ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 11, November 2016

An Efficient Secure and Delay Aware Routing Protocol for VANETs

R. Jeevitha
Research Scholar
Dept of computer science,
Kaamadhenu Arts and Science College,
Sathy, Tamilnadu

Mrs. M .Bhuvaneswari.,
Assistant Professor,
Dept of computer science,
Kaamadhenu Arts and Science College,
Sathy, Tamilnadu

Abstract

Most security- and privacy-preserving protocols in vehicular ad hoc networks (VANETs) heavily rely on time-consuming cryptographic operations which produce a huge volume of cryptographic data. These data are usually employed for many kinds of decisions, which poses the challenge of processing the received cryptographic data fast enough to avoid unaffordable reaction delay. With the present era of Vehicular Communication, a Vehicular ad-hoc network (VANET) is facing problem with vehicle anonymity and location privacy while communicating among the vehicle. To overcome that Vehicular Public Key Infrastructure using Multi-Constrained QOS aware Routing Algorithm has been used. Security becomes very important for VANET considering the criticality of safety application. The proposed model which contains two phases are delay time calculation and communication phase for transferring secure message. The delay aware routing protocol, which is based on the ad - hoc distance vector (AODV) routing protocol. The proposed system using elliptic curve cryptography algorithm it guarantees trustworthiness of vehicular communications and privacy of vehicles, and enables vehicles to react to vehicular reports containing cryptographic data within a very short delay. The proposed a mechanism in order to provide secure and efficient communication in VANET environment. We overcome the drawbacks of the existing system by using secure elliptic curve cryptography (SECC). The proposed algorithms, malicious messages are identified. It also detects the accident and other problems in the path of the vehicles.

***Index Terms*- AODV, Communication phase, Delay time calculation, Malicious messages, QOS, SECC.**

I. INTRODUCTION

Thousands of people around the world die every year in road accidents and many more are severely injured. Implementations of safety information such as speed limits and road conditions are used in many parts of the world but still more work is required. Vehicular Ad Hoc Networks (VANET) is used to collect and distribute safety information to massively reduce the number of accidents by warning drivers about the danger before they actually face it. VANET comprise of entities such as sensors and On Board Units (OBU) installed in the car as well as Road Side Units (RSU). The data collected from the sensors on the vehicles can be displayed to the driver, sent to the RSU or even broadcasted to other vehicles depending on its nature and importance. The RSU distributes this data, along with data from road sensors, weather centers, traffic control centers, etc. to the vehicles and also provides commercial services such as parking space booking, Internet access and gas payment. The network makes extensive use of wireless communications to achieve its goals but although wireless communications reached a level of maturity, a lot more is required to implement such a complex system.

Information dissemination using DSRC is quite attractive due to the large bandwidth and the possibility of using multiple channels. The IEEE standards propose employing multiple 10 MHz channels, each capable of carrying 27 Mbps of data for vehicular communications. Up to seven channels are available in the 5.9 GHz bands and one channel is supposed to be dedicated for safety applications. The remaining channels could potentially be used for content distribution and delivery. In this section, describe the different types of information that need to be disseminated in a vehicular network and the methodologies that have been considered in the research literature.

One of the key issues in all of these frameworks is how to identify efficient paths that can satisfy the given QOS constraints, commonly known as the QOS-based routing problem. Multi-constrained path selection, with or without optimization, is an NP-complete problem that cannot be exactly solved in polynomial time. Towards security issue, the attention of researchers and manufacturers are very less in comparison with other issues. Information in VANET are exchanged in the form of packets which involve life critical messages so it is necessary to secure that these messages should not altered and neither inserted through the attackers, furthermore the obligation of vehicle drivers should be made up that they advise the environment of traffic within time with effectively. The issues in security of VANET are not similar to communication network. The extent of network, versatility, geographic pertinence and soon build the installation difficult and particular from another network security.

The main aim is to design a model for delay aware routing and secure communication in VANET. The proposed a model which contains two phases of delay time calculation and communication phase for transferring secure message. The delay aware routing protocol, which is based on the ad - hoc distance vector (AODV) routing protocol. The secure communication based on ECC for the registration phase which provide public and private key to the vehicle and in

communication phase use ECC (Elliptic Curve cryptography), by which we generate a shared secret key which used for communication between vehicles. The model which propose requires less communication and computational costs. The delay aware routing protocol that addresses these challenges forwarding packets with low latency, high reliability and fast progress toward destination.

II. Related Work

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 too 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.

A cross-layer protocol called coordinated external peer communication (CEPEC) for Internet-access services and peer communications for vehicular networks. We assume that IEEE 802.16 base stations (BS) are installed along highways and that the same air interface is equipped in vehicles. Certain vehicles locating outside of the limited coverage of their nearest BSs can still get access to the Internet via a multi-hop route to their BSs.

An important property of multidimensional routing is that a nonlinear length function is required to obtain exact results. QoS routing algorithms that use a linear definition for the path length will only prove useful when the link weights are positively correlated. In all other cases a nonlinear function is necessary, which significantly complicates the problem, since no simple shortest path algorithm is available to minimize such a nonlinear function. As a consequence, multiple paths must be evaluated, requiring the use of a k-shortest path algorithm. The other important techniques are non-dominance, look-ahead, search-space reducing, rounding and scaling the weights, and the constraint values themselves.

The algorithm constructs paths starting at the source and going towards the destination. But, at each iteration, the algorithm gets rid of all paths that are guaranteed to violate the constraints, thereby keeping only those partial paths that have the potential to be turned into feasible paths, from which the optimal paths are drawn. The choice of which path to be extended first and which path can be pruned depend upon a projected path cost function, which is obtained by adding the cost already incurred to get to an intermediate node to an admissible cost to go the remaining distance to the destination. The Dijkstra's shortest path algorithm is a good choice to give a good admissible cost.Novel self-organizing approach for routing datagrams in ad hoc networks, called Distributed Ant Routing (DAR). This approach belongs to the class of routing algorithms inspired by the behavior of the ant colonies in locating and storing food. The effectiveness of the heuristic algorithm is supported by mathematical proofs and demonstrated by a comparison with the well-known Ad hoc On Demand Distance Vector (AODV) algorithm.

The strong privacy preservation (PASS), for vehicular communications. Unlike traditional pseudonymous authentication schemes, the size of the certificate revocation list (CRL) in PASS is linear with the number of revoked vehicles and unrelated to how many pseudonymous certificates are held by the revoked vehicles. PASS supports the roadside unit (RSU)-aided distributed certificate service that allows the vehicles to update certificates on road, but the service overhead is almost unrelated to the number of updated certificates.

The IAQR algorithm introduces a routing modeling with four QoS constrained requirements associated with nodes or links, and defines four rules besides congestion avoidance rule. The algorithm can find a route in ad hoc networks that satisfies more QoS requirements of the incoming traffic and at the same time reduces constrained resources consumption as much as possible. The multi-QoS routing metric (AntSensNet) is proposed. The AntSensNet protocol builds a hierarchical structure on the network before choosing suitable paths to meet various QoS requirements from different kinds of traffic, thus maximizing network utilization, while improving its performance. In addition, AntSensNet is able to use a efficient multi-path video packet scheduling in order to get minimum video distortion transmission. Finally, extensive simulations are conducted to assess the effectiveness of this novel solution and a detailed discussion regarding the effects of different system parameters is provided.

The vehicular security through reputation and plausibility checks to address the most important issue of security in VANETs. The algorithm provides security against the attacks of event modification, false event generation, data aggregation and data dropping. It performs not only detection but also the isolation of malicious nodes in the network. It employs sensors in a reputation-based system and presents a very robust yet cost efficient approach as it utilizes just vehicle to vehicle communication, thereby reducing the security issues and cost associated with the roadside infrastructure. The aim of the DeReQ algorithm is to find a route which is not only reliable but also compliant with delay requirements. We evaluate the performance of DeReQ algorithm through simulations and our simulation results demonstrate that significant performance improvement can be achieved by the combined DeReQ and AODV protocol in comparison to the original AODV protocol, an QoS-extended AODV protocol (AAC), and the location-based routing protocol (LBM).

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.

III. Proposed Approach

Security in routing is an important issue in vehicular ad hoc network (VANET) to protect the valuable information. 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. However, this intelligent transportation system (ITS) services provided by VANET are affected by the malicious vehicles. The proposed a method to secure ad hoc on-demand distance vector (AODV) routing protocol. The proposed method provides security for routing packets and can efficiently prevent the attacks. The secure safety message data dissemination in vehicle to vehicle (V2V) communications using elliptic curve cryptography. The safety applications aim at avoiding vehicular accidents by using secure broadcast vehicle-to-vehicle (V2V) communications. The Security mechanism used for authenticating broadcast V2V messages comes with overhead in terms of computation and communications. It also detects the accident and other problems in the path of the vehicles. Elliptic Curve Cryptography (ECC) algorithm is used for stronger security during communication. Extensive simulation and experimental analyses demonstrate the security and efficiency of delay aware ECC in terms of privacy-preserving and low authentication delay.

A. Network Model

Let us consider a VANET composed of a large number of vehicles V = {V1, V2, ...} and a spot of roadside units (RSUs) R = {R1,R2, ...},. In the VANET, each vehicle Vi, V has a unique nonzero identifier and moves from one place to another either along a fixed route (e.g., bus) or by choosing a dynamical path (e.g., taxi), while each RSU Rj _ R is placed at some critical locations Lj in the area. The communications between vehicle and vehicle are bidirectional, i.e., two vehicles within the transmission range TV can communicate with each other. However, since RSU's transmission range TR is larger than TV, the communication between vehicle and RSU is not entirely bidirectional. Assume that the distance between vehicle Vi and RSU Rj is D = |Vi − Rj |. When TV < D ≤ TR, only Vi can detect the existence of Rj ; when 0 ≤ D ≤ TV , Vi and Rj can communicate with each other.

B. Mobility Model

One key component of VANET simulations is the mobility pattern of vehicles, also called the mobility model. Mobility models are used to determine the location of nodes in the topology at any given instant, which strongly affects network connectivity and throughput. The current mobility models used in popular wireless simulators such as NS-2 tend to ignore real-world constraints such as street layouts and traffic signs. For example, the widely used Random-Waypoint Model (RWM) assumes that nodes move in an open field without obstructions. In contrast, the layout of roads, intersections with traffic signals, buildings, and other obstacles in urban settings constrain vehicular movement. The shortcomings of RWM are widely recognized and there has been recent research interest in modeling" realistic" mobility patterns specifically targeted for VANETs. Each of these works captures different levels of simulation. Vehicles cannot disregard physical constraints posed by the presence of streets and nearby vehicles. Every vehicle's movement is influenced by the movement pattern of its surrounding vehicles. For example, a vehicle needs to maintain a minimum safe distance from the one in front of it, increase or decrease its speed, or change to another lane to avoid congestion.

C. Secure Communication Algorithm

Propose an elliptic curve digital signature algorithm (ECDSA) based message authentication in a VANET. The operation sequence of the proposed scheme is as follows: 1) Source vehicle generates private key and public key. 2) Public key is made available to all the vehicles in the VANET. 3) Source vehicle creates a hash of the message using secured hash algorithm. 4) Secured has his encrypted using private key in the source vehicle and ends it to the destination vehicle. 5) At the destination vehicle, the received encrypted message is decrypted using the public key. The result of the decryption will be the hash of the message. 6) Destination vehicle can then hash the message in the same way as source vehicle did and compare the two hashes. Using this proposed scheme, strong authentication policy is provided for the destination vehicle.

The most important thing defines all the elements in the elliptic curve before used by all the parties. That is called as the domain parameters of the scheme. Let p be the field in the prime case and the pair (m, f) in the binary case. The elliptic curve is defined by the constants a and b use in elliptic curve equation. And the order of G, be the smallest non-negative number n such that nG=∞, it is prime. Since is the size of a subgroup of E (FP) follows from Lagrange's theorem that the number H= | E (FP) | is an integer. In cryptographic applications h, called the cofactor, must be small (H ≤) and, preferably h=1. The prime case the domain parameters are (p, a, b, N, g, h) and in the binary case they are (M, P, a, b, n, G,h).

Encryption using ECC

Sender „A" communicates to the receiver „B" by encrypting the data with public key of „B" which is known to all. Only „B" can decrypt the message with its private key. To encrypt and send a message Ym to B, A chooses a random positive integer k and produces the cipher text Cm by using B"s public key YB as shown below.

Cm = [k*G, Ym +k*YB]

Where G is a point on elliptic curve defined over the Galios Field Eq(a,b) whose order is a large value n.

Decryption using ECC

To decrypt the cipher text, B multiples the first point in the pair by B's private key nB and subtracts the result from the second point as shown by equation. Ym + k * YB - nB (k*G) = Ym+ k (nB* G) - nB (k*G) = Ym A key exchange between users A and B can be explained in following steps:

1. A selects a positive integer nA < n as A's private key. where n is a set of random numbers.
2. A generates a public key YA = nA * G which is a point in Eq(a, b).
3. B select an integer nB < n as B's private key.
4. B generates a public key YB= nB * G which is a point in Eq(a, b).
5. Public keys are exchanged between A and B. A generates the secret key k = nA * YB and B generates the secret key k = nB * YA

D. Delay aware Routing

AODV uses route discovery by broadcasting RREQ to all its neighboring nodes. The broadcasted RREQ contains addresses of source and destination, their sequence numbers, broadcast ID and a counter, which counts how many times RREQ has been generated from a specific node. When a source node broadcast a RREQ to its neighbors it acquires RREP either from its neighbors or that neighbor(s) rebroadcasts RREQ to their neighbors by increment in the hop counter. If node receives multiple route requests from same broadcast ID, it drops repeated route requests to make the communication loop free.

As in VANET, nodes (vehicles) have high mobility and moves with high speed. Proactive based routing is not suitable for it. Proactive based routing protocols may fail in VANET due to consumption of more bandwidth and large table information. AODV is a reactive routing protocol, which operates on hop-by-hop pattern. The Ad hoc On-Demand Distance Vector (AODV) algorithm enables dynamic, self-starting, multi-hop routing between participating mobile nodes wishing to establish and maintain an ad hoc network. AODV allows mobile nodes to obtain routes quickly for new destinations, and does not require nodes to maintain routes to destinations that are not in active communication. Route Requests (RREQs), Route Replies (RREPs), and Route Errors (RERRs) are the message types defined by AODV. In AODV routing, upon receipt of a broadcast query (RREQ), nodes record the address of the node sending the query in their routing table. This procedure of recording its previous hop is called backward learning. Upon arriving at the destination, a reply packet (RREP) is then sent through the complete path obtained from backward learning to the source. At each stop of the path, the node would record its previous hop, thus establishing the forward path from the source. The flooding of query and sending of reply establish a full duplex path. After the path, has been established, it is maintained as long as the source uses it. A link failure will be reported recursively to the source and will in turn trigger another query-response procedure to find a new route.

The ETX (Estimated Transmission count) metric is calculated from the beacons that a node receives from its neighbors. The formula for ETX is, ETX = 1/D f * Dr . Df and Dr forward and reverse delivery ratios respectively. The mobility metric, say, speed is assigned as a weight to a link and along with the ETX value it is coded. In order to reduce packets transmission delay, the proposed delay-aware routing. Once a node received a RREP packet, the node first checks whether it has a routing table to the destination node. If the routing table exists, the node will calculate a new transmission cost between the destination node and itself base on formula (1). The new path cost will compare to the old routing path cost. A path with less cost represents the lower transmission delay, and the sender will select the path with less cost as a new routing path.

IV. Experimental Results

In addition to Manhattan Street scenario, we also evaluate the proposed AODV protocol in a real city. In all scenarios considered, the source of message (i.e., the scene of accident) is located at the intersection approximately at the center of the network. The message source broadcasts a message only once at time t = 1000 seconds and the simulation ends two minutes after the source broadcasts the message. The region of interest is assumed to be a 1 km x 1 km area around the scene of accident. Two transmission ranges are used: 250 and 140 meters for Line-Of-Sight (LOS) and Non-LOS communication ranges, respectively.

1) Throughput: It is the amount of data per time unit that is delivered from one node to another via a communication link. The throughput is measured in Packets per unit TIL or bits per TIL. TIL is Time Interval Length. More is the throughput of sending and receiving packets better is the performance. Lesser is the throughput of dropping packets better is the performance.

2) Average throughput: It is the average of total throughput. It is also measured in Packets per unit TIL or bits per TIL.

3) Packet Drop: It shows total number of data packets that could not reach destination successfully. The reason for packet drop may arise due to congestion, faulty hardware and queue overflow etc. Lower packet drop rate shows higher protocol performance.

4) Packet size: Size of packets in bytes.

5) Average simulation End to End delay (End2End delay): This metric gives the overall delay, from packet transmission by the application agent at the source node till packet reception by the application agent at the destination node. Lower delay shows higher protocol performance.

The following equation is used to calculate the average end-to-end delay, Average End to End Delay = (T_DataR – T_DataS), Where T_DataR = Time data packets received at destination node T_DataS = Time data packets sent from source node. The end to end delay is important metrics because VANET needs a small latency to deliver quick messages. It shows the suitability of the protocol for the VANET.

6) Simulation time: Total time taken for simulation. It is measured in seconds.

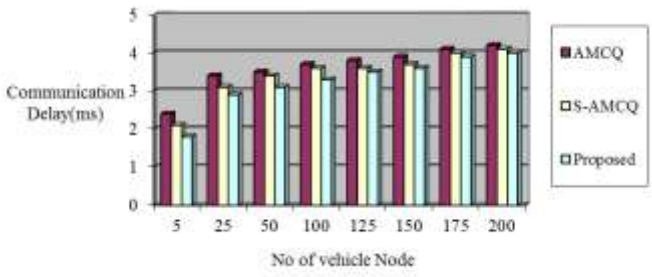

Fig. 1.1 Comparison of Communication Delay

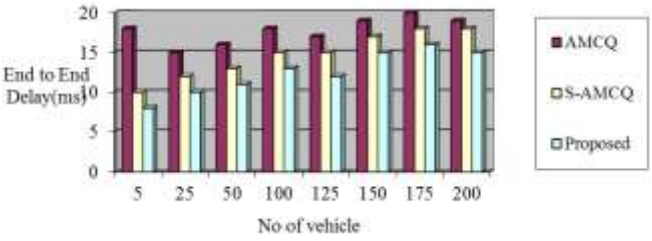

Fig. 1.2 Comparison of End-to-End Delay

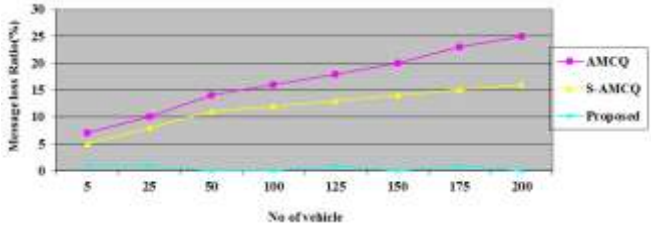

Fig. 1.3 Comparison Message loss ratio

V. CONCLUSION

Intelligent transportation systems could improve transportation safety, driving assistance and traffic management system. Vehicular Ad hoc Network (VANET) is an emerging field of technology, embedding wireless communication networks into vehicles to achieve intelligent transportation systems. The development of such systems pose many unique challenges like designing routing protocols that not only forward packets with good end to end delay but also take into consideration the reliability and progress in data packets forwarding. QoS aware routing protocols can serve to the QoS support, which concentrate on determining a path between source and destination with the QoS requirements of the flow being satisfied. Communication delay of a packet across an ad hoc network is the latency consumed by a packet to reach the destination from the source. The components of end-to-end latency of a packet at the network layer are processing delay, packetization delay, transmission delay, queuing delay and the propagation delay. The proposed system delay aware secure packet sending based om cryptography scheme ECC homomorphic encryption is applied for secure data transmitting from source to the destination.

REFERENCES

[1] K. Yang, S. Ou, H. Chen, and J. He, "A multihop Peer-communication Protocol with farines guarantee for IEEE 802.16-based vehicular networks," IEEE Trans. Veh. Technol., vol. 56, no. 6, pp. 3358–3370, Nov. 2007.

[2] M. Curado and E. Monteiro, "A survey of QoS routing algorithms,"in Proc. Int. Conf. Inform. Technol., Istanbul, Turkey, 2004,pp. 43–46.

[3] B. Zhang, J. Hao, and H. T. Mouftah, "Bidirectional multi-constrainedrouting algorithms," IEEE Trans. Comput., vol. 63, no. 9,pp. 2174–2186, Sep. 2014.

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

[5] G. Liu and K. G. Ramakrishnan, "A* prune: An algorithm for findingk shortest paths subject to multiple constraints," in Proc. IEEE20th Annu. Joint Conf. IEEE Comput. Commun. Soc., Anchorage,AK, USA, 2001, vol. 2, pp. 743–749.

[6] T. Korkmaz and M. Krunz, "Multi-constrained optimal pathselection," in Proc. IEEE 20th Ann. Joint Conf. IEEE Comput. Commun.Soc., Anchorage, AK, USA, 2001, vol. 2, pp. 834–843.

[7] L. Rosati, M. Berioli, and G. Reali, "On ant routing algorithms inad hoc networks with critical connectivity," Ad Hoc Netw., vol. 6,no. 6, pp. 827–859, Aug. 2008.

[8] M. H. Eiza and Q. Ni, "An evolving graph-based reliable routingscheme for VANETs," IEEE Trans. Veh. Technol., vol. 62, no. 4,pp. 1493–1504, May 2013.

[9] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, "An efficient pseudonymousauthentication scheme with strong privacy preservation forvehicular communications," IEEE Trans. Veh. Technol., vol. 59,no. 7, pp. 3589–3603, Sep. 2010.

[10] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditionalprivacy preservation protocol for secure vehicular communications," in Proc. 27th Conf. IEEE Comput. Commun.,Phoenix, AZ, USA, 2008, pp. 1903–1911.

[11] M. Riley, K. Akkaya, and K. Fong, "A survey of authentication schemes for vehicular ad hoc networks," Security Commun. Netw.,vol. 4, no. 10, pp. 1137–1152, Oct. 2011.

[12] H. Shokrani and S. Jabbehdari, "A novel ant-based QoS routing for mobile Ad Hoc networks," in Proc. 1st Int. Conf. Ubiquitous Future Netw., Hong Kong, Jun. 2009, pp. 79–82.

[13] M. Liu, Y. Sun, R. Liu, and X. Huang, "An improved ant colony QoS routing algorithm applied to mobile Ad Hoc networks," in Proc. Int. Conf. Wireless Commun., Netw. Mobile Comput., Shanghai, China, Sep. 2007, pp. 1641–1644.

[14] K. Kunavut and T. Sanguankotchakorn, "Multi-constrained path (MCP) QoS routing in OLSR based on multiple additive QoS metrics," in Proc. Int. Symp. Commun. Inform Technol., Tokyo, Japan, Oct. 2010, pp. 226–231.

[15] L. Cobo, A. Quintero, and S. Pierre, "Ant-based routing for wireless multimedia sensor networks using multiple QoS metrics," Comput. Netw., vol. 54, no. 17, pp. 2991–3010, Dec. 2010.

[16] N. Kumar, R. Iqbal, N. Chilamkurti, and A. James, "An ant based multi constraints QoS aware service selection algorithm in wireless mesh networks," Simul. Modelling Practice Theory, vol. 19, no. 9, pp. 1933–1945, Oct. 2011.
[17] O. A. Wahab, H. Otrok, and A. Mourad, "VANET QoS-OLSR: QoS-based clustering protocol for vehicular ad hoc networks," Comput. Commun., vol. 36, no. 13, pp. 1422–1435, Jul. 2013.
[18] E. Fonseca and A. Festag, "A survey of existing approaches for secure ad hoc routing and their applicability to VANETs," NEC Network Laboratories, Heidelberg, Germany, NEC Tech. Rep. NLE-PR-2006–19, 2006.
[19] L. Chen, S. Ng, and G. Wang, "Threshold anonymous announcement in VANETs," IEEE J. Select. Areas Comm., vol. 29, no. 3, pp. 605–615, Mar. 2011.
[20] V. Daza, J. Domingo-Ferrer, F. Sebe, and A. Viejo, "Trustworthy privacy preserving car generated announcements in vehicular Ad Hoc networks," IEEE Trans. Veh. Technol., vol. 58, no. 4, pp. 1876–1886, May 2009.
[21] Q. Li, A. Malip, K. M. Martin, S.-L. Ng, and J. Zhang, "A reputation-based announcement scheme for VANETs," IEEE Trans. Veh. Technol., vol. 61, no. 9, pp. 4095–4108, Nov. 2012.
[22] S. K. Dhurandher, M. S. Obaidat, A. Jaiswal, A. Tiwari, and A. Tyagi, "Vehicular security through reputation and plausibility checks," IEEE Syst. J., vol. 8, no. 2, pp. 384–394, Jun. 2014.
[23] Z. Niu, W. Yao, Q. Ni, and Y. Song, "DeReq: A QoS routing algorithm for multimedia communications in vehicle Ad Hoc networks," in Proc. Int. Conf. Wireless Commun. Mobile Comput., Honolulu, HI, USA, Aug. 2007, pp. 393–398.
[24] G. Mao and B. D. O. Anderson, "Graph theoretic models and tools for the analysis of dynamic wireless multihop networks," in Proc. IEEE Wireless Comm. Netw. Conf., Budapest, Hungary, Apr. 2009, pp. 1–6.
[25] A. Vinel, V. Vishnevsky, and Y. Koucheryavy, "A simple analytical model for the periodic broad casting in vehicular Ad-Hoc networks," in Proc. IEEE Globecom Workshops, New Orleans, LO, USA, Nov./Dec. 2008, pp. 1–5.