Fall 2017

# Multiple security domain model of a vehicle in an automated vehicle system

Uday Ganesh Kanteti



Department:

# MULTIPLE SECURITY DOMAIN MODEL OF A VEHICLE IN AN AUTOMATED VEHICLE SYSTEM

by

UDAY GANESH KANTETI

A THESIS

Presented to the Graduate Faculty of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

MASTER OF SCIENCE

in

COMPUTER SCIENCE

2017

Approved by

Dr. Bruce McMillin, Advisor
Dr. Daniel Tauritz
Dr. Jonathan Kimball

# ABSTRACT

This thesis 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 the system can detect attacks. The information flows among the various domains provide insights into the vulnerabilities that exist in the system by showing if an attacker's actions cannot be deduced. 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

# ACKNOWLEDGMENTS

First and foremost, I would like to express my sincere gratitude to my advisor Dr. Bruce McMillin for the continuous support of my master's study and research and for his immense knowledge, motivation, enthusiasm, and patience. His guidance helped me through all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my master's study. Besides my advisor, I would like to thank the rest of my thesis committee: Dr. Daniel Tauritz and Dr. Jonathan Kimball, for their insightful comments and encouragement and for the inputs they provided that helped me widen my research from various perspectives.

I would like to thank my fellow research students Anusha Thudimilla and Prakash Rao Dunaka for their input, feedback, and cooperation. Without their passionate participation and input, this project could not have been successfully completed. In addition, I would like to express my gratitude to some of the staff of the Computer Science department Dawn Davis and Rhonda Grayson for responding to all my queries. Also, I would like to thank my friends for accepting nothing less than excellence from me. Finally, I must express my very profound gratitude to my parents for providing me with unfailing support and continuous encouragement throughout my years of study. Thank you.

Very special gratitude goes out to National Institute of Standards and Technology, grant number 60NANB15D236 and with support from the Missouri S&T Intelligent Systems Center and the U.S. National Science Foundation, award number CNS-1505610 for helping and providing the funding for the work.

# TABLE OF CONTENTS

Page

# LIST OF ILLUSTRATIONS

# LIST OF TABLES

# NOMENCLATURE

| SYMBOL | DESCRIPTION |
|---|---|
| $s_x$ | A boolean state variable, $x$ is true or false |
| $W$ | The set of all possible worlds of the system |
| $w$ | A world of interest |
| $M$ | Model |
| $SD$ | Security Domain |
| $\phi$ | A boolean statement that can be evaluated |
| $V_x^i$ | A valuation function of boolean $x$ in domain $i$ |
| $i$ | Invariant source |

# 1. INTRODUCTION

Automated vehicle systems are likely to be the future of transportation. With the advent of VANETS (vehicular ad-hoc networks)[1] many vehicles are able to communicate through a wireless channel. The real time application of a vehicle platoon where 8-25 cars follow one another and mimic the actions performed by the vehicle in front of it is new but the concept of a vehicle platoon was introduced in PATH (Partners for Advanced Transit and Highways) project in 1986 [2] that demonstrated the benefits of a vehicle platoon. It was believed that the introduction of platoons would increase the capacity of the roads, reduce trip delays and limit energy consumption. The PATH program would also avoid accidents and breakdowns since more than 95% of accidents were caused by careless drivers and vehicle breakdowns [2].

People are often a little hesitant to trust the decision making of a driverless car. While cruise control has existed for some time, this only controls the speed but with the arrival of autonomous technology, other characteristics of a vehicle such as braking, maneuvering and acceleration can also be controlled. When the concept of a driverless vehicle is expanded to a vehicle platoon as shown in Figure 1.1, the information flow should be secure and any discrepancy in the distance or speed should be identified immediately. The goal of cyber-physical security is to figure out the cause of the discrepancy because once the source of the incorrect information is identified, appropriate steps can be taken to safeguard the infrastructure (i.e., to discard or repair). The information that is given out by the components of the vehicles needs to be protected.

Self-driving vehicles from Tesla and Google are already in the market and have been able to

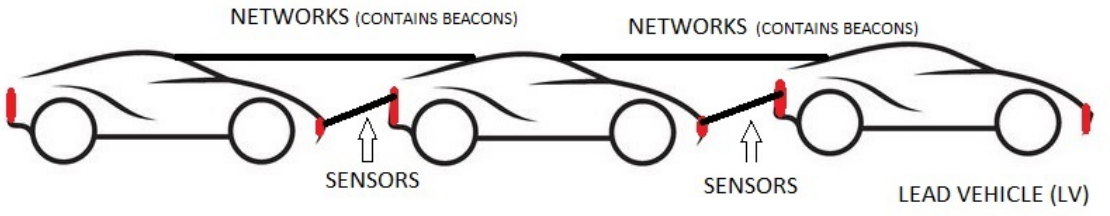


Figure 1.1. A vehicle platoon
(From https://static.dreamstime.com/t/car-line-art-vector-illustrations-48227977.jpg)

successfully demonstrate these vehicles in real traffic. These vehicles are able to handle all the driving. These cars are well equipped to detect pedestrians, cyclists, vehicles, road work and more from a distance of up to two football fields in all directions. It is logical to assume that in the coming years we would see more of self-driving vehicles and communication between vehicles is a distinct possibility.

Self-driving autonomous vehicles utilize technologies like GPS, 360-degree camera systems, sensors, beacons and powerful onboard processing computers. This gives the attacker a variety of path choices to attack but our infrastructure utilizes these information paths in such a way that even if a few paths are compromised, the remaining would help us identify the compromised path/vehicle.

The attack would be undetectable if the model is non-deducible because the vehicle would not know that there is a component in the car that has been compromised. The main contribution of the thesis is to devise a cyber-physical platoon model where an attack would be deducible and if possible alert the vehicle about the compromised source. We are trying to create security domains in such a way that if an attack occurs in one domain, then

the compromised domain could be detected with the help of information paths from other domains. The presented work and its various case scenarios demonstrate the potential to detect security issues in a cyber-physical system.

The rest of the thesis is organized as follows Section 2 presents the system model. Section 3 gives the related work, Section 4 presents the problems, attempted solutions and the proofs associated with it. Section 5 provides direction for future work and Section 6 concludes this work.

# 2. SYSTEM MODEL

The following describes how the vehicle platoon works [3]:

1. The lead vehicle(LV) decides the movement of the platoon. Lead vehicle is defined as the vehicle in front of the platoon. The vehicles behind the LV follow it.

2. The vehicles in the platoon receive this information from the previous vehicle and maneuver it accordingly.

3. If the LV wants to slow down or take a turn, it indicates this in the beacon and the vehicles follow suit.

4. Each vehicle checks and compares the information it receives through the sensors and from the communication network. If the information is consistent, it proceeds otherwise it raises a flag.

5. Other vehicles check the flagged car information and then decide to either keep the car in the platoon or remove it.

When communication between autonomous vehicles comes to mind people think of VANETs (vehicular ad-hoc networks). Although there are many benefits of VANETs, they have a drawback when it comes to scalability since each vehicle in VANETs is connected to all other vehicles and there are $n^2$ connections required for $n$ vehicles. Each vehicle in the single platoon model is connected directly to the vehicle ahead, behind and to the lead vehicle (since each vehicle mimics the lead vehicle) which reduces the number of

connections from $n$ to 3. Each platoon has a lead vehicle and all the lead vehicles of the platoon are connected. In this way, all the vehicles stay connected and the scalability problem is reduced.

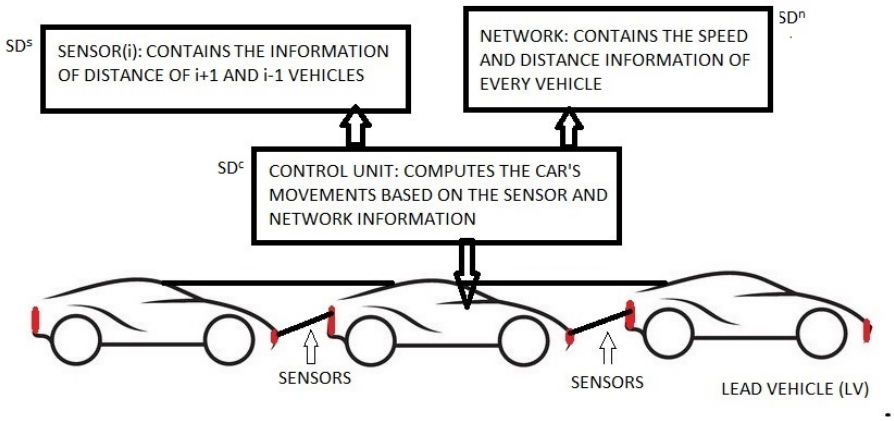


Figure 2.1. Information transfer

This cyber-physical system consists of a computer such as the control unit and a physical system, which in our case is the car. Information flows between different security domains. The security domain can be labeled as “secure” or “non secure”. Our model includes the following :

1. Communication network

   Our model can use any wireless networking technology as its basis, the most prominent of which are short-range radio technologies like WLAN (either standard Wi-Fi and ZigBee). In addition, cellular technologies or LTE can be used. In the United States, the IEEE 1609 WAVE (Wireless Access in Vehicular Environments) protocol stack builds on IEEE 802.11p WLAN operating 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 only a single radio), security, and

lightweight application layer protocols. Within the IEEE Communications Society, there is a technical subcommittee on Vehicular Networks and Telematics Applications (VNTA). A control unit captures this information. Beacon messages are passed on this network

2. Sensors

Velodyne LiDAR sensors are designed for obstacle detection and navigation of autonomous ground vehicles and marine vessels. Its durability, 360 field of view and very high data rate makes this sensor ideal for the most demanding perception applications as well as 3D mobile data collection and mapping applications. The HDL-64E's innovative laser array enables navigation and mapping systems to observe more of their environment than any other LiDAR sensor. The information received from the LiDAR would be sent to the control unit. RADAR sensors are devices used in advanced cruise control systems that can direct a vehicle's accelerator and braking systems, controlling the distance between it and another vehicle. The radar sensors note vital information such as range, angle and Doppler velocity. This information is used to determine the driving situation and warn the driver in potentially dangerous events. If the driver does not take appropriate action in time and a crash is about to happen, advanced radar systems can take control of the vehicle to avoid the crash or lessen the accident's severity. This high level of safety functionality is maintained in bad weather and no light, when driving conditions are at their worst.

Our model is independent of the sensor type. We only deal with the information that the sensor gives, we assume both give us accurate readings.

3. Control Unit

   This is the brain of the system and gives the vehicle directions. Based on the inputs it receives from various sources, the control unit makes decisions. If discrepancy in information path is detected, the control unit would alert other vehicles by sending special-purpose messages. Special-purpose messages are messages sent out to address specific issues.

4. Monitor

   We will be using the invariant equation distance=speed $\star$ time($t$) to make a calculation of where the vehicle might be at time t. An invariant is defined as a function, quantity, or property that remains unchanged when a specified transformation is applied. The assumption is that the car would have its own speed calculation mechanism like the speedometer and a clock that would give the time. At each instance, a monitor would be able to compute the distance information and send it to the control unit. The monitor uses a checker to evaluate each information source with another to see if they match. This will be further explained in detail in the case studies.

The messages (information regarding the speed and distance) are passed from the lead vehicle to the corresponding vehicles in the platoon in the form of beacons (messages that are transmitted in a network from one vehicle to another) as shown in Figure 2.1. Beacons contain information of the speed and distance of all the vehicles in front of the present vehicle. A control unit gathers information directly from sensors and also from the communication network that exist between the vehicles.

# 3. RELATED WORK ON SECURITY

Various security threats from this project arise such as integrity (attacker could change the information in a beacon), confidentiality (attacker could track the car's identity) and availability (attacker could jam the network used for communicating the distance and speed information). "Attacker" here is defined as someone/something that does not have authorization to access or modify the car or the components in the system but is able to modify it. The attacker could do the above attacks to demand money from the owner of a vehicle, to cause a traffic block or to cause a crash. Some of the devices such as the distance sensor or the camera, are exposed to the outside environment, so damage to these entities due to environmental or traffic conditions can cause the devices to malfunction. Many ideas were proposed to tackle the problem of security.

## 3.1. PRIVACY

Many works involved securing the entity itself. In [1], Ulrich Lang and Rudolf Schreiner have tried to use separate access control to prohibit change in the control statements of the car. They have divided each section on the control board and restricted the information flow based on the type of control it pertains to. They have only worked on preserving the privacy of the vehicle. They presented a list of security requirements to be enforced in ICSI (improved cooperative sensing for improved traffic efficiency), the protection of the ICSI system itself, the application data, and the user privacy. The privacy protection of vehicles has been worked on as shown in [4]. Here the idea of a virtual trip

lane (VTL) was used. By using VTL the location and speed reports can be regulated. Based on these reports, the estimated time of $VTL_1$ is calculated when the vehicle enters from $VTL_1$ to $VTL_2$ and compared to the actual arrival time in $VTL_2$. They found that the idea of only releasing trajectory data within VTL zones helps protect privacy.

## 3.2. INTEGRITY

Work has also been done to secure the information by using encryption mechanisms as seen in [5], but that model was limited in that it only provided conditional privacy (i.e., only the entities involved know about the communication). Recently cyber attacks on the vehicles were reported. These were done on a Jeep on prior notice to the drivers [6]. They took control of the ECU(Engine Control Unit), which sends out command to components in the car. They were able to kill the brakes, steer the vehicle, and control the horn and parking lights of the car.

There have been many other famous attacks. These have been done via access directly to the computer's hardware or through a wireless channel. Some of the cases are discussed below. In terms of hardware, the main idea of any attacker is to get into the CAN[1] of the vehicle through which they would be able to control the car. The vulnerabilities of the CAN are discussed in [7]. CAN packets contain no authentication fields or even any source identifier fields, meaning that any component can indistinguishably send a packet to any other component. This means that any single compromised component can be used to

[1]Controller Area Network-is a vehicle bus standard designed to allow micro-controllers and devices to communicate with each other in applications without a host computer

control all of the other components on that bus. The researchers suggested that by sending malicious data through broadcast from the infected CAN will make them take charge of the car. The researchers were able to spoof the data of speed.

The researchers in [7] have worked on wireless access which is discussed in [8]. Through the use of Bluetooth and reverse engineering they were able to gain access to the ECU. Once access is made, the attacker can make changes to the braking system, and modify the speed. Another recent attack was made on a Tesla S model by researchers from Keen Security Lab, they too were able to connect to the CAN of the vehicle wireless. The basic fault comes when the driver connects to a malicious WiFi hotspot nearby. The researchers in [9] were able to devise an alternate solution for message authentication by using ECDSA with omission techniques and TESLA++, but the problem of scalability still exists as each new vehicle has to be authenticated with every other vehicle in a group through an RSU (road side unit), although their work does reduce the authentication overhead when two groups would like to communicate. If the information is true, the vehicle is kept otherwise a special message is raised. The verification is performed by the ECU using the information from another vehicle.

### 3.3. AVAILABILITY

Blocking the availability of information is a serious problem in connected vehicles. Traditional techniques like beamforming (a technique of actively steering the beam of transmission and reception of a wireless communication system in such a way that useful signal reception is maximized while interfering signal reception is minimized), were used to avoid jamming attacks in the sensors [10]. A Sybil attack can be seen in connected

vehicles. A Sybil attack is one in which an attacker maliciously subverts the reputation system of a peer-to-peer network system 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. In [11] they have found an efficient way to detect this attack through methods that use less complex cryptography techniques and obtaining pseudonyms from RSU (road side units) at continuous intervals from a trusted source. Distinct RSUs that periodically collect reports from communicating vehicles regarding this neighborhood reduce the vulnerability.

In the long term, it is believed that the vehicles involved in the Sybil attack will give out similar information compared to the benign vehicles. The group of researchers in [12] tried to use a trust-based system to detect malicious vehicles. This was a very innovative approach where they used an iterative filtering algorithm to detect the malicious vehicles to address the problem of coalition. In their method, they could detect that vehicles which were trying to improve the trust rating of false vehicles. Another set of attacks that can be easily detected are denial of service (DOS) attacks. In [13] they take time intervals for listening on the channel and verifying if all the beacons have been received or not. If there is a beacon loss, then there should be at least two nodes involved in a collision within the same group, but to achieve this state they need to have an initialization phase. The outcome of the initialization phase is the sets of vehicle identifiers such as beacons from different sets never colliding with each other.

Attacks such as the one mentioned in [6], are difficult to detect and mitigate with only one car. The researchers in [4] used the estimated time traveled by each vehicle in each $VTL_1$, but we here take the real time data for computation. Therefore, if an attacker were to

know the position of a vehicle in a virtual trip zone, the attacker would be able to track the movement of the vehicle in real time. Attackers in [7][8] were able to spoof data coming from a communication network and the beacon. Cryptography was used to secure the messages between vehicles in [5] and [9]. Using the strongest encryption method is a good solution, but there is an assumption in cryptography that keys are exchanged securely before initiation of communication. In real-time cases such as cars it is not possible to securely share while the vehicles are in motion. The DOS (denial of service) attacks mentioned in [10] and [13] are based on reducing interference and listening to the channel periodically, but the problems arise when there are hazardous weather conditions making it difficult to listen to the channel.

Multiple Security Domain Nondeducibility (MSDND):

Nondeducibility (ND) was introduced by Sutherland [14] in an attempt to model infrastructures to secure information in a partitioned model. The partitions are grouped into two or more sets. These sets are usually labeled as high and low with all information restricted to one side of the partition or the other. Information that could not be determined from the other side of the domain is said to be nondeducibility secure. However, the partition must be absolute and it must be simplistic. Overlapping security domains present severe difficulties for Sutherland's Nondeducibility, as do information flows, which cannot be evaluated because the model lacks the required valuation functions. Let $V$ be the set of valuation functions such that $V^i_{s_x}(w)$ returns the value of state variable $s_x$ as seen by an entity $i$ in world $w$. For example, we have a control unit $c$ in our model which gets the distance information from say sensors $d_s$, then $V^c_{d_s}(w)$ will return the value true if it gets the information of distance from the sensor otherwise the value will be false.

**Definition 1** *A system is MSDND secure if there exists some world with a pair of states where one must be true and the other false (exclusive OR), but an entity i has no valuation function for those states. An entity within the security domain $SD^i$, i cannot know which state is true and which is false [15].*

$$MSDND(ES) = \exists w \in W \vdash \Box\, [\, (s_x \vee s_y)\,] \wedge \sim(s_x \wedge s_y) \wedge [\, w \models (\nexists V_x^i(w) \wedge \nexists V_y^i(w))\,]$$

*An equivalent formula is*

$$MSDND(ES) = \exists\, w \in W \vdash \Box\, [\, (s_x \oplus s_y)\,] \wedge [\, w \models (\nexists V_x^i(w) \wedge \nexists V_y^i(w))\,]$$

*Where $s_x$ and $s_y$ are states, $V_x^i$ and $V_y^i$ are the valuation functions of x in domain i and y on domain i and w is a world.*

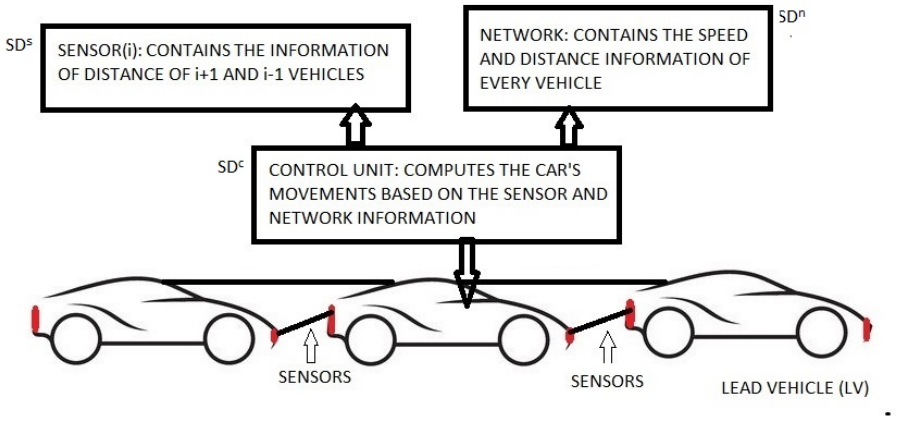


Figure 3.1. Security domains of information flow

# 4. PROBLEM STATEMENT

It is possible to devise an attack like a STUXNET attack [16] where the attacker changes the values of speed and distance, but the model needs to be able to tell if this kind of attack (change in the information of the sensor or network) is MSDND. If the attack is MSDND then it is good for the attacker as the model would not know which component is malfunctioning. Therefore, the model should be designed to eliminate attacks that are MSDND secure.

Figure 3.1 shows how the security domains are divided and also the interaction between the car and the communication points. There is a control unit in the car that computes the movement of the car. If there is a discrepancy in the distance information sent by one of the paths to the control unit, then the control unit would know that there is something wrong.

Below are the set of entities $c, s, n, ch$ that can be evaluated to determine the interactions between the car and the communication system. Here,

1. c: the control unit in the car (control unit gets the data and computes the movement accordingly) .

2. s: sensors (LiDAR) denoted by $s$ that gives distance value d(s).

3. n: communication network between the cars that gives network value d(n).

Table 4.1. Valuation function

| **Valuation** | **Result** |
|---|---|
| $V_c^c = s_0 \wedge T$ | "true" $\leftrightarrow$ Control unit is controlling the car |
| $V_{d_n}^c = s_1 \wedge T$ | "true" $\leftrightarrow$ Control unit gets input from networks |
| $V_{d_s}^c = s_2 \wedge T$ | "true" $\leftrightarrow$ Control unit gets input from sensors |
| $V_{ch}^c = s_3 \wedge T$ | "true" $\leftrightarrow$ Control unit gets result from checker |

4. ch: this is a computational unit inside the control unit that checks if the information received from the information paths is true. In this case, we have three checkers: $ch_1$(checks if d(n)=d(s)), $ch_2$(checks if d(s)=d(i)) and $ch_3$(checks if(d(i)=d(n)), where d(n), d(s) and d(i) are distance information received by the control unit from the network, sensor and invariant, respectively.

We also have d(c), which is the distance that the control unit accepts based on information received from the paths. On any given state, the valuation functions will return the value of the corresponding state variables as seen by the entity in control $c, s, n$.

The control unit will be able to detect a compromised information path if the information it receives from the sensor is not equal to the communication network. In other words it uses the result of $ch$. If it is false then the control unit would know that one of the information paths is compromised.

There are two information paths as seen in Figure 1.1, sensors and networks. For the following case, the vehicle has only one information path either sensor or network that gives the distance between itself and the car in front of it. This case shows how having one information path can make the system MSDND secure and also not MSDND secure.

## 4.1. WHEN THE CARS CONTAIN ONLY ONE INFORMATION PATH (NETWORK OR SENSOR)

**Case 1a:** Let us assume that the cars are connected only through a network, $n$ and the network is providing correct information under normal conditions, i.e., $d(n)= True$.

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

From the above statement,

MSDND (ES) = $\exists$ w $\epsilon$ W: w $\vdash$ $\Box$ (d(n)$\oplus\neg$d(n)) $\wedge$ [w $\models$ ($\exists$ $V^c_{d(n)}(w) \wedge \nexists$ $V^c_{\neg d(n)}(w)$)]

Hence, the system is not nondeducible secure to the control unit according to the definition since we have $\exists V^c_{d(n)}(w)$). In this case the goal of making the model non deducible secure is met.

**Case 1b:** Let us assume that the cars connected through a network, $n$ receive incorrect information( i.e., $\neg d(n)= True$). This is possible if an attacker is able to get into the system.

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

From the above statement,

MSDND (ES) = $\exists$ w $\epsilon$ W: w $\vdash$ $\Box$ (d(n)$\oplus\neg$d(n)) $\wedge$ [w $\models$ ($\nexists$ $V^c_{d(n)}(w) \wedge \nexists$ $V^c_{\neg d(n)}(w)$)]

Hence, the system is nondeducible secure to the control unit according to the definition. In this case the goal of making the model non deducible secure is not met.

**Case 1c:** Let us assume that the cars are connected only through $s$ where the sensor is providing correct information ( i.e., $d(s)= True$) under normal conditions.

1. w$\models$ ($\exists$ $V^{c}_{d(s)}$(w)) Control unit receives distance information from sensor.

From the above statement

MSDND (ES) = $\exists$ w $\epsilon$ W: w $\vdash$ $\Box$ (d(s)$\oplus\neg$d(s)) $\wedge$ [w $\models$ ($\exists$ $V^{c}_{d(s)}(w) \wedge \nexists$ $V^{c}_{\neg d(s)}(w)$)]

Hence, the system is not Nondeducible secure to the control unit according to the definition since we have $\exists V^{c}_{d(s)}(w)$. In this case the goal of making the model non deducible secure is met

**Case 1d:** Let us assume that the cars connected through $s$ receive incorrect information (i.e., $\neg d(s)= True$). This is possible if the attacker is able to get into the system.

1. w$\models$ ($\nexists$ $V^{c}_{\neg d(s)}$(w)) Control unit receives distance information from sensor.

From the above statement

MSDND (ES) = $\exists$ w $\epsilon$ W: w $\vdash$ $\Box$ (d(s)$\oplus\neg$d(s)) $\wedge$ [w $\models$ ($\nexists$ $V^{c}_{d(s)}(w) \wedge \nexists$ $V^{c}_{\neg d(s)}(w)$)]

Hence, the system is nondeducible secure to the control unit according to the definition. Similar to case 1b the goal is not met

Although making a model that is not Nondeducible secure is the goal, the control unit in cases 1b and 1d would believe the data and direct the vehicle. Thus, having no other information path to verify could be hazardous. So based on our initial observations we can conclude that having multiple information paths is an important criteria to make the model not Nondeducible secure.

## 4.2. WHEN THE CARS CONTAIN BOTH THE NETWORK AND SENSOR INFORMATION PATH

Now let us assume the cases where we have the sensor and communication network provide the distance information to the control unit. The control unit would receive the distance information and based on it would decide if the information provided is correct or not. The control unit would know that an information path is corrupted if there is a discrepancy in the information provided by the two paths.

**Case 2a:** If $n$ is faulty: someone has compromised the system. The attacker is able to manipulate the information and thus wrong information is received by the control unit from the network. Here, $\neg d(n) = True$ and $d(s) = True$.

1. w $\models$ ($\exists\ V^c_{d(s)}$(w)) Control unit receives information from the sensor
2. w$\models$ ($\nexists\ V^c_{\neg d(n)}$(w)) Control unit receives information from network
3. w$\models$ ($\exists V^c_{d(ch)}$) Information received from sensor and network do not match

From 3, the control unit would know that an information path has been compromised.

By combining above statements 1 and 2 we get

MSDND (ES) = $\exists$ w $\epsilon$ W:w $\vdash$ $\Box$($\neg$ d(n)$\oplus$ch)$\wedge$[w $\models$($\exists\ V^c_{d(ch)}(w)\wedge\nexists\ V^c_{\neg d(ch)}$(w))]

Hence, the system is not nondeducible to the control unit because the control unit can deduce that something is going wrong, but cannot determine exactly which information path. An extra information path is needed to indicate which path is responsible for the incorrect data being transmitted.

Table 4.2. State description

| $\phi_i$ | **state** | **description** |
|---|---|---|
| $\phi_0$ | $\sigma_0$ | Control unit is controlling the car |
| $\phi_1$ | $\sigma_1$ | Control unit gets input from networks |
| $\phi_2$ | $\sigma_2$ | Control unit gets input from sensors |
| $\phi_3$ | $\sigma_3$ | Control unit gets input from $invariant_{dist}$ |
| $\phi_4$ | $\sigma_4$ | Control unit gets result from $ch_1$ |
| $\phi_5$ | $\sigma_5$ | Control unit gets result from $ch_2$ |
| $\phi_6$ | $\sigma_6$ | Control unit gets result from $ch_3$ |
| $S_u$ | $uncompromised = T$ | $uncompromised = \phi_4 \wedge \phi_5 \wedge \phi_6$ |
| $S_h$ | $compromised = T$ | $compromised = \neg\phi_4 \vee \neg\phi_5 \vee \neg\phi_6$ |

**Case 2b:** If $s$ is faulty: someone has compromised the system. The attacker is able to manipulate the information, and hence wrong information is received by the control unit from network. Here ¬d(s)=True and $d(n) = True$

1. w $\models$ ($\nexists V^c_{\neg d(s)}$(w)) Control unit receives information from the sensor

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

3. w$\models \exists V_{ch_1}$ Information received from sensor and network do not match.

From 3, the control unit would know that an information path has been compromised.

By combining above statements 1 and 2 we get,

MSDND (ES) = $\exists$ w$\epsilon$ W:w $\vdash \Box$ (¬ d(s)$\oplus$ch)$\wedge$ [w$\models$($\exists V^c_{d(ch)}(w) \wedge \nexists\ V^c_{\neg d(s)}$(w))].

Therefore, the system is not nondeducible to the control unit because the control unit can deduce that something is going wrong, but cannot determine exactly which information path is responsible for the incorrect data being transmitted.

Now if we consider the other components in the car like the invariant, we can model the MSDND model as the following as shown in Figure 4.1:

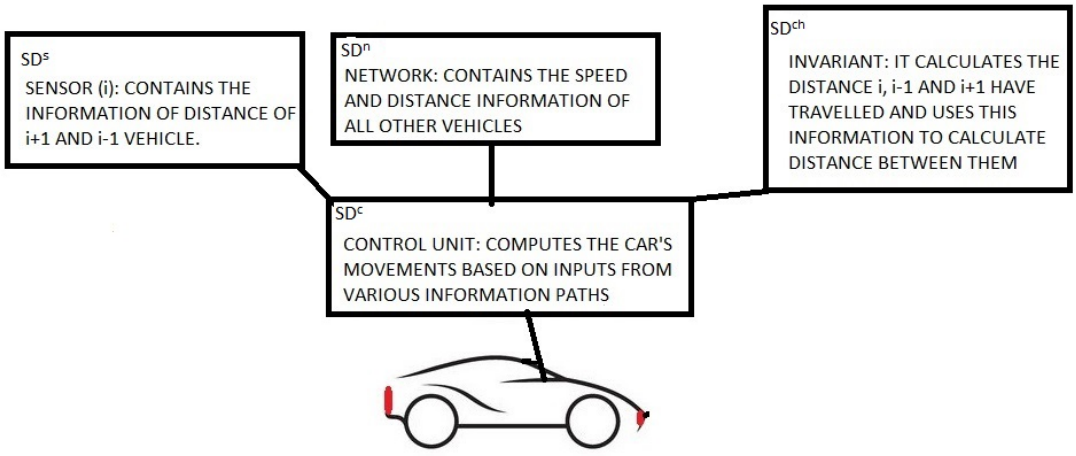


Figure 4.1. Invariant model
Here, there are 3 information paths- sensors, networks, and invariant

1. c: the control unit in the car (the control unit gets the data and computes the movement accordingly)

2. Distance estimators: sensors (LiDAR) denoted by $s$ that give the value of d(s).

3. n: communication network $n$ between the cars that gives the value of d(n).

4. $invariant_{dist}$(d(i)): distance=speed$\star$time; Every car would have its own speedometer through which it can calculate the distance it has traveled in a period of time.

5. ch: this is a computational unit inside the control unit that checks if the information received from the information paths is true. In this case, we have three checkers: $ch_1$(checks if d(n)=d(s)), $ch_2$(checks if d(s)=d(i)) and $ch_3$(checks if(d(i)=d(n)), where d(n), d(s) and d(i) are distance information received by control unit from the network, sensor and invariant, respectively.

Based on our model, the three sources providing distance information are the following:

$$d_{t2} = \begin{cases} range\ calculated\ by\ LIDAR/RADAR - d_{t1}(s) \\ speed * time - d_{t1}(i) \\ distance\ calculated\ through\ network - d_{t1}(n) \end{cases} \tag{4.1}$$

sensors vs invariant: We assume that that vehicles are driving at constant velocity. At time $1s$ let us say a sensor has given d(s) as $5m$ and at that point of time the vehicle is at $30m/sec$. Since there is no change of speed at time $5s$ in the vehicle then sensor should report d(s) as $5m$. If any other information is given, then we would know that the sensor has been compromised.

network vs invariant: The network periodically updates the information of speed as shown in Figure 4.3, location and other relevant information of the vehicle. Now if at time $t_1$ the network gives a certain location of the vehicle $V_{i+1}$ and at $t_2$ the network gives a certain location of $V_{i+1}$ Based on this information $V_i$ can calculate the distance moved by $V_{i+1}$. It also has the speed it traveled during this time and can calculate the distance. If there is any discrepancy in information then we would know that the network has been compromised. The control unit would have the correct distance information if there exists a valuation function for any one of the $ch_1, ch_2 or ch_3$.

## 4.3. WHEN THE CARS HAVE AN ADDITIONAL INVARIANT ADDED AS A SECURITY DOMAIN

Let us now add another information path (invariant) to the model. This additional information will help us in making the model not MSDND secure. The control unit would also have the correct distance information if there exists a valuation function for any one of the $ch_1, ch_2$ or $ch_3$ and in this way can indicate which path is compromised.

**Case 3a:** $n$ is faulty ,i.e., $\neg d(n) = True$:

1. w $\models$ ($\nexists$ $V^c_{\neg d(n)}$(w)) Control unit receives information from the network.
2. w $\models$ ($\exists$ $V^c_{d(s)}$(w)) Control unit receives information from the distance estimators.
3. w $\models$ ($\exists$ $V^c_{d(i)}$(w)) Control unit receives information from $invariant_{dist}$.
4. w$\models$ $\nexists V^c_{ch_1}$.
5. w$\models$ $\exists V^c_{ch_2}$.
6. w$\models$ $\nexists V^c_{ch_3}$.

   From 5 we get

7. w$\models$$\exists V^c_{d(c)}(w)$.

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

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

**Case 3b:** Let us now consider that the sensor is faulty. The control unit receives incorrect information from the sensor, $s$ is faulty, i.e., $\neg d(s) = True$.

1. w $\models (\exists\, V^{c}_{d(n)}(\mathrm{w}))$ Control unit receives information from the network.

2. w $\models (\nexists\, V^{c}_{\neg d(s)}(\mathrm{w}))$ Control unit receives information from the distance estimators.

3. w $\models (\exists\, V^{c}_{d(i)}(\mathrm{w}))$ Control unit receives information from the $invariant_{dist}$.

4. w$\models \nexists V^{c}_{ch_1}$.

5. w$\models \nexists V^{c}_{ch_2}$.

6. w$\models \exists V^{c}_{ch_3}$.

MSDND (ES) = $\exists$ w $\epsilon$ W:w $\vdash \Box(\neg$ d(s)$\oplus ch_3 \wedge$[w $\models (\exists V^{c}_{d(ch_3)}(w) \wedge \nexists\, V^{c}_{\neg d(s)}(\mathrm{w}))]$

Therefore it is not nondeducible secure because the control unit can deduce that something is going wrong and determine that distance estimators are responsible for the incorrect data being transmitted.

We have assumed that the invariant is always true and that the information about the speed is unaltered, but in [6] they can also change the information received to the control unit. If such a case arises then we would have the other two components, sensor and network, correctly give us the information as shown in case 3c.

**Case 3c:** $i$ is faulty, i.e., $\neg d(i) = True$.

1. w $\models (\exists\, V^{c}_{d(n)}(\mathrm{w}))$ Control unit receives information from the network.

2. w $\models (\exists\, V^{c}_{\neg d(s)}(\mathrm{w}))$ Control unit receives information from the distance estimators.

3. w $\models (\nexists\, V^{c}_{d(i)}(\mathrm{w}))$ Control unit receives information from the $invariant_{dist}$.

4. w$\models \exists V^{c}_{ch_1}$.

5. w$\models \nexists V^{c}_{ch_2}$.

6. w$\models \nexists V^{c}_{ch_3}$.

MSDND (ES) = $\exists$ w $\epsilon$ W:w $\vdash \Box(\neg$ d(i)$\oplus ch_1 \wedge$[w $\models(\exists V^{c}_{d(ch_1)}(w) \wedge \nexists V^{c}_{\neg d(i)}$(w))]

Therefore it is not nondeducible secure because the control unit can deduce that something is going wrong and determine that invariance is responsible for the incorrect data being transmitted.

## 4.4. PLATOON

Let us consider we have different cars in a platoon and also that, there are various platoons in a vehicle as seen in Figure 4.4. Now the following are sources of information:

1. s: sensors (LiDAR) that give distance value d(s).

2. n: communication network between the cars that gives network value d(n).

3. $Invariant_1$: distance=speed$\star$time which gives the value of $d(invariant_i)$; every car would have its own speedometer through which it could calculate the distance it has traveled in a period of time

4. $InfoSourceValidator(ISV)$: This is similar to an array data type that stores the True/False result after comparing the distance reported by each information source with another as shown in Figure 4.2. If there are more true values reported than false, then the valuation function for ISV exists.

5. $invariant_2$- As shown in Figure 4.4, communication can be made between two platoons. In this case, the A, B and P form an information path, since each car is equipped with the proximity sensors. $V_P$ has information of $\{x, y\}$. Similarly, $V_A$ has information of $\{x, z_A\}$ and $V_P$ has information of $\{y, z_B\}$. Now we would send back this information to $V_A$ and $V_B$ and $V_A$ will have information of $\{x, z_A, z_B\}$. If $z_A$ is not equal to $z_B$, then no valuation function exists for $invariant_2$; otherwise, it exists.

6. $beacon_i$: it gives information of $speed_i$ and $velocity_i$ of vehicle i in the platoon.

| | |
|---|---|
| $ch_1$ | d(s)=d(invariant$_1$) |
| $ch_2$ | d(s)=d(n) |
| $ch_3$ | d(s)=d(invariant$_2$) |
| $ch_4$ | d(s)=d(beacon$_1$) |
| $ch_5$ | d(n)=d(invariant$_2$) |
| $ch_6$ | d(n)=d(beacon$_1$) |
| . . . . | . . . . |
| $ch_y$ | d(y)=d(x) |

Figure 4.2. InfoSourceValidator ($ISV$)
follows an enumeration of checking sources against both other sources and invariants combining multiple source

**4.4.1. Single Platoon.** Let us assume that no other platoon exists nearby and there are multiple vehicles in a single platoon. We would now have communication from other cars. The cars would communicate with each other using a beacon. The beacon would now

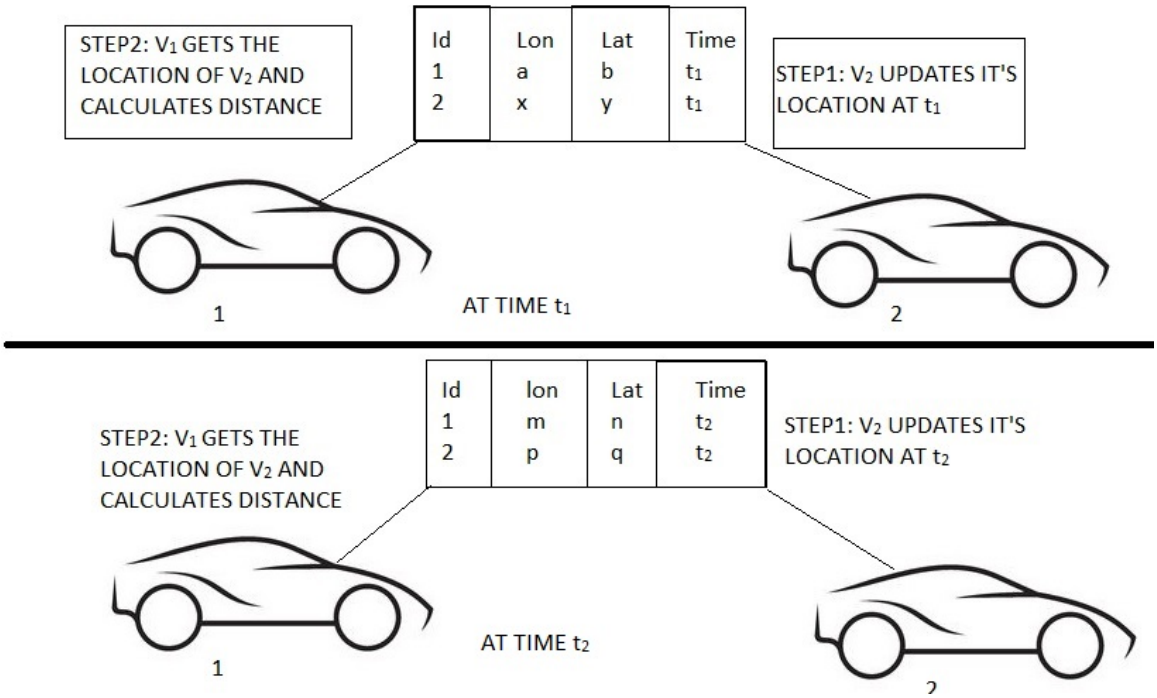


Figure 4.3. Network vs invariant

The vehicles can calculate the distance covered in $t_1 - t_2$ interval using the latitude(lat) and longitude (lon) coordinates as well as by using the equation distance= speed*time

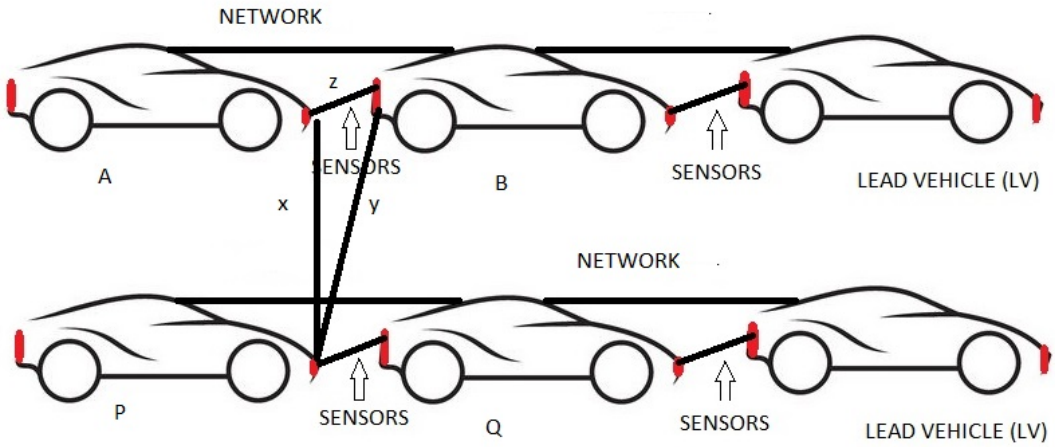


Figure 4.4. Multiple platoons

be another information path to the control unit and would help in detecting vulnerable path.

**Case 4:** Let us see if our model will be able to detect if a car is giving wrong information.

The beacon is giving incorrect information (i.e., ¬beacon=True).

Table 4.3. State description when invariant is added

| $\phi_i$ | **state** | **description** |
|---|---|---|
| $\phi_0$ | $\sigma_0$ | Control unit is controlling the car |
| $\phi_1$ | $\sigma_1$ | Control unit accepts command from networks |
| $\phi_2$ | $\sigma_2$ | Control unit accepts command from sensors |
| $\phi_3$ | $\sigma_3$ | Control unit accepts command from $invariant_1$ |
| $\phi_4$ | $\sigma_4$ | Control unit accepts command from beacon |
| $\phi_5$ | $\sigma_5$ | Control unit accepts command from $invariant_2$ |
| $\phi_6$ | $\sigma_5$ | Control unit gets result from $ISV$ |

1. w $\models$ ($\exists$ $V^c_{d(n)}$) Control unit accepts command from network.

2. w $\models$ ($\exists$ $V^c_{d(s)}$) Control unit accepts command from sensors.

3. w $\models$ ($\exists$ $V^c_{invariant_1}$) Control unit receives information from $invariant_1$.

4. w $\models$ ($\nexists$ $V^c_{beacon_i}$) Control unit receives information from beacon.

   From 1, 2, 3 we get

5. w$\models$ $\exists V^c_{ISV}$.

   From 5 we get,

6. w$\models$$\exists V^c_{d(c)}(w)$

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

Therefore, it is not nondeducible secure because the control unit can deduce that something is going wrong and determine that the $beacon_i$ is responsible for the incorrect data being transmitted. In this way, we would be able to detect if a vehicle in the platoon has been compromised.

Let us now look at the case where there are multiple platoons as shown in Figure 4.4. Here we have an information path from the adjacent platoons. These information paths help us in detecting an incorrect data path if more than one information path is compromised.

**4.4.2. Multiple Platoon.** As shown in Figure 4.4 let us consider that there are more than one platoon.

**Case 5a:** There are different platoons, and each platoon has some number of vehicles and $\neg beacon_i = True$.

1. w $\models (\exists\ V^c_{d(n)})$ Control unit accepts command from network.
2. w $\models (\exists\ V^c_{d(s)})$ Control unit accepts command from sensors.
3. w $\models (\exists\ V^c_{invariant_1})$ Control unit receives information from $invariant_1$.
4. w $\models (\nexists\ V^c_{beacon_i})$ Control unit accepts information from beacon.
5. w $\models (\exists\ V^c_{invariant_2})$ Control unit receives information from $invariant_2$.

   From 1, 2, 3, 5 we get

6. w$\models \exists V^c_{d(c)}(w)$

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

Therefore, it is not nondeducible secure because the control unit can deduce that something is going wrong and determine that the $beacon_i$ is responsible for the incorrect data being transmitted.

**Case 5b:** Let us consider that there are two paths that are compromised. For this case let us assume that the sensor ($\neg d(s) = true$) and the beacon ($\neg beacon_i = True$) are compromised.

1. w $\models (\exists\, V^{c}_{d(n)})$ Control unit accepts command from network.

2. w $\models (\nexists\, V^{c}_{d(s)})$ Control unit accepts command from sensors.

3. w $\models (\exists\, V^{c}_{invariant_1})$ Control unit receives information from $invariant_1$.

4. w $\models (\nexists\, V^{c}_{beacon_i})$ Control unit accepts information from beacon.

5. w $\models (\exists\, V^{c}_{invariant_2})$ Control unit receives information from $invariant_2$.

   From 1, 3, 5 we get

6. w$\models \exists V^{c}_{d(c)}(w)$

MSDND (ES) = $\exists$w$\epsilon$W:w $\vdash \Box\ (\neg beacon_i \oplus invariant_2) \wedge$[w$\models (\exists V^{c}_{d(c)}(w) \wedge \nexists V^{c}_{\neg d(c)}$(w))]

MSDND (ES) = $\exists$w$\epsilon$W:w $\vdash \Box\ (\neg d(s) \oplus invariant_2) \wedge$[w$\models (\exists V^{c}_{d(c)}(w) \wedge \nexists V^{c}_{\neg d(c)}$(w))]

Therefore, it is not nondeducible secure because the valuation function $\exists V^{c}_{d(c)}(w)$ exists.

In this way, we would be able to use the information from other platoons. This study tries to consider as many information paths as possible to detect the compromised information path. Platoons are considered to detect if a vehicle has been compromised because Case 4 was able to detect the compromised vehicle without a platoon, but if there are other sources that are compromised, then having this additional source could be helpful in detecting an attack.

**4.4.3. Multiple Platoons With Lane Angle Detection.** Now, let us assume that the model has an additional feature of being able to calculate the angle at which each vehicle is located. We can use techniques as discussed in [17]. These help in obtaining the angle

information and we can use the equation $c^2 = a^2 + b^2 - 2abCos\theta$.

From Figure 4.5:

$$invariant_{ang}(\theta) = \theta_1 + \theta_2 \tag{4.2}$$

$$c^2 = a^2 + b^2 - 2abCos\theta \tag{4.3}$$

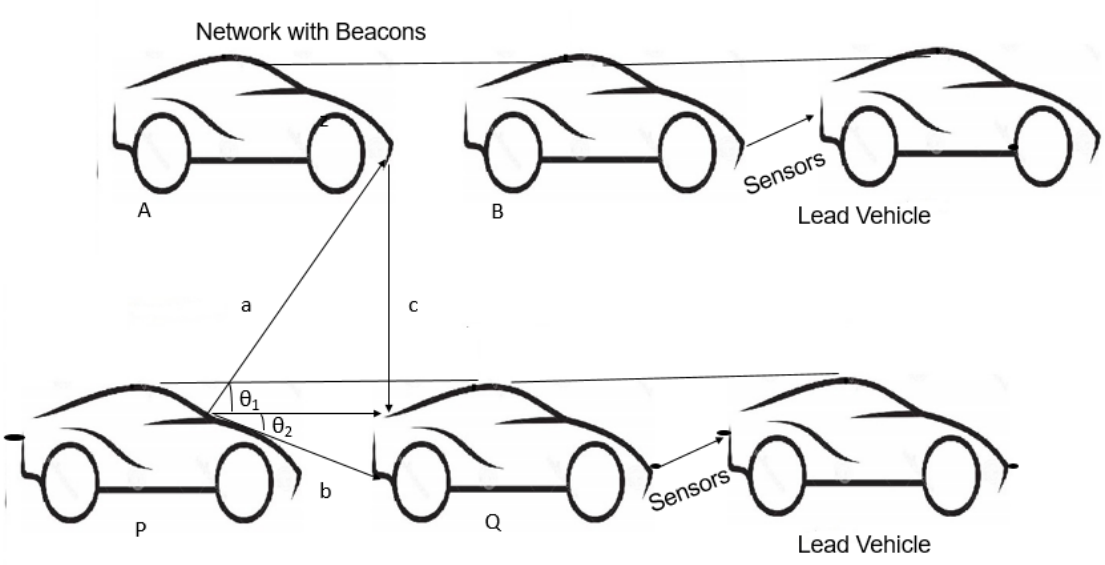


Figure 4.5. Detecting the angle

As shown in Figure 4.5, $V_P$ can calculate the distance between $V_A$ and $V_Q$ using the above information . By using this information vehicle $V_P$ can verify against the information sent to it by $V_A$ and $V_Q$ and by the information stored in the communication network.

**Case 5c:** Let us assume that the information sent out by vehicle $V_Q$ is faulty (i.e., $\neg beacon_{V_Q} = True$)

1. w $\models$ ($\exists$ $V^c_{invariant_{ang_A}}$) Control unit of vehicle $V_P$ receives the angle information of vehicle $V_A$.

2. w $\models$ ($\exists$ $V^{c}_{invariant_{ang_Q}}$) Control unit of vehicle $V_P$ receives the angle information of vehicle $V_Q$.

3. w $\models$ ($\exists$ $V^{c}_{d(s)_A}$) Control unit receives distance information of vehicle $V_A$.

4. w $\models$ ($\exists$ $V^{c}_{d(s)_Q}$) Control unit receives distance information of vehicle $V_Q$.

5. w $\models$ ($\nexists$ $V^{c}_{beacon_{V_Q}}$) Control unit receives distance information of $beacon_{V_Q}$.

   From 1, 2, 3, 4

6. w$\models\exists V^{c}_{invariant_{ang}}(w)$

   From 6

7. w$\models\exists V^{c}_{d(c)}(w)$

MSDND(ES) = $\exists$wϵW:w $\vdash\Box$ ($\neg beacon_{V_Q} \oplus invariant_{ang}$)$\wedge$[w$\models$($\exists V^{c}_{d(c)}(w) \wedge \nexists V^{c}_{\neg d(c)}$(w))]

**Case 5d:** Let us assume that there is a fault in the communication network, i.e., $\neg d(n) = True$

1. w $\models$ ($\exists$ $V^{c}_{invariant_{ang_A}}$) Control unit of vehicle $V_P$ receives the angle information of vehicle $V_A$.

2. w $\models$ ($\exists$ $V^{c}_{invariant_{ang_Q}}$) Control unit of vehicle $V_P$ receives the angle information of vehicle $V_Q$.

3. w $\models$ ($\exists$ $V^{c}_{d(s)_A}$) Control unit receives distance information of vehicle $V_A$.

4. w $\models$ ($\exists$ $V^{c}_{d(s)_Q}$) Control unit receives distance information of vehicle $V_Q$.

5. w $\models (\nexists V^c_{d(n)_Q})$ Control unit receives distance information of vehicle $V_Q$ from network.

   From 1, 2, 3, 4

6. w$\models \exists V^c_{invariant_{ang}}(w)$

   From 6

7. w$\models \exists V^c_{d(c)}(w)$

MSDND(ES) = $\exists$w$\epsilon$W:w $\vdash \Box$ $(\neg V^c_{d(n)_Q} \oplus invariant_{ang}) \wedge$[w$\models (\exists V^c_{d(c)}(w) \wedge \nexists V^c_{\neg d(c)}$(w))]

Therefore, it is not nondeducible secure because the control unit can deduce that something is going wrong and determine that the $V^c_{d(n)_Q}$ is responsible for the incorrect data being transmitted.

The total number of information paths in Figure 4.5 is six. These are

1. Sensor
2. Network
3. $beacon_i$
4. $invariant_1$ which computes the distance travelled by the vehicle using $distance = speed * time$
5. $invariant_2$ which uses the distance sensors of the vehicles nearby as seen in Figure 4.4.
6. $invariant_3$ which uses the angle between vehicles to compute the distance as seen in Figure 4.5

We have seen cases where the attacker is able to modify less than half the number of information paths.

**4.4.4. Attacker Is Able To Modify Three Information Paths.** Let us now look at cases where the attacker is able to manipulate three information paths. Since this attack compromises three information paths, two case scenarios arise.

1. Attacker can change the value of these three paths to the same incorrect information(easy to detect as shown in **Case 6a**)

2. Attacker can change the value of these three paths(difficult to detect as shown in **Case 6b**)

For the following two cases we can consider any three paths to be compromised. Let us name the compromised information paths as $compinfo_1$, $compinfo_2$, $compinfo_3$ and the three correct information paths as $path_1$, $path_2$, $path_3$.

**Case 6a**: Let us assume that the three compromised paths have different values.

1. w $\models (\exists\, V^c_{path_1})$ Control unit accepts information from path 1.

2. w $\models (\exists\, V^c_{path_2})$ Control unit accepts information from path 2.

3. w $\models (\exists\, V^c_{path_3})$ Control unit accepts information from path 3.

4. w $\models (\nexists\, V^c_{compinfo_1})$ Control unit accepts information from compromised information path 1

5. w $\models (\nexists\, V^c_{compinfo_2})$ Control unit accepts information from compromised information path 2

6. w $\models (\nexists V^{c}_{compinfo_3})$ Control unit accepts information from compromised information path 3

   From 1, 2, 3

7. w$\models \exists V^{c}_{d(c)}(w)$

MSDND (ES) = $\exists$ w $\epsilon$ W: w $\vdash \Box$ (d(c)$\oplus\neg$d(c)) $\wedge$ [w $\models (\exists V^{c}_{d(c)}(w) \wedge \nexists V^{c}_{\neg d(c)}(w))$]

Therefore, it is not Nondeducible secure because the control unit can deduce that something is going wrong and can also determine the information path responsible for the attack.

**Case 6b**: Let us assume that the three compromised paths have similar values.

1. w $\models (\exists V^{c}_{path_1})$ Control unit accepts information from path 1.
2. w $\models (\exists V^{c}_{path_2})$ Control unit accepts information from path 2.
3. w $\models (\exists V^{c}_{path_3})$ Control unit accepts information from path 3.
4. w $\models (\nexists V^{c}_{compinfo_1})$ Control unit accepts information from compromised information path 1
5. w $\models (\nexists V^{c}_{compinfo_2})$ Control unit accepts information from compromised information path 2
6. w $\models (\nexists V^{c}_{compinfo_3})$ Control unit accepts information from compromised information path 3

   From 1, 2, 3

Table 4.4. MSDND analysis results for a single car

| Case | Information Path | MSDND | Vehicle Status |
|---|---|---|---|
| 1a | $d(n)$ is not compromised | No | Secure |
| 1b | $d(n)$ is compromised | Yes | Not Secure |
| 1c | $d(s)$ is not compromised | No | Secure |
| 1d | $d(s)$ is compromised | Yes | Not Secure |
| 2a | $d(n)$ is compromised | No | Secure |
| 2b | $d(s)$ is compromised | No | Secure |
| 3a | $d(n)$ is compromised | No | Secure |
| 3b | $d(s)$ is compromised | No | Secure |
| 3c | $d(i)$ is compromised | No | Secure |

Table 4.5. MSDND analysis results for platoon

| Case | Information Path | MSDND | Vehicle Status |
|---|---|---|---|
| 4 | $beacon_i$ is compromised | No | Secure |
| 5a | $beacon_i$ is compromised | No | Secure |
| 5b | $d(s)$ is compromised | No | Secure |

Table 4.6. MSDND analysis results for multiple platoons

| Case | Information Path | MSDND | Vehicle Status |
|---|---|---|---|
| 5c | $beacon_i$ is compromised | No | Secure |
| 5b | $d(n)$ is compromised | No | Secure |

7. w$\models \exists V^c_{d(c)_1}(w)$

   From 4, 5, 6

8. w$\models \exists V^c_{d(c)_2}(w)$

MSDND (ES) = $\exists$ w $\epsilon$ W: w $\vdash \Box$ (d(c)$_1 \oplus \neg$d(c)$_1) \wedge$ [w $\models (\exists\, V^c_{d(c)_1}(w) \wedge \nexists\, V^c_{\neg d(c)_1}(w))$]

MSDND (ES) = $\exists$ w $\epsilon$ W: w $\vdash \Box$ (d(c)$_2 \oplus \neg$d(c)$_2) \wedge$ [w $\models (\exists\, V^c_{d(c)_2}(w) \wedge \nexists\, V^c_{\neg d(c)_2}(w))$]

Therefore, it is not nondeducible secure because the control unit can deduce that something is going wrong, but cannot decide which set of information paths are compromised.

Table 4.7. MSDND analysis results for multiple platoons where three paths are compromised

| Case | Information Path | MSDND | Vehicle Status |
|---|---|---|---|
| 6a | Compromised paths giving different values | No | Secure |
| 6b | Compromised paths giving same values | No | Secure |

# 5. FUTURE WORK

The main focus of this thesis is on securing the connected vehicles and platoons of connected vehicles. Minimizing the number of assumptions would be our first step ahead. We also need to handle cases where more than half of the information sources are compromised. We will try looking into cases where two sets of information sources give the same set of incorrect information. There are many scenarios to be considered, such as: lane changing, platoon joining and platoon split. There is currently no technology to simulate them in a real scenario: We can only look at case scenarios and validate if the mathematical model would work.

# 6. CONCLUSION

MSDND is useful to model attacks where the goal is to hide critical information from an attacker rather than to steal information. MSDND secure is bad for the system and good for the attacker because information can be hidden by making it impossible to evaluate the desired question or the actual valuation function can be falsified to produce an invalid valuation, thus making the information MSDND secure and undetectable.

A model that has fewer number of states where MSDND secure is possible is a good cyber-physical system. In our model, most of the cases are not MSDND secure which makes our CPS a good model. We can also observe that if we have more information paths such as the invariant and beacon, detecting an attack is easy.

As we have seen, the invariant plays an important role when the regular information paths such as sensors, networks and beacon are compromised. We have three invariant equations:

1. $distance = speed * time$
2. $c = a^2 + b^2 + abCos\theta$
3. $invariant_2$ as discussed in section 4.

We have also shown how the model is efficient in various scenarios and how this model handles the various security threats as discussed in section 3. The attacker now has to corrupt multiple information paths to compromise the system but then too we have shown a case where other information paths can be used to indicate which path is compromised.

No system is 100 percent secure and in this research work, the model fails if we have more than $n/2$ compromised paths where $n$ is the total number of information paths. We have also assumed that the invariant is always true but for some models the invariant equation may have variables that are computed based on components of the model. We have tried to make a model that is difficult to attack and tried to develop a security model in such a way that it provides more security and resilience against attackers.

# BIBLIOGRAPHY

[1] Ulrich Lang and Rudolf Schreiner. Managing security in intelligent transport systems. In *Proceedings of the 2015 IEEE 18th International Conference on Intelligent Transportation Systems*, ITSC '15, pages 48–53, Washington, DC, USA, 2015. IEEE Computer Society.

[2] S. E. Shladover. The california path program of ivhs research and its approach to vehicle-highway automation. In *Intelligent Vehicles '92 Symposium., Proceedings of the*, pages 347–352, Jun 1992.

[3] A. Wasef and X. Shen. Ppgcv: Privacy preserving group communications protocol for vehicular ad hoc networks. In *2008 IEEE International Conference on Communications*, pages 1458–1463, May 2008.

[4] Z. Sun, B. Zan, J. Ban, M. Gruteser, and P. Hao. Evaluation of privacy preserving algorithms using traffic knowledge based adversary models. In *2011 14th International IEEE Conference on Intelligent Transportation Systems (ITSC)*, pages 1075–1082, Oct 2011.

[5] 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*, 12(3):736–746, Sept 2011.

[6] Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. *in DefCon*, Aug 2015.

[7] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage. Experimental security analysis of a modern automobile. In *2010 IEEE Symposium on Security and Privacy*, pages 447–462, May 2010.

[8] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11, pages 6–6, Berkeley, CA, USA, 2011. USENIX Association.

[9] Y. J. Abueh and H. Liu. Message authentication in driverless cars. In *2016 IEEE Symposium on Technologies for Homeland Security (HST)*, pages 1–6, May 2016.

[10] G. Patounas, Y. Zhang, and S. Gjessing. Evaluating defence schemes against jamming in vehicle platoon networks. In *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, pages 2153–2158, Sept 2015.

[11] M. A. Mutaz, L. Malott, and S. Chellappan. Leveraging platoon dispersion for sybil detection in vehicular networks. In *Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on*, pages 340–347, July 2013.

[12] 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*, PP(99):1–1, 2016.

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

[14] D. Sutherland. A model of information. In *Proceedings of the 9th National Computer Security Conference, DTIC Document*, pages 175–183, Sept 1986.

[15] G. Howser and B. McMillin. A multiple security domain model of a drive-by-wire system. In *Computer Software and Applications Conference (COMPSAC), 2013 IEEE 37th Annual*, pages 369–374, July 2013.

[16] G. Howser and B. McMillin. A modal model of stuxnet attacks on cyber-physical systems: A matter of trust. In *Software Security and Reliability (SERE), 2014 Eighth International Conference on*, pages 225–234, June 2014.

[17] J. M. Dai, L. T. Wu, H. Y. Lin, and W. L. Tai. A driving assistance system with vision based vehicle detection techniques. In *2016 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA)*, pages 1–9, Dec 2016.

# VITA

Uday Ganesh Kanteti was born in Visakhapatnam, India. He earned a Bachelors of Technology from Anil Neerukonda Institute of Technology and Sciences in May 2015, majoring in Computer Science in May 2015. During his under-graduate program, he worked for Kony Labs, Hyderabad as in intern for the software development team. He worked on technologies like AJAX and node.js.

He received his master's degree in Computer Science from Missouri University of Science and Technology in December 2017. While there, he greatly enjoyed his work as a research assistant to Dr. Bruce McMillin for two years. Uday presented his research work at scientific meetings and participated in conferences discussing challenges in high performance computing. This was possible as a result of his securing competitive funding from the National Science Foundation. Uday has published his work in Eleventh IFIP WG 11.10 International Conference on Critical Infrastructure Protection.