VANETs: The Networking Platform for Future Vechicular Applications

Gayathri Chandrasekaran
Department of Computer Science
Rutgers University
chandrga@cs.rutgers.edu

***Abstract*—Taking into account the constant growth of automotive market and the increasing demand for the car safety, also driven by regulatory (governmental) domain, the potential of car-to-car connectivity is immense. The classes of applications for vehicular networks range from time critical safety applications to delay tolerant internet connectivity applications.**

In this paper, we take the position that VANETs would indeed turn out to be the networking platform that would support the future vehicular applications. We analyze the factors that are ctitical in deciding the networking framework over which the future vehicular applications would be deployed and show that there are active research efforts towards making VANETs a reality in the near future.

I. Introduction

In the recent years, vehicular networking has gained a lot of popularity among the industry and academic research community and is seen to be the most valuable concept for improving efficiency and safety for future transportations. With the wireless technology becoming pervasive and cheap, several innovative vehicular applications are being discussed. We classify these applications into two main categories -

- **Safety Related [1], [2]:** Applications like collision alert, road conditions warning, merge assistance, deceleration warning, etc. will be classified under safety related applications where the main emphasis is on timely dissemintation of safety critical alerts to nearby vehicles.
- **Internet Connectivity Related [3], [4]:** Accessing emails, web browsing, audio and video streaming are some of the connectivity related applications where the emphasis is on the availability of high bandwidth stable internet connectivity

While Infostations [5] and 3G/4G [6] primarily provide the vehicle to infrastructure(gateway) communication (V2I) in the context of vehicular communication, VANETs assumes a more generic framework that includes both the vehicle to vehicle communication (V2V) and limited V2I communication with higher emphasis on the V2V communication. It is important to understand that the V2I communication model in VANETs is not well defined and most of the current proposals assume the presence of limited or intermittent internet connectivity. In this paper, we analyze the advantages of using a VANETs based approach in comparison to a pure V2V or a pure V2I based solutions and take a position that a tight integration of the V2V and V2I functionalities would become the most succesful model for the future vehicular applications. Specifically, we emphasize that the ill-defined V2I communication infrastructure in VANETs would head towards the so-called "4G" approach where there is opportunistic utilization of the best access network. We believe that the latency concerns related to the safety applications would be served by the high bandwidth, low latency V2V infrastructure and the delay tolerant internet connectivity based applications and the security concerns would be addressed through the V2I infrastructure.

The main factors that would influence the adoption of VANET architecture for future vehicular applications would be -

1) Low latency requirements for safety applications
2) Extensive growth of interactive and multimedia applications
3) Increasing concerns about privacy and security

While there are strong reasons to adopt the VANET architecture as pointed above, there are also several research challenges that needs to be addressed before VANETs could become widespread. They include - Data dissemination techniques, Security and Privacy

concerns, Lack of simulators for protocol evaluations, Bootstrapping/Market penetration issues, Automatic incident detection and collision avoidance capability and Driver distration studies

We argue FOR the success of VANET architecture and elaborate on the above mentioned research challenges in the following sections with a hope to convince the reader that there is indeed an active effort towards bridging these gaps and VANETs with a hybrid V2I infrastructure would indeed become a reality for the future vehicular networking applications.

The rest of the paper is organized as follows. In section II, we provides a brief introduction to VANETS, Infostations and 3G/4G followed by a discussion on the factors influencing the adoption of VANETs in section III. We continue with presenting the research challenges in section IV. Section V addresses the counter claims and arguments and we conclude in section VI

II. Background

In this section, we provide a brief introduction to VANETs, infostations and the mobile communication standards including 3G and 4G and understand their differences in-terms of *Bandwidth limitations, latency, price, and the most compelling application*.

A. VANETs Infrastructure

VANETs [7] are a form of mobile ad-hoc networks to provide communications among nearby vehicles and between vehicles and nearby fixed equipment. To this end, special radios [8] and sensors would be embedded within the car. The V2V communication infrastructure assumes the presence of high bandwidth with low latency. The radios typically operate on unlicensed band making the spectrum free. The most compelling application for V2V would be the safety related application since the latency requirements for these applications are very stringent. The V2V infrastructure in VANETs can provide low latency data dissemination from the point of impact to the nearby vehicles using short range radios.

B. Infostations

Infostations [5] is a wireless system concept that can provide isolated pockets of high bandwidth connectivity to the internet for mobile terminals. In the context of vehicular communications, Infostations are the wireless Access points deployed at specific locations in the road network to support V2I communication. Infostations technology envisions ultra-high-speed radios operating at 100s of Mbps or even Gbps rates, current generations of hardware using variants of the 802.11 standard are now providing bit rates in the tens of megabits per second, using compact, low-cost hardware. As pointed out in the definition, the connectivity is intermittent and can sustain high bandwidth with low latency. The use of wireless technologies that utilize the free spectrum(unlicensed band) reduces the cost per bit thereby making internet accesses through infostation extremely cheap. The most compelling application for Infostations is internet connectivity, esp. for file transfer and bursty data transfers. Since the connectivity is intermittent, Infostations cannot sustain interactive applications and these can definitely not be used for latency critical applications(safety applications).

C. Mobile Communication standards: 3G/4G

The Mobile communication standards have emerged from first generation to the third generation and the fourth generation Mobile communication standards are actively being researched. Figure 1 plots the Data-rate Vs. Mobility (or Communication Range) trade-off. As can be seen from Figure 1, Wi-Fi has the highest data rate(around 10Mbps) but absolutely no mobility support while GSM(2.5G) has the best mobility support but can only sustain data rates of upto 180kbps. Universal Mobile Telecommunication System (UMTS) is one of the third generation cell phone technologies that is widely being adopted in the present day and it

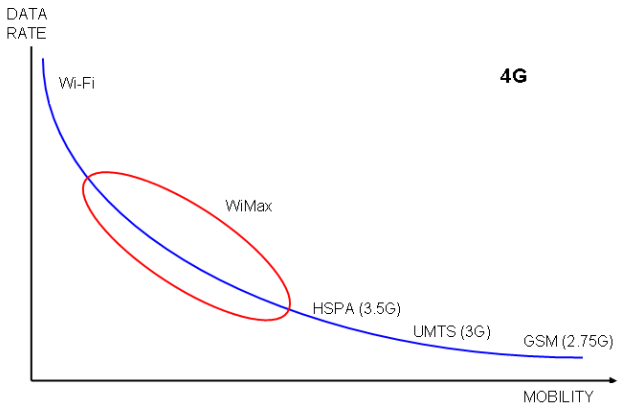

Fig. 1. Data Speed Vs. Mobility for wireless systems

could support data rates of upto 384Kbps. In general, the trend in the mobile communication standards is towards improving the data rate and sustain as much mobility as possible.

4G, the future mobile communication technology proposes to provide a radically new design rather than incremental improvements over the prior mobile communication standards. 4G promises high data-rates with high mobility support and smooth handoff across heterogeneous networks. However, at present, we have no evidence that 4G is indeed going to fulfill all these objectives, and even if it does, it is not going to be cheap in the near future. So, for the purpose of further realistic discussion, we will limit ourselves to the widespread 3G technology.

We can see that 3G networks have bandwidth constraints and inturn have higher latency with increased accesses. Since the spectrum under use is a licensed band, there is an increased cost per bit thereby making internet accesses more expensive than the infostation model. As we can readily see, there is an improved mobility support enabling more interactive intenet applications.

III. Factors influencing the adoption of VANETs

In this section, we highlight the reasons that would drive the adoption of VANETs for future vehicular applications.

A. Low latency requirements for safety applications

Safety applications like collision alert, merge assistance, road condition warning, etc requires messages to be propaged from the point of occurance to the target vehicles with very low latency (a few nano-seconds). Infostation based Infrastructure access networks have intermittent connectivity and does not provide any delay guarantees.while the 3G based cellular data access networks which can provide continuous connectivity have low bandwidths which could induce a delay of few ms to a few seconds. The natural approach is to leverage the V2V infrastructure that is cheap and can sustain the latency requirements for safety applications and VANETs are the natural candidates for this application.

B. Extensive growth of interactive and multimedia applications

The recent years have witnessed a tremendous increase in the number of multimedia applications, interactive games, and location based services and most of these applications require either intermittent or continuous internet connectivity. A pure V2V based solutions cannot address these application domains and there is a definite need for V2I infrastructure and VANETs have this V2I support as well.

C. Increasing concerns about privacy and security

The biggest threat to VANETs are privacy and security. With a pure V2V architecture, authentication and key management becomes extremely cumbersome and requires a prior knowledge of all the available public keys for the participating vehicular entities in order to verify users identity. However, having a fixed identity can inturn raise a lot of privacy concerns [9] and the proposed solution involves the use of disposable temporary identities [10] that can be assigned by a centralized key distribution agency. This centralized agency can inturn selectively geocast these temporary identities with their corresponding public keys in the most relevant geographical area to be picked up by vehicles for authentication or the vehicles can query the key distribution authority to retrieve the public key for the vehicle it needs to authenticate. Thus, to effectively verify the identities of the peers, and dynamically download the keys to address the privacy and security concerns, presence of V2I infrastructure is critical.

IV. Research towards bridging the gaps

We have to understand and acknowledge the fact that vehicular networking is relatively new and the protocols or architecture for the same are actively being developed. Even though several research challenges exist before VANETs could become practical, we point out in this section that the VANET research is converging towards bridging these gap to make it a reality. The research challenges are:

A. Data dissemination

The foreseen vehicular applications will require a vast amount of information to be exchanged and the challenge is to exchange the information in a scalable

fashion. With a highly changing topology, it is impossible to sustain unicast/multicast connections and broadcasting seems to be the most scalable solution. Broadcasting can be of two types - Flooding and dissemination. In the flooding mechanism, each individual vehicle periodically broadcasts information about itself and every time a vehicle receives a broadcast message, it stores it and immediately forwards this by re-broadcasting. While this is the easiest approach, the solution is clearly not scalable. The alternative is to disseminate data using intelligent techniques like aggregation [11], clustering [12] or location-aware broadcasting and this field of research is active towards building a scalable data dissemination strategy.

B. Security and Privacy

Security is an issue that needs to be carefully assessed and addressed in the design of the vehicular communication system. Several threats potentially exist, including fake messages causing disruption of traffic or even danger, compromising driver's private information, etc. The issues to be addressed include trust (vehicles are able to trust the messages they receive), and efficiency, e.g. real-time message authentication.

Privacy is also a major issue that will need to be addressed. Anonymity must be preserved - the communications should not make the vehicle tracking or identification possible for non-trusted parties. Several research efforts [13], [14] are being undertaken to address the privacy concerns at the design stage. SEVECOM (SEcure VEhicular COMmunications) [15] is a newly funded project that focuses on proving a full definition and implementation of security requirements for vehicular communications.

C. Lack of simulators for protocol evaluations

Road traffic has certain properties that can not be easily modeled in a straight-forward way, using the classical MANET approach. Vehicles do not move randomly but rather follow the road infrastructure; road signs, traffic lights and other cars influence node's behavior. Nodes move at high relative speed, network density changes very dynamically, depending on location, recent events (e.g. accidents) or time of day. Thus, one could either build a sophisticated road traffic mobility model on top of some popular network simulator (NS-2, OPNET, GloMoSim), or use mobility traces from another source. This could be either measurement-based road traffic traces. Several recent works [16]–[18] have addressed these issues and are coming up with a more realistic traffic simulators to model the VANETs better.

D. Bootstrapping/Market penetration

There are two mechanisms that lead to a successful market introduction for V2V technologies: either there is a visible added value of the technology for the customer or a regulative order that does not leave alternatives, requires its use. For the regulative introduction to be issued, the effectiveness of the technology has to be proven first. But in case of V2V communications, a certain market penetration is required before any effects or improvements can be shown. Hence, it cannot be expected that a regulative order is issued on the basis of promised safety and traffic flow improvements before the penetration is reached. However, the consumer can only take advantage of a technology once a certain market penetration is reached, and no one will invest in this technology before this is the case, which again means that this penetration might never occur. It was estimated that in order to make the network usable, at least penetration of 10% is needed. Provided that 50% of all newly produced cars are V2V enabled, reaching that 10% should take about three years. [19] which is not an unrealistic estimate.

E. Automatic incident detection and collision avoidance capability

Though the sensor networking technology is well developed and developing proximity sensors, speed detectors, collision avoidance infrastructure is not farfetched, without a proper vehicular testbed, it is difficult to evaluate these capabilities. UCLA [20] has a vehicular CVeT testbed will be composed of about 50 cars, vans and buses of the UCLA campus fleet. Each of these cars will be able to directly connect to the Internet through WiFi access points or, if out of access point coverage, through other cars in WiFi range. This will realize a UCLA campus car Internet backbone. The wired and wireless Internet infrastructure will stretch beyond its boundaries through cars. UCLA provides an ideal "lab" environment to test innovative designs and applications on a significant population set.

F. Driver distraction studies

Finally, several user studies need to be performed on real testbeds to evaluate the driver distraction due to information V2V and V2I information exchange.. Driver distractions are the leading cause of most vehicle crashes. According to a study released by the National Highway Traffic Safety Administration (NHTSA) and the Virginia Tech Transportation Institute (VTTI), 80% of crashes involve some form of driver distraction. The distraction occurred within three seconds before the vehicle crash. Thus applications need to consider this distraction element at the design stage for improving safety.

V. Counter Arguments

In the following subsections, we attempt to address the claims which argue that VANETs may never become the future networking platform for vehicular applications.

A. 3G is readily available and would turn out to be the platform for vehicular applications

As pointed out in section III, safety critical applications have low latency requirements. Even under the assumption of a extremely high bandwidth cellular link, there are issues relating to bandwidth sharing as the number of vehicles scale. The market for smartphones, such as the iPhone, BlackBerry and Treo, which offer e-mail and Web access, will grow from around 10 percent of the cell market in 2007 to 31 percent in 2013, according to a new study from ABI Research and the 3G (or 4G) network would have to be shared among more number of users thereby potentially reducing the available bandwidth per person. Thus a pure V2I solution based on 3G/4G can not become the networking platform for the future vehicular applications.

B. Cellular Networks are expensive, the V2I model would only be Infostations

In this paper we have argued for the opportunistic utilization of available V2I infrastructure. This counter claim argues that the cost involved with the data access through cellular networks may prove to be a hindrance for such a hybrid approach. While the cost concerns are valid, the APPLE inc. has reported to have sold 4 million iPhones during its first 200 days on sale, which it calculated to be an average of 20,000 units per day. It is important to note that iPhones are sold with data plan. With such a tremendous growth, we can see that cost concerns are easing out and with more and more users being added to the system, the cost is sure to decrease further.

C. The entire vehicular ad-hoc research is bogus. It would fail like ad-hoc networks.

This is a very interesting counter claim which argues that the entire vehicular networking research is bogus and is similar to ad-hoc research which was primarily confined to the universities. There are strong reasons against this. They are:

- Unlike Ad-hoc networks which had no user incentive for content sharing or relaying, the main incentive for VANETs are these safety applications which is of interest to every participating vehicle. The design should eliminate the possibility of just receiving safety messages without having to propagate them to avoid selfish users.
- There is a strong push from the government to bring about a safe vehicular traffic. In the US the FCC has already allocated 75 MHz of spectrum at 5.9 GHz (from 5.850 to 5.925 GHz) for V2V and V2I communications.
- The car manufacturers are also inclined towards favoring VANETs. In the recent years, the main feature additions to the car had been on the software end and, to keep up with the competition and raise the profit margins, the car companies are sponsoring research activity in making VANETs a reality.

Thus, we believe that the applications would indeed make VANETs a reality unlike the academic ad-hoc research.

VI. Conclusion

In this paper, we argued that VANETs would turn out to be THE networking infrastructure for supporting future vehicular applications. We started with describing the factors that would be critical in making VANETs a reality followed by a discussion on the research challenges. We showed that there are several challenged including security and privacy and that active research efforts are being undertaken to bridge the gaps required to make VANETs a reality. We finally discussed the counter claims that challenged

the practicality of VANETs and showed that there are indeed strong reasons for vehicular applications to be deployed and that a pure V2V or V2I based solutions will not be sufficient and VANETs would indeed succeed in catering to these applications.

REFERENCES

[1] "The FleetNet project," http://www.fleetnet.de.

[2] H. Hartenstein, H. Füßler, M. Mauve, and W. Franz, "Simulation Results and Proof-of-Concept Implementation of the FleetNet Position-Based Router," in *Proc. of Eighth International Conference on Personal Wireless Communications (PWC '03)*, Venice, Italy, 09 2003, pp. 192–197.

[3] K. Lee, S.-H. Lee, R. Cheung, U. Lee, and M. Gerla, "First experience with cartorrent in a real vehicular ad hoc network testbed," in *2007 Mobile Networking for Vehicular Environments*, 2007, pp. 109–114.

[4] J. Ott and D. Kutscher, "Drive-thru internet: Ieee 802.11b for "automobile" users," in *INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies*, vol. 1, 2004, p. 373.

[5] R. H. Frenkiel, B. R. Badrinath, J. B. As, and R. D. Yates, "The infostations challenge: Balancing cost and ubiquity in delivering wireless data," *IEEE Personal Communications*, vol. 7, pp. 66–71, 2000.

[6] "3G, Wikipedia Article," http://en.wikipedia.org/wiki/3G.

[7] "VANETs, Wikipedia Article," http://en.wikipedia.org/wiki/VANET.

[8] "DSRC Standards," http://tinyurl.com/6fy29c.

[9] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking," in *MobiSys '03: Proceedings of the 1st international conference on Mobile systems, applications and services*, 2003, pp. 31–42.

[10] ——, "Enhancing location privacy in wireless lan through disposable interface identifiers- a quantitative analysis," pp. 315–325, 2005.

[11] T. Nadeem, P. Shankar, and L. Iftode, "A comparative study of data dissemination models for vanets," in *Mobile and Ubiquitous Systems: Networking & Services, 2006 Third Annual International Conference on*, 2006, pp. 1–10.

[12] W. Chen and S. Cai, "Ad hoc peer-to-peer network architecture for vehicle safety communications," *Communications Magazine, IEEE*, vol. 43, no. 4, pp. 100–107, 2005.

[13] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications."

[14] A. Stampoulis and Z. Chai, "A survey of security in vehicular networks."

[15] "SEcure VEhicular COMmunications," http://www.sevecom.org/.

[16] R. Mangharam, D. Weller, R. Rajkumar, P. Mudalige, and F. Bai, "Groovenet: A hybrid simulator for vehicle-to-vehicle networks," in *Mobile and Ubiquitous Systems - Workshops, 2006. 3rd Annual International Conference on*, 2006, pp. 1–8.

[17] R. Baumann*, S. Heimlicher*, and M. May*, "Towards realistic mobility models for vehicular ad-hoc networks," in *2007 Mobile Networking for Vehicular Environments*, 2007, pp. 73–78.

[18] "VISSIM, Traffic Simulator," http://tinyurl.com/66ch9r.

[19] K. Matheus, R. Morich, and A. Lbke, "Economic background of car-to-car communications," *IMA*, 2004.

[20] "Vehicular Testbed in UCLA," http://www.vehicularlab.org/home.do.