Secure and Robust Multi-Constrained QoS aware Routing Algorithm for VANETs

Mahmoud Hashem Eiza, Thomas Owens, and Qiang Ni, *Senior Member, IEEE*

Abstract— Secure QoS routing algorithms are a fundamental part of wireless networks that aim to provide services with QoS and security guarantees. In Vehicular Ad hoc Networks (VANETs), vehicles perform routing functions, and at the same time act as end-systems thus routing control messages are transmitted unprotected over wireless channels. The QoS of the entire network could be degraded by an attack on the routing process, and manipulation of the routing control messages. In this paper, we propose a novel secure and reliable multi-constrained QoS aware routing algorithm for VANETs. We employ the Ant Colony Optimisation (ACO) technique to compute feasible routes in VANETs subject to multiple QoS constraints determined by the data traffic type. Moreover, we extend the VANET-oriented Evolving Graph (VoEG) model to perform plausibility checks on the routing control messages exchanged among vehicles. Simulation results show that the QoS can be guaranteed while applying security mechanisms to ensure a reliable and robust routing service.

Index Terms— ACO, evolving graph, multi-constrained QoS (MCQ), reliable routing, secure routing, VANETs

1 Introduction

In recent years, development of Vehicular Ad hoc Networks (VANETs) has received more attention and research effort from the automotive industries and academic community [1], [2], [3]. VANETs are a particular form of wireless network made by vehicles communicating among themselves and with roadside units (RSUs). The wireless communications provided by VANETs have great potential to facilitate new services that could save thousands of lives and improve the driving experience. A key requirement for such services is that they are offered with Quality of Service (QoS) guarantees in terms of service reliability and availability. However, the highly dynamic nature of VANETs and their vulnerability to both external and internal security attacks raise important technical challenges in terms of reliable and secure routing. These challenges are the subject of this paper.

QoS routing plays an essential role in identifying routes that meet the QoS requirements of the offered service over VANETs. However, identifying feasible routes in a multi-hop vehicular network subject to multiple QoS constraints is a Multi-Constrained (Optimal) Path (MC(O)P) problem, which is proven to be NP-hard [4] if the constraints are mutually independent [5]. Much work has been conducted that addresses QoS routing and the MC(O)P problem in stable networks such as Internet and wireless sensor networks [6], [7], [8], [9]. Generally, there are two distinct approaches adopted to solve MC(O)P problems, exact QoS routing algorithms and approximation routing algorithms. In the exact solutions, different strategies have been followed such as nonlinear definition of the path length [10], look-ahead feature [11], and k shortest paths [12]. Unfortunately, these strategies are not suitable for application in highly dynamic networks like VANETs. For instance, the look-ahead strategy proposes computing the shortest path tree rooted at the destination to each node in the network for each of the m link weights separately where m is the number of QoS constraints [13]. This proposal means that Dijkstra's algorithm [14] should be executed m times. This strategy is not suitable for application in VANETs because it adds extra time complexity to the routing algorithm that is expected to establish routes for real time applications. In contrast, approximation solutions such as swarm intelligence based algorithms display several features that make them particularly suitable for solving MC(O)P problems in VANETs. They are fully distributed so there is no single point of failure, the operations to be performed at each node are simple, they are self-organising, thus robust and fault tolerant, and they intrinsically adapt to traffic changes without requiring complex mechanisms [15]. Ant Colony Optimisation (ACO) is one of the most successful swarm intelligence techniques. It has been recognised as an effective technique for producing results for MC(O)P problems that are very close to those of the best performing algorithms [16]. However, how and in particular to the degree which the ACO technique can improve multi-constrained QoS (MCQ) routing in VANETs as well as mitigate security threats against the routing process have yet to be addressed.

To the best of our knowledge, none of the previously conducted work on MCQ routing in VANETs considers the security of the routing process. In general, attacks on the routing process in ad hoc networks aim to increase the adversaries control over communication between some nodes, degrade the QoS provided by the network, and increase the resource consumption of the victim nodes [17]. An adversary's capacity to mount specific at-

- *Mahmoud Hashem Eiza and Thomas Owens are with the College of Engineering, Design and Physical Sciences, Brunel University London, Middlesex UB8 3PH, U.K. E-mail: {Mahmoud.HashemEiza, Thomas.Owens}@brunel.ac.uk*
- *Qiang Ni is with the School of Computing and Communications, Lancaster University, Lancaster, LA1 4WA, U.K. E-mail: Q.Ni@lancaster.ac.uk*

tacks depends on its nature, *i.e.*, external or internal adversary. Due to the fact that vehicles' communications are not usually protected physically and may be controlled and compromised by attackers, it can be deduced that VANETs can be subject to both internal and external adversaries. Routing control messages are the main target of adversaries mounting attacks against the routing process. Route disruption, route diversion, and creation of incorrect routing states are examples of security attacks that can be mounted against the routing process by manipulating the routing control messages [17]. The information within the routing control message can be classified into mutable and immutable information. Immutable information is set by the source node and not changed during the routing process, *e.g.*, the source and destination addresses. In contrast, mutable information is changed at each intermediate node to complete the route discovery process. Changes in mutable information can be divided into traceable changes, *e.g.*, addition of a new intermediate node identifier, and untraceable changes, *e.g.*, an increase in the hop-count value. Protecting immutable information is relatively easy by applying a proper security mechanism such as digital signatures. However, protecting the mutable and more specifically untraceable mutable information such as hop-count is much harder for two reasons. First, intermediate nodes have not yet added some of this information, and the number of nodes that will contribute to this information cannot be anticipated. Second, it is not possible to tell the origin of changes or updates to this information simply by looking at its value, *e.g.*, a hop-count.

In this paper, we propose a novel secure ACO-based MCQ aware (S-AMCQ) routing algorithm for VANETs. S-AMCQ aims to identify feasible routes between two vehicles subject to multiple QoS constraints, and provide a reliable and robust routing service. The novelty of S-AMCQ lies in the unique design of its ACO-based algorithm components that considers the topological properties of VANETs including variable communication link quality and frequent link breakages. More specifically, the rules of S-AMCQ routing algorithm consider the reliability of communication links among vehicles as the most important factor while searching for a desired route. Focusing on the fundamental problem of developing a secure and robust MCQ routing algorithm, the paper makes two major contributions. Firstly, we develop S-AMCQ routing algorithm that adapts to the characteristics of the vehicular network's topology and computes the optimal route, if such a route exists. Secondly, we utilise the evolving graph theory and extend the VANET-oriented evolving graph (VoEG) model [18] that captures the evolving characteristics of the vehicular network topology. The extended VoEG (E-VoEG) model represents the vehicular network's current status, and helps to ensure consistency of the authenticated received routing control messages in S-AMCQ, *i.e.*, it mitigates suspicious behaviour or attacks that could be mounted by compromised vehicles if any exist. This is accomplished via plausibility checks that are developed specifically for S-AMCQ routing algorithm. To further illustrate the effectiveness of the proposed S-AMCQ routing algorithm, we perform simulation experiments that introduce the security information overhead into the routing process. Simulation results demonstrate that S-AMCQ can guarantee significant performance in terms of QoS guarantees and reliable routing service while applying security mechanisms.

S-AMCQ routing algorithm considers the class of applications having only a single destination, *i.e.*, unicast routing. Traffic related inquiries and general information services such as Web surfing, email, *etc.*, are examples of such applications. The performance of S-AMCQ routing algorithm is examined for a highway scenario where vehicles move at varying velocities and are allowed to stop, turn, and leave the highway as in a real world situation. Highways are expected to be the main target for the deployment of vehicular communication networks.

The rest of the paper is organised as follows. Section 2 presents the system assumptions made about the vehicular network system. Section 3 overviews the related work in this field. Section 4 defines the ACO rules developed to solve the MC(O)P problem in VANETs. Section 5 presents the E-VoEG model. Section 6 proposes S-AMCQ routing algorithm and discusses the developed plausibility checks. Section 7 assesses the performance of S-AMCQ routing algorithm. Finally, section 8 concludes the paper.

2 System Assumptions

Before describing the proposed S-AMCQ routing algorithm, we assume the following requirements are met in the vehicular network system

1. Each vehicle has a unique identity C_v. This feature can be accomplished through an Electronic Licence Plate (ELP) issued by a governmental transportation authority or an Electronic Chassis Number (ECN) issued by the vehicle manufacturer [19].
2. A Certification Authority (CA) exists that is known and trusted by all vehicles. It can be either a local transportation authority or the vehicle manufacturer.
3. Each vehicle obtains a set of pseudonymous certificates from the CA and legitimate RSUs along the road. In this paper, we adopt the pseudonymous authentication scheme (PASS) [20] where each vehicle can use a pseudonymous certificate within a specific time slot, *e.g.*, $Cert_{CA,Cv,j}$ denotes the vehicle C_v's pseudonymous certificate in the time slot TS_j issued by the CA. It is assumed that RSUs connect with the CA and provide information dissemination and certificate updating services to vehicles. The CA determines the validity period of the pseudonymous certificate and the number of certificates that a vehicle has to obtain from RSUs depending on the traffic density along the road. Unlike other pseudonymous authentication schemes such as BP [19], PASS optimises the size of the certificate revocation list (CRL) to be linear with the number of revoked vehicles and unrelated to the number of pseudonymous certificates held by the revoked vehicle, *e.g.*, 43800 pseudonymous certifi-

cates are added to the CRL when one vehicle is revoked in BP scheme [19]. Moreover, PASS provides strong privacy preservation to vehicles against the RSUs. For instance, in the efficient conditional privacy preservation (ECPP) scheme [21], the adversary can find out all the certificates that are issued by the compromised RSU for the vehicle of interest. However, in the PASS scheme, RSUs do not know what certificates a vehicle holds. The PASS scheme utilises the Schnorr digital signature algorithm [22] and SHA-1 [23] as the one-way hash function. However, since SHA-1 has been broken [24], we suggest using SHA-2 instead.

4. The public key of the CA, *i.e.*, PuK_{CA}, the one-way hash function, and the digital signature algorithm are known to each vehicle and published by the CA.
5. Vehicles cannot lie about their position, *i.e.*, a secure positioning solution is used.
6. A tamper-proof device (TPD) is used to store the cryptographic information mentioned above. A TPD is a device that provides secure storage of cryptographic information and sensitive data as well as accelerating and securing cryptographic operations [25].
7. The Dedicated Short Range Communication (DSRC) standard is deployed. DSRC is a wireless technology designed to support a variety of applications based on vehicular communications, more specifically collision prevention applications [26]. It utilises the IEEE 802.11p Wireless Access for Vehicular Environment (WAVE) standard at the PHY and MAC layers, which is more promising than other competing technologies such as the infrastructure-based LTE to support beaconing in DSRC [27]. DSRC requires each vehicle to broadcast a routine traffic message called a Basic Safety Message (BSM), also known as a beacon, every 100 *ms*. BSMs contain information on a vehicle's current status such as its location, velocity, direction, *etc*. We assume that BSMs are secured using the PASS scheme, and compromised vehicles, *i.e.*, internal adversaries, cannot alter the information a BSM contains.

3 Related Work

To the best of our knowledge, there are no previous studies on the development of a secure MCQ routing algorithm using the ACO technique in VANETs. MCQ routing and securing the routing process in ad hoc networks have been separately studied.

Recently, much work has been carried out on ACO-based QoS routing algorithms for mobile ad hoc [28], [29], [30], [31], [32], [33], [34] and sensor networks [35], [36], [37], [38]. However, little attention has been given to providing MCQ routing in VANETs utilising the ACO technique. With regard to ACO-based QoS routing algorithms for Mobile Ad hoc Networks (MANETs), Liu *et al.* [29] propose an improved ant colony QoS routing algorithm (IAQR). IAQR introduces a routing problem with four QoS constraints associated with nodes or links including delay, bandwidth, jitter, and packet loss constraints. The algorithm can find a route in a MANET that satisfies more QoS requirements of the incoming traffic. It starts by removing links and nodes that do not satisfy the defined constraints, starting with the bandwidth constraint, from the network. It then initialises the pheromones on each link with a constant value and positions a set of ants at the source node. At each iteration N_c, each ant chooses its next hop based on the transition rule and updates the pheromone value of the link using a local pheromone evaporation parameter. Once it reaches the destination node, the ant calculates the objective function based on the achieved QoS metrics. Each ant continues searching for a route until the termination condition, $N_c > N_{max}$, is met.

A QoS-based clustering protocol for VANETs, named VANET QoS-OLSR, is proposed in [39]. The goal of this protocol is to form stable clusters and maintain their stability during communication and link failures while satisfying QoS requirements. Bandwidth, connectivity, and mobility are the metrics considered when computing the QoS value per node. VANET QoS-OLSR utilises the ACO technique to present a Multipoint Relays (MPRs) selection algorithm with respect to QoS and mobility constraints. Once elected, a cluster head sends ANT-HELLO messages to its 2-hops away nodes. Each 2-hops away node that receives this ant message calculates its QoS metrics and inserts them in the message. The updated message is then propagated 2-hops away and the updating process is followed until the ant reaches the destination cluster head. Once reached, the destination cluster head extracts the QoS metrics information from the ant and calculates the pheromone value of the whole route. The nodes belonging to the route having the highest pheromone value are then selected to send an ANT-HELLO message back to the source cluster head. Finally, the source cluster head selects the nodes belonging to the discovered route that are located within its cluster as MPRs.

It can be noticed that most of the ACO-based routing algorithms, including the above two mentioned algorithms, employ the ACO technique without optimising its components for the network environment it is proposed for. For instance, pheromone deposit and evaporation processes are performed using constant parameters in most cases. Furthermore, in the context of vehicular networks, sending a set of ants to find feasible routes may not be a practical option. It implies a long delay waiting for the ants to finish their tours, and it is highly likely the network topology will have changed to a certain degree over that time, so that the discovered solutions may not be viable anymore. Therefore, the efficiency of ACO technique in the context of vehicular networks has not yet been well established in the literature.

In the context of securing the routing process of ad hoc routing protocols proposed for VANETs, much work has been done to defend the routing process against potential external and internal adversaries [40]. Security mechanisms such as digital signatures and message authentica-

tion codes are used to protect immutable information within the routing control messages, while mechanisms such as per-hop hashing and hash chains are used to protect the mutable information. Since these mechanisms are not enough to mitigate security attacks mounted by internal adversaries, two security mechanisms have been proposed: reputation systems [41], [42], [43], [44] and plausibility checks [45], [46], [47]. In the reputation system mechanism, each vehicle is assigned a reputation score based on its behaviour and feedback from other nodes. The message, generated by a node, is considered legitimate if this node has a sufficiently high reputation score. A centralised reputation system is proposed in [44] where a reputation system server collects feedback from vehicles, produces the reputation scores for vehicles, propagates these reputations scores, and admits or revokes vehicles from the system. Vehicles are supposed to communicate with the reputation server via RSUs. Digital signatures and message authentication code schemes are used to secure the communications between vehicles and the reputation system server.

On the other hand, the plausibility checks mechanism aims to build a model for the current network at each node then checks the consistency of the received message's contents against the network model. Golle *et al.* [47] assumed that each vehicle maintains a model that contains all the knowledge available to it about the vehicular network. The network model at each vehicle is based on formal definitions and logical reasoning of events and vehicles, and is used to determine if a reported event is consistent with the network model or not. For instance, if the contents of a received message claim that its sender is at a location that exceeds the maximum communication range of the receiver, then this message is considered inconsistent with the network model, *i.e.*, cannot be accepted as valid.

It can be noted that reputation systems produce extra communication overhead, and introduce higher delays into the routing process. Therefore, applying plausibility checks is preferable in VANETs since vehicular traffic information, road trajectory, and other related traffic information make it relatively easy to design formal definitions of events for the vehicular network.

4 ACO Rules for MCQ Routing in VANETs

4.1 Multi-Constrained (Optimal) Path Problem

Let $G(V, E)$ be an undirected graph representing a vehicular communication network where V is the set of vehicles and E is the set of links connecting the vehicles. Let m denote the number of QoS constraints L_i where $i = 1, 2, \ldots m$. Each link between two vehicles $l(C_1, C_2) \in E$ is associated m weights corresponding to QoS constraints such that $w_i(C_1, C_2) \geq 0$. The MC(O)P problem is to determine if there is a route P from the source node s to the destination node d such that all the QoS constraints are met as described in the following equation:

$$w_i(P) \leq L_i, \; i = 1, 2, \ldots m \tag{1}$$

If there is more than one route that satisfies the condition in (1), then the MC(O)P problem is to return the route that maximises the objective function $F(P)$ as follows

$$\text{argmax}_{P \in M(s,d)} F(P) \tag{2}$$

where $M(s, d)$ is the set of available routes between s and d and $F(P)$, the objective function, is defined as

$$F(P) = \sum_{i=1}^{m} O_i \left(\frac{L_i}{w_i(P)} \right) \tag{3}$$

where $0 < O_i \leq 1$ are optimisation factors associated with each QoS constraint and depend on the transmitted traffic type. These values are experimental and can be varied by the application during data transmission. For instance, let $L_1 = 100$ *ms* denote the end-to-end delay constraint and $L_2 = 10$ be the hop-count constraint, *i.e.*, the number of QoS constraints $m = 2$. Let $M(s, d) = \{P_1, P_2\}$ where $w_1(P_1) = 77$ *ms*, $w_2(P_1) = 8$, $w_1(P_2) = 89$ *ms*, and $w_2(P_2) = 7$. Here, w_1 represents the weight value of the end-to-end delay measured in [*ms*] and w_2 represents the weight value of the hop-count. If the application intends to transmit voice traffic, then it could determine the optimisation factor for the end-to-end delay constraint $O_1 = 1$ and for the hop-count constraint $O_2 = 0.5$. In this way, the objective function $F(P)$ in (3) favours the route that has the least end-to-end delay value since voice traffic is delay sensitive. According to (3), $F(P) = 1.923$ for P_1 and $F(P) = 1.837$ for P_2, thus P_1 is selected for voice traffic transmission. However, if the application wants to transmit background traffic, then it could determine $O_1 = 0.5$ and $O_2 = 0.8$, *i.e.*, $F(P)$ favours the shortest route with an acceptable end-to-end delay value. In this case, $F(P) = 1.649$ for P_1 and $F(P) = 1.704$ for P_2, thus P_2 is selected for background traffic transmission.

4.2 ACO Rules

In the ACO technique, a number of artificial ants build solutions to an optimisation problem and exchange information on the quality of their solutions via a communication scheme that is reminiscent of the one adopted by real ants [16]. The communication scheme includes the following rules: the state transition rule, the pheromone deposit rule, and the pheromone evaporation rule. Prior to discussing the developed ACO rules, we define the link reliability value between two vehicles. Since the ACO rules are developed to work in a vehicular network environment, it is vital for ants to traverse links that are more reliable than others. In this way, ants avoid traversing vulnerable links that are highly prone to breakage and, consequently, avoid searching near weak solutions.

In [48], we define the link reliability as the probability that a direct communication link between two vehicles C_i and C_j will stay continuously available over a specified time period. In order to calculate the link reliability $r_t(l)$, the vehicles' velocity parameters are utilised. It is assumed that vehicular velocity has a normal distribution [49], [50]. Given T_{ij} for the continuous availability of a specific link $l(C_i, C_j)$ between two vehicles at time t, the link reliability value $r_t(l)$ is defined as follows

$$r_t(l) = \begin{cases} \int_t^{t+T_{ij}} f(T)\,dt & if\ T_{ij} > 0 \\ 0 & otherwise \end{cases} \quad (4)$$

where $f(T)$ denotes the probability density function of the communication duration T and is calculated as follows

$$f(T) = \frac{4H}{\sigma_{\Delta v}\sqrt{2\pi}} \frac{1}{T^2} e^{-\frac{(\frac{2H}{T} - \mu_{\Delta v})^2}{2\sigma_{\Delta v}^2}} \quad for\ T \geq 0 \quad (5)$$

where $\mu_{\Delta v}$ and $\sigma^2_{\Delta v}$ denote the mean and the variance of the relative velocity Δv between two vehicles measured in [m/s], respectively, H denotes the wireless communication range measured in [m], and T_{ij} is calculated as follows

$$T_{ij} = \frac{H - \theta\sqrt{(y_i - y_j)^2 + (x_i - x_j)^2}}{|v_i - \vartheta v_j|} \quad (6)$$

where θ = -1 and ϑ = 1 when C_j overtakes C_i, θ = 1 and ϑ = 1 when C_i moves forward in front of C_j, θ = -1 and ϑ = -1 when C_i and C_j are moving toward each other, and θ = 1 and ϑ = -1 when C_i and C_j are moving away from each other. For any given route $P(s, d)$ between the source s and the destination d, denote the number of its links as Ω: $l_1 = (s, C_1)$, $l_2 = (C_1, C_2) \ldots l_\Omega = (C_\Omega, d)$. For each link l_ω ($\omega = 1, 2 \ldots \Omega$), denote by $r_t(l_\omega)$ the value of its link reliability as calculated using (4). The route reliability for a route P, denoted by $R(P(s, d))$, is defined as follows

$$R(P(s,d)) = \prod_{w=1}^{W} r_t(l_w) \quad where\ \ 0 \leq R(P(s,d)) \leq 1 \quad (7)$$

i.e., the route reliability value is the product of the link reliability values of the links that compose this route.

4.2.1 The State Transition Rule

While searching for feasible routes, ants select their next hop when they arrive at intermediate nodes based on a stochastic mechanism called the state transition rule. Suppose ant A_k arrives at an intermediate node C_i. If the node's pheromone table RT^i does not contain routing information to the destination node d, then ant A_k will be broadcast. Otherwise, A_k selects C_j in RT^i as its next hop toward d according to (8) if $U \leq U_0$ where U is a random number uniformly distributed in [0, 1], and U_0 is a constant number selected between 0 and 1

$$\arg\max_{C_j \in N(s^d)} \{[\tau_{ij}(t)]^\alpha [T_{ij}(t)]^\beta\} \quad (8)$$

where $\tau_{ij}(t)$ is the pheromone level associated with link $l(C_i, C_j)$, α and β are parameters that control the relative importance of the pheromone level versus the predicted link lifetime, and $N(s^d)$ is the set of neighbouring nodes of C_i yet to be visited by A_k over which a route to d is known. Otherwise, if $U > U_0$, then the probability that ant A_k selects C_j as its next hop from C_i toward d is calculated according to (9)

$$p_{ij}^{A_k} = \begin{cases} \frac{[\tau_{ij}(t)]^\alpha [T_{ij}(t)]^\beta}{\sum_{C_\varepsilon \in N(C_i)} [\tau_{ie}(t)]^\alpha [T_{ie}(t)]^\beta} & if\ C_j \in N(C_i) \\ 0 & otherwise \end{cases} \quad (9)$$

where $N(C_i)$ is the set of neighbouring nodes of C_i. The parameters U and U_0 determine the relative importance of exploration versus exploitation in the state transition rule. High values of U_0 mean that A_k prefers transition toward nodes that have larger amount of pheromone and longer link lifetimes according to (8), *i.e.*, exploitation. In this case, the probability of exploring new routes decreases and S-AMCQ algorithm could suffer from stagnation. In contrast, small values of U_0 give A_k the opportunity to explore new links rather than just exploit the pheromone level and follow the trail, *i.e.*, exploration. In the context of VANETs, selecting the value of U_0 depends on the status of vehicular topology and the degree of the environment dynamics. For instance, if the network density is high and the topology is stable, *e.g.*, a highway in rush hour, it is preferable to choose a high value for U_0 since the communication links among vehicles are relatively stable. However, if the performance of S-AMCQ algorithm decreases due to stagnation, then the U_0 value should be decreased to allow ants to explore new routes. We suggest letting the routing algorithm decide and adjust the value of U_0 depending on the vehicular topology dynamics and the performance obtained.

4.2.2 The Pheromone Deposit Rule

Generally, the level of pheromone on a communication link/route between two vehicles reflects the quality of that link/route with respect to the QoS constraints considered. The quality of the communication link depends on the traffic class it is established for, *i.e.*, the level of pheromone depends on the QoS constraints required by that traffic class. Therefore, each ant A_k carries the traffic class identifier (TC_ID) and its corresponding QoS constraints. While moving from node C_i to node C_j, a specific amount of pheromone, denoted by $\tau_{ij}^{A_k}$, is deposited on link $l(C_i, C_j)$ by ant A_k where $\tau_{ij}^{A_k}$ is calculated as follows

$$\tau_{ij}^{A_k}(t) = a(r_t(l)) + b\left(\sum_{i=1}^{n} \frac{L_i}{w_i(l)}\right) \quad (10)$$

where $a > 0$, $b > 0$, and $(a+b) = 1$. L_i denotes a QoS constraint, and $r_t(l)$ denotes the reliability value of link l. It can be noted that the relative importance of the link reliability is expressed in (10) and gives weight to the pheromone value because ants should traverse through more reliable links. In this way, the pheromone level of the link l is determined considering its QoS metrics and its reliability value. We worked out this function by experimentation and its validity is illustrated by simulation results in section 7.

4.2.3 The Pheromone Evaporation Rule

S-AMCQ routing algorithm offers a mechanism to process the evaporation of the pheromone trails left on the traversed links. The pheromone evaporation process is extremely important to avoid rapid convergence toward a suboptimal search space, and to explore new routes. In this way, the pheromone evaporation process minimises the influence of past routes and helps avoid the stagnation problem. However, unlike conventional ACO algorithms, here the evaporation process is kept separate from the pheromone deposit process. Moreover, the evapora-

tion rate is not constant but a variable value for each link depending on its status. The reasons behind these adjustments are linked to the fact that these ACO rules are proposed to perform a route discovery process in a highly dynamic network, *i.e.*, a VANET. Considering the highly dynamic nature of VANETs, the pheromone level on a communication link should have completely evaporated by the end of its expected lifetime. In this way, the next generation of ants avoids using this link, which is assumed to be unavailable. According to the link reliability definition, the expected link lifetime T_{ij}^{e} for a link $l(C_i, C_j)$ can be calculated as follows

$$T_{ij}^{e} = r_t(l)T_{ij} \tag{11}$$

Every t^{ex} seconds, each node decreases the pheromone level of all its links using the following formula

$$t_{ij}(t+t^{ex}) = (1-r)t_{ij}(t) \tag{12}$$

after η times of applying (12), where ρ is the evaporation rate $0 < \rho < 1$, assuming the initial pheromone level is τ_0 for each link where $\tau_0 > 0$, (12) can be written as follows

$$t_0 \gg (1-r)^h t_{ij} \qquad where\ h = \frac{T_{ij}^{e}}{t^{ex}} \tag{13}$$

Thus, the evaporation rate ρ can be calculated as follows

$$r = 1 - \sqrt[h]{\frac{t_0}{t_{ij}}} \tag{14}$$

5 The Extended VANET-oriented Evolving Graph (E-VoEG) Model

The evolving graph theory has been proposed as a formal abstraction of dynamic networks to help capture its behaviour when the mobility patterns are predictable [51], [52], [53]. In definition, the evolving graph is an indexed sequence of λ subgraphs of a given graph, where the subgraph at a given index corresponds to the network connectivity at the time interval indicated by the index number. Since the current evolving graph theory cannot be applied directly to VANETs, we extended the current evolving graph model in [18] to address the evolving properties of the VANET communication graph and consider only the reliability of communication links among vehicles. The extended version of the evolving graph model, called the VANET-oriented Evolving Graph (VoEG), is evolving based on the predicted dynamic patterns of vehicular traffic. In this paper, we extend the VoEG model to consider the QoS of communication links among vehicles with respect to the QoS requirements of a specific data type. Besides, we propose construction and maintenance mechanisms to securely build and maintain the E-VoEG model.

Fig. 1 illustrates an example of the E-VoEG model on a highway at t = 5s. Each node in Fig. 1 represents a vehicle on the highway. We associate the following 3-tuple (t, *TC_ID*, $\tau_t(l)$) with each edge (link), where t denotes the current time, *TC_ID* denotes the traffic class identifier this link is established for, and $\tau_t(l)$ denotes the pheromone value associated with l at time t according to the QoS constraints required by *TC_ID* as calculated in (10).

In the E-VoEG model, the communication link between two vehicles is not available if its pheromone value $\tau_t(l)$ equals 0. The pheromone value is set to 0 when the link l between two vehicles violates any of the QoS constraints required by the data traffic type, or its pheromone evaporates and falls below τ_0, *i.e.*, the link is not feasible anymore. Fig. 1 shows the E-VoEG status and the pheromone values associated with each link for *TC_ID* = 1. It can be noticed that links {*B, E*} and {*F, G*} are not eligible to be traversed since $\tau_5(\{B, E\}) = \tau_5(\{F, G\}) = 0$. Other links such as {*A, C*} are eligible to be traversed. It is worth noting that even if the link l is eligible to be traversed, it does not necessarily mean that it will be chosen to be part of the optimal route. The pheromone values, which are associated with each link, are not constant and change in accordance with the dynamics of the vehicular network topology.

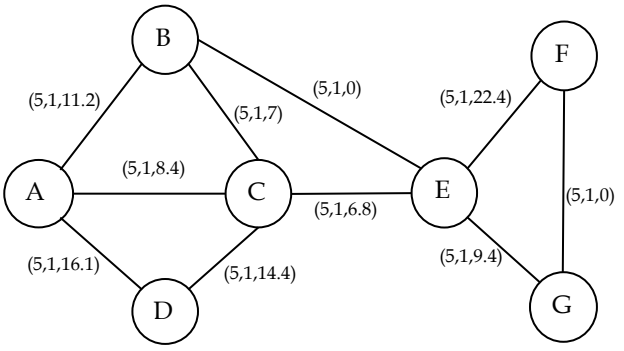

Fig. 1. The Proposed E-VoEG Model at t = 5s where *TC_ID* = 1

5.1 Construction and Maintenance Processes of the E-VoEG Model

As mentioned earlier, it is relatively easier in VANETs to build a formal model of the network topology than in other types of mobile ad hoc networks. The reason is the availability of additional information that can be useful to build and integrate a dynamic model of the VANET communication graph at each vehicle in the network. We assume that each vehicle can build and maintain an E-VoEG model of the current vehicular network status. We start with the construction process where the broadcasted BSMs are utilised. Each vehicle that receives a BSM uses its information, which is assumed to be correct and authentic due to the fact that they are protected using the PASS scheme, to construct its E-VoEG model and define its links. Each link in the constructed E-VoEG model is assigned with T_{ij}, the predicted link lifetime as calculated in (6). At this stage, no pheromone values are associated with the existed links since no route discovery process is in progress. Once the vehicle receives routing control messages, it uses the received information to assign a pheromone value to each link in the constructed E-VoEG according to the QoS requirements of *TC_ID*. In this way, each vehicle could associate different pheromone values with the same link depending on its quality with respect to a specific traffic class. It is worth noting that the E-VoEG model within each vehicle represents the local vehicular network topology that surrounds it. This is due to the fact that BSMs cannot traverse the whole network

topology as they are dropped after a specific number of hops, *e.g.*, 30 hops.

With regard to the maintenance process, each vehicle can keep an accurate state of the current E-VoEG model using the information of the received BSMs and authenticated routing control messages, and the predicted dynamic patterns of vehicular traffic. The reason that the E-VoEG maintenance process still needs to predict the mobility patterns of its nodes, *i.e.*, vehicles, is that the successful reception probability of BSMs is lower than the necessary threshold [55]. Therefore, the successfully received BSMs can be used to tune the current E-VoEG status. It is important to note that within a specific threshold, the received information at time t on location, velocity, direction, *etc.* of neighbouring vehicles should be consistent between BSMs and the predicted mobility patterns. Inconsistent received information is either suspicious, *i.e.*, BSMs are cracked, or the information used to build the original E-VoEG model is incorrect. Either way, the E-VoEG model is reinitialised, and a report on this situation is sent back to the source node when a route discovery is in progress.

6 Secure Ant-based Multi-Constrained QoS Routing Algorithm (S-AMCQ)

6.1 Routing Control Ants

The routing control ants are responsible for traversing the vehicular network to compute feasible routes from the source to the destination vehicles. The movements of these ants are restricted by the state transition rule defined in (8) and (9) when sufficient information is available at the pheromone tables, or they will be broadcast. We propose three types of routing control ants: the routing request ant (RQANT), the routing reply ant (RPANT), and the routing error ant (REANT). For each field in the proposed routing control ants, we describe its nature, *i.e.*, immutable, mutable and traceable, and mutable but untraceable, and its data type, *i.e.*, integer, double, *etc.* to estimate its size later. This description is important for explaining the secure route discovery process later.

6.1.1 Routing Request Ant (RQANT)

In addition to the default fields of conventional routing request messages such as the destination address, originator address, *etc.*, which are immutable, the following fields are added to a RQANT

1. *RQANT_ID* (*u_int8_t*) contains the ant's ID, which is immutable.
2. *RQANT_Gen* (*u_int8_t*) indicates the current ant generation, which is immutable. Different ant generations could be involved in the route discovery process of the same destination. This field plays an essential role in decreasing the proliferation of ants. When a node receives another ant from the same generation looking for the same destination, it may only be processed if it presents a better route than the existing one. Otherwise, it is discarded.
3. *RQANT_TC* (*u_int8_t*) contains the traffic class identifier *TC_ID* the current route discovery process is issued for, which is immutable. This field is important to distinguish different QoS requirements while searching for feasible routes for different traffic types.
4. *TimeStamp* (*double*) contains the time when the RQANT is generated, which is immutable.
5. *TraversedList* (*double*) contains the list of vehicles the RQANT has traversed. The first node in this list is the source node while the last one is the node that processes and forwards the RQANT. This field is mutable and traceable.
6. *QoS_Metrics* (*double*) contains the reliability and the weight value of each QoS constraint of the route that the RQANT has travelled so far. This field is mutable and traceable.
7. *QoS_Constraints* (*double*) contains the QoS constraints that should be satisfied according to the traffic class found in the *RQANT_TC* field, which is immutable. These QoS constraints are necessary to calculate the pheromone value of the traversed link/route.

6.1.2 Routing Reply Ant (RPANT)

The RPANT is designed to set up forward routes to the destination node considering the quality of the links it has traversed. The RPANT message includes the following fields

1. *RPANT_ID* (*u_int8_t*) contains the ant's ID, which is immutable. Each RPANT travels back to the source node following the pheromone trail left by the RQANT that generated it during the route discovery process.
2. *RPANT_Gen* (*u_int8_t*) indicates the current ant generation, which matches that given in the *RQANT_Gen* field of the RQANT, which generated it. This field is immutable.
3. *RPANT_TC* (*u_int8_t*) contains the traffic type the current route discovery process is issued for, which is immutable. Its contents match those of the *RQANT_TC* field of the RQANT, which generated it.
4. *TraversedList* (*double*) contains the list of vehicles the RPANT should traverse to reach the source node. This field is set by the destination node and is immutable.
5. *QoS_Constraints* (*double*) contains the QoS constraints that should be satisfied according to the traffic class found in the *RPANT_TC* field, which is immutable.

6.1.3 Routing Error Ant (REANT)

The REANT is designed to announce a link breakage when it occurs. The REANT message includes the following fields

1. *REANT_ID* (*u_int8_t*) contains the ant's ID, which is immutable. REANTs traverse back to the preceding vehicles along a route to a vehicle that became unavailable due to a link breakage.
2. *REANT_UDEST* (*IP_Address*) contains a list of ad-

dresses of the destination vehicle(s) that become unreachable due to the occurred link breakage, which is immutable. IP_Address is a 32*bit* data type for IPv4 addresses.

6.2 The Pheromone Table

Pheromone tables RT^i at each node contain the information needed to route data packets and routing control ants through the vehicular network efficiently. In addition to the conventional information such as source address, destination address, next hop, *etc.*, each entry in RT^i contains the following information

1. *TC_TYPE* contains the traffic type this entry is created for. In this way, pheromone tables could have different routes to the same destination, each associated with a specific traffic type.
2. *QoS_Metrics* contains the reliability and the weight value of each QoS constraint associated with this entry.
3. *rt_pherm* contains the pheromone level associated with this entry calculated according to the QoS constraints defined by the data traffic type.
4. *rt_evp* contains the evaporation rate of this entry. Each node uses this field to ensure the pheromone table entry evaporates at the end of its expected lifetime as explained in (12), (13) and (14).

6.3 Route Discovery Process in S-AMCQ Routing Algorithm

In this section, we describe the route discovery process in S-AMCQ routing algorithm. It can be noticed from the design of routing control ants that they do not carry the pheromone value, which is used by intermediate nodes to update their routing tables. As described earlier, the pheromone value is calculated using the information carried by the routing control ants. This is a main design advantage of S-AMCQ routing algorithm because all we need to do is to ensure that the necessary information to calculate the pheromone value is authentic, *i.e.*, created or updated by authenticated vehicles. As the plausibility checks in the next section are dedicated to defending the route discovery process against internal adversaries, we suggest using the digital signature mechanism to protect the routing control ants from external adversaries, and ensure their integrity and authenticity. The digital signature mechanism is applied to all control messages in S-AMCQ. In the following, we illustrate the route discovery process in S-AMCQ routing algorithm when plausibility checks are applied, and the digital signature mechanism from the PASS scheme is utilised.

When the source node s has data that belongs to a specific traffic class, *TC_ID*, to send, it commences a new route discovery process if no route to the destination node d associated with *TC_ID* is known. It starts by initialising the immutable fields of a RQANT and leaves the *QoS_Metrics* and *TraversedList* fields empty. After that, it uses the one-way hash function *Hash*(.) to hash all the immutable fields and produce the message digest $RQANT_m$. Then, s uses $SK_{s,j}$ the secret signing key of s for the current timeslot TS_j associated with its pseudonymous certificate $Cert_{CA,s,j}$ to sign $RQANT_m$,*i.e.*, obtains the signature $DSig_{s,RQANTm} = Sign(SK_{s,j}, RQANT_m)$. Finally, s attaches its signature to the RQANT message, and broadcasts it to its neighbours. It can be noted that the used certificate, $Cert_{CA,s,j}$, is issued directly by the CA. However, for future route discovery processes, after s has obtained an updated certificate from an authenticated RSU_x, the used certificate will be $Cert_{RSUx,s,j}$. In both cases, either s utilised $Cert_{CA,s,j}$ or $Cert_{RSUx,s,j}$, its certificate is not attached to the RQANT message because it is distributed and verified by its neighbouring vehicles during the transmission of BSMs. We assumed that BSMs are protected using the PASS scheme therefore there is no need to send the certificate again. In this way, we reduce the verification overhead at the neighbouring vehicles when they receive this RQANT, to signature verification only, and reduce the communication overhead by not transmitting the source's certificate. It is important to notice that this solution is feasible within the certificate validity period, *i.e.*, before the vehicle changes its certificate to a new one. Hence, s and other nodes should always ensure that the current utilised certificate is distributed during the transmission of BSMs.

When an intermediate node C_v receives the control message (RQANT, $DSig_{s,RQANTm}$) from s, it verifies the signature $DSig_{s,RQANTm}$ by computing the hash value over the RQANT message's immutable fields, and verifies the resulting $RQANT_m$ against the signed value attached to the RQANT. If $Verify(PK_{s,j}, RQANT_m, DSig_{s,RQANTm})$ is successful, where $PK_{s,j}$ is the public key of s for the timeslot TS_j, then the RQANT message is accepted, and the plausibility checks are performed at this stage. If the RQANT fails any of the plausibility checks, then it is discarded and the sender vehicle is reported as malicious. If the plausibility checks were successful, C_v checks if this RQANT has been processed before, *i.e.*, with the same *RQANT_ID* and *RQANT_Gen* information. If yes, then it is discarded; otherwise, C_v calculates the QoS metrics and the reliability value of the link $l(C_v, s)$. If $l(C_v, s)$ violates any of the QoS constraints determined by the data traffic class *TC_ID*, then this RQANT is discarded, and the pheromone value of $l(C_v, s)$ is set to 0. Otherwise, C_v continues by either inserting a new, or updating an existing pheromone table entry to the node it receives the RQANT from, in this case s, depending on the pheromone value calculated according to the QoS metrics and constraints determined by *TC_ID*. After that, C_v updates the mutable information of the RQANT message as follows. It inserts the new calculated QoS metrics and reliability value into *QoS_Metrics* field, and inserts its identifier into the *TraversedList* field. After that, it signs the updated RQANT message fields only, *i.e.*, *QoS_Metrics* and *TraversedList* fields, using the same mechanism described above, and attaches its signature $DSig_{Cv,RQANTm}$ along with $DSig_{s,RQANTm}$ to RQANT. In this way, each RQANT after this stage will contain two signatures, the source node's one on the immutable fields and the signature of the last node that processed this RQANT on the mutable fields. The second signature should be verified by using the identifier of the last node in *TraversedList* field to identify the public key to be used.

Finally, C_v checks its pheromone table for route entries to d. If an entry is found, the RQANT is forwarded based on the transition rule defined in (8) and (9), else it is broadcasted again. If any of the mentioned security information verifications fail, then the RQANT is discarded.

For each intermediate node that receives this RQANT message later, it verifies the two included signatures, and ensures that the node it receives this RQANT from is the last one in the *TraversedList* field. After that, it processes the RQANT as described above. The process continues until the destination node d is reached. On receipt of a valid RQANT, d generates a RPANT and sends it back to s following the route found in the *TraversedList* field, *i.e.*, following the trail of the received RQANT to arrive at s. The RPANT is protected using the signature of d only since all its fields are immutable. At each intermediate node, when the RPANT is received, the signature of d is verified, and the QoS metrics of the forward link/route toward d are evaluated based on the QoS constraints, *TC_ID*, and the E-VoEG model information. It is important to note that, in S-AMCQ, d is allowed to process multiple RQANTs and send a RPANT for each if its discovered route satisfies the QoS requirements.

Finally, s evaluates the computed routes $M(s, d) = \{P_1, P_2 \ldots P_z\}$, and selects the route that maximises the objective function $F(P)$ value defined in (3). The source node is allowed to start data transmission once it receives the first RPANT with a feasible route. If a better route becomes available upon receipt of another RPANT, then s will choose the optimal route according to (2), and so on. In both cases, all feasible routes, *i.e.*, $M(s, d)$, are kept at s for further use if needed as explained later in the route maintenance process. This is done to avoid the delay that would occur if s waited until two or more RPANTs had arrived before transmitting data.

Using the method described above, S-AMCQ ensures the authentication, integrity, and non-repudiation of the information within its control messages while protecting vehicles privacy using pseudonymous certificates. External adversaries cannot carry out route disruption, or perform creation of incorrect routing state attacks because any spoofed control message is going to be detected. However, the adversary can still create spoofed control ants and send them to one or more vehicles for verification. Although a spoofed control ant will be discarded, the verification process consumes time and may jeopardise the availability of the target vehicle(s). In case the adversary unicast the spoofed control ants, the denial of service at the target vehicle does not affect the ability of S-AMCQ to discover feasible routes that do not include the target vehicle. The reason is that S-AMCQ is originally a multipath routing algorithm. However, if the spoofed control ants are broadcast, then blocking the sender of these ants when possible can mitigate this attack.

6.4 Plausibility Checks for S-AMCQ Routing Algorithm

As the proposed mechanism described in the previous section cannot protect the routing process from internal adversaries, we suggest putting plausibility checks in place. In the following, we focus our discussion on protecting mutable information within the routing control ants based on the E-VoEG model and the properties of S-AMCQ routing algorithm.

6.4.1 QoS Metrics Check

When an intermediate node authenticates a received routing control ant from another node, it verifies the QoS metrics and reliability value it contains against those that are calculated in the E-VoEG model. As mentioned earlier, the kinematic information is primarily utilised to evaluate the link/route reliability between two vehicles. Besides that, other information such as the hop-count, when the route cost is a required constraint, is used to evaluate the QoS metrics of each link/route with respect to the required QoS constraints. Since the E-VoEG model is built and maintained using the BSMs information, the QoS metrics of its links can be calculated and updated according to the dynamics of the vehicular network topology. For instance, assume there is an internal adversary who does not perform the calculations needed to estimate the route reliability value or the route cost intentionally, *e.g.*, multiplies the reliability value by 1 or 0 instead of applying (7), or decreases the hop-count value to shorten the traversed route so the compromised node can be included in the optimal route. In this case, this falsified information can be detected using the E-VoEG model because the travelled route is found in the *TraversedList* field. Since the last node that processed the received RQANT signs this field, we ensure that no external adversary has changed its contents. Moreover, we also ensure that *TC_ID* and the QoS constraints are authenticated because they are signed by s. In this way, the last node that processed this RQANT can be reported as a malicious node, *i.e.*, an internal adversary. If a node is reported as malicious, ants should avoid traversing through this node. Moreover, any routing control ant that is received from this node is discarded immediately. It is worth noting that the estimated QoS metrics are compared with those found in *QoS_Metrics* field within a specific threshold as the E-VoEG model is based on information received from BSMs and predicted mobility patterns.

Despite the applied digital signatures and the plausibility check we mentioned above, the internal adversary is still able to mount the following attack. The adversary can modify the *TraversedList* field by either adding or removing nodes. After that, it calculates the QoS metrics with respect to the modified *TraversedList* because it has access to the E-VoEG model. This modification cannot be detected because all fields and information verify correctly. However, there is no actual gain from this attack for the following reasons. Firstly, if the adversary adds more nodes to *TraversedList* trying to prevent a specific route from being selected, the route discovery process can discover this route using other nodes since the S-AMCQ is a multipath routing algorithm. Secondly, if the adversary removes nodes to make the current route look shorter and has better QoS metrics, then it still has to do that with respect to the E-VoEG model, *e.g.*, it cannot claim to be connected to a node that is outside of its communication

range. Therefore, this modification can be detected at *s* when the received routes are evaluated. Here, we have assumed that there is only one internal adversary.

6.4.2 Control Messages Broadcast Check

According to the state transition rule in (8) and (9), RQANTs are broadcasted by *s* at the beginning of a route discovery process, and by intermediate nodes when no valid route toward the destination *d* is known. Therefore, RPANTs and REANTs cannot be broadcast at any stage. If any node receives one of these control messages as a broadcast message, then it should discard it immediately without performing any verification process. Thus, this plausibility check is performed before the verification process, which saves time and resources. In regard to RQANTs, if an intermediate node keeps receiving broadcast RQANTs from a specific node even though, according to its E-VoEG model, it does have a route to *d*, then it is reported as a malicious node. This plausibility check depends on the fact that the broadcasting of control ants in S-AMCQ is limited and it stops when the intermediate node has a route to *d*, *i.e.*, rebroadcasting is not inevitable.

6.4.3 Link Breakage Check

This plausibility check is designed to detect malicious routing error messages, *i.e.*, REANTs. The E-VoEG model is utilised to perform this check. There is a possibility that an internal adversary sends a REANT to invalidate a valid link/route between two nodes. This attack would be mounted to degrade the QoS of the network and divert the established route through specific vehicles that might have been compromised by the attacker. The consistency of the error message is checked against the current status of the vehicular network, *i.e.*, the E-VoEG model. The link that is claimed by the received REANT to be broken is verified against the E-VoEG model to ensure its pheromone value can really have evaporated at this stage, or the vehicular network topology has changed suddenly so the link breakage occurs. If the REANT is not in conformity with the E-VoEG's status, then it is discarded and the sender of that REANT is reported as a malicious node.

6.5 Route Maintenance Process in S-AMCQ Routing Algorithm

When an unpredicted link breakage occurs, it is reported back to *s* either to start a new route discovery process, or switch to another feasible route in $M(s, d)$. The plausibility check on link breakage is applied to ensure the received REANT is legitimate. If the REANT is legitimate and $M(s, d)$ is empty, *s* starts a new route discovery process. Otherwise, switching to another feasible route is commenced. Prior to making the switch, *s* should ensure this available feasible route still satisfies the QoS requirements. This task is accomplished using the E-VoEG model information at *s*. After that, *s* can select the evaluated route as a new best route because it still satisfies the QoS constraints, or *s* starts a new route discovery process. It is worth noting that we limit S-AMCQ to list two routes only at each node to the same destination to avoid the complexity of listing every route in the network.

7 Performance Evaluation of S-AMCQ Routing Algorithm

The main objective of the following performance evaluation is to investigate how the time overhead needed to sign, transmit, and verify the routing control ants can affect the performance of S-AMCQ routing algorithm. Besides, we want to investigate the effectiveness of S-AMCQ in computing feasible routes subject to multiple QoS constraints in VANETs. As the implementation of the PASS scheme is not available to us, we discuss the delays caused by the authentication process numerically, and insert the resulting numbers into the S-AMCQ implementation for the simulation experiment later.

7.1 Implementation Details and Numerical Results

In this section, the authentication overhead of PASS scheme in terms of signing, verifying, and transmitting delays of a routing control ant is discussed. The overhead of certificate revocation, certificate updating, and storage of pseudonymous certificates and signing keys are not considered in our discussion because they are not directly related to the routing algorithm. We assumed that the overhead of certificate management operations is already taken care of during the transmission of BSMs thus it is not required solely to secure the routing process. Let T_{pto} denote the processing time overhead needed to secure and verify a routing control ant, *e.g.*, RQANT. T_{pto} is calculated as follows

$$T_{pto} = T_{sign} + T_{comm} + T_{ver} \tag{15}$$

where T_{sign} is the processing time needed to sign the RQANT, T_{comm} is the time needed to transmit the signed message $\{RQANT, DSig_{s,RQANTm}, DSig_{Cv,RQANTm}\}$, which includes two digital signatures of *s* and C_v, and T_{ver} is the processing time needed to verify the signed RQANT. Based on the structure of each type of routing control ant we proposed in section 6.1, the size of each type can be estimated as follows: RQANT = 71 *bytes* and RPANT = 31 *bytes* where we assumed the number of QoS constraints m = 2 and *double* data is 4 *bytes* while *u_int8_t* data is 1 *byte*. Considering the largest control message, which is a RQANT, the Schnorr signature size is 42 *bytes* thus the resulting total message size is 71+42+42 = 155 *bytes* including the original message and the digital signatures of the source node and the last node C_v that transmitted it. It can be noted that the resulting message size is approximately twice that of the original message. Suppose the data transmission rate is 12 *Mbps*, the resulting message, which is 155 *bytes*, needs approximately T_{comm} = 0.103 *ms* to be transmitted to the next hop while the original message, which is 71 *bytes*, needs approximately 0.047 *ms*, *i.e.*, 0.056 *ms* is the communication time overhead required to transmit the security information.

The time needed to sign a *RQANT* message using the Schnorr signature algorithm is estimated to 0.6 *ms* where vehicles are assumed to be equipped with an Intel Pentium-4 3.0 *GHz* machine [20]. This overhead is acceptable and does not affect the accuracy of the control message's contents, *e.g.*, *QoS_Metrics*. Let us consider the following scenario where the observed vehicle moves on the high-

speed lane of a highway at 80 *km/h*, *i.e.*, 22.22 *m/s* on average. After generating the routing control ant, the signing operation takes about 0.6 *ms*, during this time the vehicle could change its location at most 13.33 *mm*, which does not affect the accuracy of the calculated QoS metrics or the reliability value. Finally, we estimate the verification overhead T_{ver} of the signed *RQANT* message, which includes the time needed to verify two digital signatures. In the PASS scheme, the time needed to verify the digital signature is 1.2 *ms*. Therefore, the resulting total overhead T_{pto} of RQANT in (15) is approximately 3.103 *ms* including T_{comm} = 0.103 *ms*, T_{sign} = 0.6 *ms*, and $2T_{ver}$ = 2.4 *ms*.

7.2 Simulation Setup – Voice Traffic Transmission

We choose voice traffic transmission to evaluate the performance of S-AMCQ routing algorithm because voice traffic is delay sensitive. A simple simulation scenario is constructed where a VoIP source vehicle generates a voice traffic stream and sends it over VANET to a VoIP receiver vehicle. The VoIP sender is a constant bitrate (CBR) source that alternates between talk state, where it acts as a CBR source and sends packets of size *talkPacketSize* every *packetizationInterval* seconds to the VoIP receiver over UDP, and state silence where no packets are sent.

The simulations are conducted using the *OMNet++* 4.3 network simulator [56] where 20 runs of each simulation experiment is performed, the average of the runs is obtained, and 95% confidence intervals are computed to indicate the statistical significance of the simulation results. The simulations were run on a three lanes 10 *km* highway traffic scenario where the number of vehicles is varied from 15 to 75 vehicles. We utilised the highway mobility model developed in [48], which is built based on traffic theory rules, and considers the drivers' behaviour. The average velocity of the vehicles in each lane is 40 *km/h*, 60 *km/h*, and 80 *km/h*, respectively. For each simulation run, two vehicles are chosen randomly as the observed vehicles, *i.e.*, source/destination pair. The IAQR, S-AMCQ and AMCQ routing algorithms are evaluated in the simulation experiment where AMCQ means that no security mechanisms are applied. The QoS constraints m = 2 where L_1 = 100 *ms* for the delay constraint and L_2 = 10 *hops* for the route cost constraint. The VoIP application sets the optimisation factors O_1 = 1 for the delay constraint and O_2 = 0.5 for the route cost constraint, and *talkPacketSize* = 40 *bytes* and *packetizationInterval* = 20 *ms*. The time needed to perform the plausibility checks using the E-VoEG model is neglected. For the ACO rules, $a = \beta = 0.5$, $\tau_0 = 5$, $U_0 = 0.6$, $a = 0.6$, and $b = 0.4$.

7.3 Performance Metrics

The following four performance metrics are considered in this simulation experiment

1. Average packet delivery ratio (PDR): represents the average ratio of the number of successfully received data packets at the destination node to the number of data packets sent.
2. Average time for route discovery: represents the time needed to perform the route discovery process, *i.e.*, the time interval between sending a RQANT from s and receiving the first RPANT from d.
3. Mean Opinion Score [57] (MOS): MOS is a value between 1 and 5 that indicates a human user's view of the voice quality, where 1 means a bad quality, *i.e.*, very annoying, and 5 means excellent quality, *i.e.*, imperceptible quality impairment.
4. Playout Loss rate: indicates the ratio of received late packets that miss their playout time to total packets received. Late packets are dropped.

7.4 Simulation Results

Fig. 2 shows the average packet delivery ratio achieved by each routing algorithm for the voice traffic. It can be noticed that the proposed S-AMCQ routing algorithm achieves higher packet delivery ratio than IAQR but less than AMCQ. Since the voice packets are small, only 40 *bytes*, and voice traffic is reliability tolerant but delay intolerant, the average delivery ratio increases when the network density increases because more options are available to compute feasible routes to the destination. However, the high packet delivery ratio does not mean the received voice traffic has high quality as described later in MOS and playout loss rate figures. Besides, the enhancement in PDR varies among the examined routing algorithms. Since the ACO rules are designed with vehicular network topology dynamics in mind, ants are able to select and maintain feasible routes through dynamic calculations of pheromone improvement and evaporation parameters. Using constant parameters as in IAQR does not allow the routing algorithm to benefit from knowledge of network changes, *i.e.*, the network density. With regard to S-AMCQ, higher network density usually results in longer routes between the source and the destination vehicles, and the security overhead causes lower PDR in comparison to AMCQ.

Fig. 3 shows how fast each routing algorithm can converge and start data transmission, *i.e.*, perform one route discovery process and compute a feasible route. The AMCQ and S-AMCQ routing algorithms are faster than IAQR in identifying feasible routes that satisfy the QoS constraints. This is due to the fact that the ACO rules are designed to consider the reliability of the traversed links. However, it can be seen that the security mechanisms overhead in S-AMCQ delays the route discovery process especially when the network density increases, which affects its PDR as showed in Fig. 2. Voice packets are transmitted with the added delay of the signing and verifying processes that have taken place in S-AMCQ route discovery process. In the worst case, when the network density reaches 75 vehicles, the time overhead of the route discovery process in S-AMCQ is approximately 182 *ms*. Suppose the source and the destination vehicles are moving in opposite directions at the highest velocities allowed on the highway, *i.e.*, 80 *km/h* on average. After 182 *ms*, both vehicles will have moved about 4.04 *m* away from each other, *i.e.*, about 8.08 *m* in total. This number represents the distance difference that occurs because of the delay of S-AMCQ route discovery process. If the vehi-

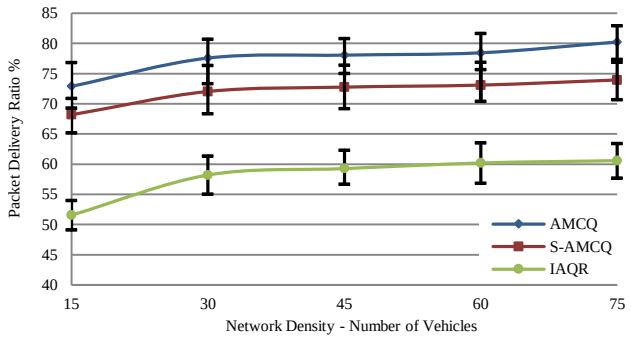

Fig. 2. Average Packet Delivery Ratio

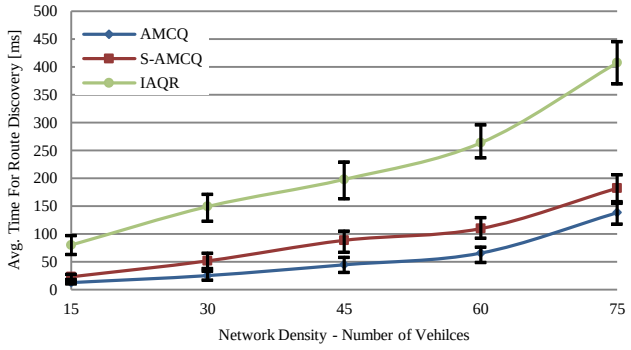

Fig. 3. Average Time for Route Discovery

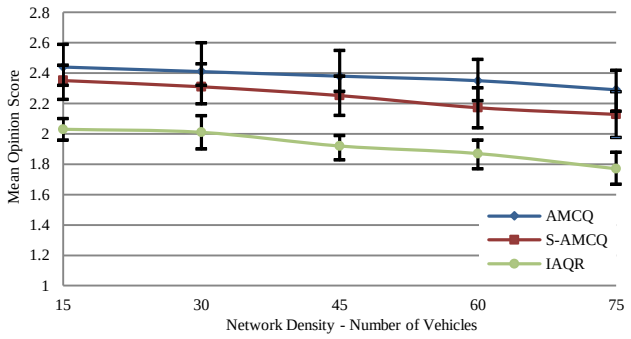

Fig. 4. Mean Opinion Score

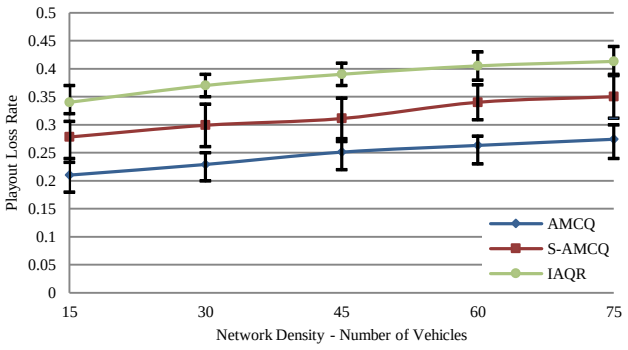

Fig. 5. Playout Loss Rate

cles are at the edge of their communication ranges, then the route is not going to be discovered, or it is going to disconnect before the beginning of data transmission. However, since different feasible routes are computed, this is not going to significantly affect the performance of S-AMCQ routing algorithm as shown above in Fig. 2.

It can be noticed in Fig. 4 that MOS reduces for all routing algorithms when the number of vehicles increases. This reduction comes from the fact that the feasible route connecting the source and the destination vehicles might be longer now, *i.e.*, the number of hops could be higher when more vehicles are available in the network. The increased number of hops of the selected route affects the quality of the transmitted voice, and decreases its MOS value. However, the decrease in the MOS of IAQR is more rapid than that in the MOS of AMCQ and S-AMCQ routing algorithms. From this figure we can conclude that the security overhead may affect the delivered voice quality by approximately 0.16 in comparison to AMCQ. The delivered voice quality is between poor and fair in S-AMCQ routing algorithm, *i.e.*, its MOS value is between 2.12 and 2.35.

Finally, Fig. 5 shows that the Playout loss rate of each routing algorithm is linked with Fig. 4, which shows their MOSs. When the Playout loss rate increases, *i.e.*, more voice packets are arriving late and missing their playout time, the MOS decreases. The reason behind the good MOS achieved by AMCQ and S-AMCQ is the lower Playout loss rate it exhibits in this figure. This means that S-AMCQ has a higher success rate than IAQR in identifying feasible routes that deliver voice packets on time to the destination, even when the security mechanisms are applied. However, its Playout loss rate is higher than that of AMCQ because data packets could arrive late at the destination vehicle because of the security mechanisms overhead. As a result, some data packets might be discarded as they miss their playout time.

8 Conclusion

In this paper, we utilise the ACO rules to propose a secure ACO-based MCQ (S-AMCQ) routing algorithm for VANETs. The ACO rules are designed to consider the dynamics of the vehicular network topology. Moreover, we design the routing control ants to be easily secured using conventional security mechanisms such as digital signatures. To defend against internal adversaries, we developed plausibility checks for the S-AMCQ routing algorithm based on its design and an extended VANET-oriented Evolving Graph (E-VoEG) model. Simulation results demonstrate that the security overhead of S-AMCQ routing algorithm slightly affects its performance. However, S-AMCQ can still guarantee significant performance in terms of identifying feasible routes, and delivering data packets in accordance with the required QoS constraints as shown for voice packets.

References

[1] A. Vinel, "Performance Aspects of Vehicular Ad-hoc Networks: Current Research and Possible Trends," *Proc. GI/ITG-Workshop MMBnet, Hamburg, Germany, Sep.* 2009.

[2] R. Yu, Y. Zhang, S. Gjessing, W. Xia, and K. Yang, "Toward Cloud-Based Vehicular Networks with Efficient Resource Management," *IEEE Network Magazine*, vol. 27, no. 5, pp. 48-54, Sep/Oct 2013, doi: 10.1109/MNET.2013.6616115.

[3] K. Yang, S. Ou, H. Chen, and J. He, "A Multihop Peer-Communication

Protocol with Fairness Guarantee for IEEE 802.16-Based Vehicular Networks," *IEEE Trans. Vehicular Technology*, vol. 56, no. 6, pp. 3358–3370, Nov 2007, doi: 10.1109/TVT.2007.906875.

[4] Z. Wang, and J. Crowcroft, "Quality-of-Service Routing for Supporting Multimedia Applications," *IEEE J. Selected Areas in Comm.*, vol. 14, no. 7, pp. 1228-1234, Sep 1996, doi: 10.1109/49.536364.

[5] D.S. Reeves, and H.F. Salama, "A Distributed Algorithm for Delay-Constrained Unicast Routing," *IEEE/ACM Trans. Networking*, vol. 8, no. 2, pp. 239-250, Apr 2000, doi: 10.1109/90.842145.

[6] M. Curado, and E. Monteiro, "A Survey of QoS Routing Algorithms, " *Proc. International Conf. on Information Technology (ICIT 2004)*, Istanbul, Turkey, pp. 43-46, 2004.

[7] Y. Bejerano, Y. Breitbart, A. Orda, R. Rastogi, and A. Sprintson, "Algorithms for Computing QoS Paths with Restoration," *IEEE/ACM Trans. Networking*, vol. 13, no. 3, pp. 648-661, June 2005, doi: 10.1109/TNET.2005.850217.

[8] B. Zhang, J. Hao, and H.T. Mouftah, "Bidirectional Multi-Constrained Routing Algorithms," *IEEE Trans. Computers*, Mar 2013, doi: 10.1109/TC.2013.54.

[9] F. Kuipers, P. Van Mieghem, T. Korkmaz, and M. Krunz, "An Overview of Constraint-Based Path Selection Algorithms for QoS Routing," *IEEE Comm. Magazine*, vol. 40, no. 12, pp. 50-55, Dec 2002, doi: 10.1109/MCOM.2002.1106159

[10] P. Van Mieghem, H.D. Neve, and F.A. Kuipers "Hop-by-Hop Quality Of Service Routing," *Computer Networks*, vol. 37, no. 3-4, pp. 407- 423, Nov 2001, doi: 10.1016/S1389-1286(01)00222-5.

[11] G. Liu, and K.G. Ramakrishnan, "A*Prune: An Algorithm for Finding K Shortest Paths Subject to Multiple Constraints," *Proc. IEEE Twentieth Ann. Joint Conf. IEEE Computer and Communications Societies* (*INFOCOM 2001*), Anchorage, AK, vol. 2, pp. 743-749, 2001, doi: 10.1109/INFCOM.2001.916263

[12] T. Korkmaz, and M. Krunz "Multi-Constrained Optimal Path Selection," *Proc. IEEE Twentieth Ann. Joint Conf. IEEE Computer and Communications Societies* (*INFOCOM 2001*), Anchorage, AK, vol. 2, pp. 834-843, 2001, doi: 10.1109/INFCOM.2001.916274.

[13] P. Van Mieghem and F. A. Kuipers, "Concepts of Exact QoS Routing Algorithms," *IEEE/ACM Trans. Networking*, vol. 12, no. 5, pp. 851-864, Oct 2004, doi: 10.1109/TNET.2004.836112.

[14] E. W. Dijkstra, "A Note on Two Problems in Connexion with Graphs", *Numerische Mathematik*, vol. 1, no. 1, pp. 269-271, Dec 1959, doi: 10.1007/BF01386390.

[15] L. Rosati, M. Berioli, and G. Reali, "On Ant Routing Algorithms in Ad Hoc Networks with Critical Connectivity," *Ad Hoc Networks*, vol. 6, no. 6, pp. 827-859, Aug 2008, doi: 10.1016/j.adhoc.2007.07.003.

[16] M. Dorigo, M. Birattari, and T. Stutzle, "Ant Colony Optimization," *IEEE Computational Intelligence Magazine*, vol. 1, no. 4, pp. 28-39, Nov 2006, doi: 10.1109/MCI.2006.329691.

[17] L. Buttyán, and J-P. Hubaux, *Security and Cooperation in Wireless Networks*. Cambridge University Press, pp. 183-211, 2007.

[18] M.H. Eiza, and Q. Ni, "An Evolving Graph-Based Reliable Routing Scheme for VANETs," *IEEE Trans. Vehicular Technology*, vol. 62, no. 4, pp. 1493-1504, May 2013, doi: 10.1109/TVT.2013.2244625.

[19] M. Raya, and J-P. Hubaux, "The Security of Vehicular Ad hoc Networks," *Proc. Third ACM Workshop on Security of Ad hoc and Sensor Networks (SASN'05)*, Alexandria, VA, USA, pp. 11-21, Nov 2005, doi: 10.1145/1102219.1102223.

[20] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An Efficient Pseudonymous Authentication Scheme With Strong Privacy Preservation for Vehicular Communications," *IEEE Trans. Vehicular Technology*, vol. 59, no. 7, pp. 3589–3603, Sep 2010, doi: 10.1109/TVT.2010.2051468.

[21] R. Lu, X. Lin, H. Zhu, P-H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications," *Proc. the 27th Conf. IEEE Computer and Communications* (*INFOCOM 2008*), Phoenix, AZ, pp. 1903-1911, 2008, doi: 10.1109/INFOCOM.2008.179.

[22] C.P. Schnorr, "Efficient Signature Generation by Smart Cards," *J. Cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[23] National Institute of Standards and Technology (NIST) "Secure Hash Standards (SHS)," *Federal Information Processing Standards (FIPS) publication*, available at: http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

[24] X. Wang, Y.L. Yin, and H. Yu, "Finding Collisions in the Full SHA-1," *Advances in Cryptology – CRYPTO 2005, Lecture Notes in Computer Science Vol. 3621*, V. Shoup, eds., Springer Berlin Heidelberg, pp. 17-36, 2005, doi: 10.1007/11535218_2.

[25] M. Riley, K. Akkaya, and K. Fong, "A Survey of Authentication Schemes for Vehicular Ad Hoc Networks," *Security and Communication Networks*, vol. 4, no. 10, pp. 1137-1152, Oct 2011, doi: 10.1002/sec.239.

[26] J.B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," *Proc. of the IEEE*, vol. 99, no. 7, pp. 1162-1182, July 2011, doi: 10.1109/JPROC.2011.2132790.

[27] A. Vinel, "3GPP LTE Versus IEEE 802.11p/WAVE: Which Technology is Able to Support Cooperative Vehicular Safety Applications?," *IEEE Wireless Communications Letters*, vol. 1, no. 2, pp. 125–128, Apr 2012, doi: 10.1109/WCL.2012.022012.120073.

[28] H. Shokrani, and S. Jabbehdari, "A Novel Ant-Based QoS Routing for Mobile Ad Hoc Networks," *First International Conf. on Ubiquitous and Future Networks (ICUFN)*, Hong Kong, pp. 79-82, June 2009, doi: 10.1109/ICUFN.2009.5174289.

[29] M. Liu, Y. Sun, R. Liu, and X. Huang, "An Improved Ant Colony QoS Routing Algorithm Applied to Mobile Ad Hoc Networks," *International Conf. on Wireless Communications, Networking and Mobile Computing, (WiCom)*, Shanghai, pp. 1641-1644, Sep 2007, doi: 10.1109/WICOM.2007.413.

[30] S. Marwaha, C.K. Tham, and D. Srinivasan "Mobile Agents Based Routing Protocol for Mobile Ad Hoc Networks," *IEEE Global Telecommunications Conf. (GLOBECOM '02)*, pp. 163-167, Nov 2002, doi: 10.1109/GLOCOM.2002.1188062.

[31] J.A.P. Martins, S.L.O.B Correia, and J. Celestino, "Ant-DYMO: A Bio-Inspired Algorithm for MANETs," *IEEE 17th International Conf. on Telecommunications (ICT)*, pp. 748-754, Apr 2010, doi: 10.1109/ICTEL.2010.5478808.

[32] M. Gunes, U. Sorges, and I. Bouazizi, "ARA-The Ant-Colony Based Routing Algorithm for MANETs," *Proc. International Conf. on Parallel Processing Workshops*, pp. 79-85, Aug 2002, doi: 10.1109/ICPPW.2002.1039715.

[33] G. Di Caro, F. Ducatelle, and L.M. Gambardella, "AntHocNet: An Adaptive Nature-Inspired Algorithm for Routing In Mobile Ad Hoc Networks," *European Trans. Telecommunications, Special Issue on Self-organization in Mobile Networking*, vol. 16, no. 5, pp. 443-455, Sep/Oct 2005, doi: 10.1002/ett.1062.

[34] K. Kunavut, and T. Sanguankotchakorn, "Multi-Constrained Path (MCP) QoS Routing in OLSR based on Multiple Additive QoS Metrics," *International Symp. Communications and Information Technologies (ISCIT)*, Tokyo, pp. 226-231, Oct 2010, doi: 10.1109/ISCIT.2010.5664843.

[35] W. Cai, X. Jin, Y. Zhang, K. Chen, and R. Wang, "ACO Based QoS Routing Algorithm for Wireless Sensor Networks," *Proc. Third Conf. on Ubiquitous Intelligence and Computing (UIC)*, Wuhan, China, pp. 419-428, 2006, doi: 10.1007/11833529_43.

[36] L. Cobo, A. Quintero, and S. Pierre, "Ant-Based Routing for Wireless Multimedia Sensor Networks Using Multiple QoS Metrics," *Computer Networks*, vol. 54, no. 17, pp. 2991-3010, Dec 2010, doi: 10.1016/j.comnet.2010.05.014.

[37] N. Kumar, R. Iqbal, N. Chilamkurti, and A. James, "An Ant Based Multi Constraints QoS Aware Service Selection Algorithm in Wireless Mesh Networks," *Simulation Modelling Practice and Theory*, vol. 19, no. 9, pp. 1933-1945, Oct 2011, doi: 10.1016/j.simpat.2011.05.007.

[38] Y. Sun, H. Ma, L. Liu, and Y. Zheng, "ASAR: An Ant-Based Service-Aware Routing Algorithm For Multimedia Sensor Networks," *Frontiers of Electrical and Electronic Eng. in China*, vol. 3, no. 1, pp. 25-33, Jan 2008, doi: 10.1007/s11460-008-0013-7.

[39] O.A. Wahab, H. Otrok, and A. Mourad, "VANET QoS-OLSR: QoS-based Clustering Protocol for Vehicular Ad hoc Networks," *Computer Communications*, vol. 36, no. 13, pp. 1422-1435, July 2013, doi: 10.1016/j.comcom.2013.07.003.

[40] E. Fonseca, and A. Festag, "A Survey of Existing Approaches for Secure Ad hoc Routing and Their Applicability to VANETs," *NEC Technical Report NLE-PR-2006-19*, 2006.

[41] L. Chen, S. Ng, and G. Wang, "Threshold Anonymous Announcement in VANETs," *IEEE J. Selected Areas in Comm.*, vol. 29, no. 3, pp. 605–615, Mar 2011, doi: 10.1109/JSAC.2011.110310.

[42] V. Daza, J. Domingo-Ferrer, F. Sebé, and A. Viejo, "Trustworthy Privacy Preserving Car Generated Announcements in Vehicular Ad Hoc Networks," *IEEE Trans. Vehicular Technology*, vol. 58, no. 4, pp. 1876–1886, May 2009, doi: 10.1109/TVT.2008.2002581.

[43] F. Dötzer, L. Fischer, and P. Magiera, "VARS: A Vehicle Ad Hoc Network Reputation System," *Sixth IEEE International Symp. World Wireless Mobile Multimedia Network*, pp. 454–456, June 2005, doi: 10.1109/WOWMOM.2005.109.

[44] Q. Li, A. Malip, K.M. Martin, S-L. Ng, and J. Zhang, "A Reputation-Based Announcement Scheme for VANETs," *IEEE Trans. Vehicular Technology*, vol. 61, no. 9, pp. 4095–4108, Nov 2012, doi: 10.1109/TVT.2012.2209903.

[45] N. Bismeyer, S. Mauthofer, K.M. Bayarou, and F. Kargl "Assessment of Node Trustworthiness in VANETs Using Data Plausibility Checks with Particle Filters," *Vehicular Network Conf. (VNC)*, Seoul, pp. 78-85, Nov 2012, doi: 10.1109/VNC.2012.6407448.

[46] S.K. Dhurandher, M.S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular Security through Reputation and Plausibility Checks," *IEEE Systems J.*, vol. 8, no. 2, pp. 384-394, June 2014, doi: 10.1109/JSYST.2013.2245971.

[47] P. Golle, D.H. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," *Proc. First ACM International Workshop on Vehicular Ad Hoc Networks*, Philadelphia, PA, USA, pp. 29–37, Sep/Oct 2004, doi: 10.1145/1023875.1023881.

[48] M.H. Eiza, Q. Ni, T. Owens, and G. Min, "Investigation of Routing Reliability of Vehicular Ad Hoc Networks," *EURASIP J. Wireless Comm. and Networking*, vol. 2013, no. 1, pp. 1-15, July 2013, doi: 10.1186/1687-1499-2013-179.

[49] Z. Niu, W. Yao, Q. Ni, and Y. Song, "DeReq: A QoS Routing Algorithm for Multimedia Communications in Vehicle Ad Hoc Networks," *Proc. International Conf. Wireless Comm. and Mobile Computing (IWCMC '07)*, Honolulu, Hawaii, pp. 393-398, Aug 2007, doi: 10.1145/1280940.1281025.

[50] M. Rudack, M. Meincke, K. Jobmann, and M. Lott, "On The Dynamics of Ad Hoc Networks for Inter Vehicle Communication (IVC)," *International Conf. Wireless Networks (ICWN '02)*, Las Vegas, NV, USA, June 2002.

[51] G. Mao, and B.D.O. Anderson, "Graph Theoretic Models and Tools for the Analysis of Dynamic Wireless Multihop Networks," *IEEE Wireless Comm. and Networking Conf. (WCNC)*, Budapest, pp. 1-6, Apr 2009, doi: 10.1109/WCNC.2009.4917738.

[52] J. Monteiro, A. Goldman, and A. Ferreira, "Performance Evaluation of Dynamic Networks Using an Evolving Graph Combinatorial Model," *IEEE International Conf. Wireless and Mobile Computing, Networking and Comm. (WiMob'2006)*, Montreal, Que, pp. 173-180, June 2006, doi: 10.1109/WIMOB.2006.1696378.

[53] A. Ferreira, "On Models and Algorithms for Dynamic Communication Networks: The Case for Evolving Graphs," *Proc. 4e Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (ALGOTEL'2002)*, Mèze, France, pp. 155–161, 2002.

[54] J. Monteiro, "The use of Evolving Graph Combinatorial Model in Routing Protocols for Dynamic Networks," *Proc. the XV Concurso Latinoamericano de Tesis de Maestrìa (CLEI '08)*, Santa Fe, Argentina, pp. 41-57, 2008.

[55] A. Vinel, V. Vishnevsky, and Y. Koucheryavy, "A Simple Analytical Model for the Periodic Broadcasting in Vehicular Ad-Hoc Networks," *IEEE Globecom Workshops*, New Orleans, LO, US, pp. 1-5, Nov/Dec 2008, doi: 10.1109/GLOCOMW.2008.ECP.73.

[56] OMNeT++ Community, OMNeT++ Network Simulator. Available at: http://www.omnetpp.org/ (Accessed: 05/20 2011).

[57] International Telecommunication Union P.800.1, ("Mean Opinion Score (MOS) Terminology," available at: http://www.itu.int/rec/T-REC-P.800.1 (Accessed: 02/22 2014)

Mahmoud Hashem Eiza received the B.Sc. degree in engineering informatics from Damascus University, Damascus, Syria, in 2007 and the M.Sc. degree (with distinction) in Data Communication Systems from Brunel University London, U.K., in 2010. He is currently working toward the Ph.D. degree in electronic and computer engineering with Brunel University London, under the supervision of Dr T. Owens and Prof Q. Ni. His main research interests are quality of service and reliable routing algorithms for wireless ad hoc networks.

Thomas Owens obtained his PhD in Electrical and Electronic Engineering from Strathclyde University in 1986. In 1987 he joined as a lecturer the Department of Electronic and Electrical Engineering, Brunel University London, which was eventually absorbed into the School of Engineering and Design in 2004 in which he is Senior Lecturer Communications. He was the project coordinator of the IST FP5 project CONFLUENT, the IST FP6 Integrated Project INSTINCT, and the FP6 Specific Support Action PARTAKE. He is the project coordinator of FP7 Support Action CHOICE. He has published more than 100 papers.

Qiang Ni (SM'08) received the B.Sc., M.Sc., and Ph.D. degrees from Huazhong University of Science and Technology, Wuhan, China, all in engineering. He is a Professor of communications and networking with the School of Computing and Communications, Lancaster University, Lancaster, U.K. Prior to that, he led the Intelligent Wireless Communication Networking Group at Brunel University London, U.K. His main research interests are wireless communications and networking, in which he has published more than 100 papers. Prof Ni was an IEEE 802.11 Wireless Standard Working Group Voting Member and a contributor to the IEEE wireless standards.