ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

SECURE PREDICTION BASED AUTHENTICATION FOR VANET COMMUNICATION

Vishnu Venugopal[*1] & Asst. Prof. Deepika M. P[2]
[*1&2]Dept. of Computer Science & Engineering, Adi ShankaraCollege of Engineering, Kalady, Kerala, India

DOI: 10.5281/zenodo.1247128

ABSTRACT
The road to a successful introduction of vehicularcommunications has to pass through the analysis of potential security threats and the design of a robust security architecture able to cope with these threats. Broadcast communications are critically important, as many safety-related applications rely on single-hop beacon messages broadcast to neighbor vehicles. It becomes a challenging problem to design a broadcast authentication scheme for secure vehicle-to-vehicle communications.In this paper, we undertake this challenge. In this paper, communication technique is used for improved road safety with aid of Secure Prediction based authentication scheme. Here, Beacons are used for secure V2V and V2R communication. When a large number of beacons arrive in a short time, vehicles are vulnerable to computation-based Denial of Service (DoS) attacks that excessive signature verification exhausts their computational resources. In contrast to most existing authentication schemes, our SPBAis an efficient and lightweight scheme since it is primarily built on symmetric cryptography. To further reduce the verification delay for some emergency applications, SPBA is designed to exploit the sender vehicles ability to predict future beacons in advance. In addition, to prevent memory-based DoS attacks, SPBA only stores shortened re-keyed Message Authentication Codes (MACs) of signatures without decreasing security.

Keywords: Secure Prediction based authentication, ITS, Denial of Service (DoS), Computational based Dos.

I. INTRODUCTION
Initiatives to create safer and more efficient driving conditionshave recently begun to draw strong support. Vehicularcommunications (VC) will play a central role in this effort,enabling a variety of applications for *safety*, *traffic efficiency*, *driver assistance*, and *infotainment*. For example, warnings for environmental hazards (e.g., ice on the pavement) or abrupt vehicle kinetic changes (e.g., emergency braking), traffic androad conditions (e.g., congestion or construction sites), and tourist information downloads will be provided by these systems. Vehicular networking protocols will allow nodes, that is, vehicles or road-side infrastructure units, to communicate with each other over single or multiple hops. In other words, nodes will act both as end points and routers, with vehicular networksemerging as the first commercial instantiation of the *mobile ad hoc networking* technology.

In this paper, we are specifically concerned with the followingproblem: how to design and build vehicular communication protocols and systems that leave as little space as possible for misbehavior and abuse, and at the same time, remain resilient to on-going attacks. We present, in Sec. II, an analysis of the vulnerabilities of vehicular networks and the salient challenges in securing their operation. Then, in Sec. III, we propose our architectural view of how VC can be secured, along with a brief (due to space limitations) overview. We present, in Sec. IV, an brief description about the system flow diagram.Finally, we conclude this emerging area of research in Sec. V.

II. VULNERABILITIES AND CHALLENGES
A. Vulnerabilities
Any wireless-enabled device that runs a rogue version of the vehicular communication protocol stack poses a threat. We denote such rogue devices deviating from the defined protocols as *adversaries* or *attackers*. The adoption of a variant of the widely deployed IEEE 802.11 protocol1 by the vehicle manufacturers makes the

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

attacker's task easier. And even possession of credentials cannot ensure alone the correct operation of the nodes. The effects of differing types of attackers (internal or external, rational or malicious, independent or colluding, persistent or random) can clearly differ. Here, rather than analyzing specific protocols,
we are after a general exploration of VC vulnerabilities.

Jamming The jammer deliberately generates interfering transmissions that prevent communication within their receptionrange. As the network coverage area, e.g., along ahighway, can be well-defined, at least locally, jamming is a low-effort exploit opportunity. As Fig. 1 illustrates, an attacker can relatively easily, without compromising cryptographic mechanisms and with limited transmission power, partition the vehicular network.

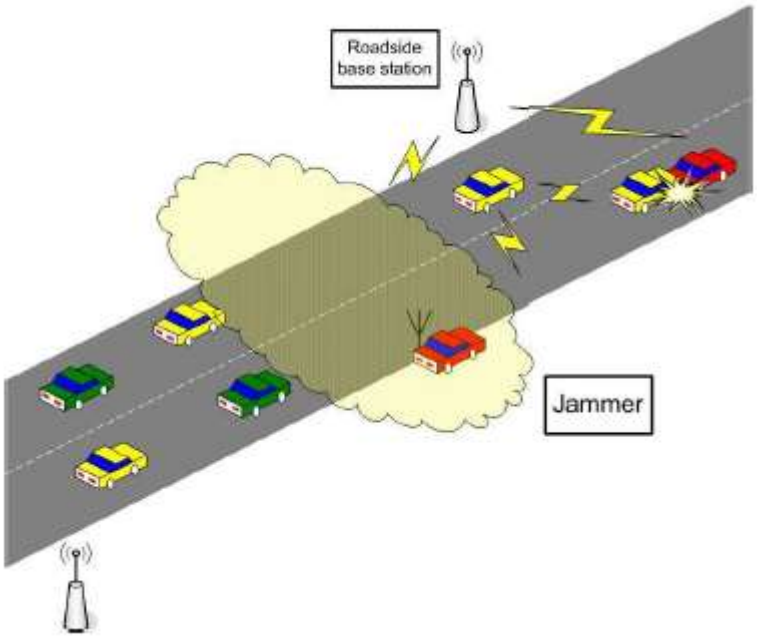


Fig. 1. Spectrum Jamming

Forgery The correctness and timely receipt of application data is a major vulnerability. Fig. 2 illustrates the rapid "contamination" of large portions of the vehicular network coverage area with false information where a single attacker forges and transmits false hazard warnings (e.g., ice formation on the pavement), which are taken up by all vehicles in both traffic streams.

In-transit Traffic Tampering Any node acting as a relay can disrupt communications of other nodes: it can *drop* or *corrupt*messages, or *meaningfully modify* messages. In this way, the reception of valuable or even critical traffic notifications or safety messages can be manipulated. Moreover, attackers can *replay* messages, e.g., to illegitimately obtain services such as traversing a toll check point. In fact, tampering with in-transit messages may be simpler and more powerful than forgery attacks.

Impersonation Message fabrication, alteration, and replay can also be used towards impersonation. Arguably, the source of messages, identified at each layer of the stack, may be of secondary importance. Often, it is not the source but the content (e.g., hazard warning) and the attributes of the message (freshness, locality, relevance to the receiver) that count the most. However, an impersonator can be a threat: consider, for example, an attacker masquerading as an emergency vehicle to mislead other vehicles to slow down and yield. Or, an adversary impersonating roadside units, spoofing serviceadvertisements or safety messages.

Privacy Violation With vehicular networks deployed, the collection of vehicle-specific information from overheard vehicular communications will become particularly easy. Then, inferences on the drivers' personal data could be made, and thus violate her or his *privacy*2. The vulnerability lies in the periodic and frequent vehicular network traffic: safety and traffic management messages, context-aware data access (e.g., maps,

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

ferryboat schedules), transaction-based communications (e.g., automated payments, car diagnostics), or other control messages (e.g., over-the-air registration with local highway authorities). In all such occasions, messages will include, by default, information (e.g., time, location, vehicle identifier, technical description, trip details) that could precisely identify the originating node (vehicle) as well as the drivers' actions and preferences (Fig. 3).

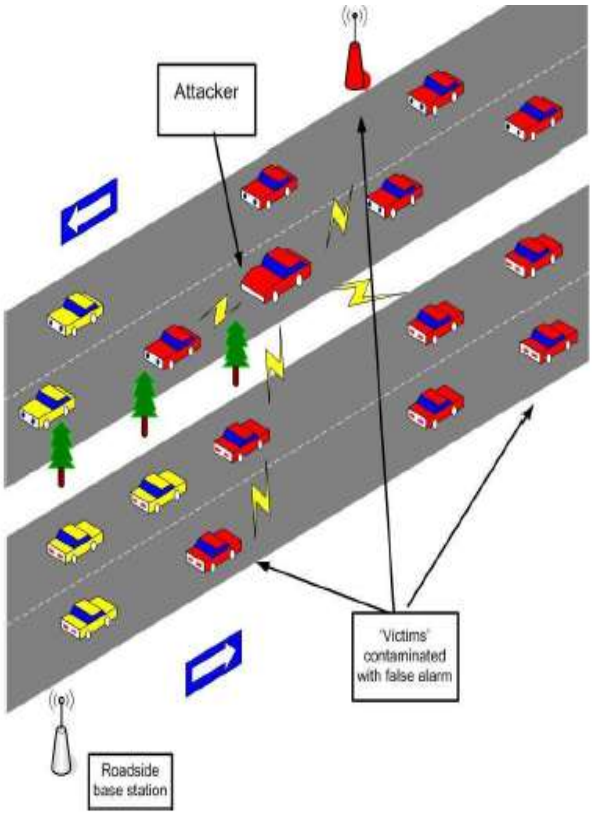


Fig. 2. Message Forgery

On-board Tampering Beyond abuse of the communication protocols, the attacker may select to tinker with data (e.g.,velocity, location, status of vehicle parts) at their source, tampering with the on-board sensing and other hardware. In fact, it may be simpler to replace or by-pass the real-time clock or the wiring of a sensor, rather than modifying the binary code implementation of the data collection and communication

protocols. Any VC security architecture should achieve atrade-off between robustness and cost due to tamper-proof hardware.

B. Challenges

The operational conditions, the constraints, and the user requirements for VC systems make security a hard problem, with the most significant challenges specific to the VC discussed here.

Network Volatility The connectivity among nodes can often be highly transient and a one-time event. For example, two vehicles (nodes) traveling on a highway may remain within their transceiver range, or within a few wireless hops, for a limited period of time. In other words, vehicular networks lack the relatively long-lived context and, possibly, the personal contact of the device users of a connection to a hot-spot or the recurrent connection to an on-line service across the Internet. Hence password-based establishment of secure channels, gradual development of trust by enlarging a circle of trusted acquaintances, or secure communication only with a handfulof endpoints may be impractical for securing VC.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

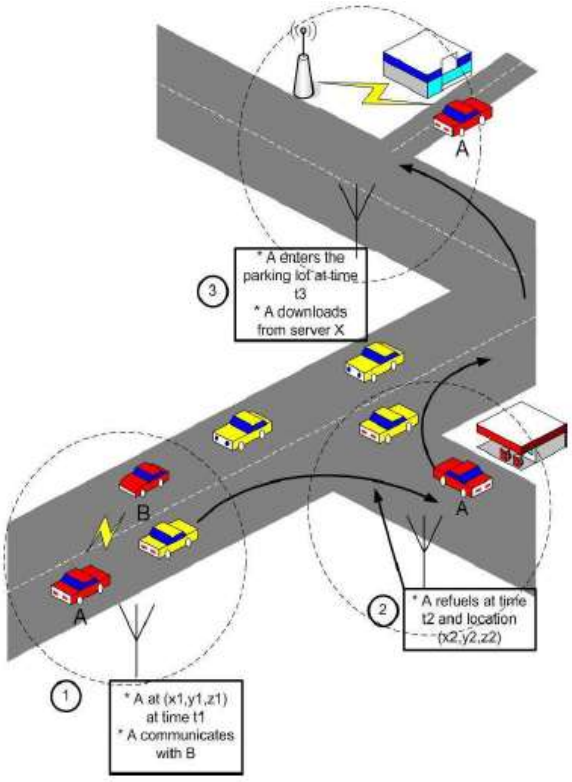


Fig. 3. Vehicle Tracking

Liability vs. Privacy To make the problem harder, accountability, and eventually liability, of the vehicles and their drivers is required. Vehicular communication is envisioned as an excellent opportunity to obtain hard-to-refute data that can assist legal investigations (e.g., in the case of accidents). This implies that, to begin with, unambiguous identification of the vehicles as sources of messages should be possible. Moreover, context-specific information, such as coordinates, time intervals, and associated vehicles, should be possible to extract or reconstruct. But such requirements raise even stronger privacy concerns. This is even more so when drivers' biometrics are considered: Biometrics, useful for enhancing vehicle access and control methods, are highly private and unique data cannot be reset or reassigned.

Delay-Sensitive Applications Many of the envisioned safety and driver-assistance applications pose strict deadlines for message delivery or are time-sensitive. Security mechanisms must take these constraints into consideration and impose low processing and messaging overhead. Not only must protocols be lightweight, but also robust to clogging denial-of-service attacks. Otherwise, it would suffice for an adversary to generate a high volume of bogus messages and consume resources so that message delivery is delayed beyond the application requirements, and thus, in practice, denied.

Network Scale The scale of the network, with roughly a billion vehicles around the globe, is another challenge. This, combined with the multitude of authorities governing transportation systems, makes the design of a facility to provide cryptographic keys a challenge per se. A technically, and perhaps politically, convincing solution is a prerequisitefor any security architecture.

Heterogeneity The heterogeneity in VC technologies and the supported applications are additional challenges, especially taking into account the gradual deployment. With nodes possibly equipped with cellular transceivers, digital audio and Geographical Positioning Service (GPS) or Galileo receivers, reliance on such external infrastructure should not be the weakest link in achieving security. For example, if GPS signaling can be spoofed, can the correctness of node coordinates and time accuracy be assumed? Second, with a range of applications with differing requirements, security solutions must retain *flexibility*, yet, remain *efficient* and *interoperable*.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

III. SECURITY ARCHITECTURE

In this section, we present the components needed to protectVC against a wide range of threats, some of which are described in the previous section. We also aim at providing an AAA (authentication, authorization, accounting) framework for VC. Fig. 4 depicts the general architecture, the components of which are described next.

Fast Auth Scheme:

One-time signature scheme named Fast Auth is used to provide lightweight, timely and nonrepudiation authentication for vehicle-to-vehicle communications. Chained Huffman hash trees is use to generate a common public key and minimize the signature size for beacons sent during one prediction interval. Exploits the predictability of future beacons to achieve the instant authentication in VANETs.

- If the receiver misses a beacon, it cannot work in the rest of the current prediction interval.
- It cannot accurately collect the entire beacon message
- Also, it cannot increase the packet delivery ratio.

Secure Prediction Based Authentication System Module:

The following are the details in the sender side and receiver side details involved in the communication. Secure Prediction based authentication is used in the sender side to detect Denial-of-Service attacks before the signature verification. Enhanced attacked packet detection algorithm is used at the receiver side to detect malicious node. To reduce the verification delay, SPBA is designed to exploit the sender vehicles ability to predict future beacons in advance. Applications rely on vehicles OBUs to broadcast outgoing beacon messages and to validate incoming ones. The broadcast beacons often contain information about position, current time, speed, direction, driving status, etc. By frequently broadcasting and receiving beacons, drivers are better aware of obstacles and collision scenarios. They may act early to avoid any possible damage, or to assign a new route in case of a traffic accident in the existing route. SPBA makes use of both ECDSA signatures and TESLA-based scheme to authenticate beacons. Similar to the TESLA scheme, SPBA also requires loose time synchronization. In VANETs, it is naturally supported since messages sent by GPS-equipped vehicles are time stamped with nanosecond-level accuracy.

Protocol Overview:

SPBA includes the process of generating a signature by a sender and verifying the signature by a receiver. First, each vehicle splits its timeline into a sequence of time frames. Each time frame is also divided into a sequence of beacon intervals, which we remark I_0; I_1; . . . ; In. In a time frame, to send the first beacon B0 for I_0, a vehicle will perform four steps: chained keys generation, position prediction, Merkle hash tree construction, and signature generation.

Sender Side Process:

- Chained Keys Generation:

At the beginning of a time frame, each vehicle generates n chained private keys for the next n beacons. It uses one interval worth of private key for authentication as the TESLA scheme. In the following description, we call these private keys TESLA keys.

- Position Prediction:

At each beacon interval, each vehicle predicts its position broadcast in the next beacon. To do so, vehicles model all the possible results of movements between two consecutive beacons based on information of the past trajectory.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

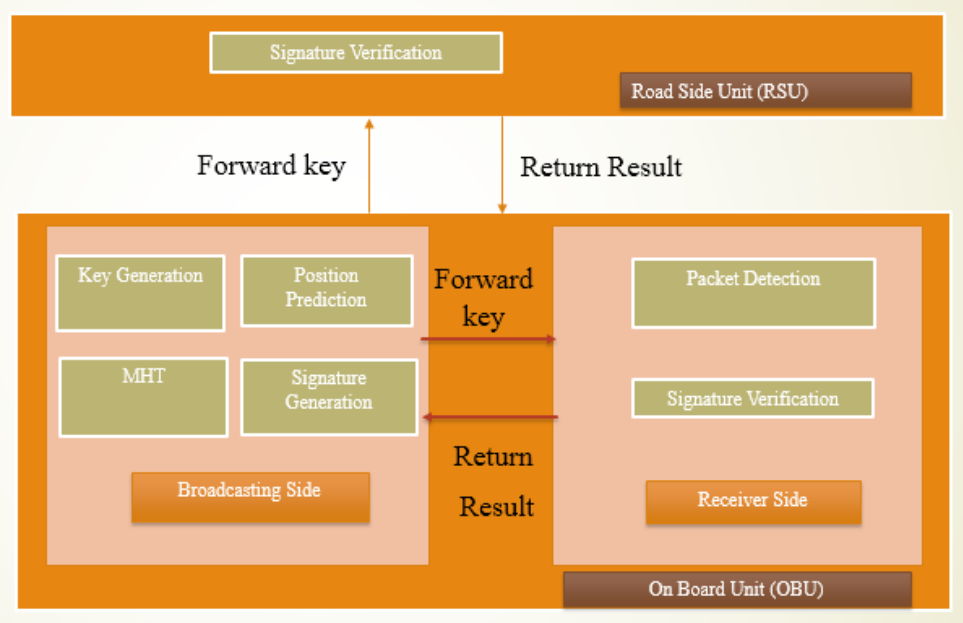


Figure 4: System Architecture

- Merkle Hash Tree Construction:

After position prediction, the vehicle will construct one interval worth of a public key and private keys. These private keys are associated with the results of movements. MHT structure is proposed to ties these pre-computed keys together and then generates a single public key or prediction outcome for all the possible movements.

- Signature generation:

After position prediction and MHT construction, a vehicle signs the commitment of the hash chain and the prediction outcome from MHT using ECDSA signatures, and broadcasts it along with the first beacon B0 in the time frame. For the rest of beacons such as B_1; B_2; . . .;B_n, the vehicle signs the message and the prediction outcome from MHT using the TESLA keys assigned in the intervals I_1; I_2;. . . ; In. It contains public keys, time stamp T_0, and other important parameters.

Receiver Side Process:

- Attack packet detection:

It is based on the position changing requirements. Attacked packets are identified by the following parameters Frequency (f), Velocity (v), is Coefficient which is determined by the road characteristics and (VMax) is the maximum speed. After receiving a beacon, a vehicle will perform the following two steps:

a) Self-generated MAC storage:

To reduce the storage cost of unverified signatures, the receiver only records a shortened re-keyed MAC. When the receiver keeps the used key secret, SPBA provides security guarantees according to the size of beacon interval and network bandwidth.

b) Signature verification:

For the first beacon, the receiver veryfies the ECDSA signature. To verify the following signed Bi, the receiver will get the corresponding TESLA key, and reconstruct the prediction outcome from MHT. If a matching MAC of prediction outcome is found in the memory, the receiver authenticates the beacon instantly. Otherwise, the receiver authenticates it with the later TESLA key.

Open Problems

In addition to the main building blocks presented in Sec. III, there remains a set of unexplored problems directly related to VC security. In this section we outline the most important of these problems.

Secure Positioning: In VC, position is one of the most important data for vehicles. Each vehicle needs to know not only its own position but also those of other vehicles in its neighborhood. GPS signals are weak, can be

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

spoofed, and are prone to jamming. Moreover, vehicles can intentionally lie about their positions. Hence the need for a secure positioning system that will also support the accountability and authorization properties, frequently related to a vehicle's position.

Data Verification helps to prevent the forging attacks illustrated in Fig. 2. This can be achieved by a *data correlation*mechanism that compares all collected data regarding a given event. A first example of such a mechanism is presented in [4], where the vehicle has a model to which it compares received data before classifying it as truthful, malicious, or unintentionally incorrect.

DoS Resilience: DoS attacks, and especially *jamming*, are relatively simple to mount yet their effects can be devastating. Existing solutions such as frequency hopping do not completely solve the problem. The use of multiple radio transceivers, operating in disjoint frequency bands, can be a feasible approach.

IV. SYSTEM FLOW DIAGRAM

Protocol Overview

The SPBA includes the process of generating a signature by a sender and verifying the signature by a receiver. We introduce them separately. First, each vehicle splits its timeline into a sequence of time frames. Each time frame is also divided into a sequence of beacon intervals, which we remark I_0; I_1; In. In a time frame, to sendthe first beacon B_0 for I_0, a vehicle will perform four steps: chained keys generation, position prediction, Merkle hash tree construction, and signature generation. To send other beacons in that time frame, the vehicle only operates the last three steps.[37]

- Chained Keys Generation: At the beginning of a time frame, each vehicle generates n chained private keys for the next n beacons. It uses one interval worth of private key for authentication as the TESLA scheme. In the following description, we call these private keys TESLA keys.

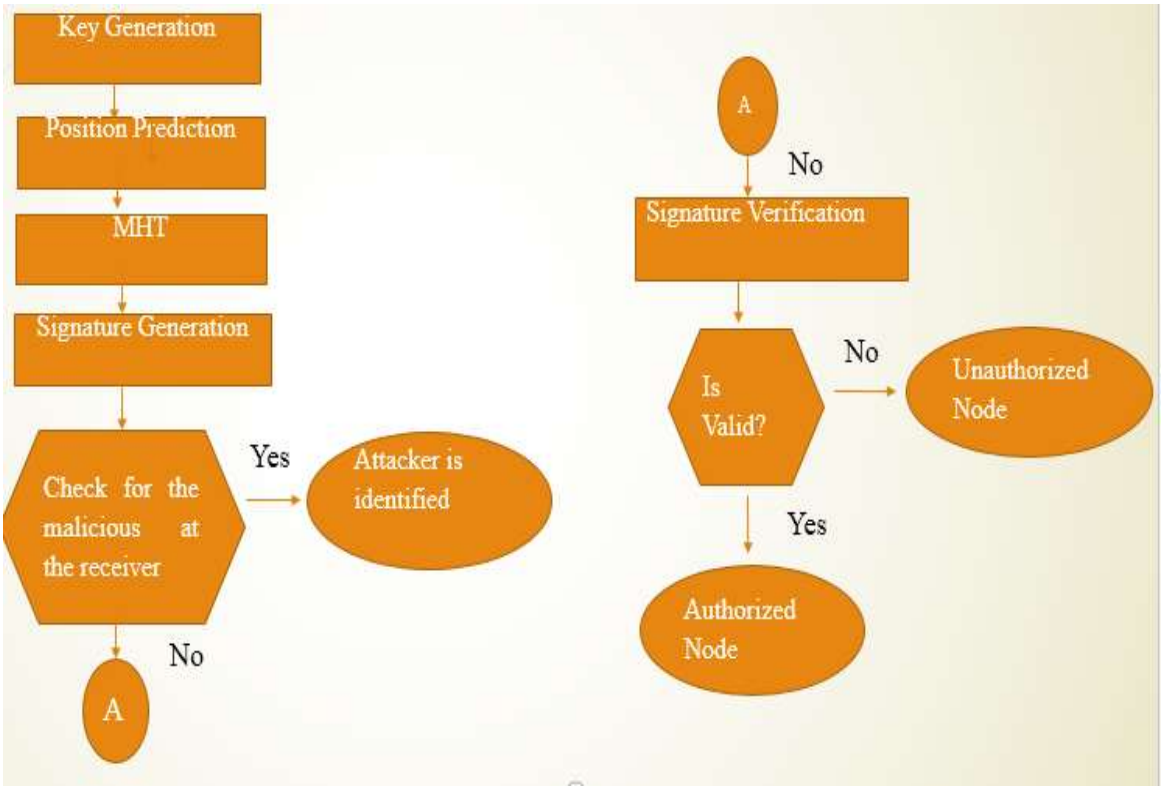


Fig 5: System Flow Diagram

- Position Prediction: At each beacon interval, each vehicle predicts its positionbroadcast in the next beacon. To do so, vehicles model all the possible resultsof movements between two consecutive beacons based on information of thepast trajectory.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

- Merkle Hash Tree Construction: After position prediction, the vehicle willconstruct one interval worth of a public key and private keys. These privatekeys are associated with the results of movements. We propose a MHT, whichties these pre-computed keys together and then generates a single public keyor prediction outcome for all the possible movements. Rooti is the predictionoutcome for all the results of movements from Ii-1 to Ii-1
- Signature Generation: After position prediction and MHT construction, avehicle signs the commitment of the hash chain and the prediction outcomefrom MHT using ECDSA signatures, and broadcasts it along with the firstbeacon B0 in the time frame. For the rest of beacons such as B1;B2;....;Bn,the vehicle signs the message and the prediction outcome from MHT using theTESLA keys assigned in the intervals I1; I2; ...In;

Chained Keys Generation

Before sending any beacon, a vehicle _rst generates n chained keys for signing anda commitment K0 like the TESLA scheme, as shown in Fig. 6. As we mentioned before, the drawback of the TESLA scheme is that the receiver needs to buffer packets some intervals before it can authenticate them. This might not be practical for certain single-hop relevant applications where timing is usually critical. We modify the basic TESLA scheme to support instant authentication, which allows the receiver to verify packets as soon as they arrive. In our TESLA-based scheme, the sender predicts the next interval's message mi+1 in the interval Ii, and gets the prediction outcome Rooti+1. To construct the beacon packet Bi, the sender picks the TESLA key Ki for Ii, and appends the MAC over mi and Rooti+1 with K0i, respectively. The last item means the disclosed TESLA key. Here, the notion j stands for message concatenation.We now briey present how our TESLA-based scheme works. When the beacon Bi with the disclosed key Ki-1 arrives at a receiver, it allows the receiver to verify the beacon Bi-1 sent in interval Ii-1. Bi-1 carries the prediction outcome Root for mi. Therefore, the message mi can be immediately verified with Rooti and Ki-1. Dealing with packet losses: If certain previous beacon, such as Bi+1, is lost or dropped due to the poor quality of wireless channel, we cannot immediately authenticate the incoming beacon Bi. However, we are able to authenticate it with the original TESLA signature MACK0i(mi), where the TESLA key Ki is disclosed in or after interval Ii+1.

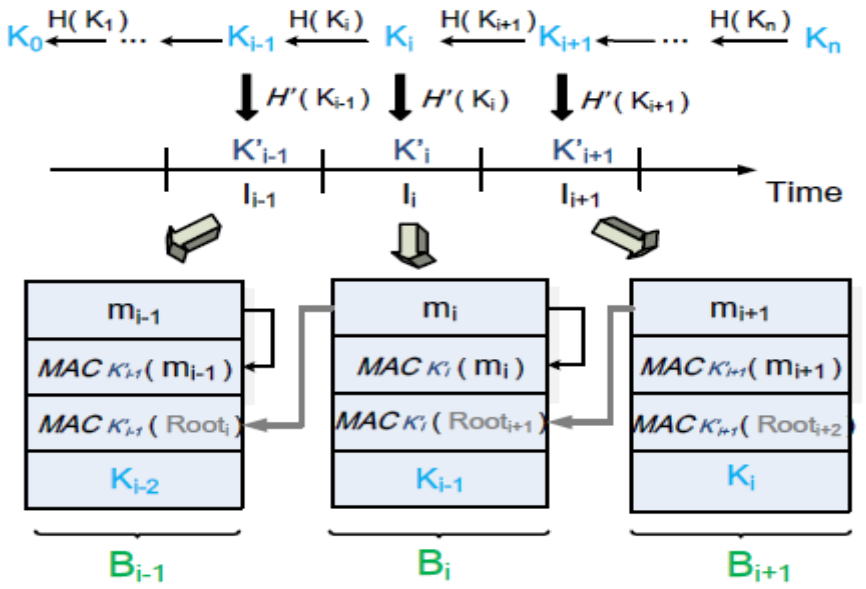


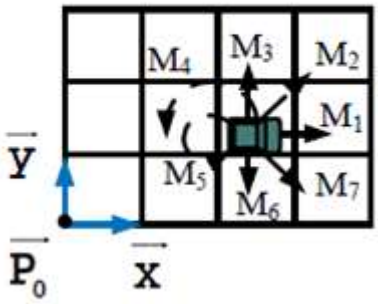
Fig 6: Chained Key Generation

Position Prediction

As position is the main source of uncertainty in beacons, we discuss how the sender vehicle predicts its own future positions. For every two consecutive beacons, such as Bi-1 and Bi, SPBA requires the sender to model all the possible results of the distance vector differences or movements between them. The output of this step is a prediction table PTi in which each entry represents one possible movement between Ii-1 and Ii. Inspired by the work, we also use a local coordinate to express the sender's future positions. We place the origin of this local coordinate at the beginning position P0 of the current time frame. A pair of orthogonal vectors (i.e., x and y) are

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

also required, the scalar of which can be chosen according to a desired level of positioning accuracy. Here, we are not interested in accurately modeling the mobility of a vehicle given the past trajectory, which is orthogonal to our work. In this work, we would like to design a broadcast signature scheme working with an arbitrary prediction model.[9]



Prediction Table

Results	Movement
M_1	(1, 0)
M_2	(1, 1)
M_3	(0, 1)
M_4	(-1, 0)
M_5	(0, 0)
M_6	(0, -1)
M_7	(1, -1)

Fig 7: Position Prediction

Merkle Hash Tree Construction

Given the prediction table, the vehicle needs to generate a single public key (or prediction outcome) for all the possible movements. It first generates private keys, which are associated with the results of movements in PTi. Then, a MHT structure is proposed to tie these keys together and generate a single public key or prediction outcome for all the movements. A MHT structure is a binary tree structure where each leaf is assigned a hash value and an inner node is assigned the hash value of its children. As shown in Fig. 3(b), for an entry Mk in PTi (which shows that the vehicle will move to location Pi-1 + Mk with a certain probability in interval Ii),

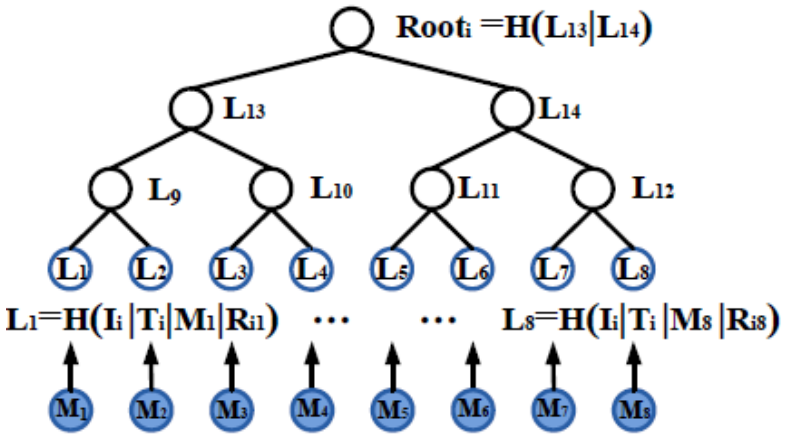


Fig 8: Merkle Hash Tree Structure

there is a leaf labeled as Lk in the MHT, where Rik is a random value to prevent signature forgery. Then, the sender obtains Rooti, which is the predication outcomeof the message mi based on the prediction table PTi.[17] Signature Generation After generating the commitment K0, constructing the prediction table with a local coordinate, and producing the MHT's root Root1 for the next beacon B1, the sender broadcasts the first beacon in a time frame. It contains public keys, time stamp T0, and other important parameters (such as, its local coordinate system). The vehicle will locate the leaf node corresponding to Pi in the MHT, and broadcast the necessary values and o_-path nodes of this leaf in mi. We define off-path nodes are the siblings of the nodes on the path from one leaf to the root of MHT. For example, in Fig. 8, the car shows the leaf associated with the current location and time. At T1, the sender moves to P1 P0 + M2, associated with L2. Hence, m1 includes

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

the random value and off-path nodes for the interval. To construct the signature of mi, the sender first picks the TESLA key Ki Then, by performing the steps of position prediction and MHT construction, it obtains the root value Rooti+1 for Ii+1. Finally, the sender signs mi and Rooti+1 with K0i. The signature of m1 includes the TESLA signature MACK01(m1) and MACK01(Root2). Thus, except the first beacon, the broadcast Bi includes the message mi, the signature Si, and the TESLA key Ki-1 which is disclosed for receivers to verify previous beacons.[31] Reducing the communication overhead: As the random value and off-path nodes are contained in the message, the size of beacon is larger than before. To reduce the communication overhead, we could decrease the number of off-path nodes with Huffman hash tree instead of Merkle hash tree. Note that, if Huffman hash tree is used to reduce the communication overhead, it will take effect only when an OBU predicts its movement accurately

Self-Generated MAC Storage

In a time frame, as the _rst beacon B0 is signed by ECDSA, a receiver will directly store K0, Root1 and To verify B1 or B2, the receiver gets the TESLA key K0 or K1, rebuilds the root of MHT with the information in B1 or B2, and then checks whether the root matches the one signed in B0 or B1. other local parameters if itpasses the veri_cation. Except B0, when the receiver gets the signature of a beaconBi, it will store a self-generated MAC to reduce memory cost. Algorithm 1 depicts the operations of the receiver. The security of the basic TESLA scheme depends on the TESLA keys that remain secret until a predetermined time period. SPBA builds on the basic TESLA scheme, so the receiver must verify the key Ki, which is used to generate the signature of the beacon, has not yet been disclosed by the sender. If this security condition does not hold, the receiver must drop the beacon, because it cannot assure the authenticity any more. Otherwise, it recomputes the MAC of the signed prediction outcome with a local secret key SKloc: MACRSi+1 = MACSKloc (MACK0i(Rooti+1)). Note that, SKloc is only known by the receiver. The receiver stores this shortened MAC (i.e., MACRSi+1) until the next interval Ii+1. The lifetime of MACRSi+1 is one interval in memory since it is only useful to achieve instant verification of Bi+1. The incoming Bi also contains the TESLA key Ki. The receiver will check whether it can use Ki to verify Bi and some previous unverified beacons. To verify Bi, the receiver _rst reconstructs the MHT's root node Root0 i. It then calculates the shortened MAC (i.e., MAC0R Si = MACSKloc (MACK0 i-1(Root0 i))), and compares it with the one stored in memory. If a matching MAC is found, mi is authenticated and the receiver can free the memory. If none of the stored MACsmatch MAC0R Si , the receiver considers that the prediction outcome of the message lost. Thus, it will compute the shortened MAC of the message (i.e., MACMSi = MACSKloc (MACK0i(mi))), store mi and MACMSi (Line 15), and wait for the later key for authentication. Moreover, the disclosed TESLA key Ki-1 might allow the receiver to verify previously received messages and then free the memory. Here, we set the size of original MACs to be 160 bits and the size of short MACs 32 bits. Given the interval of 100 ms as suggested by the IEEE standard, we will prove that receivers could use shorter MACs to store Signatures without decreasing security. We also _nd that the receiver's memory consumption is related to the packet loss rate in VANETs. Assuming the lifetime of beacons to be N, we will discuss the upper-limit of memory consumption for SPBA.

Signature verification

For the first beacon B0, ECDSA signature can provide the property of non-repudiation. It helps the receiver ensure that the sender is accountable for the parameters such as the initial position P0 and the commitment of hash chains K0, and thus prevents drivers from broadcasting malicious information. To verify the following signed Bi, the receiver verifies the validity of Ki by following the one-way key chain back to K0 signed with ECDSA. It recomputed the root value Root0 i of MHT given relevant values in the mi, and checks whether it matches Rooti stored in the memory. If not, the receiver will verify mi with the later TESLA key. The receiver gets the tree root Root1 from the _rst beacon. In I1, it reconstructs L2 from the values (e.g., R12) in the message, and calculates the hash tree root based on L2 and the off-path hashesL1; L10; L14. If the calculated root H(H(H(L1jL2)jL10)jL14) matches Root1, the receiver is convinced that the sender moves M 2 distance from I0 to I1, being located at P1 = P0 + M2. In I2, the receiver of B2 reconstructs the hash tree root as before, and then does MAC operations towards the root with the keys K01 and SKloc. If the value matches MACRS2 stored in the memory, the receiver is convinced that the sender moves M7 distance from I1 to I2, being located at P2 = P1 + M7. Public Key Rebroadcasting: As K0 is only sent at the beginning of a time frame, if a vehicle A encounters a vehicle C after C broadcasts its current 0, A cannot verify C's beacons until the next time frame. To overcome this issue, we may consider that vehicle C signs K0 by ECDSA with the certificate every second (10 beacons) on demand. Hence, after waiting several beacon intervals, the receiver A is able to authenticate beacons. Here, we do not specialize how often vehicle C signs K0 by ECDSA as we only give a general solution of broadcast authentication in VANETs. It is absolutely possible to consider the length of time frame and the

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

frequency of ECDSA signature when we have a specific application. The system designer can easily modify our scheme according to the applications' needs. For example, in an application where time demand is tight, vehicle A may send a requestpacket to vehicle C for K0, and C will return the ECDSA signature immediately. After getting it, vehicle A can initiate authentication with this trust commitment.

Algorithm 1: Self-Generated MAC.

Require: Beacon Bi, Local secret key SK_{loc}

1. Check the security condition;
2. if not satisfied then
3. Drop the beacon
4. else
5. Compute $MAC_{RSi+1} = MACS_{Kloc}(MAC_{K0i}(Root_{i+1}))$
6. Store MAC_{RSi+1}
7. if K_{i-1} is valid then
8. Reconstruct the MHT's root node Root0i
9. Recompute $MAC0_{RSi} = MAC_{SKloc}(MACK_{0i-1}(Root_{0i}))$
10. if Search $(MAC0_{RSi}) == 1$ then
11. Accept mi
12. Free memory for $MACR_{Si}$
13. else
14. Compute $MACM_{Si} = MACS_{Kloc}(MACK_{0i(mi)})$
15. Store mi and MACMSi
16. end if
17. Verify previously received messages
    Free memory for mg and MACMSg (g < i)
18. end if

V. CONCLUSION

For virtual networks communications, here an effective, efficient and scalable prediction based algorithm is used toresist the computation-based DoS attacks and packet losses in virtual networks. These technology can greatly enhance the infotainment, safety, comfort, communication and convenience value of new vehicles. As vehicles become “smarter”, security and privacy gain importance. Moreover, SPBA has the advantage of the predictability of beacons lifetime for single hop relevant applications. To defend against memory based DoS attacks, SPBA only keeps shortened MACs of signatures to reduce the storage overhead. By theoretical analysis, enhanced SPBA protocol is secure and robust in the context of virtual networks. Through a range of evaluations, SPBA has been reduced the loss rate to perform efficient even under heavy traffic places.

VI. REFERENCES

[1] F. J.Martinez, C.-K. Toh, J.-C. Cano, C. T. Calafate, and P.Manzoni, “Emergency services in future intelligent transportation systems based on vehicular communication networks,” *IEEE Intelligent Transportation SystemsMagazine*, vol. 2, no. 2, pp. 6–20, 2010.

[2] P. Fazio, F. De Rango, and A. Lupia, “A new application for enhancing VANET services in emergency situations using the WAVE/802.11p standard,” in *Proceedings of the IFIP Wireless Days (WD ’13)*, pp. 1–3, Valencia, Spain, November 2013.

[3] N. Kumar, N. Chilamkurti, and J. J. P. C. Rodrigues, “Learning automata-based opportunistic data aggregation and forwarding scheme for alert generation in vehicular ad hoc networks,”*Computer Communications*, vol. 39, pp. 22–32, 2014.

[4] K. Shafiee, J. Lee, V. C. M. Leung, and G. Chow, “Modeling and simulation of vehicular networks,” in *Proceedings of the 1st ACMInternational Symposium on Design and Analysis of IntelligentVehicular Networks and Applications (DIVANet ’11)*, pp. 77–85, ACM, New York, NY, USA, November 2011.

[5] Y.-C. Tseng, S.-Y. Ni, Y.-S. Chen, and J.-P. Sheu, “The broadcast stormproblemin a mobile ad hoc network,” *Wireless Networks*, vol. 8, no. 2-3, pp. 153–167, 2002.

[6] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, “Automatic accident detection: assistance through communication technologies and vehicles,” *IEEEVehicular Technology Magazine*, vol. 7, no. 3, pp. 90–100, 2012.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[7] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni, "A system for automatic notification and severity estimation of automotive accidents," *IEEE Transactions on Mobile Computing*, vol. 13, no. 5, pp. 948–963, 2014.
[8] M. Fogue, P. Garrido, F. J. Martinez, J.-C. Cano, C. T. Calafate, and P.Manzoni, "A novel approach for traffic accidents sanitary resource allocation based on multi-objective genetic algorithms," *Expert Systems with Applications*, vol. 40,no. 1, pp. 323– 336, 2013.
[9] P. Ruiz and P. Bouvry, "Survey on broadcast algorithms for mobile ad hoc networks," *ACM Computing Surveys*, vol. 48, no. 1, article 8, 2015.
[10] L. Cheng, B. E. Henty, R. Cooper, D. D. Stancil, and F. Bai, "A measurement study of time-scaled 802.11a waveforms over the mobile-to-mobile vehicular channel at 5.9GHz," *IEEECommunications Magazine*, vol. 46, no. 5, pp. 84–91, 2008.
[11] S. Panichpapiboon and W. Pattara-Atikom, "A review of information dissemination protocols for vehicular ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 14, no. 3, pp. 784–798, 2012.
[12] X. Li and H. Li, "A survey on data dissemination in VANETs," *Chinese Science Bulletin*, vol. 59, no. 32, pp. 4190–4200, 2014.
[13] J. Harri, F. Filali, and C. Bonnet, "Mobility models for vehicular ad hoc networks: a survey and taxonomy," *IEEE CommunicationsSurveys & Tutorials*, vol. 11, no. 4, pp. 19–41, 2009.
[14] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE CommunicationsSurveys&Tutorials*, vol. 18,no. 1, pp. 263–284, 2015.
[15] S.Madi and H. Al-Qamzi, "A survey on realistic mobility models for vehicular ad hoc networks (VANETs)," in *Proceedings ofthe 10th IEEE International Conference on Networking, Sensingand Control (ICNSC '13)*, pp. 333–339, April 2013.
[16] M. S. Al-Kahtani, "Survey on security attacks in vehicular ad hoc networks (VANETs)," in *Proceedings of the 6th InternationalConference on Signal Processing and Communication Systems(ICSPCS '12)*, pp. 1–9, Queensland, Australia, December 2012.
[17] H. Al Falasi and E. Barka, "Revocation in VANETs: a survey," in *Proceedings of the International Conference on Innovations inInformation Technology (IIT '11)*, pp. 214–219,AbuDhabi,United Arab Emirates, April 2011.
[18] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: a survey," *IEEE Vehicular Technology Magazine*, vol. 2, no. 2, pp. 12–22, 2007.
[19] H. Keshavarz and R. M. Noor, "Beacon-based geographic routing protocols in vehicular ad hoc networks: a survey and taxonomy," in *Proceedings of the IEEE Symposium on WirelessTechnology and Applications (ISWTA '12)*, pp. 309–314, IEEE, Bandung, September 2012.
[20] S. Allal and S. Boudjit, "Geocast routing protocols for VANETs: survey and guidelines," in *Proceedings of the 6th InternationalConference on Innovative Mobile and Internet Services in UbiquitousComputing (IMIS '12)*, pp. 323–328, IEEE, Palermo, Italy, July 2012.
[21] A. Sebastian, M. Tang, Y. Feng, and M. Looi, "A multicast routing scheme for efficient safety message dissemination in VANET," in *Proceedings of the IEEE Wireless Communicationsand Networking Conference (WCNC '10)*, pp. 1–6, Sydney, Australia, April 2010.
[22] F. Soldo, R. Lo Cigno, and M. Geria, "Cooperative synchronous broadcasting in infrastructure-to-vehicles networks," in *Proceedings of the 5th Annual Conference on Wireless on DemandNetwork Systems and Services (WONS '08)*, pp. 125–132, Garmisch-Partenkirchen, Germany, January 2008.
[23] F. J. Martinez, J.-C. Cano, C. T. Calafate, P. Manzoni, and J. M. Barrios, "Assessing the feasibility of a VANET driver warning system," in *Proceedings of the 4th ACM Workshop onPerformance Monitoring and Measurement of Heterogeneous Wireless and Wired Networks (PM2HW2N '09)*, pp. 39–45,ACM, 2009.
[24] G. Y. Cahng, J.-P. Sheu, and J.-H. Wu, "Typhoon: resource sharing protocol for metropolitan vehicular ad hoc networks," in *Proceedings of the IEEE Wireless Communications and NetworkingConference (WCNC '10)*, pp. 1–5, Sydney, Australia, April 2010.
[25] X.Hu, J. Zhao,D. Zhou, andV. C. M. Leung, "Asemantics-based multi-agent framework for vehicular social network development," in *Proceedings of the 1st ACM International Symposiumon Design and Analysis of Intelligent Vehicular Networks andApplications (DIVANet '11)*, pp. 87–96, ACM, New York, NY, USA, November 2011.
[26] S. Samarah, "Grid-based hierarchy structure for mining and querying vehicular ad-hoc networks," in *Proceedings of theSecond ACM International Symposium on Design and Analysis of Intelligent Vehicular Networks andApplications (DIVANet '12)*, pp. 63–68, ACM, 2012.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[27] J. Jakubiak and Y. Koucheryavy, "State of the art and research challenges for VANETs," in *Proceedings of the 5th IEEE ConsumerCommunications and Networking Conference (CCNC'08)*, pp. 912–916, Las Vegas, Nev, USA, January 2008.
[28] DoT, "United States Department of Transportation," 2015, http://www.dot.gov/.
[29] Z. Movahedi, R. Langar, and G. Pujolle, "A comprehensive overview of vehicular AdHocNetwork evaluation alternatives," in *Proceedings of the 8th Asia-Pacific Symposium on Informationand Telecommunication Technologies (APSITT '10)*, pp. 1–5, Kuching, Malaysia, June 2010.
[30] A. J. Ghandour, M. Di Felice, H. Artail, and L. Bononi, "Dissemination of safetymessages in IEEE 802.11p/WAVE vehicular network: analytical study and protocol enhancements," *Pervasiveand Mobile Computing*, vol. 11, pp. 3–18, 2014.
[31] J.Dias, J. Rodrigues, J. Isento, and J. Niu, "The impact of cooperative nodes on the performance of vehicular delaytolerant networks," *Mobile Networks and Applications*, vol. 18, no. 6, pp.867–878, 2013.
[32] J. N. G. Isento, J. J. P. C. Rodrigues, J. A. F. F. Dias, M. C. G. Paula, and A. Vinel, "Vehicular delay-tolerant networks? Anovel solution for vehicular communications," *IEEE IntelligentTransportation Systems Magazine*, vol. 5, no. 4, pp. 10–19, 2013.
[33] P. R. Pereira, A. Casaca, J. J. P. C. Rodrigues, V. N. G. J. Soares, J. Triay, and C. Cervell´o-Pastor, "From delay-tolerant networks to vehicular delay-tolerant networks," *IEEE CommunicationsSurveys and Tutorials*, vol. 14, no. 4, pp. 1166–1182, 2012.
[34] Q. Chen, D. Jiang, and L. Delgrossi, "IEEE 1609.4 DSRC multichannel operations and its implications on vehicle safety communications," in *Proceedings of the IEEE Vehicular NetworkingConference (VNC '09)*, pp. 1–8, Tokyo, Japan, October 2009.
[35] Q.Xu, T.Mak, J. Ko, andR. Sengupta, "Vehicle-to-vehicle safety messaging inDSRC," in *Proceedings of the 1st ACM InternationalWorkshop on Vehicular Ad Hoc Networks (VANET '04)*, pp. 19–28, ACM, NewYork, NY,USA, 2004.
[36] Q. Xu, T. Mak, J. Ko, and R. Sengupta, "Medium access control protocol design for vehicle—vehicle safety messages," *IEEETransactions on Vehicular Technology*, vol. 56, no. 2, pp. 499–518, 2007.
[37] M. Torrent-Moreno, P. Santi, and H. Hartenstein, "Fair sharing of bandwidth in VANETs," in *Proceedings of the 2nd ACMInternational Workshop on VehicularAdHoc Networks (VANET'05)*, pp. 49–58, New York, NY, USA, 2005.
[38] F. Farnoud and S. Valaee, "Repetition-based broadcast in vehicular ad hoc networks in Rician channel with capture," in *Proceedings of the IEEE INFOCOM Workshops*, pp. 1–6, Phoenix, Ariz, USA, April 2008.
[39] B. Hassanabadi and S. Valaee, "Reliable periodic safety message broadcasting in VANETs using network coding," *IEEE Transactionson Wireless Communications*, vol. 13, no. 3, pp. 1284–1297,2014.
[40] Y. Park and H. Kim, "Collision control of periodic safety messages with strict messaging frequency requirements," *IEEETransactions onVehicular Technology*, vol. 62,no. 2, pp.843–852, 2013.
[41] N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, and V. Sadekar, "Broadcast storm mitigation techniques in vehicular ad hoc networks," *IEEEWireless Communications*, vol. 14, no. 6, pp. 84–94, 2007.
[42] K. Suriyapaibonwattana and C. Pomavalai, "An effective safety alert broadcast algorithm for VANET," in *Proceedings of theInternational Symposium on Communications and InformationTechnologies (ISCIT '08)*, pp. 247–250,Vientiane, Laos, October 2008.
[43] K. Suriyapaiboonwattana, C. Pornavalai, and G. Chakraborty, "An adaptive alert message dissemination protocol for VANET to improve road safety," in *Proceedings of the IEEE InternationalConference on Fuzzy Systems (FUZZ-IEEE '09)*, pp. 1639–1644, Jeju Island, Republic of Korea, August 2009.
[44] M. Slavik and I. Mahgoub, "Stochastic broadcast for VANET," in *Proceedings of the 7th IEEE Consumer Communications andNetworking Conference (CCNC '10)*, pp. 1–5, IEEE, Las Vegas, Nev, USA, January 2010.
[45] F. J.Martinez, M. Fogue, M. Coll, J.-C. Cano,C.Calafate, and P. Manzoni, "Evaluating the impact of a novel warning message dissemination scheme for VANETs using real city maps," in *NETWORKING 2010: 9th International IFIP TC 6 Networking Conference, Chennai, India, May 11–15, 2010. Proceedings*, M.Crovella, L. Feeney, D. Rubenstein, and S. Raghavan, Eds.,vol. 6091 of *Lecture Notes in Computer Science*, pp. 265–276, Springer, Berlin, Germany, 2010.

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

[46] 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.

[47] F. J. Ros, P. M. Ruiz, and I. Stojmenovic, "Reliable and efficient broadcasting in vehicular ad hoc networks," in *Proceedings of theIEEE 69th Vehicular Technology Conference (VTC Spring '09)*, pp. 1–5, IEEE, April 2009.

CITE AN ARTICLE

Venugopal, V., & MP, D., Asst. Prof. (2018). SECURE PREDICTION BASED AUTHENTICATION FOR VANET COMMUNICATION. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *7*(5), 375-388.