ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse181932020.pdf
https://doi.org/10.30534/ijatcse/2020/181932020

Efficient Information Dissemination in Vehicular Networks with Topological Approach

J.Krishna[1], M.Meghana[2], M.Rudra Kumar[3]
[1]Associate Professor, Computer Science and Engineering, Annamacharya Institute of Technology and Sciences, Rajampet, A.P. India, krishna.j.jk@gmail.com
[2]M.Tech Scholar, Computer Science and Engineering, Annamacharya Institute of Technology and Sciences Rajampet, A.P., India, meghanamudda97@gmail.com
[3]Professor & Head, Computer Science and Engineering, Annamacharya Institute of Technology and Sciences, Rajampet, A.P. India, mrudrakumar@gmail.com

ABSTRACT

Owing to their ability to provide endless services such as entertainment, adaptive route selection, etc., Vehicular ad hoc networks (VANETs) have received a great deal of interest from both academia and industry in recent years. Vehicles communicate with other vehicles in VANETs and with fixed data transmission infrastructures. Vehicles in VANETs serve as intelligent sensing devices with communication and computing capabilities built in them with Application Unit (AU), and On-Board Unit (OBU). These units can be used in a wide range of applications including warning generation, community services, traffic management, and so on, and can also provide on-board passengers with security, protection, and comfort. As vehicle communications are widely used, there may be congestion in the network and the quality of service may be compromised. That also results in a deterioration of performance in data dissemination. Since its inception, a variety of research initiatives have been carried out for effective data dissemination. Most of the existing data dissemination solution in VANETs could not provide a comprehensive scheme that would meet the parameters of Quality of Service (QoS). Moreover, the existing schemes were unable to provide reliable communication and the broadcast storm problem was not been solved completely. Hence, there was a need of a new solution that meets the desired QoS parameters and ensures reliable communication. It is also necessary that the messages sent are authenticated and delivered to the vehicles in the relevant areas quickly. In this chapter, we present an efficient protocol for fast dissemination of authenticated messages in VANETs. It ensures the anonymity of the senders and also provides mechanism for law enforcement agencies to trace the messages to the senders, when necessary.

Key words: VANETS, Topology, Message, Dissemination

1. INTRODUCTION

VANETs are special class of MANETs that are distinct from MANETs in the sense that the former may have support for the infrastructure, but later not. There are a large range of VANET applications, e.g., environment sensing and monitoring, intelligent transport systems (ITS), emergency security notifications warnings, etc., that have been / were developed over the years using VANETs. Various government and private entities have invested a great deal of money in a variety of different ventures in this area with the goal of providing the passengers sitting in the vehicle with protection and comfort. Messages are transmitted from source to destination for dissemination of information in all of these applications [1,2].

The on-road vehicles communicate with each other either in a Peer-to - Peer (P2P) manner or using the existing infrastructure. In the former case, it is called Vehicle-to - Vehicle (V2V) contact while in the latter it is called Vehicle-to - Infrastructure (V2I). Help for infrastructure is provided by nearest Road Side Units (RSUs), which can serve as an intelligent router to control all vehicle activities on the road. If the vehicles are within the range of RSUs then messages would be sent directly to them otherwise, these would be passed on to the vehicles' nearest RSU. However, due to the high mobility and sparse distribution of vehicles on the road, data transmission among the vehicles is often a challenging task which can cause a long delay in delivery of messages. The distribution of message in VANETs follows store and forward strategy in which messages are held at some intermediate nodes before the strongest forwarding node (vehicles / RSUs) is found [3]. This strategy can cause lengthy delays, but this delay can affect the production of many of VANET applications.

For communication purposes, vehicles can contain some units that can be used to link to other vehicles or the infrastructure. The three major components of VANET architecture usually follow: AUs, OBUs, and RSUs. RSUs can act as a router providing services to moving customers [4],

while OBUs and AUs are the consumers for those services. Wireless standards such as IEEE 802.11p, IEEE 802.11 a / g allow communication between OBUs and AUs with RSUs. Generally, vehicles have OBUs installed on board the vehicles that can be used to communicate with other OBUs or RSUs. In addition, OBUs also have AU communications. OBUs are used for congestion control, the management of IP mobility, data collection and processing [4]. AUs are the sophisticated devices which use OBUs to provide security applications and communicate to RSUs. These can be independent units, or can be combined as a single unit with OBUs. RSUs are deployed in an optimized manner as fixed units alongside the road to preserve coverage and connectivity to all vehicles. We provide connectivity between the vehicles using dedicated short-range connectivity (DSRC) or using IEEE 802.11 a / b / g with other RSUs and OBUs. Figure 1 represents various components of a generic architecture used in VANETs.

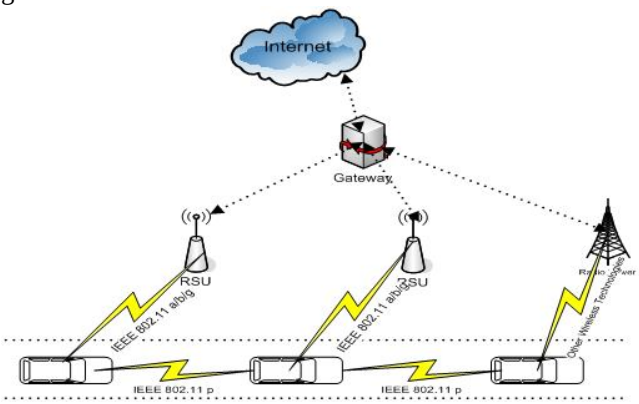

Figure 1: Generalized architecture in VANETs

2. RELATED WORK

There are many proposals for data dissemination which exploit the topology of the network. These proposals are further classified into proactive and reactive based data dissemination techniques and are explained as follows.

Proactive techniques

A list of destination is maintained by nodes in proactive data dissemination protocols. In this type of protocols, all the links are computed by exchanging beacon messages. The routing tables are distributed periodically throughout the network. The advantage of this technique is that alternate routes are known beforehand in case of link failure. It has many disadvantages as it consumes heavy bandwidth for maintaining the routes. The vehicles used Wireless Local Area Network (WLAN) and Wireless Large Area Network (WWAN) as mobile gateways in a prediction-based routing (PBR) for VANETs to connect to the Internet when on the road [5]. Due to highly dynamic topology, the main challenge for using this type of service is the frequent link breakage. Although the vehicles on the road are of high speed and change direction rapidly but their movement is still predictable. PBR used that predicted route to suggest new routes preemptively before the existing routes fail. Compared to existing proactive and reactive protocols PBR has achieved satisfactory results. In PBR protocol high gateway density was recommended to minimize the adverse effects of route length and mobility patterns.

Results [5] showed a reduction in route failures and an increased PDR provided by the PBR. The overhead for checking and predicting routes has also been very much lower and within tolerable limits. Two routing tables are maintained at each node in the Destination Sequence Distance Vector (DSDV) routing protocol namely routing table and setting time table [6]. The routing table includes the list of addresses of all other network nodes. It also has the address of next hop, metric route, sequence number of destinations, etc. In setting time table, the setting time, i.e., the time for updating advertisement, is maintained for each destination. Selected routes with later sequence number. If sequence numbers are the same, then the decision on the smallest metric is taken. DSDV offered free routes for the loops. DSDV has some drawbacks as-it has issues with unidirectional connections and caused route fluctuation.

In Fisheye State Routing (FSR) protocol, the nodes maintained accurate information of their immediate neighbors and lesser information and details of the nodes as the distance increased [7]. Nodes exchanged information with neighboring nodes and maintained Link State (LS) information. The messages containing information are exchanged by neighbors periodically rather than flooding the network when there was any change in topology. This periodic exchange of messages reduced the control message overhead.

The nearest neighbors exchanged messages most frequently, the nodes two hop away exchanged less frequently, and farthest nodes exchanged least frequently. A full topology map was maintained at each node and the shortest paths were computed from this map. Simulations have been performed using random waypoint model. LS routing protocol has less inaccuracy as it reacts fast to topology changes. As the network size increased the control overhead also increased. The higher the radius the less was inaccuracy but more was overhead. The routing accuracy of FSR is comparable to ideal LS routing with minimum routing overhead.

In Optimized Link State Routing (OLSR) protocol, an automatic optimization tool [8] is used to define the optimization problem with optimum parameter setting. OLSR is a routing protocol that follows a proactive routing strategy that uses special nodes that serve as multi-point relays (MPRs) to periodically flood control information. Throughout this scheme the links status was immediately known which allowed the hosts to know the quality of network routes throughout advance. Easy integration into existing operating systems and devices occurred without changing the format of IP message headers. OLSR is well suited for high-density networks, and is suitable for applications requiring short transmission delays. Due to the capacities of VANET nodes may use specific network interfaces to serve as gateways to other potential network interfaces to apps, handling several interfaces with

the same host address. OLSR 's functionality was conducted primarily through three separate types of messages, namely hi-messages, topology control (TC) and multiple device declaration (MID) messages. To find an optimal configuration for the routing protocol, meta-heuristic algorithms were studied. These algorithms were Differential Evolution (DE), Particle Swarm Optimization (PSO), Simulated Annealing (SA) and Genetic Algorithm (GA).

Reactive techniques

This form of protocol finds a route on demand using the packets for route request propagation and response. The heavy bandwidth usage issue has been solved but these are slower than the constructive routing in which the links are immediately usable. These protocols also react more slowly on restructuring and failures. This category 's influential protocols are analysed as follows.

In VANETs Adaptive Information Dissemination Approach (AID), each node takes advantage of local knowledge obtained from neighboring nodes [9]. Includes the number of neighbors and the distance between them. Local-parameter values have been dynamically modified. The proposed solution was tested for various metrics, such as Saved ReBroadcasts (SRB), sensitivity and latency. The results of the simulation proved the supremacy of the AID scheme compared with other state-of-the-art protocols.

A traffic signal system named CATS based on car-to-car communication which dynamically adjusted the timing patterns according to traffic demands has been proposed [10]. The cycle time has been calculated based on estimated density of vehicular traffic which helped in reducing the waiting time for vehicles at intersection and made this proposed solution collision free at intersection. The authors proposed an algorithm for election of CH and cluster formation. At start, when the cluster ID was NULL, it checked for the timer to expire. When timer expired, if the reply was received from the node whose distance is less than the threshold distance, that node which is farthest from header and within the threshold distance is elected as the CH.

Privacy Preventing Broadcast Message Authentication (PPBMA) protocol for VANETs used the features of message authentication code and hash operations to authenticate messages rather than asymmetric verification [11]. The protocol used two stages of key hash chain to prevent message losses. The key features of this protocol are that for secure communication, it is time-efficient privacy authentication protocol and is capable of providing the conditional privacy and prevents anonymity. In terms of computational and communication power, the protocol also has lower message latency and greater performance. The base station serves as sink and transmits Commitment Distribution Messages (CDM). CDM has been used by each node to authenticate the low-level hash. The simulations have been done in two scenarios namely-city driving and two-lane highway communication. The protocol has been compared with Time efficient and Secure Vehicular Communications (TSVC) with privacy preventing scheme, PPBMA, and Time Efficient Stream Loss-tolerant Authentication (TESLA). The simulation parameters were average packet delay with number of vehicles and fraction received packets with number of vehicles. The results obtained showed that PPBMA has considerable improvement as compared to other existing protocols.

A cluster-based flooding protocol called LORA CBR has been proposed and evaluation of performance of routing protocols for VANETs has been done [12]. The nodes were classified into cluster members, gateways and CHs with one CH in every cluster. Gateways nodes were connected to more than one clusters. CH maintained information of members and gateways of cluster. Packets were routed to destination node in a greedy manner. In the event the destination location was inaccessible, the source sent packets of the Location REQuest (LREQ). The CH was given the responsibility for the transmission of LREQ and Location REPly (LREP) messages. The protocol is identical to AODV [13] but the difference is that the messages were only transmitted by CH. Simulations were made for urban as well as highway scenarios. Results clearly showed that mobility and size of the network have more effect on AODV and DSR performance than LORA CBR.

In an enhanced Roadmap-based Message Dissemination (eMDR) message dissemination scheme, roadmaps were used to increase the percentage of informed vehicles and reduce notification times [14]. The proposed protocol worked successfully in urban scenarios where vehicle density is high, and buildings absorbed radio waves that only vehicles in the line-of - sight can communicate. Vehicles were operating in two modes, normal and with warning. The default behavior was regular mode but when a vehicle senses a hazardous situation it begins to work in alert mode. For sending and receiving messages two separate algorithms were proposed. In case of sending, the message priority was set for the vehicle in warning mode and the message was broadcast accordingly. The difference between sending messages in a row has also been set. The warning message in case of reception, if the distance between sender and recipient was greater than the threshold distance or if both vehicles were in separate streets then the message was re-broadcasted. If any of the above four cases were unsuccessful the message was discarded.

3. DESIGN METHODOLOGY

The Process suggested has the following phases:

• Phase 1: Group Key and Symmetric key Establishment. When a vehicle leaves the area covered by an RSU and reaches an area covered by another RSU, it initiates contact with the new RSU and creates a symmetric mutual key with the new RSU so it can send encrypted messages to the neighboring

RSU using the symmetric key. It also gets the group key and its pseudo ID from the

RSU: RSU. RSU uses group key to encrypt messages and send them to the vehicles in the RSU covered area. In all communications a vehicle is using its pseudo ID. Here, by the area covered by an RSU, we mean the area within the RSU 's range of transmission.

• Phase 2: Vehicles Sending Messages to RSU for Dissemination: Once Phase 1 is complete; a vehicle can send messages to the RSU. The shared symmetric key developed in Step 1 is used to encrypt the message and to calculate the digest of the messages it sends. This message digest lets the RSU check the validity of the messages and their credibility. Note that the RSU to which the message is sent may not be within the vehicle's transmission range sending a message, and thus a routing algorithm is used to route the messages through intermediate nodes to the RSU.

• Phase 3: Verification and Dissemination of Messages by RSUs: When an RSU receives the messages sent by the vehicles, it verifies the authenticity and integrity of the messages and transmits the messages either directly (to vehicles within its transmission range) or via other RSUs to the vehicles in appropriate regions.

Group key and Symmetric key Establishment

When a vehicle V_i leaves the region covered by an RSU and enters a region covered by a different RSU, say R_j, it initiates the key establishment process (illustrated in Figure 2). The key establishment process is based on the Diffie-Hellman key agreement protocol [15]. V_i initiates mutual authentication and key establishment by sending the message g, p, A, {g, p, A}SK_{Vi} ;C_{Vi} . In this message, {A, B, g, p} are elements of the Diffie-Hellman key agreement protocol: p is a prime number, g is primitive root mod p, A = g^a mod p, a is the secret integer kept by V_i, C_{Vi} is the certificate of V_i, g, p, A is encrypted with the private key SK_{Vi} of V_i so that the RSU can authenticate V_i by decrypting it using the public key PK_{Vi} of V_i. Upon receiving this message, the RSU R_j concatenates the pseudo ID PIDVi of Vi, the number B = g^b mod p (b kept secret by Rj), the group ID GID_j and the group key K_{Gj} and encrypts all this with the public key PK_{Vi} of V_i and sends it to V_i along with its certificate C_{Rj} . Note that A||B||Ts are encrypted using RSU's private key, which means that only authentic RSU can generate this message, hence a fake RSU attack is prevented. Finally, V_i sends an acknowledgment for having received B. Thereafter g^{ab} serves as the secret key $K_{Vi\text{-}Rj}$ between V_i and R_j and K_{Gj} is the group key used by R_j for encrypting and sending messages to all vehicles in its region. This completes the mutual authentication and key establishment phase and R_j updates its group table which contains pseudo IDs, original IDs, certificates, shared secret keys. Note that we assume that a routing algorithm is used for forwarding messages from V_i to R_j because R_j may not be within the transmission range of V_i. Note that timestamp T_s is attached to every message to prevent the replay attack.

Vehicles Sending Messages to RSU for Dissemination

After the key establishment phase between a vehicle V_i and an RSU R_j, V_i can send messages to R_j securely and without revealing its identity as follows. When V_i wants

$$V_i \rightarrow R_j : g, p, A, \{g, p, A \| T_s\} SK_{V_i}, C_{V_i}$$

$$R_j \rightarrow V_i : \{PID_{V_i} \| B \| GID_j \| K_{G_j}\} PK_{V_i}, \{A \| B \| T_s\} SK_{R_j}, C_{R_j}$$

$$V_i \rightarrow R_j : \{B \| T_s\} SK_{V_i}$$

Figure 2: Key Establishment Process

to send a message M about a sensed event, it computes M_i from M as follows and sends it to R_j .

$$M_i = ID_{R_j}, PID_{V_i}, \{M, T_s, S_q\} K_{V_i\_R_j}$$

To compute M_i, the secret key $K_{Vi\text{-}Rj}$, established between V_i and R_j is used to encrypt the message M, the sequence number of the message S_q and the timestamp T_s; the pseudo ID PID_{Vi} of V_i is also appended. Note that when R_j receives the message, it will be able to verify the authenticity of the sender and the integrity of the message based on the pseudo ID and the secret key used for encryption. However, since R_j may not be within the transmission range of V_i, the message may have to be routed through other intermediate nodes using the available routing algorithm. We must make sure that the destination RSU R_j is able to authenticate all the intermediate nodes forwarding this message. For that purpose, we adopt the onion signature scheme [16]. With onion signature, every vehicle forwarding message simply appends a signature of received message and forwards it towards the destination RSU. When an intermediate vehicle V_j receives the message M_i FROM V_i, it computes M_j, by attaching its signature as follows and forwards it to the next hop on the route.

$$M_j = ID_{RSU}, PID_{V_j}, M_i, dgt_j$$

where the digital signature dgt_j = E(H(Mi), $K_{Vj\text{-}RSU}$) is obtained by computing the hash of the received message M_i and encrypting it using the shared key of V_j and the destination RSU. This process is repeated until the message reaches the destination RSU.

Verification and Dissemination of Messages by RSUs

When an RSU receives a message sent by a vehicle V_i, since it has a shared key with each vehicle which forwarded the message, it can decrypt the signatures attached by all nodes on the route one by one and verify the authenticity of each node and the integrity of the message received. After it verifies the authenticity and integrity of the message, it disseminates the message to the vehicles in appropriate regions. Since the RSUs have higher computation power than the OBUs, RSUs can verify messages more quickly than OBUs. After checking the

integrity and authenticity of a message received from a vehicle, the RSU, say R_i, determines the areas to which the message needs to be propagated. If it needs to be propagated to only vehicles within its transmission range, then it computes the digest $dgt_i = E(H(M), SK_{Ri})$ of the message M by encrypting the hash of M. Then it encrypts the message, sequence number and the digest using the group key K_{Gi} as

$$M_{type1} = GID_i, \{M, Ts, Sq, dgt_i\}K_{G_i}$$

and broadcasts to all vehicles within its transmission range. If the message needs to be propagated to vehicles that are not within its transmission range, then it computes M_{type2} as

$$M_{type2} = ID_{receiver\_RSU}, ID_{sender\_RSU}, \{M, Ts, Sq, h, dgt_i\}PK_{receiver\_RSU}$$
$$\text{where } dgt_i = E\Big(H(M), SK_{R_i}\Big)$$

and sends the message to the respective neighboring RSUs by setting the number of hops h (i.e., the number of RSUs, through which the message needs to propagate) to the appropriate value. When an RSU receives this message, it decrements the value of h by 1 and forwards it to its neighbors if h > 1. Based on the nature of the message, an intermediate RSU can decide whether or not to disseminate the message to the vehicles within its transmission range. The detailed algorithm is given in Figure 3.

Under our algorithm, when a vehicle enters a region covered by an RSU (i.e., the area within the RSU's transmission range), it initiates key establishment with the RSU and sets a symmetric key with the RSU so that it can encrypt all the messages it needs to send to the RSU while in its region. It also gets a pseudo-ID, group ID, and group key. For all correspondence the vehicle uses only its pseudo-ID and hence the vehicle's anonymity is maintained. The RSU uses the group key to encrypt messages that it sends to its region's vehicles. So, all messages are encrypted, and the messages cannot be decrypted by any intruder. Vehicles do not broadcast messages to other vehicles for the dissemination of observed phenomena; instead, they use nearby RSU to spread the messages on their behalf. When a vehicle senses an event and wants to disseminate it to other vehicles in particular regions, it simply sends it to the nearby RSU (through the intermediate vehicles using the available routing algorithm, if the RSU is not within the transmission range of the vehicle). The nearby RSU authenticates the vehicle transmitting the message, checks the validity of the message and then transmits the message to the vehicles in the regions concerned
By other RSUs. If a message sent by a vehicle has to be tracked to the vehicles transmitting the message, this can be achieved with the aid of the RSUs because the RSUs hold the table linking the vehicles' pseudo-IDs to their actual IDs. A car never conveys a message to other vehicles. The RSUs are responsible for disseminating messages to other vehicles and thus this strategy is scalable. Messages exchanged are usually small so OBUs can use symmetric key for encryption without incurring a lot of overhead computation and RSUs can use the public key of receiving RSUs to encrypt and send messages to them; however, the algorithm can be easily adjusted so that RSUs can use symmetric key for encryption after setting a shared symmetric key with the receiving RSUs.

When a vehicle V_i wants to send a message M to the nearby RSU_j
  Let $M_i = ID_{RSU_j}, PID_{V_i}, \{M, T_s, S_q\}K_{V\_RSU}$
  Send M_i to the next hop towards the RSU

When a vehicle V_j receives the message M_i from V_i
  Let $M_j = ID_{RSU_j}, PID_{V_i}, M_i, dgt_j$,
    where $dgt_j = E(H(M_i), K_{V\_RSU})$
  Send M_j to the next hop towards the RSU

When an RSU with id ID_{RSU_i} receives a message M_k from vehicle V_k,
  It peels of the onion M_k, and retrieves the message M
  Sets h based on nature of message
  Let $M_{type1} = GID_i, \{M, Ts, Sq, dgt_i\}K_{G_i}$,
    where $dgt_i = E(H(M), SK_{R_i})$
  Disseminate M_{type1} to all vehicles in the table if needed
  if $h > 0$ then
    $h = h - 1$
    Let $M_{type2} = ID_{receiver\_RSU}, ID_{RSU_i}$,
    $\{M, Ts, Sq, h, dgt_i\}PK_{receiver\_RSU}$,
      where $dgt_i = E(H(M), SK_{RSU_i})$
    Forward M_{type2} to relevant neighboring RSUs
  end if

When an RSU with id ID_{RSU_j} receives a message M_{type2} from a neighboring RSU with ID ID_{RSU_i},
  Decrypt M_{type2} and retrieve M
  Let $M_{type1} = GID_j, \{M, Ts, Sq, dgt_j\}K_{G_j}$,
    where $dgt_j = E(H(M), SK_{RSU_j})$
  Disseminate M_{type1} to all vehicles in the table
  if $h > 0$ then
    $h = h - 1$
    Let $M_{type2} = ID_{receiver\_RSU}, ID_{RSU_j}$,
    $\{M, Ts, Sq, h, dgt_j\}PK_{receiver\_RSU}$,
      where $dgt_j = E(H(M), SK_{R_j})$
    Forward M_{type2} to relevant RSUs
  end if

When a vehicle V receives a message M_{type1} from an RSU_i
  Decrypts the message M_{type1} using group key
  and consumes it

Figure 3: The Algorithm

4. PERFORMANCE COMPARISON

In this section we compare our protocol with some related works already in existence. The protocol proposed in [17] ensures safe message delivery. But this is not portable since

every vehicle needs to be preloaded with all other vehicles' private keys and their corresponding anonymous certificates. As the number of vehicles grows in the network, it is difficult not only to keep those security data, but also storage problems can arise due to the large number of private keys and certificates that need to be stored in the limited storage space available in OBUs. In contrast, in our protocol, vehicles do not need to store the private keys and certificates of other vehicles in order to authenticate messages since RSUs authenticate messages on behalf of vehicles, therefore the storage requirements are very low compared to the above protocol.

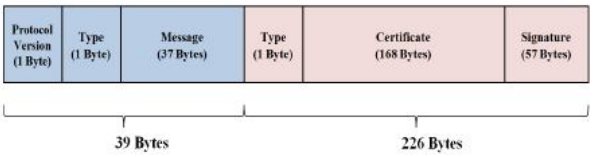

Figure 4: The Format of a Signed Message in IEEE Standard

When a vehicle sends a message, the message is attached with a certificate and a signature to authenticate the message and to ensure the integrity of the message. Figure 4 shows the signed message format derived from IEEE 1609.2 Standard [18]; the message size is 265 bytes including 39-bytes of unsigned message area, 169-bytes of certificate, and 57-bytes of signature.

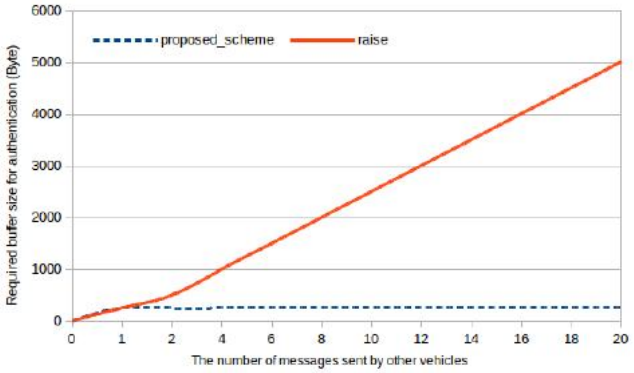

Figure 5: Storage Usage vs. Traffic Load

Figure 5 illustrates the relationship between storage usage and traffic load. The use of storage represents the buffer size needed for messages waiting to be authenticated on OBUs and the traffic load represents the number of messages sent by other vehicles. Since each signed message is 265 bytes long, the required buffer size for storing the unauthenticated messages increases under RAISE [19] as the traffic load increases while the required buffer size for storing the received message is constant under our Protocol. RAISE performs better than the PKI-based protocol[18] and community signature protocol [20] in terms of packet loss, packet delay and overhead communication because vehicles can simply authenticate messages once validation messages are received from the RSU; however, all messages received from other vehicles must be buffered by each vehicle before validation messages arrive. Thus, as message traffic increases, the vehicles demand more buffer space. The required buffer space is thus proportional to the load on the traffic. On the other hand, our protocol will not keep messages in the OBUs buffer until they are authenticated as RSUs send authenticated messages directly to the vehicles. Therefore, the buffer needed to store messages at OBUs under our protocol does not increase as the traffic load increases.

Under our protocol, messages sent by vehicles do not need to be authenticated and checked by other vehicles; RSUs that have higher processing power and lager storage than OBUs in vehicles do authenticate messages. Figures [6,7,8] compare RAISE [19] with our protocol regarding the number of retransmissions and the number of original messages sent as the number of participating vehicles ranges from 10 to 30 in the network. Under our protocol the number of message transmissions is obtained using the following equation:

$$T_n^1 = (V_n * M_n) * 1B + (M_n + 1U),$$

where T^1_n is the number of messages sent, V_n is the number of vehicles in the network, 1B is 1 broadcast and 1U is 1 unicast. And the number of message transmissions for RAISE is obtained using the following equation:

$$T_n^2 = (V_n * M_n) * 2B,$$

where T^2_n is the number of message communication, V_n is the number of vehicles in the network, and 2B is 2 broadcasts. Under RAISE, every message will be stored in each vehicle until an RSU validation message arrives, so vehicles will send a message once and the RSU will broadcast it again after verification of the message. However, under our protocol, vehicles only send a message to the RSU to reduce overhead contact and only the RSU sends the checked message to the vehicles in specific areas (through other RSUs if needed). Thus the number of message retransmissions under our protocol is reduced and this reduction obviously becomes noticeable as the number of vehicles sending messages increases.

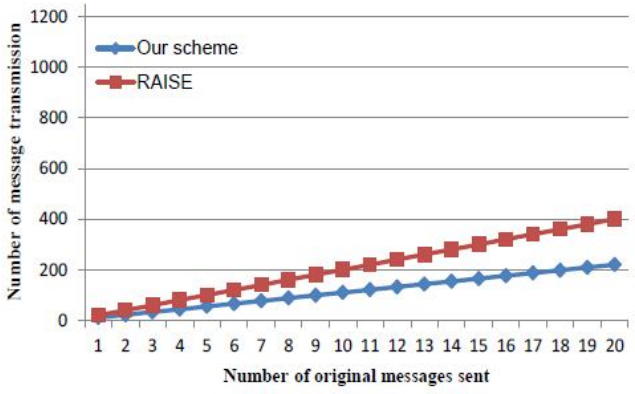

Figure 6: Number of Message Transmissions with 10 Vehicles

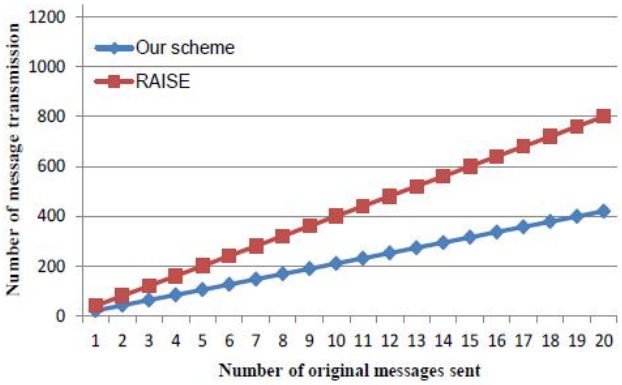

Figure 7: Number of Message transmissions with 20 Vehicles

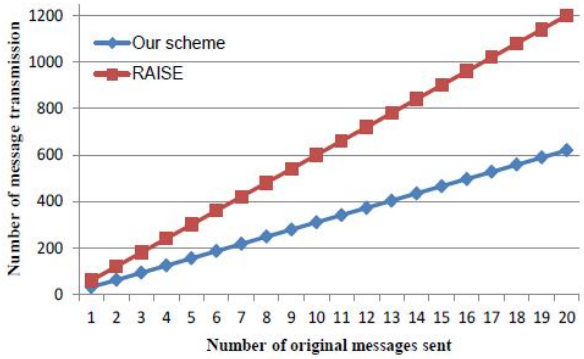

Figure 8: Number of Message Transmissions with 30 Vehicles

5. CONCLUSION AND FUTURE SCOPE

In this paper, we presented an efficient protocol for propagating the phenomena observed by vehicles in VANETs to vehicles in appropriate regions (such as accidents, road conditions, etc.) so that they can use them for informed decision making. Our protocol uses RSUs with higher computational power than OBUs for the dissemination of authenticated messages sent by vehicles within the transmission range of the RSU. Since multiple vehicles within an RSU's transmission range can observe the same phenomenon and inform the RSU about it, the RSU can suppress these messages from further dissemination regarding the observation of the same phenomenon. In addition, the RSUs have the opportunity under our system to check the sender 's validity and the credibility of the message before disseminating it to the other vehicles. Their method protects the senders' anonymity while, when needed by law enforcement authorities, at the same time helping trace a message to its sender.

REFERENCES

1. Dua, N. Kumar, and S. Bawa, "**A systematic review on routing protocols for vehicular ad hoc networks,**" *Vehicular Communications*, vol. 1, no. 1, pp. 33-52, 2014. https://doi.org/10.1016/j.vehcom.2014.01.001
2. N. Kumar and J.-H. Lee, "**Peer-to-peer cooperative caching for data dissemination in urban vehicular communications,**" *IEEE Systems Journal*, vol. 8, no. 4, pp. 1136-1144, 2014. https://doi.org/10.1109/JSYST.2013.2285611
3. N. Kumar, S. Misra, and M. S. Obaidat, **"Collaborative learning automata-based routing for rescue operations in dense urban regions using vehicular sensor networks,"** *IEEE Systems Journal*, vol. 9, no. 3, pp. 1081-1090, 2015.
4. S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, **"A comprehensive survey on vehicular ad hoc network,"** *Journal of network and computer applications*, vol. 37, pp. 380-392, 2014. https://doi.org/10.1016/j.jnca.2013.02.036
5. V. Namboodiri and L. Gao, **"Prediction-based routing for vehicular ad hoc networks,"** *IEEE Transactions on Vehicular Technology*, vol. 56, no. 4, pp. 2332-2345, 2007. https://doi.org/10.1109/TVT.2007.897656
6. C. E. Perkins and P. Bhagwat, **"Highly dynamic destination-sequenced distance vector routing (DSDV) for mobile computers,"** *in ACM SIGCOMM computer communication review*, vol. 24, no. 4. ACM, London, UK, Aug 31 - Sep 2, 1994, pp. 234-244.
7. G. Pei, M. Gerla, and T.-W. Chen, **"Fisheye state routing: A routing scheme for ad hoc wireless networks,"** *in IEEE International Conference on Communications*, ICC 2000, vol. 1. IEEE, New Orleans, LA, 18-22 June, 2000, pp. 70-74.
8. J. Toutouh, J. Garcfia-Nieto, and E. Alba, **"Intelligent OLSR routing protocol optimization for VANETs,"** *IEEE Transactions on Vehicular Technology*, vol. 61, no. 4, pp. 1884-1894, 2012.
9. M. Bakhouya, J. Gaber, and P. Lorenz, **"An adaptive approach for information dissemination in vehicular ad hoc networks,"** *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1971-1978, 2011.
10. N. Maslekar, J. Mouzna, M. Boussedjra, and H. Labiod, **"CATS: An adaptive traffic signal system based on car-to-car communication,"** *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1308-1315, 2013. https://doi.org/10.1016/j.jnca.2012.05.011
11. B. Ying, D. Makrakis, and H. T. Mouftah, **"Privacy preserving broadcast message authentication protocol for VANETs,"** *Journal of Network and Computer Applications*, vol. 36, no. 5, pp. 1352-1364, 2013.
12. R. A. Santos, A. Edwards, R. Edwards, and N. L. Seed, **"Performance evaluation of routing protocols in vehicular ad-hoc networks,"** *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 1, no. 1-2, pp. 80-91, 2005.
13. R. Kumar and K. Arya, **"A modified approach for route maintenance using alternate path in AODV,"** *in 2011 International Conference on Computational Intelligence and Communication Networks (CICN). IEEE*, Gwalior, India, 7-9 Oct, 2011, pp. 37-41.

14. M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, **"Evaluating the impact of a novel message dissemination scheme for vehicular networks using real maps,"** *Transportation Research Part C: Emerging Technologies*, vol. 25, pp. 61-80, 2012. https://doi.org/10.1016/j.trc.2012.04.017
15. W. Diffie and M. E. Hellman. **"New directions in cryptography"**. *IEEE Transactions on Information Theory*, 22(6):644{654, 1976.
16. Maxim Raya, Adel Aziz, and Jean-Pierre Hubaux. **"Efficient secure aggregation in vanets"**. *In Proceedings of the 3rd International Workshop on Vehicular ad hoc Networks*. VANET '06, pages 67-75, September 2006.
17. M Raya and JP Hubaux. **"Securing vehicular ad hoc networks".** *Journal of Computer Security*, 15(1):39-68, 2007.
18. IEEE Standard 1609.2. **"IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - security services for applications and management messages**". *IEEE Standard*, July 2006.
19. Chenxi Zhang, Xiaodong Lin, Rongxing Lu, and Pin Han Ho. **"RAISE: An efficient rsu-aided message authentication scheme in vehicular communication networks"**. *In Proceedings of IEEE International Conference Communications. ICC'08.*, pages 1451-1457, Beijing, May 2008.
20. 44 Xiaodong Lin, Xiaoting Sun, Pin Han Ho, and Xuemin Shen. **"GSIS: A secure and privacy-preserving protocol for vehicular communications".** *IEEE Transactions on Vehicular Technology*, 56(6):3442-3456, 2007.
https://doi.org/10.1109/TVT.2007.906878