International Journal of Multidisciplinary Research And Studies

Available online at https://ijmras.com/

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH AND STUDIES
ISSN: 2640 7272
Volume:04; Issue:05 (2021)

Page no.- 11/11

MODELING A VEHICLE'S SECURITY IN AN AUTONOMOUS VEHICLE SYSTEM

Manish Kumar

M.Phil., Roll No. :140404: Session: 2014-15

University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India.

E-mail: km.551988@gmail.com.

ABSTRACT

It is very likely that the future of transportation will consist of automated vehicle systems. Many cars now have the capability to connect with one another through the use of a wireless channel thanks to the development of vehicle ad-hoc networks (VANETS). The real time application of a vehicle platoon, in which 8-25 cars follow one another and mimic the actions performed by the vehicle in front of it, is relatively new. However, the concept of a vehicle platoon was first introduced in 1986 as part of a project called PATH (Partners for Advanced Transit and Highways) that demonstrated the advantages of a vehicle platoon. Both a Cyber-Physical System (CPS) and an Internet of Things (IoT) system can be construed to refer to the same thing: an autonomous vehicle. [Cyber-Physical System] Cyber-Physical Systems (CPS) are sophisticated, heterogeneous, distributed systems that generally consist of a large number of sensors and actuators that are connected to a pool of processing node.

KEYWORDS*:* Vehicle's, Security, Autonomous, Cyber-Physical Systems, Heterogeneous, VANETS.

INTRODUCTION

It is very likely that the future of transportation will consist of automated vehicle systems. Many cars now have the capability to connect with one another through the use of a wireless channel thanks to the development of vehicle ad-hoc networks (VANETS). The real time application of a vehicle platoon, in which 8-25 cars follow one another and mimic the actions performed by the vehicle in front of it, is relatively new. However, the concept of a vehicle platoon was first introduced in 1986 as part of a project called PATH (Partners for Advanced Transit and Highways) that demonstrated the advantages of a vehicle platoon. It was expected that the implementation of platoons would result in an increase in the capacity of the roads, a reduction in the amount of time spent waiting for trips, and a reduction in the amount of energy used. In light of the fact that irresponsible drivers and mechanical failures are responsible for more than 95% of all accidents the PATH programme would also help prevent collisions and breakdowns. People are often rather apprehensive when it comes to placing their faith in the judgement of a driverless automobile. Although cruise control has been around for quite some time, it only has the ability to manage the vehicle's speed. However, with the advent of autonomous technology, other aspects of a vehicle, such as its braking, manoeuvring, and acceleration, may also be controlled. When the idea of a driverless vehicle is applied to a group of vehicles known as a platoon, the flow of information should be encrypted to ensure its safety, and any deviation in the vehicles' speeds or distances should be flagged quickly.

The objective of combining cyber and physical security is to determine the reason for the discrepancy, since once the origin of the erroneous information is located, it will be possible to take the necessary precautions to protect the infrastructure (i.e., to discard or repair). It is necessary to ensure the confidentiality of any information that may be disclosed by the various components of the vehicles. Self-driving cars produced by Tesla and Google are currently available for purchase, and both companies have been able to show the viability of their products in actual traffic conditions. These automobiles are capable of taking care of all of the driving. These automobiles have sensors that can identify pedestrians, bicycles, vehicles, roadwork, and other objects at a distance of up to two football fields in either direction. These sensors can detect objects in all directions. It is reasonable to hypothesise that in the years to come there will be an increase in the number of autonomous cars, and there is a real potential that vehicles will be able to communicate with one another. Technologies such as global

Manish kumar*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: dipukarn@gmail.com.*

positioning systems (GPS), 360-degree video systems, sensors, beacons, and sophisticated onboard processing processors are utilised by self-driving autonomous cars. This provides the attacker with a selection of potential attack paths to choose from; however, our infrastructure makes use of these information paths in such a way that even if only a few paths are compromised, the remaining paths will assist us in locating the path or vehicle that has been compromised. If the model cannot be deduced, then the attack cannot be detected since the vehicle will not be aware that there is a component in the automobile that has been corrupted. This allows the attack to go undetected. The most important addition that the thesis makes is the development of a cyber-physical platoon model. In this model, an attack would be detectable, and the vehicle would be made aware of the compromised source, if at all feasible. We are attempting to construct security domains in such a manner that if an attack were to take place in one domain, the compromised domain might be identified with the assistance of information routes coming from other domains. The work that has been described and the many case scenarios that it includes illustrate the ability to discover security flaws in a cyber-physical system.

CPS SECURITY

Both a Cyber-Physical System (CPS) and an Internet of Things (IoT) system can be construed to refer to the same thing: an autonomous vehicle. [Cyber-Physical System] Cyber-Physical Systems (CPS) are sophisticated, heterogeneous, distributed systems that generally consist of a large number of sensors and actuators that are connected to a pool of processing nodes. CPS are used to monitor and control a variety of physical phenomena. CPS aim to perceive and understand changes in the physical environment, analyse the impacts of such changes on the operation of the CPS, and make intelligent decisions to respond to the changes by issuing commands to control physical objects in the system; thereby influencing the physical environment in an autonomous way. This is accomplished through the fusion of sensors, computing nodes, and actuators, which are connected through various means of communications. The connections between actuation and sensing through the physical environment, and between sensors and actuators through one or multiple (distributed) computing or intelligent control node(s), form a feedback loop that aims to achieve a desired objective or steady state. This loop is depicted in Figure 2, and it can be seen that the connections form a feedback loop. As a result, a CPS will either carry out its tasks in a fully autonomous manner or will at the very least offer support for a human-in-the-loop mechanism

Manish kumar*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: dipukarn@gmail.com.*

as a component of certain semiautonomous control operations. CPS is able to remotely influence, manage, automate, and control a wide variety of industrial activities because to its distributed closed-loop process.

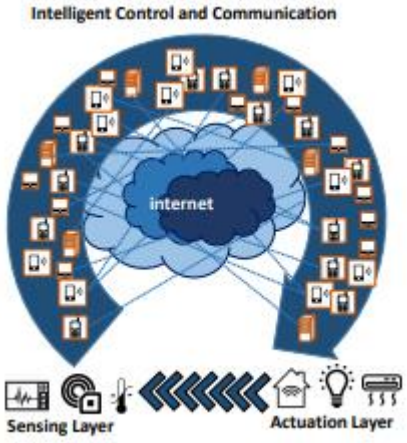

Fig 2 Interactions between sensor layer and actuator layer

CPS are also known as Operational Technology Systems (OT Systems). This is because of the operational aspect of CPS in the majority of industrial control procedures. The distinction between control and monitoring systems (CPS) and the Internet of Things (IoT) is becoming more difficult to discern as a result of the widespread deployment of Internet-connected devices (i.e., IP-enabled sensors and actuators) in CPS systems (IoT). The Internet of Things (IoT) is a notion that originated with the concept of linked smart gadgets (36), which may or may not interact with actual physical items. Consequently, there are application scenarios in the traditional OT domain that may be readily classed both as an IoT system and a CPS system. For instance, a distributed collection of sensor nodes to monitor and regulate the energy use of a manufacturing facility is one such example. Autonomous cars, which serve as the primary subject of this body of work, are among the prominent instances of CPS and IoT systems, as well as the applications that correlate to those systems. As a result, the tactics used to attack a variety of OT systems share commonalities and may be categorized as attacks on various CPS components, such as communication, storage, actuator, sensor, and computation nodes. This is because the OT systems themselves share similarities. Several of these assaults are depicted in Figure 3 which may be seen here.

Manish kumar*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: dipukarn@gmail.com.*

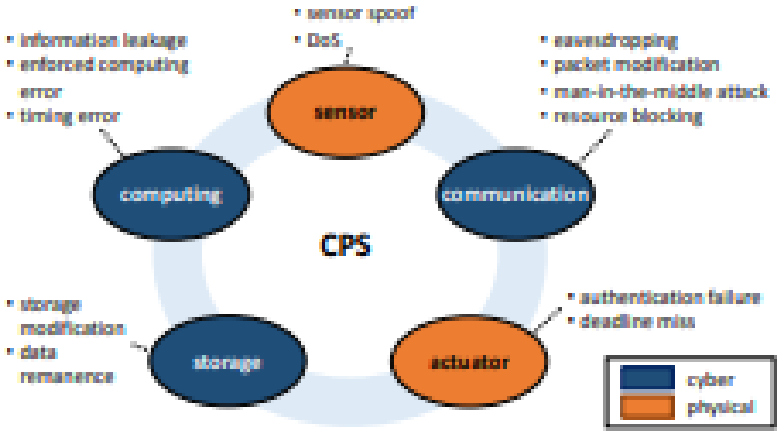

Fig 3 CPS Attacks: Generic Model

- However, this na¨ıve and isolated analysis of attacks, in the context of a specific CPS, and the adoption of the corresponding countermeasures, are grossly inadequate and misleading for several reasons.

- These generic attack studies tend to ignore the security objectives of the CPS, which aim to strike a balance between risks, cost and convenience through the adoption of a hybrid of security control measures. Thus, a seemingly insecure mechanism may be operationally acceptable due to the fact that it is operating within a controlled environment created by other security mechanisms of the system.

- Depending on the prevailing OT security practices, as well as the assumed adversarial model, it might be unnecessary to account for certain vulnerabilities

- The generalization of attacks across all CPS typically ignores the roles of Roots of Trust (RoT) and security perimeter modeling, which are the basis of many securityby-design approaches

In its most fundamental form, security-by-design for a CPS is an all-encompassing process that is seen as a subfield of systems engineering. When it comes to security design approaches, addressing individual assaults in a piecemeal and ad hoc manner is not likely to be very helpful. This paper refers to the above classification and enumeration of attacks, as done predominantly in the current literature, as generic attack studies due to the fact that these studies tend to study localized attacks in a generic setting of CPS. The reasons for this are explained in more detail

Manish kumar*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: dipukarn@gmail.com.*

later in the paper. This pattern of general attack studies is made worse by the fact that there is no clearly defined security standard for autonomous vehicles (AVs) that is aligned with the criteria for road safety. On the other hand, we place a strong focus on the security-by-design aspect of AV as a system, which is in fact a cyber-physical system. The technological obstacles that must be overcome in order to ensure the safety of autonomous vehicles are directly deduced from the primary safety goals that must be met. This is true in the context of the unique vulnerabilities that are posed by AVs that have varying degrees of autonomy.

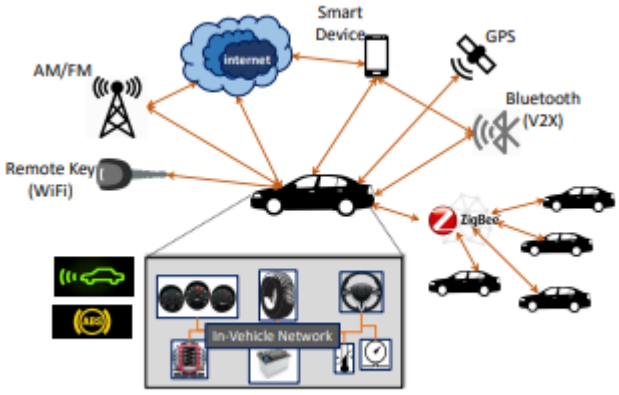

Fig 4 Exemplary Networked Vehicle

RESEARCH METHODOLOGY

SYSTEM MODEL

The following describes how the vehicle platoon works:

1. First, the platoon's direction is chosen by the LV in the lead. The first vehicle in a platoon is called the "lead vehicle." The trailing cars adhere to the LV's lead.

2. The following vehicles in the platoon get this data from the lead vehicle and adjust their course accordingly.

3. The LV can signal a turn or a decrease in speed through its beacon, and the other vehicles will adjust their speed and direction accordingly.

4. Fourth, the data from the sensors and the communication network is double-checked and compared by each vehicle. If everything checks out, it moves forward; otherwise, a warning is sent.

5. Fifth, other cars in the platoon look at the facts on the flagged automobile and then

Manish kumar*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: dipukarn@gmail.com.*

determine whether or not to keep it.

Vehicle-to-vehicle (VA) networks are the first thing that spring to mind when discussing methods of communication between autonomous cars (vehicular ad-hoc networks). While VANETs offer numerous advantages, they suffer from a lack of scalability due to the fact that every vehicle is linked to every other vehicle. This means that for n cars, n connections are needed. Since every vehicle in the single platoon model acts as a carbon copy of the lead vehicle, the number of connections drops from n to only . The platoon's lead vehicle is linked to the other vehicles in the platoon's front line. As a result, the scalability issue is mitigated and all cars may remain linked. Specifically, the automobile is the physical component of this cyber-physical system along with a computer like the control unit. There is communication between many layers of protection. The safety zone can be designated as either safe or unsafe. The following components make up our model:

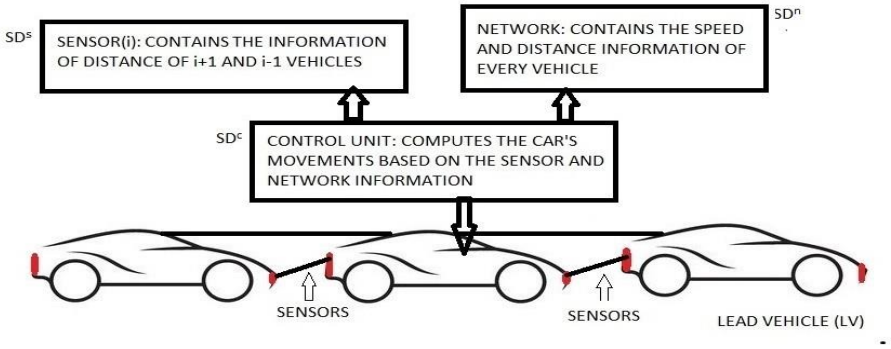

Fig 5 Information transfer

DATA ANALYSIS

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 kindof 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 componentis malfunctioning. Therefore, the model should be designed to eliminate attacks that are MSDND secure.

Figure 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.

Manish kumar*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: dipukarn@gmail.com.*

Below are the set of entities c, s, n, ch that can be evaluated to determine the inter- actions 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 ccordingly) .
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 1 Valuation function

Valuation	Result
$V^c = s_0 \wedge T$ c	"true" ↔ Control unit is controlling the car
$V^c = s_1 \wedge T$ dn	"true" ↔ Control unit gets input from networks
$V^c = s_2 \wedge T$ d_S	"true" ↔ Control unit gets input from sensors
$V^c = s_3 \wedge T$ ch	"true" ↔ Control unit gets result from checker

ch: this is a computational unit inside the control unit that checks if the informationreceived 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)), whered(n), d(s) and d(i) are distance information received by the control unit from the network, sensor and invariant, respectively.

Table 2 MSDND analysis results for a single car

Case	Information Path	MSDND	Vehicle Status

Manish kumar*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: dipukarn@gmail.com.*

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 3. 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. 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

CONCLUSION

Manish kumar*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: dipukarn@gmail.com.*

MSDND is helpful for modelling assaults whose primary objective is not to steal information from an adversary but rather to conceal vital information from that adversary. 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, making the information MSDND secure and undetectable, MSDND secure is bad for the system but good for the attacker. This is because information can be hidden by making it impossible to evaluate the desired question. A good cyber-physical system will have a model with a reduced number of states where maintaining MSDND security is still attainable. The majority of the instances in our model are not MSDND secure, which is one of the reasons why our CPS is a good model. Additionally, we are able to see that if we have additional information pathways, such as the invariant and the beacon, it is much simpler for us to identify an attack.

REFERENCE

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. 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.

Manish kumar*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: dipukarn@gmail.com.*

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,

8. 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.

9. 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.

10. 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.

11. 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.

Manish kumar*, *University Department of COMPUTER SCIENCE, B.R.A. Bihar University, Muzaffarpur, India. E-mail: dipukarn@gmail.com.*