PURDUE
UNIVERSITY

School of Electrical and Computer Engineering

Inter-office Memorandum

Scheduling of Examinations:

Student's Name: Jin Kyu Koo
Degree: Doctor of Philosophy
Type: Final Exam

Major Professor: SAURABH BAGCHI, Co-chair
Advisor 1: XIAOJUN LIN, Co-chair
Advisor 2: NINGHUI LI
Advisor 3: SONIA A. FAHMY

Examination Date: 06-14-2012
Examination Time: 1:00 PM
Building & Room: EE 118

Thesis Title: Secure Control Protocols for Resource-Constrained Embedded Systems

Abstract: Embedded systems are increasingly being deployed into the world around us. For example, they are used to monitor the environment around us, measure and control the electrical grid, and control vehicles on the road. As they are integrated in the real world, their security becomes increasingly important. However, due to their lower cost, energy constraints and slow computation speed, maintaining security for these systems is usually very challenging.

In this work, we study a range of the important security issues in the operation of embedded systems, which includes reliable synchronization, timely event reporting, and privacy-preserving data transmission. First, we propose a fast and reliable clock synchronization protocol for wireless sensor networks, called CSOnet, which is for wastewater monitoring and is deployed city-wide in a mid-sized US city, South Bend, Indiana. The nodes in CSOnet have a low duty cycle (2% in current deployment) and use an external clock, called the Real Time Clock (RTC), for triggering the sleep and the wake-up. The RTC has a very low drift (2 ppm) over the wide range of temperature fluctuations that the CSOnet nodes operate at, and it has low power consumption (0.66 mW). However, there are two challenges to using RTC for synchronization. First, RTC has a coarse time granularity of only 1 second. Therefore, it is insufficient to synchronize the RTC itself, which would lead to a synchronization error of up to 1 second . Such a large error would be unacceptable for the low duty cycle operation when each node stays awake for only 6 seconds in a 5 minute time window. The second challenge is that the synchronization has to be extremely fast because ideally the entire network should be synchronized during the 6 second wake-up period. We address these challenges by designing a synchronization protocol called HARMONIA. It has three design innovations. First, it uses the fine-granular microcontroller clock to achieve synchronization of the RTC, such that the synchronization error, despite the coarse granularity of the RTC, is in the microsecond range. Second, HARMONIA

pipelines the synchronization messages through the network resulting in fast synchronization of the entire network. Third, HARMONIA provides failure handling for transient node- and link-failures such that the network is not overburdened with synchronization messages. Further, the recovery is done locally. We evaluate HARMONIA on CSOnet nodes and compare the two metrics of synchronization error and synchronization speed with the flooding time synchronization protocol (FTSP). It performs only slightly worse in the former metric and significantly better in the latter metric

Second, we design a timely event reporting protocol for event monitoring, which is a common application of wireless sensor networks. For event monitoring, a number of sensor nodes are deployed to monitor some phenomenon. When an event is detected, the sensor nodes report it to a base station (BS), where a network operator can take appropriate action using the event report. In this paper, we are interested in scenarios where the event must be reported within a time bound to the BS, even under the case that some sensors need multiple hops to reach the BS. However, such a reporting process can be attacked by compromised nodes in the middle that drop, modify, or delay the event report. To solve such a problem, we propose SEM, a secure event monitoring protocol against arbitrary malicious attacks by Byzantine adversary nodes that may collude among themselves. SEM can provide the following provable security guarantees. As long as the compromised nodes want to stay undetected, a legitimate sensor node can report an event to the BS within a bounded time. If the compromised nodes prevent the event from being reported to the BS within the bounded time, the BS can identify a small set of nodes that is guaranteed to contain at least one compromised node. To the best of our knowledge, no prior work in the literature can provide such guarantees.

Third, we introduce a privacy-preserving mechanism for smart meters in the smart grids. In smart power grids, a smart meter placed at the customer endpoint reports fine-grained usage information to utility providers. Based on this information, the providers can perform demand prediction and set on-demand pricing. However, such a fine-grain report also threatens user privacy, since users' specific activity or behavior patterns can be deduced from the fine-granular meter readings. To resolve this issue, we design PRIVATUS, a privacy-protection mechanism that take advantage of a rechargeable battery. In PRIVATUS, the meter reading reported to the utility is probabilistically independent of the actual usage at any given time instant. PRIVATUS also considerably reduces the correlation between the meter readings and the actual usage pattern over time windows. Further, using stochastic dynamic programming, PRIVATUS charges/discharges the battery in the optimal way to maximize savings in the energy cost, by taking advantage of different price zones.

Committee Members: If you are unable to attend this examination, please contact Mr. Koo.