Securing Peer to Peer Content Distribution Network based on Network Coding in VANETs

Chirag Suryakant Thaker
Dept. of Computer Engg.
L. D. College of Engineering
Gujarat, India

Ati Shirishkumar Garg
Dept. of Computer Science
Rollwala Computer Center
Gujarat , India

Nashifa Mohmadshafi Shaikh
Dept. of Computer Science
Rollwala Computer Center
Gujarat, India

ABSTRACT

In past few years, Vehicular Ad-Hoc Network (VANET) has seen advances in research. Content sharing through vehicle-to-vehicle communication can help people find their interested content on the road. VANETs allow peer-to-peer content distribution of data items such as traffic information, audio, video and other such information. Reliability, security and fast communication are the dire need for today’s technology used in VANETs for inter-vehicular communication. In this paper a model is proposed which satisfies the above mentioned parameters. The proposed mechanism uses network coding for reliability and homomorphic hash function for security. A reliability bit is also included. It is set for safety messages to make delivery of safety messages reliable while it is not set for comfort messages.

Keywords

VANET, Network Coding, Homomorphic hash function

1. INTRODUCTION

Last few decades have speculated a significant growth in mobile technology. Its offers portable, real-time communication, and information access in a cost effective style. This encompasses a broad spectrum of applications. Recently, wireless communication has enhanced its vision to support communication between vehicles and roadside access point or other vehicles. Nonetheless there are many problems yet to be addressed. Vehicular networks have to face highly dynamic mobility patterns which are a distinct challenge. Considering vehicle communications, service can be provided employing two types of network topologies: vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) [1]. Fig. 1 shows the placement of components of VANET and architecture formed. The former topology, V2I, suggests that on-board services must have connection with the infrastructure employed along the roadside. Electronic fee collection is an example of V2I communications that uses DSRC (Dedicated Short Range Communications). DSRC helps keeping record of the path traversed by the driver, thus charging drivers automatically, as per the road and vehicle criteria. Other technologies used for V2I systems are infrared and Wi-fi. The latter V2V services extend technologies based on ad hoc networks applied to vehicular field. Because of rapid change in topology due to vehicle motion, the vehicular network closely resembles an ad hoc network. V2V doesn’t require a pre-defined infrastructure; hence it has become focal point of attraction for the researchers recently. In V2V communication is carried out on confined number of vehicles acting as sensors for transmitting data and informing each other about the unusual and hazardous accidents.

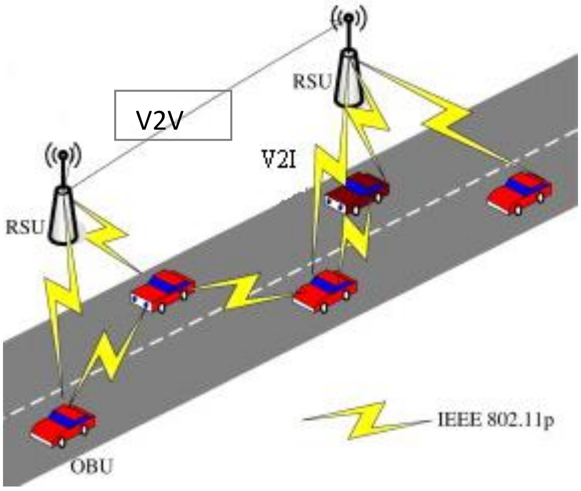

Fig 1: Infrastructure and components of VANETs

Increasing road safety is the primary concern of VANETs. It can save lives and improve traffic flow. In 1999, the U.S. Federal Communication Commission allocated 75MHz of Dedicated Short Range Communications (DSRC) spectrum at 5.9 GHz to be used exclusively for vehicle-to-vehicle and vehicle-to-infrastructure communications. IEEE 802.11p, also known as Wireless Access in Vehicular Environment (WAVE) is a draft amendment to the IEEE 802.11 standard that adds applications to fast changing vehicular networks [2], [3]. A complete communications system for WAVE needs to include support for multi-channel operations, security, and other upper layer operations.

Mainly VANETs constitute of the following two units: On Board Units (OBU) and Roadside units (RSU) [4]. OBU is one of VANET components. It makes the communication between vehicles and infrastructure and other vehicles possible. While, RSU is a communication device installed on the road side. RSU sends such as traffic information, authentication messages, multimedia messages, and etc.

The services of VANETs now have entered different dimensions. The messages transmitted in vehicular network can be categorized as comfort messages and safety messages [5]. Comfort messages are there to enhance the coziness of the passengers. Examples for this category are: traffic information system, weather information, gas station or restaurant location and price information, and interactive communication such as Internet access or music download. In the latter case, safety messages make driving safer by communication. Example applications of this class are: emergency warning system, lane-changing assistant, intersection coordination, traffic sign/signal violation warning, and road-condition warning. Applications of this class usually demand direct vehicle-to-vehicle communication due to the stringent delay requirements.

Due to highly dynamic nature of the underlying vehicular network topology, inefficiency is observed in content distribution. We will be concentrating on improvement of reliability and security parameters while transmitting data. The main idea is to use homomorphic hash function with the combination of network coding. In order to save compute cycles, type of message will be taken into consideration before applying the suggested mechanisms.

The rest of this paper is organized as follows: Section II presents the related work done in the field of VANETs. Proceeding to Section III we discuss problems that will be focused on in the inter-vehicular communication environment. A model is proposed alleviating the reliability and security issue in section IV. Finally in section V we conclude our paper.

2. RELATED WORK

There has been much research on content distribution in vehicular ad hoc networks.

Network coding (NC) [6], [13] is an efficient way of dissemination of data in wireless network. It makes best use of the available network resources by encoding several packets received from intermediate nodes. It increases throughput and robustness of network, thus making it more reliable. Nevertheless, pure NC can be applied in a network where topology is fixed. Hence, emergence of random network coding (RNC) was witnessed. It enables the use of NC in wireless networks where nodes move autonomously. Ho et al. showed that random selection of coefficients for linear codes over Gaussian Field (GF) improves the capacity of networks.

Cooperative content distribution system is a mechanism based on network coding proposed by D Zhang [7]. Network coding is used for efficient distribution of encoded data, where popular data is shared among nodes. Vehicle’s access point is predicted before vehicle arrives at that point. This is an adept method where traffic load is low and high delivery throughput is required. Drawback of this method is that it requires an established infrastructure of wi-fi access points, which require huge amount of investment for its setup. These access points must be fed with structure of contact map to predict potential vehicle access point contacts. This mechanism doesn’t consider security which is essential to guard against malicious nodes.

Atushi proposed a scheme, infocast [8], [12], based on rateless codes for collaborative content distribution for road side units to vehicular network. Rateless encoding is and end-to-end coding which allows only source to encode. Achievable delivery ratio of rateless coding is less than network coding and is not well-suited for random topology. NC can achieve high reliability saving network resources. Also it requires fixture of RSU which lead to large investment in deployment. The problem of security is still prevailing which may lead to corruption of data being transmitted.

Bayrack proposed a Secure and Privacy protecting protocol which is a PKI-based protocol [9]. Asymmetric cryptography is achieved by public/private key pair allotted to each entity. This mechanism requires a central trusted authority to generate authentic certificate for each entity. This scheme when applied to VANETs has a number of limitations, including complexity in certificate verification and management, scalability, performance in a large-scale environment, and timely access to certificate revocation information.

3. PROBLEMS IN FOCUS

To successfully deploy service-oriented vehicular network many parameters have to be taken into account. When considering VANETs a large number of challenges are hypothesized. The prime concern in VANETs is reliability. While transmitting data if any node leaves the topology, due to slow or high speed of node compared to other nodes in the topology, or gets disconnected, due to link failure or other reasons, receiving node will suffer from corrupted block of data and thus corrupting whole file. Hence, a reliable mechanism is needed which would ensure that the received file is in the intact form. Security is also a challenge which needs to be met. Any malicious misbehavior of the driver such as fabrication of data may lead to corrupted data block, thus disruption of operation in VANETs. There doesn't seem to be a practical way to verify if a peer is sending valid blocks of data until the file is decoded, which happens very near the end - far too late to detect and punish abuse. Hence it is very necessary to prevent fabricated messages from threatening safety, traffic efficiency or other user messages. There must also be a mechanism to differentiate between the message types so that as per the significance of message, mechanisms are applied. Next section proposes the model considering the problems studied in this section.

4. PROPOSED MODEL

In this paper we mainly concentrate on reliability and security parameter affecting the vehicular networks. As the paper proceeds, it will be noticed that care has been taken about the overhead incurred while applying the proposed mechanisms. Fig. 2 presents a flow chart of the proposed scheme.

Due to highly dynamic topology of vehicular networks, reliability poses a grave challenge. When a data block is transmitted in a peer-to-peer content distribution network, it is expected to remain in original format till it reaches the final destination node. Since data transmission is carried out in vehicular network, there is no fixed topology and nodes leave and join the topology at different rates. Under such condition it becomes difficult to keep track of data blocks disseminated to nodes.

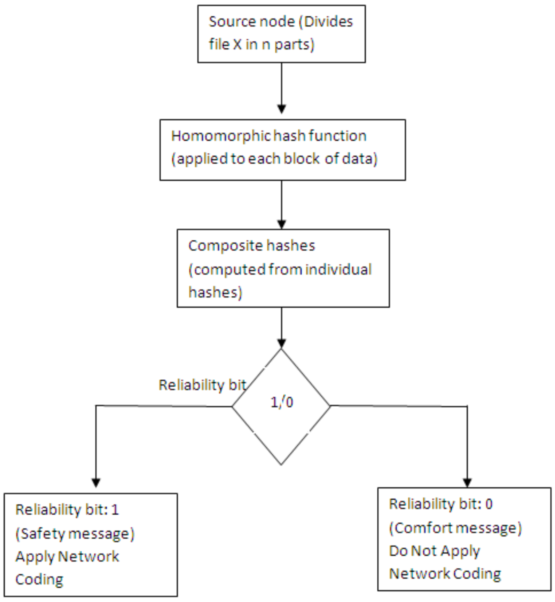
Source node (Divides file X in n parts)
Homomorphic hash function (applied to each block of data)
Composite hashes (computed from individual hashes)
Reliability bit
1/0
Reliability bit: 1 (Safety message) Apply Network Coding
Reliability bit: 0 (Comfort message) Do Not Apply Network Coding

Fig 2: Flow chart of the proposed model

If a node having a data block of particular file is disconnected from the topology due to some reasons, it becomes difficult to create complete file at final destination and again retransmission of the file has to be carried out. This problem can be solved by implementation of network coding. The proposed system implements random linear network coding. Here, a seed node divides the given file X into n pieces X1, X2, X3…XN. The arithmetic equation applied is, C=$\sum_{k=1}^{n}$ ek Xk. Here ek is the arithmetic function. Each node generates its own random coding coefficient for the encoded packet. Coefficients are sent to the destination node in the packet header. The destination can decode the packet without knowing the network topology. Encoded data blocks are transmitted to their 1-hop neighboring nodes so even if one of the nodes get disconnected during transmission, receiving node gets the same data block from another node. Thus making whole set up reliable.

The problem of security is addressed by applying homomorphic hash function. Hash of individual blocks is calculated as h1, h2, h3,…,hn. Then hash of composite block is computed from the hash of individual block. A list of individual hashes is distributed to the drivers or passengers and they could use those to verify incoming blocks as they arrive. At receiving end the encoded block x, which is linear combination of n original blocks and coefficient c1, c2, c3…cn. The individual blocks will be verified as valid by using x, C and hash values h.

When network coding and homomorphic hash function is applied parallelly, it provides neat solution to the problem of reliability and security but has its own drawbacks. They are computationally quite expensive to compute. Also, the overhead incurred is high. Considering the devices used in VANETs are generally battery-operated and are not equipped with high-end hardware and memory units. High compute cycles may lead to early exhaustion of battery in devices and may also be rendered as time consuming procedure. Due to high overhead in data packets buffer space might be exhausted and may lead to frequent dropping of packets if buffer overflow occurs due to limited small buffer space of devices. Hence, a new reliability bit is introduced in the header part. Depending upon the type of message reliability bit is set. Here two types of messages are considered: safety messages and comfort messages. The priority of safety message is higher than the comfort messages. Thus, in order to save compute cycles network coding will be applied to safety messages only. This will be indicated by reliability bit, if this bit is set to 1, then network coding is to be applied. The sender node applies network coding and then forwards it to neighboring nodes. When the packet reaches neighboring node it checks for the reliability bit in the header. If the bit is set to 1 then network coding is applied and if the bit is set to 0 then the packet is forwarded as it is. When reliability bit is 0 means the message is a safety message.

5. CONCLUSION

In this paper we have proposed a model which provides reliability and security. Reliability is provided by network coding which increases throughput and robustness of network. For security, homomorphic hash function is applied which provides a neat solution to the problem of verifying data from untrusted peers. Both the mechanisms parallelly solve our problems but have their own drawbacks. These mechanisms require high compute cycle and have high overhead. Hence to alleviate this problem reliability bit is added. If the message is safety message the reliability bit is set and network coding is applied. In the case of comfort message reliability bit is set to 0 and network coding is not applied. Thus partially saving compute cycles and reducing the processing time.

6. REFERENCES

[1] Jose Santa, Antonio F. Go´mez-Skarmeta, Marc Sa´nchez-Artigas, “Architecture and evaluation of a unified V2V and V2I communication system based on cellular networks”, Mobility Protocols for ITS/VANET, Volume 31, Issue 12, July 2008 – Elsevier

[2] Daniel Jiang, Luca Delgrossi, “IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments”, Vehicular Technology Conference, 2008, IEEE

[3] Yi Wang, Akram Ahmed, Bhaskar Krishnamachari and Konstantinos Psounis, “IEEE 802.11p Performance Evaluation and Protocol Enhancement”, Proceedings of the 2008 IEEE International Conference on Vehicular Electronics and safety.

[4] Ho-Yeon Kim, Dong-Min Kang, Jun-Ho Lee, Tai-Myuong Chung, “A Performance evaluation of Cellular Network Suitability for VANET”, World Academy of Science, Engineering and Technology, 2012

[5] Elmar Schoch, Frank Kargl, and Michael Weber, Tim Leinmüller, “Communication Patterns in VANETs”, IEEE Communications Magazine, November 2008

[6] Tatsunori Kimpara, Susumu Ishihara, “Using GNU Radio for Experiments on Data Distribution in Wireless Ad-hoc Networks”, by Information Processing Society of Japan, ICMU 2012

[7] Da Zhang, Chai Kiat Yeo “A Cooperative Content Distribution System For Vehicles”, Global Telecommunications Conference (GLOBECOM 2011), December 2011 IEEE

[8] Mohsen Sardari, Faramarz Hendessi, Faramarz Fekri, “Infocast: A New Paradigm for Collaborative Content Distribution from Roadside Units to Vehicular

Networks", Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society, June 2009 IEEE

[9] Bayrak, A.O. , Acarman, T. , "S3P: A Secure and Privacy Protecting Protocol for VANET", Wireless and Mobile Communications (ICWMC), 2010 6th International Conference, September 2010 IEEE

[10] Shabbir Ahmed, Salil S. Kanhere, "VANETCODE: Network Coding to Enhance Cooperative Downloading in Vehicular Ad-Hoc Networks", IWCMC '06 Proceedings of the 2006 international conference on Wireless communications and mobile computing, 2006 acm

[11] Shen, Pei-Yuan, Liu, Vicky, Tang, Maolin, & William, Caell, "AN EFFICIENT PUBLIC KEY MANAGEMENT SYSTEM: AN APPLICATION IN VEHICULAR AD HOC NETWORKS", *Pacific Asia Conference on Information Systems (PACIS),* AIS Electronic Library (AISeL), August 2011

[12] Atsushi Fujimura, Soon Y. Oh and Mario Gerla, "network coding vs. Erasure coding: reliable multicast in ad hoc networks", Military Communications Conference, 2008. MILCOM November 2008. IEEE

[13] Christina Fragouli, Jean-Yves Le Boudec, Jörg Widmer, "**Network coding: an instant primer",** ACM SIGCOMM Computer Communication Review, Volume 36 Issue 1, January 2006

[14] Irina Tal and Gabriel-Miro Muntean, "User-oriented cluster-based solution for multimedia content delivery over VANETs",Broadband Multimedia Systems and Broadcasting (BMSB), June 2012 IEEE International Symposium