International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

PERFORMANCE STUDY ON VEHICULAR TRAFFIC MANAGEMENT AND COLLISION DETECTION TECHNIQUES FOR PUBLIC SAFETY SERVICES

Chandramohan K[1] , Gopinath S[2]

[1]*Associate Professor- Department of Computer Science & Engineering*

[2]*Assistant Professor- Department of Computer Science & Engineering*

Gnanamani College of Technology, Namakkal(India)

ABSTRACT

The vehicular ad hoc networks (VANETs) have involved numerous courtesy owing to their appealing and promising functionalities counting vehicular security, traffic jamming prevention, and location based services. Privacy is a significant concern in VANETs. As the wireless communication channel is a common medium, replacing messages with no any security fortification can simply reveal the information that users might desire to stay private. Numerous researchers have presented papers on privacy preservation scheme in VANET. In a paper, the author Yong Hao et.Al., are going to examine the performance of the distributed key management construction based on group signature to stipulation privacy in vehicular ad hoc networks (VANETs). To accomplish the efficient and secure vehicular revolution, following three major goals are examined in the vehicular situation: 1) security; 2) expediency; and 3) diversion. Aside from security related applications, profitable applications also discover their method to entirely employ these networks. To support collaboration, the author Fu-Kuo Tseng et. Al., presented Reed–Solomon codes (RS-codes) improves its safety in VANET. Vehicle- safety-related communication services, which involve consistent and rapid message liberation, generally insist transmit communications in vehicular ad hoc networks (VANETs). The author Xiaomin Ma et. Al., proposed a distributive cross-layer system for the plan of the direct channel in dedicated short range communications with three levels of transmit services that are serious to most probable vehicle-safety-related applications. In addition to this,

the author Yong Hao et.Al., extend a medium access control (MAC) layer logical model and bring out NS2 simulations to scrutinize the key allocation delay and overlooked recognition ratio of malevolent messages, with the key organization construction being implemented over 802.11 based VANETs.

Keywords: Vehicular ad hoc networks, privacy, distributed key management, Cooperation enforcement, incentive schemes, packet forwarding, Reed–Solomon codes (RS-codes)

.

I. INTRODUCTION

With the progression and broad deployment of wireless communication skills, car constructors and telecommunication business have freshly happening to provide vehicles with wireless devices that permit the

vehicles to converse with each other and with the wayside communications to improve driving security and develop the driving knowledge. These kinds of vehicular message networks are also referred to as vehicular ad hoc networks (VANETs). VANET naturally present a perfect means of gathering active traffic information and intellection different physical amounts connected to traffic distributions at a very short cost with a high stage of correctness. Such functionalities merely twist a VANET into a vehicular sensor network (VSN), which is measured vital for attaining routine and active information compilation and synthesis in an intellectual transportation system. VSNs have the possible to transform the pouring experience and generate a novel metropolitan-area traffic stream power framework.

The enduring proceedings of vehicular ad hoc networks (VANETs) have important the bright hauling systems (ITSs) to superior levels and also completed vehicle telematics more striking to the community. In VANETs, every vehicle is prepared with an aboard unit (OBU) message device, which permits them to converse not only with all other, i.e., vehicle-to-vehicle (V2V) transportation, but with wayside units (RSUs), e.g., vehicle-to-roadside (V2R) transportation, as well. Owing to this mixture construction of VANETs, a selection of capable applications, sorting from security (e.g., appearance reporting and impact warning) to non-safety (e.g., infotainment), can be allowed to progress the road security and better pouring knowledges.

Privacy is an imperative subject in VANETs. As the wireless transportation channel is a common standard, swapping messages with no safety fortification over the process can simply escape the information that users might desire to remain private. Assumed name based approaches have been presented to conserve the position seclusion of vehicles. Nevertheless, those approaches need the vehicles to accumulate a huge number of pseudonyms and certifications, and do not sustain some significant safe functionality for instance substantiation and reliability.

Computation transparency is another serious concern in VANETs. In the security pouring application, vehicles transmit security messages every 300ms. Because the group signature is exclusive, the calculation overhead of every vehicle will develop into impossible when the mass of vehicles is high. The authors proposed a talented protocol which permit vehicles authenticate messages agreeably by utilizing probabilistic confirmation. Nevertheless, in order to assure proficient assistance, vehicles have to confirm at least twenty-five messages within 300ms which is still a serious calculation weight for the aboard unit (OBU) mounted on a vehicle. In addition, the collision of packet defeat at the average access control (MAC) layer on safety presentation.

Even though VANETs can profits us with prosperous requests on the road, the burgeon of VANETs at rest pivots up entirely perceptive and running the confronts that disquiets the public, e.g., the position isolation, which is one of the basic eminence of privacies (QoPs)1 in VANETs [5]. As VANETs are generally executed in resident scenarios, where the positions of vehicles are closely connected to the citizens, if a VANET reveals any seclusion information of citizens, e.g., position privacy, it cannot extensively be established by the public. Consequently, to present definite position privacy to citizens is a necessity for the broad reception of VANETs to the community.

II. LITERATURE REVIEW

The vehicular ad hoc networks (VANETs) have concerned numerous courtesy owing to their fascinating and capable functionalities counting vehicular safety, traffic jamming prevention, and spot based services. In [1], the author proposed a dispersed key organization framework supported on group autograph to stipulation isolation in vehicular ad hoc networks (VANETs). Dispersed key organization is projected to make possible the revocation of malevolent vehicles, preservation of the system, and varied security strategies, compared with the central key organization assumed by the presented group autograph schemes.

A current course of research on *vehicular ad hoc networks* (VANETs) has agreed us novel opportunities and confronts. Aside from safety-related applications, profitable applications also discover their method to completely exploit these networks. One of the capable applications is the distribution of profitable advertisements over VANETs. Nevertheless, there are unhelpful vehicles that might disturb the dispersion of these advertisements. In [2], Reed–Solomon codes (RS-codes) are employed to build an inducement system and improve its safety by analyzing one separate logarithm demonstration crisis. Vehicle-safety-related message services, which need consistent and rapid message delivery, frequently command transmit communications in vehicular ad hoc networks (VANETs). In [3], proposed and validate a distributive cross-layer scheme for the plan of the direct channel in DSRC with three stages of transmits services that are serious to most probable vehicle-safety-related applications.

As a major objective of the eminence of privacy in vehicular ad hoc networks (VANETs), position privacy is essential for VANETs to completely increase. Even though common alias varying presents a capable resolution for position privacy in VANETs, if the pseudonyms are distorted in an indecent point or position, such an explanation might turn into unacceptable. To manage with the question, in [4], presented an efficient alias varying at social spots (PCS) approach to realize the demonstrable position privacy. In [5], the author proposed a provisional seclusion preserving substantiation method, called *CPAS*, using pseudo identity- supported signatures for safe vehicle-to-infrastructure transportations in vehicular ad hoc networks.

Privacy is a significant concern in VANETs [6]. As the wireless communication direct is a common medium, swapping messages with no any safety fortification over the air can simply escape the information that users might desire to stay private. In [7], a safe *distributed key management* framework is designed with the road side units (RSUs) which are accountable for safe group private keys circulation in a restricted manner. Calculation overhead is a different dangerous concern in VANETs. In [8], the authors proposed a capable protocol which allows vehicles verify messages considerately by occupying probabilistic confirmation.

In the security driving application with common message communication, it is significant to intend protocols with diminutive calculation transparency for appropriate and consistent message processing. In [9], the authors proposed to utilize TESLA, which is confusion based protocol, to decrease the calculation overhead. Nevertheless, the malevolent vehicles could not be recognized in this procedure. A collective signature and certificates substantiation method is proposed in [10], which could confirm all established signatures and certificates at single time. A vehicular network can be recognized over diverse announcement/networking procedures [11] say, cellular networks, IEEE 802.16 (WiMAX), or IEEE 802.11. The 802.11 based procedures is the normal protocol for VANETs [12]. Wired network attaches RSUs and establishment broadcasts data

firmly with no packet loss. If accusers and the accused are all genuine users, suppose authorities have a valuation scheme [13] to review whether the contents of messages are fake or not. Contrast with existing schemes which preload keys into the motor vehicle off-line, the key allocation framework has several advantages [14]- [15].

Although safety-related applications [16] are the major inspiration after VANETs, these networks also supply superior platforms for large-scale extremely mobile applications. In [17], the author commenced the notion of a virtual ??flea market?? Over a vehicular ad hoc network (VANET) called FleaNet. FleaNet customers articulate their burden/offers to purchase/sell items through radio queries. These queries are opportunistically dispersed; developing the mobility of other customers, awaiting a customer/vendor is established.

A considerable confront in vehicular networks is to proficiently present mixed media services with the restraints of restricted resources, high mobility, opportunistic call, and repair time requirements. In [18], the heterogeneous standard stipulation in peer-to-peer (P2P)-based vehicular networks are considered and achieved completely active service approaches with the objectives of exploiting the entire user-satisfaction and achieving a definite quantity of fairness. The proposed scheme in [19] is distinguished by utilizing a lot of RSUs to handle the complete parking lot and is allowed by communication among vehicles and the RSUs. Vehicular ad hoc networks (VANETs) are imagined to present capable applications and services. One serious operation concern in VANETs is to encourage vehicles and their drivers to assist and donate to packet forwarding in vehicle-to-vehicle or vehicle-to-roadside transportation. In [20], the author analyzed the drawbacks of two undemanding approaches, and identified a secure motivation system to motivate collaboration in VANETs.

III. ANALYSIS OF SECURITY SCHEMES IN VANET

In an infrastructure based VANET, the entities are classified into three types:

- Authorities
- Road side infrastructure
- Nodes

Authorities are accountable for key creation and malevolent vehicle judgment. Authorities have authoritative firewalls and other safety fortifications.

Road side infrastructure comprises of road side units organized at the road sides which are in accuse of key organization in the framework.

Nodes are normal vehicles on the road that can converse with each other and RSUs during radio.

Usually, in group signature based isolation system, the communications can be separated into

- The *key distribution phase* and
- The *regular broadcast phase*.

Vehicles get keys vigorously in the key allocation phase and then initiate to transmit their geographic and road stipulation messages occasionally in the standard transmit phase. With group signature, members of a faction mark messages beneath the name of the group. In a faction, there are one faction public key and many equivalent crowd private keys. A message that is marked by any faction private keys can be established with the exclusive faction public key, and the signer's identifier will not be exposed.

Normally, attackers are inside, rational, active, global and parsimonious. Inside attackers are legitimate members of VANETs.

- Rational attackers attack for their individual benefits. They identify the safety method and they desire to assault without being noticed. If there is a mechanism that can detect them and the punishment is severe enough, they tend not to attack.
- Active attackers have the ability to send packets into wireless channels.
- Global attackers have an infinite scale which means they can listen to any information in the network. Attackers might contain strong communication power to correspond over long distances.
- Adversarial thriftiness means an attack connecting a few malevolent nodes is more probable to occur than an attack that needs collusion between a large number of nodes.

3.1 A Distributed Key Management Framework with Cooperative Message Authentication in VANETs

The author Yong Hao et.Al., adopted diminutive group signature in this paper since it has smaller communication transparency than other set signature approaches. The short group autograph works as subsequent:

- Key setup

Authorities distribute the faction public key and broadcast the group private key producer to the key dispenser of group, firmly.

- Membership registration

The faction private key for the user will be broadcasted to the user strongly behind the *group key obtains* the legitimate information of the user, such as its real identifier. Each group private key should only be assigned to one user.

- Signing and verification

Vehicles initiate to mark standard transmit messages by employing the faction private key behind they overtake the analogous RSU. Receivers only recognize messages that are permitted by faction public key in the authentication.

- Key retrieve

The faction private key of the signer can be retrieved from the signature by authorities if there is a dispute. Authorities first check the validity of the signature after they identify the group through the group ID.

The author Yong Hao et.Al., presented a protocol to perceive concussed protocol units and their assistants which is a sort novel safety concern persuaded by the dispersed key organization structure. A misbehaved protocol will allow authorities not succeed to recognize malevolent vehicles. This protocol permits vehicles to be legitimated with their genuine identifiers beneath fortification and guarantees establishments to discover concussed protocol units and uniqueness of malevolent vehicles if there is a clash. The protocol describes message types in

- Registration,
- Messages broadcasting and
- Accusation

Authorities create decisions according to the muster information that vehicles present. Hereby, the muster process is the most significant part. In the transmit message design, the "Grp ID" is the group ID which is used to recognize a group. By totaling a hash value of vehicle's I-private key and the timestamp in the message. When a vehicle discovers that other vehicles launch false messages, it will account to authorities.

3.1.1 Cooperative message authentication

Every vehicle preserves two procedures which are verifiers' collection procedure and supportive substantiation procedure, a neighborhood list, a procedure queue and a buffer. The verifiers collection procedure is in indict of choosing verifiers, locality list and process queue preservation. The supportive substantiation procedure reins message substantiation and warning message sending. In other words, verifiers' collection procedure seals the procedure queue while supportive substantiation process obvious it up after verifications. The region list environs neighbor vehicles' geographic in sequence. Messages which will not be practiced are accumulated in the buffer. When a vehicle attains a *standard transmit message* (RBM), it mines information of the position, speed, path and hastening of the sending vehicle and decides whether to verify the message or not consistent with geographic information. If a verifier discovers an illogical RBM, it will transmit one-hop caution information, which is called as *cooperative substantiation messages* (CAM), to notify others. A non-verifier resorts to the CAM transmitted by other vehicles to substantiate RBM. In the procedure, every vehicle only requires to confirm a very small amount of RBM.

In the key allocation phase, it is considered that vehicles will account fake messages to authorities when there is an argument. The *false message* means that the substance of the message is measured as wrong, but the sender's autograph can be established. For instance, a vehicle might assert a traffic jam anywhere; nevertheless in fact no traffic jam occurs there. The further expression is to use in the cooperative message substantiation is worthless message. An *illogical message* is a message that can not exceed the group autograph substantiation. In such a case, even establishment can not discover the signer of an unacceptable message.

3.1.2 Verifiers selection process

The verifier's collection process intiates when the marked vehicle obtains a message. If an RBM is established, the marked vehicle informs the neighborhood list and computes the receiver sender distance (RSD) among itself and the sender at the transporting time. After that, it attempts to choose whether it is the verifier of the message by contrasting its RSD with RSD of its neighbors. If the marked vehicle is the verifier, it will introduce the RBM to the procedure queue on the stipulation that it can be practiced inside the *substantiation period*, such as 100ms1. Verifiers are determined in a dispersed manner by vehicles themselves consistent with their positions regarding to the sender. A Cartesian match is situating up for every sender at the transferring time and the position of the sender is its derivation. The verifier collection algorithm is projected to produce verifiers symmetrically and regularly about a sender. Furthermore, the arbitrary density disparity in a tiny area could direct to disturbed verifier allocation, where a vehicle might be a verifier for numerous senders consistent with the collection procedure and thus be congested. If this congested vehicle is the only verifier in a region for a sender, the congestion might guide to overlooked discovery when the sender is malevolent. To shun such a zero-verifier situation, the author put a strategy that a verifier will route the RBMs from the contiguous sender with advanced priority over other RBMs; such a strategy is termed as the *nearest-priority policy*.

3.1.3 Cooperative authentication mechanism

The cooperative substantiation process confirms messages in the dispensation queue one by one. If the message is legitimate, it will be established. If a CRBM is illogical, it will be dived. An unacceptable RBM will be learned to others by the marked vehicle. In the CAM, there is no autograph to promise the authority of the whole message. There are numerous reasons. 1) The vehicle will forever ensure the authority of the RBM by itself after they obtain a CAM. Consequently, the signature of CAM only misuses computing capability of the OBU. 2) An elegant attacker would not connect the applicable signature to the CAM if it tries to deceive.

3.1.4 Authentication mode switching

When the vehicles are beneath the exposure of an RSU, the RSU could be a organizer to commence the substantiation mode switching. Nevertheless, the vehicle-initiated approach is more bendable. Based on the position information accepted by every standard transmit message, a vehicle can simply guess the thickness in the area sheltered by its communication range.

3.1.5 Security performance analysis

Vehicles may be attacked in both the key allocation phase and the regular transmit phase.

Key distribution phase

1) Appropriating the ID of other vehicles
2) Receiving key without acknowledgement
3) Collusion Attacks

Regular Broadcast Phase

1) Collusion and Sybil Attacks
2) Selfish Behaviors

3.1.6 MAC layer performance analysis

In MAC layer performance analysis section, the author developed a logical model for MAC layer presentation examination of the CMAP. The author considers 802.11 based VANETs, where the transmission from every vehicle is prohibited with a dispersed organization function (DCF). It is implicit that the vehicles are consistently dispersed all along the road, and thus the number of vehicles in an area has a Poisson allocation.

A. Backoff Process in Broadcast

The backoff procedure can be explained by a discrete-time Markov chain, with the condition of the chain termed as the backoff answer value. Use k to indicate a probable backoff counteract value, the one-step evolution probabilities of the Markov chain can be articulated as

$$P_{k+1,k} = 1, k \in 0, W-2$$
$$P_{0,k} = 1/W, k \in 0, W-1$$

B. MAC-layer Channel Behavior

Usually, the MAC-layer channel performance done by a marked vehicle. Let *pi*, *ps*, and *pc* denote the prospects that the marked vehicle examines an inactive direct, a thriving communication (from other vehicles), and a

impact, correspondingly. Every vehicle can be represented as a *G/G/*1 queue. Let *p*0 denote the prospect that the queue is blank; the prospect that a vehicle contact channel in an idle slot can then be termed as $(i - P_0)\tau$.

C. Average Packet Service Time

The *average packet service time* is termed as the average time phase from the immediate that a packet develops into the skull of the queue and initiates to compete for broadcast to the instant when that the packet is sent. The author route to the prospect engendering function (PGF) technique to obtain the usual packet service time. With the CMAP, there are two types of packets, one moving an RBM message and the other moving a CAM message. Let λ signify the average time of producing RBM messages in a vehicle. Use *pmal* to signify the prospect that an RBM is produced by a malevolent vehicle, and *V* signifies the average number of verifiers for every RBM. The total standard rate of creating CAM messages for confirming the RBM messages in a hauler sensing area is indicated with traffic approaches.

IV. EXPERIMENTAL EVALUATION

In section 4, NS2 simulations have been used to scrutinize the performance of the key distribution framework and cooperative authentication protocol. The author mostly considers a highway situation with three lanes in every direction. Vehicles are located consistently on the road and journey at speed of 30 ± 5m/s (roughly equivalent to the range of 56 - 80 miles/hour). The highway location gives us the expediency to assess the inferior bound of the performance, by organizing vehicles with senior speeds and superior densities to shove several units into a high-load situation. The author also simulates a characteristic city road scenario consistent with the settings, where the key allocation performance is certainly much better than that under a high-load road condition. The corporeal and MAC layer parameters of the 802.11 transmit protocol used in the simulations are listed in the table.

Parameter	value
Preamble length	40 us
PLCP header length	8 us
Slot time	16 us
MAC header size	28 bytes
Wireless channel rate	6 Mbps
Contention window	16

The simulation results illustrate that most of the vehicles obtain their G-private keys very soon after they establish the TCP association, while some vehicles practice a delay of three or more seconds. Some other vehicles are not capable to obtain the G-keys. The further delay is owing to the impact and the connected TCP break. For the TCP protocol, the original round-trip time (RTT) (used as the initial timeout value) is termed as three seconds consistent with the RFC 2988. The quantity of singularity vehicles having more than 9 seconds is much less for the intervals of 0.4 second and 0.8 second than other cases. The elucidation is that the TCP

retransmissions in these two cases diverge from the RSU transmit epochs for more collisions, while the retransmission (based on the timeout value of 3 seconds) will crash with prospect transmit epochs, if the transmit interval is 0.2, 0.6, or 1.0 second.

V. RESULTS AND DISCUSSION

The process of analyzing the performance of the VANET is processed over here with several types of mechanisms and analyzed the results efficiently with the underlying performance. The graph below describes the process of analysis of the security in VANET based on the specified schemes.

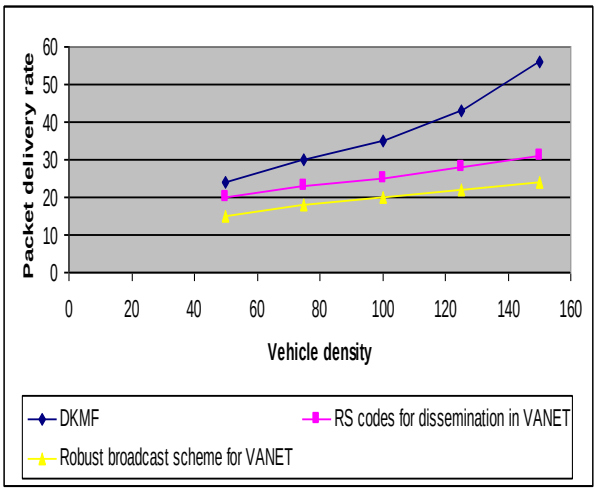

Fig 5.1 Vehicle density vs. packet delivery rate

Fig 5.1 describes the packet delivery rate based on the density of the vehicles in the network environment. The packet delivery ratio is defined as the proportion of transmissions that can be successfully received. The PDR is a critical performance measure affecting both the network utilization and security performance. A low PDR (or a high packet loss ratio due to collision) means low bandwidth utilization, and the loss of CAM tends to result in missed detection. Compared to the other works like Reed Solomon codes for dissemination in VANET and robust broadcast scheme for VANET, the author Yong Hao et.Al.,'s DKFM presented an efficient packet delivery rate based on the number of vehicles present in the network environment.

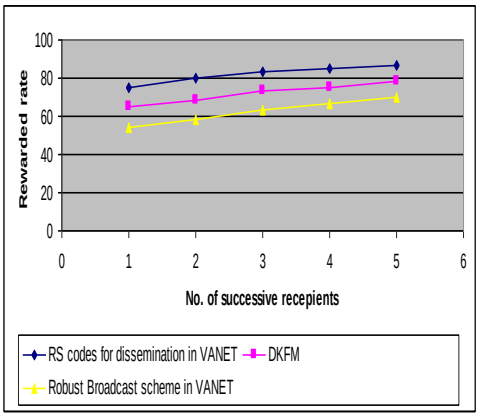

Fig 5.2 Successive recipients vs. rewarded rate

Fig 5.2 describes the rewarded rate of the vehicles present in the network environment based on the successive recipients in which they receive the packet data from source to destination in a reliable manner. The Reed Solomon code scheme in VANET needs a storage capacity to store all the receipts and vouchers and hand over to the authorities, whereas the vehicles in the signature-based scheme do not need to store anything. For the communication complexity, the reed Solomon code scheme provides less and other two approaches are relatively analyzed and processed, which are the heaviest load among these three schemes.

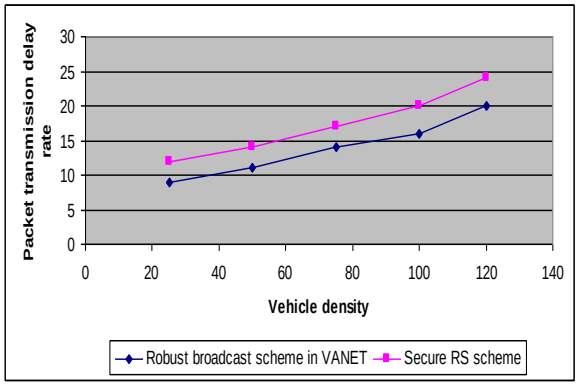

Fig 5.3 Vehicle density vs. packet transmission delay rate

Fig 5.3 describes the packet transmission delay rate based on the number of vehicles present in the network environment. Since the robust scheme used a novel protocol for reliable and fast delivery of safety-related messages, the process of identifying the packet transmission is done efficiently with the control channel for DSRC in VANET. Compared to the other two works, the Xiaomin Ma et. Al., presented an efficient packet transmission process by following the novel robust broadcast scheme in VANET.

VI. CONCLUSION

In this paper, we analyzed the performance of the novel distributed key management scheme based on the short group signature to stipulation seclusion in the VANETs. The dispersed key organization is enhanced with a supportive message substantiation protocol to improve the serious calculation overhead. We investigate the demanding matter that semi-trust RSUs may be negotiated, and compromised RSUs may even conspire with malevolent vehicles. The author designed a safety procedure to avert negotiated RSUs and malevolent vehicles from attacking. The design assures that RSUs deal out keys reasonably and supply some approaches to perceive negotiated RSUs and malevolent vehicles. Furthermore, by a supportive message substantiation protocol, a vehicle only desires to validate a diminutive amount of messages, and the calculation burden of vehicles is condensed really. In this paper, detailed analyses are taken over with the possible security attacks and the equivalent defense, in addition to expand a MAC layer logical model. Extensive NS2 simulations are also presented to estimate the performance of the techniques for VANET security.

REFERENCES

[1] Yong Hao et. Al., "A Distributed Key Management Framework with Cooperative Message Authentication in VANETs", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 29, NO. 3, MARCH 2011

[2] Fu-Kuo Tseng et. Al., "A Secure Reed–Solomon Code Incentive Scheme for Commercial Ad Dissemination Over VANETs", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 60, NO. 9, NOVEMBER 2011

[3] Xiaomin Ma et. Al., "Design and Analysis of a Robust Broadcast Scheme for VANET Safety-Related Services", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 1, JANUARY 2012

[4] Rongxing Lu, et. Al., "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 1, JANUARY 2012

[5] Kyung-Ah Shim et. Al., "*CPAS*: An Efficient Conditional Privacy-Preserving
Authentication Scheme for Vehicular Sensor Networks", IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 4, MAY 2012

[6] R. Lu, X. Lin and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks", in *Proc. IEEE INFOCOM*, San Diego, California, 2010.

[7] N. Banerjee, M.D. Corner, D. Towsley and B.N. Levine, "Relays, base station and meshes: enhancing mobile networks with infrastructure," in *Proc. ACM Mobicom*, San francisco, California, Sep. 2008.

[8] X. Sun, "Anonymous, secure and efficient vehicular communications," Master Thesis, Univeristy of Waterloo, 2007.

[9] C. Zhang, X. Lin, R. Lu, P.-H. Ho and X. Shen, "An efficient message authentication scheme for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 57, no. 6, pp. 3357-3368, 2008.

[10] C. Zhang, X. Lin, R. Lu and P.-H. Ho., "RAISE: an efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. IEEE ICC*, Beijing, China, May 19-23, 2008.

[11] A. Wasef and X. Shen, "ASIC: aggregate signatures and certificates verification scheme for vehicular networks", in *Proc. IEEE Globecom*, Honolulu, Hawaii, USA, Nov. 30 - Dec. 4, 2009.

[12] A. Studer, E. Shi, F. Bai and A. Perrig, "TACKing together efficient authentication revocation, and privacy in VANETs," in *Proc. IEEE SECON, 2009*.

[13] D. Jiang and L. Delgrossi, "IEEE 802.11p: towards an international standard for wireless access in vehicular environments," in *Proc. IEEE VTC*, May 2008.

[14] M. Raya, P. Papadimitratos, V.-D. Gligor and J.-P. Hubaux, "On datacentric
trust establishment in ephemeral ad hoc networks," in *Proc. IEEE INFOCOM*, pp. 1238-1246, Apr. 2008.

[15] Y. Hao, Y. Cheng and K. Ren, "Distributed key management with protection against RSU compromise in group signature based VANETs," in *Proc. IEEE Globecom*, New Orleans, Nov., 2008.

[16] S. Park and C.C.Zou, "Reliable traffic information propagation in vehicular ad-hoc networks," *IEEE Sarnoff Symposium*, Apr. 2008.

[17] C. Li and S. Shimamoto, "An open traffic light control model for reducing vehicles CO2 emissions based on ETC vehicles," *IEEE Trans. Veh. Technol.*, 2011, DOI: 10.1109/TVT.2011.2168836.

[18] U. Lee, J. Lee, J.-S. Park, and M. Gerla, "Fleanet: A virtual market place on vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 1, pp. 344–355, Jan. 2010.

[19] L. Zhou, Y. Zhang, K. Song,W. Jing, and A. Vasilakos, "Distributed media services in P2P-based vehicular networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 2, pp. 692–703, Feb. 2011.

[20] R. Lu, X. Lin, H. Zhu, and X. Shen, "An intelligent secure and privacy-preserving parking scheme through vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 6, pp. 2772–2785, Jul. 2010.

[21] Y. Sun, X. Lin, R. Lu, X. Shen, and J. Su, "Roadside units deployment for efficient short-time certificate updating in VANETs," in *Proc. IEEE ICC*, May 2010, pp. 1–5.