Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P) Vol.3 No.2, 2014, pp.12-17
© The Research Publication, www.trp.org.in
DOI: https://doi.org/10.51983/ajcst-2014.3.2.1740

A Warning Message Dissemination Scheme with User Privacy and Message Integrity for VANET

Salini Balakrishnan and Tripti C
Department of Computer Science, Rajagiri School of Engineering and Technology, Cochin, India
Email: salini.lunar@gmail.com

(Received 11 July 2014; Revised 22 July 2014; Accepted 19 August 2014; Available online 28 August 2014)

Abstract—Vehicular ad hoc networks (VANETs) are wireless networks which are infrastructure-less in nature because of the highly mobile nodes (vehicles) in the network. Warning message dissemination can be considered as the primary application of VANET, where in alert messages need to be quickly as well as smartly disseminated in the network to make it available for a large number of vehicles. A scheme will be effective once it reaches to maximum number of vehicles with minimum overhead and delay, for attaining the same a broadcast scheme is familiarized in this paper along with user privacy and message integrity. User privacy is an added advantage for all the participating vehicles which makes the system more acceptable as a whole. Protecting the privacy of users leads to undesirable tracking of vehicles by attackers. Apart from user privacy, message integrity is also been guaranteed in the proposed scheme. Integrity of the message can be checked in order to confirm whether the received alert is genuine. This paper presents a warning message dissemination scheme along with the mechanisms to ensure user privacy and message integrity.

Keywords-Warning Message Scheme; Alert Notification; User Privacy; Message Integrity; Broadcast Scheme;

I. INTRODUCTION

Vehicular Ad hoc Network (VANET) is a subset of Mobile Ad hoc Network (MANET), to facilitate the communication feature amongst neighbouring vehicles and Road Side Units (RSU) using two types of communications, namely Vehicle-to-Vehicle Communication (V2V) and Vehicle-to-Infrastructure Communication (V2I) Fig. 1. In VANET every vehicle can be considered as a wireless router or node, which helps to connect with the vehicles moving in and out of the communication range and thus leads to frequently varying topology. VANET is considered to be an intelligent way to improve the experience of users while they move, giving it features like self-organized and at the same time distributed network with dynamic network topology [1].

Vehicles in VANET are expected to follow an organized pattern like in a highway, than the case with nodes in MANET. Safety, comfort and commercial applications being the main objective of VANET, the system is get-ting increasingly accepted by the users world-wide. Safety applications focus on monitoring the road, neighbouringvehicles and topology of the road. Comfort applications will concentrate on road traffic management there by making the road conditions favourable for the users. Commercial applications take care of the entertainment side, by providing web access, multi-player games, audio or video streaming etc.

Among the three main applications of VANET, Safety application plays the significant role by reducing the number of accidents by effectively notifying warning messages on time. The study in [2], reveals that warning the drivers half a second before the accident can reduce the number of accidents by more than 50% of what is happening now. The safety applications are relevant mainly in three scenarios, they are: Accidents Warning, Intersection Warning and Road Safety Applications [3].

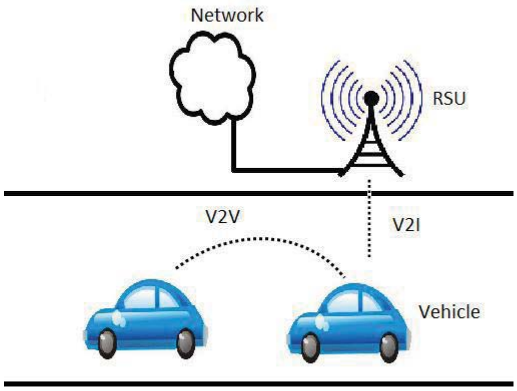

Figure 1: V2V and V2I Communication

Accident warning is provided by alerting the drivers about the accident which occurred ahead of the road and there by drivers will have an extra time to react accordingly reducing the chance of chain collision. The alert messages needs to be broadcasted in the immediate vicinity to make it available to the neighbours. Intersections warning reduce the possibility of accidents on high traffic junctions or intersections. Normally on intersections with two or three lane roads converge to, it is highly complicated for the drivers and leads to high chance of accidents. So intersection warning helps the drivers to get hold of the situation more effectively. Road congestion Warning at the same time warns about congested road and helps in choosing the best route for the vehicles to ensure smooth traffic on road.

The remainder of the paper is organized as follows: The related works similar to the proposed scheme is being familiarized in section II, in section III the proposed warning message dissemination scheme is explained in detail. Later then the importance and explanation on how message integrity and user privacy is preserved in the scheme is presented in section IV and then with a conclusion note the paper is summarized.

II. RELATED WORKS

In [4], a novel alert dissemination protocol is proposed where asymmetric and adverse radio channel communication is expected. Multi-hop is attained by taking immediate neighbours to relay the messages. End-to-End communication delays, data traffic redundancy and bandwidth utilization was high in this scheme. Ineffective alert message dissemination like this will eventually lead to many problems like broadcast storm problems. A scheme called Profile-driven Adaptive Warning Dissemination Scheme (PAWDS) [5] makes use of city road maps, uses an adaptive technique but work well when the node density is high to make the scheme be available with a lot of information of the streets. Multicast schemes like [6] a routing strategy for disseminating warning messages in Cooperative collision warning systems (CCWS) is presented. The scheme incorporated uses the concept of adaptive transmission range to identify the receiver nodes. All the required inputs, parameters and functions are obtained from the beacon messages.

In [7], a scheme in order to protect vehicle privacy and traceability is presented. A pool of short-lifetime pseudonyms are loaded in the vehicle during the time of registration. The vehicle needs to request for pseudonym update when the network is accessible and while travelling through a less crowded area. Credential Revocation List (CRL) is also maintained for revoking malicious users. But the very same usage makes the system more and more infrastructure dependant. In [8], message authentication is being focused by elliptic curve digital signature algorithm (ECDSA) approach. The proposed scheme also supports conditional privacy. The signatures are secured by ECDSA approach. Temporary identities from secure cryptographic techniques will be loaded in vehicles. Privacy of a user is preserved when vehicles uses the temporary identities for any of their communications.

In [9], Temporary Anonymous Certified Keys (TACK) system is used to protect the message integrity. The broadcast messages from the vehicle will be signed using pub-lic/private key pair. Message integrity is covered by the fact that only the owner can generate the signature from its private key. For a short period a single key-pair is used by the On Board Unit (OBU) for signing the messages. Message integrity is ensured by assuming that the underlying cryptography is secure. In [10], an adaptive protocol is presented which claims to improve the performance of an alert dissemination application of VANET. Broadcast-storm problem is addressed with adaptive wait-windows and with adaptive probability to transmit. After the initial broadcast of the alert message, rebroadcast is done with an adaptive probability. But here on each hop the message is getting rebroadcasted that will eventually causes a lot of copies of the same message in the system which is being rectified in this proposed paper.

III. THE PROPOSED WARNING MESSAGE DISSEMINATION SCHEME

A. Design Approach

Broadcasting is a vital function in wireless adhoc networks especially due to its highly dynamic nature and to provide functionalities like service discovery and data dissemination. While flooding technique leads to broadcast storm problem, where in each node rebroadcasts the messages to the system. Eventually it leads to highly redundant transmission, channel contention and packet collision as well. The general phases in the broadcast design satisfy the following procedures once a node receives an emergency broadcast message:

Message Confirmation: Each node needs to confirm whether the message is a redundant one and whether the message is an irrelevant one. To achieve this, certain data are recorded at each node and in the message header.

Rebroadcast decision: This is the core of any broadcast scheme, that determines whether one node needs to rebroadcast a message or not. The number and positions of rebroadcast nodes are important issues for reducing the effects of broadcast storm, shadowing, and intersection problems.

Connection hole prevention: The traffic flow can be interrupted in the system leading to a gap which blocks the data delivery due to less connectivity which is called as connection hole problem. By data buffering the issue is been addressed here. Carry-and-forward method overcomes the connection hole problem effectively.

Waiting delay: To prevent redundant rebroadcast, one node needs to wait for a certain delay time during which it can listen to the activities of other neighboring nodes so it can make a more accurate decision. Thus, a suitable waiting delay function is necessary.

Message confirmation feature is achieved by using a sequence number while sending each emergency message along with the source id. In order to perform message confirmation, the sequence number and source id can be extracted to check whether the message is already stored in the vehicle. Only if it is a new message, the vehicle is made to store the received emergency message. So before storing each message a redundancy check is being designed.

The rebroadcast decision can be made either by the receiver (receiver-initiated) or by the sender itself (sender-initiated). In the former scheme, receiver node decides whether it should rebroadcast or perform the next-hop of the message. While in the later scheme, the sender node chooses which node among its neighbour list will do the next-hop. In the proposed scheme, the sender-initiated scheme is being used and is done by calculating the Euclidean distance between sender node and its neighbours. The farthest node from the sender at that time point is chosen to propagate the emergency message further. By choosing the farthest node, the scheme takes advantage of maximum coverage area at minimum time.

Partially connected networks are well suited with the help of connection hole prevention feature. In this feature, messages are propagated in the network by carry-forward mechanism. When the network is fragmented, a message from one network fragment is carried and forwarded by a vehicle to the other nearby network fragments. This feature demands buffer space in each vehicle to make it possible.

A variable delay is introduced in the broadcast scheme so that second-hop of messages will happen only after a delay time. By introducing a waiting delay, an unnecessary broadcast can be made cancelled by making an early broadcast. The same is valid in the reverse case as well, like the latest rebroadcast can correct the earlier one with the updated information. Thereby waiting delay introduces advantages to the system like low redundancy and high reliability.

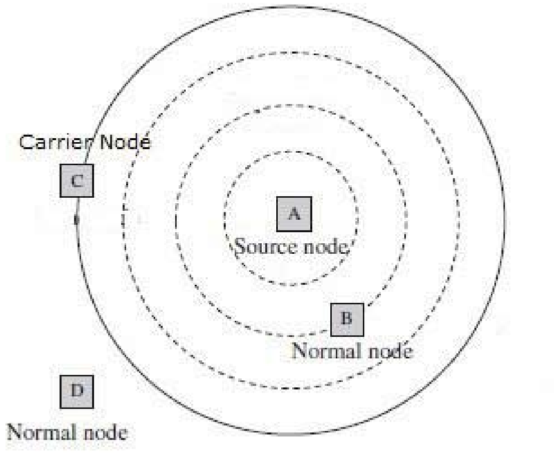

Figure 2: Nodes in the System

B. The Proposed System

The proposed method in an emergency event is a combination of broadcast and multicast. The scenario is initiated when a vehicle detects or come across an emergency event. An emergency message is broadcasted as soon as an emergency event is detected by the vehicle. By broadcasting the emergency message on the first hop, the source vehicle covers all the vehicles in its coverage area alerting them all about the emergency event. Later on message is propagated in the system by another node from the neighbouring list, which can be identified by the source node by analyzing the distance as the deciding factor.

The vehicle chosen for the next hop will multicast the emergency message further in the system so that, the alert is spread across further. In the design the vehicles are categorized as different types of nodes according to the situation. The different types of node considerations are described below and it is shown in Fig. 2 :

Normal Node: as the name suggest, its just any other node in the network, mainly in the state of listening for incoming messages and sending Hello packets periodically.

Source Node: the node which come across an emergency situation and initiates the alert dissemination.

Carrier Node: node that is selected by the sender to forward the emergency message for the next-hop.

Receiver Node: the node who received a message from the sender, source node or carrier node.

Basically, every node in the network always retains its role as a normal node. A normal node that detects an emergency event would start the warning service instantly by broadcasting the emergency packet. An external event causes a normal node to change its role to a Source Node. After a single-hop broadcast operation this node will be considered as a normal node again. If any packet is received by a normal node, then it will be considered just as a receiver node. The role transition diagram is depicted in Fig. 3:

When an emergency packet is being received, at first, the receiver node cleans up a redundant or invalid broadcast packet (message confirmation phase). If the received packet is not already present in the event table and is a valid event ie. warning time is still alive then the event details received will be added to the receivers event table. Then it checks whether Source Node chose the receiver node to be a carrier node for further propagation of the emergency event. If so, the receiver node becomes the carrier node and forwards the message only to those in its neighbours who doesn't have the event in their list. This is a multicast operation, and is done by checking the event list of each of its neighbours. So that the packet will be further multicasted only to those neighbours who don't have the event listed in their corresponding event table.

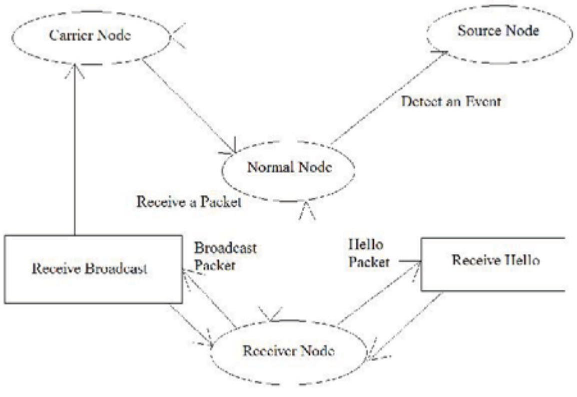

Figure 3: Nodes Role Transition

Hello packets are used for getting information on position of the near-by vehicles and so to update the neighbour list. There are two formats being used in the proposed scheme:

Basic : which carries the location of the node at that particular point of time.

Extended : comes as a reply packet after receiving a Hello packet which carries both the location of the node and the event details a node stores in the event table. Extended Hello packet is sent only to the newly found neighbours alone, not to the existing neighbours since it has already shared the event list once.

Each node in the system maintains two types of tables for better understanding of the network they are part of. They are :

Neighbor Table : The neighbor table records the status of its one-hop neighbors by listening to basic/extended hello packets. The time at which a recent hello from a neighbor is recorded in the neighbour table at recent hello time field. When the sender node goes outside the coverage area, it will be removed from the neighbour table accordingly. The successive location data received from a neighbor is recorded in the field of location history.

Event Table : The event table records valid emergency events that have been received or generated. Each entry has the same data fields as the emergency broadcast packet. An event list is generated by listing the pair of source ID and sequence number fields of each entry in the event table before sending an extended hello packet as a response to a hello packet received.

The data structures used in the proposed scheme can defined as :

Basic Hello Packet : Node ID / Node Location / Sequence Number

Extended Hello Packet : Node ID / Node Location /

Event List / Sequence Number

Emergency Broadcast Packet : Source ID / Event Content / Warning Area / Warning Time / Sender Location / Sequence Number

Neighbour Table : Node ID / Recent Hello Time / Location History

Event Table : Source ID / Event Content / Warning Area / Warning Time / Sender Location / Sequence Number

An emergency event is enclosed in an emergency broadcast packet in a particular format. An emergency broadcast packet will have a source ID field, which holds the information of the source node. A sequence number field is included in the packet, the combination of the source ID and sequence number fields uniquely identifies an emergency broadcast packet. The alert message will be included in the event content field. In order to check the sender location, a sender location field is being used which gives the location of the node that is currently sending out this broadcast packet. There is another field that specifies the warning area to specify the area where drivers should keep on the alert. There is a warning time filed which indicates the point of time when the emergency event is expected to be cleared off.

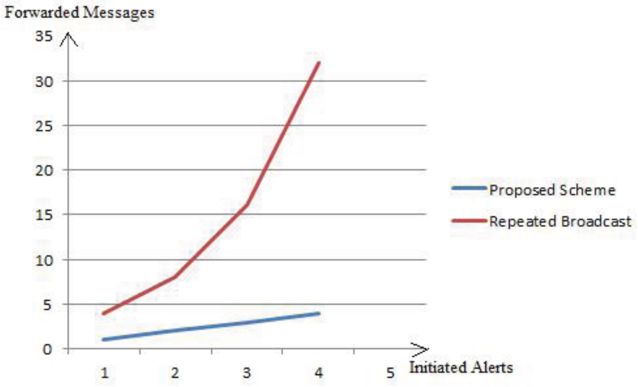

Figure 4: Comparison with Repeated Broadcast and the Proposed Scheme

An emergency event is valid for a node if the warning time is not expired and the node is currently located within the warning area. Since repeated broadcasting is avoided in the proposed scheme, broadcast storm problem is skipped or rectified. Number of duplicated messages and in effect the number of messages itself is drastically controlled by doing selective multicasting from second hop onwards. The graph showing the count difference is depicted in Fig. 4, where in the graph is plotted as a comparison between repeated broadcasting scheme and the proposed scheme.

C. Message Integrity and User Privacy

Users rely on their anonymity or privacy in the network, so a network lacking the same may not be easily accepted by the users. For instance, while preventing spoofing a vehicle’s permanent identity may be revealed and this violates privacy concern of a user. Privacy requirement and security enforcement can be balanced by codifying legal, societal and practical considerations. Privacy preserving law will differ in most countries and since main vehicle manufacturers aim on international market, there should be a system which satisfy most of these diverging laws or need to enable customization in the policies taken [11].

Users would not accept a system which has a loophole of being tracked. Still, complete anonymity is not a feasible measure at all now, especially since each vehicle got a license plate, which needs to be publicly displayed. So privacy as a whole cannot be assured in the system, even though we can ensure it to a certain acceptable level .In the proposed scheme, user privacy is achieved by encrypting the Source ID of each node before sending any packets like Hello, Extended Hello or Emergency Broadcast Packet, so that on the receivers side the ID of the sender will not be able to track or open. So that each user is guaranteed with the expected user privacy on identity while being in the system.

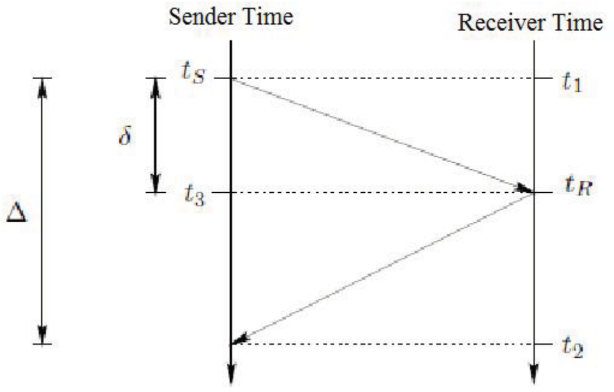

Figure 5: Time Synchronization

Likewise, the intended recipients should receive the original data or messages being sent rather than tampered or changed messages by any adversary in between. This requirement is crucial when it comes to road safety applications where we cannot afford an integrity violation [12]. So in the proposed scheme, message integrity is ensured by generating a Message Authentication Code (MAC) of the emergency event details part. In order to make the scheme work mainly it requires two important operations. They are, loosely time synchronizing sender and receiver as well as generation of a single hash key chain.

By loosely synchronizing time between a sender and receiver, the clock-skew and propagation delay between the two can be calculated vaguely. Time synchronization between two vehicles is depicted in Fig. 5.

Sender issues a time synchronization request to its neighbors at time t_S along with a nonce, at that time suppose, time at receiver end is t_1. The receiver replies to the request at time t_R with the same nonce . While loosely synchronizing time, the nodes are aimed to have an upper bound of the time difference. When the time of sender turns out to be t_s, the upper bound is calculated as t_r t_s - t_S + t_R and nonce value is also checked for its correctness. Even if the actual synchronization error is , loosely time synchronization is only concerned about the full round-trip time, which is 4.

For the Message Authentication Code a chain of keys are generated at a stretch. The key generation is shown in Fig 6. To start with, the last element of the chain is chosen, in the proposed scheme the last element is the vehicle id and the distance of the farthest node at that point of time is selected. Then by repeatedly applying a one-way hash function F a chain of keys are generated effectively. Finally from the complete chain of keys, the first element K_0 is dependent on the entire chain. Any element of the chain can be verified to be committed to the chain of keys by checking whether $F^{j\ i}(K_j) = K_i$ is i < j. The keys are used and revealed in the order opposite to its creation ie. in the order K_0, K_1,...., $K_{l\ 1}$, K_l. The keys are generated and stored on each vehicle and gets generated again once all the keys are used. N elements requires only log(N) storage and computation to access an element.

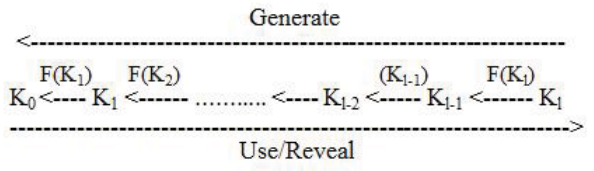
Generate
$F(K_1)$
$F(K_2)$
(K_{l-1})
$F(K_l)$
K_0 <---- K_1 <------ .... <---- K_{l-2} <----- K_{l-1} <------ K_l
Use/Reveal

Figure 6: Keys Generation

The Message Authentication Code (MAC) is generated with a key from the chain of keys generated and in the proposed scheme, the key will be disclosed to the vehicles after a small delay which can be considered as a Key Disclosure Delay. So each message will have a Message Authentication Code attached to it for the corresponding alert part. After the key disclosure delay receivers will be provided with the key and so by then they can generate a Message Authentication Code and confirm whether its the same which they have received on the last message. By loosely synchronizing the sender and receiver, each receiver knows about the round trip time between the two as well. So receivers buffer the incoming messages for a time which covers the key disclosure delay and the round trip time. Message integrity is assured by cross-checking the Message Authentication Code along which came along the message and by generating the code once the key is disclosed.

IV. CONCLUSION

The dissemination of safety-related messages is an important application in a vehicular network environment. Tra-ditional broadcast mechanisms designed for Mobile Adhoc Network (MANET) become inappropriate. Design of an efficient and high reliable broadcast scheme is a critical issue for improving traffic safety. The proposed warning dissemination scheme, follows a combination of broadcast and multicast methodology for implementing an efficient warning message dissemination service. By allowing the Source node to broadcast on the first-hop ensures maximum reachability and coverage for the emergency message. Later on, by restricting the forwarding of emergency message by Carrier node alone makes the scheme for efficient. By choosing the farthest node from source node's coverage area as carrier node make the maximum utilization of the coverage area and better forwarding of messages as well. User privacy and message integrity is an add-on features provided with the proposed warning message dissemination scheme.

REFERENCES

[1] A. Singh, M. Kumar, R. Rishi and D. K. Madan, ”A Relative Study of MANET and VANET : Its Applications, Broadcasting Approaches and Challenging Issues”, Department of Computer Science and Engineering, The Technological Institute of Textile and Science, Bhiwani, Haryana, India.

[2] C. D. Wang and J. P. Thompson, Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network, U.S. Patent 5613039, March, 1997

[3] P. Elumalai, P. Murukanantham, ”Reliable Data Dissemination for Car Safety Application in VANET”, Department of Electri-cal and Information Technology Faculty of Engineering, LTH, Lund University

[4] O.M.H Rehman, H. Bourdoucen, M. Ould-Khaoua, ”Efficient alert messages dissemination in vanets using single-hop dis-tributed protocols”, Dept. of Electr. & Comput. Eng., Sultan Qaboos Univ., Muscat, Oman

[5] F. Manuel, G.Peidad, J.Francisco, ”PAWDS: A Roadmap Profile-driven Adaptive System for Alert Dissemination in VANETs”, University of Zaragoza, Spain

[6] A. Sebastian, M. Tang, Y. Feng, and M. Looi, ”Multicast Routing Scheme for Efficient Safety Message Dissemination in VANET”, Queensland University of Technology, Brisbane Australia

[7] S. Jinyuan, Z. Chi, Z. Yanchao, F. Yuguang, ”An Identity- Based Security System for User Privacy in Vehicular Ad Hoc Networks”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 9, SEPTEMBER 2010

[8] M. Bharati, P. K. Saroj, T.C. Tarini, J.Debasish, K. J. Sanjay, ”A Secure and Efcient Message Authentication Protocol for VANETs with Privacy Preservation”, World Congress on In- formation and Communication Technologies, Mumbai, India, December 2011.

[9] S. Ahren, S. Elaine, B. Fan, P. Adrian, ”TACKing Together Efcient Authentication, Revocation, and Privacy in VANETs”, Carnegie Mellon University & General Motors

[10] S. Kanitsorn, P. Chotipat, ”An Adaptive Alert Message Dis- semination Protocol for VANET to Improve Road Safety”, FUZZ-IEEE, Korea, August 2009

[11] B. Parno, A. Perrig, ”Challenges in Securing Vehicular Net- works”, Carnegie Mellon University

[12] S. Balakrishnan, C. Tripti, R.Cyriac, ”Survey on Security Challenges in Warning Message Dissemination and Possible Solutions”, Asian Journal of Computer Science And Informa- tion Technology 4 : 3 (2014) 28 - 33.