Securing Physical Processes against Cyber Attacks in Cyber-Physical Systems

Nishanth Gaddam, G. Sudha Anil Kumar, and Arun K. Somani
Dept. of Electrical and Computer Engineering
Iowa State University, Ames, IA 50011
Email: {nishanth,anil,arun}@iastate.edu

1. Introduction

A cyber-physical system (CPS) consists of two important components namely, a physical process and a cyber system. Typically, the physical process is monitored or controlled by the cyber system, which is a networked system of several tiny devices with sensing, computing and communication (often wireless) capabilities. The physical process involved could be a natural phenomenon (e.g., a dormant volcano), a man-made physical system (e.g., an automobile, train) or a more complex combination of the two.

The cyber system closely interacts with the physical system to either control/automate some of its work or monitor it and send the information to a remote station. In general, the deeper the interaction between the cyber and physical systems the smarter is the CPS over a bare physical system (i.e., better performance and usability). On the other hand, as the interaction between the cyber and physical systems grows stronger, the physical systems become increasingly susceptible to the security vulnerabilities in the cyber system [1]. As a result, as we build smarter and tightly coupled cyber-physical systems we need to consider the impacts of cyber vulnerabilities on the physical systems.

Consider a Traffic Adaptive Inter-Vehicular CPS where each vehicle is equipped with a sensor node. The objective of the attached sensor nodes is to constantly monitor the traffic at their current location and broadcast this information to other vehicles elsewhere which are considering using the same route. This information can be used to dynamically adapt the vehicle route as per the traffic. Here the physical system consists of a set of vehicles and the traffic they create while the cyber system consists of the wireless ad-hoc network formed by the different sensor nodes to accomplish inter-vehicular communication. Now, consider a man-in-the-middle attack [2] scenario on the cyber system, where a single node can intercept crucial traffic information and modify it before forwarding it further. It is imaginable that such an attack can be launched to create extremely unbalanced and un-progressive traffic patterns sometimes leading to unrecoverable losses.

In the following, we first outline the limitations of cyber physical systems using example inter-vehicular systems. We present a brief overview of promising approaches to deal with security concerns in cyber-physical systems.

2. Limitations of Current Cyber-Physical Systems

Traffic management is a pressing problem in many developed and developing countries. Addressing this problem, several researchers have suggested inter-vehicular communication systems as a solution [3]. However, the existing solutions suffer from certain limitations, which crop-up due to the cyber vulnerabilities in the system. In the following, we identify a few attack scenarios that can be launched on the existing inter-vehicular systems and extend the discussion to outline their effects on traffic management.

- Incorrect Information Propagation in the network: This can be caused by a simple man-in-the-middle attack as discussed earlier. The consequences would include sending alarms in the network creating unnecessary panic among the public commuting through various modes of transport. An intelligent attack can divert entire traffic to specific region creating traffic jams. The severity of this attack can range from delay in traveling to the extent of blocking emergency vehicles.
- Creating Information holes in the network: This kind of a scenario can be created by launching well-known worm-hole attacks which includes advertising false routes and dropping all the packets routed through the advertised paths. Because of this, information about the traffic is dropped and farther vehicles will encounter information service disruption and become unaware of the traffic in certain regions.
- Exhausting energy in battery-driven sensor nodes: To exploit the ease of deployment oftentimes the sensor nodes are located on the route and are battery supported, such nodes are susceptible to energy-exhaustion attacks where attacker initializes unnecessary communication with each node and waits until the node drains all its energy out. Again, such attacks can create information holes in the network.

3. Security Concerns in Cyber-physical Systems: Promising Approaches

In general, building a secure cyber-physical system is very challenging as it involves dealing with the vulnerabilities in the cyber systems and their effects on physical systems in an integrated manner. A promising general approach to deal with this would be to carry out a propagation analysis from cyber vulnerabilities to the corresponding effects on the physical system or vice versa. Such an analysis can be used to rank the severity of the cyber attacks and thereby, prioritize among the various attacks to deal with. A similar analysis can be carried out backwards going from different critical functional disruptions that a physical process can undergo due its interaction with the cyber system and propagate them to understand the different cyber attacks that can cause these disruptions. Either way, an integrated consideration is needed. Although such an analysis would not solve the problem entirely, it provides a high-level procedure to narrow-down the extent of security analysis that needs to be carried out on the cyber system in a CPS.

A similar approach can be carried out in securing the traffic system from the vulnerabilities of inter-vehicular communication system. Starting from various effects that the cyber system can have, we can identify the possible attacks. For example, attacks on the cyber-system can result in unbalanced traffic re-routing and information service disruption (lack of traffic information to some vehicles). To mitigate these effects on the traffic system, the cyber system needs to develop tolerance against such attacks. The above discussion brings out a number of challenges involved in preventing, detecting and mitigating different attacks in CPS. In the following we outline them.

- **Prevention:** The attack space is large to enumerate and develop prevention mechanisms. The present cryptographic techniques may not provide a complete solution due to the additional constraints exhibited by CPS.
- **Detection:** In distributed CPS the mechanism to coordinate information for attack detection needs to be scalable. Designing such a mechanism is challenging. Sometimes it is difficult to distinguish between an attack scenario from an unusual but genuine behavior of the physical system. An effective detection mechanism should be able to make this distinction.
- **Mitigation:** Mitigation scheme should coordinate with the physical system. Depending on its state, the scheme should choose an appropriate degree of attack isolation. Mitigating an attack while still keeping the system operational is essential for few critical applications.

Our goal is to develop effective prevention, detection and mitigation mechanisms for CPS. Our immediate focus would be on developing prevention mechanisms. Specifically, we will establish a relationship between types of attacks and different failures. By deriving efficient solutions against the identified threats, corresponding failures in the physical system can be avoided.

In summary, we emphasize that attacks in cyber system can have drastic effects on the normal functionality of physical systems. Studying the interdependency between them and deriving mechanisms that would protect the physical system from external attacks is a complex task to achieve. It requires a thorough understanding of the system that is being controlled and the possible attack space that can cause functional disruptions.

References

[1] Alvaro A. Cardenas, Saurabh Amin, hankar Sastry, ”Secure Control: Towards Survivable Cyber-Physical Systems,” in Proc. of Intl. conf. on Distributed Computing Systems (ICDCS) - Workshops, pp. 495 - 500, 17-20 June 2008.

[2] H. Hwang, J. Gyeok, K. Sohn and S. Park, ”A Study on MITM (Man in the Middle) Vulnerability in Wireless Network Using 802.1X and EAP,” in Proc. of Intl. Conf. on Information Science and Security (ICISS), pp. 164-170, Jan. 10-12, 2008.

[3] M.L. Sichitiu and M. Kihl, ”Inter-vehicle communication systems: a survey,” IEEE Communications Surveys & Tutorials, Vol. 10, no. 2, pp. 88-105, 2008.

Author Biographies

Nishanth Gaddam is currently pursuing MS degree in Computer Engineering at Iowa State University. He received his BS in Electrical Engineering from BITS-Pilani, India. His research interests are in the area of wireless sensor networks, especially network routing algorithms and performance analysis.

G. Sudha Anil Kumar received his dual-degree (B.Tech and M.Tech) in Computer Science from Indian Institute of Technology (IIT), Kharagpur in 2004. He is currently a PhD candidiate in the Dept. of Electrical and Computer Engineering at Iowa State University. His PhD thesis focuses on system-level energy management in Real-Time Networked Embedded Systems.

Arun K. Somani is currently Jerry R. Junkins Endowed Chair Professor of Electrical and Computer Engineering and Anson Marston Distinguished Professor at Iowa State University where he first served as David C. Nicholas Professor during 1997-2002. He earned his MSEE and PhD degrees in electrical engineering from the McGill University, Montreal, Canada, in 1983 and 1985, respectively. Professor Somani’s research interests are in the area of fault tolerant computing, dependable computing and networking, WDM-based optical networking, and reconfigurable and parallel computer system architecture.