Security-as-a-Service for Transportation Cyber Physical Systems[1]

Brijesh Kashyap Chejerla and Sanjay Madria
Computer Science Department
Misouri University of Science & Technology,
Rolla, Missouri 65409
Email: bckd2@mail.mst.edu, madrias@mst.edu

Abstract

Cyber-Physical Systems' (CPS) concepts applied to Intelligent Transportation System (ITS) give rise to Transportation Cyber Physical Systems (TCPS). Interfacing the cyber component for computing the requests from a transportation system yields new research challenges owing to the strong coupling constraints and service requirements of the transportation system. Such complex hybrid systems require accurate processing and timely feedback owing to stability and reliability concerns. This necessitates the use of a computationally intensive cyber sub-system such as a cloud computing platform. The main aim of this cyber sub-system is to maintain system operational stability and security. However, since the structure of a TCPS is not very well defined, providing security becomes a major challenge. This necessitates a Security-as-a-Service architecture on the cloud. In this position paper, we list the various design and research challenges in constructing such an architecture and provide directions for solutions to such problems.

I. Introduction

In a TCPS, the three Cs, computation, communication and control have a complex interconnection which is constrained by latencies resulting from the interconnection. As the physical sub-system of the TCPS is composed of heterogeneous components such as vehicles, road side assistance units, central decision units, the sub-system has varied acceptable latencies, computational constraints and connectivity limitations. In order to service such a physical sub-system, the cyber sub-system should be powerful to cater to the Quality of Service (QoS) needs of the different components. In a TCPS, the job of the cyber component is not limited to just providing operational stability by maintaining interconnectivity among the heterogeneous components of the sub-systems, but, it also extends to updating the TCPS in lieu of new components being added on-the-fly to the sub-systems and deleting them upon their determination as compromised components. In such dynamic and hybrid systems, communication among peers is of utmost importance and latency constraints are very stringent owing to limited connectivity of the components and sub-components.

In a TCPS, the challenge arises due to the coupling and decoupling of the sub-systems and their interoperability. It is a non-trivial task to satisfy the varying QoS requirement of connected sub-systems while keeping the latency low to run the TCPS smoothly. Satisfying the QoS requirements under low latencies is a major bottleneck which can be severely compromised by security holes in the entire CPS. Thus, security plays a very important role in maintaining the stability and operability of the system. An attacker can cripple the system by attacking either of the coupled sub-systems and cause a malfunction in any other connected component. There are four possible attack modes of an attacker - (i) Physical attacks (ii) Physical to Cyber attack (iii) Cyber to Physical attack, and, (iv) Cyber to Cyber attack, where, the second and third kind of attacks are those in which the attacker gains access to either the cyber or the physical component and launches an attack on the other component of the integrated CPS. The last type of attack corresponds to the attacker gaining access to a part of a network and crippling another coupled network.

In this position paper, we would like to focus on the TCPS stability and operability by detecting and preventing attacks on individual sub-systems to achieve the ulterior goal of building an attack resilient and a robust TCPS. We will list out the various requirements of a TCPS and the problems that arise in coupling the transportation system to the cloud computing platform and provide a Security-as-a-Service (SaaS) functionality to cater to all the security requirements.

II. Research Challenges and Solutions

There are several challenges in providing operational stability to a TCPS. Because of the number of systems interconnected, and, with each of them having their own QoS requirements, providing stability and reliability through a blanket security solution is a complicated task. Thus, we propose to provide a Security-as-a-Service functionality on the cloud that serves the transportation component as needed with minimum latency. The Security as a Service functionality comprises of a number of modules that cater to different security problems prevalent when the transportation and cloud platforms are coupled.

A. Attack model

Largely, transportation systems that require SaaS to are road transportation systems that have several different components such as vehicles, drivers, road side assistance units etc. which disseminate and exchange information about traffic updates and infotainment. System operability through security in those systems is hard to achieve as the time a node (user or a vehicle) stays on the network is very low. Hence, it is very easy for the attacker to perform an attack without being detected. Also, since there are several points in the TCPS that the attacker can launch his attack, it becomes all the more difficult to pin point the source of the attack. For e.g., as shown in figure 1, the attacker can either be a user in a vehicle generating spurious packets into the network or he can gain access to one of the Roadside Units (RUs) and gain access to all the private data on the network. He can use mechanisms to disrupt the data connectivity by jamming the network layer, thereby, causing packet drops, increasing the latency of the control messages that are to be retransmitted onto the transportation system etc. These are the physical to cyber attacks that the attacks were classified into earlier. In addition to this, the attacker can compromise one of the computing units in the cloud and generate faulty control messages that can disrupt traffic flow which could potentially harm the safety of the transportation system. In order to provide solutions to these problems, we propose an automated and intelligent transportation control unit which is aided by our SaaS functionality in the cloud. Using cloud gives us both a centralized and a distributed architecture and can be used as needed by decoupling the sub-systems that are affected. Thus, by doing this, we ensure the safety and operability of the transportation system.

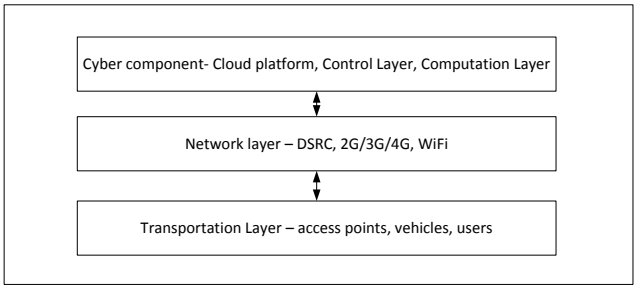

Fig. 1. Layers of Transportation Cyber-Physical System

***Proposed Research*:** While solutions to security issues have previously been studied for a transportation system in the capacity of Vehicular Ad-hoc Networks (VANETS) [1]–[3], they are insufficient in providing operability under time-based constraints. Also, largely most of the attacks that have been studied are authentication and identity based attacks such as sybill attacks [4]. Stabilizing the TCPS under large packet drops and communication disruptions caused by an attacker in the Short Range Communication models such as DSRC have not been studied effectively. Almost none of proposed solutions take into consideration latency bounds, i.e. the time bound under which such an attack has to be determined, beyond which the damage to the system is near irreparable. We intend to research on this aspect of providing SaaS under latency constraints.

Intelligent attacks in a TCPS are where the attacker can cause extensive impacts by producing many replica nodes of a few compromised nodes (both in the cyber and transportation domain) as compared to physically capturing and compromising many benign nodes. To defend against such widespread attacks, we will investigate replica detection schemes in both physical nodes (e.g. sybill attack) and on the Virtual Machines (VMs) on the cloud .

More specifically on the physical sub-system, we propose to detect static replica nodes (RUs) by leveraging the intuition that static replica nodes are placed in more than one location. For detecting mobile replicas (vehicles), we will assume that mobile replicas are in two or more locations at once and thus appear to move much faster than benign nodes. The goal is to achieve high node compromise detection capability with less overhead while rarely misidentifying benign nodes as compromised nodes in the least possible time required to detect them. Our approach will be based on repeated game theory where games are played between attackers and the defender (i.e., the network or system). The objective is to provide suitable defense strategies against node which otherwise will remain indistinguishable from genuine nodes.

To provide an effective SaaS functionality, we would like to research Information Fusion algorithms aided by graph theoretic and game theoretic approaches. Using the information fusion algorithms, we would like to integrate the concepts of traffic analysis game theory and graph theory. We intend to profile the traffic trace generated by the TCPS into a traffic model at various time instances, which will provide us with the capability to predict future traffic patterns under packet losses and network disruptions. We will research on the decision making algorithms in order to generate hypotheses and decisions for data distribution on cloud infrastructure. For instance, many parallel machine learning algorithms are used to make feature extraction and selection such as Gibbs Sampling, Belief propagation, gradient descent etc. These algorithms will be further investigated to study their runtime and effectiveness on the use of TCPS. Information that is sent from the nodes will be processed in the cloud platform and hence, effective data management and distribution strategies are essential. Load balancing, content/data distribution and resource allocation under security attacks play an important role in this phase of decision making. The post-data-processing observations will help us understand TCPS behavior better and allow us to take appropriate control decisions. These control decisions are the sent to the physical sub-system to ensure that the physical sub-system functions smoothly. Thus, our SaaS functionality on the cloud tries to provide a blanket security solution to the TCPS, where, each module of the SaaS services different kinds of attacks and the information fusion algorithms aided by graph theory determine the cause and effect relation among the various attacks and pro-actively subvert the occurrence of system malfunction or reliability issues. Most importantly, this is done under latency constraints thus providing operational stability.

REFERENCES

[1] "Security on vanets: Privacy, misbehaving nodes, false information and secure data aggregation," *Journal of Network and Computer Applications*, vol. 34, no. 6, pp. 1942 – 1955, 2011.

[2] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in *Proceedings of 4th Workshop on Vehicle to Vehicle Communications (V2VCOM)*, 2008.

[3] K. Plossl, T. Nowey, and C. Mletzko, "Towards a security architecture for vehicular ad hoc networks," in *The First International Conference on Availability, Reliability and Security, ARES*, 2006, pp. 8 pp.–.

[4] J.-W. Ho, D. Liu, M. Wright, and S. K. Das, "Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1476–1488, 2009.