Multiple security domain model of a vehicle in an automated platoon

Uday Kanteti, Bruce Mcmillin

Chapter 5

MULTIPLE SECURITY DOMAIN MODEL OF A VEHICLE IN AN AUTOMATED PLATOON

Uday Kanteti and Bruce McMillin

Abstract This chapter focuses on the security of automated vehicle platoons. Specifically, it examines the vulnerabilities that occur via disruptions of the information flows among the different types of sensors, the communications network and the control unit in each vehicle of a platoon. Multiple security domain nondeducibility is employed to determine whether or not the system can detect attacks. The information flows among the various domains provide insights into the vulnerabilities that exist in the system and whether the model is nondeducible. If nondeducibility is found to be true, then an attacker can create an undetectable attack. Defeating nondeducibility requires additional information sources, including invariants pertaining to vehicle platoon operation. A platoon is examined from the control unit perspective to determine if the vulnerabilities are associated with preventing situational awareness, which could lead to vehicle crashes.

Keywords: Automated vehicle platoons, multiple security domain nondeducibility

1. Introduction

Automated vehicle systems are likely to be the future of transportation. The concept of a vehicle platoon where 8-25 vehicles follow each other and each vehicle mimics the actions performed by the vehicle in front of it is compelling. The Partners for Advanced Transit and Highways (PART) Project was introduced in 1986 to make this concept a reality. It was believed that introducing platoons would increase road capacity, reduce trip delays and limit energy consumption. A major reason for the PATH Program was to reduce accidents and breakdowns [13]. However, many people are hesitant to trust the decision making of driverless vehicles. As such, the approach taken in this research is to

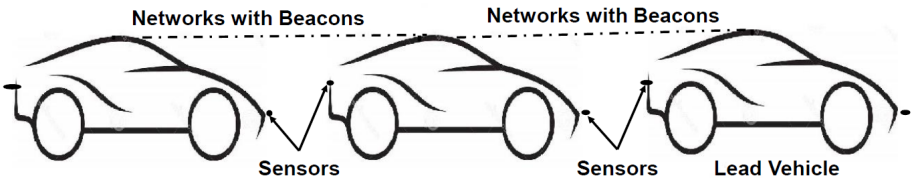

Figure 1. A vehicle platoon and its information transfer paths.

reduce the security threats that may impede vehicle decision making, reducing the barrier to the adoption of driverless vehicle technologies.

An automated vehicle is a cyber-physical system in which significant cyber, communications and physical components work together. The information present in the system may be cyber in nature or it may pertain to the physical properties of the system. Preserving correct information flows treats the security issues in the cyber-physical system uniformly. Disruption of information leads to the lack of deducibility of the system state.

The main contribution of this research is the development of a cyber-physical platoon model in which attacks are deducible. The goal is to create security domains such that, if an attack occurs in one domain, then the compromised domain can be detected with the help of information paths from the other domains. This research and its case scenarios demonstrate the potential to detect security problems in a cyber-physical system.

2. System Model

Figure 1 presents a vehicle platoon and its information transfer paths. The vehicle platoon works in the following manner [16]:

- The vehicle in front of the platoon is assigned the role of the lead vehicle. The lead vehicle decides the movements of the platoon. The vehicles behind the lead vehicle follow.
- Each vehicle in the platoon (except for the lead vehicle) receives information from the previous vehicle and maneuvers accordingly.
- If the lead vehicle wishes to slow down or take a turn, it indicates this via a beacon message and the other vehicles follow suit.
- Each vehicle checks and compares the information it receives from sensors and from the communications network. If the information is consistent, the vehicle proceeds; otherwise, it raises a flag.
- Other vehicles check the flagged vehicle information and decide whether to keep the vehicle in the platoon or remove it from the platoon.

Communications between autonomous vehicles create a vehicular ad hoc network. In platooning, each vehicle is connected directly to the vehicle in

front, to the vehicle behind it and also to the lead vehicle (since each vehicle mimics the lead vehicle). This results in a constant number of connections (i.e., three connections) for each vehicle. All the vehicles in the platoon stay connected and the scalability problem is reduced.

This cyber-physical system consists of embedded computers, control units, a physical system, the vehicles and their sensors, and a message-passing communications network, each residing in its own security domain. Information flows among the various security domains.

The proposed model includes the following components:

- **Communications Network:** A platoon may use any wireless networking technology, the most prominent being a short range radio technology such as WLAN (standard Wi-Fi or ZigBee). Cellular technologies or LTE can also be used. In the United States, the IEEE 1609 WAVE (wireless access in vehicular environments) protocol stack builds on IEEE 802.11p WLAN that operates on seven reserved channels in the 5.9 GHz frequency band. The WAVE protocol stack is designed to provide multi-channel operation (even for vehicles equipped with a single radio), security and lightweight application layer protocols.

- **Sensors:** Velodyne and HDL-64E LiDAR sensors are designed for obstacle detection and navigation by autonomous vehicles. Their durability, 360° field of view and very high data rates render the sensors ideal for the most demanding perception applications as well as for 3D mobile data collection and mapping applications. The information received from a LiDAR sensor is sent to the vehicle control unit. RADAR sensors are currently used in advanced cruise control systems to measure vital parameters such as range, angle and Doppler velocity. This information is used to assess the driving situation and signal the control unit about potentially dangerous events.

- **Control Unit:** The control unit is the brain of a vehicle and gives it directions. The control unit makes decisions based on the inputs it receives from the sources mentioned above. If discrepancies in the information paths are detected, the control unit alerts other vehicles by sending special-purpose messages. If enough information paths are available, the control unit can take corrective actions itself.

- **Monitor:** Invariant equations (e.g., distance = speed $\times$ time (t)) are evaluated by an embedded monitor to compute where the vehicle would be at time t. The assumption is that the vehicle would have its own speed calculation mechanism such as a speedometer and a clock to tell the time. At each instant, the monitor computes the distance information and sends it to the control unit. The monitor evaluates the invariant using each information source to check for consistency.

Messages with information about speed and distance are passed from the lead vehicle to other vehicles in the platoon in the form of beacons (messages

transmitted in the network from one vehicle to another) as shown in Figure 1. Beacons contain information about the speeds and distances of all the vehicles in front of a given vehicle. A control unit gathers information directly from the sensors and from the communications network that exists between the vehicles.

3. Related Work

Various security threats target confidentiality (e.g., an attacker tracks a vehicle), integrity (e.g., an attacker changes beacon information) and availability (e.g., an attacker jams the network that communicates speed and distance values). The attacker is defined as someone/something that is not authorized to access or modify the vehicle or system components, but is able to do so. The attacker may intend to cause a traffic jam or even a crash.

3.1 Confidentiality

Much research on confidentiality or privacy has focused on securing the entity itself. Separate access control [9] can prevent changes to vehicle control commands. Dividing each section on the control board restricts information flow based on the type of control implemented by the section. This preserves the privacy of the vehicle.

A virtual trip lane (VTL) with multiple zones (e.g., VTL_1 and VTL_2) [14] can preserve privacy by using the lane to regulate location and speed reports. The estimated time for VTL_1 is computed when the vehicle enters the next zone VTL_2 and is compared against the actual arrival time in VTL_2. Releasing trajectory data only within a single virtual trip lane zone helps protect privacy.

3.2 Integrity

Research has focused on securing information using encryption [7], but this only provides conditional privacy (i.e., only the entities involved in the communications know about the communications). Several integrity attacks have targeted vehicles via direct access to the hardware or via a wireless channel. The main goal of an attacker is to access the controller area network (CAN) of a vehicle and control the vehicle.

Koscher et al. [8] discuss the vulnerabilities of controller area networks. Controller area network packets contain no authentication fields or even source identifier fields, meaning that any component can "invisibly" send packets to any other component in the network. This means that just one compromised component can be used to control all the other components on the controller area network bus. Koscher et al. report that broadcasting malicious data from an infected controller area network can enable an attacker to seize control of a vehicle.

A widely-reported wireless attack [11] took control of the engine control unit (ECU) of a Jeep that sends commands to the other components in the vehicle. The attack leveraged a cellular network connected to the vehicle entertainment

system in order to compromise the controller area network. The attack was able to kill the brakes, steer the vehicle and control the horn and parking lights at will.

Koscher et al. [8] have also worked on wireless access, which is discussed in [3]. Access to the engine control unit is gained via Bluetooth and reverse engineering. Once access is gained, the attacker can make changes to the braking system and modify the speed of the vehicle.

Another recent attack targeted a Tesla S model by gaining wireless access to the controller area network of the vehicle [1]. The attack was launched when the driver connected to a malicious Wi-Fi hotspot. The researchers were able to devise an alternate authentication scheme using ECDSA with omission techniques and TESLA++. However, the problem of scalability still exists because each new vehicle has to be authenticated with every other vehicle in a group by a roadside unit (despite the fact that the authentication overhead is reduced when two groups intend to communicate). A special message is sent when the information is not authentic; the verification is performed by the engine control unit using information from another vehicle.

3.3 Availability

An attack that impacts the availability of information can cause serious problems to connected vehicles. Traditional techniques such as beamforming (i.e., actively steering wireless transmission and reception beams to maximize useful signal reception while minimizing interfering signal reception) can combat jamming attacks on sensors [12].

A Sybil attack can be used to target connected vehicles. In this attack, the reputation system of a peer-to-peer network system is subverted maliciously by creating a large number of pseudonymous identities. Using these identities, the attacker can gain a disproportionately large influence on the functioning of the system. This attack can be detected efficiently using a less complex cryptographic technique and obtaining pseudonyms from roadside units at continuous intervals from a trusted source [2]. Distinct roadside units that periodically collect reports from communicating vehicles in the neighborhood reduce the vulnerability.

In the long term, it is believed that vehicles involved in a Sybil attack would pass similar information as the benign vehicles. A trust-based system for detecting malicious vehicles can employ an iterative filtering algorithm to detect malicious vehicles and address the problem of collusion [6], where vehicles attempt to improve the trust ratings of false vehicles.

Denial-of-service (DoS) attacks can be detected easily. Lyamin et al. [10] use time intervals to listen on a channel and determine whether or not all the beacons have been received. If there is a beacon loss, two nodes may be involved in a collision within the same group. To prevent collisions, the nodes must have an initialization phase. The initialization phase ensures that the nodes start from safe states (i.e., no attacks) and do not collide with each other.

Some attacks are difficult to detect and mitigate using only one vehicle [11]. When multiple vehicles are present, the vehicles could examine the information they receive and determine that a vehicle is under attack. This is possible because the attacked vehicle would send information that would not match the information available to the other vehicles.

Sun et al. [14] have shown that the use of virtual trip lane zones can address privacy concerns. Their approach relies on real-time data. Therefore, if an attacker were to know the position of a vehicle in a virtual trip zone, the attacker would be track the movement of the vehicle in real time.

Certain attacks spoof data originating from a communications network and beacons [3, 8]. Cryptography can be used to secure messages between vehicles [1, 7]. Using a strong encryption method can secure communications, but the assumption is that the cryptographic keys are exchanged securely before communications are initiated. Another underlying assumption is that the vehicle itself is not compromised. In real-time scenarios involving vehicles it may not be possible to securely share information while the vehicles are in motion. The denial-of-service attacks discussed in [10, 12] are based on reducing interference and listening to the channel periodically, but hazardous weather conditions could make it difficult to listen to the channel. Instead of treating all these issues separately, the proposed methodology adopts a scientific approach that uniformly models the interactions of distinct security domains.

3.4 Multiple Security Domain Nondeducibility

Nondeducibility was introduced by Sutherland [15] in an attempt to model infrastructures that secure information using a partitioned model. The partitions are grouped into two or more sets. These sets are usually labeled as high and low with all the information restricted to one side of the partition or the other. Information that cannot be determined from the other side of the domain is said to be nondeducibility secure. However, the partition must be absolute and simple. Overlapping security domains present severe difficulties for nondeducibility as do information flows that cannot be evaluated because the model lacks the required valuation functions.

V is a set of valuation functions such that $V^i_{s_x}(w)$ returns the value of a state variable s_x as seen by an entity i in world w. For example, if a vehicle control unit c obtains distance information from sensor d_s, then $V^c_{d_s}(w)$ returns true; otherwise, it returns false.

Definition. A system is multiple security domain nondeducible (MSDND) secure if there exists a world with a pair of states where one state must be true and the other false (exclusive or), but an entity i has no valuation function for the states. An entity i in security domain SD^i cannot know which state is true and which state is false [4]. In particular:

$$\begin{aligned}\text{MSDND(ES)} = \exists w \in W \vdash \Box\, [\,(\, s_x \vee s_y)\,] \;\wedge \sim(\, s_x \wedge s_y) \;\wedge \\ [\, w \models (\; \not\exists\, V^i_{s_x}(\, w) \;\wedge\; \not\exists\, V^i_{s_y}(\, w)\,)\,]\end{aligned}$$

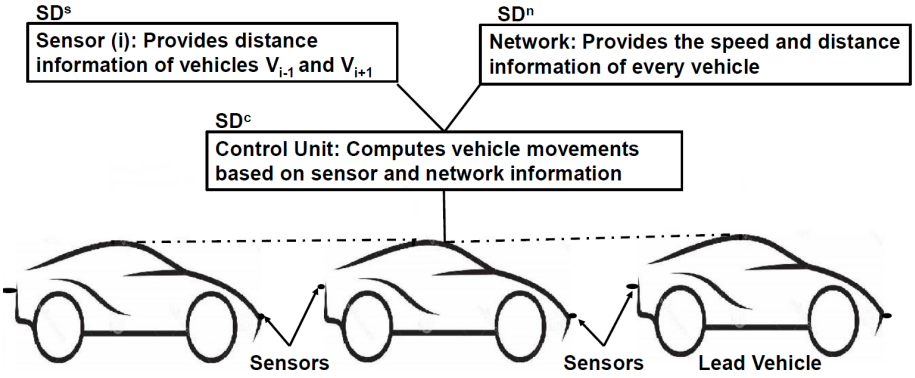

Figure 2. Security domains of information flow.

where s_x and s_y are states, V_x^i and V_y^i are the valuation functions of s_x in domain i and s_y in domain i, respectively, and w is a world.

4. Problem Statement

It is possible to devise an attack – like Stuxnet [5] – that changes the speed and distance values. However, it is important to be able to tell if the attack (i.e., changing sensor or network information) is MSDND. If the attack is MSDND, then the attacker has an advantage because the target would not know which component is malfunctioning. Therefore, the model should be designed to eliminate attacks that are MSDND secure.

Figure 2 shows the security domain partitions and the interactions between vehicle control units and communications points. A monitor positioned in a vehicle evaluates the invariants pertaining to the vehicle state. If a discrepancy exists in the distance information sent by one of the paths to the control unit, then the control unit would know that something is wrong.

The following entities can be evaluated to determine the interactions between a vehicle and the communications system:

- **c** : The vehicle control unit c obtains data and computes the movement.
- **s** : Each LiDAR sensor s provides a distance value $d(s)$.
- **n** : The communications network n between the vehicles provides the network value $d(n)$.
- **ISV** : The information source validator ISV is executed by the monitor to check if the information received from the information paths is valid. Table 1 shows that ISV sequentially checks sources against other sources and invariants that involve multiple sources.

Table 1. Information source validation performed by ISV.

Check	Source
ch_1	$d(s) = d(n)$
ch_2	$d(s) = d(invariant_1)$
ch_3	$d(n) = d(invariant_1)$
ch_4	$d(s) = d(beacon)$
ch_5	$d(s) = d(invariant_2)$
ch_6	$d(n) = d(beacon)$
$\vdots$	$\vdots$

The term $d(c)$ denotes the distance that the control unit accepts based on information received from the paths. For a given state, the valuation functions return the values of the corresponding state variables (c, s, n) as seen by the entity in control.

The control unit detects a compromised information path if the information it receives from the corresponding sensor is not equal to the value it receives from the communications network. In other words, it uses the result of a check ch_i. If the check value is false, then the control unit knows that one of the information paths has been compromised.

Five cases and their sub-cases are discussed in the following sections.

4.1 Case 1

Figure 1 shows that there are two information paths, sensor and network. Case 1 assumes that a vehicle has exactly one information path – either sensor or network – that provides information about the distance between the vehicle and the vehicle in front of it. In particular, the goal is to show that one information path can make the system MSDND secure as well as not MSDND secure. Four sub-cases are considered.

Case 1(a): Assume that the vehicles are connected only to network n and that the network provides correct information (i.e., $d(n) = \text{true}$):

- $w \models (\exists V^c_{d(n)}(w))$: Control unit receives distance information from the network.

It follows that:

$$\begin{aligned}\text{MSDND(ES)} = \exists w \in W : w \vdash \Box(d(n) \oplus \neg d(n)) \wedge \\ [w \models (\exists V^c_{d(n)}(w) \vee \nexists V^c_{\neg d(n)}(w))]\end{aligned}$$

The system is not nondeducible secure to the control unit according to the definition because $\exists V^c_{d(n)}(w)$.

Case 1(b): Assume that the vehicles connected to network n receive incorrect information (i.e., $\neg d(n) = \text{true}$):

- $w \models (\nexists V^c_{\neg d(n)}(w))$: Control unit receives distance information from the network.

It follows that:

$$\begin{aligned}\text{MSDND(ES)} = \exists w \in W : w \vdash \Box(d(n) \oplus \neg d(n)) \wedge \\ [w \models (\nexists V^c_{d(n)}(w) \vee \nexists V^c_{\neg d(n)}(w))]\end{aligned}$$

The system is nondeducible secure to the control unit according to the definition.

Case 1(c): Assume that the vehicles are connected only to sensor s, which provides correct information (i.e., $d(s) = \text{true}$). This case is similar to Case 1(a).

Case 1(d): Assume that the vehicles are connected to sensor s and receive incorrect information (i.e., $\neg d(s) = \text{true}$). This case is similar to Case 1(b).

Although the goal is to create a model that is not nondeducible secure, the control unit in Cases 1(b) and 1(d) would believe the data and direct the vehicle accordingly. Having no other information path for verification is potentially hazardous because it is nondeducible if the information received is incorrect.

4.2 Case 2

In Case 2, the sensor and communications network provide distance information to the control unit. Upon receiving the distance information, the control unit attempts to determine whether or not the information provided is correct. The control unit would know that an information path is corrupted if there is a discrepancy in the information provided by the two paths. In the following, two sub-cases are examined.

Case 2(a): If n is faulty, then the system has been compromised. The attacker can manipulate the information and, thus, incorrect information is received by the control unit from the network (i.e., $\neg d(n) = \text{true}$ and $d(s) = \text{true}$).

- **S1:** $w \models (\exists V^c_{d(s)}(w))$: Control unit receives information from the sensor.
- **S2:** $w \models (\nexists V^c_{\neg d(n)}(w))$: Control unit receives information from the network.
- **S3:** $w \models (\exists V^c_{ch_1})$: Information received from the sensor and network do not match.

From statement S3, the control unit would know that an information path has been compromised.

Combining statements S1 and S2 yields the following expression:

$$\begin{aligned}\text{MSDND(ES)} = \exists w \in W : w \vdash \Box(\neg d(n) \oplus ch) \wedge \\ [w \models (\exists\ V^c_{d(ch_1)}(w) \vee \nexists\ V^c_{\neg d(ch)}(w))]\end{aligned}$$

The system is not nondeducible to the control unit because the unit can deduce that something is wrong. But it cannot determine which information path is responsible. An additional information path is needed to determine the path that transmits incorrect data.

Case 2(b): If s is faulty, then the system has been compromised. The attacker can manipulate the information and, thus, incorrect information is received by the control unit from the network (i.e., $\neg d(s) = \text{true}$ and $d(n) = \text{true}$). The following statements hold:

- **S1:** $w \models (\nexists V^c_{\neg d(s)}(w))$: Control unit receives information from the sensor.
- **S2:** $w \models (\exists\ V^c_{d(n)}(w))$: Control unit receives information from the network.
- **S3:** $w \models (\exists V^c_{ch_1})$: Information received from the sensor and network do not match.

From statement S3, the control unit would know that an information path has been compromised. Combining statements S1 and S2 yields the following expression:

$$\begin{aligned}\text{MSDND(ES)} = \exists w \in W : w \vdash \Box(\neg d(s) \oplus ch) \\ \wedge\ [w \models (\exists V^c_{d(ch_1)}(w) \vee \nexists V^c_{\neg d(s)}(w))]\end{aligned}$$

The system is not nondeducible to the control unit because the unit can deduce that something is wrong. But it cannot determine which information path is responsible for transmitting the incorrect data.

Invariants relate the properties of a vehicle in a manner that, if one portion of the model is compromised, then the invariant is falsified. The MSDND model is extended as follows:

- $invariant_{dist}(d(i))$: distance = speed $\times$ time. Each vehicle has its own speedometer that enables it to compute the distance that it has traveled during a period of time.

Based on the model, the three sources that provide distance information are:

$$d_{t2} = \begin{cases}\text{range calculated by LiDAR/RADAR} - d_{t1}(s) \\ \text{speed} \times \text{time} - d_{t1}(i) \\ \text{distance calculated via network} - d_{t1}(n)\end{cases}$$

The three sources, sensor, network and invariant, are shown in Figure 3.

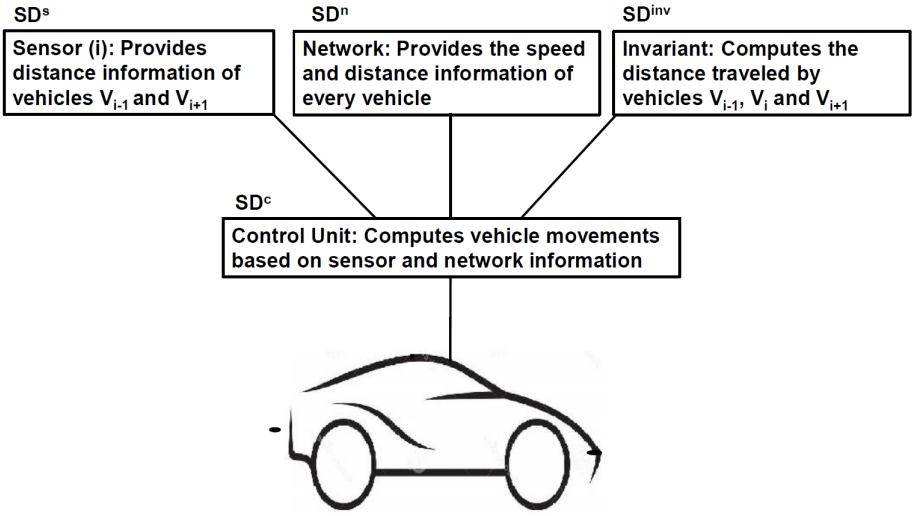

Figure 3. Invariant model with three information paths.

Sensor vs. Invariant: It is assumed that the vehicles are moving at constant velocity. Assume that, at time = 1 s, a sensor reports $d(s) = 5$ m and the vehicle speed is 30 m/sec. At time = 5 s, since there is no change in the speed of the vehicle, the sensor should report $d(s) = 5$ m. If any other information is provided, then it can be determined that the sensor has been compromised.

Network vs. Invariant: The network periodically updates the speed, location and other relevant information about a vehicle as shown in Figure 4. Specifically, the vehicle can calculate the distance covered in the $t_2 - t_1$ interval using the latitude (lat) and longitude (lon) and by computing: distance = speed $\times$ time. If at time t_1, the network gives a certain location for vehicle V_{i+1}, and at t_2, the network gives another location for V_{i+1}. Then, vehicle V_i can compute the distance moved by V_{i+1} because it has its speed and the duration. If there is a discrepancy in the information, then the network has been compromised.

The control unit would have the correct distance information if a valuation function exists for any one of ch_1, ch_2 or ch_3.

4.3 Case 3

In Case 3, another information path (invariant path) is added to the model. This additional information path helps make the model not MSDND secure. The control unit would also have the correct distance information if a valuation function exists for any one of the checks ch_1, ch_2 or ch_3, which can indicate

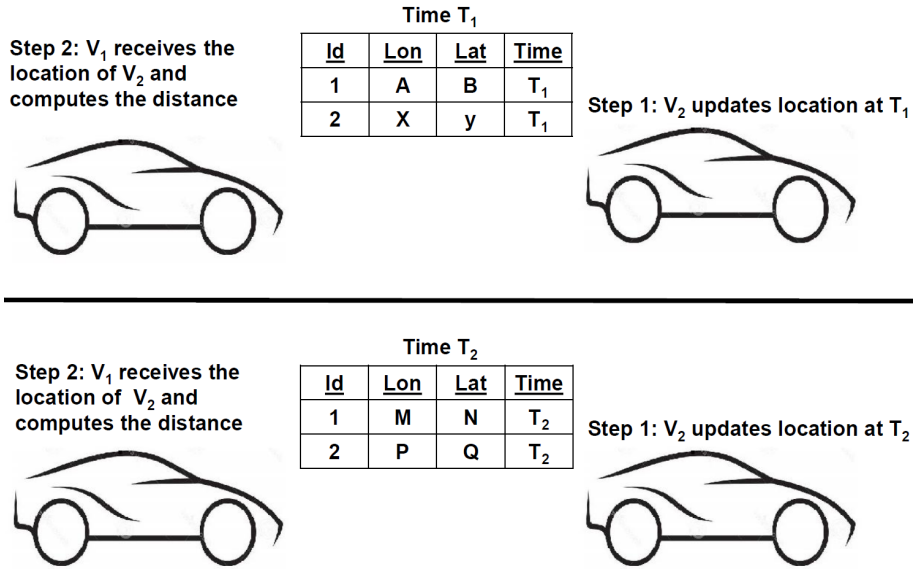

Figure 4. Network vs. invariant.

which path is compromised. Thus, the control unit can sense that something is wrong.

Case 3(a): n is faulty (i.e., $\neg d(n) = \text{true}$). The following statements hold:

- **S1:** $w \models (\nexists V^c_{\neg d(n)}(w))$: Control unit receives information from the network.
- **S2:** $w \models (\exists V^c_{d(s)}(w))$: Control unit receives information from the distance estimators.
- **S3:** $w \models (\exists V^c_{d(i)}(w))$: Control unit receives information from $invariant_{dist}$.
- **S4:** $w \models \nexists V^c_{ch_1}$.
- **S5:** $w \models \exists V^c_{ch_2}$.
- **S6:** $w \models \nexists V^c_{ch_3}$.
- **S7:** $w \models \exists V^c_{d(c)}(w)$: From statement S5.

It follows that:

$$\begin{aligned}\text{MSDND(ES)} = \exists w \in W : w \vdash \Box(\neg d(n) \oplus ch_2) \wedge \\ [w \models (\exists V^c_{d(ch_2)}(w) \vee \nexists V^c_{\neg d(n)}(w))]\end{aligned}$$

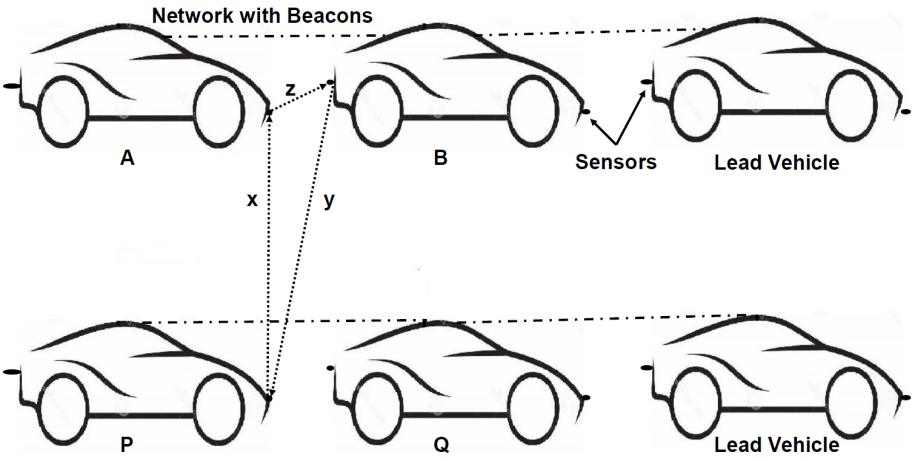

Figure 5. Multiple platoons.

This is not nondeducible secure because the control unit can deduce that something is wrong and can determine that the network is responsible for the incorrect data being transmitted.

Case 3(b): s is faulty (i.e., $\neg d(s) = \text{true}$). This case is similar to Case 3(a). It is assumed that the invariant is always true and that the information about the speed is unaltered. However, as discussed in [11], the attacker can also change the information received by the control unit. In this situation, the other two components, sensor and network, can provide the correct information.

Assume that there are multiple vehicles in the platoon and multiple platoons are nearby. This situation is shown in Figure 5.

The sources of information are:

- **s** : Each LiDAR sensor s provides a distance value $d(s)$.
- **n** : The communications network n between the vehicles provides the network value $d(n)$.
- **Invariant$_1$** : distance = speed $\times$ time gives the value of $d(invariant_i)$. Every vehicle has a speedometer with which it can compute the distance it has traveled during a period of time.
- **ISV** : The information source validator ISV is essentially an array data type that stores the true/false results after comparing the distance reported by each information source with another as shown in Table 1. If more true values are reported than false values, then a valuation function for ISV exists.
- **invariant$_2$** : As shown in Figure 5, communications can occur between two platoons. In this case, vehicles A, B and P form an information path

because each vehicle is equipped with proximity sensors. Vehicle P has the information $\{x, y\}$, vehicle A has the information $\{x, z_A\}$ and vehicle P has the information $\{y, z_B\}$. Sending this information back to vehicles A, B and C yields the information $\{x, z_A, z_B\}$. If z_A is not equal to z_B, then no valuation function exists for $invariant_2$; otherwise, a valuation function exists.

- **beacon$_i$** : This provides information about $speed_i$ and $velocity_i$ of vehicle V_i in the platoon.

4.4 Case 4

In Case 4, multiple vehicles are in a platoon and no other platoons are nearby. Vehicles communicate information between each other using beacons. A beacon is an additional information path to the control unit that can help detect an incorrect information path.

Consider the situation where a vehicle provides incorrect information (i.e., $\neg beacon$ = true). The following statements hold:

- **S1:** $w \models (\exists V^c_{d(n)})$: Control unit receives information from the network.
- **S2:** $w \models (\exists V^c_{d(s)})$: Control unit receives information from the sensor.
- **S3:** $w \models (\exists V^c_{inv_1})$: Control unit receives information from $invariant_1$.
- **S4:** $w \models (\nexists V^c_{beacon_i})$: Control unit receives information from the beacon.
- **S5:** $w \models \exists V^c_{ISV}$: From statements S1, S2 and S3.
- **S6:** $w \models \exists V^c_{d(c)}(w)$: From statement S5.

It follows that:

$$\begin{aligned}\text{MSDND(ES)} = \exists w \in W : w \vdash \Box(\neg beacon_i \oplus ISV) \wedge \\ [w \models (\exists V^c_{d(c)}(w) \vee \nexists V^c_{\neg d(c)}(w))]\end{aligned}$$

This is not nondeducible secure because the control unit can deduce that something is wrong and can determine that $beacon_i$ is responsible for the incorrect data being transmitted. Thus, it is possible to detect if a vehicle in the platoon has been compromised.

4.5 Case 5

In Case 5, there are multiple platoons as shown in Figure 5. Information paths exist between adjacent platoons. The information paths help detect an incorrect data path when multiple information paths are compromised.

Consider the situation where $\neg beacon_i$ = true. The following statements hold:

- **S1:** $w \models (\exists V^c_{d(n)})$: Control unit receives information from the network.
- **S2:** $w \models (\exists V^c_{d(s)})$: Control unit receives information from the sensor.
- **S3:** $w \models (\exists V^c_{inv_1})$: Control unit receives information from $invariant_1$.
- **S4:** $w \models (\nexists V^c_{beacon_i})$: Control unit receives information from $beacon_1$.
- **S5:** $w \models (\exists V^c_{inv_2})$: Control unit receives information from $invariant_2$.
- **S6:** $w \models \exists V^c_{inv_2}$: From statements S1, S2, S3 and S5.
- **S7:** $w \models \exists V^c_{d(c)}(w)$: From statement S5.

It follows that:

$$\begin{aligned}\text{MSDND(ES)} = \exists w \in W : w \vdash \Box(\neg beacon_i \oplus invariant_2) \wedge \\ [w \models (\exists V^c_{d(c)}(w) \vee \nexists V^c_{\neg d(c)}(w))]\end{aligned}$$

This is not nondeducible secure because the control unit can detect that something is wrong and can determine that $beacon_i$ is responsible for the incorrect data being transmitted.

As demonstrated above, information from other platoons can be used to detect the compromised information path and, ultimately, the compromised vehicle. The case where platoons can detect if a vehicle has been compromised is considered because Case 4 demonstrates that it is possible to detect a compromised vehicle without a platoon. However, if other information sources are compromised, then having the additional source assists in attack detection.

5. Conclusions

MSDND is useful to model attacks where the goal is to hide critical information from an attacker. MSDND secure is a major disadvantage to a vehicle platoon and a boon to an attacker because information can be hidden by making it impossible to detect an attack or the valuation function could be falsified to produce an invalid valuation, rendering the information MSDND secure and undetectable. As demonstrated in the case study, the vehicle control units in a platoon may be unable to determine which vehicle has been compromised.

This research has focused on securing vehicles in an automated platoon. Minimizing the number of assumptions made in the model is a topic of future research. It is also necessary to handle situations where more than half of the information sources are compromised. Another problem is to handle cases where two sets of information sources provide the same incorrect information. Other vehicular scenarios that will be considered include platoon joining, lane changing and platoon splitting.

Acknowledgement

This research was supported, in part, by the Future Renewable Electric Energy Distribution Management Center, a National Science Foundation supported Engineering Research Center, under Grant EEC 0812121; by the National Science Foundation under Grant CNS 1505610; and by the National Institute of Standards and Technology under Grant 60NANB15D236.

References

[1] Y. Abueh and H. Liu, Message authentication in driverless cars, *Proceedings of the IEEE Symposium on Technologies for Homeland Security*, 2016.

[2] M. Al Mutaz, L. Malott and S. Chellappan, Leveraging platoon dispersion for Sybil detection in vehicular networks, *Proceedings of the Eleventh International Conference on Privacy, Security and Trust*, pp. 340–347, 2013.

[3] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner and T. Kohno, Comprehensive experimental analyses of automotive attack surfaces, *Proceedings of the Twentieth USENIX Conference on Security*, 2011.

[4] G. Howser and B. McMillin, A multiple security domain model of a drive-by-wire system, *Proceedings of the Thirty-Seventh IEEE Computer Software and Applications Conference*, pp. 369–374, 2013.

[5] G. Howser and B. McMillin, A modal model of Stuxnet attacks on cyber-physical systems: A matter of trust, *Proceedings of the Eighth International Conference on Software Security and Reliability*, pp. 225–234, 2014.

[6] H. Hu, R. Lu, Z. Zhang and J. Shao, REPLACE: A reliable trust-based platoon service recommendation scheme in VANET, *IEEE Transactions on Vehicular Technology*, vol. 66(2), pp. 1786–1797, 2017.

[7] D. Huang, S. Misra, M. Verma and G. Xue, PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs, *IEEE Transactions on Intelligent Transportation Systems*, vol. 12(3), pp. 736–746, 2011.

[8] 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, *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 447–462, 2010.

[9] U. Lang and R. Schreiner, Managing security in intelligent transport systems, *Proceedings of the Eighteenth IEEE International Conference on Intelligent Transportation Systems*, pp. 48–53, 2015.

[10] N. Lyamin, A. Vinel, M. Jonsson and J. Loo, Real-time detection of denial-of-service attacks on IEEE 802.11p vehicular networks, *IEEE Communications Letters*, vol. 18(1), pp. 110–113, 2014.

[11] C. Miller and C. Valasek, Remote exploitation of an unaltered passenger vehicle, presented at *DEF CON 23*, 2015.

[12] G. Patounas, Y. Zhang and S. Gjessing, Evaluating defense schemes against jamming in vehicle platoon networks, *Proceedings of the Eighteenth IEEE International Conference on Intelligent Transportation Systems*, pp. 2153–2158, 2015.

[13] S. Shladover, The California PATH Program of IVHS research and its approach to vehicle-highway automation, *Proceedings of the Intelligent Vehicles Symposium*, pp. 347–352, 1992.

[14] Z. Sun, B. Zan, J. Ban, M. Gruteser and P. Hao, Evaluation of privacy preserving algorithms using traffic knowledge based adversary models, *Proceedings of the Fourteenth IEEE International Conference on Intelligent Transportation Systems*, pp. 1075–1082, 2011.

[15] D. Sutherland, A model of information, *Proceedings of the Ninth National Computer Security Conference*, pp. 175–183, 1986.

[16] A. Wasef and X. Shen, PPGCV: Privacy preserving group communications protocol for vehicular ad hoc networks, *Proceedings of the IEEE International Conference on Communications*, pp. 1458–1463, 2008.