A secure intersection-based routing protocol for data collection in urban vehicular networks

Tarek Bouali, El-Hassane Aglzim, Sidi-Mohammed Senouci

A Secure Intersection-Based Routing Protocol for Data Collection in Urban Vehicular Networks

Tarek Bouali, El-Hassane Aglzim and Sidi-Mohammed Senouci
DRIVE Labs, University of Burgundy, Nevers, France
Email:{tarek.bouali, el-hassane.aglzim, Sidi-Mohammed.Senouci}@u-bourgogne.fr

***Abstract*—Data routing has gained great intention since the appearance of Vehicular Networks (VANETs). However, in the presence of attackers, reliable and trustworthy operations in such networks become impossible without securing routing protocols. In this paper, we target to study and design a secure routing protocol S-GyTAR for vehicular environments. Several kinds of routing techniques are proposed in the literature and could be classified into topology-based or position-based strategies. Position-based is the most investigated strategy in vehicular networks due to the unique characteristics of such networks. For this reason, this work is based on the well-known intersection-based routing protocol GyTAR, which exploits the greedy forwarding technique to relay data. In fact, we benefit from GyTAR's characteristics and reshape it to introduce a new distributed trust management strategy to secure routing. We design a cluster-based mechanism to monitor nodes and a reputation-based schema to evaluate the vehicles and classify them. We evaluate our proposal using NS3 simulator. Simulation results show high performances regarding the detection rate of malicious nodes and overhead with an amelioration of the end-to-end communication delay in the presence of malicious vehicles.**

***Index Terms*—VANET - Routing - Security - Clustering - Reputation - Monitoring**

I. Introduction

Vehicular Ad hoc Networks are witnessing a tremendous evolution due to the race between cars manufacturers' to the deployment of the most recent technologies in their design, which promises great improvements for the human life and makes the vehicular environment an open area for research and innovations. Thanks also to the increasing availability of navigation systems, embedded sensors and newly standardized communication technologies, modern vehicles can now feel, see and speak, creating the new concept of C-ITS (Cooperative Intelligent Transport Systems and Services). Using both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, C-ITS will enable cooperation between vehicles and road infrastructure in order to achieve improvements in the areas of safety, mobility, and environment. This cooperation is based on the principle that all parties (vehicles, road side units, etc.) exchange information and makes use of them afterward to offer new services (real-time traffic information, improved road safety, etc.). However, the development of this technology creates new challenges and questions: how to collect and exchange these information in such highly dynamic network? and how to secure the communication between all the parties? In fact, security remains a weak link in these wireless networks since they are by nature vulnerable to various types of attacks (spoofing, Denial of Service - DoS, etc.). This security problem is due to the lack of infrastructure for the authentication and also the fact that all vehicles are equivalent and should play the role of routers in order to exchange data between all parties, which is necessary for a proper functioning of the network. Hence, in the presence of attackers, reliable and trustworthy operations of such networks become impossible without securing routing protocols. For this reason we target, in the actual work, to build a secure protocol to support data routing and face threats. In fact, hundreds of protocols and strategies were proposed to support data delivery from one moving node to specific zone or to another node. Topology-based routing and position-based routing are two main categories that classify the forwarding strategies in a multi-hop wireless network. However, the use of tracking technologies in new commercialized vehicles has improved the quality of position-based routing protocols and made them more efficient and convenient to VANETs then topology-based. VANET security is also treated using several methods that could be classified into two categories: distributed strategies where authentication is managed by vehicles and centralized strategies where a central authority manages and distributes keys. Till now, these two cryptographic mechanisms have been used extensively to ensure the authentication and privacy of the communication, i.e. data confidentiality. They are very useful to prevent an external attacker to corrupt the ongoing communication but they cannot prevent internal attacks coming from authenticated nodes. Intrusion Detection Systems (IDSs) with a periodic evaluation of the vehicles behavior seems to be a promising solution since they prove their efficiency in protecting the network against both internal and external attacks.

Therefore, we aim to consider a completely decentralized and real time evaluation of the traffic to identify malicious nodes and exclude them from the candidates' list of data forwarders. In fact, we based our work on the well-known position-based protocol, GyTAR[9], previously designed within the team. We benefit from its consideration to the real-time traffic and reshape it to continuously monitor vehicles to secure the routing. We consider, in this paper, the trustworthiness of a node to define its sociability and eligibility to forward a packet. So, we firstly introduce the trustworthiness calculation and after we define its impact on the network organization. Simulation results prove the rigidity of our protocol regarding its end-to-end communication delay,

its detection rate of malicious nodes and generated overhead.

The remainder of this paper is structured as follows: Section II gives an overview about routing strategies in VANETs and some trust management techniques in the literature. Section III presents the monitoring technique and forwarder selection. Section IV gives a case study to evaluate the performance of the protocol with some discussions. Section V concludes this paper.

II. Related Work

This section is organized into two subsections. In the first one, we classify and summarize some routing protocols designed to work in a vehicular environment. In the second one, we present various techniques proposed to face internal attacks and identify attackers.

A. Vehicular Routing Protocols for VANET

Data routing in a dynamic network is one of the most difficult treated fields since the appearance of wireless networks due to the frequently changing topology and the node's movement. Several works are proposed either topology or position based in the area of MANET where the position-based strategies perform better than topology-based ones [1]. Regarding the unique characteristics of VANET, position-based strategies seem to be the most convenient for routing in such kind of environments, but the protocols developed for MANET may not be directly applied for them. Several variants of position-based concept were proposed for data forwarding in vehicular environment which could be classified into three categories: (i) directional flooding or dissemination, (ii) hierarchical forwarding and (iii) greedy forwarding.

Broadcast and dissemination protocols are widely deployed in vehicular networks with several variants of techniques to alleviate the overhead. The main difference between the proposed protocols is the selection of the packet forwarder. Several broadcast protocols based on directional flooding are proposed to support data forwarding while limiting the overhead [15][12][14]. Among these, DHVN (Dissemination Protocol for Heterogeneous Cooperative Vehicular Networks)[14] exploits the vehicles with bigger radio range and height to relay a packet to a specific area. The basic idea of this work is that each node receiving a packet triggers a timer, inversely proportional to the sum of its height and range, which means that the higher node with bigger radio range will firstly forward the packet. UMB (Urban Multihop Protocol)[13], another dissemination protocol, basically benefits from the RTB/CTB (the same principle as RTS/CTS in CSMA) to choose the farthest node as a packet forwarder. In an urban area the protocol considers the topology and assumes the existence of special fixed stations called repeaters at every intersection to relay traffic to all directions. AMB (Ad hoc Multihop Broadcast protocol) [12] is a completely distributed version of UMB where the role of repeaters is delegated to vehicles within intersections due to the availability of their coordinates to each node based on a preloaded map of the roads topology. Unlike dissemination protocols, hierarchical strategies are based on decentralized or centralized self-organized clusters where a cluster head (CH), which could be a central unit or a mobile node, collects, manages and forwards data from all its affiliated cluster members. TrafficGather[2] benefits from the network organization into cluster spaces to gather and enable data exchange between nodes. It is a completely decentralized architecture, but it is not very suitable in a sparse network and it engenders an important overhead because it is based on a flooding algorithm. In [16], [17] and [5] a hybrid architecture is proposed for network organization and data forwarding. They are almost based on the same idea but with different techniques where the network is organized into clusters managed by either an RSU or a base station (BS) and the data is chained from one CH to another in a multi-hop way.

Thanks to navigation systems availability, greedy forwarding becomes very investigated in VANETs as a kind of position-based routing. Using this strategy, a node forwards the packet to the neighbor located closer to the destination. Many protocols are proposed supporting the greedy forwarding[10] [18] [6]. In [9], authors introduce a new position-based routing protocol named GyTAR. They propose an ameliorated greedy protocol to route data between two moving nodes where decision about the route to choose is made in intersections. The proposed work assumes that vehicles are equipped with localization systems and capable to know the position of a destination based on preloaded maps. GyTAR is designed to work in urban areas and its real innovation is that it takes into account information about the real-time traffic in each road segment. In fact, the protocol is composed of two main phases: the first one is the collection of information about traffic and roads densities and the second one is the routing decision. For the first phase, the authors designed a cluster-based technique to gather information about each road density where each segment is divided into small cells that each of them encompasses a one-hop cluster leaded by a cluster head (CH). This cluster head counts its neighbors to later include their number in a so-called CDP (Cells Density Packet) packet generated by a CH when it reaches an intersection and sent in backward from CH to CH until reaching the previous intersection. The second phase starts when a CDP packet reaches the anterior intersection where a weight is calculated for each road regarding its density and the distance between the next intersection and the final destination. After that, each node that reaches the intersection holding a packet should take a decision about the road the packet will follow based on their weights. Authors also take into account the case of intermittent connectivity by using the Carry and Forward (C&F) technique. In [11] (Fuzzy-assisted social-based routing for urban vehicular environments), a new alternative of routing is investigated which combines the greedy forwarding with a social criterion to choose the next forwarder. It takes the advantage of social behavior of humans in the road to design a routing protocol based on friendship relations between vehicles. In the protocol, authors aim to build a trusted community of friends to ease and secure the routing.

As said previously, we choose to base our work on GyTAR protocol for two reasons: the first is that it is based on real-time information about the traffic to make routing decisions and the second is the deployed cluster-based architecture for information gathering that we decide to use for the integration of our intrusion detection system.

B. Trustworthiness Management

Due to the continuous interaction and information exchange with other nodes, one vehicle could be exposed to potential attacks either from its authenticated neighbors in the same network or from external agents. Keys management could identify external attackers but not authenticated ones. Various kinds of internal attacks are identified in the vehicular environment and are classified as follows: Resource exhaustion, Packet Alteration, Packet dropping... But some works group all of them in the so-called Denial-of-Servie (DoS) attack.

Several techniques are proposed in the field and are based on the trustworthiness evaluation of vehicles in a distributed way. Three categories of trust modeling could be identified: entity-oriented, data-oriented and hybrid models. [3] and [19] propose a trust modelling technique for message relay control and local action decision making. It aims at establishing co-operation between vehicles to make decisions about messages using opinions. A cluster-based architecture is used to collect opinions of all cluster members about a generated message and two types of decisions are made: one is based on the vehicle's own experience with the monitored node and the other based on aggregated opinions in the received message. The two decisions are later combined to define the behavior of the message generator.

In [4], authors propose a trust management technique for the encounter-based routing in delay tolerant networks (DTN). In fact, one node i exchanges its encounter history of all the nodes it has met till now at every meeting, after that it calculates the trust of each forwarder candidate using different criteria to choose the next eligible node to forward data. In[7], the authors introduce a Markov model to manage the trustworthiness of nodes where the trust is modeled by a finite state machine with n states and each state represents a trust value. However, they settle for an analytical study without any application to a specific scenario.

III. Secure Intersection-Based Routing

The main concern of this work is to secure data exchange between moving nodes in a completely mobile network that does not contain any of the known infrastructure such as RSU or EnodeB. Therefore, a new distributed technique able to monitor the network members periodically is proposed. It is based on a cluster hierarchy where a cluster head evaluates its neighbors behavior based on a trust model, identifies attackers and alerts other nodes in the network. In the following we detail the monitoring, the network organization and the routing techniques each in a subsection.

A. Reputation & Trust Modeling

Nodes in the network are judged regarding their behavior and interactions. This behavior is translated to a quantitative criterion to enable the evaluation. A metric named trust value is introduced to model the trustworthiness degree of each node that can vary according to its reaction in the road. We highlight in this subsection the trust value calculation of each node in the network.

A cluster-head in the network maintains a trust value for each one-hop neighbor. It is always listening to its neighbors generated traffic to update their associated trust values. At the first time a new vehicle enters to its range, it is considered trustworthy and an initial trust value equal to 1 is associated to it. After that, this value is updated according to its behavior. Let's denote T_{ij} the trust value built by a cluster-head i for a node j. The CH captures all the traffic generated by each neighbor in its radio range and periodically evaluates its trust value. After each evaluation, we could guess that one node either keeps its normal behavior or tries to attack. For this reason, we introduce a new metric that reflects the reputation of the node after each evaluation and used later to get the trust value. The reputation of a cluster head i to a node j at the n-th evaluation is denoted R^n_{ij} and is calculated as described in Eq.1.

$$R^n_{ij} = \begin{cases} \lambda * R^{n-1}_{ij} + (1-\lambda) * r^n_{i,j} & \text{if} \quad n > 1 \\ r^n_{i,j} & \text{if} \quad n = 1 \end{cases} \tag{1}$$

R^{n-1}_{ij} represents the reputation of node j calculated after n-1 evaluations and λ is a weighting factor between the latest evaluation and the previous ones. While $r^n_{i,j}$ is a note given by the cluster head i to the node j at the n-th evaluation and could be equal to -1 if the node behaves maliciously and equal to 1 if it acts normally.

Because we aim to face Denial-of-Servie (DoS) attack and more precisely the resource exhaustion, in the actual work, the main criterion we are using to evaluate the nodes is the number of generated packets at each host. Therefore, we define a threshold P_{th} to specify the highest number of packets a normal node could send during the monitoring period without being considered malicious. In fact, a CH maintains for each node an association to keep a track of its generated packets and compute them. At each evaluation the number of packets is compared to the defined threshold and two cases appear:

Case 1: If $Nb^{ij}_{packet} \geq P_{th}$, the node is punished and $r^n_{i,j} = -1$.

Case 2: If $Nb^{ij}_{packet} < P_{th}$, the node is compensated and $r^n_{i,j} = 1$.

Where Nb^{ij}_{packet} is the number of captured packets by CH i and generated by neighbor j.

When the reputation related to a node j is computed, a trust value (T_{ij}) varying between 0 and 1 is attributed to j based on Eq.2 where n is the number of evaluations.

$$T_{ij} = Max\{R_{ij}/n, 0\} \tag{2}$$

B. Periodic Gathering of Traffic Data & Routing

Data, in the network, is routed based on a geographic routing using a greedy forwarding mechanism. In fact and as stated above, the actual work is based on a previous routing mechanism namely GyTAR where the packet is forwarded intersection by intersection until it reaches its final destination. The selection of the next road segment where the packet should be sent is done based on a real time collection of information about roads densities. Data about traffic is gathered based on a cluster organization proposed in GyTAR. In this work, we propose to secure this mechanism as follows. Each segment is divided into small cells and the trustworthiest and nearest node to the center of a cell is chosen as a cluster-head to collect information about traffic. The trustworthy node is identified using a pre-processing phase at the beginning of the network organization where all nodes in a cluster are mutually monitoring for a period of time to get an initial idea about the trust level of each vehicle. This pre-processing phase leads, therefore, to the choice of the node with the highest trust level to monitor nodes within the cell. After the choice of the first CH the maintenance of the architecture and the swapping of CHs would be simple as this one knows about all the trusts of its neighbors, it will directly choose the trustworthiest node to be a CH before getting out from the cell. The information in a cell (one-hop cluster) encompass the density of nodes in such a cluster and the trustworthiness of each node. Therefore, each cluster-head monitors its one-hop neighbors, identifies their reactions and behaviors regarding their packet generation rate and classifies them into two categories: normal and malicious vehicles. This classification is done based on the trust level value of each node calculated and updated based on previously described rules.

A cluster head in a cell maintains a list of its neighbors and associates with each one a trust value. It creates two types of lists: a black and a white list. The white list is used to store the neighbors identifiers that are normally behaving and trustworthy and the black list contains the nodes' identifiers that behave maliciously.

As the CH is always listening to the network, it evaluates the trustworthiness of every neighbor periodically as stated above. After each evaluation and trust level update, a node j is either considered trustworthy or malicious based on the following rules:

First case: If $T_{ij} \in [d,1]$ the node i is considered trustworthy and its identifier is stored in the white list.

Second case: If $T_{ij} \in [0,d[$ the node is classified malicious and stored in the black list to be after ejected from the network to not be used at any packet forwarding.

T_{ij} is the trust value calculated by the cluster head i for the node j and d is a maliciousness threshold indicating the tolerated limit value of trust to consider a node as trustworthy.

After the collection of information about its neighbors, their evaluation and classification, the CH calculates the density of its cluster by only counting the number of nodes contained in the white list. This strategy of calculation favours the roads with the minimum number of malicious nodes at the selection of the next intersection to which we have to route a packet at the routing phase. Fig.1 highlights the complete process of monitoring in a cluster and the information exchange between CHs to build a global overview about traffic in a road segment.

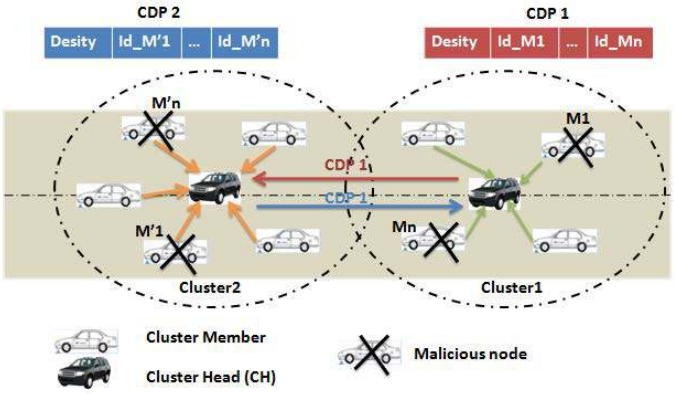

Fig. 1: The monitoring architecture

Upon the detection of malicious nodes, the CH should react in two ways: informs its one-hop neighbors about these nodes and warns the other clusters. For this reason, we use the so-called CDP packet defined in GyTAR. We reshape it to add information about monitored neighbors in each cell. The density of the cluster and the identifiers of nodes stored in the black list are fulfilled in this packet. The CDP is after diffused in the one-hop cluster and relayed by the farthest node in the radio range to the next cluster head. It is relayed hop by hop from one CH to another until it reaches the intersection. When a member in the cluster receives a CDP, it stores the contained identifiers of malicious nodes and ejects them from its routing table. However, when the packet reaches a CH it is treated in a different way. In fact, the CH firstly extracts the list of black nodes and stores them into its own black list, than it updates the packet by adding its cluster density and black list and finally it forwards it to the next CH and informs its neighbors about the new black list it has. When a CDP reaches an intersection, the forwarding and update mechanisms are stopped for two reasons: the first one is to limit the inundation of all the network by a big number of messages that could not be useful at a certain time because of the frequent change in the network topology and density and the second reason is that the information a CDP contains are really needed at the end of a segment because the routing decisions are made at each intersection. So, the node carrying a packet calculates the density of the segment from which it receives the CDP and stores black listed nodes. After the reception of the different CDPs from all underlying segments, a weight is calculated for each one by combining the white nodes density included in the packet and the distance of its next intersection from the destination (Eq.3) similar to [9]. Finally, and as in GyTAR the road with the highest weight value is chosen to forward the packet throw it.

$$Weight(j) = \alpha * f(D_k) + \beta * g(T_k) \quad (3)$$

Where $f(D_k)$ symbolizes the distance function of an intersection j from the destination of a packet and $g(T_k)$ is the density function of the segment ($\alpha+\beta=1$).

In the selected segment, a packet is routed based on the greedy forwarding technique where the selection of the next forwarder is based on the prediction of the next position of neighbors using their speeds, headings and directions. So, the farthest node of the packet carrier is chosen based on this predicted position. A recovery strategy is also provided to face intermittent connections and local optimums.

IV. Experimental Results

We implement our approach using NS3.17 simulator and we conduct simulations in a Manhattan Grid area of size 3000*3000m^2, composed of 9 intersections with a road length of 1000m. The different parameters of simulations are summarised in the table I. For the other parameters related to the calculation of the trust, we have fixed: $\lambda = 0.5$ and d=0.5. We firstly, analyze the capability of our proposed mechanism to detect malicious nodes, then, we highlight its impact on the end-to-end delay in a malicious environment and its generated overhead.

Parameter	**Value**
Simulation area	3000*3000m^2
Simulation time	400s
Road length	1000m
Number of vehicles	100 - 400
Speed	30 - 50 Km/h
Radio Range	250m
Monitoring period	5s
Pre-processing period	20s

TABLE I: Simulation parameters

Fig.2 highlights the variation of the detection rate of our proposed mechanism when the number of vehicles increases. In fact, we vary the number of malicious nodes between 10% and 40% for various densities (number of nodes between 100 to 400) and we analyze its impact on the capability of detecting malicious vehicles. Results show that our designed intrusion detection system (IDS) is able to detect all the malicious nodes when they are a little minority in the network (10% to 20%). We can also see that its performance decreases when this number increases (30% and 40%), but it stays capable of detecting above than 92% of the malicious nodes which is a very reasonable result when the number of vehicles in the network reaches 400. This decreasing in the detection rate is due to the tendency of malicious nodes to build false information and condemn normal nodes when their number become very important in the network which makes difficult for CHs to differentiate and get the right decisions. In general, our proposed work shows a very good accuracy in attacks detecting.

In Fig.3, we analyze the overhead generated by the proposed IDS compared to the basic routing protocol. In fact, we don't add any new packets to monitor and inform nodes about the black lists. The monitoring is done in a promiscuous mode

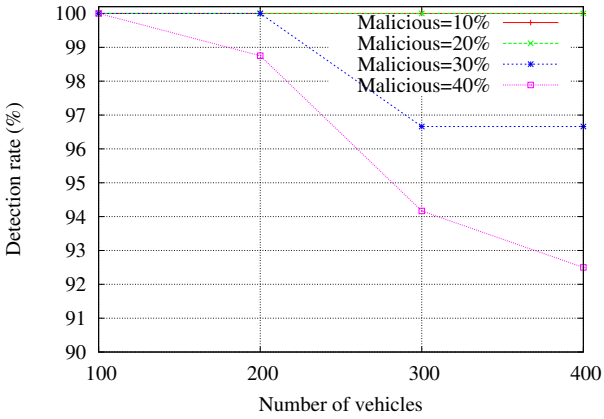

Fig. 2: The Detection rate

where one node is listening to its neighbors without any need to exchange more messages with them to count their reputations and update their trust levels locally. Therefore, the only generated overhead is due to adding black lists to the CDP packet and their update by each CH. So this overhead is relative to the number of detected malicious nodes. For this reason, we consider, in the plot, the worst case when the number of malicious nodes is very high (40% of the network) as the size of the black list would be the biggest one, which leads to the highest overhead. The given results show that our proposed mechanism only adds a little overhead compared to the basic protocol. However, the increasing of this overhead with the increase of the vehicles density is explained by the fact that the rate of generated control packets is proportional to the number of vehicles in the network.

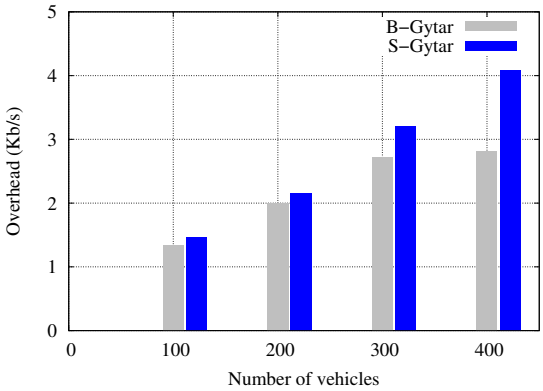

Fig. 3: The generated overhead

We, also, study the ability of our intrusion detection system (IDS) to limit the inundation of the network with packets sourced from the malicious vehicles as a malicious node tries to overload the bandwidth in a large region by flooding its packets in k hops to increase the end-to-end communication delay. So, this could impact the delivery of some packets as they are dropped at different layers if they are not received before a certain time limit. Fig.4 shows the difference between

end-to-end delays variations of a communication using a basic GyTAR (B-GyTAR) and our secure GyTAR (S-GyTAR) with the presence of 10% of attackers over the network.

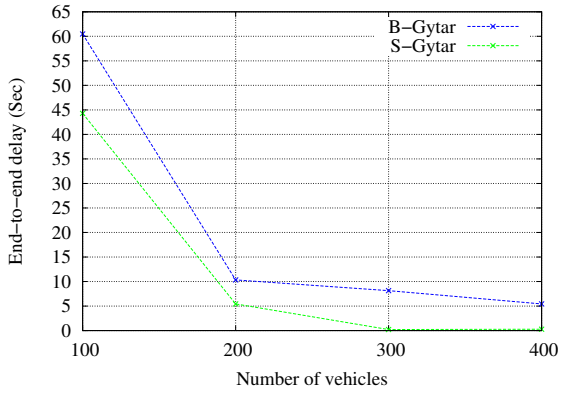

Fig. 4: The end-to-end communication delay

The given results prove the effectiveness of our proposed mechanism regarding the limitation of the end-to-end delay. Therefore, the mechanism stops the forwarding of packets issued from a detected malicious node which minimize the overload of the bandwidth from k hops to one hop and by consequence decrease the end-to-end communication delay.

V. Conclusion

Securing data routing in a vehicular environment is a very challenging field since vehicles are being always connected which make them vulnerable and usually exposed to various attacks. Several techniques based on authentication and keys management are proposed to secure routing in such frequently changing topologies. However, the proposed mechanisms are based on centralized architectures and infrastructure deployment. This made them inefficient face to some attacks, especially from authenticated vehicles. In this work, we propose a secure routing protocol, which we name S-GyTAR, based on a previous work named GyTAR designed within our teamwork. We have designed a cluster-based monitoring mechanism to evaluate vehicles behavior and eject malicious ones from the network. The network is organized into clusters each contained in a cell as the roads are divided into small cells. The trustworthiest and nearest node to the center of a cell is chosen as a cluster head. Its role is to monitor its neighbors and build a reputation model to calculate their trust levels, classify them and inform about malicious behaviors. Experimental results show its efficiency regarding its detection rate (more then 92% for 400 nodes). It doesn't, also, add an important overhead compared to the basic protocol and decreases the end-to-end communication delay in a non-confident environment. As future work, we aim to enhance the choice of CH and add a prediction mechanism to our proposed protocol.

Acknowledgment

This work has been funded by the Europeen project CarCoDe[8].

References

[1] Marwa Altayeb and Imad Mahgoub. A Survey of Vehicular Ad hoc Networks Routing Protocols. *International Journal of Innovation and Applied Studies*, 3(3):829–846, 2013.

[2] Wang-Rong Chang, Hui-Tang Lin, and Bo-Xuan Chen. Trafficgather: An efficient and scalable data collection protocol for vehicular ad hoc networks. In *Consumer Communications and Networking Conference, 2008. CCNC 2008. 5th IEEE*, pages 365–369, 2008.

[3] Chen Chen, Jie Zhang, R. Cohen, and Pin-Han Ho. A trust modeling framework for message propagation and evaluation in vanets. In *Information Technology Convergence and Services (ITCS), 2010 2nd International Conference on*, pages 1–8, 2010.

[4] Ing-Ray Chen, Fenye Bao, Moonjeong Chang, and Jin-Hee Cho. Trust management for encounter-based routing in delay tolerant networks. In *GLOBECOM*, pages 1–6. IEEE, 2010.

[5] Mohamed Oussama Cherif and Sidi-Mohammed Senouci. A geographical self-organizing approach for vehicular networks. *JCM*, 7(12):885–898, 2012.

[6] Boon chong Seet, Genping Liu, Bu sung Lee, Chuan heng Foh, and Keok kee Lee. A-star: A mobile ad hoc routing strategy for metropolis vehicular communications. In *Proc. NETWORKING 2004*, pages 989–999, 2004.

[7] Tahani Gazdar, Abderrezak Rachedi, Abderrahim Benslimane, and Abdelfettah Belghith. A distributed advanced analytical trust model for vanets. In *Global Communications Conference (GLOBECOM), 2012 IEEE*, pages 201–206, 2012.

[8] ITEA3-CarCoDe. https://itea3.org/project/carcode.html.

[9] Moez Jerbi, Sidi-Mohammed Senouci, Tinku Rasheed, and Yacine Ghamri-Doudane. Towards efficient geographic routing in urban vehicular networks. *Vehicular Technology, IEEE Transactions on*, 58(9):5048–5059, 2009.

[10] Brad Karp and H. T. Kung. Gpsr: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, MobiCom '00, pages 243–254, New York, NY, USA, 2000. ACM.

[11] Rashid Hafeez Khokhar, Rafidah Md Noor, Kayhan Zrar Ghafoor, Chih-Heng Ke, and Md. Asri Ngadi. Fuzzy-assisted social-based routing for urban vehicular environments. *EURASIP J. Wireless Comm. and Networking*, 2011:178, 2011.

[12] Gökhan Korkmaz, Eylem Ekici, and Füsun Özgüner. An efficient fully ad-hoc multi-hop broadcast protocol for inter-vehicular communication systems. In *IEEE International Conference on Communications (ICC)*, volume 1, pages 423–428. IEEE, 2006.

[13] Gökhan Korkmaz, Eylem Ekici, Füsun Özgüner, and Ümit Özgüner. Urban multi-hop broadcast protocol for inter-vehicle communication systems. In *Proceedings of the 1st ACM International Workshop on Vehicular Ad Hoc Networks*, VANET '04, pages 76–85, New York, NY, USA, 2004. ACM.

[14] Sara Mehar, Sidi-Mohammed Senouci, and Guillaume Remy. Dissemination protocol for heterogeneous cooperative vehicular networks. In *Wireless Days*, pages 1–6. IEEE, 2012.

[15] Tamer Nadeem, Sasan Dashtinezhad, Chunyuan Liao, and Liviu Iftode. Trafficview: Traffic data dissemination using car-to-car communication. *SIGMOBILE Mob. Comput. Commun. Rev.*, 8(3):6–19, July 2004.

[16] Brijesh Kumar Chaurasia Pratibha Tomar and G. S. Tomar. State of the art of data dissemination in vanets. *International Journal of Computer Theory and Engineering*, pages 957–962, 2010.

[17] Ismail Salhi, Mohamed Oussama Cherif, and Sidi Mohammed Senouci. A new architecture for data collection in vehicular networks. In *Proceedings of the 2009 IEEE international conference on Communications*, ICC'09, pages 2705–2710, Piscataway, NJ, USA, 2009. IEEE Press.

[18] Weihua Sun, Hirozumi Yamaguchi, Koji Yukimasa, and Shinji Kusumoto. Gvgrid: A qos routing protocol for vehicular ad hoc networks. In *Quality of Service, 2006. IWQoS 2006. 14th IEEE International Workshop on*, pages 130–139, 2006.

[19] Jie Zhang, Chen Chen, and Robin Cohen. Trust modeling for message relay control and local action decision making in vanets. *Sec. and Commun. Netw.*, 6(1):1–14, January 2013.