Performance and Security Evaluation of Intra-Vehicular Communication Architecture

Madhusanka Liyanage*,[1], Pardeep Kumar[2], Simone Soderi[1,3], Mika Ylianttila[1], Andrei Gurtov[4]
[1] Centre for Wireless Communication (CWC), University of Oulu, Finland
[2] Department of Computer Science, UiT The Arctic University of Norway, Norway
[3] Alstom Signalling Solutions, Italy.
[4] Helsinki Institute for Information Technology (HIIT), Aalto University, Finland and ITMO University, Russia.

***Abstract*—In this paper, we propose a secure intra-vehicular wireless communication architecture based on Host Identity Protocol (HIP). It ultimately improves the security of wireless intra-vehicular communication systems. The performance evaluation of the proposed architecture is performed in a ski tunnel which emulates the real underground transportation environment. Our results verify the feasibility of proposed architecture by providing required level of service quality. Also, it outperforms the existing secure architectures. More importantly, the proposed architecture protect the wireless intra-vehicular communication system from IP based attacks.**

***Index Terms*—Security, Intra-Vehicular Communication, HIP, IPsec, Smart-spaces, information sharing**

I. Introduction

The intra-vehicular communication plays an important role in public and cargo transportation systems (e.g., trains, trams, metros, articulated buses, cruises and cargo ships) to ensure safety and stable operation of the vehicle. Initially, intra-vehicular communication systems were used only for signaling and controlling purposes. However, recent communication systems support many passenger assisting applications such as passenger information services, smart spaces, public announcements, video surveillance, intercom, HVAC (Heating, Ventilation, and Air-Conditioning), broadband services and data-driven control systems [1].

In the present day, most of the intra-vehicular communication systems are operated as wired communication systems. A conventional wired intra-vehicle communication system relies on wired lines which are laid along vehicle body and interconnecting couplers. However, physical wires are cumbersome to install, maintain and troubleshoot.

Furthermore, wired systems have fixed bandwidths, limited data rates and limited number of ports. It cannot be expanded without reinstalling wires across the vehicle. Thus, a wired communication system is expensive and infeasible to upgrade to accommodate future demands.

On the other hand, the use of wireless technologies for intra-vehicular communication is an economical, expandable and user friendly alternative to the wired communication systems. Available wireless technologies and new trends for intra-vehicular wireless communication are discussed in [1]. In [2], authors conducted a survey on wireless techniques which are used in the railway industry. An analysis of security requirements and types of threats to a vehicular communication system are presented in [3]. Furthermore, new intra-vehicular wireless communication systems are proposed by several research articles [4] [5] [6].

However, the existing architectures are still unable to address security challenges in wireless intra-vehicular communication systems. Specifically, the open air transmission is exposing the control and user traffic to third party attackers. Especially, an alternation or an interruption of the control data may result in compromising the safety and the smooth operation of the vehicle. Therefore, security becomes a critical issue in the wireless intra-vehicular communication which is not yet properly addressed.

- Our Contribution

In this paper, we propose a secure intra-vehicular communication architecture which solves security related issues in a wireless intra-vehicular communication system. The proposed architecture exploits security features such as authentication, confidentiality, message freshness, and integrity. We discuss the security features of the proposed architecture and system implementation aspects. The solution is implemented based on OpenHIP implementation [7] which is an open source implementation of HIP. Then, it is tested in a ski tunnel which is close to the real world transport environment (i.e., railway tunnels and underground roads) to identify the performance penalty of security. More importantly, we mount several real-time attacks and analyze the impact of attacks on the proposed architecture.

The rest of the article is organized as follows. We briefly introduce intra-vehicular communication, security requirements and issues of existing systems in Section II. The proposed architecture is presented in Section III. The experiment results are illustrated in Section IV and V. We discuss the security assessment of the proposed architecture in Section VI. Finally, Section VII concludes the research and summarizes the important findings.

Project co-funded by the Tuscany Region and European Community under the 2007-2013 POR CREO FESR program, Tekes, Finland under Naked Approach and SIGMONA projects and the Russian Foundation for Basic Research, research project # 14-07-00252

*Corresponding author. Email: madhusanka@ee.oulu.fi

978-1-5090-0448-5/16/$31.00 ©2016 IEEE

II. The Security Analysis of the Intra-Vehicular Communication System

A. Security Threats in The Wireless Intra-Vehicular Communication System

Although the wireless communication provides a wide range of advantages, it is well known that the wireless channels are vulnerable to various security threats. On the other hand, safety and security are indispensable factors for public transportation systems, since the intra-vehicular data (i.e., vehicle controlling and signaling, public announcements) are very sensitive and may motivate many cyber attackers as well as corrupt persons and individual competitors.

For example, an attacker who boards to the vehicle with a high configuration laptop can intentionally perform various attacks on the intra-vehicular communication system and can disturb the operation of the vehicle. We categorized these attacks as:

1) Eavesdropping Attacks: The intra-vehicle data highly vulnerable for eavesdropping attacks as they transmit data over wireless channels and these channels are not confined within the range. As a result, an attacker can easily eavesdrops open air messages (i.e., sensitive control signals) using their own devices (laptop) and can use these data for various attacks. For instance, the attacker can generate fake hazard warnings by using the eavesdropped data to create an expected panic among the passengers or the crew.

2) Man-in-the-Middle (MitM) Attacks: In a MitM attack, an adversary may act as a middle person in the control/signal channel between two ends of the vehicle and performs following attacks

- Insert false messages into the wireless channel.
- Intercept and alter the signal data during the communication.

Any spurious messages injection into the signaling and control system could cause emergency break-downs, unexpected travel delays or may affect the vehicle speed. Furthermore, an attacker may capture some messages from the communication and replay them again and again, which could continue to send commands to controller devices in order to cause an undesirable event while the crew remains unaware of the true state of the vehicle.

3) Denial of Service (DoS) Attacks: An attacker can insert excessive amount of fake messages to the intra-vehicle communication system in an attempt to consume most of the network resources. As a result, the system will be unresponsive to legitimate traffic. For instance, SYN (Synchronize) and UDP flooding attacks can be mounted in intra-vehicle communication environment. Such DoS attacks may result in the break-down the whole control and signaling traffic transportation. Consequently, unexpected emergency break-downs and system failures may occur.

B. Weaknesses and Vulnerability of the existing Wi-Fi based Intra-Vehicle Communication Systems

Most of the existing wireless intra-vehicle communication systems are based on Wi-Fi systems [1] [2] [3] [5]. Hence, we tentatively analyze security features of existing Wi-Fi security protocols. The existing Wi-Fi security protocols such as Wired Equivalent Privacy (WEP), WEP+, Wi-Fi Protected Access (WPA), and WPA2 provide weak security services such as key management, authentication, encryption, and integrity.

WEP is vulnerable to replay attack, packet forgery attack, weak initialization vector (IV) and the lack of key management; and hence it is considered completely dead protocol in terms of security [8] [9] [10]. WEP+ is a proprietary enhancement over WEP. However, it is also susceptible to replay attacks. WPA came with the purpose of solving security problems in the WEP protocol. WPA provides authentication, confidentiality, freshness, and integrity. It is secured against forgery attack, replay attack and weak initialization vector. Moreover, it provides rekeying mechanism that defeats the key collision attack. In 2003, it is found that WPA is susceptible to the brute-force dictionary attack. Moreover, Takehiro Takahashi designed a WPA cracker tool which can easily reveal the keys from the wireless communication in late 2004 [11]. Finally, WPA2 is considered as a future of wireless network access. It provides user authentication, wireless network authentication, key distribution and pre-authentication in a mobility environment. However, WPA2 also subjects to vulnerabilities such as message spoofing and no protection against denial-of-service (DoS) through 802.11 violations, de-authentication and de-association [8].

As existing Wi-Fi security protocols have major weaknesses and not secure enough to prevent many security attacks, the use of Wi-Fi based systems without an extra secure mechanism can cause major consequences for real-time applications.

C. Security Requirements of the Intra-Vehicular Communication System

Security of an intra-vehicular communication system needs to consideration from the very beginning of architecture design. Otherwise, the whole communication system will be vulnerable and many human lives may put in a great risk. In order to make the intra-vehicle communication system as robust as possible, there is a need to implement various security services including: authentication, confidentiality, integrity and availability.

Authentication ensures the communication only between legitimate persons/equipments, i.e., no impersonation of legitimate host equipment's and no data forgery occurs. Confidentiality ensures that wireless intra-vehicular communication is not compromised, i.e., no eavesdropping and theft on wireless packets during the communication. Integrity ensures that the wireless data is not altered in transit, i.e., no message modification is taken place while wireless packets are in transit. Availability ensures that system is protected from interruption such as flooding target machine with bogus requests and disruption of control signaling.

III. Security Abstraction Layer

In this paper, we propose a HIP based bump-in-the-wire network level security architecture to secure the intra-vehicular communication. HIP is an emerging key negotiation and mobility protocol that enables IPsec security, host mobility and multihoming across different address families (IPv4 and IPv6). It also provides the end-to-end data encryption and mutual authentication [12].

A. Description of the Proposed Architecture

We define two communication planes as the control plane and the data plane. The control plane transports the signaling/controlling traffic which has the highest priority. Usually, it carries the operational and maintenance data of the vehicle. The data plane transports the user data which has a lower priority than the control traffic. It carries users' broadband, multimedia and non-controlling traffic. Figure 1 shows the protocol stack of the proposed solution.

Here we assume that the control data exchange occurs only between head and tail of the train while user data exchange all over the train.

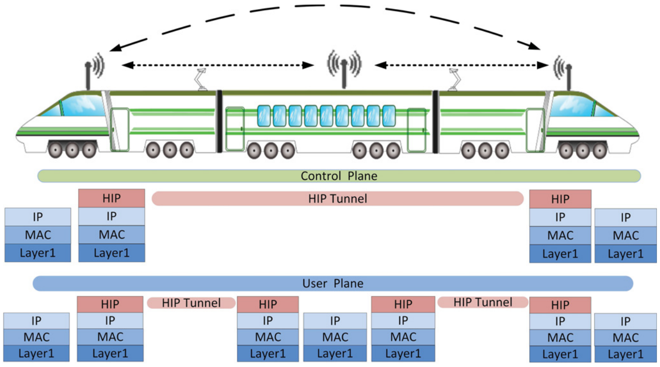


Fig. 1: The protocol stack of the proposed architecture

The basic idea of our proposal is to provide the network security in network elements as close as possible to wireless interfaces. The network topology and points of security can be seen in Figure 2. It is only illustrating the secure control data plane of the above scenario. These points of security devices can be switches, routers or other wireless devices.

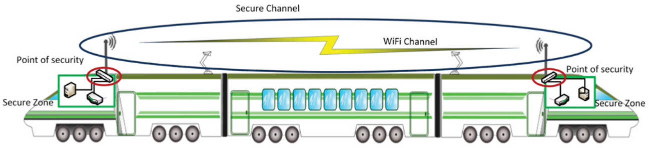


Fig. 2: The network topology and the point of security deployment

In Figure 2, the point of security is the place where HIP is implemented. The internal network which lays behind points of security are secure zones in the network. We assume that intruders do not have access to these security zones. HIP is utilized in two points of security in such a way that the security is completely transparent to other network elements and hosts inside secure zones and requires no protocol modifications at user nodes. Between two secure zones and their respective networks, packets arrive and leave as if they are normally physically connected with each other. Moreover, it is possible to implement multiple secure zones according to the requirements of the vehicle. Our architecture securely transfers the traffic between these secure zones.

The secure communication of the proposed architecture is explained in two sections; tunnel establishment and address learning mechanism.

1) Tunnel Establishment: Upon start-up, each two points of security perform HIP key negotiation exchange and form a HIP Tunnel between each other. A HIP tunnel is IPsec BEET (Bounded End-to-End Tunnel) tunnel. A four-steps Base Exchange (BEX) procedure was proposed to establish these HIP tunnels [13]. We modify the HIP BEX to establish HIP tunnels between points of security and the modified HIP BEX is illustrated in Figure 3. We use the same terminology which was used in [12] [13].

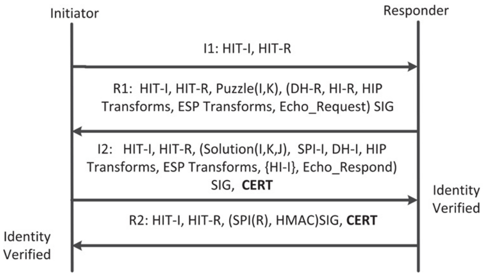

Initiator
Responder
I1: HIT-I, HIT-R
R1: HIT-I, HIT-R, Puzzle(I,K), (DH-R, HI-R, HIP Transforms, ESP Transforms, Echo_Request) SIG
I2: HIT-I, HIT-R, (Solution(I,K,J), SPI-I, DH-I, HIP Transforms, ESP Transforms, {HI-I}, Echo_Respond) SIG, CERT
Identity Verified
R2: HIT-I, HIT-R, (SPI(R), HMAC)SIG, CERT
Identity Verified

Fig. 3: The modified HIP Base Exchange

As part of the authentication process of the HIP BEX, two points of security derive a common key material for IPSec traffic by using the Diffie-Hellman (D-H) key exchange. In addition, end points mutually authenticate each other during HIP BEX. We propose to exchange a certificate to allow the communication with each other. Initially, the network administrator provides a certificate for each node during the node configuration process. However, it is possible to automate the distribution of these certificates by using an authentication server. On the other hand, this certificate contains the configuration information of Virtual Private Networks (VPNs) such as traffic prioritization informations, VPN IDs. We propose to exchange encrypted certificates. Hence, an eavesdropper can not extract the configuration information of VPNs. If the HIP BEX successfully completes, then the two ends can securely transport traffic between two secure zones over insecure wireless interfaces/channels.

On the other hand, the proposed architecture can be implemented either as a Layer 2 VPN (L2VPN) or a Layer 3 VPN (L3VPN) based on the deployed network devices in the network. The incoming traffic differentiates based on VPN ID in L2VPNs and UDP (User Datagram Protocol) port in L3VPNs [14].

2) Address Learning Mechanism: It is possible to implement several security zones in a single vehicle. However, an address learning mechanism is needed to build forwarding tables and route the traffic between these security zones. We propose to use dynamic address learning mechanism between the points of security. A point of security is the responsible entity for all devices which are placed in its security zone. Hence, each end point maintains a forwarding table to map the address of a device to the address of the responsible point of security. If an end point receive frame with unknown address, it broadcasts a dynamic address request to all security zones and retrieves the address of the corresponding point of security.

IV. The Performance Penalty of Security

The proposed architecture is tested in real world environment. The basic purpose of this experiment is to investigate the impact of security on performance and to identify the feasible range. The range is defined as the distance between the transmitter and the receiver. A ski tunnel which is located at Vuokatti, Finland is used to characterize a transport environment [15]. Either it can represent a tunnel in a train, metro or articulated bus line or a indoor passage in a cruise, ship or train. As shown in Figure 4, the length, height and width of the tunnel is 1.2 km, 4.0 m and 8.0 m respectively. The temperature inside the tunnel is -5 to -9 C year-round.

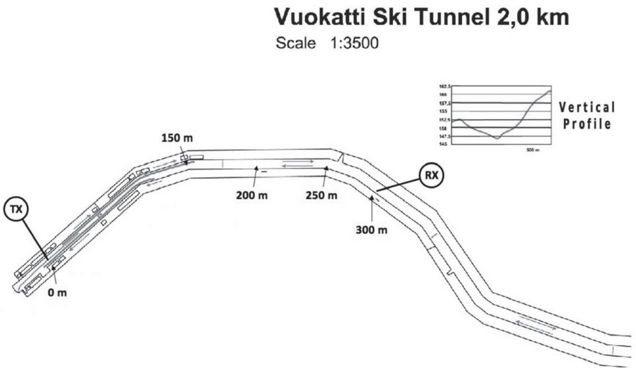


Fig. 4: Vuokatti Ski-tunnel map and the placement of devices

There are three test bed setups used for the experiment. In the first setup, two end nodes and two users are used. In the second setup, we added a third end node as a repeater. In the third setup, we check the performance of our system with the existing Tofino end boxes system [16]. Each end node has an AMD (Advanced Micro Devices) Geode LX processor with the clock speed of 433 Mhz, a cache of 256 KB, a 256 MB DDR SDRAM (Double Data Rate Synchronous Dynamic Random-Access Memory) and two antennas. These nodes are capable of transmitting and receiving the IEEE 802.11n WiFi signals. The IPERF network testing tool [17] is used to generate the UDP traffic stream between the end users.

A. Two end node scenario

Two end nodes used for the first scenario and the test bed setup is illustrated in Figure 5. We test the performance of the system with the proposed security architecture and without it.

Two traffic cases are measured during this experiment. In the first case, we use a single UDP traffic stream with a bandwidth of 10 Mbps to represent the signaling traffic. In the second case, we use two UDP traffic streams with a bandwidth of 10 Mbps and 54 Mbps to represent the signaling and non-signaling traffic respectively. We measure the throughput and jitter at the range of 200 m and 300 m for both cases.

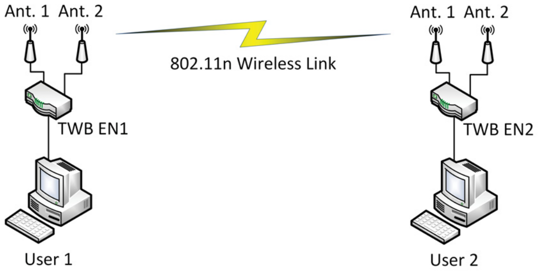


Fig. 5: Test bed setup for the two end nodes scenario

1) The impact on throughput: Figure 6 illustrates the average throughput for each case.

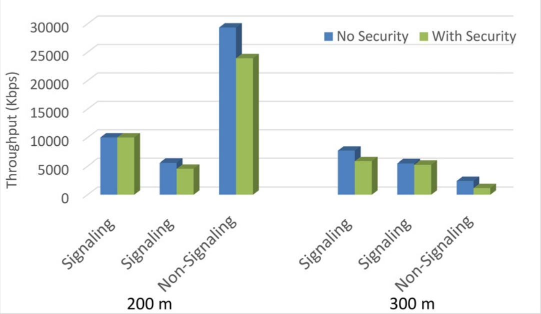


Fig. 6: The average throughput for the two end nodes scenario

Experiment results indicate that there is a throughput penalty due to the security. The percentage throughput reduction is compared with the maximum achievable throughput without security for each case. When we consider the single stream case, the throughput reduction is zero at the range of 200 m and it increases up to 24% at the range of 300 m. In the dual stream case, both signaling and non-signaling secure traffic have a throughput reduction of 18% at the range of 200 m. However, it decreases up to 4% for the secure signaling traffic and increases up to 52% for the secure non-signaling traffic at the range of 300 m. Hence, we can conclude that the security penalty on throughput is increasing with the increment of the range.

2) The impact on jitter: Figure 7 illustrates the average jitter for each case.

The experiment results indicated that the security penalty on jitter is almost zero at the range of 200 m. The proposed solution also has better performance for the single stream case. Although the security penalty on jitter is increased at the range of 300 m, still it varies in a range of 2 ms. Hence, we can conclude that the increment of the range increases the security penalty on jitter. However, the impact is less significant for both cases.

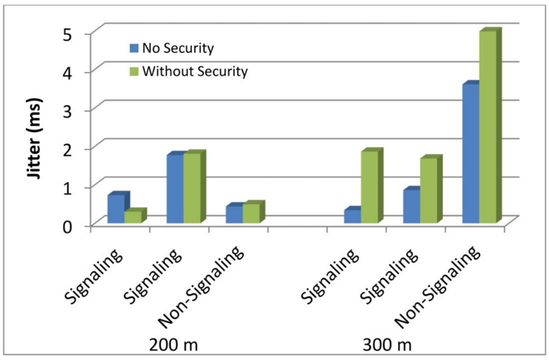


Fig. 7: The average jitter for the two end nodes scenario

B. Three end node scenario

Three end nodes used for this scenario and the test bed setup is illustrated in Figure 5. We measure the performance at the range of 300 m. The repeater is placed at the middle point of the range i.e., 150 m from each end node.

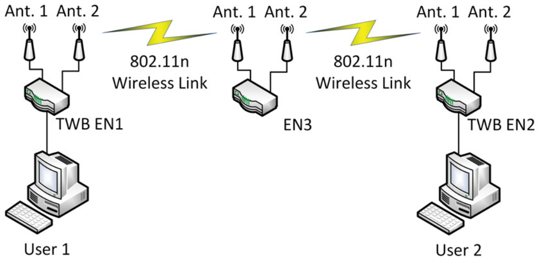
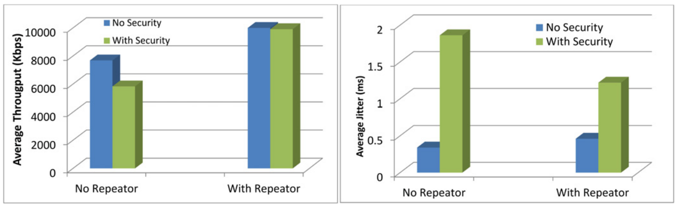


Fig. 8: Test bed setup for the two end nodes scenario



(a) The impact on throughput

(b) The impact on jitter

Fig. 9: Performance Evaluation of three end nodes scenario

The experiment results (Figure 9a) indicate that the throughput penalty due to the security is around 24% in range of 300 m without a repeater. However, we observe only a throughput penalty of 1% with a repeater. Hence, we can conclude that a repeater not only increases the average throughput but also reduces the throughput penalty due to the security.

The experiment results (Figure 9b) indicate that the presence of a repeater increases the jitter in no-security scenario and decreases the jitter in the proposed security scenario. However, the different of jitter is still below 1.5 ms.

C. Tofino End Boxes Scenario

The next step of the experiment is to compare the proposed system with the existing HIP based security mechanism. Tofino boxes provide a hardware platform that enables zones based security on Control and Supervisory Control and Data Acquisition (SCADA) networks [16]. Basically, they use HIP-based Virtual Network LAN Service (HIPLS) architecture [18], [19]. We compare Tofino end boxes which are currently used by the Boeing company to secure their airplane production line [20]. We check the applicability of a Tofino end box based security mechanism for the intra-vehicle communication. The impact of security on throughput is investigated in this experiment. The test bed setup illustrates in Figure 10. We set the range into 250 m and compare the performance.

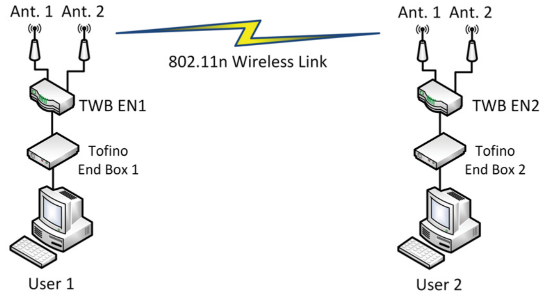
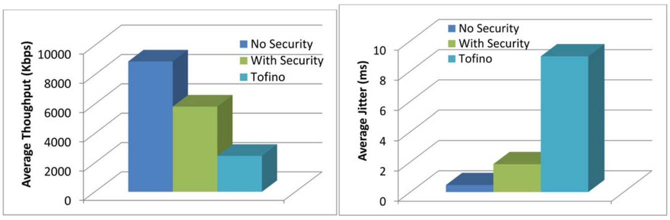


Fig. 10: Test bed setup for the Tofino end boxes scenario



(a) The impact on throughput

(b) The impact on jitter

Fig. 11: Performance Evaluation of Tofino end boxes scenario

The experiment results (Figure 11a) clearly indicate that the proposed solution has only a throughput reduction of 33% while Tofino implementation has a throughput reduction of 76%. It concludes that our proposed architecture is able to outrun the Tofino Implementation in terms of the throughput reduction.

Moreover, we can observe (Figure 11b) that the excess amount of jitter is less than 1.5 ms for the proposed solution while Tofino implementation has 8.5 ms of excess jitter. It concludes that our proposal able to outrun the Tofino Implementation and provide almost similar jitter as the non-secure architecture.

V. The Protection from IP based Attacks

A. The protection from TCP reset Attacks

TCP reset attack is a common attack scenario in IP networks. It is also known as “forged TCP resets” or “spoofed

TCP reset packets”. Each TCP packet header contains a flag called “Reset” (RST) flag. This flag is used by an end user to notify the events of failure to other user in a TCP connection. In an event of failure, a user set the RST flag to “1” on a TCP packet and send it to other user. Upon the arrival of the packet, other user terminates the TCP connection. Hence, the reset flag is set to zero in the normal mode of operation.

An attacker can eavesdrop the ongoing stream of TCP packets and extracts the TCP header information. Then, the attacker generates forged TCP packets with reset bit set to “1. These forge TCP packets contain a convincing TCP header information which were eavesdropped from legitimate TCP packets. Thereafter, the attacker injects these forge packets in to the communication channel. It is comparably easy to inject and eavesdrop the packets on a wireless channel than a wired network. If end users cannot identify these forge packets, they falsely terminate the TCP connection. Properly formatted forged TCP resets are a very effective way to disrupt any TCP connection as long as the absent of a suitable security mechanism.

This section contains the performance of the proposed intra-vehicular architecture under the TCP reset attack event. We mount a TCP reset attack to the test bed and measure the throughput of the system for with and without security scenarios. Figure 12 illustrates the test bed setup for the experiment.

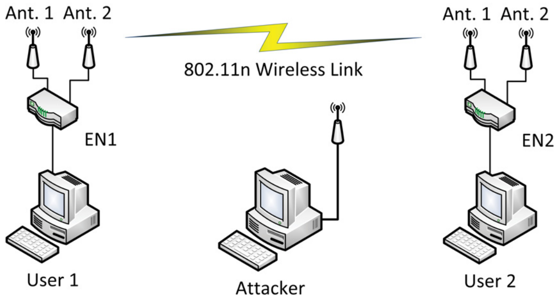


Fig. 12: Test bed setup for the TCP reset attack scenario

The TCP traffic stream between the end nodes is generated by using the same IPERF network testing tool [17].

The experiment contains four cases. The throughput of each scenario is measured and table I contains the average throughput of experiments. We send the IPERF traffic for 20 s and place the attack for last 10 s for the case 2 and 4.

TABLE I: The average throughput of the experiments

	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

When we consider the non-attacking cases (case 1 and 3), the average throughput of the non-secure scenario has 30% of higher throughput than the secure scenario. Hence, the security penalty on throughput is 30% for this test bed setup. However, the proposed system still manages to provide the same throughput even under TCP reset attack while the throughput of the non-secure architecture is reduced by 97%.

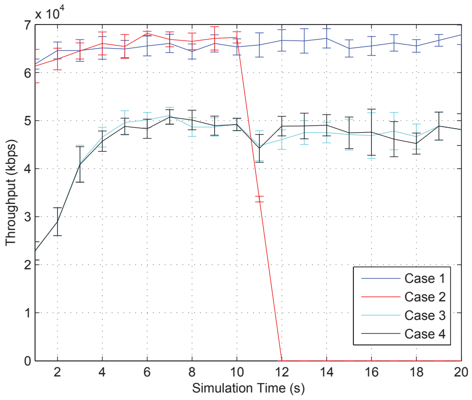


Fig. 13: Average throughput over the time

Figure 13 illustrates the average throughput variation over the simulation time. The experiment result for case 2 clearly shows that the TCP attack can terminate the communication between end users, if there is no security. It reaches zero throughput and stays there for the rest of the attacking period. However, there is no throughput drop during the TCP reset attack for the proposed architecture. It has the same behavior as the non-attacking scenario. Hence, our proposal is capable enough to protect the communication channel from such IP based attacks.

VI. Security Assessment of the Proposed Architecture

The proposed architecture provides demanded security features for the intra-vehicular communication system; authentication, confidentiality, integrity and availability. Our architecture proposes to establish HIP tunnel prior to any data exchange between security zones. It has to follow a HIP BEX procedure. HIP BEX authenticates end users by using a public key authentication mechanism. Furthermore, the solution ensures that points of security do not accept any other traffic in the wireless interfaces than traffic from HIP tunnels.

As HIP is using the IPSec ESP (Encapsulating Security Payload) protocol [12], [13], points of security do not forward out anything else but authenticated ESP packets which provides the protection against information snooping on the wireless link. Furthermore, it provides the confidentiality for both user and control traffic. In general an end-to-end security mechanism, the headers, addresses, routing, and trailer information are not encrypted. It allows attackers to learn more about captured packets and where it is headed. However, the proposed bump-in-the-wire approach mitigates this and reveals no information whatsoever about headers, addresses, and routing of secure zones. On the other hand, HIP tunnels also provide the inbuilt integrity of IPsec for the data traffic.

Moreover, our proposed architecture prevents the possible attacks in the intra-vehicle communication system. The results from our implementation have verified this fact and it secures the availability of the system. HIP tunnels provide the security against IP/TCP based attacks. In [21], [22], authors illustrated the simulation results for the protection provided by HIP tunnels against TCP SYN flood and TCP reset attacks.

The proposed architecture provides the end-to-end security at the network layer instead of hop-to-hop MAC layer security. To compare the lower layer security, in the link layer key distribution and management are more complex because each hop device must receive a key, and when keys change, each must be updated [14]. This is naturally costly and time consuming operation, and not feasible in the presence of several wireless devices or repeaters. Other weaknesses with layer 2 security include: (1) packets are decrypted at each hop; thus, more points of vulnerability exist, and (2) dependent on the physical and link layer networking technology (e.g. IEEE 802.11n).

The proposed security is implemented on the network layer with bump-in-the-wire gives more flexibility on the deployment of security features. User devices can be added, removed, and changed flexibly in the future without affecting the secure wireless link. Besides, the proposal is also independent of the physical and data link technologies of used radios. The radio technology can be changed later on without having a need to update the security on each link or go through cumbersome security audits for the new security technology that may come with it. On the other hand, proposal is not tied to applications; it is completely transparent to them.

Hence, the proposed HIP based approach provides a complete solution for networking and network security challenges inside the vehicle that can be further extended later on.

VII. Conclusion

The wireless communication is a promising method of communicating inside a large vehicle. It provides economic advantages and future expandability than existing wired systems. However, the wireless communication is considered as a less secure medium compared with a wired communication due to the open air transmission. On the other hand, security is an indispensable factor for larger public transportation systems such as trains, metro, cruises, trams, ships and buses. Hence, the security for such communication systems needs to be considered from the very beginning of system design.

In this paper, we proposed secure intra-vehicular wireless communication system based on Host Identity Protocol (HIP). It provides the required level of security by preventing common IP based attacks. We implemented the proposal and tested the performance in a ski tunnel to emulate the real environment of train, metro or bus underground transportation. Results suggest that:

1) Our proposal has an acceptable performance penalty of security in terms of throughput up to a significant range (Up to 200m without a repeater).
2) The presence of a repeater not only extends the range but also reduces the performance penalty of security.
3) The proposed architecture has outperformed existing HIP based products such as Tofino end boxes.
4) The proposed architecture successfully prevents the IP based attacks.

In future, we will conduct the experiments by moving the nodes in different speeds to evaluate the impact of mobility.

References

[1] P. Hsu, "The Future of Railway Wireless Communications Networks," Moxa Inc., Tech. Rep., 2010.

[2] G. Shafiullah, A. Gyasi-Agyei, and P. Wolfs, "Survey of Wireless Communications Applications in the Railway Industry," in *Wireless Broadband and Ultra Wideband Communications, 2007. AusWireless 2007. The 2nd International Conference on*. IEEE, 2007, pp. 65–65.

[3] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communication Systems: Design and Architecture," *Communications Magazine*, vol. 46, no. 11, pp. 100–109, 2008.

[4] Ahmed, Mohiuddin and Saraydar, Cem U and ElBatt, Tamer and Yin, Jijun and Talty, Timothy and Ames, Michael, "Intra-Vehicular Wireless Networks," in *Globecom Workshops, 2007*. IEEE, 2007, pp. 1–9.

[5] S. Steinberg and J. Varchmin, "Wireless Communication System for Train-Internal Communication," in *Wireless and Optical Communications*. ACTA Press, 2003.

[6] R. Kull and R. Klemanski, "Intra-Train Radio Communication System," 24 1998, uS Patent 5,720,455.

[7] OpenHIP, Open Source project implementing the HIP protocol. [Online]. Available: http://www.openhip.org.

[8] G. Lehembre. Wi-Fi security- WEP, WPA and WPA2. [Online]. Available: http://www.hsc.fr/ressources/articles/

[9] A. H. Lashkari and M. M. S. Danesh, "A Survey on Wireless Security protocols (WEP, WPA and WPA2/802,11i)," in *2nd IEEE international conference on Computer Science and Information Technology (ICCSIT)*, 2009.

[10] M. Juwaini, R. Alsaqour, M. Abdelhaq, and O. Alsukour, "A review on WEP Wireless Security Protocol," *Journal of Theoretical and Applied Information Technology*, vol. vol. 40, no. 1, pp. 39–43, June 2012.

[11] WPA Cracker tool. [Online]. Available: http://www.wpacrack.com/

[12] A. Gurtov, *Host Identity Protocol (HIP): Towards the Secure Mobile Internet*. Wiley, 2008.

[13] J. Okwuibe, M. Liyanage, and M. Ylianttila, "Performance Analysis of Open-Source Linux-Based HIP Implementations," in *10th IEEE International Conference on Industrial & Information Systems (ICIIS)*. IEEE, 2015.

[14] M. Liyanage, M. Ylianttila, and A. Gurtov, "IP-based Virtual Private Network Implementations in Future Cellular Networks," *Handbook of Research on Progressive Trends in Wireless Communications and Networking*, vol. 1, p. 44, 2014.

[15] H. Viittala, S. Soderi, J. Saloranta, M. Hamalainen, and J. Iinatti, "An Experimental Evaluation of WiFi-Based Vehicle-to-Vehicle (V2V) Communication in a Tunnel," in *Vehicular Technology Conference (VTC2013-Spring)*. IEEE, 2013.

[16] The Tofino Industrial Security Solution. [Online]. Available: http://www.tofinosecurity.com/

[17] Iperf. [Online]. Available: http://iperf.sourceforge.net/

[18] T. Henderson and D. Venema, S.and Mattes, "HIP-based Virtual Private LAN Service (HIPLS)," *Internet Draft*, nov 2012.

[19] M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "Secure Virtual Private LAN Services: An Overview with Performance Evaluation," in *IEEE ICC 2015 - Workshop on Advanced PHY and MAC Techniques for Super Dense Wireless Networks*. IEEE, 2015, pp. 10 297–10 303.

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

[21] M. Liyanage and A. Gurtov, "Secured VPN Models for LTE Backhaul Networks," in *Proc. of 76th Vehicular Technology Conference (VTC2012-Fall)*. IEEE, 2012.

[22] M. Liyanage, P. Kumar, M. Ylianttila, and A. Gurtov, "Novel secure VPN architectures for LTE backhaul networks," *Security and Communication Networks*, 2016.