Enhancing DSRC to Improve Reliability in Intelligent Transportation System

S.Sathya Karthika[1], J. Rethna virgil Jeny[2], J. Albert Simon[3]

Abstract—Vehicular Ad Hoc Network (VANET), which is based on Dedicated Short Range Communication (DSRC) provides an opportunity to enable communication based cooperative safety systems in order to reduce road accidents and improve traffic efficiency. This paper describes the reliability of the Dedicated Short Range Communication (DSRC) to provide message authentication scheme to ensure the received message is true and Prioritized Verification scheme among vehicles on the road for safe driving in Intelligent Transportation System. Particularly, DSRC supports both Public Safety and Private operations in roadside to vehicle and vehicle to vehicle communication modes. The co-existence of safety and non-safety messages are achieved through a periodic channel switching scheme whereby access to DSRC alternates between these two classes of applications. This model efficiently improves the receiving status by deals with the impact of false and misleading messages to its neighbors in dense and high mobility conditions. To mitigate the issue, Elliptic Curve Digital Signature Algorithm (ECDSA) is introduced so that messages of each traffic classes are verified following the VANET's medium access control (MAC) layer priorities and the application relevance of individual safety messages. Performance analysis and simulation result shows that this approach is secure, privacy preserving and resource efficient.

Index Terms—VANET, DSRC, vehicle to vehicle communication, ECDSA.

1. INTRODUCTION

In Vehicular Ad-hoc Network (VANET), the amount of interference from neighboring nodes to a communication link is governed by the vehicle density dynamics in vicinity and transmission probabilities of terminals. Dedicated Short Range Communications Protocol is a multi-channel wireless protocol, based on the IEEE 802.11a Physical Layer and the IEEE 802.11 MAC Layer. It operates over a 75 MHz licensed spectrum in the 5.9 GHz band allocated by the FCC for the support of low latency vehicle-to-vehicle and vehicle-to-infrastructure communications. The DSRC [7] band is divided into 7 channels, one control channel to support safety applications and 6 service channels to support non-safety applications. Prioritizing safety messages over non-safety ones is one of the DSRC MAC layer capabilities, this being related to multichannel coordination. The motivation behind the development of DSRC is based mainly on the need for a more tightly controlled spectrum for maximized reliability. Decline of road accidents, traffic congestion and privacy enhancing mechanisms are some serious challenge in VANET. Vehicular Ad-Hoc Network (VANET) provides a unique opportunity to establish communication based helpful safety systems. DSRC technology is envisioned as a key enabler technology for VANET. DSRC technology is based on a cost effective local area network technology. Channel conditions, node density and dynamic topology changes create challenges in VANET. Chain collision is occurred at high density and mobility conditions, that reduces the performance of DSRC protocol [10]. WAVE [5] will use CSMA/CA with EDCA [6] protocol that defines how network devices respond when two devices attempt to use a data channel simultaneously and encounter a data collision. The CSMA/CA[2] defines how long the device should wait if a collision occurs. When the medium becomes idle, the data node next in queue is able to transmit data. The data node next in queue waits for the medium to be idle again and then transmits its data. After each data node transmits the data, then the transmission order is updated to reflect what data nodes have previously transmitted, moving each data node through the queue. In IEEE 802.11p

- [1]*S.Sathya karthika, P.G Scholar, Sardar Raja College of Engineering,Tamil Nadu, India.*
- [2]*J.Rethna Virjil Jeny, Assistant Professor and Head, Sardar Raja College of Engineering,Tamil Nadu, India.*
- [3]*J.Albert Simon, Assistant Professor , Sardar Raja College of Engineering,Tamil Nadu, India.*

[3], vehicles will not send any acknowledgement for the broadcasted packets. Therefore, the transmitter cannot detect the failure of the packet reception and hence will not retransmit it and an ordinary signature scheme reveals the actual identity of a signer, which is undesirable as far as privacy, is concerned. Again, unconditional privacy may impair the prospect of vehicular communications since an anonymous entity could deliberately transmit some false and misleading messages to its neighbors. Hence, a VANET entity should be accountable to the corresponding authority in case of a critical event or dispute on road [4]. These are serious problems in VANET safety applications where all vehicles behind the accident have to receive the warning message successfully and safely in a short time to avoid chain collisions. This problem motivates us to propose an analytical model for assessing the DSRC reliability and delay taking into account the multipath fading channel in VANETs, vehicles high mobility, hidden terminal problem, Unauthorized access and transmission collisions. More specifically, the probability of successfully receiving the status messages from all vehicles around the tagged vehicle, the probability of receiving the safety or emergency messages from all vehicles up to a certain distance behind the accident scene and the delay for that safety messages to reach their intended recipients will be studied assuming unsaturated conditions.

Proposed model is built based on a new mobility model that takes into account the vehicle's follow-on safety rule to accurately derive the relationship between vehicle's speed and network density. It is shown that the current specifications of the DSRC [9] may lead to severe performance degradation in dense and high mobility conditions. While verifying messages signature verification incurs a cryptographic processing delay at the verifier's end. Although the verification delay is on the order of milliseconds, under a heavy-traffic scenario, many of the safety messages would be either discarded due to the constrained buffer size of the verification process or accepted without any verification. Therefore, during a busy traffic hour, a receiver of vehicular messages would either risk a fatal road traffic consequence, or it would reject a significant portion of received messages without authenticating as soon as its maximum verification capacity is reached. Therefore, ECDSA is introduced to increase the system's reliability in terms of the probability of packet's successful receptions and time delay of emergency messages in a harsh vehicular environment.

2. METHODOLOGY

2.1 Message Broadcasting

VANET is a self-organizing network that works on both Inter-Vehicle Communication (IVC) and Vehicle to Infrastructure communication. IVC is taken into consideration where vehicles will be equipped with sensors and GPS systems to collect information about their speed, position, direction and acceleration to be broadcasted to all vehicles within their range. Inter-Vehicle Communication (IVC) is used to classical Mobile Ad Hoc Network research. The management and control of network connections among vehicles or between vehicles and an existing network infrastructure is currently one of the most challenging research fields in the networking domain. While there are some similarities to research fields such as mobile ad-hoc networks or wireless sensor networks, the explicit characteristics of vehicular networks require different communication paradigms, different approaches to privacy and security and different wireless communication systems.

2.2 Channel Allocation

Each vehicle will alternate between the Control channel (CCH) and one of the Service Channel (SCH). On the control channel each vehicle will send periodic status messages or beacons which include its position and status information like speed, acceleration and direction to its neighboring vehicles. Upon receiving these beacons, vehicles will process this information. If any dangerous condition is detected, the vehicle can send a warning message with high priority access class to all other vehicles in the direction of interest for a certain distance to alert drivers to take the right action on time. Each vehicle will alternate between the control channel (CCH) and one of the service Channel (SCH).

2.3 Checking Density and Mobility

The proposed VANET mobility model is built based on a one way multi lane highway segment.

In VANETs, the communication range is much larger than the width of the road. Therefore, the network in each direction of the road is simplified as a one dimensional VANET. Vehicles will follow the direction of the road with a speed uniformly distributed between V_{min} and V_{max} with mean

$$\mu = (V_{min} + V_{max})/2 \qquad (2.1)$$

and variance

$$\sigma^2 = ((V_{min} + V_{max})^2)/12 \qquad (2.2)$$

In this model, the distribution of vehicles on the road, number of vehicles (N_c) around the transmitter (contention region) and the number of vehicles (N_h) in the hidden terminal areas (interference region) are estimated efficiently. An arbitrary starting point of the highway is first defined, and the number of vehicles that cross the starting point in each lane (assume the road has N_l lanes) is modeled as Poisson process with average rate β_i vehicles for the ith lane, such that the total number of vehicles per second that cross that point is

$$\beta = \sum_{i=1}^{N_l} \beta_i \qquad (2.3)$$

The Poisson process is a sufficiently accurate assumption for modeling vehicle's arrival process in a highway scenario. It is assumed that vehicles move independently of each other; hence, the total distance that a vehicle travels during an interval of (0, t) approaches a normal distribution and the inter-distance between two vehicles crossed that point with time difference τ_d also has normal distribution. To find the probability of having N_c vehicles within the range of any tagged vehicle, the mobility model [8] is extended to include the minimum safety distance between vehicles in each lane (t_s seconds rule). This means that the following vehicle, which is traveling with speed V_j, has to keep a safe distance (d_{th}) from the in front vehicle such that $d_{th} > V_j t_s$ to avoid an accident if the front vehicle stops suddenly. This minimum distance is a random variable and depends on the following vehicle's speed V_j if a fixed t_s is assumed, which is the response time for the driver to react on a sudden incident.

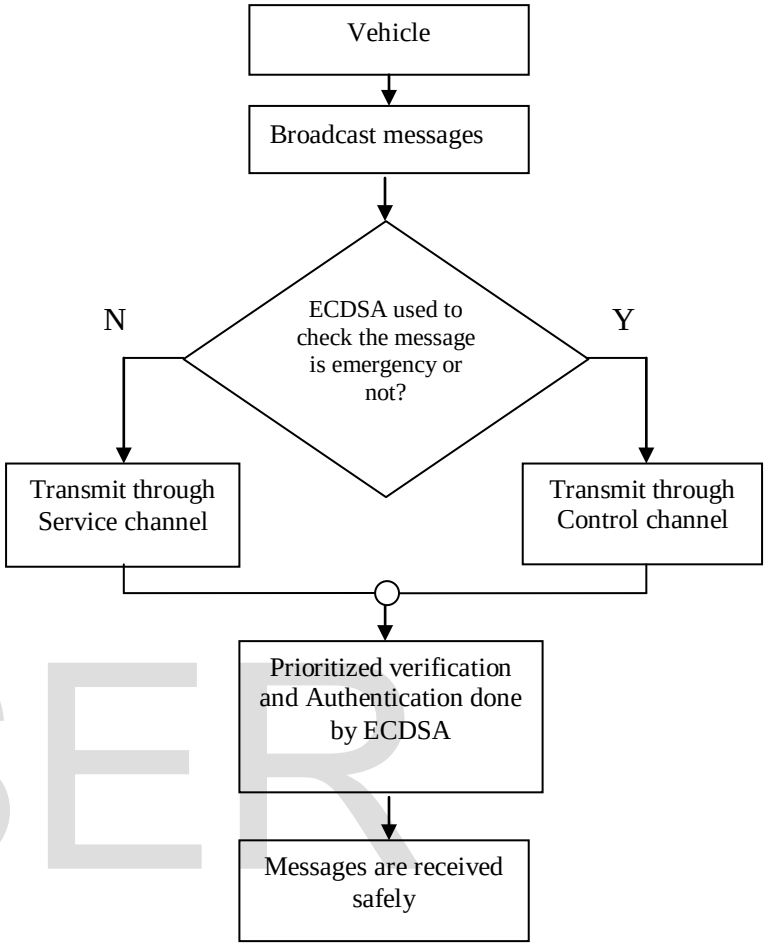

Fig. 1. Flow diagram to increase successful reception rate and to decrease delay

Evolving route selection parameters such as relative lane information, queue occupancy, speed of vehicles, link state and number of intermediate hops are useful in taking lifetime decision in VANET routing. For broadcasting of safety information in a VANET, identify packet-centric forwarding and information-centric forwarding as two basic approaches for information dissemination, and derive the necessity to support heterogeneous network architecture.

It shows that there are many conflicting parameters that affect the system reliability and its success rate. Keeping these parameters with the

fixed values as specified in the standard [1] will result in undesired performance, especially in a harsh vehicular environment where vehicles are moving in a very high speed and their density on the road is changing very frequently. That is, in a matter of seconds, the vehicle density could change from light density to the jam situation. Therefore, vehicles have to change their sending rate (λ_s), communication range (R) or (transmission power), carrier sense range (L_{CS}) and/or their minimum contention window size (W_s) based on the situation on the road in order to increase the success rate and VANETs reliability.

Several factors have been considered, such as the impact of mobility on the link availability between the transmitter and the receiver, the distribution of vehicles on the road and the average number of vehicles within the range of the transmitter. The proposed model is built on the fact that vehicles are broadcasting their status messages within the synchronization interval and in this model, each vehicle has one-dimensional Markov chain including the channel busy probability in every state. It is shown analytically and by simulation that the effective maximum communication range can be used in certain conditions to achieve certain successful rate.

When a vehicle encounters an emergency situation such as an accident, lane change or slowing down below a certain threshold speed is analyzed. The vehicle that is involved in an emergency situation will send an emergency packet to all vehicles behind it who will select another vehicle as a relay node to rebroadcast the message to its neighbors. The emergency message continues to propagate until it reaches a certain distance D defined within the message itself. The vehicle uses the high priority access class to send the emergency message after sensing an idle channel for an Arbitration Inter Frame Space Number (AIFSN). In order to increase the success packet reception, vehicles have to change their sending rate, communication range, carrier sense range and minimum contention window size. When the vehicle density increased, the effective range and success rate will decreased. At the same time the status packet delay will increase resulting in decreasing the system reliability. Increasing the carrier sense range will increase the contention region and decrease the hidden terminal region.

2.4 ECDSA Based Signature Generation

Elliptic Curve Digital Signature Algorithm generate digital signature and verification using Public and Private Key pairs with respect to a particular set of elliptic curve domain parameters.

ECDSA Domain Parameters are given by,

a. Centralized Authority chooses system secret x, where $1 < x < q$, and computes $Q = xG$.

b. CA associates random primary secret k_i (where $1 < k_i < q$) with each individual OBU_i of a particular type. The vehicle-type identifier $R_i = k_iG$. Suppose, i, i + 1, i +2, . . . , i + N − 1 are registered vehicles. CA computes the group identifier $R_i=k_i(\text{mod } q)G=k_{i+1}(\text{mod } q)G=k_{i+2}(\text{mod } q)G =\ldots.. = k_{i+N-1}(\text{mod } q)G$.

c. Hash function $H_1(.)$ is used for computing $h_i = H_1(R_i)$.

d. CA derives a unique partial delegation key (secondary key, s_i) for each vehicle i from the master secret x using the corresponding primary secret k_i and h_i values, as succeedingly indicated.

$$s_i = (1 + xh_ik_i^{-1}) \text{mod } q \quad (2.4)$$

The signing vehicle determines kp for message m (i.e).,

$$k_p = H_2(loc_p || t). \quad (2.5)$$

Then the session parameter as

$$(x_p, y_p) = k_pR_i \text{mod } q. \quad (2.6)$$

Then the Signature generated as

$$s_{p,i} = k_p^{-1}(H_1(m) \quad s_ix_p) \text{mod } q. \quad (2.7)$$

and the message is verified in receiving side by generating kp and the parameter (x_p, y_p) as,

$(x_p, y_p)=(H_1(m)R_i+x_p(R_i + h_iQ))s_{p,i}^{-1} \mod q$ (2.8)

Finally the signature is verified as valid.

2.5 Prioritized Scheme

Upon reception, a periodic safety message's data payload is passed to the designated Bloom filters, where each filter checks for the explicit part of the safety information. If a newly received message component with an acceptable tolerance matches an existing entry (i.e., any recent entry of the vehicle itself) in the corresponding Bloom filter, it returns a value 1. Otherwise, it returns a value 0. At each level of the tree, a left child of a parent node represents the corresponding relevance of safety information and is given a value of 1. On the other hand, a right child of a parent node indicates the non relevance of an coupled safety attribute and is given a value of 0. Assigned binary values from parent nodes are passed to the corresponding child nodes to determine the relevance score by concatenating the bits in sequence. Each received message in a receiving VANET entity is tagged with a relevance score specified by the leaves of the decision tree.

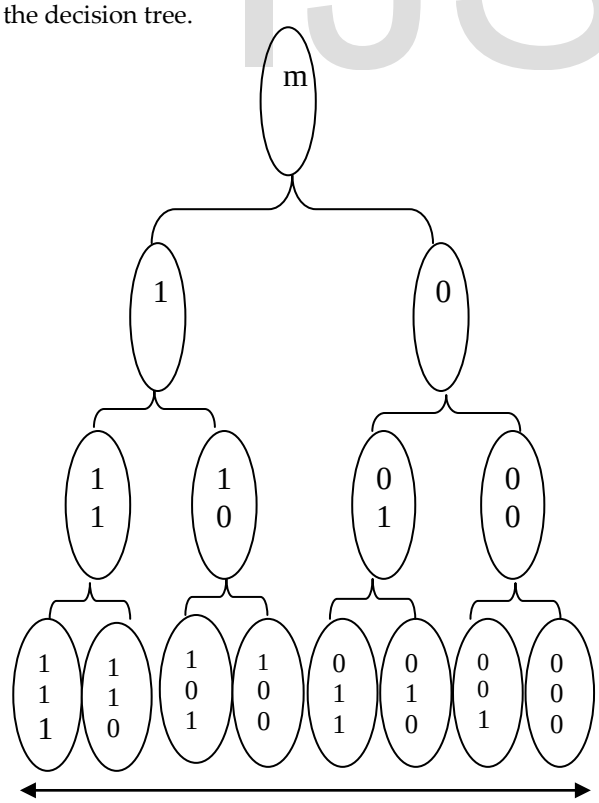

Fig 2. Binary Tree for Relevance score

Messages tagged at the leftmost leaf are the most relevant (with a relevance score of 7) as the relevance score of the tagged messages tend to get lower as we move along from left to right at the bottom of the tree.

3. RESULTS AND DISCUSSION

Table 1
SIMULATION PARAMETERS

Simulator	Network Simulator 2
Simulation Time	300s
Communication Range	3000m
Number Of Nodes	20
Packet Size	512 Bytes
Packet Interval	10 ms
Queue Length	50
Threshold Value	3.16 e-12
Status Packet Rate	10 packets/s
Number Of Lanes	4
Antenna	Omni Antenna
Queue Type	Drop Tail

We have chooses 20 fast moving nodes in the region of 3000 x 3000 m^2 with Simulation period 300 seconds. Nodes broadcast its information to all its nearby nodes within the range. In Fig -3 x-axis is considered as Data Rate and y-axis as dalay and in Fig -4 x-axis is considered as Data Rate and y-axis as throughput. Table -2 represents the comparison of Data Rate and Delay between ECDSA and AMBA Algorithm. Table -3 represents the comparison of Data Rate and Throughput between ECDSA and AMBA Algorithm.

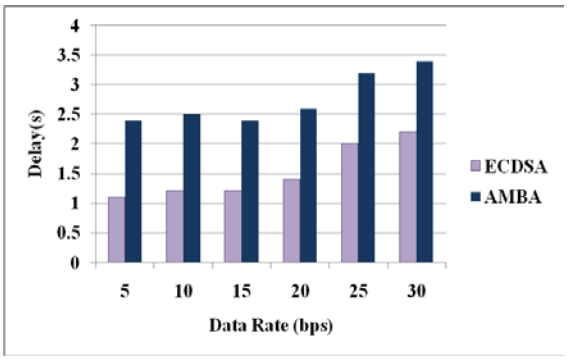

Fig. 3. Data Rate Vs Delay for ECDSA and AMBA

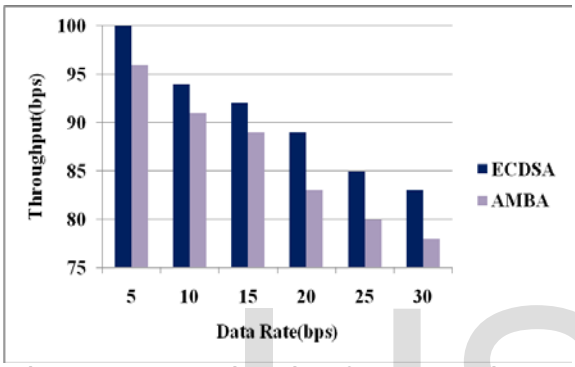

Fig. 4. Data Rate Vs Throughput for ECDSA and AMBA

Table 3
Data Rate Vs Throughput

Data Rate (bps)	Delay(s)	
	ECDSA	AMBA
5.00	1.1	2.4
10.00	1.2	2.5
15.00	1.2	2.4
20.00	1.4	2.6
25.00	2.0	3.2
30.00	2.2	3.4

Table 2
Data Rate Vs Delay

Data Rate (bps)	Throughput(bps)	
	ECDSA	AMBA
5.00	100	86
10.00	94	81
15.00	92	79
20.00	89	72
25.00	85	65
30.00	83	68

In Elliptic Curve Digital Signature Algorithm delay is reduced to 17% and Throughput is increased to 15% compared to Adaptive and Mobility Based Algorithm.

4. CONCLUSION

It is observed that vehicle-to-vehicle communications can be used as a major enabler for providing radical improvements in mitigating congestion, reducing compute time of urban workers, supporting a greener environment. In ECDSA algorithm, Prioritized verification scheme verifies the received messages based on their MAC traffic class and traffic intensity. This ensures that under rush-hour congestions or after a traffic accident, most important messages will not be missed by the verifier and also vehicles are able to calculate approximately the vehicle density in harsh environment and change their transmission parameters based on their current average speed in a secured manner to enhance VANETs' performance.

REFERENCES

[1] ASTM International, "IEEE Draft Standard for Information Technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Wireless Access in Vehicular Environments. IEEE Std 802.11p," July 2010.

[2] O. Bazan and M. Jaseemuddin, "Performance analysis of directional CSMA/CA in the presence of deafness," IET Communications, vol. 4, no. 18, pp. 2252 –2261, Dec. 2010.

[3] K. Bilstrup, E. Uhlemann, E.G. Strom, and U. Bilstrup, "Evaluation of the IEEE 802.11p MAC method for vehicle-to-vehicle communication," IEEE 68th Vehicular Technology Conference, Fall, 2008.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586–615, 2003.

[5] S. Eichler, "Performance evaluation of the IEEE 802.11p WAVE communication standard," Proc. IEEE Vehicular Technology Conf., pp. 2199–2203, 2007.

[6] J. R. Gallardo, D. Makrakis, and H. T. Mouftah, "Mathematical analysis of EDCA's performance on the control channel of an IEEE 802.11WAVE vehicular network," EURASIP J. Wireless Commun. Netw., vol. 2010, p. 489 527, 2010.

[7] J. He, Z. Tang, T. O'Farrell, and T. M. Chen, "Performance analysis of DSRC priority mechanism for road safety applications in vehicular networks,"

Wireless Communication and Mobile Computing (Wiley), vol. 11, no. 7, pp. 980–990, July 2011.

[8] C. Sommer and F. Dressler, "Progressing toward realistic mobility models in VANET simulations," IEEE Communications Magazine, vol. 46, no. 11, pp. 132 –137, Nov. 2008.

[9] H. Su, X. Zhang, H. Chen, "Cluster-based DSRC architecture for QoS provisioning over vehicle ad hoc network," IEEE GLOBECOM 2006.

[10] Z. Wang and M. Hassan, "How much of DSRC is available for non safety use?," Proceedings of the fifth ACM international workshop on Vehicular Inter-NETworking, pp. 23–29, 2008.

S.Sathya karthika received her B.E degree in Computer Science and Engineering from Anna University, Chennai in 2012 and She science and Engineering at Anna University. Her research interest includes Vehicular Ad-hoc NETwork in Networking.

J.Rethna Virgil Jeny received her B.E and M.E degrees in Computer Science and Engineering from Bharathidasan University, Trichy in 1997 and Annamalai University in 2005 respectively. She is currently doing Ph.D in wireless sensor Networks at MS University. She has received Lady Engineer Award by IEI. She is a member of IEEE, ACM, ISTE, IEI, IAENG and a senior member of IACSIT. Her research interests include Energy aware routing and Cross layer routing in Wireless Sensor Networks.

J. Albert Simon received his B.E. in Computer Science and Engineering from Anna university, Tirunelveli with Distinction in 2011 and ME in Computer Science and Engineering from Anna university, Chennai with distinction in 2013.He has secured fifth rank in Anna University M.E Examination. He has presented papers in International and National Conferences. His research interest includes Wireless Mesh Networks and Network Security.