A QoS Secured Data Communication strategy for MANET

[1]Mrs.K.Vijayalakshmi, [2]Mr.R.Kalaiselvan

[1]Lecturer, Computer Science and Engineering, Srinivasa Subbaraya Government Polytechnic College ,Puthur -609108,

[2]Assistant Professor, Computer Science and Engineering, Parisutham Institute of Technology and Science, Thanjavur -613006.

Email: mailtovijius@gmail.com

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. It is used 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 QAS (Quality Assurance Security) 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 QAS performs better in terms of packet-loss rate, jitter and end-to-end delay. Furthermore, QAS 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: 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 aspects 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 band- width 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 application 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 a source node to a destination node, 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 QAS are as follows.

- We propose a simple and lightweight scheme to select the best link from the available transmission links from a source node to a destination node, based on 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 infrastructure less 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.

2. Literature Review

In this section, the related works on MANET pertaining to QAS are presented. First, we provide a literature review on Quality of Service (QoS) in Section 2.1 and then the literature review on security provisioning in Section 2.2.

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 MANET 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.

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 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. 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 [12], 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.

2. 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.

Quality of Service Model

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

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 $L_{s,d}(t)$.

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. 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 link consisting of *Z*-hops.

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

$$B_z = (1 - \theta_z)\varepsilon_z, \qquad (3)$$

Here, $\theta_z(t)$ represents the instantaneous utilization of the *z*-th transmission link at time

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

$$B = \sum_{z=1}^{Z} B_z. \qquad (4)$$

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 trans- mission 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.

$$T_g << T \qquad (5)$$

To control saturation of the link, there must be a time gap between the transmission of consecutive data packets.

$$B_z = \frac{\varepsilon \times Y}{Y + \varepsilon \times r}. \qquad (6)$$

Now, the maximum transmission rate on an available *z*-th transmission link can be computed using Eq. 7.

$$E[B_z] = \frac{Y}{\frac{Y}{\varepsilon} + E[r]}. \qquad (7)$$

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

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 net- work 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 nod and remains unchanged throughout the network lifetime. In our scheme, α, δ and Δ are 128-bits each. During the con- figuration 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. 8.

$$R_i = M[\alpha_i, t_1]. \qquad (8)$$

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.

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.

Quality of Service Analysis

In our proposed routing scheme, nodes maintain a table of all the available trans- mission links to the destination. Therefore, we compare its performance with other table-driven routing protocols, such as Optimized Link State Routing (OLSR) protocol and Destination Sequence Distance Vector (DSDV) protocol. These routing protocols are standard routing protocols in MANETs. 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. It is shown clearly that due to the selection of an optimum link, the end-to-end delay of our proposed routing scheme

(14)

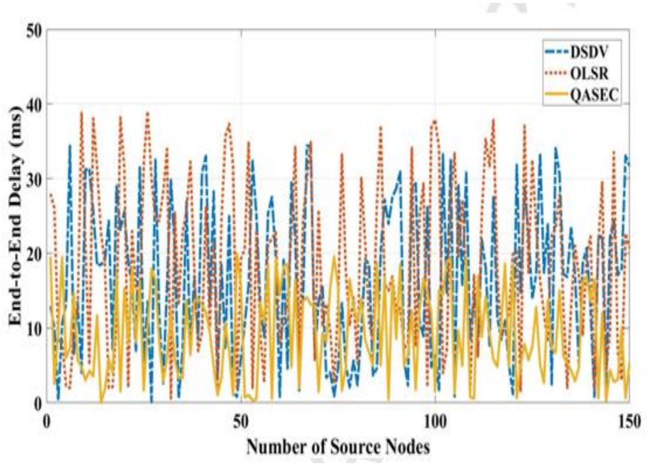

Fig. 1 Number of control packets vs. Number of hops

Security Analysis

In our proposed authentication framework, we use a symmetric encryption scheme 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 authentica- tion. 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 in- tegrity 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.

Table 1: Key Generation Costs

Schemea	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

Conclusion

In this paper, we have proposed a framework (i.e., QAS) for QoS-aware se- cured 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 rout- ing 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 con- trol 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 gray- hole 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 ser- vice 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 discov- ery in mobile ad hoc networks.

[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 con- trol 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.

go,

[13] 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 meta- heuristic 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.