Secure And Robust Multi-constrained Qos Aware Routing Algorithm For VANETS

[1]Karpagam.T
Assistant Professor
[2]Revathi.v revathirey.v@gmail.com
[3]sumithra.L sumithraloganathan@gmail.com
[4] yamunakumari.M yamunakumari165@gmail.com
[2][3][4]UG students com
Department of Computer Science and Engineering
T.J.S. Engineering College

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-Secure Routing Optimization, reliable routing, secure routing, VANETs*

1.Introduction

The performance characteristics of VANET such as security and reliability, Quality of Service (QoS), inter-networking, power consumption and multicasting have attracted more attention in academic research . Recently evolutionary and swarm intelligent routing protocols are developed to solve this problem that include Genetic Algorithm16, Particle Swarm Optimization17, Bird-flight algorithm18, Bee Colony Optimization19 and Ant Colony Optimization (ACO)20. However, it appears that the study of this hard problem under the influence of a multi-objective optimization function consisting of QoS, energy

QoS routing plays an essential role in identifying routes that meet the QoS requirements of the offered ser-vice 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 approxima-tion routing algorithms. In the exact solutions, different strategies have been followed such as nonlinear definition

.Matt [5] discussed a solution in pairing-based signature scheme, which can identify nontrivial numbers of invalid signatures in batches. Though these works are state-of-theart ,it is challenging to apply them with vanets .

2.Existing System

Existing two distinct approaches adopted to solve MC(O)P problems, exact QoS routing algorithms and approximation routing algorithms.

Unfortunately, these strategies are not suitable for application in highly dynamic networks like VANETs.

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.

3.Proposed System

We propose a novel secure ACO-based MCQ aware (S-AMCQ) routing algorithm for VANETs.

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 that captures the evolving characteristics of the vehicular network topology.

Simulation results demonstrate that S-AMCQ can guarantee significant performance in terms of QoS guarantees and reliable routing service while applying security mechanisms.

In this paper, we propose a novel secure ACO-based MCQ aware (S-AMCQ) routing algorithm for VANETs. SAMCQ aims to identify feasible routes between two vehicles subject to multiple QoS constraints, and provide a reliable and robust routing service. 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 VANEToriented evolving graph (VoEG) model 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

.

4. Existing System

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, look-ahead feature, and k shortest paths. Unfortunately, these strategies are not suitable for application in highly dynamic networks like VANETs. For instance, the look-ahead strategy proposes computing the

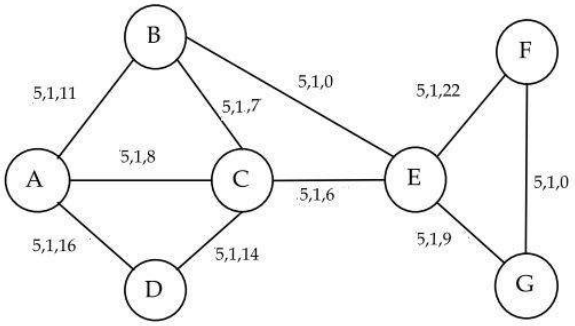
shortest path tree rooted at the destination to each node in the network for each of the m link weights separately where
m is the number of QoS constraints. This proposal means that Dijkstra's algorithm should be executed m times. This
strategy is not suitable for application in VANETs because it adds 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 organizing, thus robust and fault tolerant, and they intrinsically adapt to traffic changes without
requiring complex mechanisms. 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 algorithm seeds. Finally Propagation phase involves expanding the seeds which was removed in the filtering phase.

5.1. Proposed System

Authenticating the Routing Control Messages

The source node that originates the control message should enable authentication of it. In this way, immutable
information is protected, but mutable information, if found, cannot be authenticated because it has not been yet added
by intermediate nodes. Moreover, if we suppose that only the destination node can verify the authenticity of the control
messages, then we can ensure that it will not respond to any spoofed control message. Thus, the creation of an incorrect
routing state can be prevented at the destination node and at the source node using the same logic for routing replies.

However, intermediate nodes can still be exposed to spoofed control messages. Therefore, the creation of an incorrect
routing state is possible if they update their routing table based on the information carried by these spoofed control
messages. Hence, we need an authentication mechanism that enables every node to authenticate and verify control
messages processed by other nodes.



The proposed E-VoEG Model.

Secure AMCQ Routing Algorithm (S-AMCQ)

As we can conclude from the previous discussion, there is no mechanism to protect the routing process in VANETs
against all possible attacks. However, different security mechanisms such as digital signatures, hash chains, plausibility
checks, etc. could be applied together to protect the routing process. As we have mentioned before, using symmetric
cryptography in VANETs is not suitable due to the complexity of O(|V| 2) of the number of unique shared keys and the
lack of the nonrepudiation property needed in VANETs. Asymmetric cryptography is preferable since the problem of
high processing requirements associated with it can be alleviated in VANETs due to relaxed power consumption
constraints. Besides, vehicles usually have temporary access to infrastructure, e.g., RSUs, and require central
registrations and periodic technical inspection, therefore, CAs are able to perform necessary tasks such as certifying a

vehicle's signing keys, revoking certificates, etc. However, asymmetric cryptography still has the problem of exposing
the privacy of vehicles and drivers because the identity of the vehicle is bound with its signing keys. In the following,
we propose a novel set of security mechanisms to protect the routing control messages of the AMCQ routing algorithm
we developed in the 6. Secure Ant-Based Multi-Constrained QoS Routing for VANETs.We recall that AMCQ routing
algorithm is designed to offer significant advantages in terms of protecting the routing information within the control
messages. We exploit these advantages and propose asymmetric cryptography, more specifically public key
cryptography using pseudonymous certificates, to defend against external attackers and plausibility checks, based on an
extended version of the VoEG model, to defend against internal attackers. Plausibility checks are suggested based on
the design advantages of the AMCQ routing algorithm and its components. The integration of the proposed security
mechanisms and AMCQ results in an algorithm called S-AMCQ for Secure AMCQ routing algorithm.

I

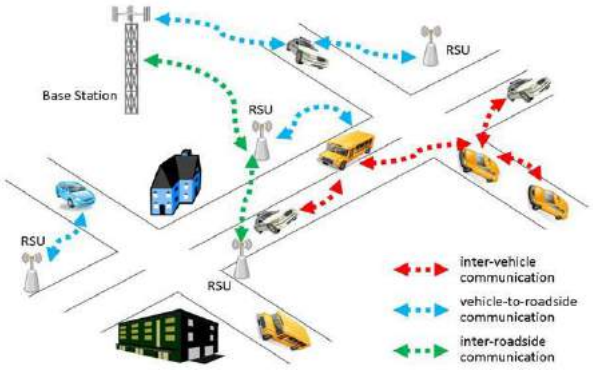
The source node that originates the control message should enable authentication of it. In this way, immutable
information is protected, but mutable information, if found, cannot be authenticated because it has not been yet added
by intermediate nodes. Moreover, if we suppose that only the destination node can verify the authenticity of the control
messages, then we can ensure that it will not respond to any spoofed control message. Thus, the creation of an incorrect
routing state can be prevented at the destination node and at the source node using the same logic for routing replies.
However, intermediate nodes can still be exposed to spoofed control messages. Therefore, the creation of an incorrect
routing state is possible if they update their routing table based on the information carried by these spoofed control
messages. Hence, we need an authentication mechanism that enables every node to authenticate and verify control
messages processed by other nodes.

.

Route Discovery Process in S-AMCQ Routing Algorithm

Before describing the route discovery process in the S-AMCQ routing algorithm, it is worth noting that the structure of
routing control ants proposed for AMCQ stays the same for S-AMCQ except for the RPANT messages. As the EVoEG
model is now available at each vehicle, the following fields are omitted from RPANTs: RT_reliability, RT_Delay, and
RT_Cost. These fields contain the reliability, end-to-end delay, and cost of the computed forward route, respectively,
and were mutable and traceable. These values can be now calculated on the basis of the E-VoEG model and the
Traversed List field information. In this way, the contents of a RPANT message are all now immutable and thus the
security information overhead needed to protect it is reduced .

System Architecture



Route Discovery Process in S-AMCQ Routing Algorithm

Before describing the route discovery process in the S-AMCQ routing algorithm, it is worth noting that the structure of
routing control ants proposed for AMCQ stays the same for S-AMCQ except for the RPANT messages. As the EVoEG
model is now available at each vehicle, the following fields are omitted from RPANTs: RT_reliability, RT_Delay, and
RT_Cost. These fields contain the reliability, end-to-end delay, and cost of the computed forward route, respectively,
and were mutable and traceable. These values can be now calculated on the basis of the E-VoEG model and the
Traversed List field information. In this way, the contents of a RPANT message are all now immutable and thus the
security information overhead needed to protect it is reduced .

Route Maintenance Process in S-AMCQ Routing Algorithm

When an unpredicted link breakage occurs, it is reported back to sr either to start a new route discovery process or to
switch to another feasible route in M TC(sr, de). The link breakage plausibility check is applied to ensure the received
REANT is legitimate. If the REANT is legitimate and M TC(sr, de) is empty, sr starts a new route discovery process.
Otherwise, switching to another feasible route is commenced. Prior to making the switch, sr should guarantee this
available feasible route still satisfies the QoS requirements. This task is accomplished using the E-VoEG model
information at sr instead of sending QMANTs like in AMCQ. After that, sr can select the evaluated route as a new best
route because it still satisfies the QoS constraints according to the E-VoEG information, or sr 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

ACORULES FOR MCQROUTING IN VANETS

4.1Multi-Constrained (Optimal) Path Problem

Let $G(V, E)$ be an undirected graph representing a vehicu-lar 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$Li$where$i$= 1, 2, …m.Each link between two vehicles $l(C1, C2) \in E$is associated $m$weightscorresponding to QoS constraints such that$wi(C1, C2) \geq 0$. 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 thatall the QoS constraints are met as describedin the following equation:

(1)wi(P)£Li,i=1,2,...m

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

(2)argmaxPÎM(s,d)F(P)

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

(3)F(P)=OiLiwi(P)æèçöø÷i=1må

where $0 < Oi \leq 1$are optimisation factors associated witheach 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 $L1$= 100 msdenote the end-to-end delayconstraintand $L2$= 10 be the hop-countconstraint, *i.e.*, the number of QoS constraints m = 2.Let $M(s, d)$ = {$P1$, $P2$}where $w1(P1)$= 77 ms, $w2(P1)$= 8, $w1(P2)$= 89 ms,and $w2(P2)$= 7.Here,$w1$rep-resents the weight value of the end-to-end delay meas-ured in [ms] and $w2$represents the weight value of the hop-count. If the application intends to transmit voice traffic,then it could determinethe optimisation factor for the end-to-end delay constraint$O1$= 1 and for the hop-count constraint $O2$= 0.5. In this way, the objective func-tion $F(P)$ in (3) favours

theroute that has the least end-to-end delay valuesince voice traffic is delay sensitive. Ac-cording to (3), $F(P) = 1.923$ for $P1$and $F(P) = 1.837$for $P2$, thus $P1$is selected for voice traffic transmission. However, if the application wants to transmit background traffic,then it could determine $O1 = 0.5$ and $O2 = 0.8$, *i.e.*, $F(P)$ favours the shortest route with an acceptable end-to-end delay value. In this case, $F(P) = 1.649$ for $P1$and $F(P) = 1.704$for $P2$, thus $P2$is selected for background traffic transmission.

8. Conclusion

Vehicular Ad hoc Networks (VANETs) are a promising wireless technology to facilitate the application of novel
services in our roads ranging from safety and traffic management to commercial applications. These services require
the transmission of different data types with different QoS requirements. However, VANETs are characterized by high
node mobility and frequent changes of network topology, and unreliable communication links. Moreover, the openness
of its wireless channels to both external and internal security attacks raises serious challenges before these networks can
be deployed successfully. In this thesis, we demonstrated how to develop a reliable ant-based multi-constrained QoS
(AMCQ) routing algorithm that accommodates the transmission of different data types with different QoS constraints
on highways for VANETs. Moreover, we proposed a novel set of security mechanisms to protect the developed AMCQ
routing algorithm from possible internal and external security attacks

Routing Request Ant (RQANT)

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

1. RQANT_ID (*u_int8_t*) containsthe ant's ID, which is immutable.
2. *RQANT_Gen* (*u_int8_t*) indicates the current ant generation, which is immutable. Different ant gen-erations 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 dis-carded.
3. *RQANT_TC*(*u_int8_t*) contains the traffic class
identifier *TC_ID*the current route discovery pro-cess is issued for, which is immutable. This field is important to distinguish different QoS require-ments while searching for feasible routes for dif-ferent 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 routethatthe RQANT has travelled so far. This fieldis mutable and traceable.
7. QoS_Constraints (*double*) contains the QoS con-straints 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.

6.1.2RoutingReply Ant (RPANT)

The RPANT is designed to set up forward routes to the

9. References

1. Vinel, "Performance aspects of vehicular ad-hoc networks: Current research and possible

trends," presented at the 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 Netw. Mag., vol. 27, no. 5, pp. 48–54, Sep./Oct. 2013.
3. K. Yang, S. Ou, H. Chen, and J. He, "A multihop peer-communica-tion protocol with fairness guarantee for IEEE 802.16-based vehic-ular networks," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3358– 3370, Nov. 2007.
4. Z. Wang and J. Crowcroft, "Quality-of-service routing for sup-porting multimedia applications," IEEE J. Select. Areas Comm., vol. 14, no. 7, pp. 1228–1234, Sep. 1996.
5. D. S. Reeves and H. F. Salama, "A distributed algorithm for delay-constrained unicast routing," IEEE/ACM Trans. Netw., vol. 8, no. 2, pp. 239–250, Apr. 2000.
6. M. Curado and E. Monteiro, "A survey of QoS routing algo-rithms," in Proc. Int. Conf. Inform. Technol., Istanbul, Turkey, 2004, 43–46.
7. Y. Bejerano, Y. Breitbart, A. Orda, R. Rastogi, and A. Sprintson, "Algorithms for computing QoS paths with restoration," IEEE/ ACM Trans. Netw., vol. 13, no. 3, pp. 648–661, Jun. 2005.
8. Zhang, J. Hao, and H. T. Mouftah, "Bidirectional multi-con-strained routing algorithms," IEEE Trans. Comput., vol. 63, no. 9, 2174–2186, Sep. 2014.
9. F. Kuipers, P. Van Mieghem, T. Korkmaz, and M. Krunz, "An overview of constraint-based path selection algorithms for QoS routing," IEEE Commun. Mag., vol. 40, no. 12, pp. 50–55, Dec. 2002.
10. P. Van Mieghem, H. D. Neve, and F. A. Kuipers, "Hop-by-hop quality of service routing," Comput. Netw., vol. 37, no. 3/4, 407–423, Nov. 2001.