DSRC Challenges with Malicious Acts and its Reliability and Survivability in VANETs

Chihsiang Wang
Computer Science
University of Idaho
Email: wang0162@vandals.uidaho.edu

***Abstract*—Reliability and Survivability are such important for the DSRC communication, since any non-malicious or malicious acts may cause severe effects. As the DSRC applications are applying to the modern vehicles to increase the safety abilities for drivers. Every researches about to detect and correct misbehaviors are important. This paper summarized some recently researches which focus on the malicious acts especially on VANETs and its strategies to avoid or react while misbehaviors happens.**

***Index Terms*—BSM, DSRC, VANET, Misbehaviors, System reliability and survivability.**

I. Introduction

As previous work[14] has been mentioned. Vehicular Ad Hoc Networks (VANETs) are becoming more important to enhance road traffic safety. In an Ad hoc network, collection of nodes dynamically forms a network without existing infrastructures or centralized administration [1]. A VANET consists of a set of vehicles equipped with on-board units (OBUs) and a set of stationary units called road side units (RSUs), communicating each other with the ad hoc connection that are established on the fly when they are in the communication range. Providing efficient Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) are the main objectives of VANETs[3]. VANET applications can be divided into two into two categories: safety applications and non-safety applications. Those applications that are critical to human life safety such as pre-crash sensing, post-crash warning, etc. are under safety application categories. Quality of Service is one of the main concerns in any type of wireless communication. In high density environment, each vehicle broadcasts message flood at a high frequency, that can easily congest the Control channel (CCH). Also, malicious acts like jamming can disable BSM works normally. Keeping CCH channel free from congestion is very important in order to ensure timely and reliable delivery of Basic Safety Messages (BSMs). The rest of this paper is organized as follows: Section 2 describes some background knowledge such as Waht Basic Safety Messages and DSRC is and what are the challenges associated with this technology. Section 3 presents types of malicious acts to DSRC system and its strategies. Section 4 concludes this paper.

II. Background

A. Vehicular Ad-hoc Network

In VANET (Vehicular Ad-hoc Network), vehicles equipped with short range radios communicate with each other (Vehicle-to-Vehicle - V2V) and with the road side infrastructure (Vehicle-to-Infrastructure - V2I) to enable range of applications from Internet access and driver assistance to transportation safety and emergency response. Network topology in VANET changes frequently due to high node mobility. V2V and V2I operates in the 75 MHz Dedicated Short Range Communication (DSRC) spectrum. The spectrum is allocated within 5.85 - 5.925 GHz band which is divided into one control channel and six service channels. All vehicles will broadcast their state information such as location, speed, vehicle size, etc., frequently in Basic Safety Message (BSMs). According to the standards, each vehicle should transmit one BSM every 100 milliseconds in DSRC.

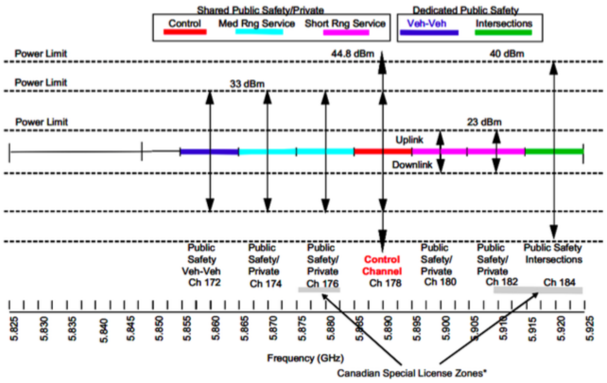

Fig. 1. DSRC channels and Power Limit[3]

B. Dedicated Short Range Communication

DSRC uses IEEE 802.11p as its PHY and MAC layer, which is, a modified standard of the IEEE 802.11e with QoS (Quality of Service) at the MAC layer and basically same PHY layer defend for 802.11a but with halved transmission rate . Yet the communication speed and the range are improved. According to [5], 802.11p provides longer duration and faster communication speed between units. Besides, the loss of packet is just half compared with 802.11a. But the performance, efficiency and reliability are still limited in the real life, since there are several challenges can effect DSRC safety. That is, high speed mobile, busy traffics between buildings or intersections, malicious attacks and more. DSRC systems are based on the orthogonal frequency division multiplexing (OFDM) systems. OFDM systems are well known for their abilities to combat inter symbol interference (ISI) in time-invariant, frequency-selective channels[8]. In this paper we are going to note some malicious acts which may affect DSRC safety. In U.S. Federal Communications Commission (FCC) has allocated 75 MHz DSRC spectrum in the 5.9 GHz band. The spectrum consists of one control channel (CCH) and six service channels (SCHs) to be used by Intelligent Transportation Systems (ITS) as shown in Figure 1.

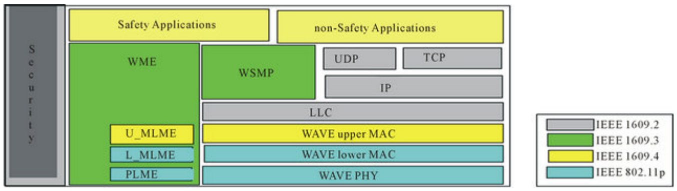

Fig. 2. Physical IP Users

C. Basic Safety Message

The Basic Safety Message (BSM) is used in multiple safety applications in each vehicle. These applications are largely independent of each other, but all make use of the incoming stream of BSMs from surrounding (nearby) vehicles to detect potential events and dangers[15]. BSM is defined by the standard ASE J2735, every mobile keep updating and sending this message every 100 micro seconds over the WSM channel. Nearby OBUs and RSUs can detect the broadcast message and process it if the format is fit its safety applications. A temporary value in the message body allows correlating BSMs to a specific vehicle for short periods of time. The rationale of the BSM is for create a most statistically frequent message seen over the airwaves.

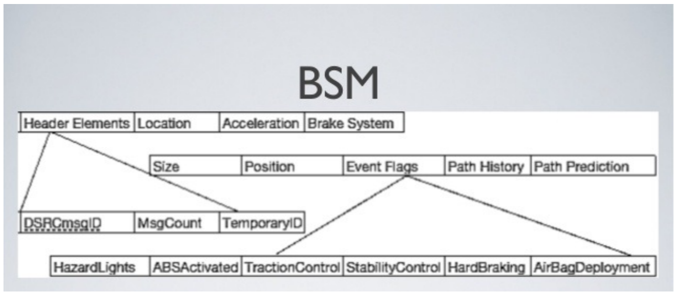

Fig. 3. BSM

There are two sections consisted in the BSM. Part 1 is always necessary to be sent during the broadcast, which combined DER encoding and some BLOB encoding, also it contains node's position, motion, time and basic status. Part 2 contains vary optional data within, safety applications may add on the extra data with it if that is useful for the processing.[15]

III. Misbehaviors

In order to meet performance goals, it is widely agreed that VANETs rely on heavily node to node communication. Since the system concern the speed of quick data transmission, it is also bring the issue that an easy access system may have more difficult security goal of data validation. [16]

A. Misbehaving Nodes

A bad or malicious data node(vehicle) in VANETs may try to send fake message such include wrong event reports, such as non-exist traffic jam, car accident and any of information content in the Basic Safety Messages like speed, location, status and many others. Wrong messages via malicious nodes can cause severe damaging if there is no strategies to detect and correct the nodes. In the VANETs, these mistakes are called misbehaviors no matter it's rational or malicious. Here we are classify the misbehaving nodes by it abilities before we get into the rationale of misbehavior nodes.

1) Rational and Malicious: Usually attackers can be divide into two groups by their objectives. Malicious attackers are purely enjoy to see the damaging of the system, rather than rational attackers, they don't consider benefit, cost or consequences. In some situations malicious attackers are more dangerous because we can't predict their intentions. [6]

2) Outsider and Insider: Outsider means those node out of the network, which has no legitimate access to the system network. In opposite the insider is the node which accepted by the system network. Usually outsiders are harder to effect the network rather than insider which may have certain control of cryptographic materials.[7]

3) Single and Multiple: The adversarial nodes can be work as single or multiple in the network. For multiple adversaries every nodes can work independently or together. If the group of adversaries are fixed during the attack, then they can be viewed as non-adaptive adversary[16]. It is also possible that the members in the adversary group change over time. The main adversary in the group can choose which node to compromise. It makes the adversary group an adaptive adversary group [4]. Although the type of collective adaptive adversary exists in theory, it is difficult to become real threat in VANETs. Because in the VANETs, the topology of nodes changes rapidly.

B. Type of Attacks

As VANETs is part of network system, it also face some similar security attacks. In this section we classify the attack types into three groups by their target.

1) Attacks target Messages in VANETs: In VANETs, there is a special type of message tempering called message suppression attack[17]. This attack is done by delay the broadcasting of some messages so that the attacker can get benefit from it. Network accidental failures are not avoidable, such like omission failure, commission failure and timing failure. With exceeded fault tolerance amount nodes, it can lead to difficult of avoid the Byzantine failure. With these malicious nodes and the failure of node communication protocol, malicious acts may modify, delete the safety messages for reliable nodes. However, Byzantine fault tolerance problem is hard to deal with in VANETs due to its highly dynamic network. As

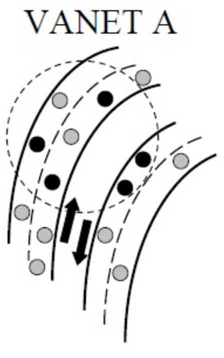

Fig. 4. Black nodes represent as malicious nodes. Gray circles represent reliable nodes. Dash line circle represent the communication range

figure 4, VANETs A shows the example that the colluding adversaries (indicated by the black circles) are successful in convincing the honest node (shown in gray at the center of the circle) of false data, but in a VANET it is difficult to maintain such a configuration for any significant duration[18].

2) Attacks target Users in VANETs: In the VANETs, every node content with personal privacy, the malicious attacker may catch the information from every node in the network. Usually there are many kinds of privacy information may directly effect the network security. One of the most important information is the node's ID. ID disclosure is dangerous if the attacker catch the safety node access of the network, it will turns to unreliable node and may do modification and overwhelm the original resource. The node ID is always related to the public key correlation, so one of the attack type is that the attacker set up two receivers on a predictable pathway, then they can analyze and steal the public key for the network access in the node has not change the key in this interval. Anonymous changeable keys may help to fix this issue, however, it will bring another difficult that every time when the key changed, the certification will need to be recheck again. So the revocation of keys and certificates is difficult issue in VANETs. Also, there are many other valuable information from the target users like location tracking, and all of these information should be well protect in case of malicious usages.

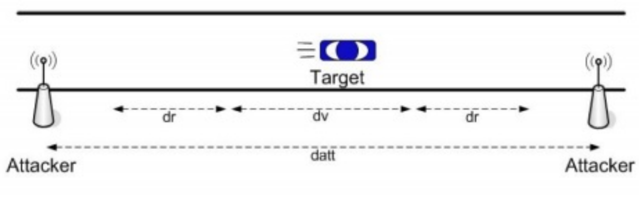

Fig. 5. Sample of attacks

3) Attacks target Network in VANETs: Denial of Service (DoS) is one of the most common way to disable a system by sending bunch of flood requests. In VENETs it can target a single node or focus on part of network, Dos can be done by cover a particular node(vehicle) resource or Jamming the channel and cause the malicious CCH(Congestion Control Channel). As a reliability concern for the network communication, jamming need to be considered with Constant Jamming and Random Jamming. Attackers may also choose to target routing protocol applied in the network [10]. [4] mentioned that there are still no widely agreed which type of routing protocol should be used in VANETs. It may be harder for attack to conduct wormhole attack than in other network system since VANETs is highly dynamic. In the research [18], they design a method to detecting and correcting errors that have been maliciously introduced into data in a VANET. "The approach relies on using sensor data, collected by nodes in the VANET, shared with immediate neighbors, and propagated to a neighboring region"[18].

And there are many other network attacks which also can be effect in the VANETs like Sybil attack, Bogus message attack, Eaves Dropping, Masquerading, Worm Hole, Message Suppression attack.[13]

IV. Conclusion

In this paper we summarized and classify the malicious acts for the VANETs. As most of researches mentioned, while nodes in the VANETs are highly dynamic and hard to apply on formal data communication security technique, so the Byzantine failures problem may be a highly concern question. As the [4] shows, some recent DSRC researches are looking for the strategies to increase Reliability and Survivability for DSRC communication. However, still there exists many challenges related brute force malicious acts. Reliability of the DSRC safety application is the major thing that should never be compromised since it related to the safety of life. But if it is almost impossible to avoid mistakes happened, the system should consider what to react rather than how to avoid, that is, survivability.

References

[1] H. Omar , W. Zhuang and L. Li *VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs*, IEEE Trans. Mobile Comput., vol. 12, no. 9, pp.1724 -1736 2013.

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

[3] A. Serageldin, and A. Krings, *The Impact of Redundancy on DSRC Safety Application Reliability under Different Data Rates*, Proc. 6th International Conference on New Technologies, Mobility and Security, (NTMS 2014), Dubai, March 30 - April 2, 2014.

[4] Philippe G.; Dan G.; Jessica S. *Detecting and Correcting Malicious Data in VANETs* in Palo Alto Research Center, 2014

[5] W. Lin, et. al., A comparison of 802.11a and 802.11p for V-to-I communication: a measurement study, ICST QShine, 2010.

[6] Maxim Raya and Jean-Pierre Hubaux. *Securing vehicular ad hoc networks*. Journal of Computer Security, 15(1):3968, 2007

[7] P. Papadimitratos, V. Gligor, and J-P. Hubaux. *Securing vehicular communications-assumptions, requirements, and principles*. In Workshop on Embedded Security in Cars (ESCAR), volume 2006, 2006.

[8] A. Serageldin, and A. Krings, *The Impact of Redundancy on DSRC Safety Application Reliability under Different Data Rates*, Proc. 6th International Conference on New Technologies, Mobility and Security, (NTMS 2014), Dubai, March 30 - April 2, 2014.

[9] Jianhua He, et. al. *Adaptive Congestion Control for DSRC Vehicle Networks*, IEEE COMMUNICATIONS LETTERS, VOL. 14, NO. 2, FEBRUARY 2010

[10] Xiaomin Ma, et. al. *Performance and Reliability of DSRC Vehicular Safety Communication: A Formal Analysis*, IEEE Commun. Mag., 2009.

[11] Nabih Jaber. *Performance Enhancement of the OFDM-Based DSRC System Using Frequency-Domain MAP Equalization and Soft-Output Demappers*, University of Windsor, 2009.

[12] Pelechrinis, K.; Iliofotou, M.; Krishnamurthy, S.V., ”Denial of Service Attacks in Wireless Networks: The Case of Jammers,” in Communications Surveys & Tutorials, IEEE , vol.13, no.2, pp.245-257, Second Quarter.

[13] Praba, V.L.; Ranichitra, A., ”Isolating malicious vehicles and avoiding collision between vehicles in VANET,” in Communications and Signal Processing (ICCSP), 2013 International Conference on , vol., no., pp.811-815, 3-5 April 2013 doi: 10.1109/iccsp.2013.6577169

[14] Anup, C.; Chihsiang W., ´DSRC Challenges and its Reliability during Congestion in Intelligent Transportation System´, in CS520 Semester Project, 2015 Computer Science University of Idaho

[15] SAE International *DSRC Implementation Guide A guide to users of SAE J2735 message sets over DSRC*, 2014.

[16] Shuxian L., *Analysis and detecting of misbehaviours in VANETs*, 2014.

[17] B. Parno and A. Perrig. *Challenges in securing vehicular networks*. In Workshop on hot topics in networks (HotNets-IV), pages 16, 2005.

[18] Philippe Golle, Dan Greene, and Jessica Staddon. 2004. *Detecting and correcting malicious data in VANETs.* In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks (VANET ’04).