2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom)
and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)

Autonomous Vehicle Security: A Taxonomy of Attacks and Defences

Vrizlynn L. L. Thing[1] and Jiaxi Wu[2]

[1]Cyber Security & Intelligence Department,
Institute for Infocomm Research, A*STAR, Singapore
vriz@i2r.a-star.edu.sg

[2]Department of Bioengineering,
Imperial College London, United Kingdom
jiaxi.wu14@imperial.ac.uk

***Abstract*—In recent years, we have seen significant advancement in technologies to bring about smarter cities worldwide. The interconnectivity of things is the key enabler in these initiatives. An important building block is smart mobility, and it revolves around resolving land transport challenges in cities with dense populations. A transformative direction that global stakeholders are looking into is autonomous vehicles and the transport infrastructure to interconnect them to the traffic management system (that is, vehicle to infrastructure connectivity), as well as to communicate with one another (that is, vehicle to vehicle connectivity) to facilitate better awareness of road conditions. A number of countries had also started to take autonomous vehicles to the roads to conduct trials and are moving towards the plan for larger scale deployment. However, an important consideration in this space is the security of the autonomous vehicles. There has been an increasing interest in the attacks and defences of autonomous vehicles as these vehicles are getting ready to go onto the roads. In this paper, we aim to organize and discuss the various methods of attacking and defending autonomous vehicles, and propose a comprehensive attack and defence taxonomy to better categorize each of them. Through this work, we hope that it provides a better understanding of how targeted defences should be put in place for targeted attacks, and for technologists to be more mindful of the pitfalls when developing architectures, algorithms and protocols, so as to realise a more secure infrastructure composed of dependable autonomous vehicles.**

***Index Terms*—Autonomous vehicles, safety and security, attacks and defences, smart cities, taxonomy.**

I. Introduction

With the push for innovations in smart cities, we have seen significant effort put forth that results in the enhancement of efficiency in the work environment and standard of living worldwide [1]. An important consideration in all smart cities is its transportation infrastructure and system. Recently, in Singapore, we see autonomous vehicles (AVs) being taken onto the streets in the form of taxis [2]. It is expected that more AVs will start to roam the roads in many other countries in the near future. As self-driving vehicles are equipped with more sensors and network connectivities than non-autonomous ones, the number of security vulnerabilities and thus, attack surface of an AV is undoubtedly increased.

Adversaries today are becoming increasingly skillful. The skillset coupled with feasible low-cost offensive devices can enable them to break into car security systems easily. It is imperative to bring to the attention of stakeholders, the existing methods of attacking an AV, whether it is by connecting to a certain port of the vehicle or hacking wirelessly into the vehicle's network. It is also important to find out which corresponding defence methods can be applied to counteract the attacks most effectively.

In this paper, we aim to organize and discuss the various methods of attacking and defending AVs. We will first explore the background on AV security and its challenges in Section II. Section III includes examples of attacks on AVs and a proposed taxonomy that can be used to classify various AV attack scenarios. We will next explore the various ways of defending the security of AVs, with a proposed defence taxonomy, in Section IV. We conclude our paper in Section V.

II. Background

Based on the recent high profile simulated attacks, it has become common knowledge that AVs are not entirely secure from malicious attacks. Before presenting our taxonomy of attacks and defences in the next sections, we first discuss why AVs are susceptible to attacks, and different approaches to test the security of AVs.

A. Increase in communication channels

When compared to non-autonomous vehicles, AVs are more susceptible to malicious cyber-attacks mainly due to the following two reasons:

1) Increased external communication between AVs and the external environment: One main type of communications is the inter-vehicular (V2V, vehicle-to-vehicle) communications that occurs on the road via the vehicular ad hoc networks (VANETs). It allows information-sharing among nearby autonomous vehicles so that each vehicle is better aware of its rapidly-changing surroundings [3]. In future, vehicle-to-infrastructure (V2I) and vehicle-to-Internet of Things (V2IoT) communications will also become more prevalent on the roads. Hence, once an

978-1-5090-5880-8/16 $31.00 © 2016 IEEE
DOI 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52

infected AV is connected to its surrounding environment, the entire network of AVs may be compromised if there is a lack of security measures.

2) Increased internal communication among systems within the AV, also known as intra-vehicular communication: AVs have many electronic control units (ECUs) interconnected via the controller area network (CAN) bus. One advantage of having a CAN bus in a vehicle is that it acts as a central network where different modules can be added to or removed from it without affecting the entire vehicle's wiring architecture. The CAN bus is currently structured into three parts:
   - Data link layer (responsible for transferring data between adjacent network nodes)
   - High-speed CAN physical layer
   - Low-speed, fault tolerant CAN physical layer

   In a modern automobile, the more important ECUs directly impact the safety of the vehicle occupants during the vehicle's operation, and are connected to the high-speed CAN layer. Examples of these ECUs are the engine control module (ECM), emergency brake control module (EBCM) and transmission control module (TCM). Other ECUs, such as the radio and remote control door lock receiver (RCDLR), are connected to the low-speed CAN layer. When necessary, a gateway bridge can route selected data between these two layers. Thus, there exists a possibility that malicious data packets are introduced into the AV's low-speed CAN layer without any detection or suspicion, before being transferred to the high-speed CAN layer via the gateway bridge, leading to more serious consequences.

   Within the AV system, CAN packets are broadcasted to all nodes. A malicious component on the internal network can thus snoop on all communications or broadcast packets to the other components. Therefore, every communication pathway within the AV should be sufficiently protected in order to ensure the security of the entire vehicle. Inevitably, there will always be new strategies devised by adversaries to threaten the security of AVs. Attacking and defending AVs is a continuous cycle. The development and improvement of one will always counteract and necessitate the development of another.

Besides its broadcast nature, another reason that the CAN bus is vulnerable to attacks is also due to the fact that CAN packets contain no authenticator field or source identifier field. Any component can indistinguishably send a packet to any other component if the former does not implement any defence mechanism [4]. One possible defence is to use the packet level authentication [5] to enable any node or component on the network to verify the authenticity of any packet without any trust association with the packet sender. This will be further discussed in Section IV.

B. Security Testing Approaches

Many practical experiments have been carried out to test the security of vehicle systems against attacks. Target modules of these tests include the airbag control system, car warning lights and electric window lift [6]. There are three main approaches to test the security or resiliency of the vehicle against attacks:

1) Bench simulations, where physically extracted hardware from the car are analysed in the lab
2) Running a CAN network analyser together with the attack tool, which may be carried out via wireless connection or connecting a laptop to the vehicle's OBD-II port
3) Testing the ECU behavior in a controlled environment, e.g. where the vehicle is immobilized on jack stands while mounting attacks

It is inevitable that a simulated attack differs from a real attack since it only represents a subset of the real attack. If the system fails after the simulated attack, it is positively proven that the system does not resist well to the real attack. On the other hand, if the system resists well against the simulated attack, it does not entirely prove resistance against the real attack, but only against the attacks which match the simulation conditions. Nonetheless, simulated attacks are necessary and useful during preliminary testing stages for finding security loopholes in AVs.

There may be ECUs which cannot be reached by the above three approaches. It may be due to the fact that the ECU is not directly connected to the CAN bus, but indirectly connected via another sub-system. One example is the Local Interconnect Network (LIN) sub-bus system, which is made up of one master control module and up to 16 slave control modules. All the communication is initiated only by the master control module only. The slave control modules cannot initiate communications in an independent manner. The master control modules of different LIN buses are connected to the CAN bus and thus, information may not be fully transmitted from the CAN bus to the slave control modules.

III. Attack Taxonomy

In this section, we classify the potential threats, vulnerabilities and attacks that an AV may encounter. We categorise each attack accordingingly to its type of attacker (source), attack vector (method), target, motive (objective/reason) and potential consequences (outcome).

A. Attacker

The attacker is the source or origin of the attack. When faced with a system error that appeared in the vehicle, other than responding to the error to resolve and mitigate it, steps should also be taken to identify the attacker is. Attacker identification helps not only in attribution and detering future attacks, but also enables understanding of the attack vectors and motives to strengthen proactive defence measures.

B. Attack Vector

An attack vector is a path or means by which an adversary can gain unauthorized access to a target system. It is also an enabler for adversaries to carry out vulnerability exploitation on the target systems. Adversaries could gain unauthorized access to autonomous vehicles via either physical access (or close proximity access) or wireless remote access.

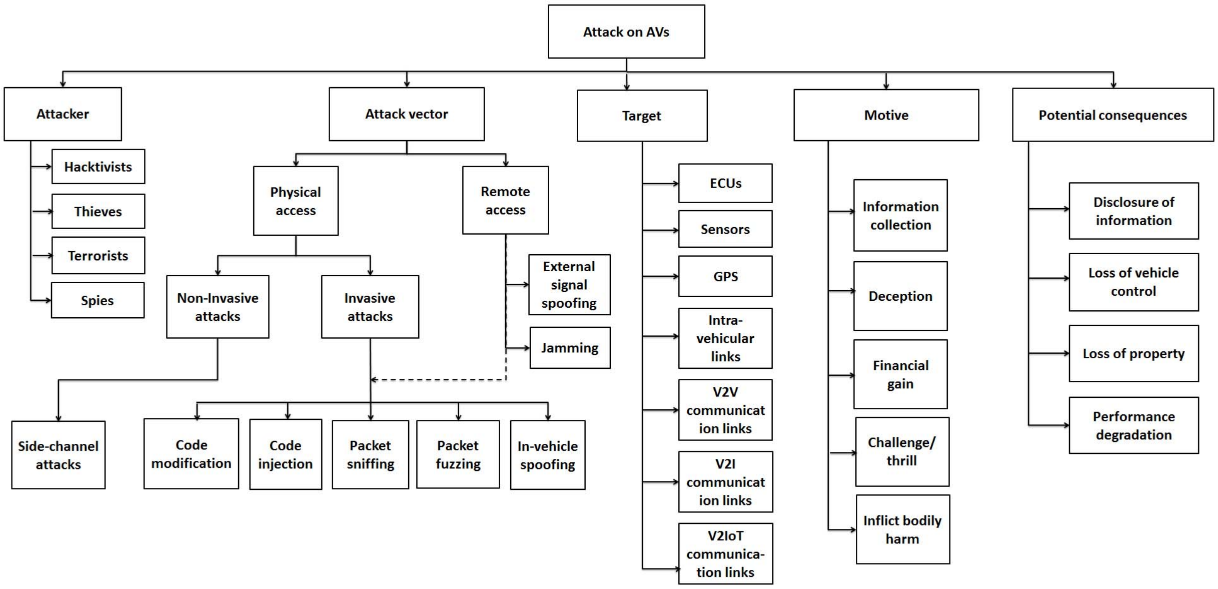

Fig. 1: Autonomous Vehicle Attack Taxonomy

1) Physical Access:

First, we look at attacks that require physical access to the vehicle. We classify these attacks further into non-invasive and invasive forms.

Non-invasive Attacks

In non-invasive attacks, the embedded device is not disassembled and physically tampered with. Thus, close proximity to the AV is needed to launch the attacks.

Side-channel attacks: A side-channel attack refers to attacks that result in revealing useful information regarding the transmitted data or the internal working of the system through alternative paths. This attack attempts to retrieve information indirectly and mainly exploit information leakage. Examples of side-channel attacks include capturing and analysing timing information, power consumption, electromagnetic leaks, acoustic signal analysis and data remanence. Defences against side-channel attacks include utilizing asynchronous processing units and shielding mechanisms (help in reducing electromagnetic emissions).

Invasive Attacks

The diagnostic OBD-II port in an AV is an opening where adversaries can connect to, so as to gain access to the vehicle's bus systems and thus, its ECUs. This attack vector can lead to several types of invasive attacks, where the security of the networks and ECUs can be compromised. In the situation where the AV is connected to the critical infrastructure and is exposed to external networks (e.g. connected to smart phones as point of control for on-vehicle devices such as the entertainment system), wireless remote access is made possible, and may further result in potential over-the-air attacks, which we will discuss in the subsequent sub-section. Here, we focus on the different categories of invasive attacks that require physical or close proximity access to the AV.

Code Modification: The OBD-II scanner is an inexpensive tool that is widely available to owners or maintenance personnel who wish to perform a diagnosis of the vehicles. More technologically advanced scanners may also have a chip-tuning feature which is able to extract and modify ECU codes. However, such tools may also be used by an adversary to carry out malicious modifications of code to compromise the system. Defences against such attacks is to ensure connections to the vehicle are password-protected so that only authorized personnel are granted access, and that only authorized and verified code modification can be carried out.

Code Injection: Similar to the code modification attacks, an adversary may inject harmful codes into ECUs after gaining access to the vehicle's networks and ECUs. Malicious payloads such as viruses, Trojan horses and spyware may infiltrate an AV through this approach too. The vehicle owners may also inject codes in the hope to improve the performance of their vehicle or to deceive regulatory checking when one or more of the vehicle's components or sub-systems are non-compliant. One method to defend against this attack would be via an intrusion detection system and finer granularity control over privileged access that should only be given to authorized personnel, which in certain circumstances, may not include the vehicle's owners.

Packet Sniffing: A packet sniffer, which can intercept and log traffic that is transmitted over a communication link, is commonly used to diagnose network-related problems. In other words, it enables the viewing of the communication details between two or among multiple nodes. Although it is a useful tool for analysts to diagnose AVs, an adversary can also use sniffers to eavesdrop on unencrypted data in the packets and collect information. It is also possible to capture packets for a replay attack. Possible defences against packet sniffing include deploying encryption techniques to protect the confidentiality of the packets in transit, as well as deploy techniques to ensure and verify the freshness of the communication signals sent and received.

Packet Fuzzing: In fuzzing, invalid data is sent to the target system or modules to explore the potential of triggering an error condition or fault. These error conditions can lead to exploitable vulnerabilities and expose security loopholes. In fact, this technique can also be used for security testing. When used during security testing, fuzzing is utilized to detect problems in the system that may lead to security issues at a later stage. Thus, to defend against adversaries, security loopholes can be identified at an early stage if testing is conducted regularly. System updates should also be put in place to fix any issue found. These updates should also be verified to be authentic before being introduced into the system.

In-Vehicle Spoofing: A spoofing attack involves the masquerading as another to falsify data. During spoofing, the adversary would need to overcome the security measures of the AV, to replace authentic components or modules with spoofing devices, or spoof in-vehicle signals so as to forge control and data packets during the vehicle's operation. Defences against in-vehicle signal spoofing include replay attack resistant techniques and module fingerprinting such as utilzing the unique but subtle clock skew of modules to differentiate between an authentic and spoofed module [8].

2) Remote Access:

Attackers may also exploit the AV's enhanced connectivity, especially the wireless connection and external facing sensor interfaces such as its LiDAR, camera and GPS.

External Signal Spoofing A specific example of external signal spoofing is GPS spoofing, which occurs over the wireless connection. This attack attempts to deceive the GPS receiver by broadcasting incorrect GPS signals through another device. The forged signal either resembles the normal GPS signals, or is a replay of the genuine signals which was captured previously. The power strength of the counterfeit signal is gradually increased by the adversary to subsequently replace the genuine signal. Eventually, the receiver only recognizes the counterfeit signal. Once the adversary is in control of the AV, it will be fed with false information that it is drifting off-course and needs to return to its right path. GPS spoofing attacks had been successfully tested on an unmanned aerial vehicle (UAV) [9] and a yacht on sea [10]. This attack is also applicable to AVs on the road as they also rely on the GPS system.

AVs are equipped with a number of sensory features. Vital vehicle sensors, such as the camera and LiDAR, are easy spoofing targets, as shown by a research work by Petit [11]. In this research, pulses of signals were recorded from a commercial LiDAR unit into a laser pointer. As these pulses were neither encoded nor encrypted, they could be repeated at any point using the laser pointer. Similar to the previous example of GPS spoofing, the counterfeit LiDAR signal was synchronized with the real one. Consequently, the LiDAR sensor on the AV detected multiple simulated and non-existent obstacles in its surroundings, ranging from 20 to 350 metres from the sensor. This denial-of-service (DoS) attack may even hinder the AV from detecting the signals of real objects.

To defend against GPS spoofing, we need to make the GPS system more secure. A feasible approach would be a combination of authentication and integrity verification techniques to prove that the signals come from authentic sources, as well as protecting the signals from being tampered with.

To protect against LiDAR signal spoofing, vehicle manufacturers can consider implementing countermeasures such as getting additional information using other sensors or from other vehicles in the vicinity, so as to perform verification of the received information from the LiDAR sensor. The system can then cross-check with this collected data and filter out those that are not plausible.

Jamming

Jamming attacks are availability attacks against the wireless medium or the external facing sensors. Consequently, the authorized communication is disrupted. Sensors that may be susceptible to this attack include the LiDAR and camera, where a jammer device can be used to block the sensors from receiving signals. In [11], blinding attacks are conducted on the AV camera by emitting light into the camera in order to hide objects from its view. Countermeasures against this attack include integrating a removable near-infrared-cut filter to the camera (only effective during day time as the filter needs to be removed at night for the AV to make use of infrared light for night vision) or the use of photochromic lenses (which can change color to filter out specific types of light).

An attack example which is composed of jamming and external signal spoofing (through replay attack) is through Samy Kamkar's invention of the RollJam device [7]. Most vehicles use a rolling code system preventing the reuse of the same code to unlock the vehicle's door the next time. The RollJam device is designed to unlock a vehicle's door without the use of the authorized car key fob. Upon the first press of the original key fob, the RollJam device jams and records the first signal, and the door fails to unlock. Naturally, the vehicle owner will press the key for the second time, which causes the RollJam to jam and record the second code, and also simultaneously broadcast its first code. The car door, upon receiving the first code, unlocks, but the RollJam has already stored the other legitimate code and is able to unlock the car door the next time using this code. This attack can be counteracted by foiling the RollJam attacks through the replacement of the codes with a system of rolling codes that expire over a short time period.

C. Attack Target

In an AV, good system health of the ECUs, sensors, GPS and networks is vital as they work together and contribute to its normal functioning. For example, the VANET is extremely useful in optimizing traffic in an urban environment to enable the reduction of congestions and pollution, while at the same time, increase passenger safety and comfort. The camera and LiDAR on the other hand, are the "eyes" of the AV and enable it to recognize objects, so that the AV can trigger further actions such as to avoid collision with obstacles. The targets of the attacker are usually motivated by the attacker's intention and the motive or the objective of the attack.

D. Attack Motive

Knowing the attackers' motives may help us put more emphasis into protecting certain parts of an AV, such as the ones that control its driving safety. An example of the motive of attackers may be to spread false information to influence the behavior of others. This is known as Deception. Malicious nodes may be injected into the VANET and deceive healthy nodes to believe information given by the malicious nodes. This attack can thus lead to hazardous situations for vehicles on the road. Another motive could be for financial gain, where thieves manipulate windows or doors of the AV so as to steal valuables that were left in the vehicle. A more serious motive with dire consequence may be to commit murder or cause severe bodily harm to the passengers in the AV.

E. Potential Consequence

This category describes the results at the end of the attack. A denial of service attack may cause certain functions of the AV to fail. If attackers succeed, there is a possible leakage of data, such as sensitive data on vehicle movements [12]. An attack may also illegally sabotage the proper functioning of the AV and cause loss of vehicular control on the road. Another consequence is that the AV's system health may also deteriorate, possibly increasing its risk of being targeted and attacked successfully during subsequent attempts.

IV. Defence Taxonomy

The problem with new attack tactics such as the RollJam is that we can never predict it before it happens. However, by expanding our knowledge about the potential security vulnerabilities, threats and attacks (as we did in the previous section), we can develop architectures, algorithms and protocols to realise a more secure infrastructure composed of dependable AVs.

There are four main categories of AV defences: preventive defence, passive defence, active defence and collaborative defence. Having various ways and layers of defence ensures a heightened level of security preparedness and resilience against attacks. Each defence category is presented and discussed as follow.

A. Preventive Defence

In preventive defence, the approach towards securing the systems mainly focuses on protection measures to defend and attempt to stop an attack from happening or become successful. It takes into consideration the normal operating conditions of the system and has lesser weight on considering the circumstances during or after an attack.

1) Secure Communication:

Encryption is fundamental and crucial in protecting vehicular data transmission. Through encryption, the confidentiality of the data transmission can be assured. Depending on the encryption scheme used, it may also be possible to rely on the keys to verify the identity of the sender. It is also necessary to have message authentication code (MAC) algorithms in place to protect and verify the integrity of the data being received.

2) In-Vehicle Device Authentication:

To ensure that the controllers of the AV can be trusted, certificates can be issued to support the authentication process, as proposed in [13]. Each of the controllers will then possess a certificate which includes its controller identifier, public key and its authorization (i.e. actions that it's authorized to carry out). The gateway will hold the list of public keys with all the accredited Original Equipment Manufacturers (OEMs) of the vehicle. If the authentication process succeeds, the respective controller and its authorization are added to the gateway's list of valid controllers .

3) User Authentication:

Another way of ensuring the authorized usage and control of the AV is to employ additional, albeit seamless layer of user authentication such as biometric identification. Biometric authentication deployed on the AV, it can be used to control access to the vehicle door lock, as well as the engine ignition system.

4) Firewall:

A firewall is a network security system that controls incoming and outgoing network traffic based on a set of rules. It is also relevant for AVs to have such segregation which acts as a barrier between the trusted network and other untrusted or less-trusted networks within the vehicle or in the V2V, V2I and V2IoT scenarios.

B. Passive Defence

Adversaries that have the opportunity, intent and capability to do harm or cause damages, may bypass preventive defences. Thus, passive defence should provide another layer of defence against the adversaries. In contrast to active defence, passive defence does not consider the moving target or adaptive security mechanisms, and do not require interactions with human analysts.

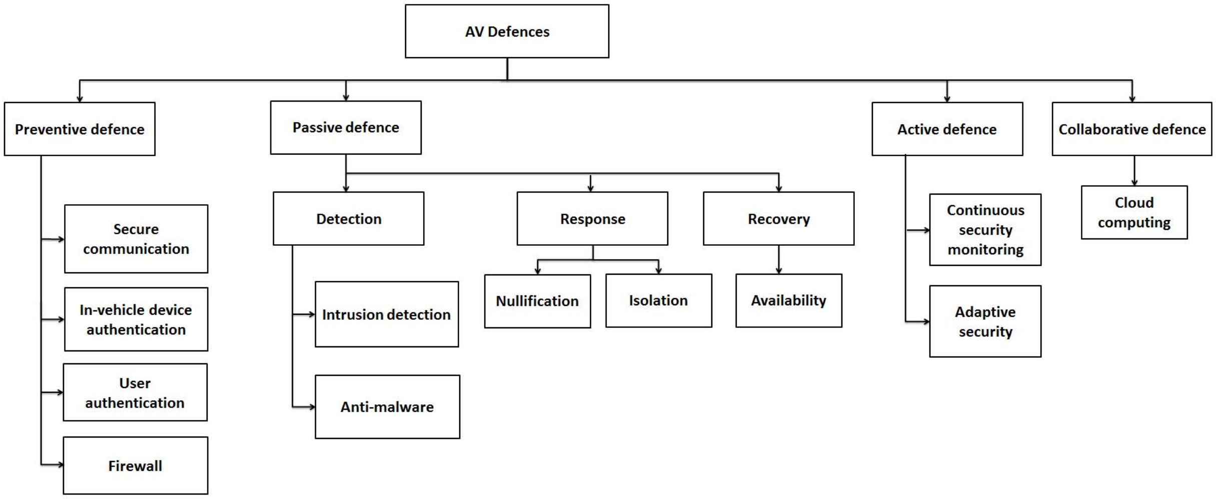

Fig. 2: Autonomous Vehicle Defence Taxonomy

1) Attack Detection:

Intrusion Detection

With the help of vehicle alarms (e.g. glass break audio sensor), modern vehicles can detect the occurrence of physical security attacks and alert its owner or any person in its vicinity. However, cyber attacks affecting the system's operations within the AVs may be less obvious or detectable. Nonetheless, different models of Intrusion Detection System (IDS) for AV security [14], [15] have been proposed and tested under computational simulation scnearios. Ideally, advancement in AV IDSes should continue and aim to achieve a higher accuracy in attack attempt detections.

In [8], the authors proposed a method to detect intrusion to the AV system by fingerprinting the clock skew (i.e. tiny timing errors within each module) of the ECUs and detect the ones that deviate from the authentic ones. This proposed method, also referred to as Clock-based IDS (CIDS) by the authors, allows a quick identification of in-vehicle intrusions with a low false-positive rate of 0.055%. Using CIDS, it is also possible to identity which ECU launches the attack.

Anti-Malware

As in normal computer systems, anti-malware solutions for AVs should be capable of defending the AVs from harmful software that attempt to infiltrate the system. As malwares for AVs are still in its infancy, there may not be a high number of malwares available in the wild. Nonetheless, signature based detection can be put in place, by first considering these malwares. At the same time, the research community should also focus more of their effort on AV attack modeling, novel malwares designed specifically for AVs, and behavioural based malware detection and mitigation for AVs.

2) Attack Response:

Nullification

Nullification refers to the ability of an entity to invalidate or neutralize a cyber-attack by using electronic or cyber capability. An example is the use of the GPS anti-jamming technologies [16]. GPS anti-jamming technologies utilizes null-forming to supress interference from jamming devices. Nominal performance of such technologies can reach 40 dB of interference suppression.

Isolation

Self-isolation of the AV during an attack can help prevent other vehicles from receiving false information. Another example is to reject the re-programming of ECUs while the engine is still running. Besides self-isolation, when an attack is attempted on an AV, the vehicle should ideally respond in a way where the other vehicles around it are made aware so that their appropriate security defence mechanism can be triggered.

Other than the AV self-isolation, at the system's level, the infected module or detected malicious code should also be isolated in a safe manner without affecting the critical operations of the AV when the engine is running.

3) Attack Recovery:

Availability

In critical systems, availability becomes a very important consideration. In the context of AVs, availability is of paramount importance as it is required so that the safety of the passengers and the other road users is not compromised. Thus, protection and fault tolerance mechanisms to ensure the AV's resiliency and that it can recover quickly in the face of an attack, has to be built into the system.

C. Active Defence

Countering advanced and determined adversaries would require an active approach to security. We discuss different approaches to active defence as follow.

1) Continuous Security Monitoring:

As AVs and its infrastructure are critical systems that can have serious consequences when their security is compromised, it is necessary to have near real-time situation awareness of their security health conditions. Thus, continuous security monitoring is required to provide snapshots of their states at regular intervals to assess their security status. It is also important to determine where and what to monitor so that the critical components and interfaces are not blindsided.

2) Adaptive Security:

In today's world, it is no longer sufficient to have static forms of defences while attacks targeting systems, networks and critical infrastucture continue to evolve at a fast pace. Therefore, it becomes necessary to design and deploy defence measure such that they are themselves, moving targets. Adaptive reconfiguration of attack targets and deception tactics can be employed to enable better control and flip the balance during an attack. In addition, detection models should also evolve through self-learning during their operation lifecycle so that they can adapt to detect new forms of attacks.

D. Collaborative Defence

1) Cloud Computing:

It may be possible for several AVs to help each other over the VANET to strengthen their cyber security. In the future, V2IoT communications may also be moved to the cloud. Although it will then become a central point of target for the adversaries, the target is by no means an easy one. More effort will need to be invested by the adversaries to breach an infrastructure that is managed by better trained security professionals. In addtion, with the possibility of more information relevance to security that can be gathered from this collaborative structure, it also becomes important to couple the security knowledge and intelligence that can be amassed at the cloud level with adaptive security defence to better protect the AVs and their critical infrastructure.

V. Conclusions

In this paper, we discussed the security of AVs in terms of vulnerabilities, attacks and potential defences. We then proposed a comprehensive taxonomy to better categorize AV attacks as well as AV defences. By expanding our knowledge about the potential security vulnerabilities, threats and attacks in an AV, as well as their corresponding defence approaches, we can be more mindful of the pitfalls when developing architectures, algorithms and protocols to realise a more secure and dependable AV and its infrastructure. Last but not least, regardless of the defence mechanisms that need to be introduced, it is of paramount importance that the solution's efficiency and non-compromise to the normal real-time operations of the vehicle are taken into serious considerations.

References

[1] V. L. L. Thing, "Cyber security for a smart nation," in *IEEE Computational Intelligence and Computing Research, pp. 1-3*, 2014.

[2] The Associated Press, "World's 1st self-driving taxi debut in singapore," http://www.bloomberg.com/news/articles/2016-08-25/world-s-first-self-driving-taxis-debut-in-singapore, August 2016.

[3] S. Kumar, L. Shi, N. Ahmed, S. Gil, D. Katabi, and D. Rus, "CarSpeak: a content-centric network for autonomous driving," in *ACM SIGCOMM Computer Communication Review, Special October issue SIGCOMM 2012 archive, Vol. 42, No. 4*, 2012.

[4] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *IEEE Symposium on Security and Privacy*, 2010.

[5] D. Lagutin, "Packet level authentication overview," in *77th Internet Engineering Task Force*, March 2010.

[6] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks - practical examples and selected short-term countermeasures," in *Computer Safety, Reliability, and Security, Lecture Notes in Computer Science, Springer, Vol. 5219, pp. 235-248*, 2008.

[7] S. Kamkar, "Drive it like you hacked it," DEFCON, August 2015.

[8] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *USENIX Security*, August 2016.

[9] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and H. T. E., "Unmanned aircraft capture and control via GPS spoofing," in *Journal of Field Robotics*, 2014.

[10] A. Couts, "Want to see this $80 million super yacht sink? with GPS spoofing, now you can!" http://www.digitaltrends.com/mobile/gps-spoofing/, accessed on 29 September 2016.

[11] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicle sensors: Experiments on camera and LiDAR," in *BlackHat Europe*, November 2015.

[12] M. K. Nasir, A. K. M. K. Islam, M. T. Rahman, and M. K. Sohel, "Taxonomy of security in vehicular ad-hoc network," in *International Journal of Scientific and Research Publications, Vol. 3, No. 3*, March 2013.

[13] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," in *The Workshop on Embedded Security in Cars*, 2004.

[14] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," in *PLoS ONE Vol. 11, No. 6*, June 2016.

[15] K. M. A. Alheeti, A. Gruebler, and K. McDonald-Maier, "On the detection of grey hole and rushing attacks in self-driving vehicular networks," in *Journal of Computers, Vol. 5, No. 3*, July 2016.

[16] Novatel, "Anti-jamming technology," http://www.novatel.com/solutions/anti-jamming-technology/, accessed on 29 September 2016.