameters, i.e., link capacity, end-to-end capacity, link bandwidth, end-to-end bandwidth, estimated time to transmit one data packet on a transmission link and estimated time to transmit all the data packets in the end-to-end communication.

Between any pair of nodes within the transmission range of each other, the transmission link capacity can be defined as the maximum transmission bit-rate of the transmitting node. There may be multiple transmission links between any pair of nodes but no more than one link can be used simultaneously. If each network resource is available between the source and destination nodes, then the time (i.e., T) required to transmit a Y-bit long packet from the source to destination nodes on an available z-th transmission link can be computed using Eq. 6.

$$T = \sum_{z=1}^{Z} \frac{Y}{\varepsilon_z}. \tag{6}$$

To control saturation of the link, there must be a time gap between the transmission of consecutive data packets. Let us denote this time gap by T_g, where

$$T_g << T. \tag{7}$$

Now, the maximum transmission rate on an available z-th transmission link can be computed using Eq. 8.

$$\varepsilon_z = \sum_{k=1}^{K} \frac{Y_k}{T_k}. \tag{8}$$

The end-to-end capacity of a multi-hop transmission link can be estimated using Eq. 2.

When the transmission channel is completely available and there is no competing node, then the time required to access and ultimately release the transmission link in a one-hop communication can be defined by a random variable r. In this case, the bandwidth of the z-th link can be computed by Eq. 9.

$$B_z = \frac{\varepsilon \times Y}{Y + \varepsilon \times r}. \tag{9}$$

If the transmission rate is ε bits per second and the data packet is Y-bit long, then the expected value of the link bandwidth (i.e., $E[B_z]$) can be computed using Eq. 10.

$$E[B_z] = \frac{Y}{\frac{Y}{\varepsilon} + E[r]}. \tag{10}$$

Under an ideal scheduling scheme, the average time (i.e., $\overline{r}$) required to transmit Y-bit long packet z-th link can be estimated by the following equation.

$$\overline{r} = \sum_{z=1}^{Z} \left(\frac{Y}{\varepsilon_z} + E[r] \right) \tag{11}$$

The expected end-to-end bandwidth of a multi-hop path can be estimated using Eq. 12.

$$E[B] = \min_{z=1,2,\cdots,Z} \frac{Y}{\overline{r}}. \tag{12}$$

In a network of multiple transmission links, the z-th link can transmit P packets at time t. The P includes all the transmitted data packets and control packets on a link forwarded by all the sources sharing the link. The estimated time (i.e., $\overline{T}$) to transmit all the data packets in a multi-hop communication can be computed using Eq. 13.

$$E[\overline{T}] = T \times P. \tag{13}$$

3.2. Mutual Authentication Framework

In this section, we propose an efficient authentication framework for mobile nodes, interacting in a MANET environment. The frequent topological changes within the network require a dynamic approach for securing communication among the nodes. Therefore, each incoming node needs to authenticate itself before participating in network communication. Like any other network, compromising the nodes within a MANET is a severe type of attack and each node needs an adequate level of security to ensure reliable transmission of data. Our approach uses symmetric encryption and it consists of two main phases: Configuration Phase and Authentication Phase.

During the configuration phase, each node is configured and provided with its own identity (α), a unique session key (δ) and an authentication token (Δ). It is important to mention here that α is hard-coded on each node and remains unchanged throughout the network lifetime. In our scheme, α, δ and Δ are 128-bits each. During the configuration phase, all nodes are configured offline at the time of network deployment. Each node, be it an already deployed node or an incoming node to the network, has knowledge about the identities of the legitimate nodes.

During the authentication phase, the nodes initiate mutual authentication which enable them to validate the identities of their neighboring nodes. This phase consists of four simple steps. In the first step, a node i, where $i \in \{1, 2, \cdots, N\}$, generates a request message R_i by appending α_i with t_1, as shown in Eq. 14.

$$R_i = M[\alpha_i, t_1]. \tag{14}$$

where t_1 is the assigned time stamp.

Each node broadcasts a request and assumes it to be acknowledged within a specified time period. The R_i message is usually acknowledged by one-hop neighboring nodes of node i. In the second step, node j, where $j \in \{1, 2, \cdots, N\}$, receives R_i and retrieves α_i from it. Here, node j is a one-hop neighbour of node i and $(i \neq j)$. After retrieving α_i from R_i, node j checks its own database for a matching Δ_i. The presence of α_i means that node i is a legitimate node. At this point, node j retrieves Δ_i from its own database and creates an encrypted response $\overline{R}_j$ for node i, as shown in Eq. 15.

$$\overline{R}_j = M[\Delta_i, (\Delta_i \ \oplus \delta_j)|\mu_j, t_2]. \tag{15}$$

In Eq. 15, $\overline{R}_j$ is created by node j while encrypting μ_j and δ_j with Δ_i. Here, μ_j is a pseudo-random nonce, a temporary number used only once by a node during the entire authentication process. In this equation, δ_j is a secret session key generated by node j. The exclusive-OR operation on Δ_i and δ_j generates a 128-bit result which is appended with μ_j to produce a 256-bit $\overline{R}_j$. Besides Δ_i, node j also retrieves t_1 from R_i and attaches a new time stamp t_2 to $\overline{R}_j$. The node i expects to fetch a response within the duration of its allocated time stamp t_1. An intruder node would require 2^{128} attempts to generate $\overline{R}_j$ in absence of a valid Δ_i. The security can be enhanced further if α_i is of a larger size. The presence of time stamp within R_i means that node i is expecting a response sooner and an intruder may not have sufficient time to provide a valid response. Finally, the message is encrypted with Δ_i and broadcasts to the neighboring nodes.

In the third step, node i receives $\overline{R}_j$ from node j and retrieves the encrypted parameters. At this point, node i uses its Δ_i to decrypt $\overline{R}_j$. Only a legitimate node having a valid Δ_i can decrypt $\overline{R}_j$. Here, node i retrieves δ_j and stores in its own database. Furthermore, it gains access to μ_j and checks t_2. It then calculates the difference (i.e., $\overline{t}$ =t_1-t_2) and checks if $\overline{t}$ is within the specified time period. If that is the case, it means that $\overline{R}_j$ is received from a legitimate node. At this point, node i generates its own encrypted response $\overline{R}_i$, as shown in Eq. 16.

$$\overline{R}_i = M[\delta_j, (\Delta_i \ \oplus \mu_j)|\mu_i, t_3]. \tag{16}$$

In Eq. 16, node i creates an encrypted response $\overline{R}_i$ and sends it back to node j. First, an exclusive-OR operation is performed on Δ_i and μ_j and the result is appended with μ_i. In this case, μ_i is a 128-bit pseudo-random nonce generated by node i. Finally, the result is encrypted with δ_j, and sends it back to node j with a new time stamp t_3. The receiver needs to acknowledge $\overline{R}_i$ within the duration specified by t_3.

In the fourth step, node j deciphers $\overline{R}_i$ of node i to observe μ_j in it. If present, the node j realizes that node i has successfully authenticated itself because only a legitimate node can provide μ_j. At this point, both the nodes have successfully exchanged δ_j without any tampering. The node j retrieves μ_i and creates an acknowledgment A_j as shown in Eq. 17.

$$A_j = M[\Delta_i, (\mu_i|\delta_j)]. \tag{17}$$

In Eq. 17, node j appends μ_i with δ_j and encrypts with Δ_i. The 256-bit encrypted A_j is transmitted over the wireless link. Any nearby node can receives this encrypted message, however, only one particular node that possesses a valid δ_j, can decrypt A_j. Apart from δ_j, the receiver needs to have a valid μ_i and Δ_i to understand A_j. In this case, only node i satisfies the required conditions. Upon reception, this node decrypts A_j and observe μ_i in it. At this point, node j has also authenticated itself because it has provided with node i's generated μ_i. Furthermore, both nodes have access to the same δ_j that is used for data transmission among them.

4. Experimental Setup and Simulation Results

In this section, first we explain the simulation environment for our proposed QASEC. Next, we analyze the performance of QASEC in terms of QoS in Section 4.2, followed by security consideration in Section 4.3.

4.1. Network Simulation Setup

We use Matlab for network simulation. In our experiments, 1000 mobile nodes are randomly deployed in an area of 2000×2000 m^2. Due to such a large scale network, the Matlab takes a significant amount of time to execute the simulation. The wireless communication is based on IEEE 802.11 standard and the transmission range of each mobile node is set to 100 m. The multi-path transmission helps in reducing the computational load on the hops. The mobile nodes move with a speed of 1 m/s and change their positions after every 60 seconds. The simulations run on a system with Core $i5$, 3.30 GHz processing unit and 16GB RAM. The total number of data generating sources can be either fixed or variable. In our simulations, we fix the data generating sources to 150. We execute the simulation for three times to monitor the performance of our proposed QASEC scheme. Overall, the simulation runs for more than 10 hours due to the large scale of network.

4.2. Quality of Service Analysis

In our proposed routing scheme, nodes maintain a table of all the available transmission links to the destination. Therefore, we compare its performance with other table-driven routing protocols, such as Optimized Link State Routing (OLSR) protocol [22] and Destination Sequence Distance Vector (DSDV) protocol [23]. These routing protocols are standard routing protocols in MANETs [24, 25, 26]. The comparison is performed based on different metrics, such as end-to-end delay, jitter, packet-loss rate and total number of control packets. The experiments are performed under constant bit-rate scenario, i.e., each data packet has the same size. Fig. 1 shows a comparison of the end-to-end delay for 150 data generating sources. Due to the selection of the optimum link, the end-to-end delay of our proposed routing scheme is lower than the OLSR and DSDV protocols.

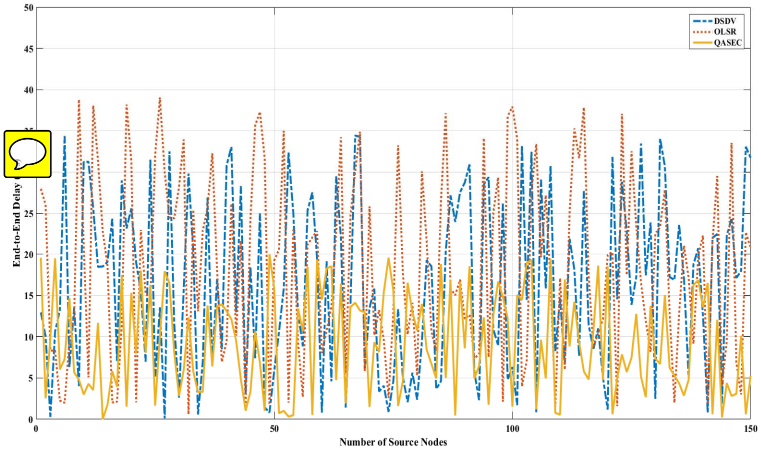

Figure 1: Packet-loss rate vs. Number of source nodes

The selection of the optimum link also helps in reducing the jitter as shown in Fig. 2. In MANETs, the end-to-end delay and jitter increase with an increase in the number of hops between the source and destination nodes. Packet-loss by the hops requires retransmission of the data packets and is very common in the constant bit-rate scenario. The drop of the data packets has a direct relationship with the end-to-end delay as shown in Fig. 3. A higher ratio of packet-loss increases the end-to-end delay.

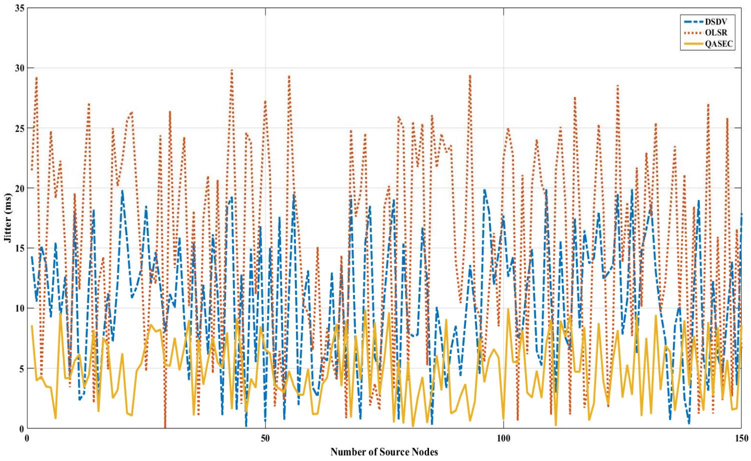

Figure 2: Jitter vs. Number of source nodes

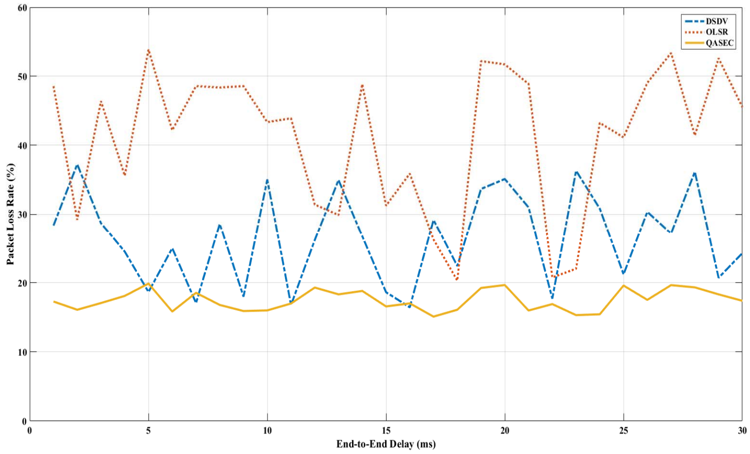

Figure 3: Packet loss rate vs. End-to-end delay (ms)

Backup of multiple transmission paths help in efficiently utilizing the network resources. Due to the increasing ratio of packet-drop, more retransmission attempts are required. These retransmission attempts increase the network traffic and consume a sufficient amount of bandwidth. More retransmission attempts also degrade the QoS. Finally, the control packets are monitored. Our proposed routing scheme continuously monitors the status of the network and updates the tables of available transmission links. In the table-driven routing, the mobile nodes share the routing tables with each other. Therefore, the overhead of control packets is almost the same in our proposed routing scheme when compared with OLSR and DSDV protocols, as shown in Fig. 4.

4.3. Security Analysis

In our proposed authentication framework, we use symmetric encryption in which secret keys and identification tokens are used to secure the exchange of data. We use Advanced Encryption Standard (AES) with a key length of 128 bits in Cipher Block Chaining (CBC) mode to generate various requests and responses of authentication. AES-128 in CBC mode is extremely lightweight for resource-constrained nodes and incurs less computational overhead on each node. To verify the authenticity and integrity of messages, we use cipher block chaining in CBC-MAC mode. In this section, we analyze various performance metrics to evaluate our proposed security scheme.

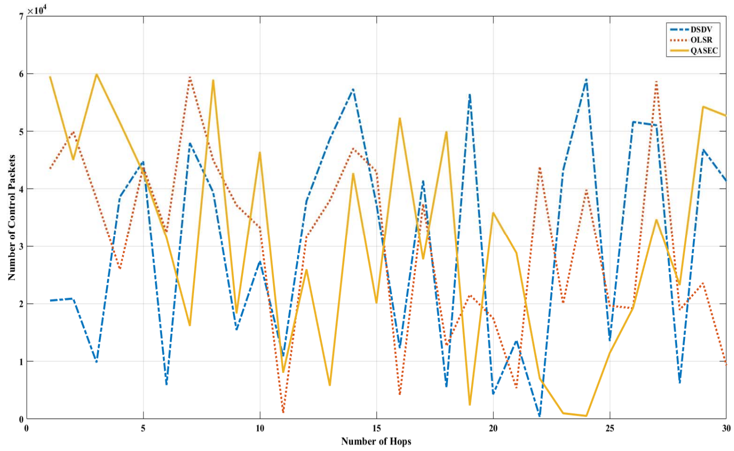

Figure 4: Number of control packets vs. Number of hops

4.3.1. *Key Generation Cost*

In Table 1, the cost associated with key generation for various schemes is shown. In the case of the existing works proposed in [20] and [19], a lot of resources are consumed in terms of timing and energy consumption. In [20], ECC-based operations are performed, whereas in [19], certificates are generated. Both these operations consume a significant among of time and energy during keys generation. In our proposed scheme, the session key is generated instantly once a match is found with the device identity, within the stored database. As a result, our proposed scheme performs much better in terms of timing and energy consumption.

Table 1: Key Generation Cost

Operation Costs	Timing (ms)	Energy (mj)
Gharb et al. [20]	738.27	226.65
Dahshaen et al. [19]	1384.27	1150.55
Proposed Scheme	257.49	199.23

4.3.2. *Encryption Cost*

In Table 2, the encryption cost of our proposed scheme is compared against the existing schemes of [20] and [19]. In these schemes, resource-intensive operations are performed during the encryption. As a result, they incur much higher cost. In our scheme, a simple handshake mechanism is initiated, once a match is found for the device identity. In terms of timing, our proposed scheme takes only 102.1 ms to complete the mutual handshake between the communicating nodes, on a specific path. The lightweight handshaking approach of our scheme consumes only 119.3 mJ of energy. Please note that the encryption cost does not include the cost associated with the first step of our proposed scheme. This is because this step only aims to generate a key at the receiver end.

Table 2: Encryption Cost

Operation Costs	Timing (ms)	Energy (mJ)
Gharb et al. [20]	151.4	134.2
Dahshaen et al. [19]	364.8	513.8
Proposed Scheme	102.1	119.3

4.3.3. Storage and Communication Costs

In Table 3, a comparison is made with the existing schemes in terms of storage requirement and communication overhead costs. When the number of nodes is 100 and the path length is 10, the existing scheme of [20] requires a storage capacity of 6.09 KB and has a communication overhead of 22.19 MB. For the same number of nodes and path length, [19] has a storage requirement of 10 KB and a communication overhead of 88.95 MB. The ECC-based operation of [20] and the certificate-based operations of [19] incur higher storage and communication costs. Unlike the existing schemes, our proposed approach does not require the exchange of certificates and complex encryption. As a result, it has less storage and communication costs.

Table 3: Storage and Communication Costs

Operation Costs	Storage (KB)	Communication (MB)
Gharb et al. [20]	6.09	22.19
Dahshaen et al. [19]	10	88.95
Proposed Scheme	3.77	16.25

5. Conclusion

In this paper, we have proposed a framework (i.e., QASEC) for QoS-aware secured end-to-end data communication in MANETs. The QoS has been improved by selecting the optimal transmission links between the source and destination nodes. The optimal link has been selected, based on the available bandwidth and response time for an end-to-end communication. Besides QoS-aware routing, we have proposed a simple end-to-end secured communication framework for the nodes along a particular path towards the destination. The proposed approach engages the neighboring nodes to authenticate themselves. A simple handshake mechanism is deployed to validate the identities of communicating entities. In the experimental results, our proposed routing scheme have shown better performance as compared to the standard table-driven routing protocols in terms of packet loss rate, jitter and end-to-end delay. The experimental results also have proved that the proposed authentication scheme has performed better than the existing authentication schemes based on various associated costs, such as key generation, authentication, and storage and communication.

References

[1] Q. Ye, W. Zhuang, L. Li, P. Vigneron, Traffic load adaptive medium access control for fully-connected mobile ad hoc networks, Vehicular Technology, IEEE Transactions on 65 (2016) 9358–9371.

[2] A. Nadembega, A. Hafid, T. Taleb, An integrated predictive mobile-oriented bandwidth-reservation framework to support mobile multimedia streaming, IEEE Transactions on wireless communications 13 (2014) 6863–6875.

[3] N. Schweitzer, A. Stulman, A. Shabtai, R. D. Margalit, Contradiction based grayhole attack minimization for ad-hoc networks, IEEE Transactions on Mobile Computing (2016).

[4] J.-M. Chang, P.-C. Tsou, I. Woungang, H.-C. Chao, C.-F. Lai, Defending against collaborative attacks by malicious nodes in manets: A cooperative bait detection approach, IEEE systems journal 9 (2015) 65–75.

[5] N. Schweitzer, A. Stulman, A. Shabtai, R. D. Margalit, Mitigating denial of service attacks in olsr protocol using fictitious nodes, IEEE Transactions on Mobile Computing 15 (2016) 163–172.

[6] R. Zhang, J. Sun, Y. Zhang, X. Huang, Jamming-resilient secure neighbor discovery in mobile ad hoc networks, IEEE Transactions on Wireless Communications 14 (2015) 5588–5601.

[7] G. A. Walikar, R. C. Biradar, A survey on hybrid routing mechanisms in mobile ad hoc networks, Journal of Network and Computer Applications (2016).

[8] A. Mousaouii, A. Boukram, A survey of routing protocols based on link-stability in mobile ad hoc networks, Journal of Network and Computer Applications 47 (2015) 1–10.

[9] M. Al Mojamed, M. Kolberg, Structured peer-to-peer overlay deployment on manet: A survey, Computer Networks 96 (2016) 29–47.

[10] W. Castellanos, J. C. Guerri, P. Arce, Performance evaluation of scalable video streaming in mobile ad hoc networks, IEEE Latin America Transactions 14 (2016) 122–129.

[11] X. M. Zhang, Y. Zhang, F. Yan, A. V. Vasilakos, Interference-based topology control algorithm for delay-constrained mobile ad hoc networks, IEEE Transactions on Mobile Computing 14 (2015) 742–754.

[12] Y.-H. Chen, E. H.-K. Wu, G.-H. Chen, Bandwidth-satisfied multicast by multiple trees and network coding in lossy manets, IEEE Systems Journal 11 (2017) 1116–1127.

[13] F. De Rango, P. Fazio, F. Scarcello, F. Conte, A new distributed application and network layer protocol for voip in mobile ad hoc networks, IEEE Transactions on Mobile Computing 13 (2014) 2185–2198.

[14] V. Mandhare, V. Thool, R. Manthalkar, Qos routing enhancement using metaheuristic approach in mobile ad-hoc network, Computer Networks 110 (2016) 180–191.

[15] K. Govindan, P. Mohapatra, Trust computations and trust dynamics in mobile adhoc networks: A survey, IEEE Communications Surveys & Tutorials 14 (2012) 279–298.

[16] R. Akbani, T. Korkmaz, G. Raju, Emltrust: an enhanced machine learning based reputation system for manets, Ad Hoc Networks 10 (2012) 435–457.

[17] L. Zhou, Z. J. Haas, Securing ad hoc networks, IEEE network 13 (1999) 24–30.

[18] S. Maity, R. C. Hansdah, Self-organized public key management in manets with enhanced security and without certificate-chains, Computer Networks 65 (2014) 183–211.

[19] H. Dahshaen, S. Irvine, A robust self-organized public key scheme for manets, Security and Communication Networks 3 (2010) 16–30.

[20] M. A. Gharb, Z. Moradhlou, M. A. Dostaari, A. Moovagher, Fully-distributed ecc based key management scheme for manets, Computer Networks 113 (2017) 269–283.

[21] M. Mauve, J. Widmer, H. Hartenstein, A survey on position-based routing in mobile ad hoc networks, IEEE network 15 (2001) 30–39.

[22] T. Clausen, P. Jacquet, Optimized link state routing protocol (OLSR), Technical Report, 2003.

[23] C. E. Perkins, P. Bhagwat, Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers, in: ACM SIGCOMM computer communication review, volume 24, ACM, 1994, pp. 234–244.

[24] M. Abolhasan, T. Wysocki, E. Dutkiewicz, A review of routing protocols for mobile ad hoc networks, Ad hoc networks 2 (2004) 1–22.

[25] G. A. Walikar, R. C. Biradar, A survey on hybrid routing mechanisms in mobile ad hoc networks, Journal of Network and Computer Applications 77 (2017) 48–63.

[26] M. Tarique, K. E. Tepe, S. Adibi, S. Erfani, Survey of multipath routing protocols for mobile ad hoc networks, Journal of Network and Computer Applications 32 (2009) 1125–1143.