International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325
Volume3, Issue 8 (August '2017)

AUTHENTICATION FRAMEWORK WITH DELAY-TOLERANT DATA TRAFFIC TO VANET

M.Meena,
M.Phil Scholar,
Department of Computer Science,
PRIST University,
Thanjavur,Tamilnadu,India.

T. Karunakaran,
Assistant Professor,
Department of Computer Science,
PRIST University,
Thanjavur,Tamilnadu,India.

Abstract: Research focus on reducing the computational complexity, delay-tolerant using with partially observable Markov decision process in vehicular networks. The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moves, cars as nodes in a network to create a mobile network with an aim of providing efficient and safe transportation. Connected vehicles and RSUs with embedded computing, storage, and positioning devices cooperate with each other and form a connected vehicle network. Current research on connected vehicle networks focuses on delivering the data generated from or, required by the vehicle networks themselves, of which the data traffic is light; thus, the vehicle-network resource utilization efficiency is low. On the other hand, a large amount of delay-tolerant traffic in other data networks consumes significant communication resources. Introduce a new architecture to utilize efficiently the potential resource for connecting vehicles and to mitigate the congestion problem in other data networks. An optimal distributed data hopping mechanism is also proposed to enable delay-tolerant data routing over connected vehicle networks. Research formulates the next-hop decision optimization problem as a partially observable Markov decision process (POMDP) and propose a heuristic algorithm to reduce computational complexity.

Keywords: Connected vehicle network, delay-tolerant data, partially observable Markov decision process (POMDP), traffic offloading.

I.INTRODUCTION

To fully utilize the wireless bandwidth provided by APs,we propose a representative-based prefetching mechanism, in which a set of representative APs are carefully selected and then share their prefetched data with others. The selection process explicitly takes into account the AP's storage capacity, storage status, inter-APs bandwidth and traffic loads on the backhaul links. We apply network coding in CCDSV to augment the distribution of shared contents. The selection of shared contents to be prefetched on an AP is based on the storage status of neighboring APs in the contact map in order to increase the information utility of each prefetched data piece. Through extensive simulations, CCDSV proves its effectiveness in vehicular content distribution under various scenarios.

Mobile Social Networks (MoSoNets) is a mobile communications system which involves the social relationship of the users. MoSoNets provides data delivery services exploring the social relationship among mobile users. Mobile Social Networks is a means of transmitting information (communicating) using a combination of voice and data devices over networks including cellular technology and elements of private and public IP infrastructure (such as the Internet). Presently Mobile Social Networks extensively used in online social networking applications, healthcare services, location based services, wearable services and in personal area networks.

II. LITERATURE SURVEY

Vehicular Sensor Networks (VSNs) [4] focus on the human driving experiences and traffic flow control systems. C. Zhang, R. Lu, X. Lin, P.-H. Ho and X. Shen employed a digital signature scheme that is widely recognized as the most effective approach for VSNs to achieve authentication, integrity, and validity. However, when the number of signatures received by a Roadside Unit (RSU) becomes large, a scalability problem emerges immediately, where the RSU could be difficult to sequentially verify each received signature within 300 ms interval according to the current Dedicated Short Range Communications (DSRC) broadcast protocol. An efficient batch signature verification scheme for communications between vehicles and RSUs (or termed vehicle- to-Infrastructure (V2I) communications) was adopted, in which an RSU can verify multiple received signatures at the same time such that the total verification time can be reduced. A novel RSU- aided message authentication scheme

[5] was presented in the year 2008 by C. Zhang to reduce the communication overhead imposed by the previous paper. When the traffic density becomes larger, a vehicle cannot verify all signatures of the messages sent by its neighbours in a timely manner, which results in message loss. A novel RSUaided messages authentication scheme, called RAISE was introduced. With RAISE, roadside units (RSUs) are responsible for verifying the authenticity of the messages sent from vehicles and for notifying the results back to vehicles. In VANETs, vehicles are equipped with wireless on-broad units (OBUs), which communicate with each other or with roadside units (RSUs) with a dedicated short range communications (DSRC) protocol. According to DSRC, each vehicle periodically broadcast its routine traffic-related information containing its current speed, location, deceleration/acceleration, etc. With the received information,

other drivers can make an early response in case of exceptional situations such as accidents, emergent braking, and traffic jams. RAISE explores the unique features of VANETs by employing RSUs to assist vehicles in authenticating messages. Each IVC message will be attached with a short keyed hash message authentication (HMAC) code generated by the vehicle, and the corresponding RSU in the range will verify these HMACs and disseminate the notice of authenticity to each vehicle. Compared to the previous paper, with the implementation of RAISE, communication overhead is reduced and deals with scalability issue too. With the key chain commitments distributed by RSUs, a vehicle can effectively authenticate any received message from vehicles nearby even in the presence of frequent group membership fluctuation. Compared with previously reported public key infrastructure (PKI)- based packet authentication protocols for security and privacy, the communication overhead and computation cost of the proposed protocol are significantly reduced due to the adoption of a short message authentication code (MAC) tag attached in each packet for the packet source authentication and packet integrity check.

.

III.PROBLEM STATEMENT

VANETs are utilized for a broad range of safety applications, and non-safety applications (such as collision warnings, road navigation, traffic information and mobile infotainment). In VANETs, the user authentication is a crucial security service for access control in both inter-vehicle and vehicle-roadside communication. On the other hand, vehicles have to be protected from the misuse of their private data and the attacks on their privacy, meanwhile, be capable of being investigated from accidents or liabilities for non-repudiation. Peculiarly, safety applications require a strong mutual authentication, because most of the safety- related messages may contain life-critical information. Therefore The research, along with the development of the VANET technology based on advancing smart vehicles, and other undiscovered potential threats on security. To solving the issues of authentication with privacy preservation and non-repudiation in VANETs.

IV. EXISTING SYSTEM

The number of research work related to the authentication issue in VANETs, by applying symmetric or asymmetric key managements. The research work ACPN provides the conditional vehicle anonymity for privacy preservation with traceability for the non-repudiation, in case that malicious vehicles abuse anonymous authentication techniques to achieve malicious attacks. The public-key cryptography (PKC) to the pseudonym generation, which ensures a legitimate third party to achieve non-repudiation of vehicles by obtaining their real IDs. A PKC-based adaptive pseudonym scheme by using self-generated pseudonyms instead of real-world IDs in authentication for privacy preservation and non-repudiation, in which the update of the pseudonyms depends on vehicular demands. In ACPN, utilize the IBS scheme for the vehicle- to-roadside (V2R) authentication and the roadside-to-vehicle (R2V) authentication, which is efficient in communication. To reduce the computation overhead by IBS in authentication, the IBOOS scheme is used for the vehicle-to-vehicle (V2V) authentication. The feasibility of ACPN with respect to the system analysis on the objectives, such as authentication, privacy preservation, non-repudiation, time constraint, independency, availability and integration. Moreover, the storage and computation over-head of ACPN is evaluated by quantitative calculations in the performance evaluation.

Demerits:

- The disadvantage of using public key infrastructure (PKI) based authentication frameworks have been proposed, the system availability is still not pervasive or feasible, because such frameworks require additional communication to manage the vehicular certificates and the certificate revocation lists (CRLs) that may cause heavy communication and computation overheads.

V.PROPOSED METHOD

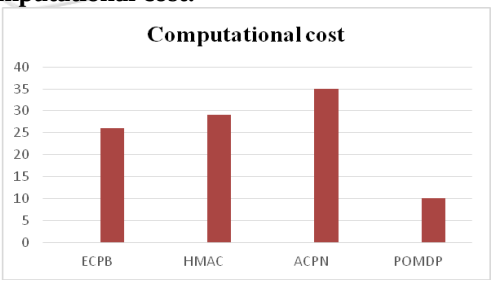
A QoS-aware traffic offloading scheme is proposed to allow the delivery of delay tolerant data over the connected vehicle networks, no matter whether the data are from/to the connected vehicle networks. Thus, more resources from other data networks with continuous connectivity and better QoS performance could be utilized for delay-sensitive traffic. This is a low cost solution to handle the data traffic explosion because no deployment of extra infrastructure or hardware is required. A distributed data hopping mechanism is proposed to facilitate delay-tolerant data routing over the connected vehicle networks. Communication resources in vehicle networks are efficiently utilized without affecting other data traffic, such as road safety and driver assistance.

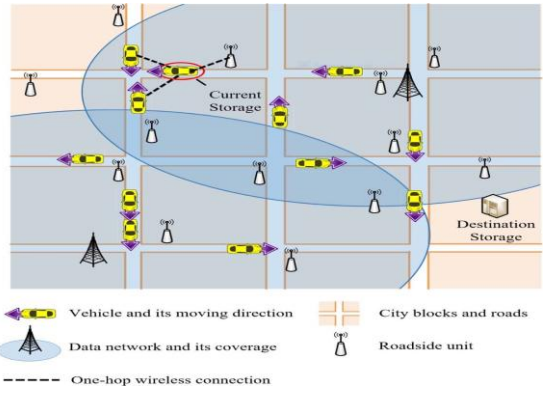
Merits:

- Provides the conditional vehicle anonymity for privacy preservation with traceability for the non-repudiation.
- Reduce the computational cost and avoid time delay to send the data.
- A partially observable Markov decision process (POMDP) and propose a heuristic algorithm to reduce computational complexity.

V. EXPERIMENTAL RESULT

Low computational cost:





VI.ALGORITHM

POMDP and Heuristic:

Sending process:

$k \leftarrow 1$;
while $k \leq K$ do
if $t_k \leq t \leq t_{k+1}$ then
for each $\psi \in \Psi_e$ do
Update the observation $o(k)$;
Calculate the optimal decision $a^*(k)$ based on $o(k)$ and other states; if $a^*(k) = 0$ then
Transmit the DB with ID ψ to the data network;
end if if $a^*(k) = 2$ then
Multicast the DB with ID ψ to the storage devices in $E'(k)$, with $E'(k)$ and ψenclosed; end if
if an ACK is received then Obtain ψ from the ACK; if$\psi' = \psi$ then
Remove the DB with ID ψ from the storage;
$k \leftarrow k + 1$;
Update t;

Receiving process:

while $t \leq t_K$ do

if a delay-tolerant DB is received then
Obtain $\mathscr{E}'(k)$ and ψ' from the DB; if$e \in \mathscr{E}'(k)$ then
Put the DB in the storage;
Multicast an ACK to the DB source and the storage devices in $E'(k)$, with$e$, $\mathscr{E}'(k)$ and ψ'enclosed;
if an ACK is received then
Obtain $\mathscr{E}'(k)$ and ψ' from the packet; if$e \in \mathscr{E}'(k)$ then
Stop receiving the DB with ID ψ; end if
end if
Update t;

VII. SYSTEM MODEL

Network Formation: When this module is to create the vehicle and it can create different no of access points for different location. Then it can form the one network to system These APs are characterized by short-range coverage (hundreds of meters), relatively cheap and easy deployment and high data access rate.

Assign Neighbours: In one network the different no of access point can appear that access point distance and its range can add to calculate the maximum value.in which access points distance less than from maximum value that access point are assign from neighbour for itself to network

Accesspoint Allocation: When more access point are in the network in which access point is created to the network first that access point allocated to the vehicle access point. When vehicle move from the access point new access point allocated to the system

Host Server Updating: When the admin can update the road side information, traffic information, location information, to server database.the admin only have update permissions for the network

Download Information: When vehicle can request the location related data .that request send to access point when access point can forward request from the webservice.webservice can retrieve the data from database. then webservice response the request to access point .when ap can forward the data to the requested vehicle

VIII. CONCLUSION

The explosion of data traffic has brought serious congestion and delay problems to the current networks. To cope with this problem, they have proposed a new architecture, to utilize efficiently the spare network resource from connected vehicle networks for delay-tolerant data traffic delivery. With the architecture, delay-tolerant traffic is offloaded from the data networks to the connected vehicle networks, without extra infrastructure or hardware deployment. A distributed data-hopping mechanism was also proposed to enable delay-tolerant data routing over the connected vehicle networks. The hopping optimization problem was formulated as a POMDP to achieve optimized performance and tackle the problem of instable wireless connections. Extensive simulation results were presented to demonstrate the significant performance improvement of the proposed scheme.

Future Work: The future research, there is needed to build a generic architectural framework towards addressing these security and privacy issues/challenges in a holistic manner. Future research will sign and verifying protocol must be optimized to reduce the execution time. So everybody is warmly invited to provide a safe, secure and trusted environment to moving objects. The future will increase the security and throughput.

IX. REFERENCES

[1]. Jie Li; Huang Lu, "ACPN: A Novel Authentication Framework with Conditional Privacy-Preservation and Non-Repudiation for VANETs", IEEE Transactions on Parallel And Distributed Systems Year: 2016, Volume: 26, Issue: 4.
[2]. Gaurav Sharma, Maninder kaur, "A Review Paper On A Novel Cluster Based Approach For Preventing Dos Attack In Vanet", International Journal Of Technology And Computing (IJTC).
[3]. Sharvari G, H K Chandrashekar, "An Authenticated Way for Privacy Preservation to Enhance Network Lifetime for VANETS", International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-5, Issue-5).
[4]. P.Savitha, A. John Clement Sunder, M.Balapriya, "Enhanced ID based Message Authentication and Secure Navigation in VANET", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE).
[5]. Gauri Dudhat, Karuna Bagde, "Implementation of Authentication Framework for VANET with Conditional Privacy Preservation", International Journal of Computer Science and Mobile Computing.
[6]. R.Balamurugan, S.Kungumavathi, "Implementing a Billing Scheme with Fine Grained Distributed Access Control for Service Oriented Vehicular Networks",

International Journal of Innovative Research in Science, Engineering and Technology.

[7]. Dr.Sohan Kumar Gupta, "A Survey on Authentication Framework with Conditional Privacy Preservation and NON-repudiation for VANET's", International Journal of Combined Research & Development (IJCRD).

[8]. Yimin Wang, Hong Zhong, "ECPB: Efficient Conditional Privacy-Preserving Authentication Scheme Supporting Batch Verification for VANETs", International Journal of Network Security, Vol.18, No.2, PP.374-382.

[9]. R. Janani, P. Sathishkumar, "Supportive Data Scheduling and Broadcast through VANET using Batch Signature", South Asian Journal of Engineering and Technology Vol.2, No.17 (2016) 87–94.

