INTISARI

DETEKSI SERANGAN *CYBER-PHYSICAL* PADA *INDUSTRIAL CONTROL SYSTEMS* BERDASARKAN MODEL SISTEM FISIK

Oleh
Joko Supriyadi
17/420340/SPA/00609

Deteksi terhadap serangan *cyber-physical* yang menggabungkan elemen *cyber* dan fisik terhadap sistem kendali industri dapat dilakukan pada ranah *cyber* maupun ranah fisik. Deteksi pada ranah fisik dapat menggunakan model sistem fisik sebagai pelacak perilaku sistem. Pada umumnya model fisik yang digunakan adalah model analitik, sedangkan teknik identifikasi sistem berbasis data pengukuran jarang digunakan. Selain itu, penelitian identifikasi sistem seringkali hanya menggunakan pendekatan luaran. Akibatnya model yang diperoleh berpotensi tidak memodelkan sistem fisik dengan cukup baik untuk mendeteksi adanya anomali.

Untuk mengatasi hal tersebut, studi ini menggunakan identifikasi sistem dengan pendekatan masukan-luaran untuk memodelkan perilaku sistem. Metode identifikasi sistem yang digunakan *adalah dynamic mode decomposition with control* (DMDc). Studi ini menggunakan data set dari *test bed Secure Water Treatment* (SWaT) yang merupakan replika sistem pengolahan air. Subsistem pertama dari SWaT menjadi subjek penelitian ini.

Pemodelan dilakukan dengan metode DMDc di mana model yang diperoleh kemudian diuji dan menghasilkan nilai *goodness of fit* sebesar 99,7%. Model yang diperoleh kemudian digunakan untuk mendeteksi 10 serangan terhadap subsistem yang dimodelkan tersebut. Dalam penelitian ini ditemukan bahwa detektor yang umumnya digunakan untuk mendeteksi serangan mengasumsikan data *residual* yang normal, sementara *residual* dalam penelitian ini tidak berdistribusi normal. Oleh karena itu detektor yang digunakan dalam penelitian ini *adalah exponential weighted moving average* (EWMA) nonparametrik karena *residual* yang diperoleh tidak mengikuti distribusi normal. Metode yang digunakan dalam penelitian ini berhasil mengidentifikasi 8 dari 10 serangan yang diuji pada subsistem yang dimodelkan.

Kata kunci : ***serangan cyber-physical, metode masukan-luaran, dynamic mode decomposition with control, exponential weighted moving average nonparametrik***

ABSTRACT

DETECTION OF CYBER-PHYSICAL ATTACKS ON INDUSTRIAL CONTROL SYSTEMS (ICS) BASED ON PHYSICAL SYSTEM MODEL

By

Joko Supriyadi
17/420340/SPA/00609

Detection of *cyber-physical* attacks that combine cyber and physical spaces against industrial control systems can be carried out in both the cyber space and the physical space. Detection in the physical space can use the physical system model as a system behavior tracker. In general, the physical model used is an analytical model, while data-driven system identification techniques are rarely used. In addition, system identification research often uses an output approach only. As a result, the model obtained has the potential to not model the physical system well enough to detect an anomaly.

To overcome this, this study uses system identification with an input-output approach to model system behavior. The system identification method used is dynamic mode decomposition with control (DMDc). This study uses a data set from a Secure Water Treatment (SWaT) test bed, which is a replica of a water treatment system. The first subsystem of SWaT is the subject of this research.

Modeling was carried out using the DMDc method, in which the model obtained was then tested and produced a goodness of fit value of 99,7%. The model obtained is then used to detect 10 attacks on the subsystem being modeled. In this study, it was found that the detectors that are generally used to detect attacks assume *residual* data with a normal distribution, while the *residual*s in this study are not normally distributed. Therefore, the detector used in this study is a nonparametric exponential weighted moving average (EWMA) because the *residual*s obtained do not follow a normal distribution. The method used in this study succeeded in identifying 8 out of 10 attacks tested on the subsystem being modeled.

Keyword : ***cyber-physical attacks, input-output method, dynamic mode decomposition with control, nonparametric exponential weighted moving average***