Towards Cyber-Physical Security of Flow-based CPS

Mahima A. Suresh, Radu Stoleru, Texas A&M University

1. Flow-based CPS: vision and cyber-physical security issues

Flow-based cyber-physical systems (CPS) comprise of physical systems (e.g., transportation system, water distribution systems, oil & gas pipelines) which can be modeled as flow networks where physical entities (e.g., cars and buses, water or oil) flow along the edges of the network. Such systems are vulnerable to attacks that can potentially have severe health and economic impacts (e.g., chemical spills, malicious interference with vehicles' computer systems, open drains - need to be identified in early stages to avoid the risk of fatal accidents, etc.). Securing such systems against attacks is of paramount importance. This has been typically achieved by using complex, costly and frequently imprecise static sensors placed at critical locations in the system [1]. To equip such systems with cyber-physical security without incurring huge costs, we have proposed a cyber-physical system architecture comprised of mobile nodes (their movement is aided by the inherent flow) and static beacons which help locating mobile nodes and collecting their data. In this position paper, we propose an architecture for cyber-physical security of flow-based CPS based on mobile sensors and beacons residing in the physical system residing continuously in the flow-based CPS, monitoring/reporting data and controlling certain aspects of the system (e.g., controlling flows with the help of traffic signals or valves, controlling the release of chemicals, etc.) to aid in the process. Mobile sensor nodes sense the environment and communicate among themselves. Sensor nodes are able to communicate with static beacons that are placed strategically for the purpose of data collection and cyber-physical attack localization. Additionally, beacons aid sensors in time synchronization and collect data from them. The data collected by beacons is processed for event detection, localization, and to provide control inputs.

2. Cyber-physical Water Distribution Systems

We have worked on a Cyber-Physical System for continuous monitoring of Water Distribution System (WDS), i.e., a Cyber-Physical Water Distribution System (CPWDS). We developed a CPWDS where mobile sensors move in the main pipes of the WDS, their movement aided by the flow of water. They exchange sensed data among themselves using underwater acoustic communication and report data to static beacons placed outside the pipes (i.e., communication in the cyber aspect of the CPS). The beacons predict the paths that the sensors will travel after they communicate with them and transmit the information to the sensors. It is also important to decide when and where to deploy the mobile sensors and static beacons [2] (i.e., computation in the cyber aspect of the CPS). So as to ensure sensing coverage of the WDS (i.e., the sensors move around in the main pipes without getting stuck), a control system operates valves and pumps to change the direction of flows in certain pipes (i.e., control in the cyber aspect of the CPS). The CPWDS is therefore described by the three key pieces - Communication, Computation, and Control.

A CPWDS poses several research challenges in communication, computation, and control. The mobile sensors of a CPWDS are equipped with acoustic modems to communicate among each other. Underwater acoustic communication in itself is challenging to handle due to the high propagation delay [3]. A MAC protocol that is able to function in such environments is challenging to design. In a CPWDS, it is essential also to determine when and what data needs to be sent. On the other hand, beacons reside outside the pipes and are aware of the entire topology of the WDS. This information is useful to sensors in pipes that are not aware of their locations. It is challenging to design algorithms to be executed by beacons to provide information about the WDS in an efficient way (i.e., avoiding redundant and unnecessary information) to sensors. The probabilistic nature of movement of sensors in a WDS makes it challenging to decide sensor and beacon deployment. In a WDS, owing to the varying demands of the consumers and valve actions, the flows in the pipes change in magnitude over time. The main pipes of a WDS are usually of larger diameter than the pipes leading to consumers. We observed that if a sensor was designed to have a large form factor and deployed in the WDS, they move around in the WDS without getting stuck in small pipes. However, they may move to parts of the WDS where flows do not change directions over time. In order to effectively monitor a WDS with mobile sensors, the sensors are required to traverse the main pipes regularly. We have addressed these challenges by developing MAC/group communication protocols for communication among sensors, global view algorithms to be executed by beacons, to provide an external perspective to mobile sensors and improve communication among sensors, and a control system designed to enable flow reversal in the WDS, essential to ensure that sensors cover the main pipes of the WDS. We have implemented our algorithms in a simulator specifically designed to emulate movement of sensors in a WDS and are investigating implementations on real hardware. We have also demonstrated flow reversal in several pipes of a WDS by controlling valves.

3. Cyber-physical Security for Transportation Systems

Similar to WDS, transportation systems are prone to cyber and physical attacks. Such attacks can be fatal if they are not identified and resolved. Most vehicles are equipped with several on-board sensors that collect information about the vehicle and also about the environment that is useful in identifying attacks. We envision a flow of data through devices placed on vehicles that collect any requested information from the vehicle's on-board sensors. They may also be equipped with sensors of their own. The mobile agents in the transportation system are the vehicles carrying information and exchanging data among each other. Special access points optimally placed in the network collect information from the vehicles and process the data collected to identify the presence and location of events. Such a system providing cyber-physical security to a transportation CPS poses interesting research questions similar to the CPWDS. Some of them are: (i) what is the best set of vehicles to request information from? We cannot deterministically know the paths of each vehicle on the road. Therefore, the movement of data on the cars is probabilistic and fits the framework of a flow-based system. (ii) where should the access points be placed so as to maximize the likelihood of detecting and locating events? Placing access points at all traffic signals is inefficient and expensive.

References

[1] I. Stoianov, L. Nachman, S. Madden, T. Tokmouline, “PIPENET: a wireless sensor network for pipeline monitoring.” in Proceedings of the 6th international conference on Information processing in sensor networks (IPSN), 2007.

[2] M.A. Suresh, R. Stoleru, E. Zechman, B. Shihada, “On Event Detection and Localization in Acyclic Flow Networks,” in IEEE Transactions on Systems, Man, and Cybernetics: Systems, May 2013.

[3] A.A. Syed. Y. Wei, J. Heidemann, “T-Lohi: A New Class of MAC Protocols for Underwater Acoustic Sensor Networks," In Proceedings of Conference on Computer Communications (INFOCOM), 2008.

Mahima A. Suresh

Mahima A. Suresh is currently a PhD student in the Department of Computer Science and Engineering at Texas A&M University. She is a member of the Laboratory for Embedded & Networked Sensor Systems (LENSS) headed by Dr. Radu Stoleru. She received her B Tech degree from the National Institute of Technology, Karnataka, Surathkal, India in 2009. Her research interests include wireless sensor networks, algorithms and complexity theory, graph theory, and random processes.

Radu Stoleru

Dr. Radu Stoleru is an Associate Professor in the Department of Computer Science and Engineering at Texas A&M University, and the head of the Laboratory for Embedded & Networked Sensor Systems (LENSS). Dr. Stoleru's research interests are in deeply embedded wireless sensor systems, cyber-physical systems, distributed systems, embedded computing, and computer networking. He is the recipient of the NSF CAREER Award in 2013. Dr. Stoleru received his Ph.D. in computer science from the University of Virginia in 2007. While at the University of Virginia, Dr. Stoleru received from the Department of Computer Science the Outstanding Graduate Student Research Award for 2007. He has authored or co-authored over 60 conference and journal papers with over 2,500 citations (Google Scholar). He is currently serving as an editorial board member for international journals and has served as technical program committee member on numerous international conferences.