**Autonomous Cars and Vehicular Communication**

**(December 2014)**

Louis Fead, Andrew Walwema

*Abstract* - Cars have revolutionized the way humans go about in their daily lives. Over the past decade technology has taken a significant role in changing the way people drive and it could change the way people live their daily lives. With self-driving cars (autonomous) being on the verge of reality, there is still some research needed to be done in order for technology such as Vehicle-to-Vehicle Communication (V2V) to help fully transition towards autonomous cars. Many car companies have successfully developed the concept V2V technology and its network applications. With this new technology, come safety issues, such as hacking and the efficiency of this technology. This academic paper researches on how V2V works and solutions to the potential security risks V2V technology may have if they are breached.

1. **INTRODUCTION**

Vehicles have become increasingly autonomous with the introduction of safety systems like the anti-lock braking system (ABS) and OnStar. More similar features are continuously being added to the concept of an autonomous car. These smart cars are the future of transportation, with the use of GPS networks and Inter-Vehicle Communication (IVC ) and/or Vehicle-to-Vehicle Communication (V2V), they can navigate the roads by themselves without the interference of human interaction. Due to a limited amount of time we have over the semester, we have chosen to mainly focus on V2V technology because it is a topic researched in more detail

and is the next major step towards Autonomous vehicle technology. When it comes to V2V technology, safety is the number one priority in the upcoming age of autonomous cars. With V2V technology, cars will have to communicate with over 100 cars within a 1,000 foot radius interpreting over 100 messages in less than 2 seconds. Having to authenticate and act on several messages in short periods of time could be potentially hazardous especially if a hacker is able to infiltrate a car. This academic paper focuses on how V2V works and solutions to the potential security risks that may arise.

1. **INFRASTRUCTURE OF VEHICLE-TO VEHICLE COMMUNICATION**

*A. Description*

Vehicle-to-Vehicle (V2V) is the wireless transmission of data between two or more vehicles. The vehicles use an Ad-hoc network which allows the cars to communicate among other cars within a certain range [10]. With an Ad-hoc network, cars can act as a horst or end user without having to go through a central server. One compelling issue that comes to surface with V2V technology is the authentication and verification of the legitimacy of the messages been sent to and from the vehicles. Finding a valid solution to this issue could cause a delay to standardizing V2V technology toward the public, potentially preventing breakthrough technology that could save lives.

*B. Current Research and Technology*

V2V technology is a hot research topic among automotive companies, universities, governments, and select companies that aren’t primarily automotive-related. Ford, General Motors, BMW, and several other car companies have already began implementing their own technology and have goals of releasing these modern vehicles by the end of the decade [reference]. Institutions such as Clemson University and the University of Michigan have been doing extensive research that has benefited the development of this technology. Even Google, an Internet-service based company, had the first car pass a U.S. self-driving test [10, 17].

*C. Physical and Conceptual Structure of V2V Technology*

The implementation of V2V communication is a step closer to fully realizing fully-autonomous cars. In addition to being able to communicate with vehicles, cars will also be able to communicate with the outdoor infrastructure, such as gas stations, posted signs, and the traffic lights (Figure 1). To reach full effectiveness, the technology will have to be nearly ubiquitous. The background technology, such as the hardware and transmission protocols have been standardized, here is an overview:

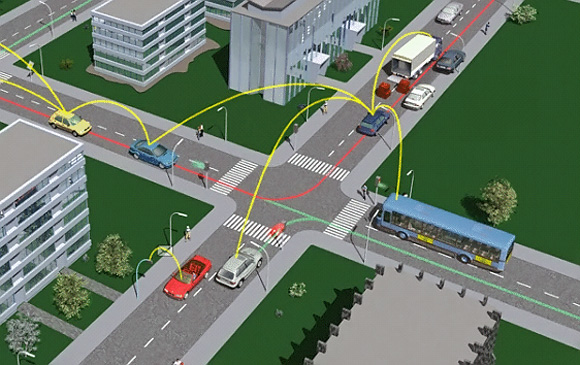


Figure 1: V2V in conjunction with V2I (Image from Extreme Tech [1])

Using dedicated short-range communications (DSRC), vehicles can communicate with each other, ranging from 300 to 1000 feet (set and regulated by the FCC). V2V technology supports two types of applications which require two different types of networks, non-safety applications and safety applications. Non-safety applications- which normally require internet access use the traditional protocol stack with TCP /IP with the standardized IEEE 802.11 a/b/g technology. Entertainment applications such as Pandora, which is used for listening to music, would be considered a non-safety application. Safety applications use a local area network but TCP/IP is not suitable for this application. Instead the safety and other traffic applications directly communicate with each other with an ad hoc mesh network. 802.11p radio technology, which is directly derived from IEEE 802.11a, is the physical hardware customized to fit the vehicular environment. The radio technology occupies 75 MHz of the 5.85 to 5.925 GHz of the spectrum [5].

In order for Vehicles to exchange information with each other, different protocol layers are needed to optimize the performance of the V2V system design. Here is a visual explanation of the structural architecture V2V is based upon:

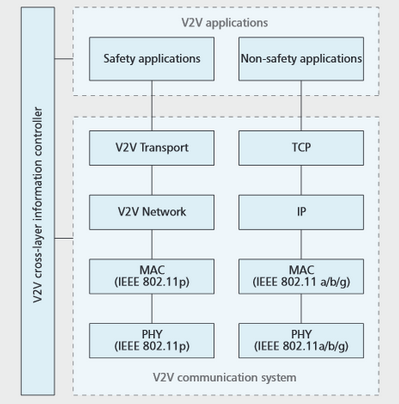


Fig 2: V2V Application Model

1. POTENTIAL PROBLEMS AND SOLUTIONS TO LATENCY CAUSED BY MULTIPLE SIMULTANEOUS MESSAGES

*A. Problem*

Most of the time when we are on the road, we share the road with many cars and if all or most are VANET (Vehicular ad hoc network) enabled, that means there would be multiple messages being sent simultaneously between every car (and infrastructure). These multiple simultaneous messages become an issue once the processor is overwhelmed with authenticating all the messages and thus creating major latency problems in a situation which expediency is everything [4].

One solution is proposed by the Verify-On-Demand system put forth in a paper by Hariharan Krishnan of General Motors Company and Andre Weimerskirch of escrypt, Incorporated for the overwhelming multiple simultaneous messages which assign the messages a priority level based on threat level to the safety of the vehicle. This reduces unnecessary processing on less important messages such as application messages without decreasing the level of vehicle safety [4].

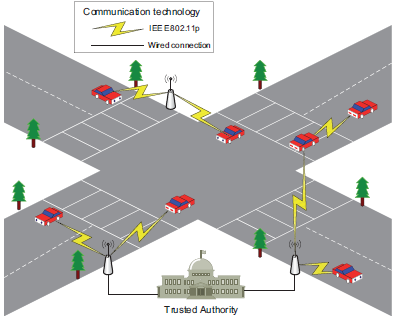
The other problem that comes to light is the legitimacy of the message and its sender. In order to authenticate both message and sender, we can use the following approaches according to the research paper “Anonymous Authentication Protocols for Vehicular Ad Hoc Networks: An Overview” by Hu Xiong et. al.:

1. RSU-based approach
2. Group-oriented signature-based approach
3. Pseudonyms-based approach
4. Priori -based approach

All but the first are decentralized approaches

*B.RSU-based approach*

In the first, the RSU-based approach, authentication is done by a certifying authority based out of the infrastructure. This minimizes the amount of processing power devoted to authentication and enables conditional privacy. However, it is limited to the infrastructure that supports it. [5]



*C. Group-oriented signature-based approach*

The second, a Group-oriented signature-based approach proposed by Chaum and Heyst uses a proposed type of signature scheme called group signatures. This allows a member of the group to “anonymously” sign for the entire group. Only the group manager, a trusted third party can reveal the identity of the actual signer at a later stage for auditing purposes. The group manager is an entity composed of at least one individual [5].

Another Group-oriented signature-based approach is proposed by Lin et al. In this, each vehicle stores only a private key and a group public key. To prevent messages from exposed to the public, it is encrypted with the group key. This way only the trusted authority is able to reveal the identity of the sender. However, the time need to process each verification grows linearly with each blacklisted vehicle in the network, thus extending processing time. Additionally, once the number of blacklisted vehicles reaches some threshold, then the group must calculated a new group public key adding even more time. [6]

*D. Pseudonyms-based approach*

The basic method of the third, the Pseudonyms-based approach uses a large number of private keys and the corresponding anonymous certificates on each vehicle. In order to sign a message, the sending vehicle selects a random a key and certificate pair. On the other end, the receiving vehicle uses the sender’s public key, enclosed with the message, to authenticate the message’s source. The anonymous certificates are generated from a pseudo- identifier instead of any personal identifier of the operator or the vehicle and have a short lifetime. This method is inefficient though it meets the privacy requirements. [6]

A more efficient version is based on the Timed Efficient Stream Loss-tolerant Authentication (TESLA) broadcasting protocol. The protocol utilizes a one-way hash chain in which each hast is a private keys used to authenticate messages. Using TESLA, data is sent at predefined intervals, known to both sender and receiver. Each hash chain element contains a key that corresponds to a time interval. If the message is received at the given interval and the corresponding hash is received, then the message is authenticated. However, since the method requires loose synchronization between the nodes and thus results in delayed message authentication. [6]

Another version based on TESLA method is dubbed the ‘time-efficient and secure vehicle communication’ (TSVC) method. Using this method, a vehicle commits itself to the hash chain then relays this to nearby vehicles. Then it generates a message authentication code from hash chain elements that can be used to authenticate the vehicle’s messages. Since the TSVC method uses the fast message authentication code authentication, it is faster than the first TESLA method. However, TSVC requires a large set anonymous private-public key and certificate pairs to be installed in each vehicle, additionally, should a vehicle broadcast it commitment to the chain at a much higher frequency such as where there is a high flow of traffic. [6]

*E. Priori -based approach*

The fourth, the Priori -based approach requires a message to be endorsed by other vehicles and requires these endorsements to reach a given number in order for the message to considered valid. This reduces messages, both valid and false, to only those endorsed in vast numbers. It excludes attacks that are few in numbers. However, this still leaves attacks that use vast numbers in their attacks similar to denial-of-service attacks. [8]

1. CONCLUSION

In view of the complexity of the problems presented by multiple simultaneous messages from the vehicles, a combination of the above proposed solutions as one solution does not cover everything nor has exploitable weaknesses. We recommend utilizing a priority-based approach to weed out messages that are harmful, the Verify-On-Demand system to prioritize messages and utilizing the group-oriented signature-based approach proposed by Lin et al.

1. REFERENCES

[1] Azogu, Ikechukwu K., Michael T. Ferreira, Jonathan A. Larcom, and Hong Liu. "A New Anti-jamming Strategy for VANET Metrics-directed Security Defense." *IEEE Xplore*. IEE, 9 Dec. 2013. Web. 17 Sept. 2014.

[2] Cheng, Lee, Daniel D. Stancil, and Fan Bai. "Get the Latest News about Solution-driven Research, Technology and Scholarship at North Carolina State University." *NC State News New Model to Improve VehicletoVehicle Communication for Intelligent Transportation Comments*. IEEE, 9 Sept. 2013. Web. 17 Sept. 2014.

[3] Conti, J.P., "Smart cars," *Communications Engineer* , vol.3, no.6, pp.25,29, Dec./Jan. 2005. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1604921&isnumber=33720>

[4] Hariharan Krishnan, André Weimerskirch, "[Verify-on-Demand - A Practical and Scalable Approach for Broadcast Authentication in Vehicle-to-Vehicle Communication](http://www.weika.eu/papers/KrishnanWeimerskirch_VOD.pdf)", SAE 2011, World Congress, April 12-14, 2011, Detroit, USA. 11/3/2014

[5] Howard, Bill. "V2V: What Are Vehicle-to-vehicle Communications and How Do They Work? | ExtremeTech." *ExtremeTech*. Ziff Davis, LLC, 6 Feb. 2014. Web. 06 Oct. 2014.

[6] Hu Xiong, Zhi Guan, Jianbin Hu and Zhong Chen (2012). Anonymous Authentication Protocols for Vehicular Ad Hoc Networks: An Overview, Applied Cryptography and Network Security, Dr. Jaydip Sen (Ed.), ISBN: 978-953-51-0218-2, InTech, Available from: <http://www.intechopen.com/books/applied-cryptography-and-networksecurity/privacy-issue-in-vehicular-ad-hoc-networks>

[7] Le, Dong-Hyun, Yoon-Ho Choi, and Seung-Woo Seo. "A Heuristic Task Allocation Methodology for Designing the Secure In-vehicle Network." *IEEE Xplore*. IEEE, 18 June 2012. Web. 17 Sept. 2014.

[8] Pouyan, Ali A., and Mahdiyeh Alimohammadi. "Sybil Attack Detection in Vehicular Networks." *Sybil Attack Detection in Vehicular Networks* (2014): 467-89. Horizon Research Publishing, 2014. Web. 17 Sept. 2014.

[9] Wang, Cheng-Xiang, Xiang Cheng, and D. Laurenson. "Vehicle-to-vehicle channel modeling and measurements: recent advances and future challenges.

[10] Ko, Sun. "Clemson Vehicular Electronics Laboratory: Vehicle to Vehicle Communication Technology." Clemson Vehicular Electronics Laboratory: Vehicle to Vehicle Communication Technology. Clemson University, n.d. Web. 11 Dec. 2014. <http://www.cvel.clemson.edu/auto/AuE835\_Projects\_2011/Ko\_project.html>.

[11] Shipman, Matt. "New Model to Improve Vehicle-to-Vehicle Communication for ‘Intelligent Transportation’." NC State News New Model to Improve VehicletoVehicle Communication for Intelligent Transportation Comments. North Carolina State University, 16 July 2013. Web. 11 Dec. 2014. <http://news.ncsu.edu/2013/07/wms-stancil-v2v/>.

[12] Özguner, Ümit. "Vehicle-to-Vehicle Communication for Intelligent Transportation | The Ohio State Center for Automotive Research." Vehicle-to-Vehicle Communication for Intelligent Transportation | The Ohio State Center for Automotive Research. Ohio State University, n.d. Web. 11 Dec. 2014. <http://car.osu.edu/vehicle-vehicle-communication-intelligent-transportation>.

[13] DeGroat, Bernie. "U-M Transportation Research Institute Leads Way in 'smart Car' Technology." U-M Transportation Research Institute Leads Way in 'smart Car' Technology | University of Michigan News. University of Michigan, 21 Aug. 2012. Web. 11 Dec. 2014. <http://ns.umich.edu/new/releases/20685-u-m-transportation-research-institute-leads-way-in-smart-car-technology>.

[14] Kapsner, Christiana. "High-Tech Traffic Control." V2V Technology. University of Minnesota Duluth, Sept. 2011. Web. 11 Dec. 2014. <http://www.d.umn.edu/unirel/homepage/11/vehicletechnology.html>.

[15] BMW. "BMW Technology Guide: Car-to-car Communication." BMW Technology Guide: Car-to-car Communication. BMW, n.d. Web. 11 Dec. 2014. <http://www.bmw.com/com/en/insights/technology/technology\_guide/articles/cartocar\_communication.html>.

[16] Daimler. "Car-to-X Technology from Mercedes-Benz | Daimler Technology & Innovation."Car-to-X Technology from Mercedes-Benz | Daimler Technology & Innovation. Daimler, n.d. Web. 11 Dec. 2014. <http://www.daimler.com/dccom/0-5-1613460-1-1456863-1-0-0-1457041-0-0-135-0-0-0-0-0-0-0-0.html>.

[17] Harris, Mark. "How Google's Autonomous Car Passed the First U.S. State Self-Driving Test." IEEE Spectrum. IEEE, 10 Sept. 2014. Web. 10 Dec. 2014.

[18] Lavrinc, Damon. "Ford Unveils Its First Autonomous Vehicle Prototype | WIRED."Wired.com. Conde Nast Digital, 11 Dec. 0013. Web. 11 Dec. 2014. <http://www.wired.com/2013/12/ford-fusion-hybrid-autonomous/>.

[19] General Motors. "GM: Self-Driving Vehicles Could Be Ready by End of Decade."Media.gm.com. General Motors, 16 Nov. 2011. Web. 11 Dec. 2014. <http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2011/Oct/1016\_autonomous.html>.

[20] Honda. "Honda Worldwide | CSR | Developing Safety Technologies | Evolution and Developing Safety Technologies." Honda Worldwide | CSR | Developing Safety Technologies | Evolution and Developing Safety Technologies. Honda, n.d. Web. 11 Dec. 2014. <http://world.honda.com/CSR/safety-technology/activity/>.