Intra-Vehicular Wireless Communication

Alex Aleyan

Villanova University Student.

aaleyan@villanova.edu

ABSTRACT

The growing number of components found in automotive systems has blustered the amount of wiring required to interconnect the resultant sensors and control modules. Not only such wiring adds weight to the vehicle thus negatively affecting its fuel efficiency, it also complicates design, manufacturing, and diagnostic processes. Additionally, such rigid systems are hard to upgrade once they are in production. This survey paper on intra-vehicular wireless communications reviews the proposed solutions that span the Physical, MAC, and IP/Application Layers of the intra-vehicular wireless network.

SECTION I. INTRODUCTION

The modern vehicle's powertrain, body, chassis, and networking systems heavily rely onto wired connection which introduces complexity during design and manufacturing. Additionally, added weight due to wiring reduces vehicle's fuel efficiency. To address these issues, the research in intra-vehicular wireless networking has been gaining momentum. This survey paper reviews the proposed solutions to the stated problem by exploring the subject at the layer by layer approach. Section II explores the suggested methods of wireless communication at the PHY Level and MAC layers utilizing such technologies as RFID, Bluetooth, ZigBee, and UWB. Section III reviews the application of the history-based MAC and priority-based MAC in intra-vehicular networks. In Section IV, the security within intra-vehicular wireless communication at the application layer is reviewed.

SECTION II. PHYSICAL LAYER

When considering the design of the wireless network's physical layer and architecture, one should keep in mind [1], [2]:

1. intra-vehicular sensors and control units are stationary [1], [2].
2. energy efficiency is of concern due to limitation imposed by the power output of the gasoline vehicle's alternator, or due to the electric vehicle's battery charge capacitance [1], [2].

3. Real time requirements imposed onto the communication system for such systems as ABS (antilock braking), traction control, DAS (driver assist system), autopilot. Additionally, the sensory data must be delivered on time to the engine's control module for the engine to run reliably [1], [2].
4. Reliability of the wireless system's communication [1], [2]. No data packets should be dropped for the same reasons as mentioned in point 3 above.
5. Since the data must be delivered in real time, as mentioned in point 3 above, the wireless communication system must transfer the data in short but frequent bursts [1], [2]. A good example would be utilizing wireless communication for engine speed sensor. Because gasoline engine's controls and their output depend on the current state of the engine's speed and vary with respect to it, buffering output of the engine speed sensor and delivering large packet of this data will cause the engine to stall. As a result, utilizing IP layer is impractical due to introduced overhead. Utilizing ad hoc protocol is also impractical due to the protocol wrappers.

The RFID as a PHY Layer is determined to be unsuitable due to not meeting the reliability and latency requirements [1]. The relatively high-power consumption and the complexity of the Bluetooth makes it unsuitable [1]. The ZigBee and UWB at the PHY Layer are the two choices that meet the energy [3], speed and reliability requirements imposed by the intra-vehicular communication [1]. However, when the performance under RF interference of the Bluetooth Low Energy (BLE) and the ZigBee were tested, the BLE has been shown to outperform the ZigBee when exposed to Wi-Fi or Bluetooth interference [2] with the next results:

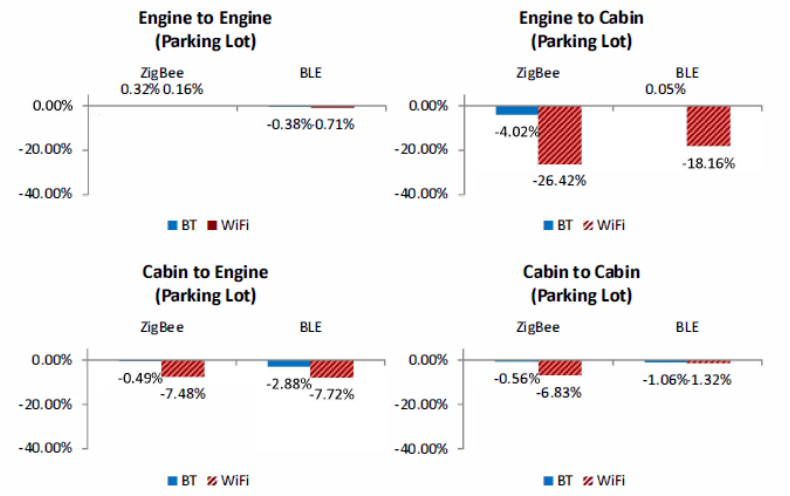

Figure 1. Degradation of the BLE and ZigBee under RF Interference [2].

In the figure above, the 4 test scenarios used are [2]:

1. Engine to Engine (Parking Lot): both the transmitter and receiver are placed inside the engine bay [2].
2. Engine to Cabin (Parking Lot): the transmitter is placed inside the engine bay while the receiver is placed inside the passenger compartment [2].
3. Cabin to Engine (Parking Lot): the transmitter is placed inside the passenger compartment while the receiver is placed inside engine bay [2].
4. Cabin to Cabin (Parking Lot): both the transmitter and receiver are placed inside the passenger compartment [2].

SECTION III. MAC LAYER

The large number of sensory elements, actuators and control modules present within a vehicle may quickly consume the link capacity of a wireless network. To address this issue, the history-based MAC and priority-based MAC are analyzed as possible resolution [4]. According to the author [4], the History-based MAC handles the traffic growth using the latest successful transmission parameters for the current transmission attempt while Priority-based MAC provides timing synchronization of the node [4]. The authors [4] also mention that Priority-based protocol's prioritization scheme introduces high transmission delay which can be catastrophic for time sensitive data while the History-based protocol reduces queueing delay at the cost of the dropped packets. Comparing the History-based MAC and the Priority-based MAC showed that the Priority-based method has greater PDR rate at the cost of greater queuing delay than the History-based scheme [4]. The quantitative results are obtained by the authors [4] using next simulation setup:

1. The two schemes under test are to experience fair packet arrival rate at the device buffer, and the packet transmission timing [4]
2. The regular/periodic phase pattern and the random phase pattern are used to emulate intra-vehicular network's traffic [4].
3. Each simulation session contains a regular phase during which packets arrive at the buffers at regulated intervals, and emergency phases during which packets arrive at the buffers at random intervals [4].
4. The α designates the fraction of the simulation time allocated for the emergency phase where α can be any value between 0 and 1 [4].
5. The packet delivery ratio (PDR) is used to quantify the packet drop severity [4].

Thus, these results are obtain for the History-Based MAC and Priority-based MAC:

Table I. The PDR results of the History-Based MAC [4]

Number of Nodes	PDR (%)		
	$\alpha = 0.25$	$\alpha = 0.4$	$\alpha = 0.55$
125	25.78	20	15.75
150	20.34	15.35	11.77
175	16.32	12.14	9.16
200	13.36	9.8	7.23
225	11.12	8.05	5.87
250	9.38	6.71	4.86

Table II. The PDR results of the Priority-Based MAC [4].

Number of Nodes	PDR (%)		
	$\alpha = 0.25$	$\alpha = 0.4$	$\alpha = 0.55$
125	61.97	48.6	34.13
150	47.78	36.62	24.79
175	40.22	30.73	18.62
200	32.75	23.7	14.87
225	28.42	20.33	12.5
250	25	17.09	10.5

From the Table I above, the best results are obtained when PDR is equal to 25.78% at α is set to 0.25 when 125 nodes are present in the network. Thus, the History-Based MAC performs the best when the number of nodes present in the network is the lowest and the packets arrive in the regular and periodic manner.

The data presents in Table II above indicates that the best results are obtained when PDR is equal to 61.97% at α is set to 0.25 when 125 nodes are present in the network. Thus, the Priority-Based MAC performs the best when the number of nodes present in the network is the lowest and the packets arrive in the regular and periodic manner.

By comparing the data above provided for each protocol, the Priority-based MAC Protocol outperforms the History-based MAC in terms of the best achievable PDR.

Next, the authors [4] calculate the queueing delay as the difference in enqueueing time and dequeuing time. The resultant data is shown in figure below:

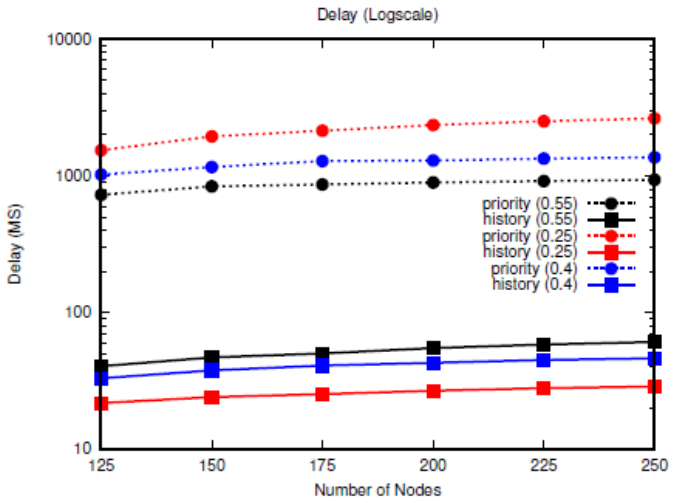

Figure 2. The queueing delay of the History-based MAC and Priority-based MAC protocols [4].

The data presented in the figure above indicates that the History-based MAC Protocol yields lower queueing delay than the Priority-based Protocol thus outperforming it.

The authors [4] conclude that while the Priority-based MAC Protocol yields higher PDR rate, it does so at the cost of higher queuing delay.

SECTION IV. SECURITY WITHIN THE APPLICATION LAYER

While some authors suggest that implementing IP and Application layers is unfeasible in the intra-vehicular networks due to the time sensitivity of the system [1], other authors [5] propose network security means by implementing a network architecture based on the Host Identity Protocol (HIP) [5], [6] which provides protections from the IP level attacks. It should be noted that while the part of the intra-vehicular network requiring real-time performance may not implement IP and Application Layers or even be on the wireless network at ll, the networks responsible for passenger information services, public announcements, video surveillance, intercom, HVAC, and broadband services may take advantage of the added security in these Layers [5].

The proposed security methods address the issues found in open air transmission which may expose the control and user traffic to an attacker who is attempting to alter or jam the control data [5]. The proposed architecture utilizes OpenHIP implementation and its security features as [5], [6]:

1. Authentication.
2. Confidentiality.
3. Message freshness.
4. Integrity.

The authors [5] utilize the above features to prevent attacks at the IP level. The proposed architecture is tested by the authors in the ski tunnel which yielded an acceptable throughput with the range up to 200 meters without utilization of a repeater while averting the IP Based attacks. The proposed architecture divides the wireless communication into the high priority controlling traffic, and low priority data plane used for user data. The proposal [5] assumes the network security is to be implemented at the wireless interfaces as shown in the figure below:

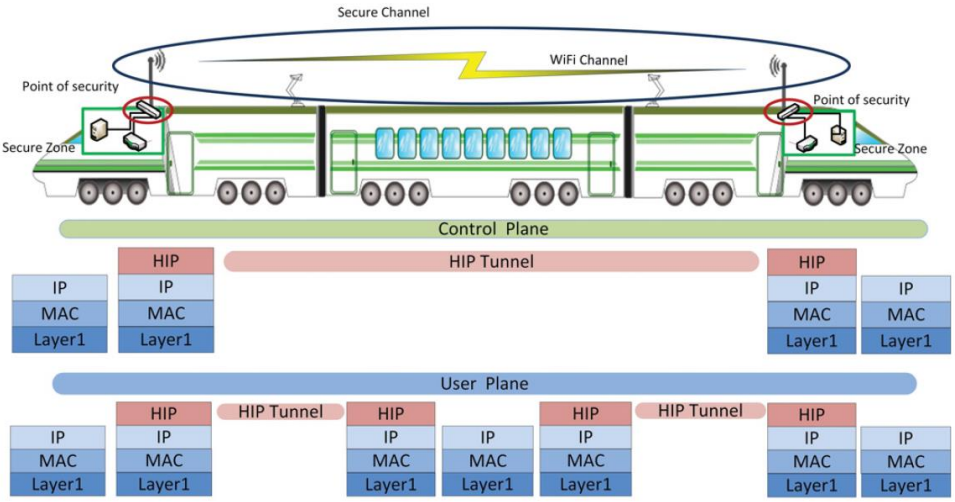

Figure 3. Network Topology, security points, and the proposed protocol stack are shown [5].

Inside the Secure Zones, the hosts do not require protocol modifications at the nodes, and the proposed architecture transfers the traffic between the secure zones over the air. The proposed architecture provides security for the traffic traveling between the secure zones. These two mechanisms are utilized by the proposed architecture:

1. Tunnel Establishment which starts with HIP key negotiation exchange and forming of the HIP Tunnel.
2. Address Learning Mechanism: responsible for traffic routing and forwarding tables accumulation. Authors suggest using dynamic address learning mechanism instead of using static configurations.

Using TCP Reset Attack in which the adversary attempts to terminate the TCP connection by sending a spoofed TCP packet with the reset field set to 1, the proposed network architecture was tested for the throughput. These results are provided by the authors [5]:

Table III. The average throughput of the experiment [5].

	Scenario	Average Throughput (Kbps)
Case 1	Without security and without attack	65562
Case 2	Without security and with attack	1724
Case 3	With security and without attack	45409
Case 4	With security and with attack	45439

The data provided in the table above indicates a throughput penalty of 30% due to proposed security architecture.

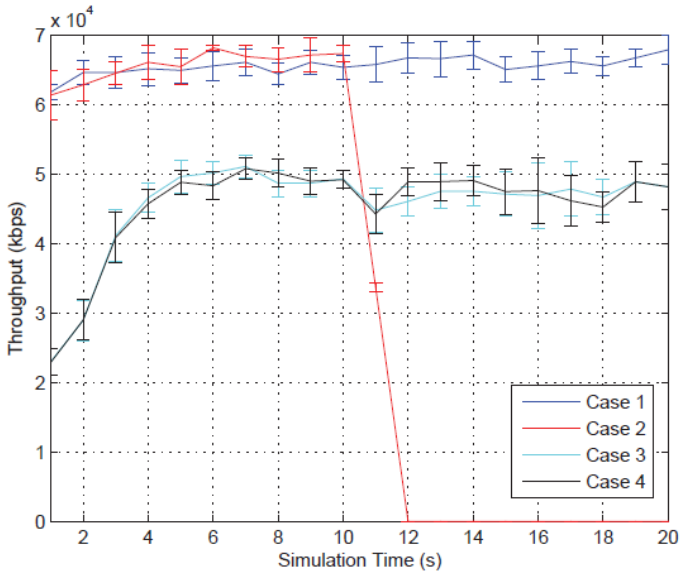

Figure 4. The average throughput over the time [5]

However, using the data shown in Figure 4, we can see that the proposed architecture maintains constant throughput even under attack while the same system without security implementation has its throughput dropped to 3%.

SECTION V. CONCLUSION

This survey paper covers the inter-vehicular wireless networks at multiple layers starting with the PHY level and concluding with the security considerations at the IP Layer implemented in the Application Layer. It was determined that UWB communication protocol offers significant improvements over other protocols within the PHY Layer. It is also observed that while the Priority-based MAC Protocol yields higher PDR rate, it does so at the cost of higher queuing delay. Additionally, the suggested security architecture implemented in the Application layer offers consistent performance at the cost of reduced throughput by 30%.

REFERENCES

[1] M. Ahmed, C. U. Saraydar, T. Elbatt, J. Yin, T. Talty, and M. Ames, "Intra-vehicular Wireless Networks," 2007 IEEE Globecom Workshops, 2007.

[2] J.-R. Lin, T. Talty, and O. K. Tonguz, "An empirical performance study of Intra-vehicular Wireless Sensor Networks under WiFi and Bluetooth interference," 2013 IEEE Global Communications Conference (GLOBECOM), 2013.

[3] W. Niu, J. Li, and T. Talty, "Intra-Vehicle UWB Channel Measurements and Statistical Analysis," IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference, 2008.

[4] I. F. Kurniawan, M. A. Rahman, A. T. Asyhari, and M. Z. A. Bhuiyan, "Performance Evaluation of History-Based and Priority-Based MAC for Traffic-Differentiated Intra-Vehicular Network," 2018 IEEE 16th Intl Conf on Dependable, Autonomic and Secure Computing, 16th Intl Conf on Pervasive Intelligence and Computing, 4th Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech), 2018.

[5] M. Liyanage, P. Kumar, S. Soderi, M. Ylianttila, and A. Gurtov, "Performance and security evaluation of intra-vehicular communication architecture," 2016 IEEE International Conference on Communications Workshops (ICC), 2016.

[6] T. Henderson and A. Gurtov, "The Host Identity Protocol (HIP) Experiment Report," RFC 6538, IETF, March 2012.