Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

ENHANCED CONTEXT-AWARE NETWORK CODED REPETITION WITH PRIVACY-PRESERVING SCHEME AND TRAFFIC CONGESTION AVOIDANCE IN VEHICULAR AD-HOC NETWORK

Dr. P. Boobalan[1], B. Nivetha[2], S. Saieswari Goliate[3], S. Sharmila[4]

[1]Pondicherry Engineering College, boobalan@pec.edu

[2]Pondicherry Engineering College, nivethanjn@gmail.com

[3]Pondicherry Engineering College, saieswarigoliate@gmail.com

[4]Pondicherry Engineering College, sharisiva171@gmail.com

ABSTRACT- In vehicular ad hoc networks, safety applications allow people to avoid dangerous situations based on the condition of the vehicles in their proximity. Such proximity awareness is realized by admitting each vehicle to collect safety messages called beacons, which are periodically and locally transmitted from its neighbouring vehicles. The reliability of beacon transmissions is a crucial factor that makes safety applications effective in practice. Due to the open medium of communication in vehicular ad hoc network it is vulnerable to many attacks. Therefore, we provide an efficient anonymous authentication scheme with low computational cost. In addition, we introduce congestion detection algorithms to detect areas of high traffic density with low speeds. Altogether we propose a new scheme called Enhanced Context-Aware Network Coded Repetition with Privacy-Preserving Scheme and Traffic Congestion Avoidance in Vehicular Ad-hoc Network to avoid malicious vehicles entering into the VANET and to avoid traffic congestion by suggesting optimal path to vehicles.

KEYWORDS - Authentication, Beacon, Car Agent, coded packet, Privacy Preserving, Road side unit, Signal Agent, Security, Traffic congestion detection, Trusted Authority, Vehicular ad hoc network.

I. INTRODUCTION

The Vehicular Ad-Hoc Network, is a technology that uses motion cars as nodes in a network to create a mobile network. VANET considers every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect. As cars fall out of the signal range and come out of the network, other cars can join in, connecting vehicles to another vehicles so that a mobile Internet is created. Every vehicles communicate with each other for safety application.

In vehicular ad-hoc networks, vehicles frequently share a safety message called beacon with their neighbors. The beacon message contains information of the state of vehicle such as position of vehicle, velocity, heading information, emergency reporting, collision warning, lane change assistance, and other safety-related information. (This task of advertising the presence of a vehicle to its neighboring vehicles is usually called "beaconing"). Hence, active safety applications installed on the vehicle can regularly trace the state of the vehicles in their proximity, and helps the drivers to avoid adversity situations through notifications.

Specifically, the loss recovery should be achieved within the short lifetime of beacons (i.e., 100ms) because information contained in beacon messages is valid only for some period of time. In repetition-based retransmission schemes, the dissemination of the same beacon message is repeatedly transmitted several times by the sender within a short duration in order to allow neighboring vehicles to have chances to recover the lost packet in time.

The key contributions of this paper are: 1) To trace the vehicles or roadside units that abuse the VANET by an efficient anonymous authentication scheme 2) To avoid traffic congestion by suggesting optimal path to vehicle. In this paper, we therefore propose a new scheme called Enhanced Context-Aware Network Coded Repetition with Privacy-Preserving Scheme and Traffic Congestion Avoidance in Vehicular Ad-hoc Network to avoid malicious vehicles entering into the VANET and to avoid traffic congestion by suggesting optimal path to vehicles.

II. RELATED WORK

In [1] the author has discussed about CANCORE: Context-Aware Network Coded Repetition for VANETs, this paper focus on reducing coding overhead by using NC-based repetition scheme for maximizing the effectiveness of safety applications. The NC-based mechanism is nothing but XORing two highly scored beacons which will disseminate to the neighboring vehicles. This method will avoid collision.

In [2] the author has discussed about Efficient Anonymous Authentication With Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks. The methodology used is Privacy tracking mechanism to identity and also to reveal the real identity of the malicious vehicle for enhancing the efficiency of the VANET system. Merits of this scheme provides secure vehicular communication in Vehicular Ad Hoc Networks.

In [3] the author has discussed about Traffic Congestion Detection and Avoidance in Vehicular Ad Hoc Networks based on Congestion detection algorithms are to detect areas of high traffic density with low speeds and also it will suggest optimal path to the vehicles in that particular region. The advantage of this algorithm is to timing saving purpose.

In [4] the author has discussed about XOR-Forwarding for Wireless Networks based on localized network coding-based packet forwarding protocol for wireless networks and the advantage is the network throughput about 139% as compared to the classical unicast forwarding.

In [5] the author has discussed about a cooperative approach to traffic congestion detection with complex event processing in Vehicular Ad Hoc Networks , this paper uses event-driven architecture (EDA) as a novel mechanism to get insight into VANET messages to detect different levels of traffic Jams. The advantages is it can detect different types of traffic congestion on a road.

In [6] the author has discussed about A Hybrid Approach for Efficient Privacy-Preserving Authentication in Vehicular Ad Hoc Networks based on light-weight pseudonym with trapdoor mechanism that eliminates the need of CRL that will reduce packet loss.

In [7] the author has discussed about An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme for Vehicular Ad Hoc Networks, the mechanism used is conditional privacy-preserving authentication (CPPA) scheme without using bilinear pairing to enhance secure communication in Vehicular Ad Hoc Networks. The advantage of this paper is it will reduce the computational complexity of information processing in VANET and this mechanism also support both mutual authentication and privacy protection simultaneously.

In [8] the author has discussed about A Distributed Vehicular Traffic Re-Routing System for Congestion Avoidance is re-routing process for vehicles and this method is a hybrid system because it uses both server and Internet communication to determine an accurate global view of the traffic. The advantage of this hybrid system is it increases the user privacy by 92 percent on average.

In [9] the author has discussed about Applications of VANETs: Present & Future. In this paper they had explained about various possible applications of vehicular network, along with its features. This paper explained elaborately about vehicular network application such as Safety oriented, Commercial oriented, Convenience oriented and Productive Applications.

In [10] the author has discussed about Anonymity Analysis on Social Spot Based Pseudonym Changing for Location Privacy in VANETs. This paper focus on location privacy of a vehicles to achieve this they had used a technique called social spot based pseudonyms changing technique which gives an efficient result when compared to the old techniques.

In [11] the author has discussed about Security in vehicular ad-hoc network. In this paper they focused on giving techniques for security service and preserving driver's privacy. And also they focused on two fundamental issues such as certificate revocation and conditional privacy preservation, both are considered the most challenging design goals in vehicular ad hoc networks. Vehicular communication networking is a promising approach to facilitating road safety, traffic management, and infotainment transmissions for drivers and passengers. One of the main objective in the design of this networking is to avoid various malicious activities and security attacks.

In [12] the author has discussed about Comprehensive survey on security services in vehicular ad-hoc networks which is a survey of security issues in VANET. Because VANET is platform which is more prone to many security attacks. In this paper they had given the overview and characteristics of the security in Vehicular ad hoc networks. This paper had discussed about possible security attacks on security services like availability, confidentiality, authentication, integrity and non-repudiation and their corresponding solutions to make VANET communications more secure.

In [13] the author has discussed about Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks. In this paper, the author discussed on providing some security related premium schemes through internet for passenger as well as drivers. Because, security is the major issue in Vehicular ad hoc network by introducing a Trusted Authority (TA). This paper used a mechanism called dual authentication scheme to provide a high level of security to enhance security in Vehicular ad hoc network. The merits of this dual authentication and key management scheme is computationally efficient compared with all other existing schemes.

In [14] the author has discussed about D2D for Intelligent Transportation Systems: A Feasibility Study. In this paper, they had addressed the feasibility study for device to device communication (D2D). And also they focused on dynamic spectrum management problem due to vehicular-to-vehicular and vehicular-to-infrastructure communications. This paper provided some solution for the problem faced by the above technology.

In [15] the author has discussed about Electrified Vehicles and the Smart Grid: The ITS Perspective. This paper focused on Vehicle electrification is envisioned to be a significant component of the upcoming smart grid. In this paper, a smart grid vision of the electric vehicles for the next 30 years and beyond is presented from six perspectives related to intelligent transportation systems: 1) vehicles; 2) infrastructure; 3) travelers; 4) systems, operations, and scenarios; 5) communications; and 6) social, economic, and political.

In [16] the author has discussed about Computationally Efficient Privacy Preserving Anonymous Authentication Scheme for Vehicular Ad Hoc Networks. This paper introduced a new mechanism called anonymous mutual authentication mechanism which more efficient than the other schemes. The advantage of this scheme is, it reduced computation cost in the certificate revocation list (CRL) checking process and in the certificate and the signature verification process, and also it reduced message loss. This scheme efficiently checks large number of messages.

III. METHODOLOGY

The main objectives of the project is to avoid malicious vehicles entering into the VANET and to avoid traffic congestion by suggesting optimal path to vehicles. In VANETs, each vehicle is outfitted with an on-board unit (OBU) which allows it to communicate with more vehicles and this kind of communication is vehicle-to-vehicle (V2V) communication. In vehicular ad-hoc networks, vehicles repeatedly transfer a security message called beacon with their neighbors. The beacon message generally carries information on the state of vehicle such as position of vehicle, velocity, emergency reporting, collision warning, lane change assistance, and other safety-related information. A misuse of these information may lead to a hazardous situations and therefore, vehicle authentication is a necessary requirement. Hence, effective safety applications equipped on the vehicle can constantly trace the state of the vehicles in their proximity, and help drivers avoid hazardous situations through notifications or mechanical reactions [9]. Moreover, the vehicles can also communicate with roadside units (RSUs), which is called as vehicle-to-RSU (V2R) communication [10], [11]. In addition, the Anonymous Authentication of Vehicles and RSU module offers a conditional tracing mechanism to trace the malicious vehicles or roadside units that abuse the VANET. As a result, the privacy of malicious vehicles will be revoked in order to provide conditional privacy in a computationally efficient way through which the VANET entities will be anonymous to each other until they are revoked from the VANET system. The main objectives behind the development of congestion detection algorithms are to identify areas of high traffic density with low speeds. Collision avoidance systems are designed to identify a traffic incident in real-time and rapidly pass on this message to adjacent vehicles to prevent a traffic collision. The best suitable method for Traffic Congestion Avoidance is to identify the Traffic Congestion areas and provide the details to other vehicles coming on the same tracks. We can avoid traffic congestion by suggesting optimal path to vehicles [3].

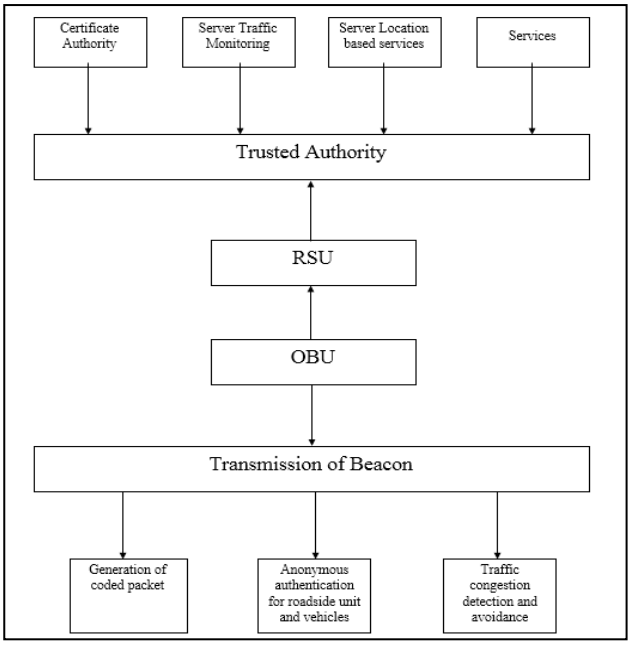

Figure 1. System Architecture

A. Generation of coded packets

This module generates coded packets allowing more receivers to acquire beacons useful for avoiding impending dangerous situations. Specifically, loss recovery should be achieved within the short lifetime of beacons (i.e., 100ms) since information contained in beacon messages is valid only within the lifetime, in repetition-based retransmission schemes, the transmission of the same beacon message is repeatedly transmitted several times by the sender within a short period of time, in order to allow neighbouring vehicles to have multiple chances to recover the lost packet in time. In order to reduce the number of retransmissions significant for loss recovery, two beacon packets are merged into a single XOR-ed packet which is also known as coded packet and each vehicle broadcasts the coded packet rather than broadcasting each packet individually. The covered area of a particular sender *BO* (Beacon Originator) can be divided into four regions the area is first divided into two parts by the centre line, and each part is further divided into two regions by the line through *BO* that is perpendicular to the centre line, the vehicles above the centre line move in a rightward direction and vehicles below the centre line move in a leftward direction. Note that vehicles within the *TargetRegions* are called target vehicles. Beacon Originator can efficiently produce a coded packet profitable to vehicles within the Target Regions. Given target regions, a sender should generate a coded packet useful to as many target vehicles as possible in order to minimize the coding overhead, to achieve this goal, a sender assigns a score to each of beacons it holds, and it finally selects the most appropriate two beacons based on the scores of beacons [1]. This module allows a sender to assign a higher score to a beacon *b* and the lower score is assigned to *b*. If a sender recognize which beacons each neighbor maintains, it can accurately compute the scores of beacons.

B. Anonymous Authentication of Vehicles and RSU

Due to the open-medium nature of these communications, it is significant to give fundamental security requirements such as authentication and privacy in an anonymous manner. Unless proper security measures are taken, the VANET users may potentially be vulnerable to a number of attacks, namely, bogus information attack, impersonation attack and RSU replication attack, Identity Revealing Attack, Masquerading, Key and/or Certificate Replication Attack, Forgery Attack etc [12]. Authentication is considered to be the first line of defense against malicious vehicles and messages [13]. If authentication is not given, a malicious vehicle may impersonate as an emergency vehicle to exceed speed limits without being permitted, if message integrity is not provided, a malicious vehicle could change the content of a message that is sent by the legitimate vehicle user or a legitimate RSU [2]. By doing so, the genuine user would be made responsible for the damage caused. Moreover, if an anonymous vehicle in the VANET system turns malicious, then its privacy should be revoked by the Trusted Authority (TA) and revealed to other vehicles, so that it can no longer be anonymous to protect the performance of the system and then the revoked identity is placed in the identity revocation list (IRL) which is maintained by the TA [2]. This scheme not only provides the anonymous authentication with low certificate and signature verification costs which are essentially required in the VANET applications, but also able to provide an efficient conditional privacy tracking mechanism to reveal the real identity of the malicious vehicle for enhancing the efficiency of the VANET system [2].

C. Traffic Congestion Avoidance

The best suitable method for Traffic Congestion Avoidance is to identify the Traffic Congestion areas and provide the details to more vehicles coming on the same path. Collision avoidance systems are designed to detect a traffic incident in real-time and quickly pass on this information to nearby vehicles to prevent a traffic collision [3]. Steps to detect traffic congestion area: 1) Check if the current speed of the vehicle is less than the minimum speed then declare SelfCongestion. 2) For each road block assign road vehicle counter as 0. 3) Identify the threshold value of no of vehicles for each road block. 4) Check the CongestionStatus from neighboring vehicles if the neighboring vehicles detect congestion then set Congestion Status as True. 5) Find the Total number of vehicles who detect congestion, if Total Congestion is grater then Thresholdvalue then declare total area as a congestion Area. 6) OBU will broadcast the congestion detected message with CongestionArea, Congestion Time, Congestion Affect No of Vehicle, Approximate Congestion Release Time. 7) Whenever CA enters in the range of Signal Agent (SA), CA send the details of Car ID (CID), Current Position (CP), Current Speed (CS), Maximum Speed (MS), Number of Neighbor CA (NCA), Road Block ID (RBID) to SA and if CA enters in the range of SA, counter will be incremented by one and if CA goes out of the range of SA, counter will be decrement by one.

IV. CONCLUSION

Proposed to increase the reliability of beacon transmission by allocating high priority to the beacons of the vehicles belonging to the coding region, the beacons from the front vehicle have more chances to be delivered to rearward. This approach is also effective in reducing coding overhead because there is a high probability that one of the two beacons used for network coding has been received from the opposite coding region. An RSU can effectively authenticate vehicles in an anonymous manner before providing beacon messages to vehicles. Similarly, vehicles can also authenticate an RSU in an anonymous manner before receiving beacon messages from RSUs provide an efficient conditional privacy tracking mechanism to detect and also to reveal the real identity of the malicious vehicle for increasing the efficiency of the VANET system. Vehicles and RSUs, which can do the communication with each other. RSU gathers traffic information from vehicles traversing through the given road segment and can suggest optimal path to other Vehicles.

V. REFERENCES

[1] Hyunwoo Kang1, Hongseok Yoo,Dongkyun Kim, And Yun-Su Chung1 Cancore : Context-Aware Network Coded Repetition For Vanets *10.1109/Access.2017.2681804.*

[2] Maria Azees, Pandi Vijayakumar, and Lazarus Jegatha Deboarh Eaap: Efficient Anonymous Authentication with Conditional Privacy-Preserving Scheme for Vehicular Ad Hoc Networks. Ieee Transactions On Intelligent Transportation Systems November 26, 2016.

[3] Dhaval Khatri Professor Dushyantsingh Rathod Professor.Ashish A. Gajjar Dr.Samrat Khanna Traffic Congestion Detection And Avoidance In Vanet International Journal For Scientific Research & Development| Vol. 2, Issue 03, 2014.

[4] Hsiang-Po Wang, Yi-Ta Chuang, Chih-Wei Yi, Yu-Chee Tseng And Pin-Chuan Liu Xor-Forwarding For Wireless .Global Telecommunication conference, 2009. Globe commmunication 2009. IEEE,Issues 04 March 2010.

[5] Fernando Terroso-Sáenz, Mercedes Valdés-Vela, Cristina Sotomayor-Martínez, RafaelToledo-Moreo, And Antonio F. Gómez-Skarmeta A Cooperative Approach To Traffic Congestion Detection With Complex Event Processing And Vanet IEEE Transactions On Intelligent Transportation Systems, Vol. 13, No. 2, June 2016.

[6] Ubaidullah Rajput, Fizza Abbas, Hasoo Eun, And Heekuck Oh A Hybrid Approach For Efficient Privacy-Preserving Authentication In Vanet IEEE Transactions July 17, 2017.

[7] Debiao He, Sherali Zeadally, Baowen Xu And Xinyi Huang An Efficient Identity-Based Conditional Privacy-Preserving Authentication Scheme For Vehicular Ad-Hoc Networks IEEE Transactions On Information Forensics And Security July 17,2015.

[8] Juan (Susan) Pan, Iulian Sandu Popa, And Cristian Borcea Divert: A Distributed Vehicular Traffic Re-Routing System For Congestion Avoidance IEEE Transactions On Mobile Computing 1536-1233 (C) 2015 IEEE.

[9] V. Kumar, S. Mishra, and N. Chand,``Applications of VANETs:Present & Future," *Commun. Netw. Sci. Res.*, vol. 5, no. 1, pp. 12_15, 2013.

[10] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Anonymity analysis on social spot based pseudonym changing for location privacy in VANETs," in *Proc. IEEE ICC*, Kyoto, Japan, Jun. 2011, pp. 1–5.

[11] X. Lin, R. Lu, C. Zhang, H. Zhu, P. H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *IEEE Commun. Mag.*, vol. 46, no. 4, pp. 88–95, Apr. 2008.

[12] M. Azees, P. Vijayakumar, and L. J. Deborah, "Comprehensive surveyon security services in vehicular *ad-hoc* networks," *IET Intell. Trans. Syst.*, vol. 10, no. 6, pp. 379–388, 2016, doi: 10.1049/iet-its.2015.0072.

[13] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1015–1028, Apr. 2016.

[14] X. Cheng, L. Yang, and X. Shen, "D2D for intelligent transportation systems: A feasibility study," *IEEE Trans. Intell. Trans. Syst.*, vol. 16, no. 4, pp. 1784–1793, Jan. 2015.

[15] X. Cheng *et al.*, "Electrified vehicles and the smart grid: The ITS perspective," *IEEE Trans. Intell. Transp. Syst.*, vol. 15, no. 4,
pp. 1388–1404, Aug. 2014.

[16] P. Vijayakumar, M. Azees, and L. J. Deborah, "CPAV: Computationally efficient privacy preserving anonymous authentication scheme for vehicular ad hoc networks," in *Proc. 2nd IEEE Int. Conf. Cyber Secur. Cloud Comput. (CSCloud)*, New York, NY, USA, Nov. 2015,
pp. 62–67.

Author Biography

Dr. P. Boobalan, Associate Professor, Pondicherry Engineering College, working in the field of optical networks, Member of ISTE, 24 years of teaching experience, published 15 papers in International / National Conferences / Journals, Co-ordinated and conducted many workshops.

B. Nivetha pursuing B.Tech degree in the Department of Information Technology in Pondicherry Engineering College.

S. Saieswari Goliate pursuing B.Tech degree in the Department of Information Technology in Pondicherry Engineering College.

S. Sharmila pursuing B.Tech degree in the Department of Information Technology in Pondicherry Engineering College.