SECURE AND RELIABLE INFRASTRUCTURE TO SUPPORT FUTURE CITY MOBILITY AND SAFETY APPLICATIONS

Axel Krings, *University of Idaho, Department of Computer Science*
Mohamed S. Mohamed and Sherif Hussein *Military Technical College, Egypt*
Ahmed Abdel-Rahim, *University of Idaho, Department of Civil and Environmental Engineering*

Abstract

The implementation and integration of smart city, autonomous vehicles, and connected vehicle applications in future cities will depend on extensive communication of computing devices. Many of the smart city safety and mobility applications are based on vehicle-to-vehicle and vehicle-to-infrastructure data exchanges between different devices through wireless communication. Therefore they may be subjected to the full spectrum of security concerns associated with wireless networks that are susceptible to different types of attacks. Furthermore, since they operate in a critical infrastructure, where failure of applications could result in injury and loss of life, reliability is crucial. The deployment of Vehicular Ad Hoc Networks (VANET) requires well-defined technologies in order to ensure safe, resilient, and reliable system operation. In this paper we first introduce the underlying technologies associated with VANET that can be used in future cities. Second we address security challenges and attacks ranging from simple denial of service of communication to sophisticated attacks, and discuss mitigation strategies against such attacks.

I. Introduction and General System View

Communication between vehicles and the signal infrastructure are continuously evolving towards a transportation control infrastructure that is faster, safer, more reliable, and efficient. Wireless communications, on-board computer processing, advanced vehicle sensors, and continuous tracking of vehicle movement via the Global Positioning System (GPS) allow vehicles to work collaboratively with the signal control infrastructure in an active real-time manner to maximize the network performance.

The connected-vehicle-based traffic control applications are growing and will be evolving over the years, depending on the advancement of the technologies, market adoption, and market needs. Examples of connected-vehicle (CV)-based applications relevant to signal control include, but are not limited to, pedestrian safety applications, CV-based priority for freight and emergency vehicles, and cooperative adaptive control to maximize throughput and minimize delay and stops.

The signal infrastructure is a critical element for the optimization of traffic flow at intersections, particularly in congested urban areas. Traditional signal controllers are based on point detection of vehicle presence and queue length information and do not have the capability to send and receive information from vehicles and roadside units. The CV environment is expected to provide a real-time high-resolution data exchange and facilitate advanced control algorithms operating with real-time data. Traffic signal controllers are expected to interface with Roadside Units and Connected / Connected Autonomous Vehicles (CV/CAVs) for applications utilizing Signal Phase and Timing (SPaT) data. A typical communication infrastructure for a CV traffic signal system application is shown in Figure 1.

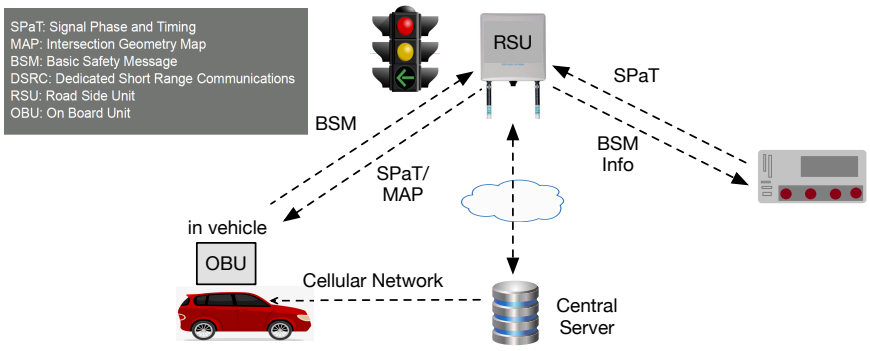

Fig. 1. System Overview

There are four major elements of the signal infrastructure regarding CV-based signal control optimization and deployment: (a) the communication technology that enables the bi-directional data exchange among vehicles, controllers, and roadside units, (b) the roadside units (either isolated or connected to the traffic controller), (c) the on-board units inside the car, and (d) the data storage and processing unit for optimization and decision-making. The two major competing candidates for communication

technologies in a CV environment are Dedicated Short Range Communications (DSRC) and cellular communications. Other communications technologies used within traffic signal systems may include Wi-Fi 802.11, Bluetooth, Wi Max, Terrestrial Digital Radio, and Two-Way Satellite. Optimal solutions of a CV approach may include combinations of technologies to attain the most benefits. The data exchange frequency and the coverage area for an application in the CV environment should determine the suitability of the communication technology.

Any awareness of vehicles and the fixed infrastructure can be aided by standard sensor technologies. Vehicles may be equipped with multiple sensors and drive with different levels of autonomy. Specifically, NHTSA defines vehicle automation as having five levels [1]: *No-Automation* (Level 0) indicates that the driver completely controls the vehicle at all times. *Function-specific Automation* (Level 1) assumes that automation involves one or mores specific control functions, e.g., where the vehicle provides electronic stability control or automatically assists with braking. *Combined Function Automation* (Level 2) includes automation of at least two primary control function, e.g., adaptive cruise control in combination with lane centering. *Limited Self-Driving Automation* (Level 3) enables the vehicle to fully control safety-critical functions under certain critical conditions induced by traffic or the environment. Finally, *Full Self-Driving Automation* (Level 4) is what is assumed for autonomous vehicles that may be occupied or unoccupied.

The above automation levels do not explicitly assume that the standard sensor technologies are augmented by wireless communications involving Dedicated Short Range Communications (DSRC) or cell-based technology, which however are the basis for Connected Vehicles (CV). In connected vehicle terminology Vehicle-to-Vehicle (V2V) denotes wireless communication between two or more vehicles, whereas Vehicle-to-Infrastructure (V2I) addresses wireless communication between vehicles and the infrastructure. The term Vehicle-to-X (V2X) combines these principles to include vehicles, the infrastructure, but may also include other entities, e.g., pedestrians, bicycles, or wheelchair operators. The communicating nodes in V2X are said to implement a Vehicular Ad Hoc Network (VANET), which is similar to a Mobile Ad Hoc Network (MANET), however, it is defined by short communication and a fast changing topology.

In the context of VANET different technologies have been considered. In the United States the USDOT assessed already in 2015 that DSRC is ready for deployment and that DSRC-based technologies and applications offer a path to a safer and more efficient surface transportation system for America [2]. However, recently, Cellular Vehicle-to-Everything (C-V2X) has been discussed. Whereas cellular technology typically assumes communication with base stations, C-V2X, also known as Device-to-Device (D2D), has relaxed this constraint by allowing out-of-coverage communication (without base stations) directly between vehicles [3]. There are different advantages and disadvantages for using DSRC and C-V2X, with arguments driven by discussions of the spectrum under siege, transmission speeds, message delay, and the technology curve. A further and perhaps more important issues with respect to security is the question whether a dedicated spectrum, such as in DSRC, or general technology, like LTE-Advanced or 5G, are preferable.

Whether the winning technology in the future will be DSRC or cell-based, it should be clear that all depend on wireless communications with its intrinsic strengths and weaknesses. Specifically, they have similar fundamental attack vectors, e.g., jamming, spoofing, or time manipulations, that could seriously affect the applications, e.g., safety applications. Whereas we will focus on DSRC, the general approaches for attack and defense strategies are expected to have their parallels in all wireless communication technologies.

In the big picture the range of visions to apply technologies have no limitations. For example, in [4] scenarios are described that combine different concepts, e.g., phone calls to request cars, platooning of the requested vehicles to the customer, self parking, or automatic drop-off, and each step may have its own technical challenges. The scenario in Figure 1 represents only a fraction of the infrastructure involved. The discussion in this paper does not focus directly on operation or optimization of such complex scenarios as discussed in [4], but we will use the reliability of safety application under attack as the focus. The reason for this is that these safety applications include the most critical aspects of the overall system. Any attack on these applications, and the issues involved in the attacks, have implications on the safe operation on any parts of the infrastructure. We will therefore make an argument for the case of DSRC safety application, again noting that we assume that cell-based communication will be equally affected, as the root of the problem is the ability to attack wireless communication in general.

Safety applications are aiming at reducing the number of accidents, and thus injuries and fatalities. According to the National Highway Traffic Safety Administration (NHTSA) report from August 2016 [5], the United States had 35,092 fatalities from crashes on U.S. roadways during 2015, an increase from 32,744 in 2014. The number of people injured on the Nations roads increased in 2015 from 2.34 to 2.44 million. Crashes might occur due to reasons that are out of our control, such as low visibility, or due to driver behavior. The NHTSA estimated that the critical reason for crashes can be assigned to the driver 93% of the time [6]. It is the utilization of technology to implement safety applications in the hope of reducing these numbers significantly. These safety applications should help avoiding collisions by alerting drivers of impending hazards or dangerous situations. It is obvious that the need for reliability and survivability of the safety application is of great importance as any compromise, may it be due to benign or malicious reasons does not only have the potential to cause injury or death, but it could also undermine public trust in the technologies and the entire concepts.

II. Background

In this section we will present the basic concepts related to this research. First we will introduce DSRC and the basic safety messages, whose content and timeliness are the key to providing reliable operation of safety applications. We want to reemphasized that, whereas we will focus on DSRC, many of the basic concepts are also relevant for cell-based communication.

A. DSRC and CV Infrastructure

Connected vehicle technologies deploy DSRC safety applications that are intended to alert drivers of dangerous road conditions and road hazards, e.g., during low visibility, to reduce accidents. DSRC enables vehicles to exchange their status information, including GPS coordinates and time values, using V2V communication. This requires that each vehicle be equipped with an On-Board Unit (OBU). A GPS receiver attached to each OBU is considered the main source of a vehicle's location information to be exchanged between vehicles. The OBU also enables V2I communication, which requires that the infrastructure, e.g., an intersection, is equipped with a Road Side Unit (RSU).

The Federal Communications Commission (FCC), in collaboration with the United States Department of Transportation (USDoT), considered 75 MHz of bandwidth at 5.9 GHz (5.850-5.925 GHz) to be utilized by DSRC communication [7], [8]. The DSRC bandwidth is divided into seven 10 MHz channels, one Control Channel (CCH) denoted by CH178, and six Service Channels (SCH), i.e., CH172, 174, 176, 180, 182, and 184. The remaining 5 MHz are reserved for future use. This research considers CH172, which is dedicated for V2V public safety communications and DSRC safety applications.

B. Basic Safety Message (BSM)

DSRC safety applications rely on a beacon messages called Basic Safety Message (BSM). A BSM is periodically exchanged between vehicles every 100ms [9]. As defined in standard SAE J2735 [10], a BSM consists of two parts. The first part is mandatory and contains specific BSMs such as speed, heading, location, brake status and a time stamp. The second part is optional and includes additional information for certain applications.

C. DSRC Safety Applications

Several DSRC safety applications were developed to operate in VANET. These applications focus on accident prevention and hazard avoidance. They enables vehicles to exchange their status information, including GPS coordinates and time values, in the BSMs they broadcast. Each vehicle executes safety applications and contributes by sending or receiving information collaboratively. From a safety application point of view, we refer to the vehicle generating an alert as Remote Vehicle (RV), and the vehicle making a decision in response to the alert as Host Vehicle (HV). A range of DSRC safety applications focusing on crash scenarios and their prevention have been described in [11]. *Forward Collision Warning* (FCW) alerts the driver of the HV in case of an imminent rear-end collision with the RV, driving ahead in the same lane and direction. FCW is useful in scenarios when approaching a vehicle that is decelerating or stopped. *Emergency Electronic Brake Lights* (EEBL) alerts the driver of the HV to decelerate once receiving a hard brake event from an RV. *Do Not Pass Warning* (DNPW) warns the driver of the HV during a passing maneuver attempt that another vehicle is traveling in the opposite direction. *Blind Spot Warning + Lane Change Warning* (BSW+LCW) warns the driver of the HV attempting to change into a lane, which happens to be occupied by another vehicle traveling in the same direction, but is in its blind-spot. *Intersection Movement Assist* (IMA) warns the driver of an HV entering an intersection that there is a high probability of collision with an RV. *Intersection Collision Avoidance* (ICA) is similar to the IMA safety application, however, it adds autonomous braking as a system response in case the driver ignores the warning.

D. Safety Applications Reliability

In line with the standard definition of reliability, the reliability of a safety application is defined as the probability that the safety application functions up to specification during the entire time interval of interest. For safety application this is directly linked to the probability of receiving at least one BSM containing important information such as an event, e.g., hard braking, before it is too late to react to alert the driver. The timing issues of FCW related to the HV and RV are shown in Figure 2. Starting with the moment of hard braking at time t_{brake} the RV emits BSM messages every 100ms. The HV needs to be alerted of the potential collision with the RV early enough to react. The reaction time is the time from the driver receiving an alert to his/her reaction, i.e., the time from t_{react} to t_{brake}, and is approximately 1 second. Reaction is only possible if the HV receives at least one BSM message from the RV, which is the minimum the application requires to detect the event, before t_{react}. As seen in Figure 2, this means that the HV must receive at least one of the first x BSM messages, i.e., BSM_1, ..., BSM_x. Any BSM message received after that will arrive too late for a driver to be able to react.

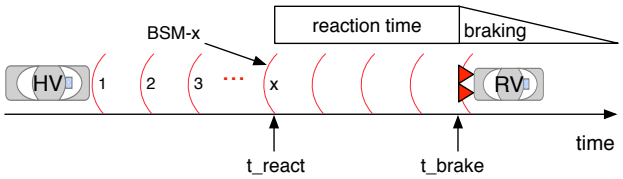

Fig. 2. BSM Propagation and Timing of sample Safety Application

III. Security Challenges and Attacks

The reliable exchange of information in a timely manner is the key to the intended operation of applications. However, as communication is based on wireless technology, there are intrinsic vulnerabilities. There are many potential ways to attack VANETs [12], [13], [14] and enumerating all attack possibilities is impossible. But in the end, it is the faults that these attacks attempt to produce that count. Taxonomies of fault types and their impact are often referred to as *fault models*. From a fault model point of view, omissive faults and value faults are of main concern for safety applications. Omissions can be the result of benign causes like collisions or environmental issues, e.g., shadowing. A simple example is a BSM that is corrupted during transmission and thus discarded by the recipient, or a collision due to the well-knows *hidden terminal* problem. The potential introduction of value faults less obvious. Typically, the manipulation of the content of a BSM due to malicious act comes to mind. For example, a malicious entity broadcasts a BSM with incorrect GPS coordinates. Whereas there are security mechanisms that help address such faults, e.g., by using authentication by means of certificates to verify the legitimacy of the sender of a message, there are ways to bypass such safe guards, for example, an attacker may use stolen devices. What is less obvious are attacks affecting the freshness of the information with the intend of tricking safety applications into discarding the messages, as they appear outdated. Jamming attacks are capable of inducing such faults will be discussed next.

A. Jamming and its Implications

Jamming is a very effective method to attack wireless communications. Different jammers were discussed in [15]. Specifically, a *Constant Jammer* emits a constant stream of random data that does not follow the Medium Access Control (MAC) layer protocol. Thus, the medium appears to be busy, blocking legitimate nodes from access. However, it may also result in corruption of ongoing packets. A *Deceptive Jammer* does not follow the channel access protocol by continually injecting a stream of what appears to be valid packets without any gaps between them. A *Random Jammer* switches randomly between periods of jamming and sleeping. During the jamming period its behavior resembles that of a constant jammer. A *Reactive Jammer* senses the medium for ongoing communication. When it senses a packet transmission it emits a radio signal that collides with the packet, thus corrupting it. Perhaps the most sophisticated jammer is the Intelligent Jammer. It is a protocol-aware jammer that has the capability of corrupting specific packets. It may target control packets, such as *RTS, CTS* or *ACK*, but could also target *DATA* packets, as described in [16].

In the context of DSRC safety applications jamming resistant strategies like frequency hopping or spread spectrum [17] do not apply as an attacker may use the same devices, e.g., OBUs, to launch the attacks. However, jamming may not always be the curse it seems to be, as will be demonstrated in Figure 3. If the intensity of jamming is high enough to allow for detection,

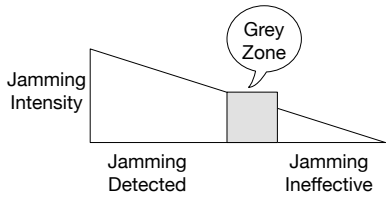

Fig. 3. The Impact of Jamming on Safety Applications

then safety applications can transition to a fail-safe mode, e.g., alerting the driver of the unavailability of its service. Such fail-safe options are common practice. For example, the owner of a car with self-parking capability will have experienced that the option is sometimes unavailable, which implies that the system could not reliably determine the exact properties of the parking space. If the impact of jamming is too weak to affect the application, then no actions need to be taken. However, there is a grey zone where jamming has the potential to introduce the timing or value faults referred to above. It is here where effective mitigation is most critical.

B. Redundancy as Mitigation Option

Redundancy to tolerate different fault types to improve the reliability of systems has been used effectively in the area of fault-tolerance [18]. Specifically, spatial, time, and information redundancy are the standard redundancy techniques. Spatial

redundancy uses multiple instances of subsystems to tolerate faults occurring in a number of instances below a certain threshold in order to avoid system failure. For example, using n subsystems, $n-1$ benign faults can be tolerated, leaving one functioning subsystem to perform system tasks. For value faults this is more complicated. In the case of symmetric faults, where s instances may produce the same wrong value, it takes $n \geq 2s+1$ instances to mask the faults [19]. In the case of asymmetric faults, also called Byzantine faults, this threshold increases to $n \geq 3a+1$, where a is the number of faulty nodes, with no assumptions about the behavior of the nodes. In addition to the large spatial overhead associated with mitigating asymmetric faults the execution of agreement algorithms with high communication cost are required to reach consensus [20]. In time redundancy the same computations are performed more than once and the results are checked. This may also apply to multiple copies of data transmitted. Time redundancy is typically useful where using additional time to perform tasks is of less concern than other issues, e.g., the cost of hardware. The periodic sending of BSMs does not constitute time redundancy, as each BSM has different information. Lastly, information redundancy uses additional information, such as used in error detection and correction methods.

Redundancy can only improve reliability under the *independence of fault* assumption, since otherwise a common-mode fault can occur. For example, assume the case of spatial redundancy where multiple computers are running the same operating system with a vulnerability. An exploit to the vulnerability can affect all computers alike, thus nullifying the intended effect of redundancy.

An approach based on redundancy was used in [21], [22]. Specifically, redundant communication channels with different message types were used to mitigate the impact of jamming. Analysis and experimental validation showed that DSRC safety applications that use redundant communication can overcome jamming attacks if data rates of 3Mbps and 6Mbps are used. It was concluded that rates of 12Mbps and above are not advisable as they are too heavily impacted by jamming.

In general, the overhead of spatial redundancy is n-fold, where n is the level of redundancy. In addition there is communication and computational overhead, as a consensus on the final value is the result of communicating values between redundant components and applying a convergence function, e.g., majority voting for the case of symmetric faults. If redundant communication is out-of-band, as in the case of [21], [22], then the burden on the channel is not increased, e.g., the number of messages on safety channel CS172 did not increase as the redundant communication was on other channels. Applying a convergence function such as majority is computationally negligible. If multiple communication channels are used to broadcast important event data, then a safety application can use the earliest received message, i.e., the one with the smallest transmission delay.

C. Value Faults as the Result of Jamming

One concern about jamming as a denial of service is that it has the potential to introduce symmetric and asymmetric faults in a way that is not quite intuitive at first sight, i.e., it has the potential to cause omissive and transmissive versions of these faults [23].

Let's consider symmetric faults. A transmissive symmetric fault, often simply called symmetric faults, occurs when the same faulty value is received by all nodes (vehicles). On the other hand, an omissive symmetric fault does not include faulty values at all, but implies that no message is received by any node. This may cause applications to use default values different from those in the lost message.

In wireless networks it is difficult to know which nodes may or may not have received a message. It is likely that some nodes receive a message and some nodes do not. Those nodes that have received the message will use its value. However, those who have not received the message will use a default value, e.g., a predetermined value or perhaps the value of the last received message. For an application that needs to come to a consensus about the value sent, this however is indistinguishable from an asymmetric fault. For example, assume that TRUE is the correct value of the message and FALSE is the default value an application uses if no message was received. This is indistinguishable from the malicious scenario where value TRUE was sent to some nodes and FALSE to others, i.e., those that did not receive it in the previous scenario.

Asymmetric faults can be a real problem for safety applications looking for confirmations about the validity of events by observing vehicles in the neighborhood [24], [25], [26]. Consider the scenario shown in Figure 4, disregarding the jammer. Assume that the RV sends out BSMs indicating an event related to hard braking. One way to verify the validity of an event is to observe vehicles in the neighborhood of the RV to see if their reaction confirms the event. In the figure no other vehicles in the detection area (that should have witnessed the same event) are braking. This gives reasons to believe that the event indicated by the RV was false, and the safety applications in the HVs that execute a voting algorithm come to the same conclusion by voting on the responses from vehicles in the detection area. It should be noted that the time for the HVs in the decision area to come to any conclusion has to be early enough to allow the driver to react to the alert. Now consider Figure 4 including the strategically placed jammer. This constitutes the dangerous scenario where the jammer controls the results of the vote. A solution for this situation was presented in [24].

The impact of jamming can however go beyond typical denial of service. In [27] a hybrid jammer was presented that uses short jamming bursts to force HVs to queue their BSMs during the time of jamming. When the medium becomes available again the HVs flush their buffers. If the durations of the jamming bursts are small enough to not cause the internal packet queues of the HV's OBUs to overrun, then no packets are lost, they are only delayed. Thus no jamming detection algorithms based

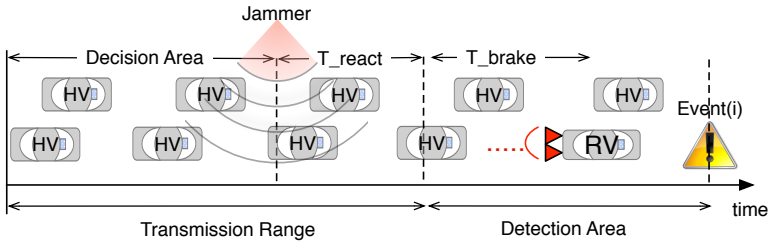

Fig. 4. Neighborhood Event Confirmation

on the Packet Delivery Ratio (PDR) notice the attack. The delay of BSMs may however have huge implications. According to [28] the time-to-live of a BSM should be no more than 500ms. Older messages are considered to be outdated. With a BSM period of 100ms this implies that if the hybrid jammer can cause an OBU to queue up 5 BSMs, then the time-to-live threshold is compromised. Experiments on Arada System Locomate Classic OBUs in the context of the research in [27], [29] revealed that the OBUs could queue up to 40 messages, leaving much room for the jammer to operate.

A serious problem in VANET is the potential for Sybil attacks. Here a rogue node pretends to be multiple nodes by impersonating their identities using stolen or fake IDs. This illusion could be used by an attacker to gain advantages ranging from fooling traffic management systems to redirect traffic away from the attackers path, to dangerous scenarios causing DSRC safety applications to fail. For example, undetected Sybil nodes have the potential to affect the votes of neighborhood confirmation approaches, such as presented in [24]. But even the presence of single Sybil nodes could have devastating effects. Imagine a dense traffic situation where suddenly BSMs from a non-existing node, the Sybil node, indicate a hard-braking event.

The detection of Sybil attacks is non-trivial in static power environments, and very difficult in dynamic power environments [29]. Here the power environment refers to the assumed transmission power of OBUs and RSUs. For dynamic power environments Sybil detection in [29] is directly linked to the probability of detecting small message delays caused by intentionally injected detection packets. The trade-off space of induced overhead and effectiveness was investigated and overall feasibility of detection was discussed.

D. Time Manipulation via GPS Time Spoofing

Whereas jamming was the primary reason in the previous discussion for BSMs to exceed their time-to-life threshold, it can be shown that value faults can also be injected into vehicles via GPS time spoofing. This has to be seen in the context of frequent GPS signal outages, especially in dense urban areas, tunnels, or parking garages. GPS time spoofing implies that GPS spoofing equipment is used to fake GPS time stamps, which are the basis for clock synchronization in OBUs. Such faults may cause safety applications to fail due to the messages being perceived as outdated. Specifically, the time difference between vehicles that are attacked and other vehicles are the reason for time discrepancies, which are then interpreted as lateness. The result is that the safety application of the HV disregards the messages, thereby causing potential safety application failure.

In order to eliminate the GPS as a centralized source for clock synchronization, and thus a single point of failure, decentralized clock synchronization, such as the approach in [30], was proposed to mitigate the impact of GPS timing faults that cause vehicles' clocks to drift apart. The synchronization is based on Approximate Agreement (AA) [31], where vehicles agree on clock values that are within a predefined tolerance of each other. Convergence is then achieved in a sequence of voting rounds, in which the domain of values collected from the immediate neighbors is gradually reduced to the specified tolerance. The decentralized clock synchronization algorithm uses time stamps from BSMs received by other vehicles as values in the agreement algorithm.

The approach proposed in [30] was extended in [32], where an Enhanced Clock Synchronization Algorithm (ECSA) for VANET was introduced that augments the GPS centralized clock synchronization in times of GPS outages or GPS spoofing attacks. In addition to [30] it considers a more realistic and stronger fault model. Specifically, it allows for lost or corrupted messages, and for situations where malicious nodes aim at preventing clock synchronization in order to cause failure in safety applications. The primary reasons for omission faults are environmental conditions such as shadowing effects and signal fading. Malicious faults are caused by malicious behavior of nodes that generate erroneous, potentially pathological clock values to other nodes. They show that malicious behavior makes agreement considerably more complex, especially if the malicious nodes are undetectable. Three fault models were investigated, i.e., omission faults, malicious faults, and a hybrid fault model consisting of both omission and malicious faults, and several agreement algorithms were presented. It should be said that the main criteria for time-to-live violations due to time value faults is a fast convergence rate, i.e., the number of rounds it takes to converge to the 500ms threshold in [28] is critical. Given a BSM rate of 100ms, which consequently dictates the rounds of the clock synchronization algorithm, convergence needs to be timely enough to compensate for induced time spoofing. Whereas

typically round-based agreement algorithms introduce much message overhead, here there is no such overhead since normal BSM messages are the basis for the values in the agreement. No other messages are introduced.

IV. Conclusion

This paper focussed on attacks on V2X communication and mitigation. As the attack vectors are unknown and impossible to enumerate, their impact on the kinds of faults they can produce in VANET were considered. Thus, attacks were discussed in the context of potential fault models. The discussion uses DSRC as the basis for communication, however, cell-based and in fact any wireless technology will be similarly affected. Security and reliability considerations were presented using safety applications, as they include the most critical aspects of VANET, which also span into mobility applications.

References

[1] U.S. Department of Transportation Releases Policy on Automated Vehicle Development, NHTSA 14-13, May 30, 2013. Available at https://www.transportation.gov/briefing-room/us-department-transportation-releases-policy-automated-vehicle-development

[2] *Status of the Dedicated Short-Range Communications Technology and Applications*, Report to Congress, FHWA-JPO-15-218, Final Report, July 2015.

[3] F. Jameel, et. al., *A Survey of Device-to-Device Communications: Research Issues and Challenges*, IEEE Communications Surveys & Tutorials, Vol. 20, No. 3, Third Quarter 2018.

[4] M. Boban, A. Kousaridas, K. Manolakis, J. Eichinger, and W. Xu, *Connected Roads of the Future - Use Cases, Requirements, and Design Considerations for Vehicle-to-Everything Communications*, IEEE Vehicular Technology Magazine, September 2018.

[5] *Traffic Safety Facts: Crash Stats, U.S. Department of Transportation*, National Highway Traffic Safety Administration, DOT HS 812 326, August 2016.

[6] *Critical reasons for crashes investigated in the National Motor Vehicle Crash Causation Survey*, US Department of Transportation, National Highway Traffic Safety Administration reportDOT HS 812 115, 2015.

[7] *Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems - 5 GHz Band Dedicated Short Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Spec.*, ASTM E2213-03, 2010.

[8] *Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band)*, Federal Communications Commission FCC 03-324, 2004.

[9] J. B. Kenney, *Dedicated Short-Range Communications (DSRC) Standards in the United States*, Proc. of the IEEE, vol. 99, no. 7, pp. 1162-1182, 2011.

[10] *Dedicated Short Range Communications (DSRC) Message Set Dictionary. Society of Automotive Engineers* SAE J2735, November 2009.

[11] *Vehicle Safety Communications-Applications (VSC-A) Final Report*, DOT HS 811 492 A. U.S. DoT, NHTSA. September 2011.

[12] M. S. Al-Kahtani, *Survey on security attacks in vehicular ad hoc networks (VANETs)*, in 6th International Conference on Signal Processing and Communication Systems (ICSPCS), pages 19. IEEE, 2012.

[13] Vinh Hoa La, Ana Cavalli, *Security Attacks and Solutions in Vehicular Ad Hoc Networks: S Survey*, International Journal on AdHoc Networking Systems (IJANS) Vol. 4, No. 2, April, 2014.

[14] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, *A comprehensive survey on vehicular ad hoc network*, Journal of network and computer applications, 37:380392, 2014.

[15] Xu W, Trappe W, Zhang Y, Wood T, *The feasibility of launching and detecting jamming attacks in wireless networks*, in Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp 46-57, 2005.

[16] K. Pelechrinis, M. Iliofotou, S.V. Krishnamurthy, *Denial of Service Attacks in Wireless Networks: The Case of Jammers*, Communications Surveys & Tutorials, IEEE , Vol.13, No.2, pp.245-257, 2011.

[17] William Stallings, *Data and Computer Communications*, Prentice Hall, 10th edition, ISBN:0133506487 9780133506488.

[18] W. B. Johnson, *Design and Analysis of Fault-Tolerant Digital Systems*, Addison-Wesley Publishing Company, New York, 1989.

[19] P. Thambidurai, Y-K, Park, *Interactive Consistence with Multiple Failure Mode*s, 7th Reliable Distributed Systems Symposium, (1988), 93-100.

[20] M. Pease, T. Shostak, L. Lamport, *Reaching Agreement in the Presence of Faults*, Journal of the ACM, (1980), 27(2), 228-234.

[21] Ahmed Serageldin, Hani Alturkostani, and Axel Krings, *On the Reliability of DSRC Safety Applications: A Case of Jamming*, in Proc. International Conference on Connected Vehicles & Expo, ICCVE 2013, Dec. 2-6, 2013, Las Vegas, 2013.

[22] Ahmed Serageldin, and Axel Krings, *The Impact of Dissimilarity and Redundancy on the Reliability of DSRC Safety Applications*, in Proc. Tenth International Symposium on Frontiers of Information Systems and Network Applications, (FINA 2014), Victoria, Canada, May 13-16, 2014.

[23] M.H. Azadmanesh, and R.M. Kieckhafer, *Exploiting Omissive Faults in Synchronous Approximate Agreement*, IEEE Trans. Computers, 49(10), pp. 1031-1042, Oct. 2000.

[24] Hani Alturkostani, and Axel Krings, *The Impact of Jamming on Threshold-Based Agreement in VANET*, in Proc. The 3rd International Conference on Connected Vehicles and Expo, (ICCVE 2014), Nov 3-7, Messe Wien, Vienna, Austria, 2014.

[25] B. Ostermaier, F. Dotzer, and M.Strassberger, *Enhancing the security of local danger warnings in vanets - a simulative analysis of voting schemes*, in Availability, Reliability and Security, 2007. ARES 2007. The Second International Conference on. IEEE, pp. 422431, 2007.

[26] J. Petit and Z. Mammeri, *Dynamic consensus for secured vehicular ad hoc networks*, in Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE 7th International Conference on. IEEE, 2011, pp. 18, 2011.

[27] S. Hussein, M. Mohamed, and A. Krings, "A New Hybrid Jammer and its Impact on DSRC Safety Application Reliability", in Proc. 7th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, Canada, (7 pages), 13-15 October, 2016.

[28] X. Ma, X. Yin, and K.S. Trivedi, *On the Reliability of Safety Applications in VANETs*, Invited paper, International Journal of Performability Engineering Special Issue on Dependability of Wireless Systems and Networks, 8(2), March 2012.

[29] Mohamed S. Mohamed, Sherif Hussein, and Axel Krings, "An Enhanced Voting Algorithm for Hybrid Jamming Attacks in VANET", in Proc. IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, January 9-11, 7 pages, 2017. (pdf)

[30] S. Hussein, A. Krings and A. Azadmanesh, *VANET clock synchronization for resilient DSRC safety applications*, 2017 Resilience Week (RWS), Wilmington, DE, USA, 2017, pp. 57-63.

[31] R. M. Kieckhafer and M. H. Azadmanesh, *Reaching approximate agreement with mixed-mode faults*, in IEEE Transactions on Parallel and Distributed Systems, vol. 5, no. 1, pp. 53-63, Jan 1994.

[32] S. Hussein, A. Krings and A. Azadmanesh, *Fault Tolerant Solutions for DSRC Safety Applications in VANET*, Ph.D. dissertation, University of Idaho, Computer Science Department, August 2018.