ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

A Novel Secure and Reliable Multi-Constrained QoS Aware Routing Algorithm for VANETS

Tabitha. V[1], C.H. Sudarsan Raju[2]

M.Tech Student, Department of ECE, BIT Institute of Technology, Hindupur, India[1]

Associate Professor, Department of ECE, BIT Institute of Technology, Hindupur, India[2]

ABSTRACT: Vehicular Ad hoc Networks (VANETs) are a particular form of wireless network made by vehicles communicating among themselves and with roadside base stations. A wide range of services has been developed for VANETs ranging from safety to infotainment applications. A key requirement for such services is that they are offered with Quality of Service (QoS) guarantees in terms of service reliability and availability. Furthermore, due to the openness of VANET's wireless channels to both internal and external attacks, the application of security mechanisms is mandatory to protect the offered QoS guarantees. QoS routing plays an essential role in identifying routes that meet the QoS requirements of the offered service over VANETs. However, searching for feasible routes subject to multiple QoS constraints is in general NP-hard problem. Moreover, routing reliability needs to be given special attention as communication links frequently break in VANETs. To date, most existing QoS routing algorithms are designed for stable networks without considering the security of the routing process. Therefore, they are not suitable for applications in VANETs. 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, a novel secure and reliable multi-constrained QoS aware routing algorithm for VANETs is proposed and the ant colony optimisation (ACO) technique is employed 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 demonstrate that S-AMCQ can guarantee significant performance in terms of QoS guarantees and reliable routing service while applying security mechanisms.

KEYWORDS: Provenance, security, sensor networks, Packet drop attack, Wireless Sensor Networks, Provenance attack.

1. INTRODUCTION

Vehicular Ad-Hoc Networks, (VANET), are a particular kind of Mobile Ad Hoc Network, (MANET), in which vehicles act as nodes and each vehicle is equipped with transmission capabilities which are interconnected to form a network. The topology created by vehicles is usually very dynamic and significantly non-uniformly distributed. In order to transfer information about these kinds of networks, standard MANET routing algorithms are not appropriate. With the rapid growth of vehicles and roadside traffic monitors, the advancement of navigation systems, and the low cost of wireless network devices, promising peer-to-peer (P2P) applications and externally-driven services to vehicles became available. For this purpose, the Intelligent Transportation Systems (ITS) have proposed the Wireless Access in Vehicular Environments (WAVE) standards that define an architecture that collectively enables vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications (ITS, 2012). According to architectures of network, VANET can be divided into three categories, the first of which is the Wireless Wide Area Network (WWAN) in which the access points of the cellular gateways are fixed in order to allow direct communication between the vehicles and the access points. However, these access points require costly installation, which is not feasible. The second category is the Hybrid Wireless Architecture in which WWAN access points are used at certain points while an ad hoc communication provides access and communication in between those access points. The third and final category is the Ad Hoc V2V

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

Communication which does not require any fixed access points in order for the vehicles to communicate. Vehicles are equipped with wireless network cards, and a spontaneous setting up of an ad hoc network can be done for each vehicle (Li and Wang, 2007). This study will focus on studying ad hoc V2V communication networks, which are also known as VANETs. The purpose of VANET is to allow wireless communication between vehicles on the road including the roadside wireless sensors, enabling the transfer of information to ensure driving safety and planning for dynamic routing, allowing mobile sensing as well as providing in-car entertainment. VANETs require geographical routing protocols that utilize the Global Positioning System (GPS) to locate the next available node on the network.
Similar to MANETs, nodes in VANETs self-organize and self-manage the information in a distributed fashion, *i.e.*, without a centralised server controlling the communications. This means nodes can act as servers and/or clients at the same time and exchange information with other nodes. However, nodes in VANETs have special attractive features over MANETs and other wireless sensor networks. These features are Unrestricted transmission power and storage. Mobile device power issues are not usually a significant constraint in VANETs since the vehicle can provide continuous power for computing and communication devices.

Higher computational capability. It is assumed that vehicles can provide the communication devices on board with significant computing and sensing capabilities.
Vehicle registration and periodic inspection. Vehicles have an obligation to register with a governmental authority and be regularly inspected. This feature is unique for VANETs and can offer significant advantages in terms of checking the communication system integrity and security information updates.
Besides the pleasing features mentioned above, there are some technical challenges raised by the unique behaviour and characteristics of VANETs. These challenges should be resolved in order to deploy these networks effectively and bring the proposed applications to fruition. These technical challenges include.
Potentially large scale. VANETs are almost the only ad hoc network that expected to have hundreds of nodes participating in the communication process. Network nodes include vehicles and potential road infrastructure such as RSUs. Therefore, VANETs should be scalable with a very high number of network nodes.

II. LITERATURE SURVEY

Over the last decade, much work has been carried out on ACO-based QoS routing algorithms for MANETs and wireless sensor networks.
However, to the best of our knowledge, little attention has been given to providing MCQ routing in VANETs using the ACO technique. Next, we provide a brief review of some related work.

1) In regard to ACO-based QoS routing algorithms for 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. 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, specifically the bandwidth, from the network. It then initializes the pheromones on each link with a constant value and positions a set of $\mathcal{J}$ 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 using a local pheromone evaporation parameter ρ. Once it arrives at the destination node, the ant calculates the objective function based on the achieved QoS metrics. The algorithm continues until the termination condition $N_c > N_{max}$, is met. IAQR uses periodical HELLO broadcasting to maintain local connectivity.

2) Cobo *et al.* propose AntSensNet, a QoS routing algorithm for wireless multimedia sensor networks based on a tailored ant colony algorithm. AntSensNet builds a hierarchical structure on the network before choosing suitable routes to meet various QoS requirements from different kinds of traffic. The main goal of AntSensNet is to save the energy of wireless nodes, which is a valuable resource in a sensor network. Cobo *et al.* assume that both sink and sensor nodes are not mobile in the network. Once the clustering process finishes, the cluster head generates a number of forward ants (FANTs) to search for routes leading to the sink. Each FANT chooses the next hop cluster head based on a calculated probabilistic value as the addition of all QoS parameters collected by the ants, *i.e.*, energy, delay, bandwidth, packet loss, and available memory pheromones are normalised into a single quantity. When a FANT reaches the sink,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

the evaluation of the discovered route is carried out. If it meets the application requirements, the sink generates a backward ant (BANT). The BANT traverses back to the source and updates pheromone values at each node by increasing the pheromone value on the incoming
link and decreasing it on the other links according to different constant evaporation parameters associated with each QoS constraint.

3) In VANETs, the ACO technique has been used in many studies to facilitate single constraint routing and multi-constrained routing. With regard to single constraint routing, Rana *et al*. utilise the vehicles' movements pattern, vehicles' density, vehicles' velocities, and vehicle fading conditions to develop a hybrid, multipath ACO based routing algorithm called Mobility Aware Zone based Ant Colony Optimisation Routing for VANET (MAZACORNET). The vehicular network is divided into multiple zones, and a proactive approach is used to find a route within the zone and a reactive approach is utilised to find routes between zones. The link quality between the communicating vehicles is estimated using the link stability (LS), which is calculated using the velocity and position values of the vehicles, and the probability of successfully receiving the message, which depends on the distance between the vehicles lying within same communication range, estimated using the Nakagami Fading Model. MAZACORNET uses five different types of ants: internal forward ants, external forward ants, backward ants, notification ants, and error ants to perform the route discovery process. Besides that, MAZACORNET uses two types of routing tables: the Intra zone routing table and the Inter zone routing table. The Intra zone routing table proactively updates the information within the zone using internal forward ants, which are transmitted every 20 *s*, whereas, the Inter zone routing table tracks the information between the zones, on demand. MAZACORNET is suitable for dense network scenarios where a large number of vehicles exist within the zone. Due to the proactive approach used to update the Intra zone routing table, MAZACORNET results in a high routing control overhead.

III. 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 algorithms

IV. PROPOSED SYSTEM

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 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 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

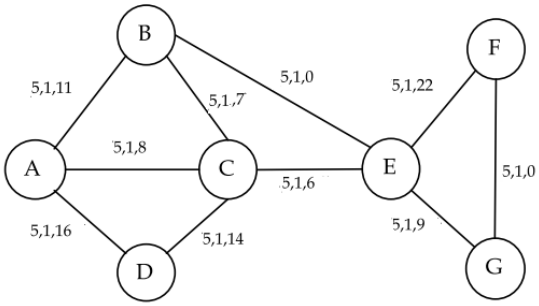
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

or attacks that could be mounted by compromised vehicles if any exist. Simulation results demonstrate that S-AMCQ can guarantee significant performance in terms of QoS guarantees and reliable routing service while applying security mechanisms.



The proposed E-VoEG Model.

V. IMPLEMENTATION

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.

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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

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.

Performance Evaluation of S-AMCQ

The aim of this performance evaluation is to investigate how the time overhead needed to sign, transmit and verify the routing control ants can affect the performance of the S-AMCQ routing algorithm. As the implementation of the PASS scheme is not available to us, we discuss the delays caused by the authentication scheme numerically and insert the resulting numbers into the S-AMCQ implementation for the simulations later.

VI. NETWORK SIMULATOR

The Network Simulator is the Software using and Version 2.28.Network Simulator (NS2) is a discrete event driven simulator developed at UC Berkeley. It is part of the VINT project.
The goal of NS2 is to support networking research and education. It is suitable for designing new protocols, comparing different protocols and traffic evaluations.
NS2 is developed as a collaborative environment. It is distributed freely and open source. Versions are available for FreeBSD, Linux, Solaris, Windows and Mac OS X.
NS2 is built using object oriented methods in C++and OTCL (object oriented variant of TCL).
TCL - Tool Command Language used for specifying scenarios and events.
Nam is a TCL/TK based animation tool for viewing network simulation traces and real world packet traces. It supports topology layout, packet level animation, and various data inspection tools.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

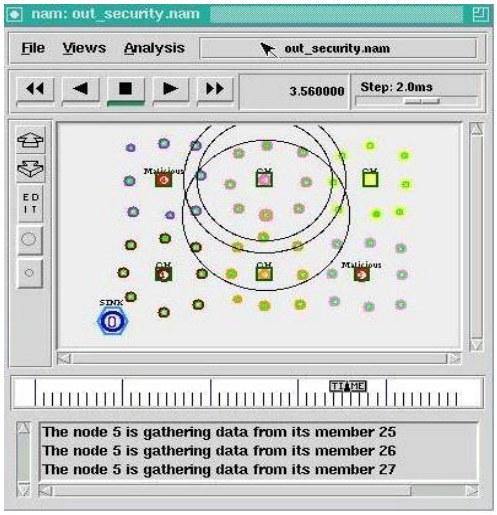


Fig 2

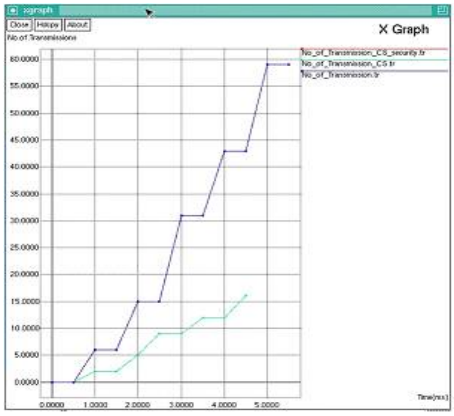


Fig 3

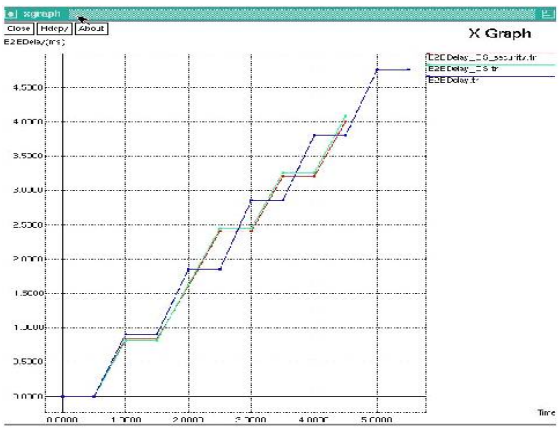


Fig 4

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 11, November 2016

VII. CONCLUSION AND FUTURE SCOPE

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

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.

BIOGRAPHY

Tabitha V received Bachelor's degree in Electronics and communication engineering from Intell engineering college, Anantapur and pursuing Master's degree in Digital Systems and Computer Electronics in BIT Institute of Technology, Hindupur affiliated to JNTU ,Anantapur, AP

Mr. Ch. Sudarsan Raju received Bachelor’s Degree in Electrical and Electronics Engineering from SJMIT, Chitradurga, Karnataka and Master’s degree in Digital Systems and Computer Electronics from JNTU, Anantapur. He is a life time member of Indian Society for Technical Education (ISTE).He is also a life time member of IMAPS. He is currently working as Associate Professor with Department of Electronics and Communication Engineering in BIT Institute of Technology, Hindupur. His research interests include wireless networks and Vehicular Ad Hoc and Sensor Networks.