Accepted Manuscript

QoS guaranteeing robust scheduling in attack resilient cloud integrated cyber physical system

Brijesh Kashyap Chejerla, Sanjay. K. Madria

PII: S0167-739X(17)30265-0
DOI: http://dx.doi.org/10.1016/j.future.2017.02.034
Reference: FUTURE 3352

To appear in: *Future Generation Computer Systems*

Received date: 2 November 2015
Revised date: 12 November 2016
Accepted date: 17 February 2017

Please cite this article as: B.K. Chejerla, S.K. Madria, QoS guaranteeing robust scheduling in attack resilient cloud integrated cyber physical system, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.02.034

*Highlights (for review)

In this paper, we propose a security framework based on the semi-network form game in unison with a robust and attack resilient scheduling mechanism for a cloud integrated Cyber Physical System (CPS). As CPS moves from the traditional Sensing Control and Data Acquisition (SCADA) systems with limited on-board processing units, the need to use cloud computing arises owing to the ever increasing processing demands of heterogeneous CPS applications. In such systems, system stability and critical operational capability have the highest priority. This multi-system coupling can have security vulnerabilities which can cripple the speed and effectiveness of data processing, which is unacceptable in time and resource critical CPS applications owing to the need for satisfying the stringent Quality of Service (QoS) requirements. Therefore, a robust scheduling mechanism invulnerable to security attacks is needed to efficiently utilize the scalable processing components as provided by a cloud computing platform. However, scalability brought in by the cloud integration and data migration increases the attack space of an attacker due to an increase in available access points. To address this issue, we developed a new method of learning procedure using Bayesian Networks for the semi-network form game to aid our scheduling algorithm. We employ game theoretic principles to proactively understand the behavior of an attacker based on the strategic decisions made by the defender. This helps us in building a robust scheduling mechanism that schedules tasks based on the decisions made from the output of the game.