International Journal of Security and Its Application
Vol.11, No.1 (2017), pp.135-148
http://dx.doi.org/10.14257/ijsia.2017.11.1.12

# Greedy Modes of Data Integrity Attacks on Industrial Control Systems: A Case Study of Tennessee Eastman Process

Weize Li[1], Lun Xie[1*], Yu Rong[2] and Zhiliang Wang[1]

[1] *School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, China*
[2] *Beijing ChenJiGuoTai Science & Technology Co., Ltd. China*
*xielun@ustb.edu.cn*

***Abstract***

*Various modes of data integrity attacks are based on the assumption that attackers have the prior knowledge of the acceptable limits of the target variables. From the defensive perspective, such assumption is useful for identifying stealthy malicious actions. However, from the attacking perspective, such assumption may be unrealistic. In this paper, such assumption is relaxed and a greedy attack strategy (GAS) is proposed. Based on the GAS, two greedy modes (GMs) and three performance indicators are presented. The Tennessee Eastman (TE) process simulations are used to compare the GMs with the prior knowledge-based attacks. Experimental results show that the attacks without prior knowledge consume more time to shut down the process than the attacks with prior knowledge, but there are no significant differences in consumed time between the GMs and the global optimum attacks. Besides, the simulations are also used to assess the attack validity (AV) and the attack cost (AC) of the GMs. The results demonstrate that the GMs on the process measurements have a higher AV and a lower AC than the GMs on the process manipulated variables. That is, if the adversary performs the greedy attacks on the process measurements, there will be a higher probability of success to shut down the TE process.*

***Keywords****: Greedy Attacks, Data Integrity Attacks, Cyber-Physical Attacks, Process Control Systems, Industrial Control Systems*

## 1. Introduction

Integrity is one of the three basic security requirements, which include confidentiality, integrity, and availability [1]. The integrity objective refers to preventing the unauthorized modification of information and ensuring the authenticity of data [2]. In traditional IT systems, the violation of integrity can cause economic or reputation losses, but in industrial control systems (ICSs), it can cause serious damage to equipment, environment or even people's lives. For instance, a malicious modification to the frequency of a converter could lead to the speed fluctuation of the centrifuge, which eventually resulted in severe damage or complete destruction of the centrifuge [3].

During the past ten years, various modes of data integrity (DI) attacks have been discussed. Huang *et al*. [4] described four integrity attack modes on control systems: the max attack, the min attack, the scaling attack, and the additive attack. All these attacks were assumed to lie within the allowable range of controller output values or sensor values, for the reason that signals outside the allowable range could be easily detected by fault-tolerant algorithms. Sridhar *et al*. [5] adopted the min and max attack modes and extended them to the automatic generation control (AGC), which function was to correct

* Lun Xie is the corresponding author.

ISSN: 1738-9976 IJSIA

the tie-line flow and frequency deviation in a power network. Eyisi *1*. [6] modeled two modes of energy-based integrity attacks: the max energy attack and the min energy attack. The former attempted to dissipate maximum amount of energy, and the latter attempted to inject the largest amount of energy. Amin *et al*. [7] presented the block attack model and studied the effect of such attack on the proportional-integral (PI) control scheme in a water SCADA system. All these attacks we mentioned above have the requirement that attack values should lie within a predetermined range. Such requirement means that the attackers must have the prior knowledge of the maximum and minimum allowable values.

Sridhar *et al*. [8] discussed the impact of DI attacks on power system and presented four attack modes: the scaling attack, the ramp attack, the pulse attack, and the random attack. Although there was no clear indication of the maximum or minimum limits in these attacks, the selection of the attack parameters had to satisfy the requirement that the attacks could not trigger any data quality alarms in the control center. In other words, these attacks also required that the attackers possessed the prior knowledge of the acceptable limits of the target variables.

Cardenas *et al*. [9] proposed a general sensor attack model to represent integrity attacks. In that model, the attack signals lay within a dynamic range, which was limited by the minimum and maximum allowable values of the sensors. Besides, they modeled three modes of DI attacks (*i.e*., surge attacks, bias attacks and geometric attacks) based on the assumption that the attacker had the knowledge of the physical system model. Kwon *et al*. [10] investigated the performance of three kinds of stealthy deception attacks on a linear time-invariant system. The results showed that if the attackers had the perfect knowledge of the system model, the attacks could be carefully designed to avoid being detected by the monitoring system. Manandhar *et al*. [11] studied the false data injection attack on the state-space model of a power system, and the attackers were also assumed to have the prior knowledge of the system model. Similar assumptions can be found in the recent work of Smith [12], Bai *et al*. [13], Teixeira *et al*. [14] and Pang *et al*. [15].

In summary, the studies cited above have a common characteristic: the attackers are assumed to have prior quantitative knowledge of the target physical system at different levels. More specifically, attackers are assumed to have the allowable range knowledge of the variable value at the variable level or the full model knowledge of the physical process at the system level. From the defensive perspective, such assumptions are very useful for identifying subtle, complex and stealthy malicious actions. However, from the attacking perspective, such assumptions may be unrealistic and unadaptable. To gain the model knowledge of the physical process is usually a hard problem and not all the attackers have that power.

Recently, Yuan and Mo [16] relaxed the assumption that the adversary had prior knowledge of the physical system model. The authors argued that if the physical system model was unknown, the adversary might still be able to identify it by observing the input-output data from the system. Based on the spectral factorization, they proved a necessary condition and a sufficient condition, under which the adversary could successfully identify the system model. Motivated by that work, we relaxed the assumption that the adversary had the allowable range knowledge of the variable value and proposed a corresponding attack strategy, which could be easily implemented.

Overall, the contributions of this work are threefold. First, we propose a Greedy Attack (GA) strategy with no prior knowledge of the acceptable limits of the target variables, and present two GA modes as well as the corresponding models. Second, in order to compare the performance with the prior knowledge based attacks, three performance indicators are proposed. Third, we provide a case study of Tennessee Eastman (TE) process to illustrate the GA modes and evaluate the performance results.

The rest of this paper is organized as follows. Section 2 gives the corresponding attack strategy, the GA modes and the corresponding models. Section 3 briefly introduces the TE process, the setup of the experiments and the assessment methods. Section 4 presents

 

the results of the performed experiments. Finally, conclusions and future work are summarized in Section 5.

## 2. Greedy Modes of Data Integrity Attacks

In this section we introduce the attack strategy, based on which we propose the GA modes and the corresponding models.

### 2.1. Attack Strategy

Consider an abstraction of a control system as shown in Figure 1. The controller gathers sensing data (y) from sensors and issues control data (u) to actuators to control the physical system. The goal of the attackers is to disrupt the physical system by violating the integrity of the sensing data or the control data. The attackers are assumed to have the ability to monitor and alter the sensing or control data, but they have no prior knowledge of the acceptable limits of these data. In such a situation, the controller and the physical system are like a "black box". The data obtained from the monitoring are time series, that is, a series of observations $x_i(k)$, where $i=1,\ldots,m$ and $k=1,\ldots,n$. The term $i$ indexes the different values of sensing and control data captured at each time point $k$.

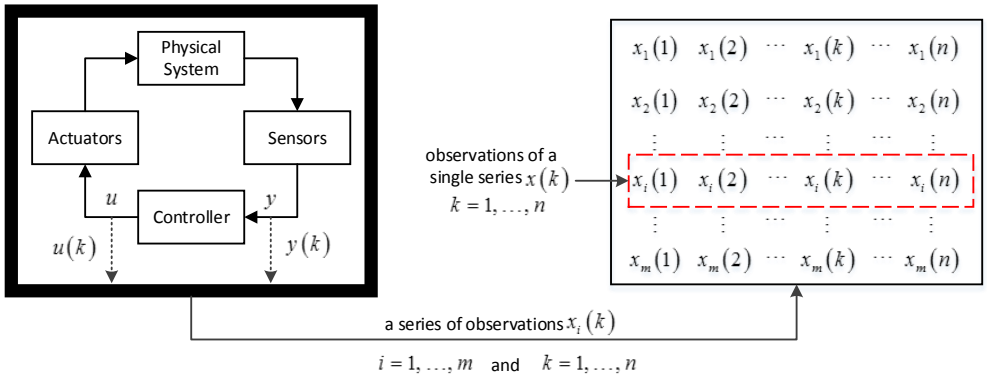


**Figure 1. Abstraction of a Control System**

Consider the observations of a single series $x(k)$ randomly selected from the series of observations $x_i(k)$. In general, as shown in Figure 2(a), there may be two types of limits: (1) limits of the normal operations, and (2) limits of equipment protection. If the former are exceeded, the normal process may be disrupted. If the latter are exceeded, the process will be shut down. Assume that the attacker doesn't know both of the two types of limits. In order to affect the system operation and move the physical process into an unsafe state, the attacker has to make the attack value as close as possible to the high limits or the low limits.

For a process variable, if it does have the limits, then there must be a normal value that is closest to its high limits or its low limits in the whole process. We name such value as the "global optimal point" of the attack. However, in fact, it is almost impossible for the attacker to get the global optimum. On the one hand, the attacker may have already missed the chance to capture this value when he penetrates the control system. On the other hand, the attacker without any prior quantitative knowledge is unable to tell whether the current value is the global optimum or not, unless the whole process is completed, which means the attacker has lost the chance to attack the variable.

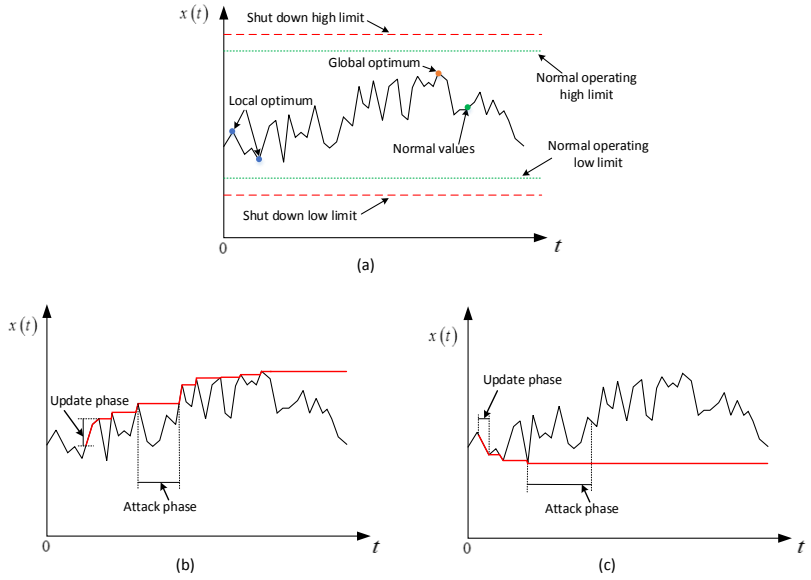


**Figure 2. The Greedy Attack Strategy. (a) Types of Limits; (b) the GM-Max Mode; and (c) the GM-Min Mode**

Compared with the global optimum, the local optimum is a more practical choice for the attacker, *i.e.*, the local peak or valley value, as shown in Figure 2(a). By continually updating the local optimum, the attacker can get a value as close as possible to the global optimum. However, due to the possibility of having a better value in the future, the attacker has to decide when to stop updating the attack value and to modify the normal value.

The core idea of the Greedy Attack Strategy (GAS) is that it always takes the best immediate choice, namely the nearest local optimum, and iteratively applies the GAS to approximate the global optimum which is hard to obtain directly. To be specific, the GAS mainly consists of two behaviors: 1) the update behavior and 2) the attack behavior. The former will update the attack value when a higher peak or a lower valley is captured; the latter will modify the value if it is higher than the selected valley or lower than the selected peak. The period of performing the update behavior is called the update phase, and the period of performing the attack behavior is called the attack phase.

Based on the GAS, we provide two Greedy Modes (GMs): 1) the maximized mode and 2) the minimized mode. For the GM-Max mode, as shown in Figure 2(b), the attack value is always updated towards a higher peak in order to approximate the normal operating high limit or the shut-down high limit. For the GM-Min mode, as shown in Figure 2(c), the attack value is always updated towards a lower valley in order to approximate the normal operating low limit or the shut-down low limit. Moreover, the term greedy in the expression "greedy attack" means that once the attack begins, it will not stop until it exhausts the available resources, *i.e.*, the disclosure resources and the disruption resources [17]. Next, the two GMs will be respectively described in detail by the formalized models.

### 2.2. Attack Models

Consider a control system that has $p$ sensor variables and $q$ control variables. Assume that at least one of these variables has been compromised by the attacker, that is, the attacker can both gather and modify the values of this variable.

Select any one of these compromised variables and the G-Max attack corresponding to this variable can be modeled as

 

$$\hat{x}(t_k)=\begin{cases} x(t_0) & for\ k=0 \\ \hat{x}(t_{k-1}) & for\ k>0\ and\ x(t_k)\le \hat{x}(t_{k-1}) \\ x(t_k) & for\ k>0\ and\ x(t_k)>\hat{x}(t_{k-1}) \end{cases} \quad (1)$$

where $t_k$ denotes the sampling instant of time with $k=0,1,\ldots,n$ and $n<\infty$; $x(t_k)$ is the normal value of the variable captured by the attacker at time $t_k$; $\hat{x}(t_k)$ is the attack value used to replace the corresponding normal value at time $t_k$.

Similarly, the G-Min attack corresponding to this variable can be modeled as

$$\hat{x}(t_k)=\begin{cases} x(t_0) & for\ k=0 \\ \hat{x}(t_{k-1}) & for\ k>0\ and\ x(t_k)>\hat{x}(t_{k-1}) \\ x(t_k) & for\ k>0\ and\ x(t_k)\le \hat{x}(t_{k-1}) \end{cases} \quad (2)$$

## 3. Experiment Overview

To test the attacks, we use the Tennessee-Eastman (TE) chemical process, which is simulated in the MATLAB/SIMULINK. This section briefly introduces the TE process, the setup of the experiments and the assessment methods, which will be used to compare and analyze the experimental results in Section 4.

### 3.1. Tennessee-Eastman Chemical Process

The TE process is a well-known case in the process control field. The TE model, based on an actual industrial process, is proposed by Down and Vogel [18] for the purpose of studying and evaluating process control technology. The process produces two products from four reactants. The main reactions are:

$$A(g) + C(g) + D(g) \rightarrow G(liq), \quad \text{Product 1},$$
$$A(g) + C(g) + E(g) \rightarrow H(liq), \quad \text{Product 2}.$$

As shown in Figure 3, it has five major unit operations: the reactor, the product condenser, the vapor-liquid separator, the recycle compressor and the product stripper. The process has 41 measurements variables XMEAS {1-41} and 12 manipulated variables XMV {1-12}. There are 20 disturbance modes IDV {1-20} and six modes of process operation at three different G/H mass ratios. Details about these parameters are available in the paper [18].

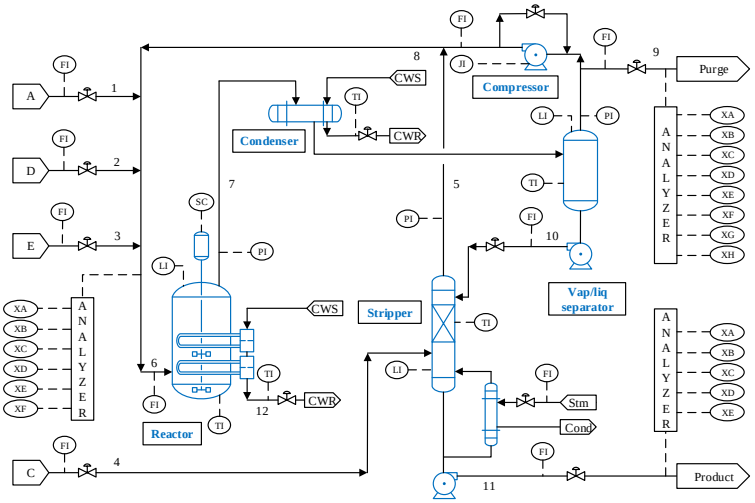


**Figure 3. The Tennessee-Eastman Process**

### 3.2. Experiment Setup

The original TE process does not include any control strategy, and it has more manipulated variables than necessary for controlling. There have been various approaches to control the TE process [19]. In our experiments, we use the MATLAB models of the TE process developed by Ricker [20]. These TE models involve the decentralized control strategy [21] and the self-optimizing control strategy [22].

**Table 1. Simulations of the Attack Experiments**

| Simulation number | Mode of process operation | Control strategy | Process disturbance |
|---|---|---|---|
| Simulation 1 (S1) | Mode 1 | decentralized control | No disturbance |
| Simulation 2 (S2) | Mode 1 | decentralized control | IDV(8) |
| Simulation 3 (S3) | Mode 3 | decentralized control | No disturbance |
| Simulation 4 (S4) | Mode 1 | self-optimizing control | No disturbance |

Table 1 lists the four simulation experiments that were conducted to analyze the performance of the proposed attacks in different control conditions. The S1 is used as a baseline reference of the other three simulations. Compared with the baseline simulation, the S2, S3 and S4 are respectively different in process disturbance, mode of process operation, and control strategy. The source code of TE process we used in the experiments can be obtained from the web sites: http://depts.washington.edu/control/LARRY/TE/ download.html.

### 3.3. Assessment Methods

Attacks on the TE process may affect the product rate, the product quality, or the plant safety. In this paper, we focus on the physical impact caused by the attacks. A physical impact on the process means the attack eventually violates the specific constraints, *i.e.*, exceeding the limits of shutdown. For a chemical process, one of the typical control objectives is to keep the process operating conditions within the constraints, which are primarily for the plant safety. Table 2 lists the operational constraints in TE process [18]. The low and high shutdown limits are used to shut down the process in the event that it gets out of hand.

**Table 2. Process Operating Constraints**

| Process variable | Normal operating limits | | Shutdown limits | |
|---|---|---|---|---|
| | Low limit | High limit | Low limit | High limit |
| Reactor pressure | none | 2895 kPa | none | 3000 kPa |
| Reactor level | 50% ($11.8\ m^3$) | 100% ($21.3 m^3$) | $2.0\ m^3$ | $24.0 m^3$ |
| Reactor temperature | none | 150 °C | none | 175 °C |
| Product separator level | 30% ($3.3\ m^3$) | 100% ($9.0\ m^3$) | $1.0\ m^3$ | $12.0\ m^3$ |
| Stripper base level | 30% ($3.5\ m^3$) | 100% ($6.6\ m^3$) | $1.0\ m^3$ | $8.0\ m^3$ |

In order to compare and analyze the experimental results, three indicators for the performance assessment are used and they are defined as follows：

- Consumed Time (CT), denoted by $\tau_{ct}$. It is the time from the start of the attack until the shutdown of the process. The lower the consumed time, the more effective the attack. The term “effective” means that the attack makes the process shut down within the simulation time period.
- Attack Validity (AV), denoted by $\rho_{av} = m / n$. The term $m$ denotes the number of the effective attacks and the term $n$ denotes the total number of the attacks in one experiment. A high value of the attack validity means the adversary has a high probability of success to attack this process.

 

- Attack Cost (AC), denoted by $\eta_{ae} = \left( \sum_{i=1}^{m} \tau_{ct}^{i} \right) / m$. It is the average consumed time of all the effective attack in one experiment. For the case of the same $\rho_{av}$, the lower the attack cost, the more efficient the attack.

The above indicators provide a way to quantitatively evaluate the performance of the attacks performed in the experiments. In the next section, we will show the details of how to use them.

## 4. Experimental Results

This section presents the results of the performed experiments. The experimental environment consists of four simulations, *i.e.*, S1, S2, S3 and S4. There are two groups of tests in each simulation. One is used to compare the GMs with the prior knowledge-based attacks, and the other is used to assess the AV and AC of the GMs. The attacks carried out in all tests start at t = 0 and persist until the process is shut down. All the simulations are conducted with the default sampling rate of 100s/h, and the simulation time of each test is 50 hours. That is, there will be 5000 samples in a normal simulation. The experimental results are detailed below.

### 4.1. Group 1

In order to compare the effect of the attacks on the TE process with and without prior knowledge, we performed 8 kinds of attacks on 5 process measurements XMEAS {7-9; 12; 15} respectively. These measurements are chosen because they are limited by the operational constraints, which can be considered as the prior knowledge. Besides, Table 3 lists the global optima of the 5 process measurements within 50 hours in different simulations. As previously discussed in Section 2, it is almost impossible for the attacker to identify these global optima, unless the whole process is completed.

**Table 3. Different Limits of the Five Process Measurements**

| Limits | | | XMEAS(7) Reactor Pressure (kPa) | XMEAS(8) Reactor Level (%) | XMEAS(9) Reactor Temperature (°C) | XMEAS(12) Product Separator Level (%) | XMEAS(15) Stripper Base Level (%) |
|---|---|---|---|---|---|---|---|
| Shutdown limits | | Low | -- | 10.5263 | -- | 12.2807 | 22.5806 |
| | | High | 3000 | 126.3158 | 175 | 147.3684 | 180.6452 |
| Normal operating limits | | Low | -- | 50 | -- | 30 | 30 |
| | | High | 2895 | 100 | 150 | 100 | 100 |
| Global optimum (50h) | S1 | Low | 2796.7061 | 63.0394 | 122.8612 | 45.8990 | 46.3230 |
| | | High | 2803.0727 | 66.9921 | 122.9398 | 53.2809 | 54.0234 |
| | S2 | Low | 2697.3774 | 62.0076 | 122.8494 | 40.5485 | 18.1367 |
| | | High | 2830.6626 | 67.7412 | 122.9774 | 62.2822 | 69.3727 |
| | S3 | Low | 2795.4101 | 63.0292 | 121.8451 | 45.8828 | 46.1152 |
| | | High | 2804.0857 | 66.9673 | 121.9443 | 53.3126 | 54.0607 |
| | S4 | Low | 2796.0265 | 63.0512 | 122.8609 | 45.7958 | 46.4632 |
| | | High | 2804.8373 | 66.9258 | 122.9383 | 53.4583 | 53.9608 |

For each process measurement, four Max attacks and four Min attacks are performed:

- Shutdown high limit attack (SD_Max)
- Normal operating high limit attack (NO_Max)
- Global optimum-maximum attack (GO_Max)
- Greedy mode-maximized attack (GM_Max)

- Shutdown low limit attack (SD_Min)
- Normal operating low limit attack (NO_Min)
- Global optimum-minimum attack (GO_Min)
- Greedy mode-minimized attack (GM_Min).

The attacks with prior knowledge are SD_Max, NO_Max, SD_Min and NO_Min. The attacks without prior knowledge are GO_Max, GM_Max, GO_Min and GM_Min. Because there are no shutdown low limit and normal operating low limit on the XMEAS (7) and XMEAS (9), the corresponding attacks (*i.e.*, SD_Min and NO_Min) are not performed. Table 4 lists the consumed time of the eight attacks in four different simulations.

**Table 4. Results of the Eight Attacks in Different Simulations**

| Type | Variable number | SD_Min (h) | SD_Max (h) | NO_Min (h) | NO_Max (h) | GO_Min (h) | GO_Max (h) | GM_Min (h) | GM_Max (h) |
|---|---|---|---|---|---|---|---|---|---|
| S1 | XMEAS(7) | | - | | - | 6.571 | - | 7.6045 | - |
| | XMEAS(8) | 0.4005 | 0.4300 | 0.5695 | 0.5220 | 2.9990 | 2.9755 | 3.8340 | 3.5885 |
| | XMEAS(9) | | 0.1005 | | 0.1005 | 3.2245 | 0.7490 | 4.6195 | 1.7120 |
| | XMEAS(12) | 1.3170 | 0.4605 | 3.2390 | 0.8520 | 9.6580 | 7.6455 | 11.6110 | 8.6310 |
| | XMEAS(15) | 4.4340 | 1.3930 | 5.5040 | 2.9365 | 15.8505 | 14.4940 | 17.9565 | 17.8710 |
| S2 | XMEAS(7) | | - | | - | 5.906 | - | 7.6045 | - |
| | XMEAS(8) | 0.4005 | 0.4300 | 0.5695 | 0.5220 | 2.3120 | 2.4750 | 3.8340 | 3.5885 |
| | XMEAS(9) | | 0.1005 | | 0.1005 | 2.5440 | 0.4850 | 4.6195 | 1.7120 |
| | XMEAS(12) | 1.3170 | 0.4605 | 3.2390 | 0.8520 | 5.6060 | 3.0480 | 11.5730 | 8.6835 |
| | XMEAS(15) | 4.4340 | 1.3930 | 5.5040 | 2.9365 | 3.9970 | 5.5340 | 17.5435 | 18.0955 |
| S3 | XMEAS(7) | | 6.1925 | | 6.2590 | 7.4725 | 9.8930 | 7.6685 | 16.1085 |
| | XMEAS(8) | 0.3435 | 0.908 | 1.667 | 0.9230 | 4.3585 | 3.2865 | 5.2675 | 3.8920 |
| | XMEAS(9) | | 0.1005 | | 0.1005 | 2.3120 | 1.4090 | 6.0935 | 2.3295 |
| | XMEAS(12) | 1.3895 | 0.5705 | 2.9250 | 1.0435 | 10.2285 | 8.5220 | 12.5480 | 9.1915 |
| | XMEAS(15) | 5.0200 | 1.8105 | 6.2075 | 3.3880 | 16.9850 | 16.6895 | 19.8580 | 20.3260 |
| S4 | XMEAS(7) | | - | | - | 8.7885 | - | 10.2075 | - |
| | XMEAS(8) | 0.3995 | 0.4325 | 0.5725 | 0.5240 | 3.1080 | 3.1255 | 3.9425 | 3.7870 |
| | XMEAS(9) | | 0.1005 | | 0.1005 | 1.4980 | 0.7080 | 4.5475 | 0.9910 |
| | XMEAS(12) | 1.3150 | 0.4605 | 3.0955 | 0.8540 | 9.3230 | 7.2625 | 11.4375 | 8.5150 |
| | XMEAS(15) | 4.3765 | 1.3920 | 5.4195 | 2.9210 | 15.8190 | 14.8085 | 18.7315 | 16.8110 |

Figure 4 compares the results of the four Min attacks. For the same simulation, as can be seen from each column of Figure 4, the consumed time of these attacks on different process measurements is different. The attacks on XMEAS {8; 9} consume less time to shut down the process than the attacks on XMEAS {7; 12; 15}. For the same process measurement, as can be seen from each row of Figure 4, the Min attacks without prior knowledge consume more time to shut down the process than the Min attacks with prior knowledge, and such difference varies greatly with different process measurements. The consumed time of the GO_Min and GM_Min attack on XMEAS (8) is the closest to the results of the SD_Min and NO_Min attack.

For the same simulation and the same process measurement, the consumed time of the GM_Min attack is generally longer than the GO_Min attack, but the difference is not significant. Specially, the consumed time of the GO_Min attack on XMEAS {12; 15} has a great difference between S2 and S1, but the corresponding result of GM_Min attack have not changed much. This indicates that a random disturbance may change the global

 

optimum and thus affect the result of the GO_Min attack. However, this result on its own doesn't mean that the random disturbance has no impact on the GM_Min attack, and this point will be further discussed in the section of Group 2.

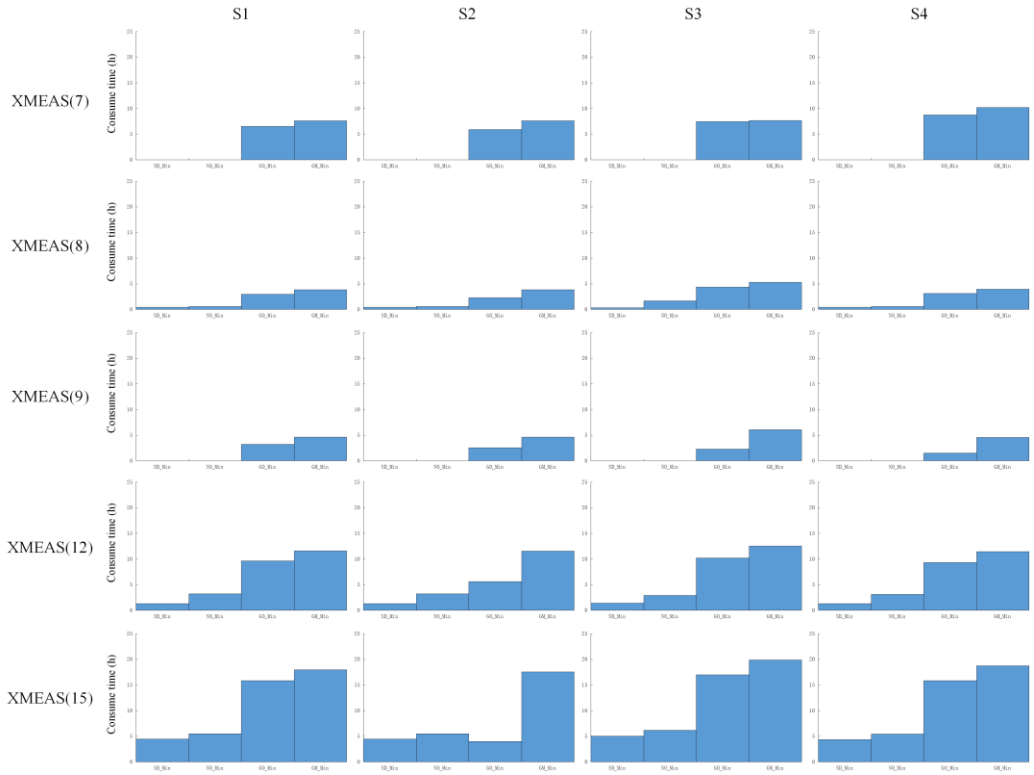


**Figure 4. Results of the Min Attacks on XMEAS {7-9; 12; 15} in Four Simulations**

Figure 5 compares the results of the four Max attacks. Similar to the case of the Min attacks, the consumed time of the Max attacks on different process measurements is also different. The attacks on XMEAS {8; 9} consume less time to shut down the process than the attacks on XMEAS {12; 15}. Besides, all the Max attacks on XMEAS (7) cannot shut the process down within 50 hours in the simulation S1, S2 and S4, but they are effective in the simulation S3. Such result shows that the effectiveness of the attack on a process variable is related to the mode of the process operation. As can be seen from each row of Figure 5, the Max attacks without prior knowledge also consume more time to shut down the process than the Max attacks with prior knowledge.

Among all the process measurements, the consumed time of the GO_Max and GM_Max attack on XMEAS (9) is the closest to the results of the SD_Max and NO_Max attack. For the same simulation and the same process measurement, the consumed time of the GM_Max attack is generally longer than the GO_Max attack. In the simulation S2, the consumed time of the GO_Max attack on XMEAS {12; 15} is significantly lower than the results in the simulation S1, and this once again suggests that the random disturbance can change the global optimum.

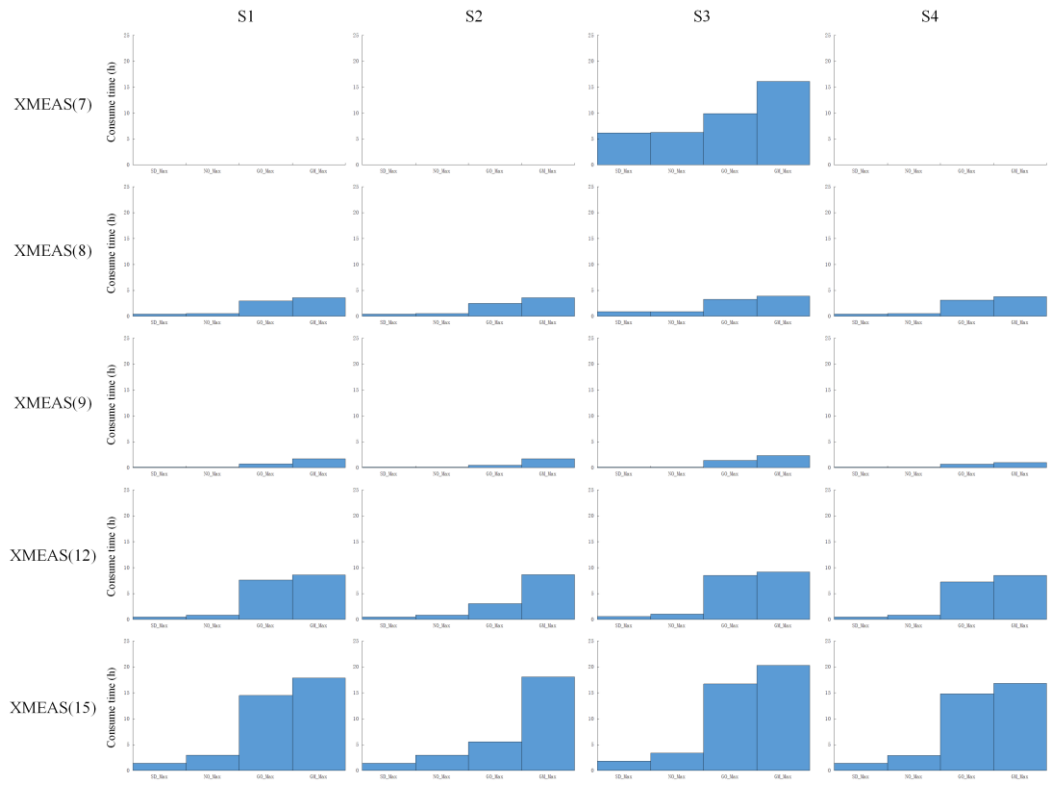


**Figure 5. Results of the Max Attacks on XMEAS {7-9; 12; 15} in Four Simulations**

In summary, according to the results from Figure 4 and Figure 5, the attacks without prior knowledge consume more time to shut down the process than the attacks with prior knowledge. Furthermore, the GMs generally consume more time than the global optimum attacks, but the differences between them are not significant. Besides, from an overall perspective, not all the consumed time of the GMs is higher than that of the attacks with prior knowledge. For example, in the simulation S1, the consumed time of the GM_Min on XMEAS (8) is 3.8340 hours, while the consumed time of the SD_Min on XMEAS (15) is 4.4340 hours.

### 4.2. Group 2

In order to assess the attack validity (AV) and the attack cost (AC) of the GMs, the GM_Min attack and the GM_Max attack are performed in the four different simulations respectively. As previously mentioned, the TE process has 53 variables that are more than necessary for controlling, so not all the variables are used in the attack tests. The simulation S1 and S2 involve nine manipulated variables XMV {1-4; 6-8; 10-11} and sixteen measurements variables XMEAS {1-4; 7-12; 14-15; 17; 23; 25; 40}. The simulation S3 involves ten manipulated variables XMV {1-8; 10-11} and sixteen measurements variables XMEAS {1-4; 7-12; 14-15; 17; 23; 25; 40}. The simulation S4 involves nine manipulated variables XMV {1-4; 6-8; 10-11} and sixteen measurements variables XMEAS {1-5; 7-12; 14-15; 17; 31; 40}. The variables we used in the tests are identified primarily based on the process operation mode and the control strategy of the MATLAB TE models [17]. In addition, although the XMV {9; 12} are also used to control the TE process in the S3, they are not considered in the tests for the reason that the value of them is fixed. This is the same with the XMV {5; 9; 12} in the S1, S2 and S4. In all the simulations, the attack affects only one variable in each test. That is, in the S1, S2 and S4, there are 25 GM_Min attacks and 25 GM_Max attacks; in the S3, there are 26

 

GM_Min attacks and 26 GM_Max attacks. Based on the consumed time of each attack, Table 5 lists the results of the AV and the AC, which are calculated by the method proposed in Section 3.

**Table 5. The AV and AC of the GMs in Four Simulations**

| Simulation type | Variable group | AV | | AC | |
|---|---|---|---|---|---|
| | | GM_Min | GM_Max | GM_Min (h) | GM_Max (h) |
| S1 | XMV | 0.2222 | 0.4444 | 16.0838 | 17.1088 |
| | XMEAS | 0.6250 | 0.5625 | 16.9632 | 13.5798 |
| | ALL | 0.4800 | 0.5200 | 16.8166 | 14.6656 |
| S2 | XMV | 0.5556 | 0.4444 | 26.4207 | 19.5878 |
| | XMEAS | 0.6875 | 0.6875 | 18.8612 | 18.1902 |
| | ALL | 0.6400 | 0.6000 | 21.2235 | 18.5629 |
| S3 | XMV | 0.1000 | 0.4000 | 35.7375 | 32.1269 |
| | XMEAS | 0.6250 | 0.6875 | 14.3296 | 12.4626 |
| | ALL | 0.4231 | 0.5769 | 16.2758 | 17.7064 |
| S4 | XMV | 0.2222 | 0.3333 | 21.0473 | 11.7340 |
| | XMEAS | 0.6875 | 0.6250 | 12.4585 | 10.7520 |
| | ALL | 0.5200 | 0.5200 | 13.7799 | 10.9786 |

Figure 6 shows the attack validity of the GMs attacks in four simulations. As can be seen from Figure 6(a) and 6(b), the GMs on the XMEAS are more effective than the GMs on the XMV. The results from Figure 6(c) present that the GM_Min attacks on the XMV are more easily affected by control condition change than the GM_Max attacks on the XMV. From Figure 6(c) and 6(d), it can be observed that the GMs on the XMEAS are more effective and more reliable than the GMs on the XMV.

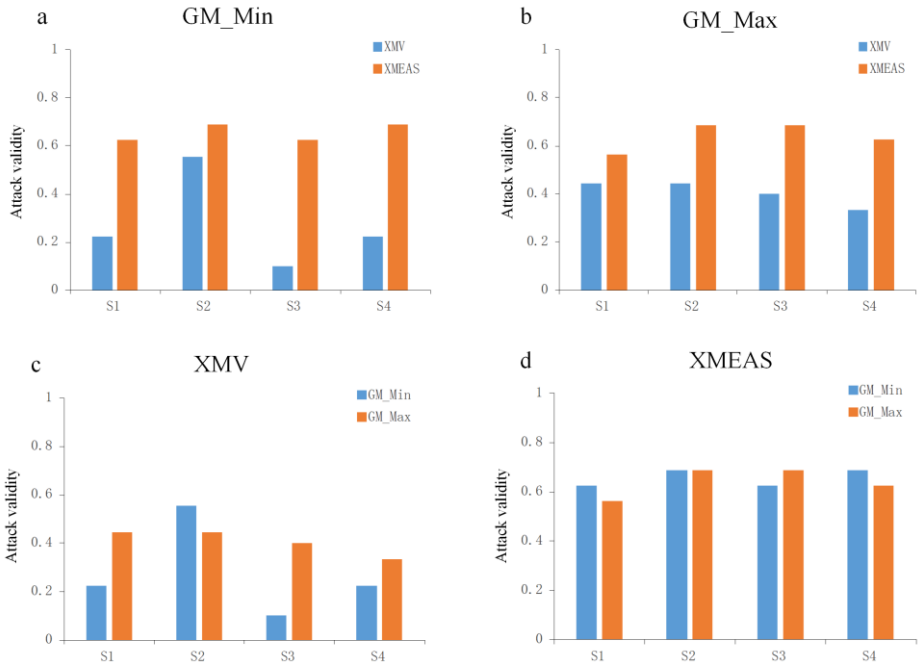


**Figure 6. The Attack Validity of the GMs on the XMV and the XMEAS in Four Simulations**

Figure 7 shows the attack cost of the GMs attacks in four simulations. As can be seen from Figure 7(a) and 7(b), the AC of the GMs on the XMV is generally higher than the AC of the GMs on the XMEAS, which means the GMs on the XMEAS are more efficient than the GMs on the XMV. From Figure 7(c) and 7(d), it can be observed that the GMs on the XMV are more easily affected by control condition change than the GMs on the XMEAS.

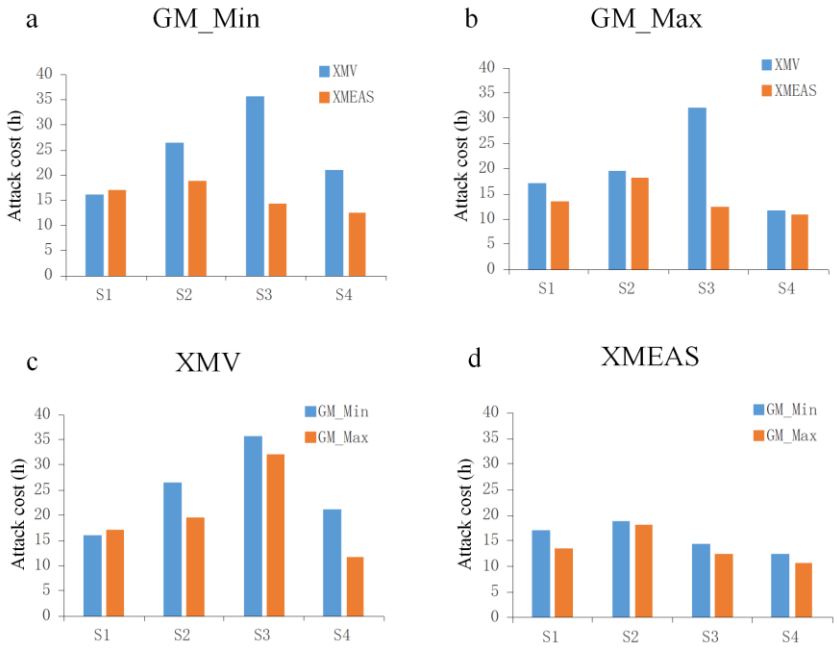


**Figure 7. The Attack Cost of the GMs on the XMV and XMEAS in Four Simulations**

In summary, according to the results from Figure 6 and Figure 7, the GMs on the XMEAS have a higher AV and a lower AC than the GMs on the XMV. Moreover, the GMs on the XMEAS are more reliable in the face of control condition change. Therefore, if the adversary performs the GM_Min or GM_Max attack on the XMEAS of the TE process, there will be a higher probability of success.

## 5. Conclusions

This paper proposed two greedy modes of the data integrity attack based on the greedy attack strategy, which can be implemented very simply and easily. On the one hand, four simulations based on the TE process model are used to compare the greedy attack modes with the prior knowledge-based attacks. The results show that the attacks without prior knowledge consume more time to shut down the process than the attacks with prior knowledge. Furthermore, the greedy attack modes consume more time than the global optimum attacks, but the differences between them are not significant. On the other hand, four simulations are also used to assess the attack validity and the attack cost of the greedy attack modes. The results demonstrate that the GMs on the process measurements have a higher AV and a lower AC than the GMs on the process manipulated variables, which means that the GMs on the process measurements are more effective and more efficient than the GMs on the process manipulated variables. For future work, it would be interesting to explore the method to improve the AV and reduce the AC of the GMs. Specifically, future research directions include narrowing the selection of the process measurements and improving the model of the GMs.

## Acknowledgments

This work is supported by National Key Technologies R&D Program of China (No.2014BAF08B04), National Natural Science Foundation of China (Key Project No.61432004) and the Foundation of Beijing Engineering and Technology Center for Convergence Networks and Ubiquitous Services.

## References

[1] M. Cheminod, L. Durante and A. Valenzano, "Review of security issues in industrial networks", IEEE Transactions on Industrial Informatics, vol. 9, no. 1, **(2013)**, pp. 277-293.
[2] A. Teixeira, K. C. Sou, H. Sandberg and K. H. JohAnSSon, "Secure Control Systems: A Quantitative Risk Management Approach", IEEE Control Systems Magazine, vol. 35, no. 1, (**2015**), pp. 24-45.
[3] M. M. Combs, "Impact of the Stuxnet Virus on Industrial Control Systems", XIII International Forummodern Information Society Formation Problems, Perspectives, Innovation Approaches, (**2011**), pp. 5-10.
[4] Y. L. Huang, A. A. Cárdenas, S. Amin, Z. S. Lin, H. Y. Tsai and S. Sastry, "Understanding the physical and economic consequences of attacks on control systems", International Journal of Critical Infrastructure Protection, vol. 2, no. 3, (**2009**), pp. 73-83.
[5] S. Sridhar and G. Manimaran, "Data integrity attacks and their impacts on SCADA control system", 2010 IEEE Power and Energy Society General Meeting, (**2010**) 1-6.
[6] E. Eyisi and X. Koutsoukos, "Energy-based attack detection in networked control systems", Proceedings of the 3rd international conference on High confidence networked systems, (**2014**) 115-124.
[7] S. Amin, X. Litrico, S. Sastry and A. M. Bayen, "Cyber security of water SCADA systems—part I: analysis and experimentation of stealthy deception attacks", IEEE Transactions on Control Systems Technology, vol. 21, no. 5, (**2013**), pp. 1963-1970.
[8] S. Sridhar S and M. Govindarasu, "Model-based attack detection and mitigation for automatic generation control", IEEE Transactions on Smart Grid, vol. 5, no. 2, (**2014**), pp. 580-591.
[9] A. A. Cárdenas, S. Amin, Z. S. Lin, Y. L. Huang, C. Y. Huang and S. Sastry, "Attacks against process control systems: risk assessment, detection, and response", Proceedings of the 6th ACM symposium on information, computer and communications security, (**2011**) 355-366.
[10] C. Kwon, W. Liu and I. Hwang, "Security analysis for cyber-physical systems against stealthy deception attacks", 2013 American Control Conference, (**2013**) 3344-3349.
[11] K. Manandhar, X. Cao, F. Hu and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter", IEEE Transactions on Control of Network Systems, vol.1, no. 4, (**2014**), pp. 370-379.
[12] R. S. Smith, "Covert misappropriation of networked control systems: Presenting a feedback structure", IEEE Control Systems Magazine, vol. 35, no.1, (**2015**), pp. 82-92.
[13] C. Z. Bai, F. Pasqualetti and V. Gupta, "Security in stochastic control systems: Fundamental limitations and performance bounds", 2015 American Control Conference (ACC), (**2015**), 195-200.
[14] A. Teixeira, H. Sandberg and K. H. Johansson, "Strategic stealthy attacks: The output-to-output l2-gain", 2015 54th IEEE Conference on Decision and Control (CDC), (**2015**) 2582-2587.
[15] Z. H. Pang, G. P. Liu, D. Zhou, F. Y. Hou and D. H. Sun, "Two-channel false data injection attacks against output tracking control of networked systems", IEEE Transactions on Industrial Electronics, vol. 63, no. 5, (**2016**), pp. 3242-3251.
[16] Y. Yuan and Y. Mo, "Security in cyber-physical systems: Controller design against Known-Plaintext Attack", 2015 54th IEEE Conference on Decision and Control (CDC), (**2015**), 5814-5819.
[17] A. Teixeira, I. Shames I, H. Sandberg and K. H. Johansson, "A secure control framework for resource-limited adversaries", Automatica, vol. 51, (**2015**), pp. 135-148.
[18] J. J. Downs and E. F. Vogel, "A plant-wide industrial process control problem", Computers & chemical engineering, vol. 17, no. 3, (**1993**), pp. 245-255.
[19] T. Larsson and S. Skogestad, "Plantwide control-A review and a new design procedure" Modeling, Identification and Control, vol. 21, no. 4, (**2000**), pp. 209.
[20] N. L. Ricker, Tennessee Eastman Challenge Archive, http://depts.washington.edu/control/LARRY/TE/download.html. July, 2016.
[21] N. L. Ricker, "Decentralized control of the Tennessee Eastman challenge process", Journal of Process Control, vol. 6, no. 4, (**1996**), pp. 205-221.
[22] T. Larsson, K. Hestetun, E. Hovland and S. Skogestad, "Self-optimizing control of a large-scale plant: the Tennessee Eastman process", Industrial & engineering chemistry research, vol. 40, no. 22, (**2001**), pp. 4889-4901.

 

## Authors

**Weize Li,** he is currently a Ph.D. candidate in the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. His current research interests include machine learning and industrial control systems security.

**Lun Xie,** he received his Ph.D. degree in control theory and control engineering in 2002 from University of Science and Technology Beijing, China. He is a professor in School of Computer and Communication Engineering, University of Science and Technology Beijing, China. He is a board member of China Artificial Society. His main research interests are security of networked control systems and the artificial intelligence.

**Yu Rong,** he received his B.S. degree in intelligent science and technology in 1987 from University of Science and Technology Beijing, China. He is currently a general manager of Beijing ChenJiGuoTai Science & Technology Co., Ltd in China. His main research interests include metallurgy and control engineering.

**Zhiliang Wang,** he is a professor at the University of Science and Technology Beijing, China. He is a senior board member of China Artificial Society. He received his Ph.D. degree in Harbin Institute of Technology, China. His current research interests include artificial psychology and the Internet of Things.

 