Efficient QoS And Secure Routing In VANET Using Group Based Routing Management Protocol

Imran Khan.I [1], Rajeshwari[2]
Department of ECE
[1]PSN College of Engineering and Technology, Tirunelveli.
[2]Assistant Professor,PSN College of Engineering and Technology, Tirunelveli.

Abstract-*A growing number of networking protocols and location-aware services require that mobile nodes learn the position of their neighbors. However, such a process can be easily abused or disrupted by adversarial nodes. In absence of a-priori trusted nodes, the discovery and verification of neighbor positions presents challenges that have been scarcely investigated in the literature. we address this open issue by proposing a fully-distributed cooperative solution that is robust against independent and colluding adversaries, and can be impaired only by an overwhelming presence of adversaries. We use our proposed approacfor reduce the false rejection ratio in nodes & agents. Finally we identify the trusted nodes in networks then packets will send through that trusted nodes. Trusted nodes are identified based on trust values for identify the neighboring nodes for verification process. Here we use Group based routing Management protocol for secure and malicious node detection.*

I. 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. 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 multihop vehicular network subject to multiple QoS constraints is a multi-constrained (Optimal) Path (MC(O)P) problem, which is proven to be NP-hard if the constraints are mutually independent. 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. 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 selforganising, 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 algorithms. 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. An adversary’s capacity to mount specific attacks 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. 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.

II. RELATED WORK

Recently, much work has been carried out on ACO-based QoS routing algorithms for mobile ad hoc . 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. 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 initializes the pheromones on each link with a constant value and positions a set of ants at the source node. At each iteration Nc, 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, Nc > Nmax, is met.

A QoS-based clustering protocol for VANETs, named VANET QoS-OLSR, is proposed in. 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 two-hops away nodes. Each two-hops away node that receives this ant message calculates its QoS metrics and inserts them in the message. The updated message is then propagated twohops 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 ANTHELLO 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. Security mechanisms such as digital signatures and message authentication 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 and plausibility checks. 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 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.

III. THE PROPOSED FRAMEWORK

The proposed method consists of modules such as

- Network creation
- Packet and Network configurations
- Group based routing management protocol implementation
- Malicious node detection due to trust values
- Secure routing implementation

A. Network creation

In this module, we configured the packet for channel type, link & MAC layer type, IEEE 802.11, max packet frequency etc.,

B. Packet and Network configurations

In this module, we configured the packet for channel type, link & MAC layer type, IEEE 802.11, max packet frequency etc.,

C. Group based routing management protocol implementation

We form a number of cluster based on node positions and energy values. We implement Trust management protocol through identify the neiboring node position from request and acknowledgement.

D. Malicious node detection due to trust values

In this module, we monitor packet lost and traffic system of network. We transmit the data only trusted nodes between source to destination. Using this module, we can reduce the traffic and packet lost in network transmission Find the malicious node between transmission path. Finally we transmit the packet in secure via through trusted nodes.

E. Secure routing implementation

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.

Routing Request Ant

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.

Routing Reply Ant

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 sourcenode 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.

Routing Error Ant

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

IV. 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 (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.

V. SIMULATION RESULTS

Fig. 5(a) 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.

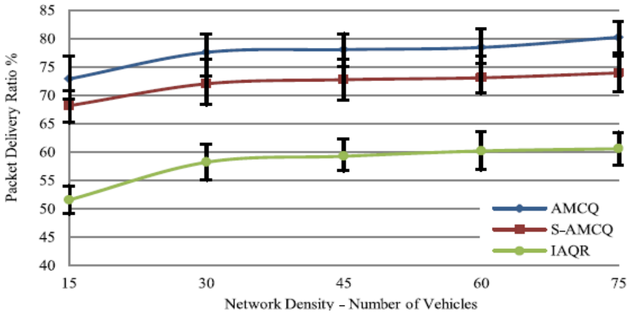

Fig.5. (a) Average packet delivery ratio

Fig. 5(b) 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 SAMCQ delays the route discovery process especially when the network density increases, which affects its PDR as showed in Fig. 5(a). 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 SAMCQ 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 vehicles 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. 5(a).

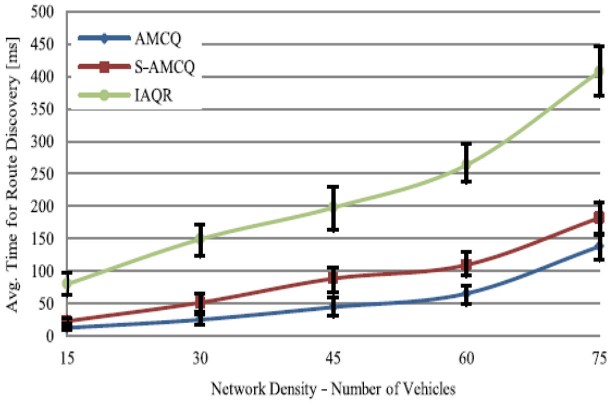

Fig. 5(b) Average time for route discovery.

It can be noticed in Fig. 5(c) 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(d) shows that the Playout loss rate of each routing algorithm is linked with Fig. 5(c), 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.

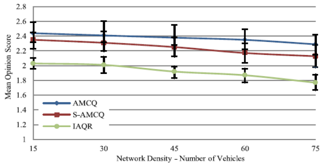

Fig.(c).Meanopinionscore

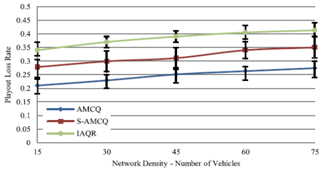

Fig.5(d). Playout loss rate

VI. CONCLUSION

In this paper, we utilize the ACO rules to propose a secure ACO-based MCQ routing algorithm for VANETs. The ACO rules are designed to consider the dynamics of the vehicular network topology. Moreover, we design 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 SAMCQ routing algorithm based on its design and an extended VANET-oriented Evolving Graph 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,” presented at the GI/ITGWorkshop 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 multi hop peer-communication protocol with fairness guarantee for IEEE 802.16-based vehicular 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 supporting 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 algorithms,”in Proc. Int. Conf. Inform. Technol., Istanbul, Turkey, 2004,pp. 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] B. Zhang, J. Hao, and H. T. Mouftah, “Bidirectional multi-constrained routing algorithms,” IEEE Trans. Comput., vol. 63, no. 9,pp. 2174–2186, Sep. 2014.

[9] F. Kuipers, P. Van Mieghem, T. Korkmaz, and M. Krunz, “Anoverview of constraint-based path selection algorithms for QoS routing,” IEEE Commun. Mag., vol. 40, no. 12, pp. 50–55,Dec. 2002.