# 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

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

*Manuscript received 29 June 2014; revised 30 Oct. 2014; accepted 18 Nov. 2014. Date of publication 12 Jan. 2015; date of current version 20 Jan. 2016. For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier no. 10.1109/TDSC.2014.2382602*