CPS PI meeting 2011

A Study of Security Countermeasure for Cyber-Physical Systems

NSF Award Number: 1059116

Wei Zhao[1], Yuhong Zhang[2]
1. Temple University, Philadelphia, PA 2. Texas Southern University, Houston, TX

INTRODUCTION

A *cyber-physical cyber system* integrates computing and communication capabilities with the monitoring and/or control of entities in the physical world which should be safe, secure, dependable, efficient and in real-time. It requires high lever securities, which means that a CPS should work as expected even when there are malicious attacks.

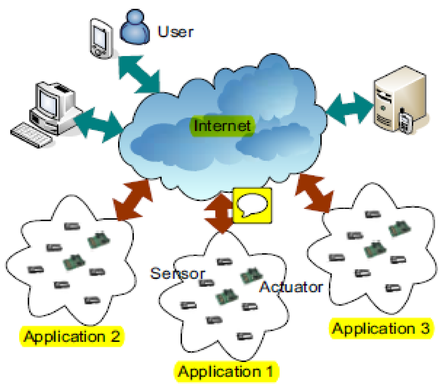


Figure 1: CPS systems (cited from F. Xia's Network QoS Management in Cyber-Physical Systems)

In this project, we develop techniques for secured real-time services for cyber-physical systems. In contrast to the traditional approaches, our work involves radically different approaches. We leverage the characteristics of cyber-physical systems and consider solutions that especially address the mission critical needs of the cyber-physical systems. In particular, we propose to incorporate *real-time traffic modeling techniques* into the security service, consequently enhancing both system security *and* real-time capabilities in an adverse environment.

PROJECT OBJECTIVE

The objective of this project is to develop techniques for secured real-time services for cyber-physical systems. In particular, we intend

- to develop technologies that effectively shield network resources and payload connections from passive attacks and that support rapid recognition of active attacks, and
- to develop tool sets that help to build systems that exhibit inherent survivability properties, i.e., the ability to continue real-time operation in the face of attacks that are partially successful.

PROJECT TASKS

Task 1: Security Countermeasures Based on Traffic Modeling Theory

Attacks to networks are classified as passive attacks and active attacks. Passive attacks are those when an intruder listens to network traffic in order to gain access to sensitive information. Active threats are the modification, insertion, or deletion of messages by an intruder. We will develop countermeasures for both kinds of attacks.

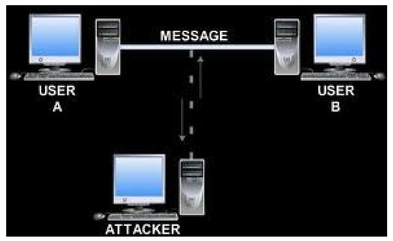


Figure 2: Passive attack (cited from http://www.infinityexplore.com/hak/attack/passive_attack.html)

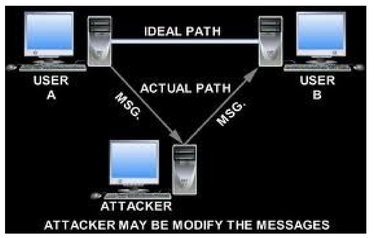
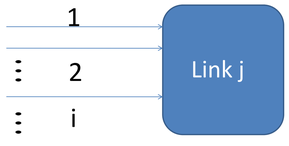


Figure 3: Active attack (cited from http://www.infinityexplore.com/hak/attack/active_attack.html)

- **Countermeasure for Passive attacks**

The countermeasure for passive attacks is to properly schedule the stuffing messages over the network such that an enemy cannot detect what the current operational mode is. One simple way to mask the operational mode is to make all the operational modes appears the same. This means that the aggregated traffic on each link should appear as constant rate traffic. That is, in terms of our traffic modeling terminology, for every link *j,*

$$\sum_i F_{i,j}(I) + S_j(I) = \alpha I$$



where $F_{i,j}(\cdot)$ is the traffic function for the traffic over link *j* from connection *i*, $S_j(\cdot)$ is the traffic function for stuffing messages over link *j*, and α is the desired constant rate that is invariant in all the links and for all the operational modes.

- **Countermeasure for Active attacks**

With traffic modeling theory, a node should be able to examine the traffic pattern and decide if it is as predicted by the theory. Any unexplained inconsistency would imply an intruder's activity. Consider an arbitrary point (say link j) in the network where connection i traverses. The traffic theory can predict the traffic behavior in terms of the maximum and minimum traffic function. These functions provide the upper and lower bound on the traffic from connection *i* that is transmitted through this link. Now, if we can observe the traffic and find that the actual traffic violates these bounds, then a (potential) intrusion is detected.

Task 2: Tool Set for Secured Real-Time Communication Services

The objective of the proposed tool set is to provide secured real-time communication services. The tool set we develop in this task will have the following functions:

- to direct message stuffing activities so that the filler messages are sent at the right time and at the right place,
- to detect denial-of-service attack and determine the attacked component (e.g., router),
- to dynamically reconfigure the routes that are potentially damaged by attackers, and
- to make admission decisions for real-time traffic flow so that the deadlines of cyber-physical messages are guaranteed even if the system is under attacks.

OUTREACH ACTIVITIES

One important education goal of this project is to popularize ideas and concepts in science and engineering to K-12 teachers and students. We plan to achieve this objective by actively involving in a summer pre-college engineering program held by the Department of Engineering Technology in Texas Southern University. More than 90% of these high school students are African American including a large number of female students. Figure 4 show the high school students in the lab of the Department of Engineering Technology at Texas Southern University

Figure 4: High school students in the Lab of TSU

PROJECT PROGRESS

The project made good progress. Our goal is to study architectural models for cyber physical systems. One of our paper "Representation of a Stochastic Traffic Bound" (IEEE Trans. Parall. Distrib. Sys. 21[9]: 1368-72, September 2010) has been identified by Thomson Reuters Essential Science Indicators as a featured Fast-Breaking Paper in the field of Computer Science, which means it is one of the most-cited papers in this discipline published during the past two years. This gives us a new direction in analyzing the real-time traffic in the Cyber-Physical Systems and its impact on related architectural issues

SUMMARY

We have proposed an innovative methodology to address security issues in cyber-physical systems. Specifically, our work involves radically different approaches from traditional security methodologies. We take into account the characteristics of cyber-physical systems and propose to incorporate *real-time traffic modeling techniques* into the security service, consequently enhancing both system security and *real-time* capabilities in an adverse environment.

Acknowledgements: We would like to thank Dr. Helen Gill, CISE\CNS and National Science Foundation for the support of this project.