Data Centric Rogue Node Detection in VANETs

Kamran Zaidi, Milos Milojevic, Veselin Rakocevic, Muttukrishnan Rajarajan
School of Engineering and Mathematical Sciences, City University London, London, EC1V 0HB, UK
(Kamran.Zaidi.1, Milos.Milojevic.1, Veselin.Rakocevic.1, R.Muttukrishnan)@city.ac.uk

***Abstract*—Vehicular ad hoc networks (VANETs) are the future of vehicular technology and Traffic Information Systems. In VANETs vehicles communicate by different types of beacon messages to inform each other of their position and speed to give them a sense of traffic around them. Vehicles can also send emergency messages in case of accidents or other hazards. The very fast moving nodes have to act quickly based on these emergency messages. However, a rogue node which sends false emergency messages can wreak havoc in the network that may even result in fatalities. This paper develops and simulates a technique to detect a rogue node that is sending false emergency messages in VANETs by cooperative exchange of data without the need of any infrastructure or revocation list. Also, the proposed mechanism will make VANETs fault tolerant and resilient against injection of false data.**

Index Terms **-** Security, wireless networks, ad-hoc, cryptography, fault tolerance, VANETs.

I. INTRODUCTION

VANETs are considered important due to their huge potential and numerous applications. VANETs not only offer immense safety enhancements but also many commercial opportunities. The recent announcements by major car manufacturers to equip their vehicles with wireless access vehicular environment (WAVE) devices from 2014 shows their imminent deployment. WAVE protocols are based on IEEE 802.11p standard and provide the basic radio standard for Dedicated Short Range Communication (DSRC) in VANETs. Vehicles use DSRC to communicate with each other i.e. vehicle to vehicle (V2V) and with the infrastructure i.e. vehicle to infrastructure (V2I) communication.

VANETs are just above the horizon and have the potential to make road travel as safer and enjoyable as air travel. The highways can be made much safer by integrating sensors in vehicles and allowing the vehicles to communicate with each other in order to have a better understanding of their surroundings and of the road up ahead. This is exactly what VANETs aim to do, however, there are serious challenges in implementing VANETs. The vehicles exchange messages with each other periodically called beacon messages and can also send emergency messages. As nodes in VANETs are vehicles moving at very high speeds, it is imperative that messages received are correct and give a true picture of the road conditions.

The existing mechanism for authenticating messages in VANETs involves the use of cryptography and trust. Cryptographic techniques involve paired keys and overhead in terms of computing cost, storage and time. Time is of the essence in VANETs especially in case of emergency messages when critical decisions have to be taken quickly. Even if emergency messages are kept unencrypted for faster processing, a false emergency message can cause severe damage. Emergency messages include emergency braking, accident, black ice on road etc. These messages are to be transmitted automatically to the vehicles behind so that effective safety measures can be taken.

The emergency messages for cases like accidents or emergency braking are time critical and require immediate action and therefore, it is recommended to transmit these unencrypted. However, a false emergency message can cause severe problems on the highways and can even result in fatalities. The condition is exacerbated when an emergency message is broadcast to be relayed by vehicles to others behind them in a multi hop fashion to convey the information as far back as possible. This raises the problem of broadcast storm in an already bandwidth limited channel when density of vehicles is high. Also, questions such as how far the emergency message should travel and when should vehicles stop transmitting it has been the focus of discussion for many years now. Furthermore, if messages are being relayed then the messages could be tampered with and would be impossible to detect.

A lot of research has been done in the past to secure VANETs by encrypting messages with the help of paired keys. The vehicles authenticate themselves with the TA and then RSU and obtain keys or certificates that they can use within the region of the RSU to exchange messages with other vehicles. Other vehicles do the same and therefore, whoever has obtained valid keys / certificates after authentication is assumed to be a trusted user and its messages are assumed to be correct as long as the credentials are valid. However, if a valid user turns rogue or transmits false data due to a faulty sensor then he can not be stopped and this can result in serious damage. Therefore, there is a need for developing security mechanisms for VANETs that are data centric rather than identity centric.

A. Contributions and Outline

Our main contributions in this paper are:

- The proposed scheme enables vehicles to detect and correct traffic parameters and highway conditions using a traffic model - Greenshield's model.
- The presented scheme, Co-operative Detection And Correction (C-DAC), enables vehicles to detect rogue nodes that are falsifying emergency messages in VANETs without the use of revocation list or any infrastructure.
- Make VANETs resilient against false data and enable them to detect and correct traffic data.
- Prevent Broadcast storm in case of emergency messages.

The rest of this paper is organized as follows: related work is discussed in Section II. In Section III, the system model for the proposed protocol is presented. Section IV, gives the overview of the proposed scheme. Section V analyses security performance of the proposed scheme in detail. The results are discussed in Section VI and the conclusion and future work is given in Section VII.

II. RELATED WORK

Security in Vehicular ad-hoc networks has been the focus of attention for researchers for many years now. It is important to secure VANET communications because the user is exchanging his location and a pseudo identity in all his messages. Without securing the messages, an adversary would be able to track a user by listening to their messages. In order to prevent eavesdropping, cryptography is used by first authenticating the user and then issuing keys / certificates. In VANETs, authentication and non-repudiation is achieved by digital signatures as described in [2], [3], [4]. Non-repudiation means that a sender can't deny sending a message and can, therefore, be held accountable for it. Many different schemes have been proposed including Public Key Infrastructure (PKI) [6], [7], [8] and elliptic curve cryptographic system (ECC) based PKI [5].

In order to preserve the location privacy of a user, the pseudo identity or public / private key pairs are changed frequently by each user. However, the Pseudonym (PN) or public and private key pairs can only be used once which means the OBU has to store them in large numbers. This raises the question of how to replenish them in the OBU once they have been used up. Furthermore, revocation is a difficult issue when using PNs and public / private key pairs e.g. if a vehicle is revoked then all the PNs or public and private key pairs assigned to that vehicle have to be revoked [3], [4] and added to a Revocation List (RL). Therefore, if a single vehicle is revoked then there might be several thousand entries added to the list [13]. This growing RL can cause serious problems at the RSU when verifying hundreds or thousands of messages every 300 ms (as dictated by VSC [10]). Moreover, vehicular networks are fast moving and highly dynamic networks in which decisions have to be taken very quickly and RLs do not conform with these requirements at all.

Privacy can also be achieved by using group signatures [9]. In group signatures only one member of a group communicates at a time on behalf of the group. A message from a group member cannot be associated or linked to any member of the group thereby preserving the identity of all the users in the group. However, if a node within a group turns rogue then it is very difficult to evict the node.

Some researchers have also proposed trust and reputation based schemes as a solution to securing the VANETs. This trust based on reputation can either be infrastructure based or self organising as proposed in [17]. Self organising trust is based on forming an opinion about a user based on past interactions or the length of current interaction with that user or getting feedback from other users about a new user and assigning a trust score to them. Reputation based schemes have been proposed in [18], [19], [20]. In [19], [20] a decentralized infrastructure has been adopted whereas in [18] a centralized infrastructure is used. In [18] a reputation score is assigned to each vehicle based on its reliability in the past. This score is collected, updated and certified by a reputation server. The score evolves with time i.e. increases with positive feedback and decreases with negative feedback. However, interactions in VANETs are short lived and there can be millions of nodes / users in the networks. Therefore, centralized trust management is neither easy nor practical. Similarly, self organising trust is also very difficult as a node can be honest till a certain time and then go rogue.

Due to the highly volatile and ad-hoc nature of VANETs, these cryptographic algorithms have to be designed to be a trade-off between security and performance. Moreover, malicious behaviour e.g. injection of false data is still possible even in case of strong cryptography. Researchers in [12] suggest using data centric techniques to make information in VANETs more reliable by data centric trust establishment.

Some data centric misbehaviour detection techniques have been proposed in [14], [15]. In [14] the authors propose a model of VANETs to be used to detect and correct errors in the data being sent out by vehicles. The messages that conform to the model is accepted and rejected otherwise. However, the authors do not specify the model in detail but only the events. In the proposed scheme a VANET model is defined and implemented against which messages are judged for correctness. In [15] emergency messages are relayed and false information is identified based on the kind of message and the subsequent behaviour of the sending vehicle. Such a technique will not be feasible for emergency messages which need to be acted on quickly. Also, such a scheme will increase the computation cost for the nodes.

A misbehaviour detection system and eviction mechanism is proposed in [16] where nodes are termed misbehaving if their info is inconsistent with the situation. Once a node is classified as misbehaving node then the neighbouring nodes can temporarily evict them by sharing warning messages about them and later their credentials are passed on to the CA which revokes them by adding them to a Revocation List (RL). However, RLs are themselves difficult to manage which is why data centric schemes are more suited to VANETs.

III. PRELIMINARIES

A. Authentication

In VANETs, it is imperative that vehicles can be distinguished from one another. This implies that all nodes authenticate themselves with a Certificate Authority (CA). It is assumed that all vehicles have authenticated themselves with a certificate authority and obtained a valid certificate and public/private key pairs. The vehicles use the keys to encrypt their messages and others can authenticate and decrypt the messages by using the relevant public keys. It is also assumed that all vehicles have enough key pairs to last them a long time and they keep changing these keys in a reasonable time i.e.

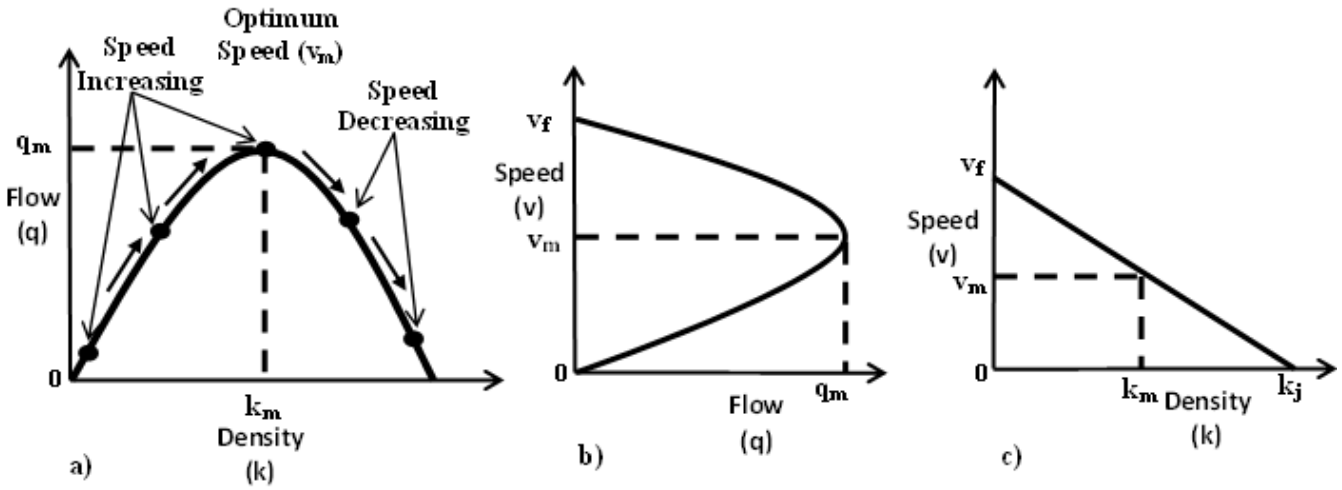


Fig. 1: Greenshield's Fundamental Diagrams (a)Flow vs Density, (b)Speed vs Flow, (c)Speed vs Density

not too quickly to avoid short term linkability [1]. Moreover, each vehicle has communicated with the other vehicle at least once before during which the identity (certificate) has been validated. This means that in case of an emergency message, the vehicle recognizes the identity of the vehicle. This is a reasonable assumption to make as vehicles are exchanging messages every 100ms.

B. VANET Model

Greenshield's model is considered to be a fairly reasonable model in traffic engineering for estimating and modelling traffic when it is uninterrupted (without traffic signals etc). Greenshield's model uses standard parameters such as flow (vehicles per hour) and density (vehicles per km). The model describes the relationship between speed (v) and density (k) of vehicles as being negatively correlated with density increasing with the decrease in speed as shown in Fig 1(c). In the figure v_f is the free flow speed when density is zero i.e. vehicles can choose to move freely as there are no or very few vehicles on the road. As the density of vehicles increases the speed decreases till density reaches the maximum which is referred to as jam density or k_j at which point the speed becomes zero and vehicles are stuck in a jam. In the figure k_m and v_m are the optimal density and speed respectively which allows the traffic to progress at the optimum rate of flow - q_m Fig 1 (a), (b) & (c). The relationship between speed and density is given as:

$$v = v_f - \frac{k}{k_j} v_f \tag{1}$$

The relationship between speed, density and flow is as follows:

$$q = k \times v \tag{2}$$

From (1) & (2) the relationship between speed and density can be found to be:

$$q = v_f k - \frac{k^2}{k_j} v_f \tag{3}$$

C. Message Format

Each vehicle creates its own message m for beacon and apart from the usual values also includes the following:

$$m(Speed_{own}, Density_{calc}, Flow_{OWN})$$

Each beacon message m is hashed ($H(m)$) and signed by the vehicle using its secret key (SK).

$$sig = SK(H(m))$$

The details of how this signature is generated and how they are verified are beyond the scope of this paper. In case of emergency e.g. an accident or emergency breaking, each vehicle generates an emergency message which has the following format:

$$EmergencyMsg(Type, Speed_{Own}, Density_{calc}, Flow_{OWN})$$

It must be noted that the emergency messages are not encrypted.

D. Rogue Node Model

A node is termed as rogue if it starts to inject false data in the network either on purpose with malicious intent or due to faulty sensors. Moreover, the rogue node can start sending false data at any time and can falsify values of their own speed and their calculated values of flow and density either

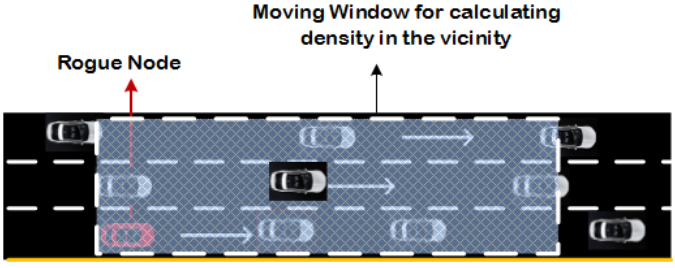


Fig. 2: Estimating density of vehicles in VANETs

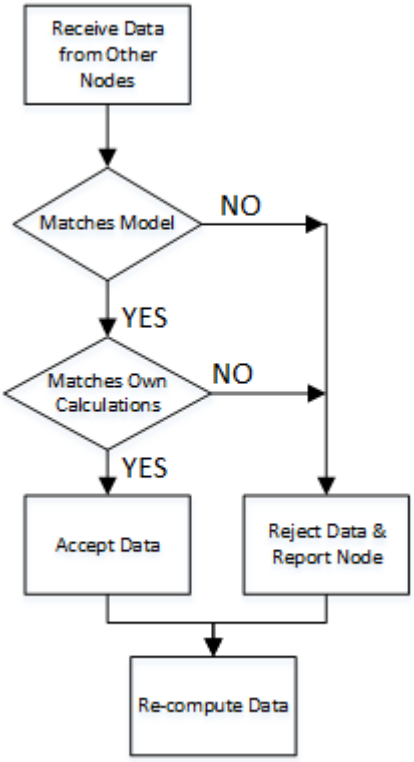


Fig. 3: Overview of Detection And Correction scheme (C-DAC)

in beacon message or emergency message. However, a rogue node can't modify values of other nodes in the network. In case of a false emergency message the rogue node will start sending a low value of Flow or sudden decrease in speed or both to indicate an accident or emergency braking.

IV. SCHEME OVERVIEW

In this paper a scheme C-DAC is proposed by which all vehicles calculate their own values of flow. Vehicles send their speed, flow, density and location information to other vehicles and each vehicle can calculate their own value of flow which gives them a very good model of the traffic in their vicinity and up ahead as well. Each vehicle can predict the density of vehicles on the highway by the number of messages it receives from other vehicles by checking their IDs from messages. This enables each vehicle to calculate the density quite accurately in a moving window around itself as shown in Fig 2. The size of this density window is equal to the transmission and reception range of a vehicle (500 meters). This means that a vehicle can receive messages from a vehicle which is up to 500m ahead of it and 500m behind it. Therefore, each vehicle has a communication window of 1000m around it that it can use to calculate the density ($Density_{calc}$). Also, each vehicle can calculate the average speed of vehicles ($Speed_{AVG}$) within its communication window. In our scheme each vehicle transmits not only its location and speed but the calculated value of flow as well. Therefore, the vehicles calculate the traffic flow parameter using density and average speed of other vehicles

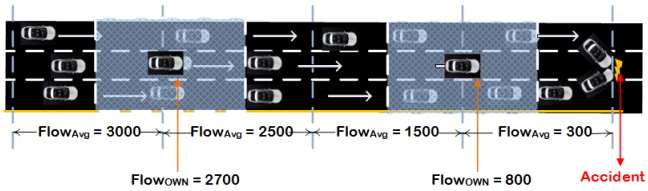


Fig. 4: Varying Value of Flow in an Accident Scenario

through Greenshields model. The flow serves as a global parameter which each vehicle calculates on its own and should be very similar for vehicles that are close to each other in the same traffic conditions.

The idea is that in case of an actual emergency situation, a vehicle will generate a message that has a very small value of flow that indicates that the flow of vehicles on that stretch of road has suddenly reduced. This will be confirmed by other vehicles as well which calculate a similar small value of flow on their own and generate messages. However, if a node generates a false message indicating a small value of flow either with malicious intent or due to some fault then it would be the only vehicle that generates such a value and can be singled out. The vehicle's speed has been used by some researchers [11] to estimate density but it does not give good results as the assumption is that given the opportunity the vehicle will try to achieve the maximum speed possible which is not true in real life.

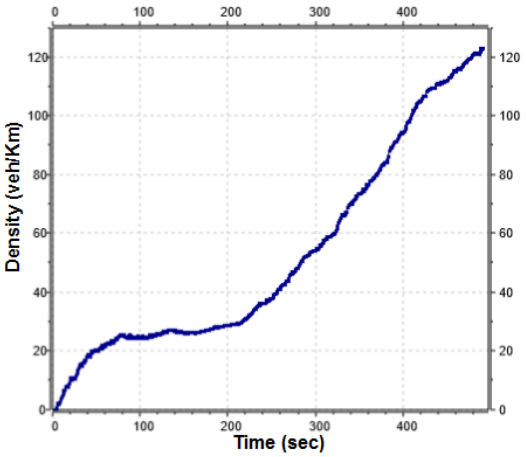
Each vehicle transmits its $Flow_{OWN}$ which becomes $Flow_{Rcvd}$ for other vehicles. If a vehicle receives a value of Flow from another vehicle that does not agree with the VANET model then the data is rejected and vehicles' ID is noted and reported. If the data agrees with the model then the receiving node checks the data with its own calculated values to confirm if values are indeed correct (shown in Fig. 3). If the values do not agree with the node's own calculated parameters of Flow, Speed and density then the values are discarded and the sender ID is reported. The two values of flow are calculated as follows:

$$Flow_{OWN} = Speed_{AVG} \times Density_{calc} \tag{4}$$

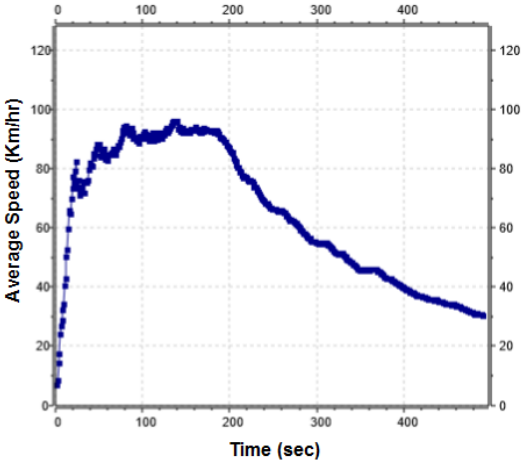
$$Flow_{AVG} = \sum^{n} \frac{Flow_{Rcvd}}{n} \tag{5}$$

TABLE I: SIMULATION PARAMETERS

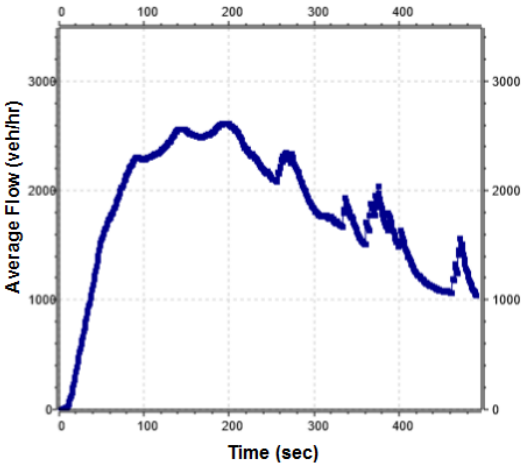
PARAMETER	VALUE
Simulation Time	500 sec
Scenario	3 Lane Highway
Highway Length	5-Kms
Max Vehicle Speed	28 m/sec or 100 Km/hr
Mobility Tool	VACaMobil
Network Simulation Package	OMNET++
Vehicular Traffic Generation Tool	SUMO
Number of Vehicles	330
Vehicle Density	20-30 veh / Km
Wireless Protocol	802.11p
Transmission Range	500m in each direction



(a) Increasing density in case of real accident

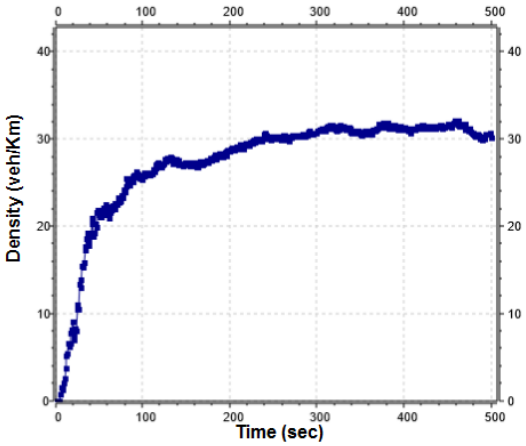


(b) Decreasing speed in case of real accident

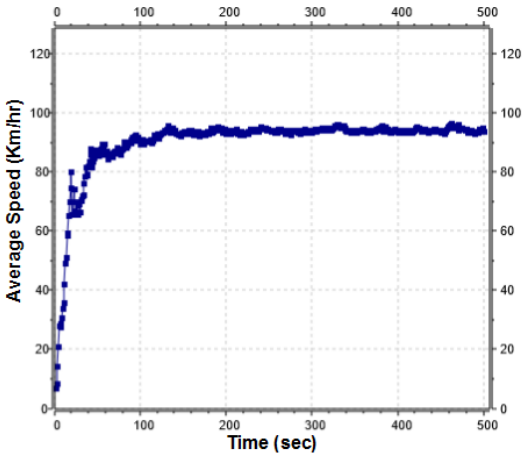


(c) Decreasing flow in case of real accident

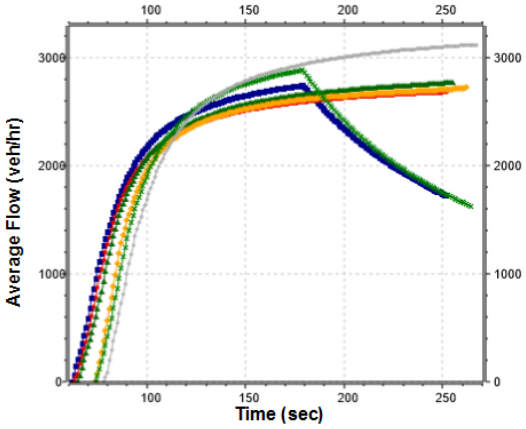
Fig. 5: Real Accident Scenario



(a) Constant density in case of rogue nodes



(b) Constant speed in case of rogue nodes



(c) 2 rogue nodes reporting lower values of flow

Fig. 6: Rogue nodes scenario without accident

However, in case of an actual accident the low value should be reported by all vehicles and it should propagate throughout the highway efficiently and gradually as shown in Fig 4. Moreover, in case of actual accident the speed of the vehicle that is receiving the messages will come down as well as it can detect obstacles with the help of on-board radar etc. Therefore, the main assumption is that the vehicle will be able to trust its own calculated values even if it can't trust anyone else. As, vehicle's own speed comes down then from eq. (4) the $Flow_{OWN}$ should come down as well which is then sent to other vehicles. If the received data doesn't conform to the VANET model, own calculated values or both then the data will be discarded and the node will be reported. The flow chart for our scheme C-DAC is shown in Fig. 3.

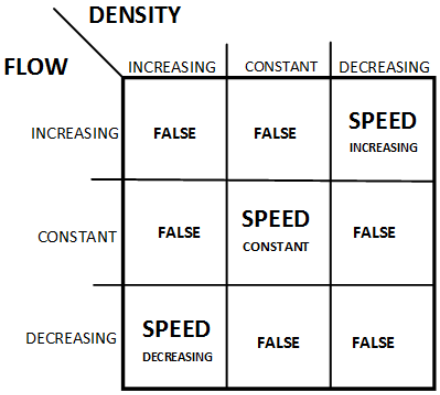


Fig. 7: Decision for Data Correctness

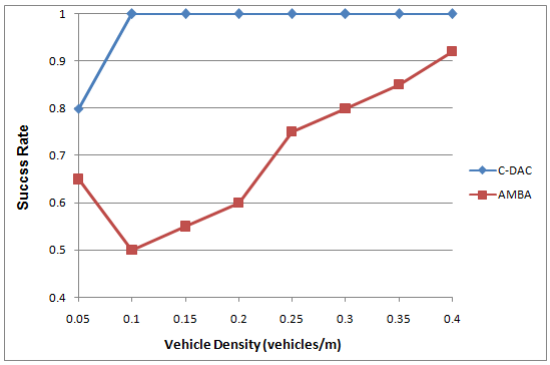


Fig. 8: Percentage of vehicles within the distance 3000m that received the emergency information successfully

V. PERFORMANCE EVALUATION

A. Simulation Setup

In order to check the proposed model it is simulated using OMNET++, SUMO [22] and VACaMobil [21]. OMNET is a modular C++ library and framework that is used for network simulations. Simulation of Urban Mobility (SUMO) is a software tool used to generate vehicular traffic by specifying speed, types, behaviour of vehicles and road types and conditions. VACaMobil is a car mobility manager for OMNET that works in parallel with SUMO.

The scenario is simulated with parameters shown in Table I. In order to validate the model an accident is simulated which takes place at t=180 sec and the results are recorded. Nodes 0, 1, 2, 3, 4 suffer an accident and block all three lanes of the highway. The result for $Density_{AVG}$, $Speed_{AVG}$ and $Flow_{AVG}$ are shown in Fig. 5 a), b) and c) respectively. Another scenario is simulated when there are three rogue nodes which start sending low false values of $Flow_{OWN}$ from t=180 sec incorrectly indicating an accident up ahead. The results for this scenario (where every 10th node is a rogue node) for $Density_{calc}$ and $Speed_{AVG}$ are shown in Fig. 6 a) and b) respectively whereas the , $Flow_{AVG}$ values for 6 vehicles (out of which 2 are rogue) are shown in Fig 6 c).

B. Simulation Results

1) Actual Accident Scenario: The results for the actual accident scenario are shown in Fig. 5 a), b) and c). It can be seen from Fig. 5(a) that the accident is causing the number of vehicles (density) to build up after the accident and all vehicles are reporting the same. Similarly, the flow value that each vehicle is computing is decreasing immediately after the accident (Fig 5c). Also, as the vehicles come to a stop their speeds decrease quite abruptly(Fig. 5b). This result gives a true - real VANET model against which received values are compared in case of rogue nodes.

2) No Accident - Rogue Node Scenario: In Fig. 6 a), b) and c) every 10th vehicle is a rogue node which are travelling normally without any accident and the rogue nodes are transmitting a low false value of Flow whereas the others are transmitting a (true) high value. In this case, the rogue nodes are not modifying the values of density or speed and can easily be seen and classified as faulty or rogue values.

C. Data Centric Rogue Node Detection

The honest nodes can decide whether a value being shared is correct or not by using a decision table shown in Fig. 7 which is directly derived from the Greenshield's model as shown in Fig. 1 a). As in the case of our simulation if the value of Flow being reported by a node is decreasing but the speed and density reported from that node remain constant then the value being reported is false. Similarly, another case could be when a node reports a decreasing value of flow and increasing value of density but the average speed remains constant in that region then again this implies that the data being reported is false and can be discarded.

The results show that by using our technique, messages can be authenticated based on the relevance and freshness of data without authenticating the identity of nodes. Such nodes can then be reported or their messages be simply discarded. Also, the information about an accident can be propagated down the highway gradually and gracefully so that the traffic keeps flowing as long as it can and comes to stop gradually.

D. Comparison

The success rate of the proposed scheme C-DAC is compared to the AMBA (Adaptive and mobility based algorithm) presented in [11]. The success rate is the percentage of vehicles within a 3km distance that receive the emergency information successfully and is shown in Fig. 8. In our scheme C-DAC, the success rate reaches 100 % as there is no congestion because the emergency messages are not being relayed as in AMBA. Instead, in C-DAC the emergency info is being propagated through communication of some global traffic parameters as discussed previously and information can be relayed to all nodes even very large distances away.

VI. DISCUSSION

In this section we discuss the direct and indirect effects of our proposed system on the network, its reliability and robustness.

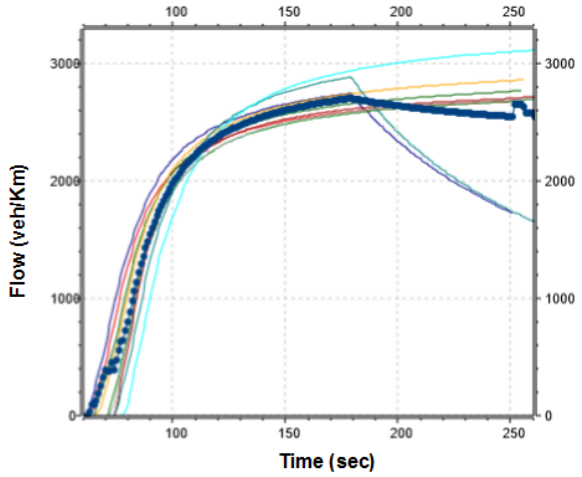


Fig. 9: Average Flow in case of No-Accident with Rogue Nodes

A. Fault Tolerance

Moreover, as the data is being calculated by each vehicle and it is being compared with the readings calculated by the vehicle itself and other vehicles, therefore, this introduces a built-in fault tolerance in the network which is highly useful and desirable for highly volatile and rapidly changing VANETs. Even if a node is able to distort the values of the reported parameters (Density, Flow and Speed) so as not to raise a red flag with other vehicles, it results in a small error in the overall reading as shown in Fig. 9, it shows values of $Flow_{own}$ in case of no accident and two rogue nodes that start transmitting a false value of Flow at t=180 sec and the average value of flow shown in blue line. This value shows that even if the false flow values are not rejected initially they will cause little deviation if the number of rogue nodes is small as compared to honest nodes in the neighbourhood.

B. Self Detection and Correction

In a vehicular ad-hoc network with fast moving nodes, it is highly desirable for the nodes to be able to detect and correct data on their own. Due to the volatile nature of VANETs it is impractical to use any techniques that rely on reputation or trust of users to ensure correctness of information. Moreover, a valid identity of vehicles is important for distinguishing them from each other but should not be used as the basis of the acceptance of information in a protocol. This means that an authenticated node doesn't guarantee that the node will behave honestly. With the latest technology being introduced in the vehicles including radars and cameras for obstacle detection, these technologies can be combined with a technique like ours to ensure safety of travel. With driver-less features becoming a reality with Google car, it is important that the vehicle starts behaving autonomously not only in terms of driving but also planning ahead. This means that at high speeds on the highways, a driver-less car should be able to estimate or predict the road and traffic conditions quite early and with reasonable accuracy. This is only possible if the highway traffic is modelled and used by the OBUs to detect and correct anomalies in the information being received. The notion of revocation quickly in a highly agile and temporary network doesn't look realistic till now.

C. Congestion Avoidance

In case of emergency messages in VANETs, the currently proposed method of propagating such messages is by relaying the message by receiving vehicles to others behind them. This can cause a broadcast storm where every vehicle is relaying the same message repeatedly and flooding the region in an attempt to inform other vehicles of the emergency. This quickly, consumes the small bandwidth available and can choke the network. However, in our proposed scheme there is no channel congestion as there is no need for multi-hop retransmissions and a sudden drop in the flow or speed values can indicate an emergency. Moreover, as only the vehicles within range behind the vehicle experiencing the accident receive the emergency message, they are able to identify that vehicle quickly as they have communicated with it before. These vehicles then modify their own values of flow and send them to others.

D. Resilience to Sybil Attacks

In case of a Sybil attack, an attacker presents multiple identities with an intent to either vote out a user maliciously or in our case more likely to create the illusion that there is congestion or accidents up ahead. As all vehicles are reporting their location along with their speed, density and flow values in their vicinity. In case of a sybil attack, an honest vehicle which is behind a sybil node will receive multiple (false) messages with different identities and each message will report a low value of flow but if the vehicle's own speed is not decreasing then it can start ignoring those messages. Therefore, C-DAC provides resilience against sybil attacks.

E. Effective Dissemination of Information

In our scheme the information about an accident or similar situation is disseminated effectively to other vehicles long way back gradually and efficiently. This means that in case of traffic congestion, the system will inform users to slow down gradually and not tell them to come to a halt altogether. This case was predicted in Fig. 4 and can be seen in Fig. 5 c) as well. In Fig. 5 c) the value of the Flow is coming down in the whole network gradually and gracefully validating our model.

F. Limitations of C-DAC

The presented technique, C-DAC will be unable to identify the actual rogue node during a sybil attack when the rogue node is presenting multiple identities / pseudonyms. Moreover, if there are multiple attackers that collude to launch an attack e.g. two or three cars intentionally block the lanes of the highway and send multiple messages with different identities reporting an accident or congestion then it will not be detected by C-DAC. The reason is that in such an attack the data will satisfy both the VANET model and will also match the vehicle's own readings. However, such

an attack is very expensive to launch as it requires multiple rogue nodes to be present together in a region.

In case of an actual accident the density increases all of a sudden whereas the flow value doesn't go down as quickly, therefore, the flow value that a vehicle will calculate will increase for a short time before going down. During this transition phase, it is difficult to distinguish between a rogue node and an honest node apart from the vehicle's own calculations.

VII. CONCLUSION AND FUTURE WORK

In this paper we have shown that data centric rogue node detection and data correction is possible using our proposed scheme C-DAC without the need for any revocation list. By using a model of the network, each node is able to predict and estimate the current state of the network. The strength of the proposed scheme is that an honest node can always trust its own data regardless of what values are being reported by other nodes. By calculating and sharing a few global parameters each vehicle can get a reasonably accurate model of the traffic conditions which can be used to single out the rogue node whose data can then be discarded. Such data centric schemes are highly suited to VANETs where trust based schemes are impractical to implement due to very large number of nodes and ephemeral nature of network. However, the proposed scheme will not be able to detect false data or identify sybil nodes if the data they are sending conforms to the model and also to the values being calculated by the receiving vehicle itself.

Our proposed scheme can be extended if RSUs are used to provide confirmation of one or more global parameters. One way in which this can be done is by calculating the flow of vehicles along a segment of highways and then reporting this value to all vehicles in the region to correct the data that they are receiving from other vehicles and fine tune their estimated traffic model. This value of flow can be calculated quite easily by using existing traffic cameras used for traffic monitoring by authorities and applying simple image processing techniques. This will further improve reliability and robustness of the system even in case of Sybil attacks.

REFERENCES

[1] A. Studer, E. Shi, F. Bai, and A. Perrig. "TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs," *Proc. 6th Annual IEEE Commun. Society Conf. (SECON '09)*., pp. 1–9, 2009.

[2] D. Huang, S. Misra, G. Xue, and M. Verma, "PACP: An Efficient Pseudonymous Authentication Based Conditional Privacy Protocol for VANETS, *IEEE Trans. Intell. Transp. Syst*., vol. 12, no. 3, pp. 736-746, Sep. 2011.

[3] A.-N. Shen, S. Guo, D. Zeng, and G. Mohsen. "A Lightweight Privacy-Preserving Protocol using Chameleon Hashing for Secure Vehicular Communications," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, pp. 2543–2548, 2012.

[4] R. Lu, X. Li, T. H. Luan, X. Liang, and X. Shen. "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs," *In IEEE Trans. Veh. Technol*., vol. 61, no. 1, pp. 86–96, 2012.

[5] I. Blake, G. Seroussi, and N. Smart, "Advances in Elliptic Curve Cryptography," Number 317 in London Mathematical Society Lecture Note Series. Cambridge Univ. Press, Cambridge, U.K. 2005.

[6] M. Raya, and J-P. Hubaux, "Securing Vehicular Adhoc Networks," *Journal of Computer Security*, Special Issue on Security of Ad Hoc and Sensor Networks, vol. 15, no. 1, pp. 39–68, 2007.

[7] P. Papadimitratos, A. Kung, J. P. Hubaux, and F. Kargl, "Privacy and Identity Management for Vehicular Communication Systems: A Position Paper," in *Workshop on Standards for Privacy in User-Centric Identity Management*, Zurich, Switzerland, July 2006.

[8] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications", in *Proc. IEEE 27th Conf. Comp. Commun.* pp. 1229–1237, Apr. 2008.

[9] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: A Secure and Privacy Preserving Protocol for Vehicular Communication," in *IEEE Trans. Veh. Technol*., vol. 56, no. 6, pp. 3442-3456, Nov. 2007.

[10] Vehicle Safety Communications Project Final Report: Identify Intelligent Vehicle Safety Applications Enabled by DSRC. s.l. :U.S. Department of Transportation, National Highway Traffic Safety Administration, 2005.

[11] K.A. Hafeez, L. Zhao, B. Ma, J.W. Mark, "Performance Analysis and Enhancement of the DSRC for VANET's Safety Applications," *IEEE Trans. Veh. Technol*., vol.62, no.7, pp.3069-3083, Sept. 2013.

[12] F. Kargl, P. Papadimitratos, L. Buttyan, M. Muter, E. Schoch, B. Wiedersheim, Ta-Vinh Thong, G. Calandriello, A. Held, A. Kung, J-P Hubaux, "Secure vehicular communication systems: implementation, performance, and research challenges," *IEEE Commun. Mag*., vol.46, no.11, pp.110-118, November 2008

[13] J. J. Haas, Y-C. Hu, and K. P. Laberteaux. "Efficient Certificate Revocation List Organization and Distribution, *IEEE J. Sel. Areas Commun*. vol. 29, no. 3, pp. 595-604, 2011.

[14] P. Golle, D. Greene, J. Staddon. "Detecting and correcting malicious data in VANETs," in *Proc. 1st ACM Int. workshop Veh. ad hoc networks*, pp. 29-37. ACM, 2004.

[15] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, I. Stojmenovic. "On data-centric misbehavior detection in VANETs," in *Veh. Technol. Conf. (VTC Fall)*, 2011 IEEE, pp. 1-5. IEEE, 2011.

[16] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks," *IEEE J. Sel. Areas Commun*, vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[17] P. Wex, J. Breuer, A. Held, T. Leinmuller, L. Delgrossi. "Trust Issues for Vehicular Ad Hoc Networks," *Veh. Technol. Conf. (VTC Spring 2008)*, pp.2800-2804, 11-14 May 2008.

[18] L. Qin, A. Malip, K. M. Martin, S. Ng, and J. Zhang. "A reputation-based announcement scheme for VANETs," *IEEE Trans. Veh. Technol.,*vol 61,pp 4095-4108,Nov. 2012.

[19] U. Minhas, J. Zhang, T. Tran, and R. Cohen, "Towards expanded trust management for agents in vehicular ad hoc networks, *Int. J. Comput. Intell. Theory Pract*., vol. 5, no. 1, pp. 3-15, Jun. 2010.

[20] A. Patwardhan, A. Joshi, T. Finin, and Y. Yesha, "A data intensive reputation management scheme for vehicular ad hoc networks," in *Proc. 3rd Annual International Conf. Mobile Ubiquitous Systems*, pp. 1-8. 2006.

[21] M. Baguena, S. Tornell, A. Torres, C. Calafate, J.-C. Cano, and P. Manzoni, "Vacamobil: Vanet car mobility manager for omnet++," in *Communications Workshops (ICC), 2013 IEEE International Conf. on*, 2013, pp. 1057-1061, Jun. 2013.

[22] M. Behrisch, L. Bieker, J. Erdmann, and D. Krajzewicz. "Sumo - Simulation of Urban Mobility: An overview," in *SIMUL 2011, The 3rd International Conference on Advances in System Simulation*, pages 63-68, Oct. 2011.