Literature Study Final Report – CPRE 537 Group 2

5G Vehicular Ad-hoc network (IoV) security

Abstract:

As vehicles become smarter, they are becoming interconnected to more devices, people, and infrastructure. With the large number of vehicles on the road, and their increasing criticality in sharing information, we must look towards new technologies that reduce data transmission latency and improve reliability. This means that security is going to become a larger concern as more services become interconnected and our reliance on such services increases. In our literature study we will be exploring the topic of 5G Internet of Vehicles (IoV); how it uses 5G's benefits, the different use case scenarios, security concerns and potential solutions, and finally, what research is taking place for the betterment of this technology. We will focus on reviewing security threats such as Authentication, MITM attacks and Jamming.

Introduction

The internet of things is an amazing concept only possible after the widespread adoption of the internet in developed countries. IoT is gaining in popularity and usefulness through the introduction of 5G wireless network technology. 5G started as a cellular network technology to enhance mobile broadband, widen bandwidths and create redundant and reliable device to device links. The use of network slicing has been introduced to improve the flexibility of the network. The device-to-device functionality of 5G improves spectral efficiency through allowing independent communication from the base station and core network. Some of the uses of the IoT concepts include vehicle to vehicle, vehicle to infrastructure and vehicle to pedestrian. Like every technology invented, there are security threats to the IoT devices and infrastructure. Some of these threats include authentication challenges, man in the middle attacks and signal jamming.

Introduction to IoV

What is the IoT?

The Internet of things concept is one of connecting anything with sensing and communication capabilities to the Internet and/or each other. These devices collect and transmit data over the Internet and include anything from cellular phones and industrial equipment, to washing machines and refrigerators. So, the general rule is to assume that anything that can be connected to the Internet will be connected, to make a giant network of connected things. The connections are not just among devices, but people as well in a people-to-people, people-to-things or things-to-things manner. The widespread connectivity through various communication technologies from Wi-Fi and Bluetooth to cellular data, using mobile broadband cloud computing, and smart terminals; all allowing this transformation of the way people perceive the world around them by generating new applications, business uses and general use cases as the technology is expanded. (Ahmad 2018) (Attaran 2019)

Benefits of 5G architecture in the IoT space

Cellular Ad-hoc network:

5G will support many types of smart devices from wearable technology and telemedicine to self-driving cars. As 5G expands in availability, the applications of IoT are going to increase behind the expansion. New technological advancements will follow from the fast speeds of 5G to handling hundreds of billions of connections with ultra-low latency transmission speeds. There is also the hope of providing more reliable services in rural areas to decrease the urban rural digital divide. (Attaran 2019)

Benefits of 5G technology include high reliability, low latency, and mobility. 5G has built on all the previous cellular technology that has been evolving since 1981. 1G was built on the existing analog technology of radios. 2G was the first to have digital technology standards, while improving coverage and capacity. The high-speed data transfer and video capabilities came with 3G. This is where mobile broadband was invented and had a significant improvement over 2G. 4G and 4G LTE improved the data capacity and speed, while being based on IP protocols. (Attaran 2019) (W Duan 2020)

The main improvements of the 5G systems over all previous cellular technology, includes enhanced mobile broadband, dynamic low latency, wider bandwidths, device-centric mobility, simultaneous redundant and reliable device-to-device links, more advanced antenna technology, and landline placement and shared spectrum. There is an expectation that 5G will cover about 40% of the world's population with approximately 1.5 billion subscribers by 2024. (Attaran 2019)

Range and layout are going to require a major change to move to 5G from 4G LTE. The old 4G network design used large high power cell towers to radiate signals over long distances, according to a grid of cell sites. 5G uses short range millimeter wave spectrum between 30 GHz and 300 GHz that is subject to interference from weather and physical obstacles. This is going to require many small cell stations spread across various types of mounting structures, from streetlights to rooftops. The short-range communications will allow faster speeds and more bandwidth for the consumer users of the network spectrum. The ability to support machine-to-machine communication is the main new feature that allows 5G to include Vehicle Ad-hoc Network (VANET) applications. In non-VANET uses, the machine-to-machine functions will allow lower battery consumption, lower power and lower latency than the old 4G network. The short-range system also allows an extreme mobile broadband level of access, along with hundreds of billions of connections. (Attaran 2019)

Autonomous cars and IoT devices are expected to be major revenue streams for the new 5G networks. Recent device count estimates expect there to be up to seven connected devices for every person on earth, or over 50 billion devices. Growth of IoT connected devices is driven by factors such as increasing availability of broadband Internet and tremendous decrease in the cost of connecting to the Internet and bandwidth. (Attaran 2019)

Network Slicing:

Network slicing divides a network into multiples separate logical networks. Because the standard “one-size-fits-all" network architecture is not scalable and flexible enough to address the various cost, performance and security requirements, network slicing is an approach proposed to enable 5G network

customization. The smaller separate networks can provide areas to customize for different services and use cases (Zhang 2019).

The 3 main categories of 5G use cases are as follows:

- Enhanced Mobile Broadband Connectivity (eMBB); This is a use case that enhances current mobile broadband by improving the connection speeds and reliability in the increasing demand of high-speed trains, autonomous vehicles and aircraft.
- Massive Machine Type Communications (mMTC); This category supports the requirements of low-cost, low-power, long-range MTC devices which are expected to be of a high density in the near future. People's clothing, traffic meters, environmental monitoring and most other smart services fall under this category.
- Ultra-Reliable Critical Communication Services (URCC); This category caters to use cases that depend on real-time interaction.

The key implementation of Network slicing is to split the physical layer into several virtual layers, but overall, there are 3 logical network layers (Zhang 2019):

- Service Instance Layer: Represents the end user services or business services that can be supported. Each service is represented by a service instance.
- Network Slice Instance Layer: Includes the network slice instances that can be provided. A network slice instance provides the network features that are required by the service instance.
- Resource Layer: Provides all virtual or physical resources and network functions that are necessary to create a network slice instance.

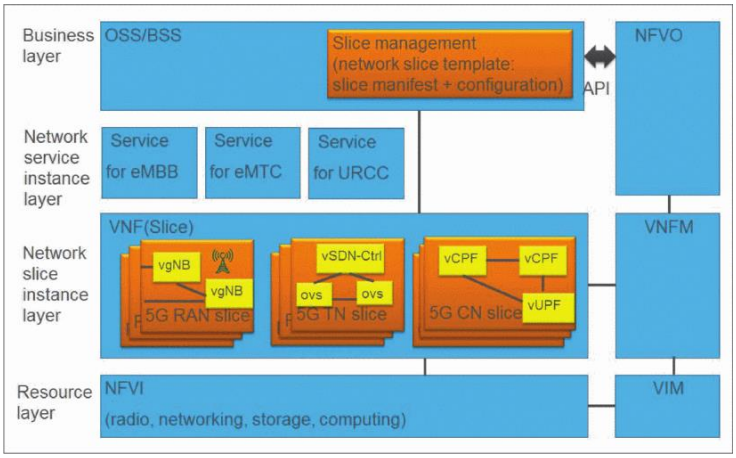


Figure 1: Graphical representation of the network slices (Zhang 2019)

We already have many virtualization and cloud computing services, which are leveraged so that shared physical resources can be dynamically allocated to the 3 logical network layers. This means that various

use cases like radio access networks, cloud infrastructure and transport networks get resources allocated based on their changing needs as the network slices can adapt and schedule resource pooling.

In IOV scenarios, the following approach is advised by W. Duan *et al*:

The future development of 5G IoV applications will have the requirements to improve the flexibility of the system using slicing by controlling slice granularity, integrate artificial intelligence to adjust network resources to maximize the slice management with minimal effort and consider the impact on other slices and the overall network when designing security protocols. (W Duan 2020)

Spectral Efficiency Improvement with 5G:

Device to device (D2D) improves spectral efficiency, energy efficiency, throughput, delay and network fairness by allowing independent communication from the base station and core network. This is one of the key technologies in LTE and 5G communications. The frequent changes of the network structure, environment topology and demands leave traditional D2D not completely satisfying these needs. (W Duan 2020)

Research done by J. Wang *et al* implemented 3 key 5G technologies to perform field tests with respect to spectral efficiency improvements. They used Sparse code multiple access (SCMA), Polar codes, and filtered orthogonal frequency-division multiplexing (f-OFDM) to test their results using a 5G testbed designed by NTT DOCOMO and Huawei.

Since the complete explanation of the technologies is out of this paper's scope, a very brief explanation and comparison with the previous iteration of technology is attempted:

SCMA:

Where OFDMA is an orthogonal multiple access technique meaning sub-channels eliminate crosstalk and inter-carrier guard bands is not required, SCMA is non-orthogonal. The term “sparse code” comes from the idea that multiple user equipment share the same time-frequency resources by mapping their data onto different sparse codewords (J.Wang et al, 2017). Each layer in SCMA has its dedicated codebook mapping, so each incoming data stream is mapped to a codeword, where each codeword represents a spread transmission layer. From their research, they claim that depending on how the codebook is designed, there can be higher coding gain. To simplify, the codebook is an algorithm to decode the transmissions in different subchannels/sub-carriers.

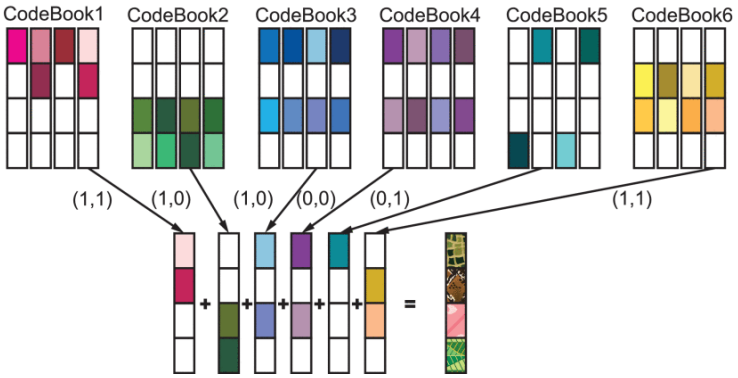


Figure 2: SCMA multiplexing

Polar codes:

This is based on Shannon's information theory with the same concept as error correction coding, where the idea is that it is possible to achieve error-free transmission even in very noisy channels through channel coding up to channel capacity. Shannon did not elaborate on how to achieve "channel capacity" codes. LTE uses Turbo codes which come close to channel capacity but fails this tasks. The Polar Codes coding scheme is proven to achieve channel capacity. The paper also states that under the same MCS (modulation coding scheme), polar code has higher successful decoding rates than LTE Turbo scheme with similar channel conditions. Their experiment claims that polar has higher throughput and better coverage.

f-OFDM:

A paper by Javad *et al* proposed the implementation of filtered OFDM. The paper mentions that the drawbacks of regular OFDM are high peak-to-average power ratio (resolved in LTE Discrete Fourier transform-spread) and high side lobes in frequency. OFDM has a rectangular pulse shape whose side lobes drop with frequency *f*. The frequency spectrum is therefore not well optimized, which can interfere with other systems in adjacent carriers (Javad et al). Another important note is that frequency mask regulations force OFDM to reserve 10% of edge frequency as a guard band, reducing spectral efficiency. The proposal stated that f-OFDM has all the advantages of regular OFDM (even LTE's improvements) but additionally allows asynchronous multiple access. Finally, the authors claim that f-OFDM enables the "co-existence of different time-frequency granularities, e.g., different subcarrier spacings, in the system so that different parts of the waveform in frequency can be optimized for different transmission conditions and applications."

Their baseline comparison was done with LTE settings (OFDMA, Turbo codes and no filter) and then they experimented by enabling each of the three 5G technologies to find a result that showed 100% spectral efficiency improvement over the baseline. Particularly, they gained 90% efficiency by utilizing SCMA

compared to OFDMA. Polar coding resulted in around 10% more gain compared to LTE's coding scheme. Their f-OFDM method gained another 7% while there was only a limited impact of interference from neighboring spectrum bands.

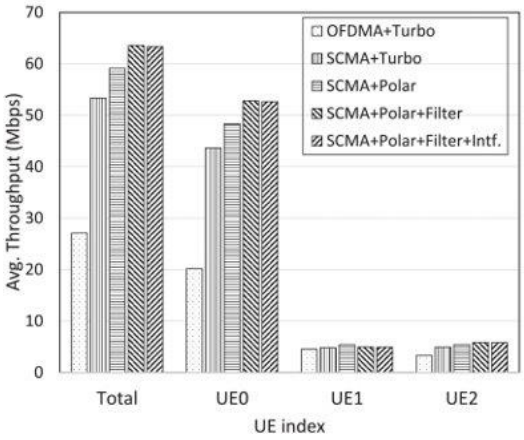


Figure 3: Throughput Improvement Diagram

IOV use cases (Applications of 5G technology)

Many technologies have been incorporated into the Internet of Vehicles (IoV) systems, including global position system (GPS), radio frequency identification (RFID) sensors, and data mining. Vehicle-to-everything (V2X) is an expansion of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) to adapt to the emerging integrated environment of a variety of devices beyond just vehicles and roadside modules, such as vehicle-to-pedestrian (V2P) and vehicle-to-infrastructure/network (V2I/N). V2X technology allows information sharing for a single vehicle and improves the autonomous driving ability and intelligence level. This allows the building of comprehensive services that include comfortable, safe, intelligent, efficient and energy savings. So far, the main technology used in V2X systems has been cellular mobile communications and dedicated short range communication (DSRC). (W Duan 2020)

Traditional network architecture is based on static fixed elements, which is the opposite of the IoV architecture with its requirements for rapid development, mass management, high quality service and real time application. 5G telecommunications technology is being rapidly developed on a large commercial scale to be able to help solve some of these issues. 5G combines ultra-dense network and device-to-device (D2D) along with massive multi-input multi-output (MIMO) to achieve diverse application performance scenarios using a more flexible architecture. The benefits of the new 5G technology are expected to solve some of the IoV issues with previous technology, such as a better performance for the vehicle communications unit while engaging in high-speed transitions. It is

expected that 5G will enable IoV to operate without constant connection to the service infrastructure and base station. (W Duan 2020)

Vehicle-to-Vehicle:

The Internet of things has captured many different areas, including transportation. Intelligent transportation systems technology has several types of communication, one of which is the vehicle ad-hoc network (VANET). VANET allows connected vehicles to communicate among each other and roadside units (RSUs). This type of communication has the potential to offer traffic efficiency and improve road safety. Various applications can be provided to the connected vehicle ranging from road condition warnings like step curve alerts and collision avoidance, to infotainment. (Ahmad 2018)

The Internet of vehicles (IoV) is a new emerging sub field of the IoT revolution, made possible by the advent of 5G wireless technology. The high bandwidth and low latency connections will allow real time tracking and transmission in high traffic areas to support vehicle movements. There is an expectation for the automotive industry to have a 20% impact out of the total economic impact of 5G in amounts close to $2.4 trillion. This covers the automotive supply chain and consumer purchasing. The impact to the automotive industry is expected to be about $67 billion generated to the sector and include the prospect of self-driving cars. (Attaran 2019)

Self-driving cars are expected to make intelligent driving safer and more efficient to have a positive impact on future autonomous urban ride services. These benefits can only be realized with 5G due to the high bandwidth, quick responses and continuous connectivity requirements from the network. The network providers can support these requirements with new robust 5G connections. The consumer will be interested in purchasing the smart cars due to the ability of auto manufacturers to offer more services, including navigation, traffic information, e-tolling, hazard and collision warnings, weather updates, media streaming services and cybersecurity updates. Autonomous vehicles show promising benefits with the possible reduction in drunk, fatigued or distracted drivers. People could be freed from the task of having to drive, while traffic congestion could be reduced. (Attaran 2019) (Liu 2020)

Network congestion will result from the security information for the vehicles exceeding the load the base station can manage when there is a large density of vehicles. For conventional low data rate mobile services, the traffic normally goes through the base station. Direct communications are being widely considered as high data rates are being rapidly developed. (W Duan 2020)

Current research issues include large scale D2D communications, dynamic QoS requirements, D2D communication cellular networks and impact of vehicle mobility in D2D communications. (W Duan 2020)

Vehicle-to-Infrastructure:

V2I is a model that allows vehicles to communicate with roadside infrastructure such as traffic lights, cameras, lane markers, streetlights, parking meters, etc. The key components required at minimum are the Vehicle On-board Unit (vOBU), Roadside unit (RSU) and a secure communication channel. A vehicle's OBU comprises of a GPS system, DRSC system, and a channel to communicate with other vehicles and

the RSUs. The RSU has similar hardware but is located within intersections, patrol stations and interchanges. The main functionality of an RSU is private (vehicle specific) data transfer and message priority management. Meaning that messages related to vehicle safety and road systems have the highest priority whereas entertainment related messages have the lowest priority.

According to Ndashimye *et al*, The DSRC system mentioned earlier uses a licensed spectrum at 5.9GHZ with seven channels. The center channel is dedicated to safety applications, the two ends for special purposes and the rest are service channels. The two classes of devices; vOBU and RSU use the IEEE802.11p protocol and uses orthogonal frequency division multiplexing to split the main signal into multiple narrowband signals. In their study, they proposed some research to be done in some key areas such as efficient network discovery, QoS requirements, and a protocol suite to support seamless vertical handover in 5G heterogeneous network environments.

They propose a network selection method that improves handover of V2I communication over multi-tier heterogeneous networks using certain parameters such as relative direction index, proximity index and network load index. They claim that their approach, when run on the OPNET network simulator, reduces unnecessary handover up to 50%, higher throughput by 50% and lower end-to-end delay up to 43% compared to conventional switching methods.

Some of these approaches are namely: Game theory, MCDM (multiple parameter approach), Resource management and Speed adaptation. Their research while improving network related performance, eventually leads to higher resource usage in the device's processors and memory which is an important limitation.

Security in these systems currently use public key cryptosystems which require higher memory overhead and may be unreasonable in latency critical scenarios, their research advises to further develop and research Intrusion detection systems as an alternative. They also show two other approaches to V2I security such as C-ITS Security Layer and RSU-cantered security (opposed to standard IEE1609.2). These approaches improve end-to-end delay and provide a more complete secure communications systems between ITS stations albeit at the limitations of having to update to current TCP/IP architecture and other hardware changes to existing RSU systems.

The emerging development of vehicle-to-everything (V2X) connectivity is bringing about more discussions on safety concerns. The roadside units (RSUs) are going to play a critical part in the IoV because of their capacity for high communications volume. The RSUs are short range receivers that allow constant communication among vehicles through vehicle-to-infrastructure (V2I) communication. The RSUs allow dedicated short-range communication (DSRC) technology to create connections between vehicles. The RSUs have limited communications ranges. (Mekala 2021)

Multicast technology can be used to satisfy requests for comparative services from multiple vehicles. The information can be provided from either a RSU or a fog server through a single multicast transmission. This allows requests to be fulfilled since there is a high density of vehicles in urban areas and messages have large content sizes. Unmet requests can be offloaded to a server to help enhance the quality of experience (QoE).(Mekala 2021)

Vehicle-to-Pedestrians:

Current urban traffic communication with pedestrians relies on the human driver-pedestrian communication path. This path uses nonverbal negotiation between the two humans involved in the situation. This communication takes place using several informal communication channels, one such channel uses aspects of the vehicle such as standard vehicle signals of horns and turn signals. Expected behavior is another communication channel, such as forward, turning and stopping based on the situation. The nonverbal communication between the people such as facial expression, gesture and eye contact make up another communication pathway. Given the possibility of human drivers being removed in future autonomous vehicles, there needs to be a replacement path for this communication. (Liu 2020)

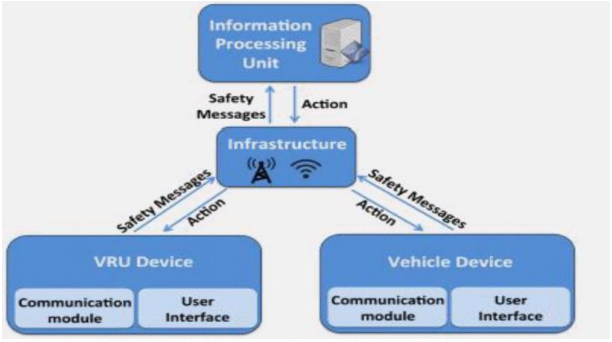
So, we can say that V2P communication is probably the most important factor in providing safety to pedestrians through the V2X network.

V2P systems have the following operational hardware units (Malik *et al*):

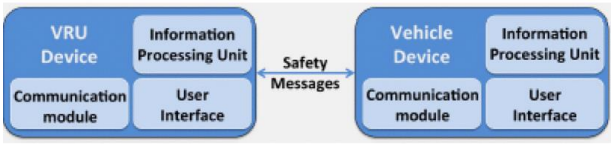
- Vehicle device OBU,
- Pedestrian's device (smartphone, wearable sensors).
- RSU Infrastructure,
- Information processing unit.

Vehicles with OBUs share information with RSUs and pedestrian devices; for example, the GPS system on a mobile phone is interconnected with the neighboring area's vehicles which notify pedestrians of accidents through their mobile apps (Google Maps, Apple Maps, etc.). Some scenarios mentioned in Malik *et al's* study can be critical to pedestrian safety; for instance, sensors within vehicles that detect pedestrian devices for collision avoidance (crossing roads) although the main limitation would be the sensor's line of sight or poor visibility conditions (fog, haze, storms, etc).

According to Malik *et al*, the two communication types within V2P networks are as follows: Direct communication using vehicle ad-hoc communication technologies (802.11p) and a more indirect system using infrastructure based (cellular) technology.



(a) V2P Architecture - Direct Communication



(b) V2P Architecture - Indirect Communication

Figure 4: V2P architectures

The paper discussed many issues in the communication systems and some proposals for their mitigations, but we will only briefly discuss them as they are too in-depth for the scope of this paper. There are several studies currently in place to improve direct communication. One proposal is the multiple priority supported MAC protocol for VANET. An extension of the 801.11p protocol called the Highway Multi-hop broadcast for vehicles to address issues such as hidden nodes, broadcast storm and the general reliability of multi-hop broadcasting in VANETs. One of the issues discussed was the disconnected link problem, which they aim to mitigate using a geo-cast forwarding protocol technique.

For the improvement of road and safety from Indirect Communication, there are studies about real-time control and active transportation management. One of the proposals being Service-Actuated Multi Channel Operation which provides a logic that controls channel switching timing based on service priority.

There are many different applications of V2P, but the most critical ones according to Malik *et al* are the pedestrian tracking and trajectory prediction, movement and behavior and position detection. There is a significant amount of work in the process to aid these use cases. Pedestrian tracking and trajectory prediction is being studied by using LIDAR (Light Detection and Ranging) for tracking and modelling the data through the Gaussian Mixture Model. Simulation using dynamic Social Force model is used to mimic crowd behavior; there is a proposal on a new “Swarm Optimization” algorithm which is supposed to help emulate crowd evacuations and crowd related behavior/patterns which can be seen in real life examples. The current research work will be crucial for the future of safety systems and is aimed at reducing the accident rates that people interact with.

Security issues and potential solutions

VANET transmits critical and time sensitive information through the network. Because of this there needs to be a secure, trustworthy and attack free environment in which to communicate. The messages need to be authentic and generated from legitimate vehicles. Critical messages such as black ice warning messages can have a direct impact on human lives. Because of the critical nature of the messages transmitted, there should be the expectation for satisfying basic traditional security requirements such as confidentiality, integrity, availability, authenticity, privacy and non-repudiation. Given that VANET is a wireless network without static participants, it is susceptible to many security challenges. (Ahmad 2018)

Traditional security management approaches are becoming less sufficient to address the increasing sophistication of cyber threats and vulnerabilities that are targeting the future next generation wireless networks. The newly developing challenging environment includes high traffic volume and diverse technologies that are vulnerable to exploitation. Adding artificial intelligence (AI) to the security management approaches could result in adaptive, autonomous and intelligent security management. This could reduce the costs of detection and mitigation of a wide variety of security threats. Machine learning is of particular interest for integrating it into telecommunications networks. (C. Benzaïd 2020)

Using AI for monitoring and responding to security threats and vulnerabilities will bring about a new era in more sophisticated cyber threats that are autonomous, faster, stealthy and scalable. The self-management functions of AI managed networks can address the massive numbers of connected devices and the ultra-high bandwidth, but that also creates an attractive target for cyber criminals. The network management functions can allow an attacker to use any vulnerabilities to attack the performance and security measures. Like every good invention there are ways of misuse and becoming a threat. (C Benzaid 2020)

Authentication:

A timely and robust authentication mechanism is required in vehicle networks due to the sensitive and timely nature of the traffic carried. The voluntary associations between and among vehicles and infrastructure need to be fast and precise. The message authentication must be extremely fast to allow the recipient vehicle to respond and act on the time sensitive warning messages received. The sender can be impersonated, or the origin of the message could be falsified by an adversary. It is also possible for vehicles with identical static attributes to not be authenticated. This makes the issue of authentication one that could generate a life-threatening situation because the wireless radio communication channels do not support location binding or authentication between communication nodes. (Dolev 2017)

The US Department of Transportation issued updated traffic rules requiring inspection authorities or police to track and stop any vehicle suspected of violating traffic rules. For this to be enforced correctly, there must be precise identification of vehicles. One possible way to identify vehicles is using pre-certified vehicle attributes, visual sensors and optical communication channels. These can combine to make a unique visual mapping for each vehicle. (Dolev 2017)

Using this visual mapping there can be a wireless radio channel that uses an auxiliary communication channel. This channel is used to visually bind the vehicle to a secure session. The issue here is that static identification methods may be unreliable for moving vehicles. One solution is to use both dynamic (non-certified information such as location and direction) and static (certified information such as VIN, license plate, brand) attributes of the vehicle and its public key. The vehicle then verifies this coupled information to acknowledge the start of communication. (Dolev 2017)

Dynamic attributes are unable to be pre-certified, so one idea is to use laser technology using a directional laser beam to verify the dynamic attributes and combine with the static attributes and a public key. The laser interface requires the sender to generate its own messages and thus be accountable for all messages sent and received through its own laser interface. This brings into the picture authentication and authenticity like digital certificate signing of email messages. (Dolev 2017)

IEEE 1609.2 provides certificate-based authentication and has had updates proposed for modifying the certificate structure of the security standard. But certificate structure alone is not enough to stop impersonation attacks. This is because static attributes that are verified along with the public key could still lead to impersonation attacks in some malicious identical vehicle scenarios. (Dolev 2017)

Man-in-the-Middle Attacks:

Vehicle ad hoc network (VANET) communication has network communication vulnerabilities, as does every connected network. One such risk is man-in-the-middle (MITM) attacks. A MITM attack has malicious interference that intercepts or eavesdrops or alters messages in transit between network nodes. The MITM attacks have three goals with this type of disturbance, message delay, message tampering and dropping messages. Results of these tampering include high packet loss, high delays and high numbers of compromised messages. (Ahmad 2018)

Since VANET messages contain sensitive and delay intolerant information the MITM attacks can send out compromised or incorrect information throughout the network. This violates the main security pillars of confidentiality, availability and integrity. Malicious information then replaces, alters or removes legitimate messages. (Ahmad 2018)

VANET by design makes use of the IoT design principles and smart cites as transmission and connection paths. The vehicles exchange messages with each other through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) methods that allow various applications from safety warnings to occupant entertainment. (Ahmad 2018)

MITM attacks come in two different forms, passive and active attacks. The passive attacks are of the eavesdropping, watching the network form. The active attacks are of the interacting with the traffic to drop, delay or change the messages going through the network. A passive attack would involve the benefit of use data, such as law enforcement vehicle communications data. This data would then be shared with interested parties for their own illegitimate use. An active attack would involve delaying, dropping or changing messages about, say, a traffic incident. The legitimate vehicles will not have complete legitimate information preventing the best possible outcomes. (Ahmad 2018)

Jamming:

Jamming is one of the major and serious threats to vehicle-based networks. Jamming attacks were prominent in basic wireless communication networks. Jamming attacks are performed by a jammer emitting a high-powered electromagnetic signal designed to make legitimate signals unrecognizable from the signal coming from the jamming device. Smart jammers can reconfigure the signal strength and frequency band to match the specific transmission characteristics being targeted. This is easily implemented when compared to other attacks and is extremely disruptive. (S Feng 2019)

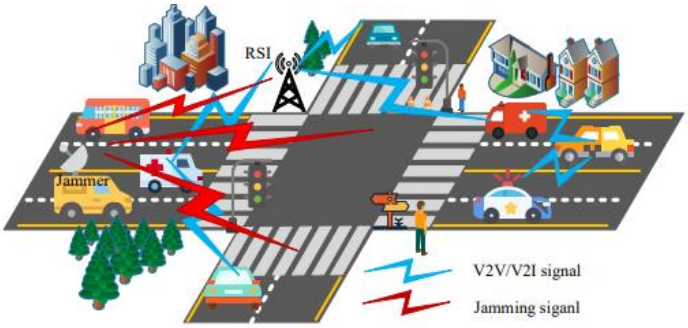


Figure 5: Jamming Attacks on a vehicular network

Generic jamming attacks come in several different types; constant, reactive, deceptive, and frequency sweeping jamming. There are also jamming attacks designed specifically for V2X networks (Hossein et al). In an attack studied by Azogu et al, the jamming signal dynamically switched to channels in use and targeted it. Another form of attack, called a data integrity attack, captures packets and alters the content which is then relayed to vehicles or roadside units.

The paper by Hossein et al says that anti-jamming techniques for VANET are not really researched because the general idea of mitigating jamming is to simply switch to a different network available and by frequency hopping after failed communications. In this paper, they mention notable research done by Kumar et al. Which uses machine learning to locate the jamming device. The idea of this is to detect undesired frequency changes in the V2V network, then use a filter to remove noise components from the jammed signal and use this filtered signal in a Catboost algorithm (ML algorithm for making decision trees) which determines the location of the jammer. They claim that their scheme, when run on a simulator, can predict the jammer's location with 99.9% accuracy.

New/Ongoing Research on IOV

Conclusion

Since the 5G evolution, the internet of things has revolutionized the modern industrial society. The smart home and smart factory revolution has almost completed, while the internet of vehicles is just barely emerging. 5G is supporting this revolution as it gets rolled out to the major cities. As more devices connect to the internet and each other, network slicing, wide bandwidths and redundant device to

device improvements in 5G will make this possible. The expansion into vehicle-based communications allows the device-to-device nature of the IoT concept to be realized. While the security challenges remain, there are developing artificial intelligence techniques to help with threat mitigation. The future remains bright for vehicle-based networks that include the possibility of autonomous driven vehicles.

References

Ahmad, F., Adnane, A., Franqueira, V. N., Kurugollu, F., & Liu, L. (2018). Man-In-The-Middle Attacks in Vehicular Ad-Hoc Networks: Evaluating the Impact of Attackers' Strategies. Sensors, 18(11), 440-459. doi:https://doi.org/10.3390/s18114040

Attaran, M. (2019). 5G wireless: A transformative, disruptive technology. Industrial Management, 61(3), 16. https://www.proquest.com/trade-journals/5g-wireless-transformative-disruptive-technology/docview/2264566113/se-2?accountid=10906

C. Benzaïd and T. Taleb, "AI for Beyond 5G Networks: A Cyber-Security Defense or Offense Enabler?," in IEEE Network, vol. 34, no. 6, pp. 140-147, November/December 2020, doi: 10.1109/MNET.011.2000088

Dolev, S., Krzywiecki, U., Panwar, N., & Segal, M. (2017). Dynamic attribute based vehicle authentication. *Wireless Networks*, 23(4), 1045-1062. http://dx.doi.org/10.1007/s11276-016-1203-5

S. Feng and S. Haykin, "Cognitive Risk Control for Anti-Jamming V2V Communications in Autonomous Vehicle Networks," in IEEE Transactions on Vehicular Technology, vol. 68, no. 10, pp. 9920-9934, Oct. 2019, doi: 10.1109/TVT.2019.2935999.

W. Duan, J. Gu, M. Wen, G. Zhang, Y. Ji and S. Mumtaz, "Emerging Technologies for 5G-IoV Networks: Applications, Trends and Opportunities," in IEEE Network, vol. 34, no. 5, pp. 283-289, September/October 2020, doi: 10.1109/MNET.001.1900659.

Liu, Y., Lyu, Y., Böttcher, K., & Rötting, M. (2020). External Interface-based Autonomous Vehicle-to-Pedestrian Communication in Urban Traffic: Communication Needs and Design Considerations. *International Journal of Human-Computer Interaction*, 36(13), 1258–1272. https://doi.org/10.1080/10447318.2020.1736891

Mekala, M. S., Dhiman, G., Patan, R., Kallam, S., Ramana, K., Yadav, K., & Alharbi, A. O. (2021). Deep learning-influenced joint vehicle-to-infrastructure and vehicle-to-vehicle communication approach for internet of vehicles. *Expert Systems*, 1. https://doi.org/10.1111/exsy.12815

H. Ullah, N. Gopalakrishnan Nair, A. Moore, C. Nugent, P. Muschamp and M. Cuevas, "5G Communication: An Overview of Vehicle-to-Everything, Drones, and Healthcare Use-Cases," in IEEE Access, vol. 7, pp. 37251-37268, 2019, doi: 10.1109/ACCESS.2019.2905347

Emmanuel Ndashimye, Sayan K. Ray, Nurul I Sarkar, Jairo A. Gutiérrez, “Vehicle-to-infrastructure communication over multi-tier heterogeneous networks: A survey”. ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2016.11.008.

R. Q. Malik, K. N. Ramli, Z. H. Kareem, M. I. Habelalmatee, A. H. Abbas and A. Alamoody, "An Overview on V2P Communication System: Architecture and Application," 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), 2020, pp. 174-178, doi:10.1109/IICETA50496.2020.9318863.

S. Zhang, "An Overview of Network Slicing for 5G," in IEEE Wireless Communications, vol. 26, no. 3, pp. 111-117, June 2019, doi: 10.1109/MWC.2019.1800234.

J. Wang et al., "Spectral Efficiency Improvement With 5G Technologies: Results From Field Tests," in IEEE Journal on Selected Areas in Communications, vol. 35, no. 8, pp. 1867-1875, Aug. 2017, doi: 10.1109/JSAC.2017.2713498.

Hossein Pirayesh and Huacheng Zeng, “Jamming Attacks and Anti-Jamming Strategies in Wireless Networks: A Comprehensive Survey”, Jan 2021, https://arxiv.org/pdf/2101.00292.pdf