A Secure Mechanism for Content Distribution in Vehicular Ad-hoc Networks

Neeraja R[1], M. Jebakumari[2]

[1]Department of Computer Science and Engineering, Nehru Institute of Technology, Anna University Chennai, Kaliyapuram, Coimbatore – 641105, India
[2]Associate Professor, Department of Computer Science and Engineering, Nehru Institute of Technology, Anna University Chennai, Kaliyapuram, Coimbatore – 641105, India

Abstract: ***Content distribution through roadside Access Points (APs) has become indispensable for vehicular users to obtain good road safety. Cooperative Content Distribution System for Vehicles (CCDSV) operates upon a network of infrastructure APs to distribute contents to moving vehicles collaboratively. In this paper, a Cooperative Content Distribution System for Vehicles using cooperative APs in a hybrid structure called the contact map, that takes advantage of the roadside units (RSUs) that are connected to the Internet and providing various types of information to VANET users, is introduced. A new LMS (Live Multimedia Streaming) scheme using Symbol-level network coding (SLNC) mechanism to secure the system is also included.***

Keywords: Cooperative Content Distribution, Access Points, Security, Master Key Generation, Symbol-level network coding

1. Introduction

Vehicular Adhoc Networks (VANETs) aid vehicles to communicate with each other and with roadside units (RSUs).Content distribution to vehicular users via wireless network access shows potential service which is essential in assisting better road safety and enhancement of driving experience. Although the cellular network is basically accepted because of its omnipresent accessibility, it experiences an fiery growth of subscribers and the demands for multimedia contents seem to go beyond its capability limit. However the Wi-Fi-based Access Points (APs) have shown their probability in content distribution for vehicles. These APs can be either Roadside Units (RSUs) put up by network service providers or Hot-spots that are established in roadside shops or buildings and arranged for public access. In spite of the fact that these APs are eminent by short-range coverage they are comparatively cheaper and it is possible to have simple deployment and high data access rate. The general architecture of Wi-Fi-based vehicular content distribution system is made up of a network of interconnected APs, which are geologically set in positions near the roads, running the tailored protocols for collaboration. A Vehicular Ad hoc network is shown in fig.1.

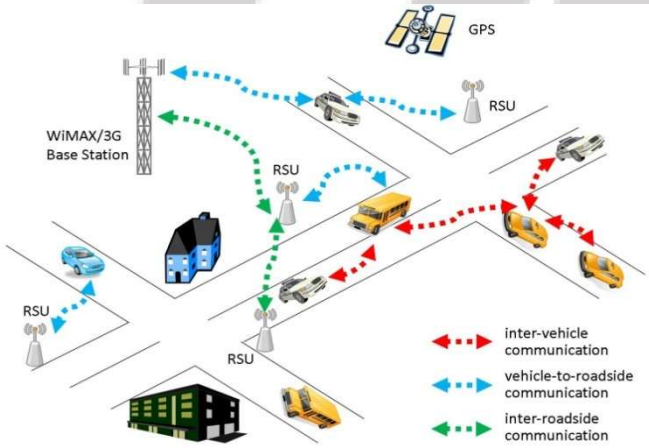

Figure 1: Vehicular Adhoc network

The APs can communicate with each other via backhaul links to the Internet. Data-origin servers are the content distributers, providing vehicular users with both the shared and private contents. However such network access schemes face many challenges on the system design for effective content distribution to vehicles restraining the data transfer opportunities. In order to resolve the various confronts in vehicular content distribution, several recent works accepted prefetching scheme, which is extensively helpful to computer structural design, web accessing, etc. The requested data is prefetched onto the APs ahead along the vehicle path that can then download the prefetched data with a high throughput when connection is expected, without resorting to the remote server or being delayed by the AP's backhaul link. Such techniques, on the contrary, demand careful design when it is applied to large-scale and real systems.

2. Related Works

In this section, quite a few important issues arising from the design of a prefetching system for vehicular content distribution are presented and the related works and their limitations are investigated. The content distribution systems based on prefetching require the mobility prediction component to predict the vehicular trajectory and the APs that will be connected by the vehicles shortly[1].Accordingly, the prediction accuracy directly affects the system performance, since false prediction would make the vehicle miss the prefetched data[2]. However the accuracy of mobility prediction is not easy to maintain at a high level and it varies mostly [5] especially under the highly dynamic vehicular environment [6]. Furthermore, the intelligent AP selection [7] which is based on the ever-changing metrics of APs such as signal strength, available wireless bandwidth etc. worsens such prediction accuracy when a vehicle is exposed to several surrounding APs [8]. Majority of the prior works have the design of prefetching component and mobility prediction component separately, not including the explicit consideration that whether the prefetching component can still work correctly under low-accuracy mobility predictions or not.

Yet, most of the related works assume unlimited storage resources. In [2], storage limitation is taken into consideration and the system uses a centralized content manager that periodically executes the content distribution algorithm to decide on the APs to cache parts of the requested files while satisfying the storage restraint. Due to the high vehicular speed and small AP coverage, the vehicular download process usually continues across multiple APs and thus it is common for the original multimedia content to be divided into multiple pieces and be stored along the specific Aps placed ahead [10]. A secure and efficient scheme with privacy preservation is proposed by Li et al. [11] where a vehicle needs to acquire a blind signature before it can access the desired services from the RSU in close proximity. A service provider (SP) verifies the validity of signatures. An RSU is made to sign and deliver messages to end users on behalf of Certificate Authority (CA) discussed in [13],. The CA obtains a secondary secret key from its private key and sends it to the RSU. The receiver verifies by checking both the correctness of the key signature and the location of the sender.

More recently, Symbol-level network coding (SLNC) was proposed by Katti et.al. [16], to improve unicast throughput in wireless mesh networks. It is inspired from the observation that in lossy wireless links, for a packet received with errors, some symbols of the packet are still likely to be received correctly. SLNC can gain benefits from both network coding and symbol-level diversity. A cooperative transmission scheme based on SLNC is proposed by Kim et.al. [17], to explore its use in the physical layer of multichannel wireless networks (such as WiMAX). It is shown in a recent work [18], that SLNC outperforms PLNC (Packet Level Network Coding) for content distribution in VANETs.

3. Vehicular Content Distribution

The proposed CCDSV is a prefetching system built upon cooperative APs for speeding up content distribution to vehicular users and efficiently utilizing the resource of storage and backhaul bandwidth on APs. This CCDSV provides the maximum vehicular download performance which is obtained from the APs while reducing as possible both the data and control traffic introduced into the set of APs. In addition, a special technique in constructing the contact map which is defined as an overlay structure on top of the network of APs and encoding the vehicle-AP contact patterns, in order to accurately predict the future contact APs and feed comprehensive information to the prefetching component is also implemented. A new representative-based prefetching strategy for upgrading the stability of the system performance in the occurrence of varied mobility prediction accuracy and at the same time, controlling the overhead incurred is used. The storage containing the prefetched contents and cached contents which coexist is managed efficiently. Additionally the metric, RankSum of the neighboring APs in the contact map for selecting the prefetch contents with the intention of augmenting the information utility under practical network coding is included The detailed descriptions of the techniques are covered in the following sections.

3.1 Contact map

Contact map is the structure on top of the APs network and it encodes the observed patterns of vehicle-AP contacts. Contact map is used for predicting a vehicle's potential contact AP(s) to the lead on the route and the respective transition probabilities to them. After predicting the APs and probabilities, the building blocks are formed for representative-AP selection. A table with three columns, [next ap, previous ap, probability] to represent the local view is used. A vehicle V is assumed to have sequentially contact three APs, ap_s, ap_i and ap_t. Through V's feedback, ap_i can observe the contact sequence (. . . , ap_s, ap_i, ap_t . . .) and then update the corresponding row of its local view table with a 2-tuple (ap_t, ap_s) update probability, if there exists a row with (next_ap, previous_ap) = (ap_t, ap_s); otherwise, add a new row. The corresponding probability of this row is calculated as

$$\text{Prob}\,(ap_i \rightarrow ap_t \,|ap_s) = \frac{N(ap_i \rightarrow ap_t|ap_s)}{N(ap_s \rightarrow ap_i)} \quad (1)$$

Where$N(ap_i \rightarrow ap_t\,|ap_s)$ is the number of times the tuple (ap_t, ap_s) has been observed (initially set to 1 if this tuple is first added) and $N(ap_s \rightarrow ap_i)$ is the sum of observation numbers of all the rows with previous_ap being ap_s. The prediction function at an AP (says api) returns a set of potential APs, R(i), to be contacted next and the respective transition probabilities Pi(j) for each apj ∈R(i). For vehicles which can provide the identity of the previous contact AP, say aps, the predicting AP api can directly make the prediction by querying its local view table with the keyword aps to obtain the results list. Otherwise, the prediction function of api will return all the APs in $NB^+(i)$ (here R(i) = $NB^+(i)$) with transition probability for each one as

$$P_i(x) = \Sigma\, P_i(x/y).\ \text{Prob}\,(ap_y \rightarrow ap_i) \quad (2)$$

With the aim of giving sufficient time for the APs ahead to complete the prefetching; it is sometimes not enough to consider the prefetching on the next-contact APs alone.

3.2 Representative-Based Prefetching Approach

The foremost goal of the Representative-based AP selection is to optimize the selection of a set of prefetching APs. In other words, the system can offer requesting vehicles with maximum gain in download performance. Actually there presentative-based approach groups the look ahead-APs into an overlay structure consisting of clusters with representative APs as cluster heads and client APs as cluster members. To enumerate the performance gain and loss, the metric vehicular download volume (VDV), i.e. the data volume a vehicle can download from the AP, is defined. After that D(i, j) is determined as the VDV at Api which fetches data from entity j (either the remote data-origin server or a representative AP) to satisfy the download request.

Prefetching for one vehicle can cause the replacement of some contents previously prefetched for other vehicles because of the predetermined storage capacity and thus risk degrading the overall performance in terms of VDV. Hence the storage management algorithm tries to expel a set of

prefetched objects with minimum loss in terms of VDV while facing insufficient storage space. Next the value for prefetch volume (PV), i.e., the size of the content to be prefetched is determined. The prefetch volume is upper bound by the vehicle-AP contact capacity (CC) which is the maximum data volume a vehicle in driving can download from an AP. Then the objective of maximizing the overall vehicular download volume into an optimization problem is formulated.

3.3 Network Coding

The APs prefetch data in units of pieces as the encoding is done at piece level. Capricious combination of pieces in network coding makes no piece in the same generation special or essential. The vehicle can recover the original generation as long as enough independent pieces are collected. Accordingly, it need not be considered whether specific pieces of one generation are prefetched on the APs but only need to determine how many pieces from each generation are prefetched, satisfying the constraint of total prefetch volume.

In fact, for the vehicle which triggers the prefetching, the process of content selection is simple: i.e. prefetching the pieces that are disjoint with the ones the requesting vehicle has collected already. A pair of pieces is “disjoint” then they are either independent piecein the same generation or belonging to different generations. However the prefetched data is expected to satisfy the demands of other vehicles passing by later with the aim of increasing the information utility of each of the prefetched content and saving on the system resources. Naturally, prefetching pieces from the generation with smaller RankSum would result in a lower probability that these prefetched pieces duplicate with other pieces stored in the locality.

4. Secure Mechanism for Content Distribution

The proposed technique allows the users to register with the RSUs online (through the Internet) before they initiate connection to the RSUs from their vehicle and after registration; the RSUs get a master key (Km) from a trusted authority (TA) for the user. The vehicle users get their Km the first time they connect to an RSU. A novel algorithm that uses the password of users to securely transfer their Km is the main part of secured mechanism. Km is used to encrypt the initial packet key, which is assigned to the user at the beginning of each session. Each RSU has a secure connection to a database server that stores the RSUs’ private information. Moreover, each RSU will be monitored by a TA, which, upon detecting a malicious behavior from the RSU, will isolate it from the network by informing other RSUs, which consecutively inform vehicles that are being connected to them. RSUs and Vehicles exchange messages using unicast when they are within direct range depending on the network-layer routing protocol. An efficient routing protocol transfers messages between a vehicle and an RSU (and vice versa) through other vehicles in a reliable manner.

5. Symbol Level Network Coding (SLNC)

Since compared with conventional packet-level network coding (PLNC), Symbol-level network coding (SLNC) performs network coding on smaller symbols, which refers to a group of consecutive bits within a packet, it is used. By recovering correctly received symbols from erroneous packets, SLNC reduces the impact of lossy links and packet collisions. By improving the utility of each transmission it also reduces the total number of transmissions.

6. Experimental Results

The proposed mechanism is implemented in NS2 simulator and the communication between APs and vehicles and between vehicles is shown in the screen shots of figures2 and 3 respectively.

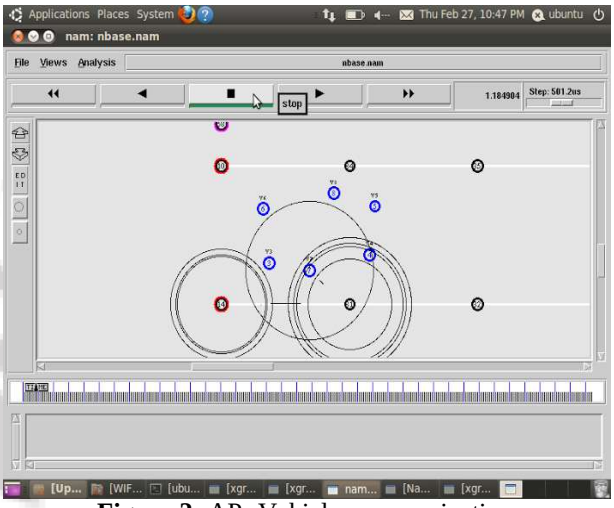

Figure 2: AP -Vehicle communication

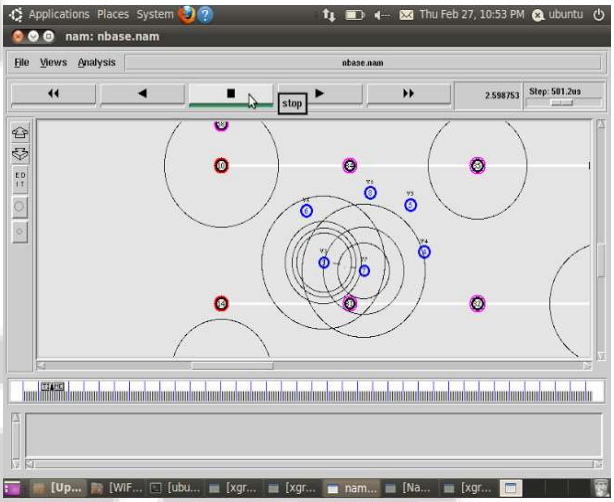

Figure 3: Vehicle-vehicle communication

As a promising scenario, a highway with bidirectional traffic is considered. At one end of the road, an AP is deployed, which continuously broadcasts contents about its local traffic condition to all the vehicles driving towards it for providing intelligent navigation. The performance of the system is evaluated by using parameters such as downloading rate and backhaul traffic.

Download rate is the average download throughput (in Kbps) perceived by vehicular users driving across the deployed APs. The graph in figure 4 gives the downloading rate comparison between the existing and proposed system. It is well observed that the proposed system has high download rate compared to the existing system.

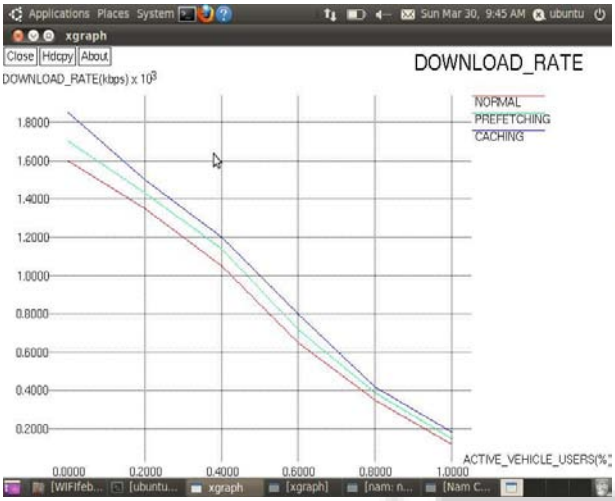

Figure 4: Comparison of download rate

Backhaul traffic is defined as the average data amount per second (in Kbps) flowing into each AP through backhaul link during the simulation. Backhaul traffic introduced by prefetching service is expected to be as low as possible to avoid overloading the APs and the saved bandwidth can be exploited to include more data services. The following graph of figure 5 gives the Backhaul traffic comparison between the existing and proposed system. In this graph, x axis represents active vehicle users (%) and y axis, the Backhaul traffic (kpbs). The proposed system has low Backhaul traffic compared to the existing system.

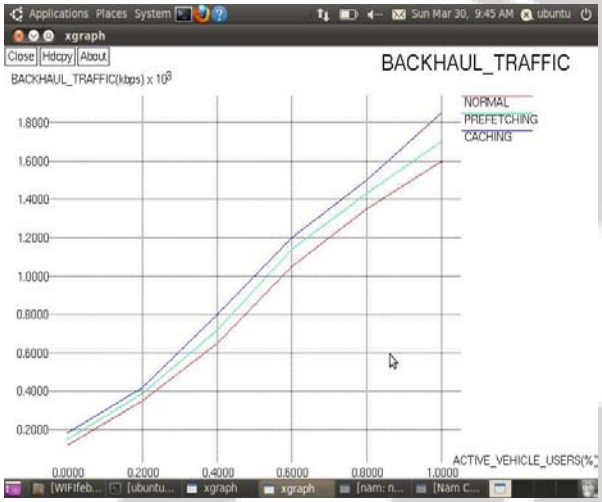

Figure 5: Comparison of Backhaul traffic

7. Conclusion

In this paper, a cooperative content distribution system for vehicles (CCDSV) through infrastructure APs is presented to achieve efficient cooperation among the network of APs so that vehicular users can effectively utilize the opportunistically encountered and short-lived AP connections. A structure called contact map is maintained distributedly on top of the APs, learning and predicting the potential vehicle-AP contacts. With the representative-based scheme, CCDSV carefully selects the ones from the predicted set of look ahead APs to perform prefetching so that overloading AP's backhaul link and ejecting the prefetched/cached data is avoided. In addition, an efficient mechanism to provide security for vehicular content distribution and privacy to the vehicular user is included.

References

[1] P. Deshpande, A. Kashyap, C. Sung, and S. Das, "Predictive Methods for Improved Vehicular Wi-Fi Access," Proc. Seventh Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), pp. 263- 276, 2009.

[2] Y. Huang, Y. Gao, K. Nahrstedt and W. He, "Optimizing File Retrieval in Delay-Tolerant Content Distribution Community," Proc. IEEE 29th Int'l Conf. Distributed Computing Systems (ICDCS), pp. 308-316, 2009.

[3] B. Chen and M. Chan, "MobTorrent: A Framework for Mobile Internet Access from Vehicles," Proc. IEEE INFOCOM, pp. 1404- 1412, 2009.

[4] U. Shevade, Y.-C. Chen, L. Qiu, Y. Zhang, V. Chandar, M.K. Han, H.H. Song, and Y. Seung, "Enabling High-Bandwidth Vehicular Content Distribution," Proc. ACM Int'l Conf. Emerging Networking EXperiments and Technologies (CoNEXT), pp. 23:1-23:12, 2010.

[5] A.J. Nicholson and B.D. Noble, "Breadcrumbs: Forecasting Mobile Connectivity," Proc. ACM MobiCom, pp. 46-57, 2008.

[6] L. Song D. Kotz, R. Jain, X. He "Evaluating Location Predictors with Extensive Wi-Fi Mobility Data" Proc. IEEE INFOCOM, vol. 2, pp. 1414-1424, 2004.

[7] A.J. Nicholson, Y. Chawathe, M.Y. Chen, B.D. Noble, and D. Wetherall, "Improved Access Point Selection," Proc. Fourth Int'l Conf. Mobile Systems, Applications and Services (MobiSys '06), pp. 233-245, 2006.

[8] J. Pang, B. Greenstein, M. Kaminsky, D. McCoy, and S. Seshan, "Wifi-Reports: Improving Wireless Network Selection with Collaboration," Proc. Seventh Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '09), pp. 123-136, 2009.

[9] A. Balasubramanian, B.N. Levine, and A. Venkataramani, "Enhancing Interactive Web Applications in Hybrid Networks," Proc. ACM MobiCom, pp. 70-80, 2008.

[10] M. Fiore and J. Barcelo-Ordinas, "Cooperative Download in Urban Vehicular Networks," Proc. IEEE Sixth Int'l Conf. Mobile Adhoc and Sensor Systems (MASS '09), pp. 20-29, 2009.

[11] C. T. Li, M. S. Hwang, and Y. P. Chu, "A secure and efficient communication scheme with authenticated key establishment and privacy preserving for vehicular ad hoc networks," Comput. Commun, vol. 31, no. 12, pp. 2803–2814, Jul. 2008.

[12] J. L. Huang, L. Y. Yeh, and H. Y. Chien, "ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 60, no. 1, pp. 248–262, Jan. 2011.

[13] S. Biswas, J. Misic, and V. Misic, "ID-based safety message authentication for security and trust in vehicular networks," in Proc. 31st ICDCSW, Minneapolis, MN, Jun. 2011, pp. 323–331.

[14] P. Bucciol, E. Masala, N. Kawaguchi, K. Takeda, and J. De Martin, "Performance evaluation of h. 264 video streaming over inter-vehicular 802.11 ad hoc networks," in Proc. 2005 PIMRC, pp. 1936–1940.

[15] M. Bonuccelli, G. Giunta, F. Lonetti, and F. Martelli, "Real-time video transmission in vehicular networks," in Proc. 2007 Mobile Networking for Vehicular Environments, pp. 115–120.

[16] R. Kim, J. Jin, and B. Li, "Drizzle: cooperative symbol-level network coding in multichannel wireless networks," IEEE Trans. Veh. Technol., vol. 59, no. 3, pp. 1415–1432, Mar. 2010.
[17] M. Li, Z. Yang, and W. Lou, "Codeon: cooperative popular content distribution for vehicular networks using symbol level network coding," accepted by IEEE J. Sel. Areas Commun., 2010.

Author Profile

Neeraja R received the B.Tech degree in Computer Science and Engineering from Mount Zion College of Engineering Pathanamthitta in 2011 under Mahatma Gandhi University Kottayam, Kerala. She is pursuing her M.E. in Computer Science and Engineering from Nehru Institute of Technology Coimbatore under Anna University Chennai.