Igor Povarich

VEHICULAR AD-HOC NETWORKS AND THEIR APPLICATIONS

The following article describes a research survey performed around the field of Vehicular Ad-Hoc Networks (VANET) and their Applications. It also outlines the experiment to be performed in the interest of learning and validation of the 802.11p protocol.

1 BACKGROUND / LITERATURE REVIEW

While commercial vehicles have, in recent years, seen a plethora of new and improved safety features such as anti-lock braking, seat belts, airbags, rear-view cameras, electronic stability control, etc., vehicle accidents have nevertheless continued to rise. [1] Some studies have claimed that up to 60% of accidents on motorways could be avoided if warning messages were provided to the drivers just a few seconds prior to the moment of the crash [2].

In recent years, much interest has been garnered for implementation of VANETs (Vehicular Ad-Hoc Networks) as a potential solution to increase road safety while also providing opportunities for user applications to increase convenience, and working toward an Intelligent Transport System (ITS). VANETs are a sub-category of MANETs (Mobile Ad-hoc Networks), with some specific types of challenges.

Research is ongoing in many institutions and companies around the world, but in 1999 the ECC and FCC reserved a five and seven 10MHz band of the 5.9GHz spectrum specifically for emergency V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) applications in Europe and the US, respectively. Several standards have already been established around this allocation, namely a group of standards called 802.11p (which includes the PHY and MAC layers) and the Wireless Access in Vehicular Environments (WAVE) in order to help facilitate the implementation of ITS. [3] [5]

The physical layer of 802.11p is very similar to 802.11a (in order to use the same chipsets), using orthogonal frequency division multiplexing (OFDM) with the major difference being a doubling of the physical parameters in the time domain to decrease inter-symbol interference caused by the multipath delay spread and the Doppler spread effects. 802.11p is also considered a hybrid of 802.11a and 802.11e because it uses the extended DCF defined in 802.11e, which adds support for Quality of Service (QoS). [4]

Most ongoing research experiments use IEEE 802.11a, b, g, or the previously mentioned new 802.11p standard. Due to the very dynamic nature of VANETs, low latency requirements, and stringent PHY/MAC requirements, this renders many types of traditional networks, such as TCP/IP, MANETs, 3g/4g cellular problematic as solutions, hence the development of this

new standard.

More modern implementations of VANETs are also evaluating using SDN controllers to help improve connectivity, routing selection, channel selection, and power selection in complex networks. [6]

Another major area of development necessary for VANETs to be successfully implemented is around security. [7] [8] The packets that are being broadcast will often contain sensitive information about the vehicle/owner and the low latency and ad-hoc requirements of the topology make it a potentially tempting target for attackers. Another concern is that a malicious agent could, for example, issue a false accident report or traffic jam, potentially causing disruptions or congestion in other parts of the roadway or increasing the risk of fatal accidents.

2 Methodology / Metrics

For the experimental implementation of this project, an 802.11p transceiver/receiver will be implemented in GNURadio similar to that in [5]. Simulated noise will be varied at several levels as well as the modulation scheme (BPSK,QPSK,QAM-16,and QAM-64). The performance with respect to error rate and throughput. As a performance comparison, several similar networks, such as 802.11a and 802.11e will be implemented in a similar manner. [9]

As mentioned earlier, another major concern in VANET topologies is around security. Some of the major concerns have been addressed in some of the recent updates to the IEEE 1609.2b standard [10] through the use of administrative tools such as encryption keys and Secure Protocol Data Units (SPDUs). The benefits of these standards and potential gaps will be discussed.

3 References

[1] Eze, Elias C., Sijing Zhang, and Enjie Liu. “Vehicular Ad Hoc Networks (VANETs): Current State, Challenges, Potentials and Way Forward.” In *2014 20th International Conference on Automation and Computing*, 176–81. Cranfield, Bedfordshire, United Kingdom: IEEE, 2014. https://doi.org/10.1109/IConAC.2014.6935482.

[2] Wang, C. David, and James P. Thompson. Apparatus and method for motion detection and tracking of objects in a region for collision avoidance utilizing a real-time adaptive probabilistic neural network. United States US5613039A, filed January 3, 1994, and issued March 18, 1997. https://patents.google.com/patent/US5613039A/en.

[3] “ITS Standards Program | Fact Sheets | ITS Standards Fact Sheets.” Accessed October 5, 2021. https://www.standards.its.dot.gov/Factsheets/Factsheet/80.

[4] Toor, Yasser, Paul Muhlethaler, Anis Laouiti, and Arnaud La Fortelle. “Vehicle Ad Hoc Networks:

Applications and Related Technical Issues." *IEEE Communications Surveys & Tutorials* 10, no. 3 (2008): 74–88. https://doi.org/10.1109/COMST.2008.4625806.

[5] Bloessl, Bastian, Michele Segata, Christoph Sommer, and Falko Dressler. "Towards an Open Source IEEE 802.11p Stack: A Full SDR-Based Transceiver in GNU Radio." In *2013 IEEE Vehicular Networking Conference*, 143–49. Boston, MA, USA: IEEE, 2013. https://doi.org/10.1109/VNC.2013.6737601.

[6] Al-Heety, Othman S., Zahriladha Zakaria, Mahamod Ismail, Mohammed Mudhafar Shakir, Sameer Alani, and Hussein Alsariera. "A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET." *IEEE Access* 8 (2020): 91028–47. https://doi.org/10.1109/ACCESS.2020.2992580.

[7] Mishra, Rashmi, Akhilesh Singh, and Rakesh Kumar. "VANET Security: Issues, Challenges and Solutions." In *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 1050–55. Chennai, India: IEEE, 2016. https://doi.org/10.1109/ICEEOT.2016.7754846.

[8] Goyal, Amit Kumar, Arun Kumar Tripathi, and Gaurav Agarwal. "Security Attacks, Requirements and Authentication Schemes in VANET." In *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, 1–5. GHAZIABAD, India: IEEE, 2019. https://doi.org/10.1109/ICICT46931.2019.8977656.

[9] Bloessl, Bastian. *Table of Contents*. C++, 2021. https://github.com/bastibl/gr-ieee802-11.

[10] "1609.2b-2019 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages - Amendment 2--PDU Functional Types and Encryption Key Management | IEEE Standard | IEEE Xplore." Accessed October 5, 2021. https://ieeexplore.ieee.org/document/8734860.