Supporting Situational Awareness in VANET Attack Scenarios

Dimah Almani, Steven Furnell and Tim Muller
University of Nottingham, UK
dimah.almani@nottingham.ac.uk
steven.furnell@nottingham.ac.uk
tim.muller@nottingham.ac.uk

Abstract: The integration of sensors and communication technologies is enabling vehicles to become increasingly intelligent and autonomous. The Internet of Vehicles (IoVs) is built from intelligent vehicles that work collaboratively and interact with the surrounding environment in real time. The underlying communications infrastructure is provided by Vehicular Ad-hoc Networks (VANETs), for vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) communications. The volume of autonomous vehicles (AVs) increases, as well as the level of automation for vehicles. The potential for related incidents and attacks increases as a result. A particular concern is the ability to disseminate alerts and emergency messages effectively and securely via the V2V/V2I nodes, given the diminishing involvement of autonomous vehicle users with the operation of the autonomous vehicles. With this challenge in mind, this paper investigates the issue of situational awareness for occupants in autonomous vehicles. Building from the concept of VANETs and recognised classification of automation levels, the discussion considers a range of related attack scenarios that could be encountered, each of which illustrates also contexts in which occupants may need to be made aware and take decisions in response. Consideration is then given to resulting support for situational awareness that would be required, particularly highlighting the associated requirements for user responsibility at different levels of automation. The resulting discussion serves to articulate the challenge and serves as a basis for further research to inform the mechanisms to address the resulting requirements.

Keywords: autonomous vehicles, VANET, situational-awareness, attacks, messages, communications

1. Introduction

The Internet of Vehicles (IoVs) evolves towards ever-higher levels of vehicle autonomy. Autonomous Vehicles (AVs) are the most essential entities in Vehicular Ad-hoc Networks (VANETs) that facilitate wireless communication and exchange safety messages (e.g., attacks and congestions) through vehicle- to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. Exchanging safety messages in VANETs has different scenarios based on vehicle automation. The current Society of Automation Engineers (Inagaki and Sheridan, 2019) automation level for vehicles provides a clear breakdown of environmental monitoring, autonomy control, fallback procedures, and system limitations. However, it does not expressly classify situations where the driver should resume control of the vehicle, which relates to situational awareness (environmental monitoring).

This study investigates users' situational awareness in VANET based on different levels of automation. In a partially autonomous system, users shift to a more supervisory position. However, they have to remain situation aware as they may be called upon to retake control of the vehicle or decide if the AV cannot deal with some incidents effectively. This discussion is divided into five sections: Section 2 discusses an overview of VANET technologies, as well as the different levels automation that are possible within vehicular contexts. Section 3 then proceeds to examine different attacks scenarios in VANETs and the different elements of security that may be targeted. Section 4 represents the main contribution of the paper and considers the resulting requirements for Situational Awareness, highlighting the types of messages involved and extent to which users need to be alerted to them at different levels of automation. Finally, section 5 concludes the discussion and highlights the resulting directions for future work.

2. Background

This section provides an overview of the supporting concepts that underpin the discussion in the paper, beginning with background on nature of VANETs and then examining the level of automation

2.1 An overview of Vehicular Ad-Hoc Networks (VANETs)

A VANET is a type of mobile ad-hoc network (MANET); it is capable of spontaneous creation of a network of mobile vehicles. In VANETs, vehicles are moving wireless access nodes, providing wireless connectivity to other vehicles and users in their surroundings. Expanding this concept is the Internet of Vehicles (IoV), which vehicles turn into intelligent nodes on the road, with their storage, compute, and networking capability (Qian and

Moayeri, 2008). From an engineering perspective, the study of VANETs focuses on network infrastructure, and the vehicle is mainly considered as a node that distributes different messages (i.e., V2V or V2I).

In the IoV, each vehicle is considered an intelligent entity equipped with an efficient multi-sensor platform, computation units, communications tools, and IP-based connectivity in V2V/V2X either directly or indirectly. Additionally, a vehicle in IoVs is envisioned as a multi-communication system that enables communications between intra-vehicle components, V2V, V2I, and V2X. As (Sateesh and Zavarsky, 2020) stated, VANETs consist of On-Board Units (OBUs) and Roadside Units (RSUs). The former is installed on the vehicle to provide wireless communication with other vehicles or RSUs, while RSUs themselves are communication units located aside the road. They are connected to the application server and trusted authority (TA). The main VANET components and their purposes can be summarised as shown in Table 1.

Table 1: Outlining the main components of a VANET

VANET Component	Definition	Purpose
On-Board Unit (OBU)	A GPS-based tracking system embedded in each AV that allow the vehicles to communicate with each other and with RSU.	Retrieving the vital information. Supporting many electronic components such as resource command processor (RCP), sensor devices and user interfaces. Communicating between different RSUs and OBUs via a wireless link.
Roadside Unit (RSU)	A computation unit fixed at specific location on roads, intersections, and parking areas.	Providing the V2I connectivity. Supporting vehicle's localization. Connecting vehicle with other RSUs using different network topologies. Calculate vehicles' trajectories to avoid threats.
Trusted Authority (TA)	Controls the entire VANET processes. Only legitimate RSUs and vehicle OBUs can be registered and communicate.	Affording protection by checking the OBU ID. Detecting malicious nodes or suspicious behaviour.

In terms of data broadcasting, VANET is a tool for controlling messages. It regulates message broadcasting between vehicles to support the timely delivery of safety messages. Furthermore, VANET aims to support security on the roads during potentially dangerous scenarios such as congestion and accidents. Specifically, vehicles communicate with their neighbours to share safety messages (Mariani, 2018). It is this context that is of particular interest in this paper, as it leads to the role of the AV occupant as the target of messages.

2.2 Levels of automation

The VANET environment in which a vehicle operates is complex. For example, a vehicle or user may have to respond to confused traffic situations, such as accidents and congestion. Therefore, the ability to understand AV system and respond to any events in VANETs (even with partial information) is critical. To communicate effectively in VANET (L3-L5), users will need to share personal information over V2V or V2I. However, sending/ receiving, collecting, and storing data pose a risk to users during this process, leading to attacks and exploitation. To illustrate, AV users might need to reveal personal information to RSU or other AV users. It is similar to using internet services. However, in VANETs, the collected data will be more accurate such as user identity, IP address, video, emotional state, etc. Therefore, the large-scale collection of data makes exploiting personal information more accessible and more lucrative; hence, the attacker will find it an attractive environment to launch attacks.

VANETs have increasingly exhibited advantages and made numerous benefits for AV users. However, AV users tend to have low acceptance of autonomous systems. Forecasting the acceptance and the understanding of autonomous driving is a new topic. Furthermore, the established understanding of automated driving is constantly being updated and now automatically recognises the need for occasional user's control, even at high levels (Mutzenich et al, 2021).

As shown in Table 2, the Society of Automation Engineers (SAE) identified six automation levels (Inagaki, and Sheridan, 2019). At higher levels of taxonomy, vehicles become fully autonomous, and the passenger is not normally required to take action. However, even fully autonomous vehicles of this type sometimes require user intervention. Therefore, providing secure vehicular communication to guarantee the user-safety is the main goal

in implementing VANETs where vehicles can send and receive safety messages to each other to ensure user safety (Muhammad and Al Hussein, 2021).

Table 2: Level of automation in autonomous vehicles

SAE Level		Description	Engagement level	Occupant role
0	Zero Autonomy	The driver must perform all the driving tasks.	No Automation	Driver
1	Driver assistance	An advanced driver assistance system (ADAS) assists the driver with either steering or breaking/ accelerating, but not both simultaneously.	Hands on	
2	Partial Automation	ADAS on the vehicle controls both steering and accelerating simultaneously under some circumstances. The driver must continue to control the tasks (monitor the driving environment) and performs the rest of driving task.	Hands off	
3	Conditional Automation	An Automated Driving System (ADS) performs all the driving task under some circumstances. The driver must be attention to take back control at any time when the ADS requests.	Eyes off	Passenger
4	High Automation	ADS on the vehicle performs all driving tasks and monitor the driving environment. Do all the driving- in certain circumstances. The driver needs not to pay attention in those circumstances.	Mind off	
5	Full Automation	ADS performs all the driving tasks under all circumstances, even when there is no occupant in the vehicle.	Body off	

Consideration needs to be given to the implications of the different automation levels in the event of an attack. This issue is highlighted because the user in L0-L2 is often expected to be aware of the situation and be fully responsible, whereas, in L3-L5, the situation will be different. Therefore, the user cannot respond correctly, for example, in a sudden emergency in L3-L5, where users may be responsible for having adequate situational awareness, they may have performed other tasks (social media/sleep) and therefore may not be fully conscious. However, prior to exploring this aspect further, it is firstly relevant to consider the types of attack that may occur in the VANET context.

3. Attacks scenarios in VANETs

As VANETs are open-access and self-organised networks, they are prone to potential attack. Some attacks aim to disseminate fake messages to disrupt safety-related services or misuse the VANET's communication systems, leading to various types of damage such as Denial of Service (DoS) (Poongodi et al, 2019). In this study, a focus on the attackers and their behaviour of launching attacks on VANET will be stated. Attacks are considered the most severe threats in VANETs that compromise V2V and V2I communications messages. Therefore, broadcasting emergency messages in VANETs to prevent attacks is a significant concern. For example, some VANET users need to broadly announce specific messages in real-time (e.g., emergency messages). Selecting a single trusted node to store and disseminate critical information will also be challenging. Unfortunately, users might not trust the automated driving system, preventing handing over the driving task or entirely focusing on the other task. We assert that enhancing situational awareness can increase a user's trust in Automation and lead to better decision-making. In addition, it is essential to mention VANET security requirements, as failure to meet these will lead to various vulnerabilities. At a high level, the requirements in VANETs requirements are broadly common to other areas and have been categorised into five main classes: Authenticity, confidentiality, availability, integrity, and nonrepudiation (Zubairu, 2018; Poongodi et al, 2019).

To illustrate how the security requirements may be compromised by particular attacks, Figure 1 depicts a range of scenarios that may be launched in VANET at L3-L4 automation. The scenarios are described as follows:

- **Scenario A:** This scenario depicts a Sybil attack (Figure 1A), in which the attacker (red vehicle) will have different fake identities to disrupt the standard mode of VANET operation. First, the malicious vehicle broadcasts multiple counterfeit messages. Then, the attack manipulates other vehicles' directions. For example, the attacker will broadcast congestion ahead; if the victim vehicle acts upon this, it is forced to alter its paths and exit. In this case, AV users should react quickly to confirm the received safety messages with RSU to thwart such attacks.
- **Scenario B:** In broadcast tampering, attackers' issue false safety messages in the VANET. These sometimes hide traffic threats, which can lead to situations like accidents and road congestion. As shown in Figure 1B,

the malicious vehicle will broadcast fake messages "there is no congestion ahead, and the road is clear" to mislead other vehicles to continue straight. The white front vehicle, for example, will continue proceeding then will encounter congestion. By monitoring the AV sensors, users can identify the attack, ignore the fake message, and exit the road. Moreover, users can safeguard the VANET by alerting other vehicles on the road by broadcasting a corrective message.

- **Scenario C**: This attack occurs in the middle of V2V communications (Figure 1C). The attacker checks the target vehicles closely then alters the messages between them. In this case, the attacker manipulates the V2V communications while they think they communicate privately. Under this attack, AV users must be aware of their surroundings and authenticate the source of the received messages by using cryptography techniques such as PKI.
- **Scenario D**: A masquerading attack occurs when the attacker logins into the VANET system using a stolen ID and passwords then attempts to broadcast false messages which appear to come from the registered vehicle (Bagga et al., 2020). For example, in Figure 1D, the red vehicle pretends to be police, then forces the yellow front vehicle to expose information such as an ID or a social number. In this case, AV users need to be aware of this situation and know how to react to deny revealing information to the untrusted vehicle; they also need to check the accuracy of received messages with the Trusted Authority before starting the communication.
- **Scenario E**: In this scenario, two or more vehicles share the same key. The two vehicles will not be distinguished from each other, so their actions can be repudiated. For example, as shown in Figure 1E, after the malicious vehicle (A) did the road accident, the attacker (A) will send malicious messages in VANET. As stated in Figure 1E, the same (A) yellow vehicle that caused the accident continued proceed as if nothing happened and denying the fact of sending the message in case of any dispute.
- **Scenario F:** This depicts a replay attack, in which the malicious vehicle replays the previous message's transmission to exploit its contents at the moment of transmission. As shown in Figure 1F, a malicious vehicle alters a duplicate of the received message then resends it again to the neighbouring vehicles causing further VANET incidents.

While the notion of AVs is fundamentally aimed towards reducing or removing the need for human involvement, it is still crucial to define what responsibilities users may still be required to fulfil (such as roles and duties, control transfer, operational mode, and most importantly, decision making). Security, legal and ethical responsibilities need that occupant to remain aware of the VANET situation. AV drivers will shift to a more supervisor position in such a scenario. They have to remain situation-aware as they may be called upon to make decisions or take control of the vehicle as the vehicle will be confused, and the AV system will be unable to address this situation successfully. Under this concept, the taxonomy of AVs by the National Highway Traffic Safety Administration (NHTSA) specifies that the occupant in L2 must be situation-aware at all times (Mutzenich et al, 2021). In L3, the occupant must become situation-aware and control the vehicle after a brief period. In VANETs, since the attentional demand will be low, maintaining adequate alertness will be a challenge. It is therefore necessary to assess the level of situation awareness that occupants maintain in different scenarios in VANETs. Critical decisions in some attack scenarios depend on whether the occupants are responsive and aware of external conditions. For example, based on the Sybil attack scenario (shown in Scenario A in Figure 1), a different forged identity is launched in VANETs by sending numerous incorrect messages to the neighbouring vehicles. As a result, these vehicles will leave the road to let the attacker pass the road quickly. In this case, the real identities of the sender will be hidden, and the attackers create a deception to the other vehicles. Hence, the occupant needs to be aware of such an event to verify the receiving messages and authenticate these messages with the third agent on the roadside.

As the safety messages are broadcast in an open-access system, the whole communication in VANETs disturbs if the attacker injects, alters, or blocks the messages in VANETs. Moreover, it will make VANETs more vulnerable to other attacks that may fill bogus information in the transmitted message. These challenges expose VANETs to various scenarios of dangerous attacks.

Interaction mechanisms in AVs need an appropriate design for exchanging information and function. The functions in AVs have to meet the cognitive characteristics of users and guarantee the efficiency and safety of any communication during autonomous driving (Ghazi et al, 2020). Generally, since machines and humans differ significantly in terms of their competences and capacities any design in AV must enable the user and the automation to function over a high-level guarantee of quality system performance (Petersen et al, 2019).

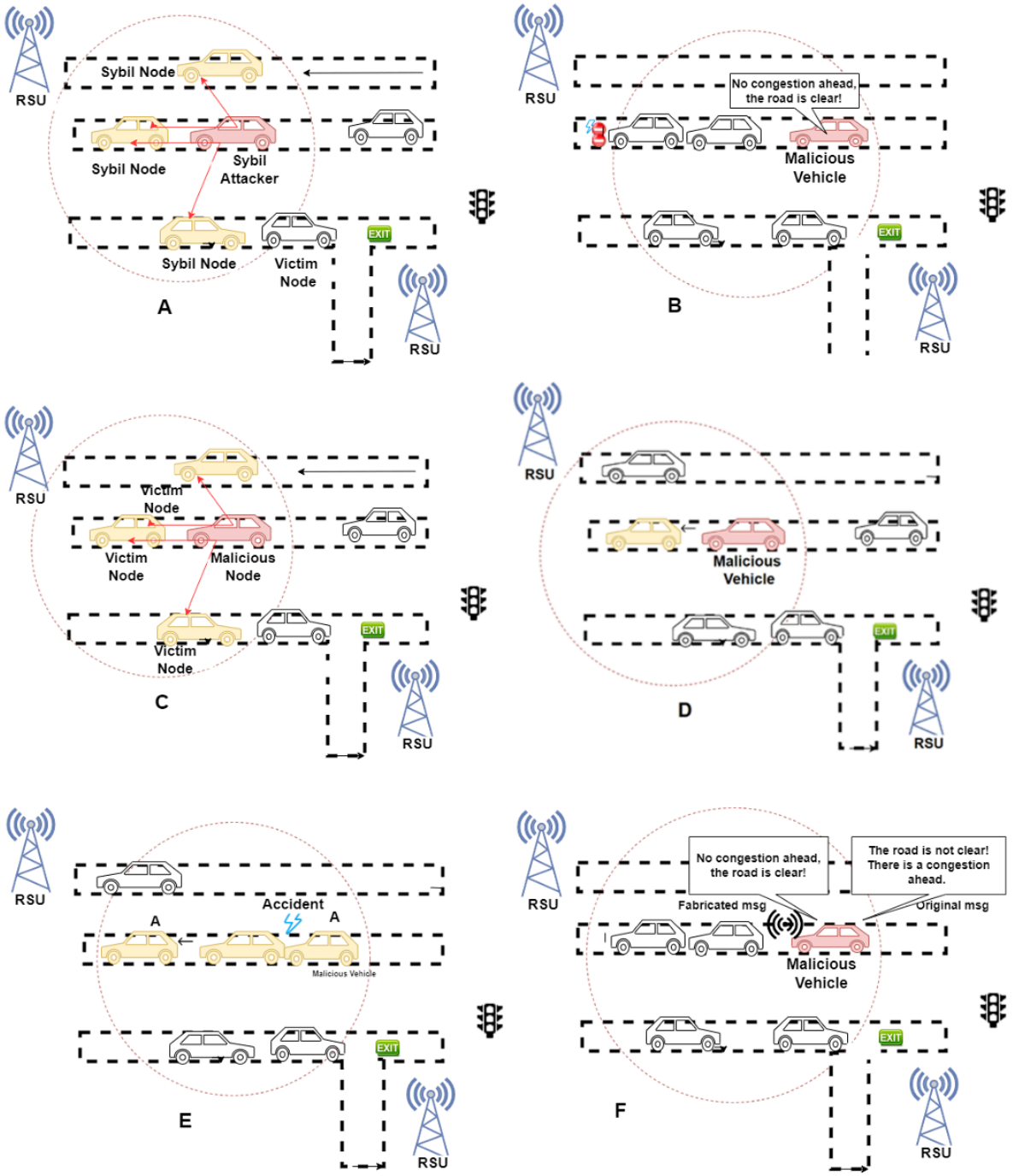

Figure 1: Scenarios where VANET vehicle is susceptible to different malicious attacks

4. Recognising situational awareness requirements in VANETs

Situations mean understanding the perceived data, starting by taking the activity, then predicting the following appropriate action based on the taken activities. It has been used widely in the aviation industry for pilots. Recently, it has started gaining notoriety in the automotive system. Situational awareness can be classified in three stages (Hashem et al, 2015) as follows:

- Perception: Extracting information as features from VANETs.
- Comprehension: Collecting all the extracted information and providing an understanding to them. This stage may take actions based on the understanding of the features.
- Projection: Predicting the future state based on the action taken in the comprehension stage.

The issue of real situations identification plays a significant role in avoiding road incidents and attacks. In V2V communications, it is suggested that 60% of the dangerous incidents could be avoided if the warning messages had been disseminated to alert neighbouring vehicles on time (Moharrum and Al-Darkish, 2012). Therefore, a key role of AV users is verifying the receiving warning message and selecting the correct next reception of warning messages in the vehicle's neighbourhood as soon as an emergency occurs. The collaboration of AV users in V2V will reduce the message delivery latency for nearby vehicles and achieve higher awareness for vehicles in the vicinity.

Studies that considered role of Situational Awareness in AV have been limited to automation levels 0-3 in which users have to take over the driving of an AV that can operate autonomously in a specific time. These have included calculating the response times of users taking control after receiving an emergency message has been studied (Banks et al, 2018), and examining the issues of complacency when users are needed to be in charge of monitoring state for prolonged periods in AVs (Larsson et al, 2014). However, there is no clear guideline for L3-L5 users explaining their responsibilities and the right direction to deal with an attack. (e.g., communications with the safety messages).

With the above in mind and to ensure occupant safety from attacks over VANETs, it is essential to ascertain the following questions across the wider range of automation levels:

- How do AV users exchange emergency messages in different automation levels under attack?
- Will AV users be aware in the event of attacks?
- What will be the information and functions required to support such activities?

To date, relatively few studies have attempted to answer the above questions. However, recent works (Liu and Parkinson, 2020) have suggested the need to analyse this concept in-depth to design an efficient framework that supports AV user awareness under any attacks over VANETs. As such, the implications of the questions are discussed in the sub-sections that follow.

4.1 AV user's role in exchanging messages in VANETs

Little research has been done in respect of clearly illustrates the AV users' role in emergencies. Therefore, understanding the types of emergency messaging in VANETs is the key to comprehending the communication to improve road safety. Generally, the communication in VANETs is classified into six types of safety messages, as shown in Table 3.

Table 3: Types of safety messages in VANETs

Message Type	Description	Comm. type	Priority
Group Communication	AV users who share the same or some vehicles features can participate in this communication. E.g., vehicles, that have the same models, or vehicles sharing the exact location in the time interval.	V2V	Low
Road Condition Warning	Nearby Vehicles exchange safety messages about the condition of the road (e.g., congestion, maintenance, closed road, etc.)	V2V	Medium
Low Connection Warning	The exchange messages contain information about the VANET connection conditions in some areas (e. g. type of wireless and the communication speed. etc.)	I2V V2V	Medium
Collision Warning	In different collision situations, safety messages are needed to be sent to a nearby vehicles to avoid further incidents and increase safety. (e.g., post and pre-crash warning.)	V2V	High
VANET Warning	The warning messages alert all the nearby vehicles about the event of any incidents (disruption, attacks) affecting the VANET. These messages can contain the security incidents features and behaviour (e.g., Vehicle colour, model, speed, velocity etc.).	V2V V2I	High
I2V Warning	The infrastructure broadcast messages via RSUs to all vehicles within its surrounding area about environmental weather and safety issues when an issue is detected.	I2V	High

Osika et al. (2017) emphasised that AV users will be unaware of their surroundings; they used a simulated AV to prove their view and explore user activity situations. Their experiment analysed some non-driving activities, including smart device usage, reading a book, and sleeping. As they found, the unsecured non-driving activities

are open to all risks, which means that any corresponding driver-vehicle interaction will be subject to high levels of attacks. In addition, users have high expectations for AVs to relieve them from driving responsibilities to engage in other activities. In such a case, AV users will be unaware of their surroundings and will be less able to take the right action to face such an attack. This leads to the need to ensure user awareness at key points when it becomes relevant.

4.2 AV user's awareness in the event of attack

Despite the advantages obtained from AV in high levels of automation, the sole source of communication in VANETs is through wireless links, which are sensitive to a variety of attacks. Depending upon the implementation, VANET entities may be susceptible to third parties injecting faked messages (altering and repeating old messages). Because these messages are urgent and usually life critical. While they may no longer be performing the traditional driving task, AV users need to suitably aware the technology they use as well as how to take the appropriate action in the right time.

Warning messages in VANET are sent in broadcast mode where all the vehicles inside the coverage area of the sender should receive the message. However, as vehicles with the same area can receive the emergency messages, some vehicles from outside the area are unable to receive any alert or receive it late, which results in undesirable consequences. Therefore, research in this area suggests AV users engage in V2V/V2I communications to boost VANET safety. Under this area, many vehicle concepts have been devoted to proving how driving might change when it reaches the highest level of automation, where a user is neither needed nor, in some circumstances, even recommended to monitor the vehicle. However, based on SAE's six levels, any system short of full automation will still need driver control in some situations, and some fully automated vehicles will still recommend driver monitoring under some conditions.

While SAE Level 0 means no automation and Level 5 means full autonomy, the middle levels are rather more blurred. The SAE is clear that the first three levels (L0, L1, and L2) must be referred to as "Driver Support Systems", while L3 to L5 are actual "Automated Driving Systems". A survey conducted by Tang et al. (2020) noted that users in high automation levels (L3-L5) will primarily attend non-driving activities, such as sleep and social media. However, unlike low-level automation (L0 to L2) where there is no vehicle connectivity (no possibilities of communication attack), the high-level automation contexts require users to be aware of their surroundings to protect themselves from any attacks, as explained in Table 4.

Table 4: Levels of user awareness based on the automation levels

Automation Level	Level 3 Conditional	Level 4 High	Level 5 Full
Features	Has its own internal connectivity (i.e. connected services inside the vehicle only)	In-vehicle experience of a broad range of online services that can be ported inside and outside the vehicle	In-vehicle experience of a broad range of online services that can be ported inside and outside the vehicle
Vehicle Connectivity	Vehicles are connected partially in V2V/V2I	Vehicles are directly connected in V2V/ V2I	Vehicles are connected to everything (i.e. V2X)
User Awareness Tasks	Check the vehicle connections. Monitor the system (non-driving activities). Control the communication (V2V/V2I) Make decisions in emergency situations.	Monitor the system (non-driving activities). Control the communication (V2V/V2I) Make decisions in emergency situations.	A 'driver' is not expected to be present in the vehicle. User needs to remotely monitor the system. Control the communication (V2X) Make decisions in emergency situations.
Primary occupant role	Monitor/Passenger	Monitor/Passenger	Passenger/ Remote driver

4.3 The required information that supports the AV user's awareness

AV users need to understand AV technology to support the decision-making under any VANET threat. Furthermore, an attacker may compose these messages then compromise the user's privacy by obtaining his location. Thus, the privacy of the user must be protected from unauthorised access. Various even new types of

attacks might be launched on VANET differently. The impact of these attacks depends on the intention of the attacker and the way used to perform the attack.

The different awareness and intervention requirements at different levels of automation suggest different assessments and responsibilities, depending on how the AV user is involved in the driving task. However, vehicle automation is relatively new and constantly changes, especially when automation is high (L4, L5). Therefore, there is no clear timetable for control transitions and no unified responsibility model for different levels of vehicle automation. The current model will continue to apply as long as most daily traffic remains at 0-3 levels, but AV users may need to review and reassess their roles for future accountability.

In order to raise SA in AV users, it is necessary to develop an effective human control mechanism with a well-designed user interface so that users can efficiently monitor and control AVs in when circumstances require it. However, understanding of users' activities during problem scenarios is still limited. The published data corresponding to the AV users and their responsibilities under VANET attack is insignificant. Recent fatal AV accident investigations have revealed issues such as over-reliance on systems and a low SA, resulting in poor driving handling in an emergency (Litman T, 2021). Nonetheless, it is recognised that user presence is a critical factor in driving safety. Hence, ignoring the user responsibility in the event of attacks and other events will result in undesired consequences. Moreover, the ability to take the correct actions in AV will serve to both protect the occupants and support the security of communications over the VANET more generally.

5. Conclusion and future work

Attempting to understand the issue of vehicular automation is a long-term process, and the implications and challenges arising from the different levels of automation are yet to be fully understood and resolved. Our study offers insights into the requirements to support situational awareness for users in AVs context to safeguard VANETs in the event of attacks that seek to compromise V2V/V2I communications. Until vehicles are fully autonomous and sufficiently trustworthy, a level of user engagement and responsibility is likely to required, which necessitates making them appropriately aware of the current situation. While the paper has illustrated some contexts that are likely to drive the need for awareness and identified the challenges in achieving this as the automation levels change, work is still required to establish the actual mechanisms that would support this in practice. This will therefore form one of the areas of further attention, and the authors intend to build upon this conceptual foundation as part of ongoing research.

References

Bagga, P., Das, A. K., Wazid, M., Rodrigues, J. J. P. C., and Park, Y. (2020). Authentication Protocols in Internet of Vehicles: Taxonomy, Analysis, and Challenges. IEEE Access, 8, 54314–54344. https://doi.org/10.1109/access.2020.2981397

Ghazi, M., Khan Khattak, M., Shabir, B., Malik, A. and Sher Ramzan, M., 2020. Emergency Message Dissemination in Vehicular Networks: A Review. IEEE Access, 8, pp.38606-38621

Hashem Eiza, M., Owens, T., Qiang Ni, and Qi Shi. (2015). Situation-Aware QoS Routing Algorithm for Vehicular Ad Hoc Networks. IEEE Transactions on Vehicular Technology, 64(12), 5520–5535. https://doi.org/10.1109/tvt.2015.2485305

Inagaki, T., and Sheridan, T. B. (2019). A critique of the SAE conditional driving automation definition, and analyses of options for improvement. Cognition, technology & work, 21(4), 569-578.

Larsson, A. F. L., Kircher, K., and Hultgren, J. A. (2014). Learning from experience: Familiarity with ACC and responding to a cut-in situation in automated driving. Transport. Res. F Traffic Psychol. Behav. 27, 229–237. https://doi.org/10.1016/j.trf.2014.05.008

Lee, J. M., Park, S. W., and Ju, D. Y. (2020). Drivers' user-interface information prioritization in manual and autonomous vehicles. International Journal of Automotive Technology, 21(6), 1355-1367.

Liu, N., Nikitas, A., and Parkinson, S. (2020). Exploring expert perceptions about the cyber security and privacy of Connected and Autonomous Vehicles: A thematic analysis approach. Transportation research part F: traffic psychology and behaviour, 75, 66-86.

Litman.T. (2021), Autonomous Vehicle Implementation Predictions: Implications for Transport Planning, Victoria Transport Policy Institute, 17 December 2021.

Mariani, R. (2018, March). An overview of autonomous vehicles safety. In 2018 IEEE International Reliability Physics Symposium (IRPS) (pp. 6A-1). IEEE.

Moharrum. M and Al-Daraiseh. A, Toward Secure Vehicular Ad-hoc Networks: A Survey, IETE Technical Review (Medknow Publications & Media Pvt. Ltd.), vol. 29, no. 1, pp. 80-89, Jan/Feb 2012.

Muhammad, G., and Alhussein, M. (2021). Security, Trust, and Privacy for the Internet of Vehicles: A Deep Learning Approach. IEEE Consumer Electronics Magazine, 1. https://doi.org/10.1109/mce.2021.3089880

Mutzenich, C., Durant, S., Helman, S., and Dalton, P. (2021). Updating our understanding of situation awareness in relation to remote operators of autonomous vehicles. Cognitive Research: Principles and Implications, 6(1). https://doi.org/10.1186/s41235-021-00271-8

Petersen, L., Robert, L., Yang, J., and Tilbury, D. (2019). Situational Awareness, Driver's Trust in Automated Driving Systems and Secondary Task Performance. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3345543

Poongodi, M., Vijayakumar, V., Al-Turjman, F., Hamdi, M., and Ma, M. (2019). Intrusion prevention system for DDoS attack on VANET with reCAPTCHA controller using information-based metrics. IEEE Access, 7, 158481-158491.

Qian, Y., and Moayeri, N. (2008, May). Design of secure and application oriented VANETs. In VTC Spring 2008-IEEE Vehicular Technology Conference (pp. 2794-2799). IEEE.

Rashid, S. A., Hamdi, M. M., and Alani, S. (2020, June). An overview on quality of service and data dissemination in VANETs. In 2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) (pp. 1-5). IEEE.

Sateesh, H., and Zavarsky, P. (2020, November). State-of-the-Art VANET Trust Models: Challenges and Recommendations. In 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON) (pp. 0757-0764). IEEE.

Sun, X., Cao, S., and Tang, P. (2021). Shaping driver-vehicle interaction in autonomous vehicles: How the new in-vehicle systems match the human needs. Applied Ergonomics, 90, 103238. https://doi.org/10.1016/j.apergo.2020.103238

Zavvos, E. Gerding, V. Yazdanpanah, C. Maple, S. Stein and m. Schraefel, Privacy and Trust in the Internet of Vehicles, IEEE Transactions on Intelligent Transportation Systems, pp. 1-16, 2021. https://doi.org/10.1109/tits.2021.3121125

Zubairu, B. (2018). Novel approach of spoofing attack in VANET location verification for non-line-of-sight (NLOS). In Innovations in Computational Intelligence (pp. 45-59). Springer, Singapore.