Encryption Scheme for Vehicular Ad hoc Network

Trambak R. Pawar **Prof. AmitKumar Manekar**

Abstract — **In Vehicular Ad hoc Networks (VANETs), integrity of data is important security concern for the inter-vehicle and vehicle to roadside communications. Vehicles and the information have to be protected from the attacks on their privacy and from the misuse of their private data which is shared over communication. Recent studies show that vehicular ad hoc network authentication and the privacy preservation can be achieved by using various techniques. Safety information exchange enables life-critical applications, like lane merging and the alerting functionality during intersection traversing. So security plays an important role in VANET applications. We propose a lightweight encryption scheme called Enhanced P-coding scheme to provide confidentiality and integrity to data for VANET's in transmission. The basic idea of P-coding encryption is to the convert the source message into cipher text then divide that converted message into no. of blocks and then randomly permute the blocks, before transmitting to receiver. Without knowing the intermediate recoding, eavesdroppers cannot decrypt coded message in the transmission and thus cannot obtain any meaningful information.**

I. INTRODUCTION

VANET- Vehicular Ad-Hoc Network is the network in which communication has been done in between road side units to cars, car to car in a short range. A VANET uses cars as mobile nodes in a MANET to create a mobile network. A VANET turns each participating vehicle into a wireless router , allowing cars around 50 to 250 meters of each other to connect the vehicle create a network with a wide range. As car fall out of the signal range and drop out of the ad hoc network, other cars also join in then connect the other vehicles to one another so that the wireless ad hoc network is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. The world largest automotive companies promote this VANET technology like BMW, AUDI, Mercedes, FORD. Vehicular Ad Hoc Networks (VANETs) are important wireless communication paradigms. The System and infrastructure less nature of VANETs makes them suitable for collecting emergency data in disastrous areas. A critical issue in VANETs is how to reduce energy consumption and maintain a longer life time for nodes in VANET. Several energy-efficient schemes are proposed to resolve this issue. Recent studies demonstrate that network coding can achieves a lower energy consumption in VANETs. The energy saving comes from fact that less transmissions are required when in-network nodes are enabled to encode packets. Besides basic transmissions, energy consumption can also come from encryption and decryption operations at each node, as most VANETs need some level of protection on their content. For example, in a battle field, the data communicated between soldiers with mobile devices can be very sensitive, and should be kept confidential during transmissions. In fact, the information mixing feature of network coding provides a security, based on which a more efficient encryption scheme can be designed. Vile la et al propose such a scheme, in which the source vehicle performs random linear coding on the messages to be sent and locks/encrypts the coding vectors using the symmetric key shared between it and all sinks.

II. RELATED WORK

VANET has become an active area of research, standardization, and development because it has tremendous potential to improve vehicle and road safety, traffic efficiency, and convenience as well as comfort to both drivers and passengers. Recent research efforts have placed a strong emphasis on novel VANET design architectures and implementations. A lot of VANET research work focused on specific areas including routing, broadcasting, Quality of Service (QoS), and security. This survey some of the recent research results in these areas. VANET research challenges that still need to be addressed to enable the ubiquitous deployment and wide spread adoption of scalable, reliable, robust, and secure architecture, protocols, technologies and services. Vehicular ad hoc networks (VANET) are created by vehicles equipped with short and medium range wireless communication. Communication is possible between vehicles within each other's radio range, and with fixed gateways along the road. The ability of vehicles to communicate directly with each other via wireless links and form ad hoc networks is opening up a plethora of exciting applications. In particular, these networks have important applications in Intelligent Transportation Systems (ITS) [1]. Due to the highly dynamic nature of these networks which results in their frequent fragmentation into disconnected clusters that merge and disintegrates dynamically. In vehicular ad hoc networks (VANETs), the speed of a vehicle is changed from 10 to 40 m/s (36–144 km/h); therefore, the need for efficient authentication is inevitable. Compared with the current key agreement scheme, ABAKA can efficiently authenticate multiple requests by one verification operation and negotiate a session key with each vehicle by one broadcast message. Elliptic curve cryptography is adopted to reduce the verification delay and transmission overhead [2]. Although the number of accidents in developed countries declines despite increasing traffic density, novel vehicle-2-x communications (V2X) systems promise to reduce the remaining fatal accidents to almost zero. For this reason, current research is engaging in VANETs where vehicles exchange short messages with each other on the one hand and with the infrastructure on the other. By putting traffic relevant vehicle data into those messages, cooperative driver assistance services can be realized, which help to increase safety and comfort [3]. VANETs exhibit dynamic topology and intermittent connectivity due to high vehicle mobility. These distinguished features declare a challenging question: how to detect on the fly vehicular networks such that we can explore mobility-assisted message dissemination and topology control in VANETs. VANETs manifest dynamic topology and intermittent connectivity due to high mobility of vehicles[4]. Although VANETs can benefit us with rich applications on the road, the flourish of VANETs still hinges up fully understanding and managing the challenges that concerns the public, e.g., the location privacy, which is one of the fundamental quality of privacies (QoPs) in VANETs [5]. Shen introduce a new attack termed wormhole-aided sybil attack on PBR, the wormhole-aided sybil attack has the worst impact on the packet delivery in PBR[6]. Vehicle safety related communication services, which require reliable and fast message delivery, usually demand broadcast communications in vehicular ad hoc networks (VANETs). The new scheme for enhancing broadcast reliability includes preemptive priority in safety services, dynamic receiver oriented packet repetitions for one-hop emergency warning message dissemination, a multi frequency busy tone and mini slot within the distributed inter frame space (DIFS) in IEEE 802.11, and robust distance-based relay selection for multi hop broadcast of emergency notification messages [7].

Nowadays the massive deployment of VANETs is imminent with the standardization of VANET technologies like dedicated short-range communications, DSR, and wireless access vehicular environment, WAVE underway. Thus, it becomes both necessary and feasible to explore new value added applications for VANETs, such as multiplayer games and road surface weather services[8]. Providing secure group communication, however, can be challenging in VANETs because of high mobility of the vehicles. In order to provide confidentiality and ensure only the authorized users have access to information, group communication applications can use cryptographic tools and techniques. A common traffic encryption key (TEK) shared among all members of the group can be used to encrypt and decrypt data and this will ensure confidentially and legitimacy of access[9]. One of the most important characters of VANETs is that almost every vehicle is equipped with a global positioning system (GPS). The trust and reputation models are proposed as new approaches to circumvent with this constraint and to filter out inaccurate messages and malicious vehicles. Trust establishment is tagged in many existing research works for peer to peer, sensors, and mobile ad hoc networks [11].

Now the research is focused on the security of the Vehicular Ad hoc Network. This research contains the requirements of the VANET security and the threats to that security. The recent solution is also evaluated in the research. As the development in VANET technology there are various security and privacy challenges are also introduced as below. The security of VANETs is crucial as their very existence relates to critical life threatening situations. It is imperative that vital information cannot be inserted or modified by a malicious person. The system must be able to determine the liability of drivers while still maintaining their privacy. These problems are difficult to solve because of the network size, the speed of the vehicles, their relative geographic position, and the randomness of the connectivity between them. An advantage of vehicular networks over the more common ad hoc networks is that they provide ample computational and power resources. For instance, a typical vehicle in such a network could host several tens or even hundreds of microprocessors. The attackers having three dimensions: “insider versus outsider”, “malicious versus rational”, and “active versus passive”. The types of attacks against messages, can be described as follows: “Bogus Information”, “Cheating with Positioning Information”, “ID disclosure”, “Denial of Service”, and “Masquerade”. The reliability of a system where information is gathered and shared among entities in a VANET raises concerns about data authenticity. For example, a sender could misrepresent observations to gain advantage (e.g., a vehicle falsely reports that its desired road is jammed with traffic, thereby encouraging others to avoid this route and providing a less congested trip).More malicious reporters could impersonate other vehicles or road-side infrastructure to trigger safety hazards. Vehicles could reduce this threat by creating networks of trust and ignoring, or at least distrusting, information from untrusted senders.

III. METHODOLOGY

3.1 Enhanced P-Coding Technique:-

To solve the security issues we use the cryptography technique which provides high security to the message send and received by the vehicles connected in the VANET. We design the encryption scheme called as P- Coding technique which converts the plain text message into the cipher text called as encoding of message. This encoded message is send to the particular destination vehicle by using the wireless network channel. At receiving end the receiver again convert the cipher text message known as the decoding of message. This technique avoids the man in middle attack as well as the denial of service attack.

The working of P-coding as follows:-
P-Coding is basically divided into three operations

1. Source Encoding
2. Intermediate Recording
3. Sink decoding

1. Source Encoding:-

In this operation the original message is converted into the encoded message i.e. cipher text is generated. We use different symbol instead of characters the substitution technique is best for the source encoding of message. The substitution means replacing with another character at the old character. By using the different symbols the attacker cannot guess the original content. The pigpen cipher scheme is used for this source encoding in which each symbol is assigned to a particular alphabet.

e.g.

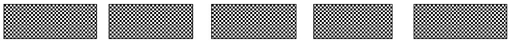
Plain Text	This is beautiful flower
Cipher Text	•□€£ ¥© ¶»¡÷òćøʅ ɌƒƓȡƟƻ

2. Intermediate Recoding :-

The Intermediate Recoding technique divides the cipher text message C into no of small messages c1,c2,c3…. cn. Each small message block is having a no are arranged in the such manner that it will very difficult to the attacker to access that data. The transposition technique is used for arranging the message block. Each message block contains the unique no. this is store in in vector called as Global Encoding Vector i.e. GEV.

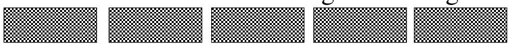
The original message

The message is divided into blocks.



1 2 3 4 5

Now after the intermediate recording the message will be



3 5 4 1 2

3. Sink Decoding:-

The sink decoding is the process in which we append the GEV key to the message. We either attach the GEV to the start of message or at the end of the message i.e. append to the message.

IV. Block Diagram

The fig 4.1 shows the working of the encryption system, the architecture consist of the no. of vehicles these can operate as a sender and receiver of the message. RSU is roadside unit which is connected to the base station. The base station is main part of the VANET. The base station performs information sharing and broadcasting of the messages. In the proposed system we use the base station for providing secure communication using encryption scheme known as a P-Coding. The basic idea of P-Coding is the source randomly permute the symbols of each packet (which is prefixed with its coding vector), before sending to transmission. Without knowing the permutation, eavesdroppers cannot locate coding vectors for correct decoding, and thus cannot obtain any meaningful information. When a Vehicle A sends the message to RSU, it forwards that message to Base Station. The function of the base station is encoding of the messages using P-coding scheme. The encoding message is known as cipher text. This encoded message is forwarded to base stations as per the address of receiver. The base station performs the reverse operation of P-coding i.e. decoding of message. Then this plaintext message is received to the appropriate receiver. The main objective of performing the P-coding operation in base station is to reduce the overhead of the connected node. The process of encoding and decoding of data burdens the connected vehicles. We use the P-coding encryption scheme because it is lightweight encryption scheme. This scheme is used in Mobile Ad hoc Network[32] using network coding. We use the pigpen cipher which is the simple cryptographic scheme. This pigpen cipher is a simple substitution cipher technique which is use the set of different symbols to replace the characters of the original message. The special symbols can be shared only with the base stations. So that the attacker i.e. eavesdropper cannot monitor the original message. Even if the attacker can get access to set of symbols he unable to get original message because of we use the intermediate recoding of the cipher text.

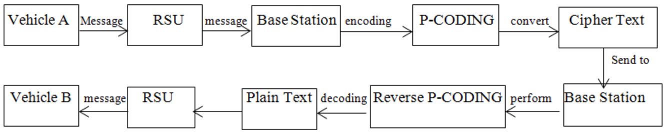


FIG. 4.1 BLOCK DIAGRAM

V. Analysis Model

Following is the mathematical model for the current system,
1.Let S be the P-coding Encryption Technique which provide secure communication in VANET Network between vehicles.
Such that S={ V, R, P, B, C, E, D ǀΦ S}
Where
V represent the vehicle V={v1,v2,…….. vn},
R represent the receiver R={r1,r2,…… rn};
P represents the plain text of message P={p1,p2,…… pn};
B represents the base station B={b1,b2…. Bn};
C represents the ciphertext C={c1,c2,…. C3};
E represents the Encoding process E={e1,e2,… en};
D represents the Decoding process D={d1,d2,… dn};
2.Let the f(v) be the rule of V into R such that for any vehicle there is a receiver
f(v) {v1,v2,.. vn } -> { r1,r2,… rn} ϵ R
3.Let the f(v) be the rule of V into P such that for any vehicle there is a Plaintext message
f(v) {v1,v2,.. vn } -> { p1,p2,… pn} ϵ P
4.Let the f(v) be the rule of V into B such that for any vehicle there is a Base Station
f(v) {v1,v2,.. vn } -> { b1,b2,… bn} ϵ B
5.Let the f(r) be the rule of R into S such that for any receiver there is a Sender
f(r) {r1,r2,.. rn } -> { v1,v2,… vn} ϵ S
6.Let the f(r) be the rule of R into B such that for any receiver there is a Base Station
f(r) {r1,r2,.. rn } -> { b1,b2,… bn} ϵ B
7.Let the f(r) be the rule of R into P such that for any receiver there is a plain text message
f(r) {r1,r2,.. rn } -> { p1,p2,… pn} ϵ P

8.Let the f(b) be the rule of B into P such that for any base station there is a plain text message
f(b) {b1,b2,.. bn } -> { p1,p2,… pn} ϵ P
9.Let the f(b) be the rule of B into C such that for any base station there is a cipher text message
f(b) {b1,b2,.. bn } -> { c1,c2,… cn} ϵ C
10.Let the f(b) be the rule of B into E such that for any base station there is a Encoding message
f(b) {b1,b2,.. bn } -> { e1,e2,… en} ϵ E
11.Let the f(b) be the rule of B into D such that for any base station there is a Decoding message
f(b) {b1,b2,.. bn } -> { d1,d2,… dn} ϵ D

VI. Performance Analysis

The performance of the proposed system is analyzed by using the three main characteristics of any network. These include encryption time, energy consumption and the throughput as well as the failure rate of the system. We perform various experiments to compare the existing system with proposed system.

6.1 Encryption Time:-

We perform the experiments to calculate the total encryption time of the proposed system. We increase the message size with each experiment. The fig 6.1 of graph shows the total encryption time of the system. This graph shows that the proposed system has very less encryption time than existing system. As the message increases the encryption time of the system is increased with less amount of time.

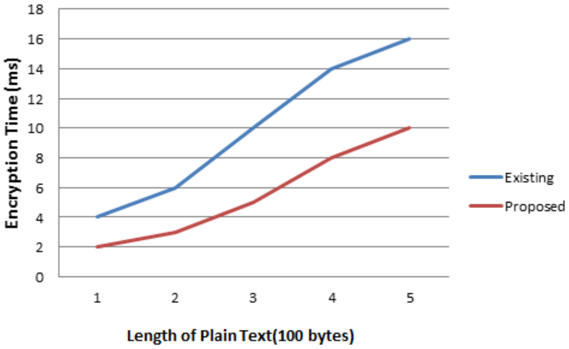


FIG 6.1 Encryption Time

6.2 Throughput:-

The throughput of the network is the total no. of messages transferred to a system at a time. The throughput of the system is calculated by the size of message per unit time i.e. seconds, minutes, hours. The throughput of system is always high. In proposed system the throughput is higher than the existing system as less encryption time means larger throughput [1].

6.3 Energy Consumption:-

As the proposed system is ad hoc network, it uses the limited source of energy. So we have to reduce the energy consumption of the system used for encryption of the messages. Less encryption time also means fewer CPU cycles, and less energy consumptions [1]. The proposed system uses the simple substitution technique so the CPU utilization of the system is lower as compared to the existing system. Less CPU utilization of the system consumes the less energy. The difference between the proposed system and existing system is shown in fig 6.2.

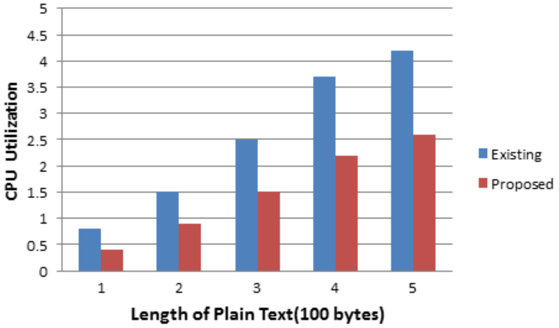
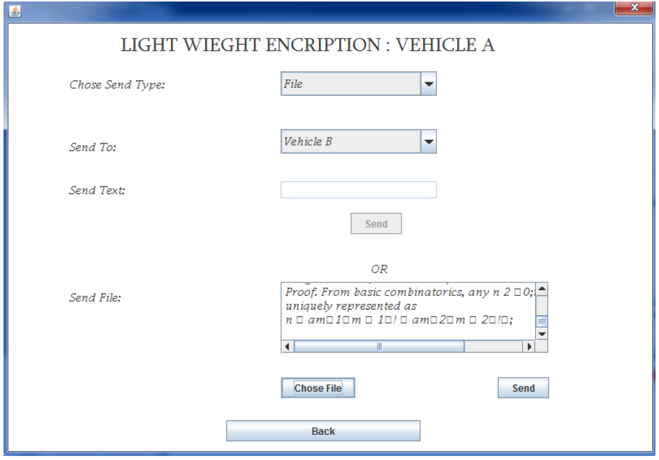


FIG 6.2 CPU Utilization

VII. Result

The output of the proposed system is the secure delivery of messages from one vehicle to another in less energy consumption. The proposed system take less time to convert the plain text message to cipher text in less time and less energy consumption as the vehicle are using the limited source of energy.


LIGHT WIEGHT ENCRIPTION : VEHICLE A

Chose Send Type: File

Send To: Vehicle B

Send Text:

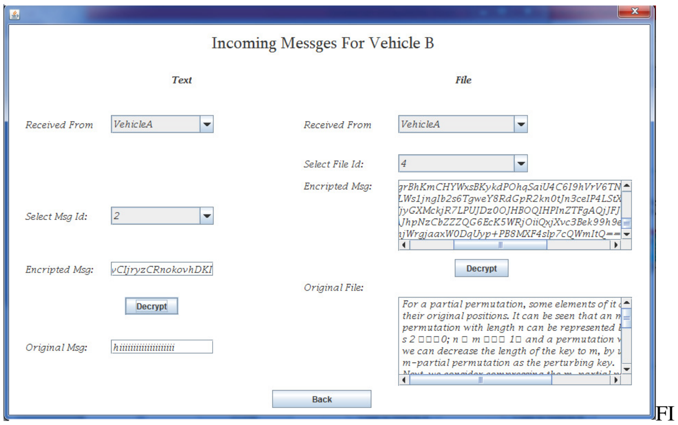
OR

Send File:

Proof. From basic combinatorics, any n 2 □0;
uniquely represented as
n □ am□1□m □ 1□! □ am□2□m □ 2□!□;

FIG 7.1 Sending Vehicle

The above fig shows the encryption process of the text file at one node vehicle A. this file is send to the vehicle B. In this process the message converted into plain text to cipher text. This requires less time for encoding process.



Incoming Messges For Vehicle B

Text

Received From: VehicleA

Select Msg Id: 2

Encripted Msg: vCIjryzCRnokovhDKI

Decrypt

Original Msg: hiiiiiiiiiiiiiiiiii

File

Received From: VehicleA

Select File Id: 4

Encripted Msg:
grBhKmCHYWxsBKykdPOhqSaiU4C6I9hVrV6TN
LWs1jngIb2s6TgweY8RdGpR2kn0tJn3ceIP4LStX
jyGXMckjR7LPUJDz0OJHBOQIHPInZTFgAQjJFJ
JhpNzCbZZZQG6EcK5WRjOiiQxjXvc3Bek99h9e
ijWrgjaaxW0DqUyp+PB8MXF4slp7cQWmItQ==

Decrypt

Original File:
For a partial permutation, some elements of it
their original positions. It can be seen that an m
permutation with length n can be represented
s 2 □□□□0; n □ m □□□ 1□ and a permutation
we can decrease the length of the key to m, by
m-partial permutation as the perturbing key.

Back

FIG 7.2 Incoming Messages

The above fig shows the incoming messages from vehicle A. The vehicle B has to choose the text or file from the list of vehicles connected to it. The each message has the unique source id to distinguish the various messages from single node.

CONCLUSION

In this work studied the various problems of communication and information sharing in VANET based on wireless network. Previous studies demonstrated that information sharing through wireless network has many security issues like data integrity, repudiation, confidentiality and other privacy issues. To resolve the data integrity the proposed Enhanced P-Coding, a lightweight encryption scheme for messages, to provide the integrity of data as well as the decrease the load of encoding and decoding operation on nodes. P-Coding uses simple permutation encryptions to generate considerable confusion to eavesdropping adversaries. P-Coding is efficient in computation, and less overhead of operation for encryptions/decryptions.

REFERENCES

[1]. Peng Zhang, Chuang Lin, Yixin Jiang, Yanfei Fan, and `Xuemin (Sherman) Shen ,"A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 9, SEPTEMBER 2014

[2]. Yujin Li, Ming Zhao, Wenye Wang ,"Intermittently Connected Vehicle-to-Vehicle Networks: Detection and Analysis", 2011 IEEE

[3]. Tahani Gazdar, Abderrahim Benslimane and Abdelfettah Belghith,"Secure Clustering Scheme Based Keys Management in VANETs", 2011 IEEE

[4]. Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien,"ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 60, No. 1, January 2011

[5]. Stefan Lobach,Ilja Radusch, "Integration of Communication Security into Advanced Simulation Environments for ITS", 2011 IEEE

[6]. Rongxing Lu, Xiaodong Lin, Tom H. Luan,Xiaohui Liang, and Xuemin (Sherman) Shen,"Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANETs", Ieee Transactions On Vehicular Technology, VOL. 61, NO. 1, JANUARY 2012

[7]. Nizar Alsharif, Albert Wasef, and Xuemin (Sherman) Shen,"Mitigating the Effects of Position-Based Routing Attacks in Vehicular Ad Hoc Networks", 2011 IEEE

[8]. Zhengming Li, Congyi Liu, And Chunxiao Chigan,"Gpas: A General-Purpose Automatic Survey System Based On Vehicular Ad Hoc Networks", IEEE Wireless Communications, August 2011

[9]. Dushan Aththidiyavidanalage Don, Vaibhav Pandit, and Dharma P. Agrawal,"Multivariate Symmetric Polynomial Based Group Key Management for Vehicular Ad hoc Networks", 2012 IEEE

[10]. Pengfei Zhang, Zhenxia Zhang, Azzedine Boukerche,"Cooperative Location Verification for Vehicular Ad-Hoc Networks", IEEE ICC 2012 - Ad-hoc and Sensor Networking Symposium

[11]. Tahani Gazdar, Abderrezak Rachedi, Abderrahim Benslimane and Abdelfettah Belghith,"A Distributed Advanced Analytical Trust Model for VANETs", Globecom 2012 - Ad Hoc and Sensor Networking Symposium 2012 IEEE

[12]. Joseph Benin, Michael Nowatkowski, and Henry Owen,"Vehicular Network Pseudonym Distribution in Congested Urban Environments, 978-1-4673-1375-9/12/$31.00 ©2012 IEEE

[13]. Sanaa Taha and Xuemin (Sherman) Shen,"A Link-layer Authentication and Key Agreement Scheme for Mobile Public Hotspots in NEMO based VANET", Globecom 2012 - Communication and Information System Security Symposium, 2012 IEEE

[14]. Yujin Li and Wenye Wang ,"Geo-Dissemination in Vehicular Ad Hoc Networks", IEEE ICC 2012

[15]. Subir Biswas, Jelena Miˇsi´,"Relevance-based Verification of VANET Safety Messages", 2012 IEEE

[16]. Zhengming Li, Congyi Liu, and Chunxiao Chigan,"On Secure VANET-Based Ad Dissemination With Pragmatic Cost and Effect Control", IEEE Transactions On Intelligent Transportation Systems, Vol. 14, No. 1, March 2013

[17]. Khaleel Mershad and Hassan Artail,"A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 62, No. 2, February 2013

[18]. Stefan Dietzel, Jonathan Petit, Geert Heijenk, and Frank Kargl ,"Graph-Based Metrics for Insider Attack Detection in VANET Multihop Data Dissemination Protocols", IEEE Transactions On Vehicular Technology, Vol. 62, No. 4, May 2013 1505

[19]. Rongxing Lu, Xiaodong Lin, Zhiguo Shi, Xuemin (Sherman) Shen, ,"A Lightweight Conditional Privacy-Preservation Protocol for Vehicular Traffic-Monitoring Systems", 2013 IEEE

[20]. Shi-Jinn Horng, Shiang-Feng Tzeng, Yi Pan, Pingzhi Fan, XianWang, Tianrui Li, Muhammad Khurram Khan ,"b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 11, November 2013

[21]. Xinyi Wang, Zheng Huang, Qiaoyan Wen, Hua Zhang,"An Efficient Anonymous Batch Authenticated and Key Agreement Scheme Using Self-Certified Public Keys in VANETs", 2013 IEEE

[22]. Albert Wasef and Xuemin (Sherman) Shen,"EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks", IEEE Transactions On Mobile Computing, Vol. 12, No. 1, January 2013

[23]. Yong Hao, Jin Tang and Yu Cheng,"Secure Cooperative Data Downloading in Vehicular Ad Hoc Networks", IEEE Journal On Selected Areas In Communications/Supplement, Vol. 31, No. 9, September 2013

[24]. Xiaodong Lin and Xu Li,"Achieving Efficient Cooperative Message Authentication in Vehicular Ad Hoc Networks", IEEE Transactions On Vehicular Technology, Vol. 62, No. 7, September 2013

[25]. Subir Biswas and Jelena Miši´c,"A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE-Enabled VANETs", IEEE Transactions On Vehicular Technology, Vol. 62, No. 5, June 2013

[26]. Sanaa Taha and Xuemin (Sherman) Shen,"A Physical-Layer Location Privacy-Preserving Scheme for Mobile Public Hotspots in NEMO-Based VANETs", IEEE Transactions On Intelligent Transportation Systems, Vol. 14, No. 4, December 2013

[27]. Sanjay K. Dhurandher, Mohammad S. Obaidat, Amrit Jaiswal, Akanksha Tiwari, and Ankur Tyagi,"Vehicular Security Through

Reputation and Plausibility Checks”, IEEE SYSTEMS JOURNAL, VOL. 8, NO. 2, JUNE 2014

[28]. Jie Li, Huang Lu, Mohsen Guizani, “ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs”, 10.1109/TPDS.2014.2308215, IEEE Transactions on Parallel and Distributed Systems

[29]. Nikita Lyamin, Alexey Vinel, Magnus Jonsson, and Jonathan Loo,”Real-Time Detection of Denial-of-Service Attacks in IEEE 802.11p Vehicular Networks”, IEEE COMMUNICATIONS LETTERS, VOL. 18, NO. 1, JANUARY 2014

[30]. Sourav Kumar Bhoi, Pabitra Mohan Khilar,“Vehicular communication: a survey”, www.ietdl.org, ISSN 2047-4954, doi: 10.1049/iet-net.2013

[31]. Xiaomin Ma, Jinsong Zhang, Xiaoyan Yin, and Kishor S. Trivedi,“Design and Analysis of a Robust Broadcast Scheme for VANET Safety-Related Services”, IEEE Transactions On Vehicular Technology, Vol. 61, No. 1, January 2012

[32]. Sailesh Bharati and Weihua Zhuang,“CAH-MAC: Cooperative ADHOC MAC for Vehicular Networks”, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS/SUPPLEMENT, VOL. 31, NO. 9, SEPTEMBER 2013

[33]. Yiliang Liu, Liangmin Wang, Hsiao-Hwa Chen,”Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. XXX, MONTH YYY, YEAR 2014

[34]. Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, and Hui Li,“Efficient Privacy-Preserving Authentication for Vehicular Ad Hoc Networks”, IEEE Transactions On Vehicular Technology, Vol. 63, No. 2, February 2014

[35]. Maziar Nekovee and Benedikt Bjarni Bogason ,“Reliable and Efficient Information Dissemination in Intermittently Connected Vehicular Adhoc Networks”, 2007 IEEE

[36]. Vikash Porwal,Rajeev Patel, Dr. R. K. Kapoor ,“Review of Internal Security Attacks in Vehicular Adhoc Networks (VANETs)”, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181 ,Vol. 3 Issue 8, August - 2014

AUTHOR’S PROFILE

Author’s Name : Trambak Pawar
is a P.G. student of Computer Engineering at SITRC College of Engineering , Nasik under Savitribai Phule Pune University . He has completed his undergraduate Course of engineering from Savitribai Phule Pune University. His areas of interest include Network Security..