Vehicle to Vehicle Communication: Spoofing Traffic

Sumayyah Alahmadi, Hans Johnson and Thomas Slota

I. INTRODUCTION

As vehicle to vehicle (V2V) communication becomes widely deployed, its crucial to consider the security perspective of this new technology. In this paper, we will present the potential security threats of spoofing communications that are sent between vehicles. For the project implementation part of this paper, we will be required to use vehicle to vehicle protocols using a LimeSDR kit for our transmission and a receiving of this communication. We will also be using GNU Radio to configure the SDR which includes a GUI that you can use to construct flow graphs using boxes that are proposed for specific configurations. For our testing environment, we are looking to set up a single LimeSDR kit for our scenario. Using the two transmitter antennas on the SDR, we can send a broadcast packets out using the band dedicated for Intelligent Transportation Systems. After, we use the to receiving antennas on the SDR to capture the broadcast packets and then process them for verification. This environment will allow us to test our spoofed packets that we create. With this research, we are looking to conduct research on V2V communication and provide information on whether the current standards used in todays vehicles are secure. If spoofing of this type of information is feasible, then we will also be able to further provide recommendations on potential solutions that would mitigate these threats. Advancements in V2V communication will continue to progress as the world shifts from manually monitored and controlled environments to automated, self-thinking systems. This type of movement is now starting to take over within the automotive industry and as this continues, security should be a top-priority. Cars are now produced with advanced technologies allowing communication between vehicles and providing information regarding traffic patterns, collision prevention, etc. With that being said, being able to forge and produce false information could be catastrophic. In this paper, we hope to shed light on some of the theoretical possibilities of what could occur from an adversaries prospective.

II. LITERATURE REVIEW

Biswas et al looks at designing a system that cars can communicate with each other to help stop traffic accidents. This system will be able to tell the car behind it what is in front of it so that the driver can respond in a timely manner. This would also open up the car to an attack vector which is what we are going to implement in this paper. This being the use of spoofing traffic to vehicles to make them think something is happening, but isn't actually occurring.

In [2] Biswas et al discusses the need to implement Intelligent Transportation Systems (ITS) to help combat the problem of traffic accidents in the United States. The main reason that they decide is the reason for most car crashes is the limited view beyond the car in front of you. You must react to the car in front and this is not enough in emergency situations. So, they come up with introducing these ITS to help reduce the numbers of traffic incidents per year. With these Intelligent Transport Systems comes a huge problem that we will discuss in this paper. This problem which is the focus of this paper is being able to spoof the traffic coming into and out of these systems to fool an automobile into thinking that something is happening, when there is nothing going on. This can be extremely dangerous because if these systems have access to crucial parts of an automobile, like the brake system, cruise control, etc., the V2V communication can be used to overtake a vehicle and cause a mass car crash.

Lyu et al. propose a secure method to authenticate broadcast messages in vehicle-to-vehicle communication which is based on predicting future beacon messages in advance. This is to defend against DoS attack and packet losses in VANETs [1]. Instead of exhausting resources with a large number of signature verification beacon messages arriving in a short time period, Prediction-Based Authentication (PBA) schema leverages the predictability of beacons for fast verification to prevent Computational-based DoS attacks. Furthermore, the schema also has an advantage of minimizing the storage overhead to thwart memory-based DoS attacks by storing only shortened message

authentication code (MAC). The PBA schema proves to be secure and efficient even with high-density traffic and a lossy wireless environment due to the high mobility of the vehicles. Studying authentication and threat of interception in VANET is significantly related to our focus in this paper as we are examining different methods to mitigate spoofing. Authentication and cryptography are the main countermeasure to thwart manipulating the communication by sending illegitimate messages to the receiver. Thus, the more ways we find to authenticate and encrypt the communication between vehicles, the more difficult for the attacker to pretended to be another entity to the receiver. With this in mind, knowing these obstacles and how they function provides us a better understanding about what types of road blocks we may face when trying to spoof V2V communications.

The idea of our paper came from reading the work done by Chen et al. This paper focuses on analysis and identification vulnerability in connected vehicle environment by looking into a spoofing strategy that can potentially affect traffic control and cause traffic congestion. The result of the vulnerability analysis in the real-world setting is that the signal control design and implementation is vulnerable to spoofing attacks. Our thought was how could we implement this technique of spoofing vehicle to vehicle communication using other methods to design an attack. In [3] the spoofing technique that they implement is spoofing the location and speed of a vehicle approaching a stop light. Doing this they could manipulate how long the light would stay green. This resulted in a congestion attack that would pile up cars and jam the intersection. This attack could be very useful in forcing cars into a set route to take. The parts of this implementation that we can use and implement more on are the spoofing the vehicle speed and location. If we were able to use these techniques in another area we could create a seperate attack all together.

In [6], Wu et al. a discussion is had about the current technology used by Dedicated Short-Range Communication (DSRC) which supports vehicular communication in terms of safety and reliable performance in dense and highly mobile environments. Though vehicular communication used DSRC has proven to increase the safety and reduce the total crash percentages on the road, there are still a couple of challenges with the performance of DCRS. These challenges include channel estimation and time diversity in the physical layer and packet collision in the MAC layer. Also, based on these challenges, a few of solutions have been discussed to enhance DSRC wireless communication performance. As DSRC is considered as an official wireless technology standard in vehicle -to-vehicle communication, we will use this standard as the band to operate on when discussing the implementation of our spoofing technique.

Connected vehicles are facing cyber threats and challenges as stated in [7]. Parkinson et al. review and analysis identified vulnerability and mitigation techniques, and highlight some of the knowledge gap that should be addressed to minimize potential cyber threats in connected autonomous vehicle communications. The authors lists and talks about a couple of identified vulnerabilities which are categorized based on the type of the attack. An example of some of these listed attacks are rough updates, phishing, network protocol attack and network protocol attack. One of these identified vulnerabilities is spoofing the Global Positioning System (GPS) signal where valid, but incorrect GPS broadcast signals are sent to mislead the GPS receiver. The GPS position is then to be modified as the power of the adversarys signal increases.

III. Proposed Methods

Our proposed idea is to spoof vehicle to vehicle communication to a moving vehicle. The information that we would be spoofing is its location and speed inside the Basic Safety Message (BSM). The idea here is to manipulate the traffic so that the targeted car would alert the driver to slam on the brake or if it is a self driving car slam on the brakes itself. This would be done by sending the vehicle a spoofed communication saying that its current location is the target cars location with an offset of a car length and a speed of half the speed limit or a speed of 0. This would result in the targets car thinking that it is going to crash into the car in front of it and slam on the brakes.

The Basic Safety Message specifications are described in [4]. The BSM is broken up into 2 parts, the mandatory part (part 1) and the optional part (part 2). The general information that is communicated inside part 1 is position, motion, brake system status, and vehicle size. In the optional part some of the information that can be transmitted are wiper status, steering wheel angle, sun sensor, and brake system status.

Basic Safety Messages are used to send information to other vehicles around you and inform them based on current events. An example that the National Highway Traffic Safety Administration used at their SAE Government Industry Meeting in January 2016 is using

tractor-trailers. The Basic Safety Messages are used in this case to alert the cars following a tractor trailer that it is going to make a right hand turn and must take more space than needed to make this sharp turn. The BSM are used to communicate to the following cars where exactly the end of the tractor trailer will be during the turn. This will allow the following vehicle to slow down to get out of the way of the turning tractor trailer. The purpose of these messages are to send information to other vehicles around it to help limit the number of traffic accidents.

IV. Implementation

A. Environment

For testing our spoofing technique, our environment consists of a LimeSDR that is controlled by a GNU radio. The LimeSDR is an apps-enabled software-defined radio (SDR) platform that can be used to support any type of wireless communication standard and comes with 4 antennas. Specifically, we will use the transmitter to send the spoofed packets as broadcast messages repeatedly at around 10 packets a second. Our receiver will be listening for these messages as they are transmitted and collect the packets as they arrive. To operate the LimeSDR, we are using GNU Radio which is a toolkit that provides signal processing blocks to implement software-defined radios and signal-processing systems. With these tools we are able to generate our own spoofed packets, transmit them over one antenna and receive them on another, and test to see if we can construct packets that could then be processed as real BSM data.

B. Packet Spoofing

The band we will be operating on is DSRC or Dedicated short-range communications. DSRC is a one-way or two-way short-range to medium-range wireless communication channels specifically designed for automotive use and a corresponding set of protocols and standards. DSRC operates on the 5.9 GHz band which is what we will be using for our testing in this case. Inside DSRC there are 7 different channels which are 10 MHz each .This correlates to a 75 MHz spectrum. They range from 5.850 GHz to 5.925 GHz. The first channel which is 172 is reserved for Basic Safety Messages. This is a SAE J2735 standard in the DSRC Message Set Dictionary which supports interoperability within DSRC applications [5].

The information that we will be spoofing is inside the Basic Safety Message in the required section (part 1). These data points are speed, latitude, longitude, heading and angle. Using these data points in the message, we can construct a possible malicious attacks against a specific car or multiple cars using spoofed data.

C. Packet Verification

Using Wireshark we can verify that the messages we are able to generate have a legitimate structure since Wireshark is able to identify the WAVE packets. Therefore, this would tell us whether the limeSDR is able to transmit and receive the same packet structure that a connected vehicle would receive. This is a great tool for verification of the Vehicle to Vehicle packets we were attempting to spoof.

V. Evaluation

A. Spoofing Outcomes

Through our research, we discovered just how dangerous spoofing vehicle to vehicle communication is. Any malicious person capable of this type of spoofing could launch massive attacks as well as single targeted attacks to either cause chaos or to benefit themselves.The possible outcomes of spoofing vehicle to vehicle communication are endless and very dangerous. There are a multitude of different values that can be spoofed inside the Basic Safety Message that when in contribution with others would result in the target reacting differently and can be used to manipulate how a vehicle behaves. For instance it would be possible to spoof the location of a car to be directly in front of another car, which would make the target car react by alerting the driver or the car will react by slowing down. You could also spoof the speed of fake cars surrounding a target car which would alter the speed of cars with automated cruise control. To say that you had a small computer that was able to consistently spoof while attached to a person's car, adjusting the angle of fake surrounding cars could make the target car react by using lower gears and wear the cars transmission.

Another thing to mention is that the behaviour of a car also depends on how much the system actually interferes with the manual control of the driver or whether the manufacturer designed the car to only give warnings. This factor is important to consider since many cars are made differently and the V2V system in the car can interpret data and make decisions differently as well. With malicious BSM packets, you could still send false positives to the cars that are less interactive with assisting the drivers and still influence the driver by raising certain warnings in the car. For the most part,

a driver will react the same way based on the warnings he gets when compared to a vehicle assisted reaction.

B. Real World Scenario

A real world scenario where this would be applicable is on a busy highway. Our transmitter would be setup at a rest stop along the highway where multiple packets could be sent spoofing a fake car (or cars) on the road. As cars pass, they will broadcast their BSM messages out to other cars. We could collect these messages using a receiver that takes and processes these messages to get the location information. With this, we can then add an offset of the location of these cars and also factor in trajectory information, making it possible to generate an accurate offset that is located in front of the corresponding cars by only a few feet. This location is then sent out in spoofed BSM packet. This would be interpreted by the car and cause the car to slow down either by warning the driver or by automatically slowing the car down if it had assisted driving. To do this in a more brute force tactic. we can just repeatedly send out a spoofed location so that any car that comes into that location would get the spoofed message and be alerted to brake. This would not require us to figure out the target cars location before spoofing.

C. Detection

There have been many proof of concept implementations to try an deal with the security concerns of vehicle to vehicle communication. These include encryption, having messages signed by a trusted certificate authority, and have unique identifiers to trust the sending party. One way that we can use to detect the spoofing technique done within this paper is by correlating all the BSM data together. This means that we can validate the data that we are being given and detect any data that is abnormal. This would allow the vehicle to be able to ignore the spoofed packets. If we take a look at all the BSM data that is getting sent we can look at each individual data point and see if an anomaly is present and whether that piece of data is accurate according to other provided pieces of data in that BSM. For example, if the acceleration field doesn't match with the speed field, the car direction does not match with the steering wheel values, etc. This correlation would effectively remove the possibility of using this attack in this scenario.

VI. Conclusion

The research that was conducted here lead to the conclusion that if spoofing was possible to an adversary, the possible damage that could be done is up to the malicious persons imagination. As cars start to become more automated and data driven, a conversation needs to be had about the problems that could occur from this new movement in the car industry. Though much of the technology is for the benefit of the driver and the safety of the people in cars that are on the same road, the dangers of this technology is something to think about as well. When we consider V2V technology, data needs to be moved and interpreted quickly so that the car or person driving can make split second decisions that could save peoples lives. They also rely on information that is real and accurate so that the decisions made are not the wrong choice and could end up being more harmful than helpful.

With these factors laid out, we also consider the security of this technology. Being that this information needs to be moved quickly, the current standards in place for DSRC use a high transmission rate that is an adequate solution for the speed that V2V information needs to be sent. The other part of its quick delivery is the complexity of the data that arrives and how much interpretation is needed. If we want good security for V2V, we would need encryption to establish privacy of the data. This slows the processing of data and would need to be a less complex cryptographic algorithm that has quick encryption and decryption capabilities. Another consideration for security is the trusting of the source of data. In this case there are many solutions that are being researched. One that is included in DSRC is the support for certificates which would help vehicles trust the information that they receive. The issue with this however, is that data needs to be processed in a reasonable amount of time. Therefore, waiting on important data because the certificate is being searched wastes valuable time. Overall, each of these security factors must continue to either be minimal and efficient.

In terms of a malicious adversary, each of these would benefit his or her intentions. Being able to spoof Basic Safety Messages would allow for an abusive amount of control in terms of a single driver or for mass traffic manipulation. With minimal security, this makes it easier for an adversary to spoof whatever data they so choose. Overall, this understanding means that BSM data must be protected and authenticated with high security standards. The dangers of this data when it is unprotected are too viable to ignore. This takes away from efficiency of data processing, but could be fixed with faster hardware in the vehicle side. It may be a more expensive option, but that option could also

protect people from malicious activity.

REFERENCES

[1] Lyu, C., Gu, D., Zeng, Y.,Mohapatra, P. (2016). PBA: Prediction-Based Authentication for Vehicle-to-Vehicle Communications. IEEE Transactions on Dependable and Secure Computing,13(1), 71-83. doi:10.1109/tdsc.2015.2399297

[2] Biswas, S., Tatchikou, R., Dion, F. (2006) Vehicle-to-Vehicle wireless communication protocols for enhancing highway traffic safety. IEEE Communications Magazine, 44(1), 74-82, DOI:10.1109/MCOM.2006.1580935

[3] Chen, Q., Yin, Y., Feng, Y., Mao, Z. and Liu, H. (2018). Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control. In: Network and Distributed Systems Security (NDSS) Symposium. DOI:10.14722/ndss.2018.23222

[4] Cts.virginia.edu. (2018). 5.9 GHz Dedicated Short Range Communication Vehicle-based Road and Weather Condition Application. [online] Available at: http://www.cts.virginia.edu/wp-content/uploads/2014/04/PFS_DSRC02_Task1_Messaging_Reqs_007-101-02.pdf [Accessed 17 Dec. 2018]

[5] Standards.its.dot.gov. (2009). ITS Standards Program — Fact Sheets — ITS Standards Fact Sheets. [online] Available at: https://www.standards.its.dot.gov/Factsheets/Factsheet/71 [Accessed 18 Dec. 2018].

[6] Wu, X., Subramanian, S., Guha, R., White, R. G., Li, J., Lu, K. W., . . . Zhang, T. (2013). Vehicular Communications Using DSRC: Challenges, Enhancements, and Evolution. IEEE Journal on Selected Areas in Communications,31(9), 399-408. doi:10.1109/jsac.2013.sup.0513036

[7] Parkinson, S., Ward, P., Wilson, K., Miller, J. (2017). Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges. IEEE Transactions on Intelligent Transportation Systems,18(11), 2898-2915. doi:10.1109/tits.2017.2665968