Computers and Electrical Engineering 41 (2015) 86–101

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Dynamic security management for real-time embedded applications in industrial networks ☆

Wei Jiang [a,*], Yue Ma [b], Nan Sang [a], Ziguo Zhong [c]

[a] School of Information and Software Engineering, University of Electronic Science and Technology of China, China
[b] Department of Computer Science and Engineering, University of Notre Dame, United States
[c] Department of Computer Science and Engineering, University of Nebraska – Lincoln, United States

ARTICLE INFO

Article history:
Received 18 October 2013
Received in revised form 25 September 2014
Accepted 2 October 2014
Available online 25 October 2014

Keywords:
Real-time embedded system
Security management
Risk
Feedback control
Scheduling

ABSTRACT

Widely deployed real-time embedded systems can improve the performance of industrial applications, but these systems also face the critical challenge of providing high quality security in an unpredictable network environment. We measure the time and energy consumptions of commonly used cryptographic algorithms on a real embedded platform and introduce a method to quantify the security risk of real-time applications. We propose a Dynamic Security Risk Management (DSRM) mechanism to manage the aperiodic real-time tasks for networked industrial applications. Inspired by the feedback design philosophy, DSRM is designed as a two-level control mechanism. The upper-level component makes efforts to admit or reject the arrival tasks and assigns the reasonable security level for each admitted task. With three proportional feedback controllers at the lower level, the security level of each ready task can be adjusted adaptively according to the dynamic environments. Simulation results show the superiority of the proposed mechanism.

1. Introduction

Mission-critical industrial systems, composed of interconnected embedded systems, have to function correctly and meet dependable constraints. Typical examples of mission-critical industrial systems are power grid systems [1] and automation control systems [2]. Although digital systems and communication among them have been designed to be very reliable, networked industrial systems are still facing serious security challenges [3]. Industrial systems are generally real-time systems and are increasingly deployed in open environments where operating conditions are dynamic and security threatened. Energy efficiency is also a challenge because the supply of energy is generally inconvenient for many embedded systems. Quick energy consumption or early exhaustion of battery may lead to failure of critical task, which may result in degeneration of security quality. For industrial applications, there is a strong need to meet multiple constraints including real-time, secure and energy efficiency simultaneously. This situation is even worse when the workloads cannot be estimated in advance. Therefore, it is an imperative and significant task to design a suitable management mechanism for security-critical industrial applications operating in dynamic and resource-limited environments.

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Associate Editor Dr. Felix Gomez.
* Corresponding author.
E-mail address: weijiang@uestc.edu.cn (W. Jiang).

http://dx.doi.org/10.1016/j.compeleceng.2014.10.002
0045-7906/

Adaptive scheduling is essential towards high performance in embedded real-time systems. Incipient real-time scheduling algorithms are designed for static and priority based scheduling situations [4]. Unfortunately, these works are based on the assumption of knowing most information of applications such as the worst case execution time of each task. These mechanisms are designed in an open-loop mode and cannot be adjusted according to unpredicted situations, which will result in poor performance under dynamic working conditions. This situation gets more severer when considering security protection. For example, security-critical embedded control servers generally run in network environments where the potential threats cannot be modeled accurately. To guarantee the system performance in such unpredicted environments, several feedback control-based adaptive QoS scheduling algorithms have been developed [5]. Recently, feedback control methods have been applied in many applications, such as thermal control [6], fault-tolerance management [7] and dynamic voltage scaling [8]. To improve the security quality of real-time systems, several researchers have proposed some effective algorithms and models [9–12]. However, none of these researches considers dynamic security management for real-time embedded applications in industrial networks.

Given these motivations, based on the research already published by the same authors in [13], we are interested in the design of adaptive security risk management mechanisms for the uniprocessor real-time embedded systems running in security-critical industrial networks. Taking features of aperiodic real-time user requests into account, we propose an adaptive and security risk-aware real-time scheduling mechanism. Administrators just need to appoint the desired system performance, and then the proposed design automatically monitors the system status and chooses the most appropriate cryptography algorithms to achieve satisfactory overall performance. In addition, there should be an advanced mechanism to manage tasks, i.e. admitting or rejecting some user requests. Inspired by the automatic control related work in storage system [14], a two-level control scheme is employed in this paper. The upper-level part mainly admits or rejects the newly arrival requests and then initializes the appropriate security protection. At the lower level, our proposal can change the deployed cryptography algorithms to guarantee the real-time and security performance dynamically.

The primary contributions of this paper are:

- Introducing security-critical applications based on embedded control server systems for industrial networks.
- Establishing the security-aware task model, security overhead model, and security risk model for aperiodic real-time applications.
- Combining the soft real-time and security requirements in a unified framework and deploying proportional controllers to achieve satisfied fine-grained control.

The rest of this paper is organized as follows. Section 2 reviews mostly related work. The typical industry network applications and security protection demands are discussed in Section 3. Section 4 presents the system model. The design problem and a motivating example are given in Section 5 and then a dynamic security management mechanism is proposed in Section 6. In Section 7, we conduct simulations and analyze the experimental results. Finally, conclusions are drawn in Section 8.

2. Related work

To improve the security protection of mission-critical embedded systems, the research on algorithms and models of security management has become a hot topic. Main security issues are identified and several effective solutions are proposed for real-time peer-to-peer communication [15]. Based on a trust job model, Ref. [12] focused on scheduling algorithms for independent jobs over grid computing environments and proposed a space–time genetic strategy. Combining group-level security model with classic real-time scheduling method, Lin et al. designed two security-aware scheduling schemes based on EDF (Earliest Deadline First) policy [16]. Jiang et al. proposed a hardware/software co-design technique to satisfy the confidentiality requirements of automobile systems with communication security constraints [17]. A dynamic security-aware packet scheduling mechanism for wireless networks was designed in [18], which can obtain high quality of security of messages and satisfy the requirement of soft real-time. Gebotys et al. combined the security performance and energy-efficiency then proposed a static low-power security optimization algorithm [11]. Karakehayov designed a static hierarchical communication model with the focus on routing protocols under the real-time, security and energy requirements [19]. Though these researches are meaningful and instructional to improve the security, they are static and cannot be adaptive to unpredicted security threats. Due to the lack of feedback control loop, these works have no adaptability and are not competent for dynamic industrial real-time embedded systems.

To address the issues of static scheduling algorithms, lots of dynamic and adaptive QoS (Quality of Service) scheduling policies have been proposed. A general survey of feedback performance control in software systems was proposed in [20]. Following the in-depth research of feedback control theory, dynamic scheduling mechanisms have been used in many other applications like dynamic voltage scaling [6,8] and fault-tolerant reliable real-time systems [7]. With the rapid development of feedback control theory, advanced controllers haven been designed. Lu et al. deployed an MPC (Model Predictive Control) controller in distributed real-time system, which was designed to control the utilization of end-to-end tasks [21]. However, due to not taking security factors into consideration, these researches cannot be directly used for security-critical industrial systems.