Analysis of Realistic Attack Scenarios in Vehicle Ad-hoc Networks

Jan Lastinec
Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava (STU)
Bratislava, Slovak Republic
jan.lastinec@stuba.sk

Mario Keszeli
Faculty of Informatics and Information Technologies
Slovak University of Technology in Bratislava (STU)
Bratislava, Slovak Republic
xkeszeli@stuba.sk

***Abstract*— The pace of technological development in automotive and transportation has been accelerating rapidly in recent years. Automation of driver assistance systems, autonomous driving, increasing vehicle connectivity and emerging inter-vehicular communication (V2V) are among the most disruptive innovations, the latter of which also raises numerous unprecedented security concerns. This paper is focused on the security of V2V communication in vehicle ad-hoc networks (VANET) with the main goal of identifying realistic attack scenarios and evaluating their impact, as well as possible security countermeasures to thwart the attacks. The evaluation has been done in OMNeT++ simulation environment and the results indicate that common attacks, such as replay attack or message falsification, can be eliminated by utilizing digital signatures and message validation. However, detection and mitigation of advanced attacks such as Sybil attack requires more complex approach. The paper also presents a simple detection method of Sybil nodes based on measuring the signal strength of received messages and maintaining reputation of sending nodes. The evaluation results suggest that the presented method is able to detect Sybil nodes in VANET and contributes to the improvement of traffic flow.**

Keywords*— *V2V, VANET, Security, Attacks, Sybil Attack, OMNeT++

I. INTRODUCTION

Communication in vehicle networks is considered an important milestone in the development of Intelligent Transportation Systems (ITS) and safer vehicles capable of fully autonomous driving. Its importance lies within the full spectrum of reasons. Firstly, statistics indicate an ever-increasing number of vehicles on the roads across the globe. According to recent estimations [1], there are over 1.2 billion vehicles registered worldwide and this figure might double by the year 2040. Another serious issue is that approximately 1.25 million people die annually due to road accidents [2]. Even though the trend is decreasing, casualty figures are still alarming. Last but not least, the emergence of self-driving vehicles and increasing vehicle connectivity virtually asks for vehicles to be connected to each other, to be able to communicate and cooperate in a multitude of traffic situations. The cooperation is not limited only to vehicle-to-vehicle communication (V2V) but it is beneficial to extend it to other nodes (e.g. road-side infrastructure, pedestrians, etc.), collectively known as vehicle-to-everything communication (V2X). It is evident that the motivation for V2X communication increases, however there are still some unresolved issues that need to be addressed before it makes its way into production. One of the most crucial challenges is the effort to ensure secure communication and protect the privacy of driver and passengers.

Security of V2X communication is also critical in order to ensure road safety because wireless communication interfaces can be used as attack vector to gain remote access to in-vehicle networks [3]. There are multiple works demonstrating successful attacks on vehicle control systems once connected to vehicle's internal network [4, 5].

This paper is focused on security of V2V communication in VANETs. The aim of our work is to identify attack scenarios based on the analysis of security threats, implement those scenarios in the simulator environment, and evaluate security measures to mitigate the attacks. A key benefit of our work is the fact that we build upon a realistic and probable attacker's motivation which helped us understand the nature of likely real-world network attacks. We see the main contributions of our paper in the following points:

- Identification of three highly probable and specific attack scenarios that exploit the V2V communication mechanisms by broadcasting false information to other vehicles on the road: 1) Replay attack that aims to impersonate an emergency vehicle by re-broadcasting a previous message indicating its presence. 2) Message falsification attack that fabricates false message also with the aim to impersonate an emergency vehicle. 3) Sybil attack that creates virtual traffic-jams by spoofing counterfeit identities in the network and slows down the traffic.
- Design of novel, simple method for detecting Sybil nodes that is based on measuring the signal strength of received messages and does not require cooperation with other nodes.
- Proof-of-concept implementation of the identified attacks and proposed mitigation measures in simulation environment that proves the attacks' usability and

This research was partially supported by the Eset Research Centre and the Ministry of Education, Science, Research and Sport of the Slovak Republic, Incentives for Research and Development, Grant No.: 2018/14427:1-26C0.
978-1-7281-2827-6/19/$31.00 ©2019 European Union

confirms the ability of proposed security measures to mitigate the attacks.

The rest of the paper is structured as follows: Section 2 provides background information on VANET networks and their security. In Section 3 we describe the identified attack scenarios and possible mitigation measures including our Sybil detection proposal. Section 4 contains description of used method and the experimental evaluation, Section 5 contains the experimental results and their interpretation. The last Section concludes and discusses the findings.

II. Background

Vehicular ad-hoc network (VANET) is a mobile, wireless, self-organized network characterized by high mobility of nodes, dynamic topology and low latency demands [6]. Vehicles are almost constantly in motion at relatively high speed, whilst often travelling in the opposite direction, resulting in frequent network topology changes. New connections are regularly established with vehicles joining the network, while on the other hand nodes leave the network and connections are lost.

The technology behind the inter-vehicular communication is being formalized into standards – ETSI ITS-G5 [7] in the EU and IEEE 1609 (WAVE) [8] in the US. Both specify common physical layer based on standard IEEE 802.11p and both operate in 5.9 GHz radio frequency band. Their differences are becoming a little more obvious in the higher layers of the protocol stack, even though they are still somewhat similar in principle. Regarding the safety-critical applications, there are two types of messages defined in the application layer - periodical awareness messages and event-based messages. The former, referred to as BSM (Basic Safety Message) in the US standard and CAM (Cooperative Awareness Message) in the EU standard, respectively, carries basic information about vehicle state. Each vehicle broadcasts this message in short regular intervals. In contrast, the latter, known as BSM part II in the US and DENM (Distributed Environmental Notification Message) in the EU, is being sent solely in response to certain events. In addition to information about the event, it also includes a number of further vehicle parameters and data on past and predicted future position.

The problem of secure vehicle-to-vehicle communication is the subject of several research projects, therefore we chose only a fraction of the most notable ones. Current state-of-the-art works are funded pre-dominantly by the European Commission in the EU and by the National Highway Traffic Safety Administration (NHTSA), federal agency of the U.S. DoT. SeVeCom (Secure Vehicle Communication), which ran from 2006 to 2009, was among the very first research initiatives in this field. The project focused on identifying security threats and specifying security architecture of the inter-vehicular communication. SeVeCom addressed key and identity management, secure communication protocols including secure routing, device tamper-proofing and privacy issue [9]. Aforementioned NHTSA, in collaboration with the consortium of automakers associated in CAMP (Crash Avoidance Metrics Partnership) set similar goals for their VSC (Vehicle Safety Communications) programme. Under the proposed security architecture each message would include substantial overhead and the message signatures would take time to process once they are received. Authors also stipulate that the management of a public key infrastructure (PKI) for roadside units would be necessary [10]. Building on theoretical foundations laid by a number of existing projects, authors of PRESERVE (Preparing Secure Vehicle-to-X Communication Systems) program successfully managed to implement and field test security subsystem of the communication system [11]. Results from the research projects have also contributed to the development of security architectures present in ETSI ITS-G5 and IEEE WAVE standards. The security is based on digital signatures and PKI which can be used to provide security services needed to mitigate common attacks (e.g. message replay, falsification, or eavesdropping) [12].

III. Network Attacks

In this Section we firstly define the attacker model used in our analysis and then propose attack scenarios exploiting V2V communication in VANET. The scenarios are based on known types of attacks in VANETs.

A. Attacker Model

We consider the pursuit of personal benefit as the most likely driving force behind the attack, i.e. an attacker freeing the road for him/herself. The adversary is an external active attacker with the ability to modify the software of the on-board unit within his/her possession. We consider a mobile attacker whose position and speed can change in time. To execute an attack successfully, the adversary must be in the victims' communication range.

B. Replay Attack

Replay attack is a type of network attack in which the attacker listens to the communication channel and intercepts messages so that they can be rebroadcasted later. Utilizing this approach would allow attacker to impersonate an emergency vehicle (e.g. an ambulance) to free the road for him/herself. The scenario is as follows: attacker is following the emergency vehicle. Using BSM part II message, the emergency vehicle is notifying all vehicles in its communication range about its presence. Message is received by all vehicles in a close proximity including attacker's vehicle. While legitimate users being approached from behind by the emergency vehicle respond by decelerating and pulling over to the side of the road, attacker captures and resends the message originating from the emergency vehicle. Legitimate users respond as if it was another emergency vehicle. Attacker takes the advantage of free road lane. Furthermore, messages could be stored or shared with other attackers and consequently exploited repeatedly in the future.

C. Message Falsification

Message falsification is an attack in which the attacker modifies existing valid message and retransmits this falsified message. The attack scenario is similar to the scenario of replay attack, the only difference is that in this attack the attacker does not need the presence of the emergency vehicle

since he/she can modify any intercepted message or fabricate a completely new false message.

D. Sybil Attack

Sybil attack is an identity spoofing attack that is based on creating a forged identity in a network and misusing it for his needs. Sybil attack in VANET could be exploited to free the road by imitating a traffic jam. In this attack the attacker simulates several different counterfeit identities through which he/she disseminates status messages that give an impression of multiple standing or slow-moving vehicles. Upon receipt of those messages from counterfeit nodes fabricated by the attacker, legitimate user perceives inevitable traffic jam, hence responds by decelerating and remains in his/her current lane. The danger of this attack lies in the attacker being able to simulate complex traffic situations involving several vehicles which are, in fact, virtual, but perceived as real by legitimate users. Thus, victims could be navigated right where the attacker wants them to be. Sybil attack can be static or dynamic. Static Sybil attack generates counterfeit nodes (referred to as Sybil nodes) with fixed positions while the dynamic attack prepares Sybil nodes for each vehicle. For our scenario we have chosen the dynamic version of Sybil attack which is more efficient in achieving the attacker's goal. The scenario consists of several steps:

1) Monitoring of surroundings and collecting the periodic awareness messages in order to identify the victims.
2) Maintaining two lists that store the information about last known position of all victim vehicles and parameters of Sybil nodes for each victim.
3) Controlling the Sybil nodes. After receiving an awareness message, the attacker firstly checks if the corresponding sender is located before him/her. If the condition holds true (there is no sense to attack vehicles behind), the attacker evaluates if he has already a list of Sybil nodes for this vehicle. If yes, he can use them to further slow the vehicle down. In case of new vehicle the attacker proceeds with fabricating the Sybil nodes for it (i.e. broadcasting awareness messages simulating standing vehicles in front of the victim vehicle).

E. Mitigation Measures

Message falsification (modification) can be mitigated by signing the messages using the sender's private key and verifying at the receiving node using the sender's public key that is stored in his certificate. These secured messages guarantee integrity and authenticity of exchanged data. If the message is changed in transit, the signature of the message will not match and it will be ignored by the receiver. However, the proper management of revoked certificates is needed to prevent misuse of compromised certificates.

Replay attack mitigation involves checking the temporal validity of received messages. This can be achieved either by using sequence numbers or timestamps. We evaluated the timestamp method where two timestamps are added into each transmitted message – one specifies the time when message was sent and the other defines the validity period. Alternatively, it is possible to include only sending time and define the validity period locally at the receiving node. Each node is then responsible for verifying the validity of the messages. The drawback to this solution is that if the attacker manages to retransmit the message before its validity expires, replay attack will be successful. Furthermore, it is crucial to guarantee the integrity of messages because otherwise the attacker could simply modify the timestamp fields and prolong the validity period.

Current ITS standards do not define particular methods to mitigate Sybil attacks therefore we propose our own minimal and fast approach which is described in the following Subsection.

F. Detection of Sybil Nodes

The proposed approach for detecting Sybil attacks is based on the measurement of receiving signal strength and the distance of the sender. To map these two quantities, we used free space propagation model available in the used simulator. The values of signal strength and corresponding sender distance have been processed into a lookup table which is used to verify if the position announced by the sender matches the real position with relatively high precision. As can be seen from the Fig. 1, the detection of Sybil nodes is becoming less ambiguous with increasing distance from the attacker. The red values represent measurements with the presence of the attacker generating false identities and the blue values represent legitimate network nodes.

Each vehicle maintains a list of its active neighbours which is updated after every received awareness message. Each entry contains the information about one node: timestamp of the last update, position, speed, and reputation. The reputation is assigned based on how truthfully the node announces its position. The process of updating the list is depicted in the Fig. 2.

To maintain information only about active nodes, inactive entries in the list of neighbours are periodically removed every 100 milliseconds. The reputation is used within the process of active collision prevention which is used to maintain safe distance from the vehicle in front. The nodes with lower reputation than a set threshold are marked as false and are ignored in collision prevention calculations.

IV. Method

The presented attacks and mitigation methods have been evaluated in simulation environment. The simulation consists of mobility simulation and network simulation. We used the following simulators which are open-source:

- Mobility simulator – SUMO 0.30.0,
- Network simulator – OMNeT++ 5.2 with Veins 4.6 model for simulating VANET communication.

The computer code used to implement the simulations is available from the authors upon request.

Fig. 1. Dependence of signal strength and distance between sender and receiver with the presence of Sybil nodes (red).

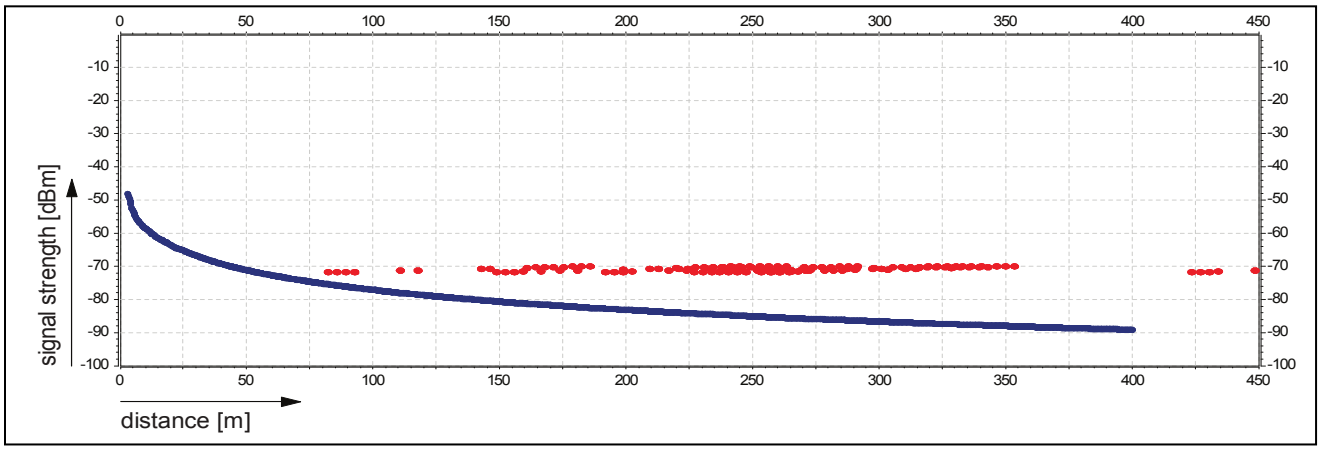
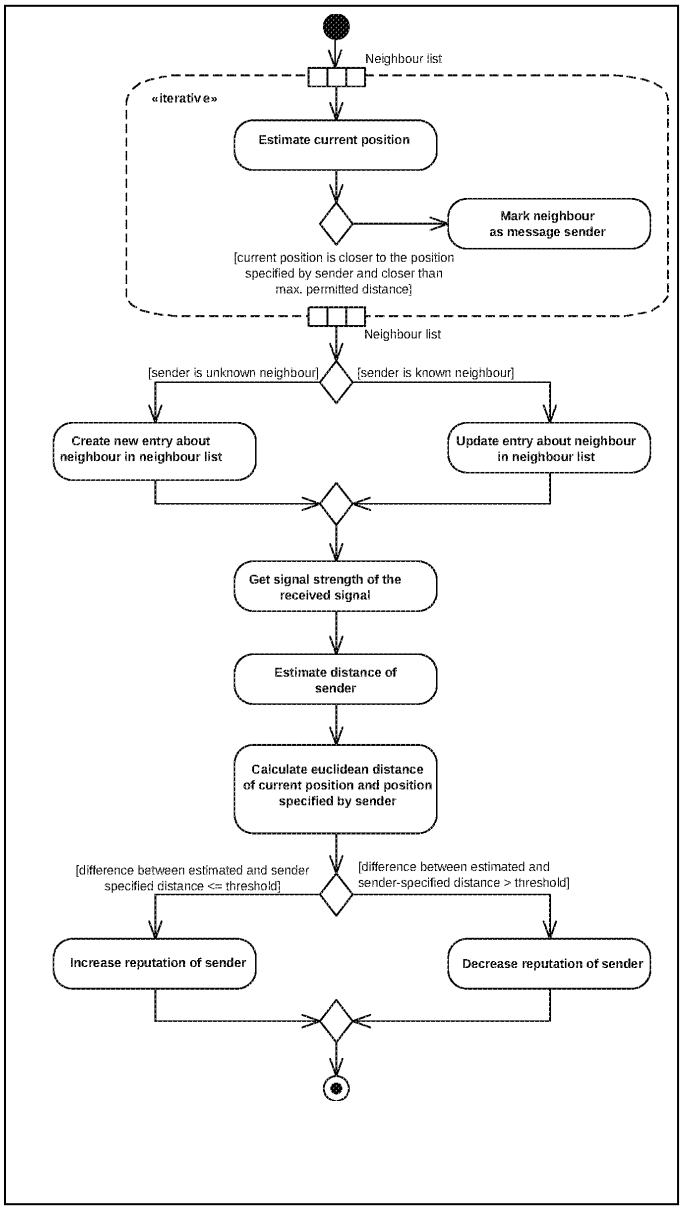


Fig. 2. Algorithm of updating neighbour list and node reputation.



A. *Simulation of Mobility*

The basis of mobility simulation is a section of highway road with two lanes and the length of 5000 m. Maximum speed is limited to 36.11 $m.s^{-1}$ (approx. 130 km per hour). There are three vehicle types that share the same route from the beginning to the end of the highway section. The movement of each vehicle is modelled explicitly. The simulation parameters are summarised in the Tab. 1.

B. *Network Simulation*

Network simulation consists of three simulation scenarios corresponding to the attacks presented in the previous Section. The simulation parameters are summarised in the Tab. 2. We are focused on evaluating the attack scenarios under the IEEE WAVE standard as it is currently the only supported standard of the VANET simulation framework (Veins). The source code of the Veins simulation framework has been extended to support presented attack and mitigation use-cases: two timestamps, certificates, and digital signatures have been added to Basic Safety Message; BSM Part 2 has been defined; application layers that define the behaviour of ambulance, attacker, and normal vehicles have been implemented.

C. *Evaluation Metrics*

The goals of evaluation for individual attack scenarios are different and therefore the evaluation metrics vary. In replay attack scenario, we monitored traffic-related metrics in order to evaluate if the attacker managed to slow down other vehicles and gain free road. Specifically we focused on the speed of vehicles and time taken to travel from the beginning to the end of the defined highway section. We also evaluated the bandwidth overhead of the mitigation method.

In message falsification scenario, we focused on evaluating the overhead of using digital signatures to secure messages. We compared the bandwidth and performance requirements for using ECDSA algorithm with 224-bit keys, which is preferred option across related literature, and RSA algorithm with equivalently strong 2048-bit key.

In Sybil attack scenario, we analysed the impact of Sybil attack and our mitigation method on the speed of vehicles and flow of the road traffic.

TABLE I. PARAMETERS OF SIMULATION OS MOBILITY

Parameter	Ambulance	Attacker	Normal car
Acceleration [m.s^{-2}]	2.0	4.5	2.5
Deceleration [m.s^{-2}]	7.0	10.0	8.0
Length [m]	6.0	4.8	4.5
Maximum speed [m.s^{-1}]	50.0	85	40
Speed factor	1.5	1.75	0.9
Speed deviation	0.1	0.1	0.05
Sigma	0.1	0.1	0.5

V. RESULTS

Replay attack. Attacker's speed during the replay attack is shown in Fig. 3. It can be seen that in the beginning of the simulation the attacker was moving slowly, however after the emergency vehicle has passed he quickly gained speed and became the fastest vehicle (blue line). On the other hand, after introducing the validity checking of the received messages the attacker's speed was significantly lower and the route took two times longer (red line). The validity checks do not affect the speed of the emergency vehicle. Regarding the overhead of adding the timestamp fields to messages it can be concluded that increase in bandwidth usage is practically negligible

Message falsification attack. This scenario was focused on impact of mitigation techniques using digital signature on network performance. In general, the periodic messages in VANET are broadcasted every 100 ms and after introducing the signing of these messages every node has to be able to sign one message in this time interval. Furthermore as a receiver, it has to verify the signature of every received awareness message in order to communicate with the nearby vehicles. This means that the overhead of two additional processes (signing and verification) and additional data increases the transmission time due to increased length of messages that include signatures and certificates. The communication delay with overhead of using digital signatures can be described as:

$$t_{delay} = t_{sign} + t_{transmit} + t_{verify} \quad (1)$$

The results of simulating the impact on transmission time indicate that the increase in transmission time due to including signature and certificate in messages is not critical (approx. 0.5ms for ECDSA and 1 ms for RSA). The time required for signing and verifying digital signatures depends on the performance of specific On Board Unit. In the simulation we used performance figures of Raspberry Pi board with BCM2837 @ 1.2 GHz CPU, 1 GB RAM, and Raspbian 4.1 OS. The signing and verification delays using openssl library are provided in the Tab. 3. Interesting finding to note is that verification using ECDSA takes significantly longer than in case of RSA. This is a little concerning because vehicles have to verify more messages (from all vehicles in communication range) compared to signing only their own messages before sending. On the other hand using RSA in scenarios with heavy traffic (such as in a city) can quickly overload the network and therefore ECDSA is the preferred algorithm.

TABLE II. PARAMETERS OF NETWORK SIMULATION

Parameter	Value
Network area	5500 x 500 x 50 m
Communication standard	IEEE 802.11p, MAC 1609.4
Carrier frequency	5890 MHz
TX Power	20 mW
Thermal noise	-110 dBm
Sensitivity	-89 dBm
Bitrate	6 Mbps
Header length	80 bits
Beacon interval	0.1 s

TABLE III. RSA AND ECDSA SIGNING AND VERIFICATION DELAY

Algorithm	Signing [ms]	Verification [ms]
RSA 2048-bit	22.737	0.599
ECDSA 224-bit	0.800	3.000

Sybil attack. The Fig. 4 shows the speed of the attacker during the Sybil attack scenario. In the run without detection of Sybil nodes (blue line) the attacker initially moved slowly as he had to pass a number of vehicles stuck in a virtual traffic-jam, however after that he was able to maintain high speed on the unobstructed road. The comparison of the results with the second run that applied proposed mitigation measures (red line) proves that our detection method is able to effectively mitigate the Sybil attack. Moreover, the speed measurements of legitimate vehicles (not included due to space constraints) indicate that after the introduction of mitigation measures against Sybil attack the traffic flow was significantly improved.

VI. CONCLUSIONS

In this paper, we defined the attacker model, network attack scenarios against V2V communication, and described possible mitigation measures including our proposed method of detecting Sybil attack. We focused on highly probable real-world attack scenarios where the attacker's motivation is to gain personal benefit (free road) by exploiting the mechanism of periodic awareness messages present in both US and EU ITS standards. We have implemented a proof-of-concept simulation of the presented scenarios and mitigations.

Based on the evaluation results it can be concluded that current ITS standards provide replay protection and secure message services to mitigate common attacks. The testing of performance overhead of using digital signatures confirmed that computing resources of recent embedded systems are sufficient for secured V2V communication. Therefore we propose that these services should be applied to all safety critical periodic and event-based awareness messages.

Defense against Sybil attack is more complex but provides additional layer of protection for V2V communication which is desirable especially for autonomous vehicles where no human element is present to discover the attack.

Fig. 3. Attacker speed during replay attack without mitigation (blue) and with mitigation (red).

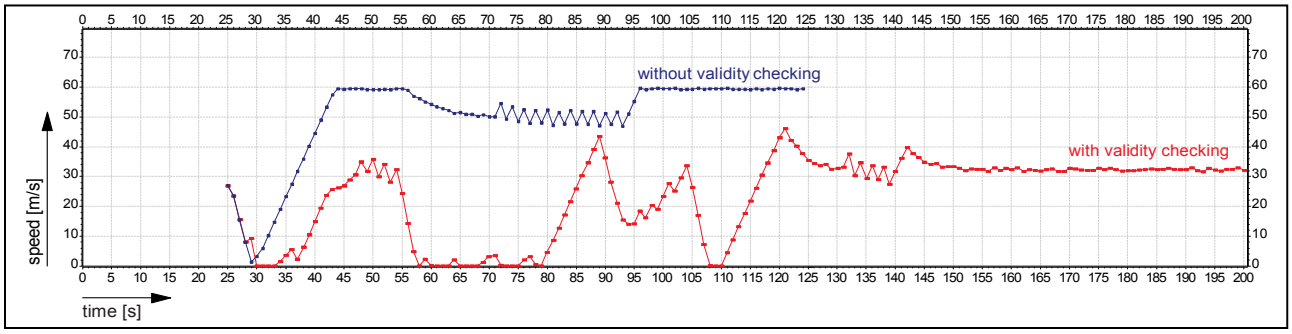
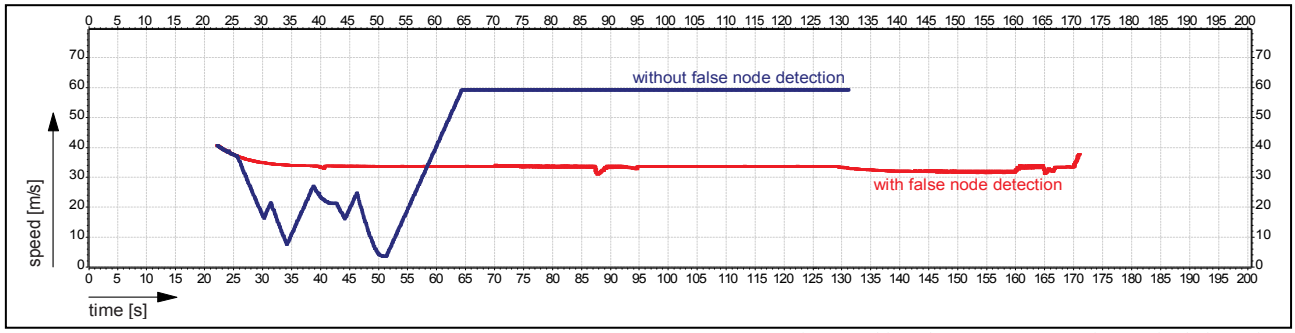


Fig. 4. Attacker speed during Sybil attack without mitigation (blue) and with mitigation (red).



Several existing works [13, 14, 15] deal with detection of Sybil nodes based on the assessment of signal strength and position information included in the message. These solutions are relatively complex and often require active cooperation with neighbouring nodes or introduce impractical constraints. We proposed a simpler approach that does not require cooperation between neighbours to detect Sybil nodes. The simulation results suggest that our approach is a viable solution for Sybil attack detection and mitigation. The main disadvantage is limited detection capability in case an attacker is able to modify the transmit power to match the virtual distance of Sybil node from the victim. Cooperative detection provides better results in this case, however it is not the ultimate solution because legitimate neighbour vehicles need to be present in communication range.

Therefore it is planned to evaluate other possibilities such as sensors and V2I communication. We also plan to research potential attacks on V2I, digital signatures, and PKI. At present, our development is based on the US standard, however in the future we aim to analyse the EU standard as well.

REFERENCES

[1] "Transportation Forecast: Light Duty Vehicles," [Online]. Available: http://www.navigantresearch.com/research/transportation-forecast-light-duty-vehicles. [Accessed 6-Jan-2019]

[2] WHO, "Road traffic injuries," [Online]. Available: http://www.who.int/mediacentre/factsheets/fs358/en/. [Accessed: 6-Jan-2019]

[3] L. Liu, S. Nie, and Y. Du, "Free-Fall: Hacking Tesla from Wireless to CAN Bus," In Proceedings of the Black Hat USA 2017, Las Vegas, NV, USA, 2017.

[4] C. Miller, and C. Valasek, "Adventures in Automotive Networks and Control Units," [Online]. Available: http://illmatics.com/car_hacking.pdf. [Accessed: 6-Jan-2019]

[5] R. Currie, "Hacking the CAN Bus: Basic Manipulation of a Modern Automobile Through CAN Bus Reverse Engineering," STI Graduate Student Research, Maryland: SANS Technology Institute, 2017.

[6] F. Li, and Y. Wang, "Routing in vehicular ad hoc networks: A survey," In IEEE Vehicular Technology Magazine, vol. 2, 2007, pp. 12–22.

[7] European Telecommunications Standards Institute (ETSI), "Intelligent Transport Systems (ITS); Access layer specification for Intelligent Transport Systems operating in the 5 GHz frequency band," EN 302 663 V1.2.1, Sophia-Antipolis: ETSI, 2013.

[8] Vehicular Technology Society (VTS), Intelligent Transportation Systems Committee (ITSC), Institute of Electrical and Electronics Engineers (IEEE), "1609.0-2013 IEEE Guide for Wireless Access in Vehicular Environments (WAVE) - Architecture," New York: IEEE, 2014.

[9] Transport Research and Innovation Monitoring and Information System (TRIMIS), "SEcure VEhicle COMmunication," [Online]. Available: https://trimis.ec.europa.eu/project/secure-vehicle-communication. [Accessed: 6-Jan-2019]

[10] National Highway Traffic Safety Administration (NHTSA), "Vehicle Safety Communications Project, Final Report," DOT HS 810 591, Washington: NHTSA, 2006.

[11] "Preparing Secure Vehicle-to-X Communication Systems," [Online]. Available: https://www.preserve-project.eu/. [Accessed: 30-Mar-2019]

[12] B. Fernandes, J. Rufino, M. Alam, and J. Fereira, "Implementation and Analysis of IEEE and ETSI Security Standards for Vehicular Communications," in Mobile Networks and Applications, vol. 23 Berlin, Heidelberg: Springer-Verlag, 2018, pp. 469–478.

[13] W. R. Pires, T. H. de Paula Figueiredo, H. C. Wong, and A. A. F. Loureiro, "Malicious node detection in wireless sensor networks," In Proc. 18th International Parallel and Distributed Processing Symposium 2004, Santa Fe, NM, USA, 2004.

[14] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETs," In Proc. 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks (DIWANS '06), New York, NY, USA, 2006, pp. 1–8.

[15] S. M. Bouassida, G. Guette, and M. Shawky, "Sybil Nodes Detection Based on Received Signal Strength Variations within VANET," in I. J. Network Security, vol. 9, 2009, pp. 22–33.