Use the template dedic.tex *together with the Springer document class SVMono for monograph-type books or SVMult for contributed volumes to style a quotation or a dedication at the very beginning of your book in the Springer layout*

Foreword

Use the template *foreword.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style your foreword in the Springer layout.

The foreword covers introductory remarks preceding the text of a book that are written by a *person other than the author or editor* of the book. If applicable, the foreword precedes the preface which is written by the author or editor of the book.

Place, month year *Firstname Surname*

Preface

Use the template *preface.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style your preface in the Springer layout.

A preface is a book's preliminary statement, usually written by the *author or editor* of a work, which states its origin, scope, purpose, plan, and intended audience, and which sometimes includes afterthoughts and acknowledgments of assistance.

When written by a person other than the author, it is called a foreword. The preface or foreword is distinct from the introduction, which deals with the subject of the work.

Customarily *acknowledgments* are included as last part of the preface.

Place(s), *Firstname Surname*
month year *Firstname Surname*

Acknowledgements

Use the template *acknow.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) if you prefer to set your acknowledgement section as a separate chapter instead of including it as last part of your preface.

Contents

Part I Part Title

List of Contributors

Annarita Giani
CNLS, Los Alamos National Laboratory, Los Alamos, NH 87545, USA,
e-mail: annarita@lanl.gov

Ondrej Linda
University of Idaho, Idaho Falls, ID, 83401, USA,
e-mail: olinda@uidaho.edu

Milos Manic
University of Idaho, Idaho Falls, ID, 83401, USA,
e-mail: misko@uidaho.edu

Miles McQueen
Idaho National Laboratory, Idaho Falls, ID, 83401, USA,
e-mail: Miles.McQueen@inl.gov

Acronyms

Use the template *acronym.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style your list(s) of abbreviations or symbols in the Springer layout.

Lists of abbreviations, symbols and the like are easily formatted with the help of the Springer-enhanced `description` environment.

ABC	Spelled-out abbreviation and definition
BABI	Spelled-out abbreviation and definition
CABR	Spelled-out abbreviation and definition

Part I
Part Title

Use the template *part.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style your part title page and, if desired, a short introductory text (maximum one page) on its verso page in the Springer layout.

Chapter 1
Known Secure Sensor Measurements Concept and Its Application for Critical Infrastructure Systems

Annarita Giani, Ondrej Linda, Milos Manic, Miles McQueen

Abstract The manipulation of critical physical processes and the falsification of system state is a relevant concern for many modern control systems. Common approaches to this problem such as network traffic and host based state information analysis feature difficulties such as high false alarm rate. Furthermore, issues in integrating the system state falsification detection into an existing control system such as cost or technical issues, impose additional difficulties. To alleviate these issues, a low cost and low false alarm rate method for improved cyber-state awareness of critical control systems, the Known Secure Sensor Measurements (KSSM) method, was proposed by the authors of this chapter. This chapter reviews the previously developed theoretical KSSM concept and then describes a simulation of the KSSM system.

The presented KSSM method constitutes a reliable mechanism for detecting manipulation of critical physical processes and falsification of system state. Unlike other network based approaches, the method utilizes the physical measurements of the process being controlled to detect falsification of state. In addition, the KSSM method can be incrementally integrated with existing control systems for critical infrastructures. To demonstrate the performance and effectiveness in detecting various intrusion scenarios, a simulated experimental control system network was combined with the KSSM components. The KSSM method is intended to be incorporated into the design of new, resilient, cost effective critical infrastructure control systems.

Annarita Giani
CNLS, Los Alamos National Laboratory, e-mail: annarita@lanl.gov

Ondrej Linda
University of Idaho, e-mail: olinda@uidaho.edu

Milos Manic
University of Idaho, e-mail: misko@uidaho.edu

Miles McQueen
Idaho National Laboratory, e-mail: Miles.McQueen@inl.gov

1.1 Introduction

Resiliency and enhanced state-awareness are crucial properties of modern control systems. Critical infrastructures, such as energy and industrial systems, would benefit from being equipped with intelligent components for timely reporting and understanding of the status of the control system. This goal can be achieved via complex system monitoring, real-time system behavior analysis and timely reporting of the system state to the responsible human operators [1].

In [2] a resilient control system was defined as follows: *" one that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature"*. Here, the enhanced state-awareness is understood as a set of diverse performance criteria such as cyber or intelligent analysis that is used to maximize the adaptive capacity of the system to respond to threats.

Falsification of physical system state can pose significant danger to the operation of a control system. An intelligent adversary attempts to deceive the operator with the intention to achieve desired manipulation of the control system without early detection. An intuitive way for achieving this task is modification of physical measurement values sent to the operators by injecting false information. Hence, protection of measurement values is of high importance. There exist cryptographic techniques that provide sufficient level of information protection [3, 4]. However these techniques require increased computational cycles, increased power, and higher available network bandwidth, which might not be available on many currently deployed control systems.

To address these issues, a novel, low cost, low false alarm rate, and high reliability detection technique for identifying manipulation of critical physical process and falsification of system state was previously proposed [5, 6]. This technique, called Known Secure Sensor Measurements (KSSM), uses the idea of obtaining a randomly selected subset of encrypted (i.e. known secure) physical measurements that are sent in sequence after the plain-text (i.e. insecure and unencrypted) measurements used for control. The subsequent comparison of the randomly selected plain-text and the known secure values reveals potential system falsification. By randomly modifying this selected subset of KSSM sensors, a complex cyber-state awareness of the control system and falsification of system state can be maintained while imposing as little additional computational and bandwidth cost as desired. Hence, by utilizing the physical measurements themselves for aiding cyber-security, the KSSM method differs from traditional approaches to network system security such as anomaly or signature detection systems [7, 8, 9, 10].

A variety of techniques for protecting critical infrastructure control systems from cyber attacks have been proposed. These proposals have included cryptographic techniques such as those recommended in AGA-12 [12, 13], intrusion detection for industrial control systems [14, 15], use of deception [16], and many other general techniques and concepts for securing IT systems from cyber attack which have been adapted to control systems. While all of these adaptations seem to have some merit for protecting control systems, relatively few have focused on the fundamentally unique aspects of general control systems, which in our view is that they control a physical process; have much longer life cycles than standard IT systems; and may have severe resource constraints, including cost. There are exceptions to this of course, such as the large body of research into protecting the electric power grid, see for example [6, 17]. The Known Secure Sensor Measurement technique described in this chapter is unique in that it blends IT security concepts with the physical processes measurement and control in order to enhance the detection of an attack on the physical process even if the entire communication infrastructure has been compromised through a cyber attack.

In this chapter we first explain the KSSM concept, including the technical objectives and research approach and then we will show on specific simulation examples how the KSSM system could be implemented. The overall architecture of the system is presented, followed by description of the two major components, Sensor Selector and Signal Analyzer. The Sensor Selector uses an algorithm to perform pseudo-random sensor selection based on multiple criteria. The Signal Analyzer contains a buffer of requested KSSM values and performs measurement comparison and system state falsification detection. The designed KSSM system architecture was integrated with a virtual control system communication network. The performance of the system is demonstrated on several test scenarios. As a practical application we show how the generalized concept of known secure sensor measurement can be used as a countermeasure against a collection of data integrity attack to the smart grid.

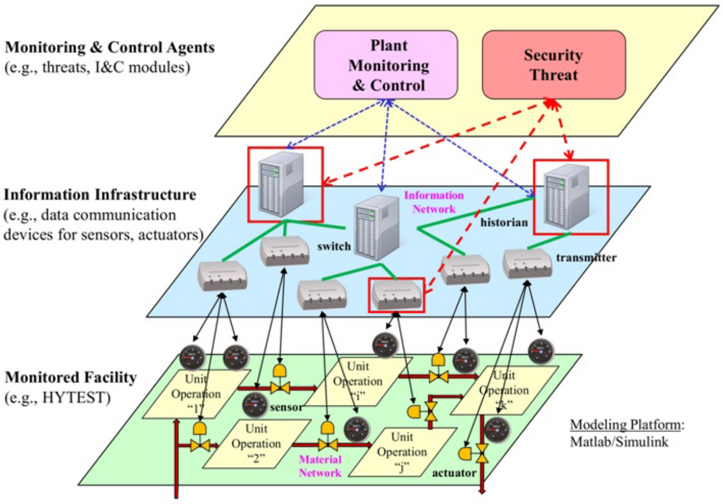


Fig. 1.1 Hybrid energy production facility.

This chapter provides an overview of the previously published work on the KSSM concept [1, 5].

1.2 Known Secure Sensor Measurement Concept

The concept of Known Secure Sensor Measurements was previously proposed in [5]. The KSSM technique constitutes a novel low cost, low false alarm rate, and high reliability detection technique for identifying malicious manipulation of critical physical processes and the associated falsification of system state. The fundamental idea of the method is to obtain a randomly selected subset of encrypted (known secure) physical measurements that are sent in sequence together with the plain-text (unencrypted) measurements used for control. The comparison of the randomly selected plain-text and KSSM values reveals potential falsification of system state.

The developed KSSM concept is targeted for critical infrastructure control systems that lack robust cryptographic techniques and have limited computational and communication bandwidth resources. It is important to note here that most critical infrastructures fit well within this targeted group. Hence, the KSSM method is widely applicable.

The fundamental assumption of the KSSM method is that the intelligent attacker is able to compromise any of the components in the information layer of the control system. The information layer is a communication layer which communicates physical process measurements to the process control layer, where they are presented to the operator. Figure 1.1 depicts an exemplary hybrid energy production system with highlighted physical, information and process control layers. In addition, it is assumed that the attacker will not be detected in the system as long as no transmitted measurement values are modified or blocked. It is important to emphasize here that the KSSM concept is intended not to detect anomalous process activity or whether the system functions within its normal operation envelope. Instead, the KSSM concept is designed to verify the system state information presented to the operator and reject system state falsification due to adversarial sensor measurement value corruption.

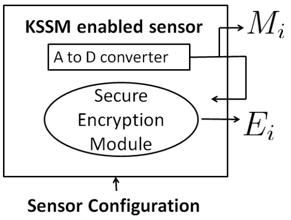


Fig. 1.2 Sample KSSM enabled sensor.

The main hypothesis of the KSSM concept is the idea that a small subset of sensor measurements, which are known to be secure (i.e. cannot be falsified in the physical layer), has the potential to significantly improve the observability of adversarial process manipulation due to cyber-attack. Furthermore, randomly selecting this small subset of known secure sensors can make more difficult for the attacker to identify which sensors measurements are being secured at particular time. Finally, it is assumed that there is only limited communication bandwidth available and the size of the selected KSSM sensor subset can be selected such that the real-time control of the system is not disrupted. We will describe in more detail these hypotheses in section 1.3.2.

In order to allow protection against an intelligent adversary, it must be possible to trust specific components of the system. In the KSSM system a cryptographic sensor module constitutes this trusted component as depicted in figure 1.2. The cryptographic sensor may be KSSM enabled with software or hardware as a mean to forward the plain-text measurement value M_i through a secure encryption module to produce a KSSM value E_i. If the particular sensor is part of the randomly selected subset of KSSM sensors, the encrypted measurement value E_i is sent to the control room after the plain-text measurement M_i.

The KSSM control module resides in the control room of the plant. The module is responsible for performing selection of the random subset of KSSM-enabled sensors. In addition, the control module also compares the received KSSM values with the plain-text measurements in order to detect falsification of the system state.

1.2.1 Attack Scenarios

While not required, we assume that all process sensors are KSSM hardware or software enabled, all encryption modules are secure from cyber attack, and the KSSM control room module, including the detection engine, are secure. Any other component in the system, including the entire information infrastructure layer may be assumed to be compromised by an attacker.

Figure 1.3 presents two scenarios. The system in scenario 1 has no KSSM sensors available. The adversary has compromised choke points in the communication network and is behaving as a man in the middle by preventing all valid sensor signals to the control room and replacing them with corrupted, signals C_i. This deception could be done, as Stuxnet partially demonstrated, through collection and then replay of sensor measurement data. The attacker is now able to manipulate the process as desired while the operators remain completely unaware. This level of attack may be undetectable without KSSM and will leave the operators completely blind to the actual system state.

KSSM sensors are available in scenario 2 and the attacker is choosing to corrupt only those signals which he knows are not providing encrypted values back to the detection engine. If the attacker corrupted the signals for which an encrypted ver-

SCENARIO 1 **SCENARIO 2**

$$M_i \to C_i \qquad M_i \to C_i \vee M_i \vee (C_i \wedge E_i) \vee (M_i \wedge E_i) \qquad \text{for all } i = 1 \text{ to } N.$$

Fig. 1.3 M_i is the measurement from sensor i. C_i is the corrupted version of measurement M_i. E_i is the encrypted version of measurement M_i. $\vee$ and $\wedge$ are the logic disjunction and conjunction.

sion was sent at a later time then the corruption would be instantly recognized by the KSSM detector. Given that the encrypted signals are sent at some δ time after the unencrypted signal the attacker can only know which sensors will provide the encrypted signal by observing the network traffic for some period of time.
The attack in figure 1.4 consists on corrupting signals and blocking some of the encrypted versions. In fact attack would be easily detectable if the encrypted version of the measurement reached the detection engine and be compared against the corrupted version.
A way to make the above attack more difficult is to *periodically and unpredictably modify the subset of sensors providing encrypted values*. This ongoing and unpredictable selection of new sensors (and deselection of others) may be based on current system state, or communication network topology (for example not selecting KSSM sensors such that their encrypted measurements are all going through the same router).

SCENARIO 3

$$M_i \to C_i \vee M_i \vee (C_i \wedge E_i) \vee (M_i \wedge E_i) \vee (C_i \wedge \underset{\underset{\text{BLOCKED}}{\uparrow}}{E_i}) \quad \text{for all } i = 1 \text{ to } N$$

Fig. 1.4 Attacker identifies which sensors are providing encrypted versions of measurements. During the attack only a few of the sensors are blocked.

Figure 1.5 schematically depicts the considered system state falsification scenarios and the counter-measures used by the KSSM system. The plain system state falsification is demonstrated in figure 1.5 (scenario 1). Here, the sensor measurements M_i are potentially corrupted by the attacker within the information layer. The falsified measurement values C_i reach the control operator. The basic idea of the KSSM system is depicted in figure 1.5 (Scenario 2), where a subset of the KSSM-enabled sensors is requested to report encrypted measurement values E_i to the control room. In this specific example, there will be a mismatch between values C_i and the decoded value of E_i. Further, an attacker aware of the KSSM protection system might attempt to deceive the system by blocking the encrypted values E_i from reaching the control room, as shown in figure 1.5 (Scenario 3). However, the KSSM system randomly modifies the subset of KSSM-enabled sensors, thus making it increasingly difficult for the attacker to design an attack with reliable detection delay. This is shown in figure 1.5 (Scenario 4), where the values C_1 and E_1 from the newly selected KSSM-enabled sensor would produce a mismatch and indicate a presence of system state falsification.

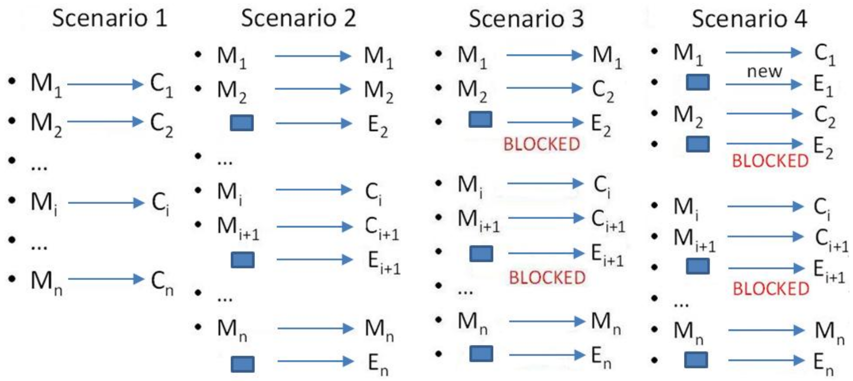


Fig. 1.5 Communication Scenarios.

1.3 Technical Objectives and Research Approach

Our objective is to investigate the value of KSSM for effective detection of unauthorized process manipulation and falsification of system state.

1.3.1 Targeted Facilities

As mentioned before a hypothetical hybrid energy plant is shown in figure 1.1. This figure represents a hybrid energy production facility with three abstract layers. The lowest layer is the physical process which consists of a set of production units each of which consists of reactors, tanks, gas flows, coolers, heaters, valves and other physical components. The information layer, in the middle, is responsible for communication. The sensors in the physical layer communicate with control devices and commands are sent to the edge controllers that drive actuator behavior. The highest layer is represented by the primary functions of plant control, and security threat monitoring and alarming. These highest level functions make use of real time data feeds from the physical plant up through the communication layer, and may also make use of information derived over time through initial monitoring of the system (e.g. passive network discovery).

We assume that the attacker can compromise any of the components in the information layer without being detected as long as the attacker does not modify the sensor signals being transmitted back to the controller and the control room. KSSM is not designed to detect the system process exceeding its operational performance envelope, normal system monitoring is expected to detect that situation.

1.3.2 KSSM System Hypotheses

We created the following four hypotheses to stay focused on the core issues in conceptualizing, designing, and validating a prototype of a KSSM system.

1. **(H1)** A small set of sensor measurements, which are known to be secure, can significantly aid the operator and detection engine in more quickly and accurately identifying a cyber attack.

2. **(H2)** Some known secure measurements from randomly chosen sets of sensors providing data within selected time frames will harden the process against covert cyber attacks attempting to blind the operator and KSSM detection engine. Neither the enhanced operator effectiveness nor enhanced detection engine performance (gained from using a fixed set of known secure data) will be degraded by the changing and diverse sets of sensors selected for providing the known secure data.

3. **(H3)** It is possible to create a very low cost, limited bandwidth, and highly secure measurement capture and communication channel for transmitting k_i% $(0 < k_i < 100)$ of a chosen sensor's physical measurements, end to end, from sensor to detection engine for analysis. The channel will involve adaptation of known cryptographic protocols to provide message and measurement integrity, and detection of replay attacks. Tradeoffs between cryptographic computational requirements at the sensor, power restrictions of a sensor, network bandwidth limitations, and the speed and accuracy of detection will be assessed in selecting specific cryptographic techniques for KSSM systems and establishing appropriate value for k_i.

4. **(H4)** Heuristics for selecting the set of sensors providing known secure sensor measurements can be developed which allow for the results of this research to be easily adapted for use in the design, implementation, and configuration of many diverse industrial control systems and infrastructures.

In a KSSM enabled infrastructure, the attacker will be unable to reliably falsify the process state to the control room operators.

1.3.3 KSSM Sensor

Figure 1.2 represents a KSSM hardware enabled sensor. The signal from the AD converter is tapped off and available to the secure encryption module. This module, at some randomized time δ after the unencrypted measurement M_i is sent, forwards the encrypted version E_i of the measurement value to the KSSM detection module running on a control room computer. Whether or not the encrypted version of the plaintext measurement is sent depends on whether that particular sensor is currently selected by the KSSM control room module, and whether the secure encryption module selects it as one of the k_i of measurements for which a dual encrypted value will be expected. We note that these sensor functions may also be implemented in software and reside in the sensor or closest computational edge point. The KSSM detection algorithm in the control room, which must also be trusted, will compare the two versions of the measured value, unencrypted and encrypted, and trigger an alarm if there is any difference. For the exposition of the idea in this chapter, we are making simplifying assumptions related to reliable transport of measurements, both plaintext and ciphertext, and to the reliability of the sensor and encryption hardware.

1.3.4 KSSM Control Room Module

The KSSM module residing in the control room is represented in figure 1.6. It is responsible for modifying the subset of KSSM-enabled sensors which perform encryption, and is also responsible for detecting attacks. Many functions are needed to provide these capabilities and we will very briefly describe only the highest level functions.

The *system analyzer* receives input from network discovery tools which can both reside on the system and operate in real time, or can be one time only devices used during a phase such as system acceptance testing. It develops simplified models of the communication network to aid the sensor selection function in choosing smart subsets of sensors.

The *signal analyzer* is responsible for analyzing the sensor measurements that are provided to the control room, and alarming when appropriate. If encrypted and associated unencrypted values do not match then an alarm will be set; if some number of requested encrypted values do not arrive in a timely fashion, and are distributed over a variety of communication paths then it may be appropriate to raise an alarm based on probabilistic assessment of likely communication and sensor failures.

The *sensor selection algorithm* will incorporate what is known about the communication topology and the failure rates of all components within the system. The failure rates may be based on empirical data or models built into the algorithm. Further some understanding of the limits on computation cycles available, sensor power restrictions, and limitations in communication bandwidth will be incorporated to aid, not only the selection of a new subset of sensors for KSSM but also the selection for each chosen sensor of the k_i of measurements that will be encrypted and forwarded.

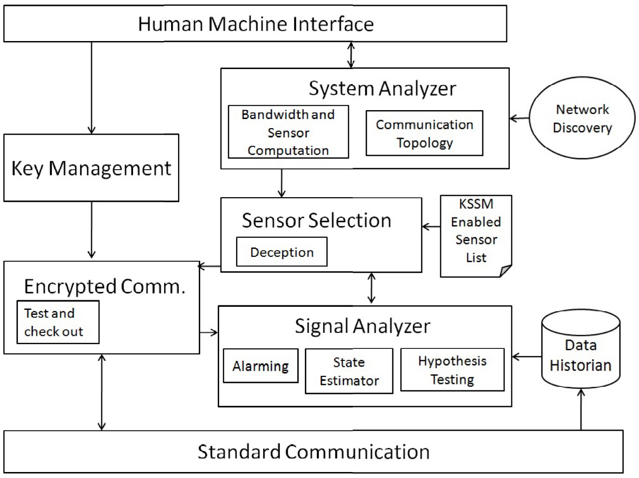


Fig. 1.6 Block diagram of KSSM module residing in the control room.

Sensor selection and the percent of measurements for which dual encrypted values are required may also be made selectable by the operators so that they have control in limiting the sensor processor cycles, sensor power consumption, and communication bandwidth utilized by KSSM

The *cryptographic functions* will be adopted from currently well understood cryptographic components and systems. The KSSM-enabled sensor list is needed so that sensor selection can accommodate systems that are slowly being upgraded with KSSM-enabled sensors. And the KSSM user interface will be separate from all other devices in the control room in order to provide as much hardening against attack as possible.

1.4 Known Secure Sensor Measurement System Simulation

This section describes the design and simulation of the KSSM-equipped control systems. First the overall architecture is presented. Next its major components of Sensor Selector and Signal Analyzer are described in more detail.

1.4.1 KSSM System Architecture

The overall KSSM system architecture is depicted in figure 1.7. The system is composed of two major parts, the KSSM control module and the communication network which connects the control module with those sensors that are KSSM-enabled. The KSSM control module is composed of two main components, the Signal Analyzer and the Sensor Selector. All components monitor network traffic in the control system and communicate among each other to perform effective system state falsification detection while minimizing the impact on the system's communication bandwidth.

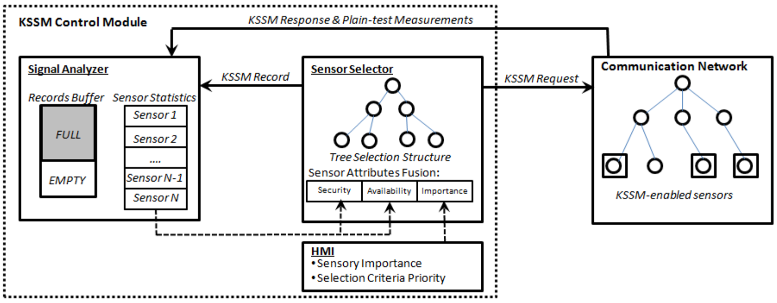


Fig. 1.7 Architecture of the KSSM system.

The Sensor Selector component is responsible for selecting a subset of KSSM-enabled sensors every time iteration. The sensor selection is performed using a tree-like sensor selection data structure, which resembles the known network topology. The Sensor Selector uses several criteria, including subjective human input to calculate the selection weight of each sensor. A randomization algorithm is then applied to ensure representative sensor selection from the communication network. Every time a subset of sensors is selected by the Sensor Selector a KSSM request is sent to the sensors and a KSSM record about the selection is stored in the Signal Analyzer. The Signal Analyzer is responsible for monitoring both the plain-text and the KSSM encrypted network messages. Every time a KSSM record about sensor selection is received from the Sensor Selector, the Signal Analyzer stores the record in a record buffer. Upon receiving the previously requested KSSM message from the network, the KSSM value is paired with its plain-text value stored in the record buffer and their values are compared. The Signal Analyzer also keeps track of important network traffic statistics such as sensor availability and response latency, which are used for adjusting the sensor selection process.

1.4.2 KSSM Sensor Selector

The main task of the Sensor Selector is to perform randomized sensor selection every time iteration. To achieve this, the Sensor Selector contains an approximate model of the network topology in a form of a tree data structure. The root of the tree corresponds to the main communication node of the control system network. Branches connect the root node to possibly multiple levels of nodes. Each node corresponds to a sub-network in the real network system. Finally, leafs of the tree structure correspond to individual KSSM-enabled sensors. It should be noted that it is not required for the tree structure to exactly match the real communication network topology. Rather, the branches of the tree should correspond to logical units in the control system network, in order to achieve evenly distributed sensor selection. The process of sensor selection is performed by randomly descending from the root of the tree to particular leaf. All branches in the selection tree emanating from a particular node are assigned a specific selection probability, which guides the random descending process. This method is repeated until the new subset of KSSM enabled sensors has been selected. The branch selection probabilities are updated after selection of each sensor so that more probability is distributed to the branches that were not assigned. The pseudo-code of this randomized sensor selection algorithm can be summarized as follows:

```
1. Initialize the sensor selection probabilities $p_{ij}$ of each branch in the selection
   tree.
2. Repeat for all $k$ KSSM sensors.
     a. Set current node $n_i$ as root.
     b. Repeat, until current node $n_i$ is a leaf.
          i. Randomly select $j^{th}$ branch of current node ni based on branch selection probabilities
             $p_{ij}$.
         ii. If there exist unselected leafs in the sub tree connected to the $j^{th}$ branch
             descend to the $j^{th}$ children of current node $n_i$.
     c. Return the index of the sensor in the selected leaf.
     d. Repeat until current node $n_i$ is a root
          i. For all siblings of current node $n_i$ compute the new branch selection probability
             from their parent as:
                  $p_{kj} = \begin{cases} p_{kj}(1-\alpha), & \text{if } k=i \\ p_{kj}+\frac{\alpha p_{ij}}{k-1}, & \text{if } k \neq i \end{cases}$
         ii. Ascent to the parent of node $n_i$.
```

Coefficient α controls the spatial diversification of the selected sensors. Values close to 1 will result in large spatial diversification (e.g. sensors sampled in different areas of the network), while values closer to 0 will result in selected sensors being more likely to be close to each other (e.g. in the same sub-network). Parameter k denotes the cardinality of the selected KSSM sensor subset. This process of KSSM enabled sensor selection and selection weight updates is depicted in 1.8. Due to the re-distribution of branch selection weights, the subset of sensors is more likely to be distributed throughout the network. Hence, KSSM and plain text message loss rate due to random component failures in parts of the communication system can be reduced.

After the subset of KSSM enabled sensors has been specified the Sensor Selector re-computes the initial branch selection probabilities in the selection tree to reflect

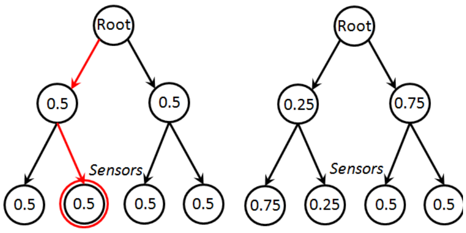


Fig. 1.8 Architecture of the KSSM system.

the most current behavior of the communication system. These recomputed branch selection probabilities are used to initialize the tree parameters in Step 1. This process for computing the initial branch selection probabilities is composed of three parts: 1) sensor selection weight calculation, 2) bottom-up selection weight propagation, and 3) top-down selection probabilities normalization.

The sensor selection weight is calculated for each KSSM-enabled sensor based on a weighted average of three parameters: availability, security and importance. The availability can be computed as the inverse value of the averaged time interval of obtaining the requested KSSM value from the particular sensor. When the sensor response time increases, its availability is decreased and the sensor will be selected less often to ease the work load of the particular sensor and its part of the network.

The security is computed as the averaged time interval between receiving two mismatching KSSM-values and plain text values. Because random noise might corrupt the KSSM messages, single mismatch should not immediately raise an alarm. However, when the frequency of mismatched messages is significantly increased the security is increased, which results in sensor being selected more often to quickly converge to final detection. Here, a significant increase is considered to be an increase above the normal frequency of mismatched measurement values due to ordinary communication noise.

Finally, the importance attributed to a sensor is a subjective value provided by the operator, which can help to fine-tune the selection algorithm (e.g. some sensors might be more important for the control and thus should be sampled more often). In addition, the operator can specify the weighting coefficients for the weighted average of these attributes.

The bottom-up selection weight propagation proceeds in a recursive manner and its purpose is to propagate the sensor selection weights up the tree. The algorithm reads the selection weight from all children into their common parent, the weights are summed and recursively propagated to the higher level until the root node is reached.

In the final stage, the selection weights need to be converted into branch selection probabilities. This is achieved by descending from the tree root to individual leafs and normalizing the selection weights for all branches emanating from each node. The normalization procedure ensures that all branch selection probabilities sum up to 1 for each node.

1.4.3 KSSM Signal Analyzer

The main task of the Signal Analyzer is to monitor the network traffic and detect potential falsification of system state. Every time a KSSM request is sent to a particular sensor a record about this is stored in the record buffer in the Signal Analyzer. Upon receiving the KSSM measurement value, the corresponding plain-text measurement is looked up in the record buffer. The KSSM measurement is decrypted and compared to the plain-text value. A measurement mismatch can be used to indicate a potential presence of an intelligent adversary in the information layer of the system. The intelligent adversary who is aware of the KSSM system might attempt to avoid detection by preventing the KSSM values from reaching the Signal Analyzer. For this reason, the record buffer contains an upper limit on the number of active KSSM records. When a KSSM message is blocked its plain-text counterpart will not be removed from the record buffer and the capacity of the buffer will be decreased. When this capacity reaches the specified threshold, an indication of potential attempt to falsify the system can be reported.

The Signal Analyzer also gathers important network traffic attributes, which are used to adapt the KSSM system to the specifics of the current network traffic. First, the time interval of requesting and receiving a KSSM value is computed for each sensor. This information is used to calculate the availability of individual KSSM-enabled sensors. Next, the time interval between obtaining two mismatched plain-text and KSSM values for each sensor is being monitored. This information is used to calculate the security of individual sensors and used for sensor selection. Finally, the Signal Analyzer stores the response time of obtaining the plain-text measurements, which can be used to monitor and adjust the appropriate size of the requested KSSM sensor subset so that the response of the control system is not affected. This adaptive mechanism is explained below.

The Signal Analyzer monitors the maximum response time of any plain-text sensor and compares that to the requested allowed response time. For example, if the sensor values should be reported to the control room once every second then the maximum allowed response time can be set to 0.8 seconds to create a safety buffer. The difference between maximum and the allowed response time creates a feedback signal that could be used to adjust the number of sampled KSSM sensors so that the real-time system response is not affected. When the maximum response time is below the allowed threshold for a certain period of time, the number k of sampled KSSM sensors is increased by one. Similarly, when the maximum response time is greater then the allowed threshold for certain amount of time, the number k of sampled KSSM sensors is decreased in order to preserve the real-time response of the system.

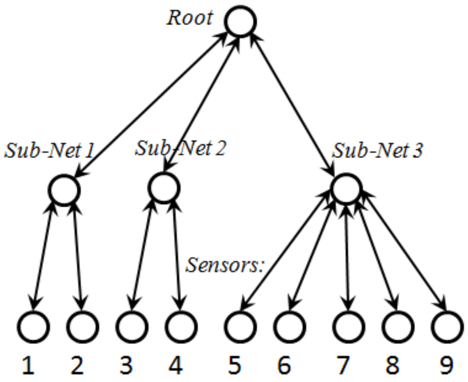


Fig. 1.9 Testing network topology.

1.5 Sensor Selection: Experimental Results

This section first describes the implemented virtual communication network used as an experimental test-bed. Next, a set of testing scenarios is used to demonstrate the performance of the proposed KSSM system.

1.5.1 Experimental Test-Bed

In order to validate the performance of the designed KSSM system a virtual communication network was implemented. The network simulator models packet-based traffic in control system communication networks. The network is composed of communication nodes and sensor nodes. The communication nodes are equipped with packet buffers and routing tables. The packet buffer dispatches packets on first-in first-out basis. The sensor nodes can generate the plain-text measurement value as well as its encrypted version upon request. The network simulator can simulate various deterministic as well as stochastic properties of the network. For example, the desired throughput can be set for individual network nodes as well as stochastic packet loss rates or packet corruption rates. The KSSM Control module is connected to the communication network interface, where KSSM requests can be passed into the network and plain-text and KSSM messages can be received. For the purpose of experimental testing a simple control system communication network was constructed. The network gathers measurements from 9 sensors, which are grouped into 3 sub-networks as depicted in 1.9.

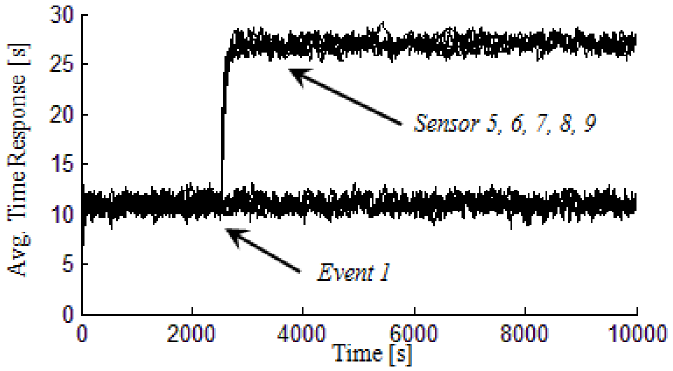


Fig. 1.10 Average time response for various KSSM sensors.

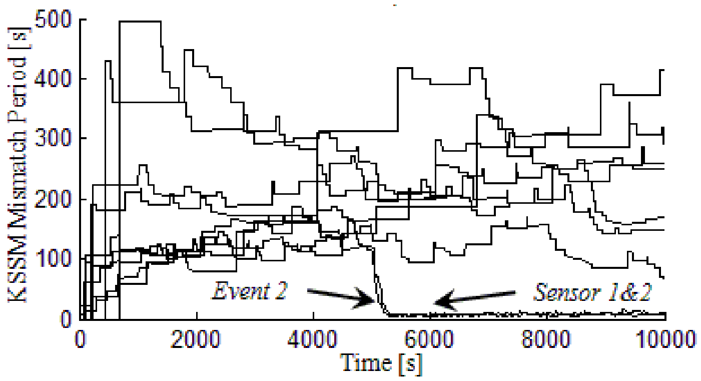


Fig. 1.11 KSSM values mismatch period.

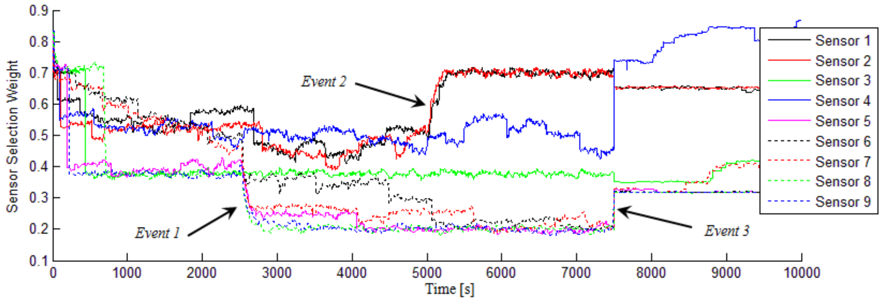


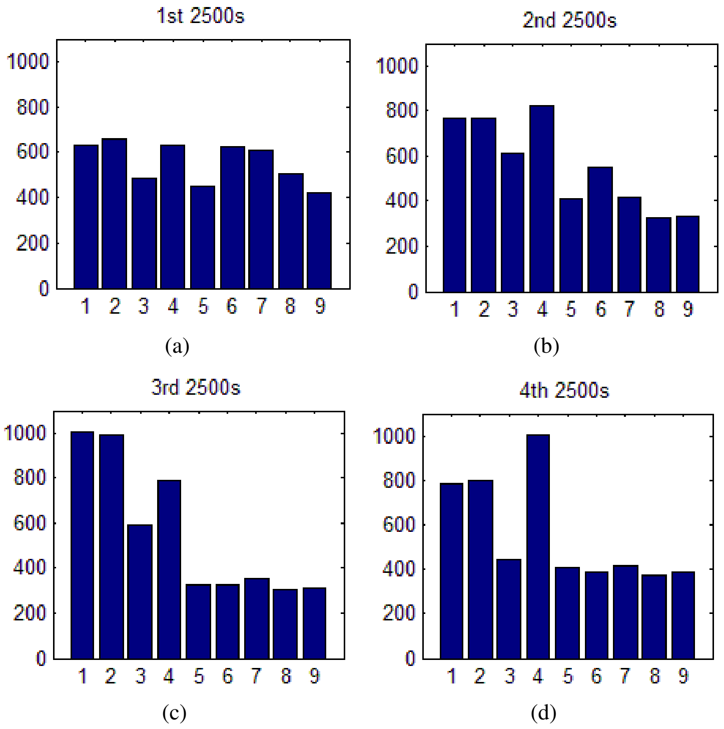
Fig. 1.12 Selection weight for different sensors during the test scenario.

1.5.2 Sensor Selection

The purpose of the first testing scenario was to demonstrate the automatic adaptation of the sensor selection algorithm to reflect the current behavior of the observed network traffic. In this scenario, the control system is run for 10,000 seconds and the sensor data is gathered once every second. In addition, $k = 2$ known secure sensor values are requested every second. The communication network is initialized with uniformly distributed time delay and packet loss and corruption rates throughout the entire network. Also, all of the selection criteria for individual sensors are weighted equally. Three events are used to simulate various changes of the environment to demonstrate the adaptation mechanism of the Sensor Selector.

- Event 1: At time t = 2500s the network traffic in the larger sub-network 3 becomes congested, which is implemented as decreased throughput of particular communication node. Hence, the availability of sensors 5-9 is decreased.
- Event 2: At time t = 5000s a possible cyber-attack is simulated on sub-network 1. This attack is implemented as an increased packet corruption rate for the associated communication node leading to increased number of mismatched plain-text and KSSM messages from sensors 1 and 2.
- Event 3: At time t = 7,500s the operator decides to adjust the sensor selection mechanism via the HMI by assigning weight 1.0 to the importance attribute and decreasing the weight of the security and availability attributes to 0.1. In addition, the operator subjectively increases importance of sensor 4 to its maximum value of 1.0.

Event 1 affects the availability of sensors 5-9. After the time delay for messages from sub-network 3 was increased, the response times of the KSSM messages from sensors 5-9 were increased. This resulted in decreased availability of sensors 5-9 as shown in figure 1.10. Event 2 affects the security of sensors 1 and 2. The increased probability of obtaining an incorrect KSSM message from sensors 1 and 2 causes the time interval of receiving two mismatching plain-text and KSSM messages to decrease. Hence, the security of these sensors is increased, which can be observed in figure 1.11. Figure 1.12 shows the evolution of the sensor selection weight for individual sensors. It is apparent how the sensor selection weights are converging to a uniform distribution during the first 2,500s of the simulation. The diverse selection weights at the start of the simulation are due to the stochastic sampling process, which must be first averaged over certain amount of time to obtain good initial results. Next, it is apparent that the decreased availability of sensors 5-9 when event 1 occurs leads to their lower selection weight. Furthermore it can also be seen that the increased security of compromised sensors 1 and 2 when event 2 occurs leads to their increased selection weight. Finally, Event 3 at time 7,500s can be observed when the operator overrides the selection criteria importance and modifies the selection weight, which increases the weight of sensor 4 due to its higher importance. To verify the influence of the sensor selection weight on the KSSM sensor sampling process, figure 1.13 shows histograms of sensor selection for the four quarters of the simulation. It can again be observed that the decreased value of the availability parameter leads to less frequent selection of sensors 5-9 in figure 1.13 (b) and the increased security of sensors 1 and 2 leads to their more frequent selection in figure 1.13 (c). Finally, the higher importance of sensor 4 results in its more frequent sampling together with sensors 1 and 2 that were likely compromised by an attacker, as shown in figure 1.13 (d). In summary, figure 1.13 demonstrates that the KSSM system adjusts the sensor selection algorithm to obtain more samples from likely compromised sensors and to obtain less samples from congested parts of the communication network.



(a) (b) (c) (d)

Fig. 1.13 Sensor selection histograms for different intervals of the simulation.

1.5.3 Variable network bandwidth

The following test scenario was designed to demonstrate the automatic update of the number k of sampled KSSM messages. The essential property of the KSSM system is that it should use the available communication bandwidth in the control system network without compromising its real-time response. In this scenario, the identical communication network as shown in figure 1.9 was used. The network was simulated for 4,000s and the sensor measurements have been reported once every second. In order to achieve the requested real-time response of obtaining sensor measurements once every second, maximum desired response for plain-text measurement was set to 0.8s. For the initial 1000s, the network was simulated with low average time-delay for individual network nodes (0.05s average latency of network node per packet). At time 1000s the average time delay of the larger sub-net 3 was increased to 0.075s. Next, at time 2000s the average time delay of sub-net 3 was increased to 0.1s. And finally at time 3000s the average time delay of sub-net 3 was increased to 0,125s. Note that the actual time delay for a specific packet was computed using a uniform distribution with standard deviation of 0.02s centered at the average time delay value. Figures 1.14 and 1.15 demonstrate the behavior of the system. First, figure 1.14 depicts the maximum observed response time of the plain-text measurements. It is apparent how this maximum response time increases at times 1000s, 2000s, and 3000s. Next, figure 1.15 shows the number k of selected KSSM sensors. The algorithm starts with $k = 0$ KSSM sensors and first observes the maximum response time of the plain-text measurements. When this maximum response time is found to be below the desired threshold of 0.8s, the number k of selected KSSM messages is incrementally increased up to the maximum value of all 9 sensors sending encrypted messages. The first increase in time-delay at time 1000s caused several plain-text messages to be delivered later than the required real-time response and the system quickly lowers the value of k in order not to disrupt the real-time response. Consequently, the system attempts to sequentially increase the number of sampled KSSM values, while monitoring the real-time performance. Finally, in the last part of the simulation the system stabilizes and samples mostly a single KSSM value per iteration. Hence, it can be observed that the KSSM system attempts to provide the maximum level of cyber-state awareness given the available communication bandwidth.

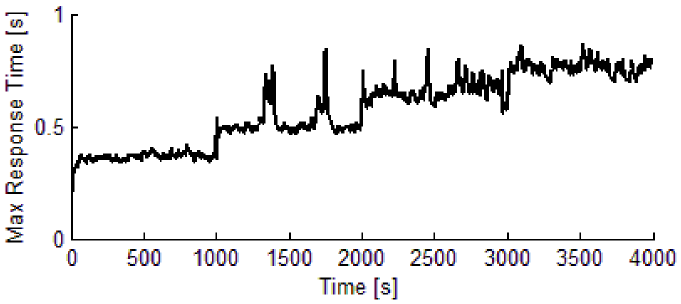


Fig. 1.14 Maximum response time of plain-text measurements.

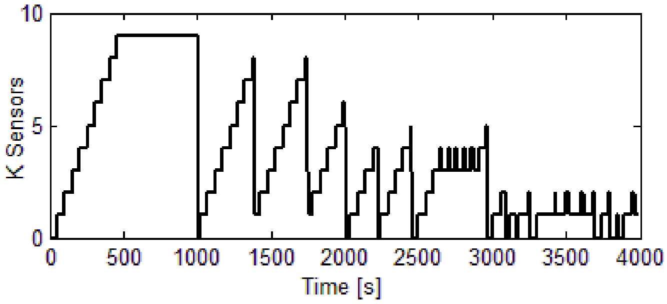


Fig. 1.15 Number of selected KSSM values.

1.6 Future Work

As previously stated one of the most important features of the presented KSSM system is that it can be incrementally integrated with existing control systems. This incremental integration is allowed by utilizing the existing physical measurements and by using the available communication network bandwidth. For larger scale control systems with high number of physical sensors the incremental integration with the KSSM system might have to be performed in several stages. In each stage a small subset of physical sensors would be enhanced with an encryption module. The newly enhanced sensor would then be added to the list of KSSM-enabled sensors and it could be consequently used to for system state falsification detection.

Once all available physical sensors are KSSM-enabled the KSSM system can provide the maximum level of cyber-security given the communication network resources available. However, in the earlier stages of the KSSM system implementation where not all physical sensors are KSSM-enabled, it is important to prioritize which sensors should be made KSSM-enabled in the current stage so that the current level of provided cyber-security is maximized. This prioritization constitutes a complex multi-criteria decision making task because multiple potentially conflicting constraints such as economical, time or other subjective constraints might be simultaneously present. Optimal prioritizing and staging the implementation process is a crucial component of applying the KSSM concept to real world systems.

Our future work will be to further research and apply the KSSM concept to a variety of explicit real world systems on both a macro and micro scale. On the macro scale, we will apply multi-criteria decision making to the question of optimal placement of a limited number of PMUs in portions of the U.S. power grid. This will be evaluated with the understanding that the placement of PMUs will be staged in over many years. On the micro scale we will research and evaluate building KSSM concepts in at a local level, such as at significant individual substations. Within each substation, the intent will be to build in local KSSM agents within sensors and actuators so that they may autonomically manage a localized KSSM process for substation state awareness. The localized state awareness may then be transmitted back to the control room for regional level state awareness or used for localized response to detected cyber attacks. These KSSM agents will of course be applied with the understanding that they must not ever interfere with necessary communication and operations of the substation in the absence of cyber attack.

Acknowledgements This work was partially supported by the U.S. Department of Energy under DOE Idaho Operations Office Contract DEAC07-05ID14517, performed as part of the Known Secure Sensor Measurements and Experimental Security projects at Idaho National Laboratory, the Los Alamos National Laboratory LDRD project Optimization and Control Theory for Smart Grids, the Center for Nonlinear studies at Los Alamos National Laboratory.

Appendix

References

1. O. Linda, M. Manic, T. R. McJunkin, ‘Anomaly Detection for Resilient Control Systems Using Fuzzy-Neural data Fusion Engine,’ in Proc. IEEE Symposium on Resilient Control Systems, Aug. 2011.
2. C. G. Rieger, D. I. Gertman, M. A. McQueen, ‘Resilient Control Systems: Next Generation Design Research,’ in Proc. 2nd IEEE Conf. on Human System Interactions, Catania, Italy, pp. 632-636, May 2009.
3. M. Stamp, Information Security, 2nd edition, John Wiley and Sons, Chapters 3-5, and 9, 2011.
4. N. Ferguson, B. Schneier, T. Kohno, Cryptography Engineering, Chapters 3-7, 2010.
5. M. McQueen, A. Giani, ‘Known Secure Sensor Measurements’ for Critical Infrastructure Systems: Detecting Falsification of Systems State,’ in Proc. of SERENE, 2011.
6. A. Giani, E. Bitar, M. McQueen, P. Khargonekar, K. Poolla, ‘Smart Grid Data Integrity Attacks: Characterization and Countermeasures,’ in Proc. Of IEEE SmartGridComm, Oct. 2011.
7. O. Linda, T. Vollmer, M. Manic ‘Neural Network based Intrusion Detection System for Critical Infrastructure,’ in Proc. IJCNN 2009, June 2009.
8. O. Linda, M. Manic, T. Vollmer, J. Wright, ‘Fuzzy Logic Based Anomaly Detection for Embedded Network Security Cyber Sensor,’ in Proc. of IEEE Symposium on Computational Intelligence, pp. 202-209, April, 2011.
9. D. Yang, A. Usynin, J. W. Hines, ‘Anomaly-Based Intrusion Detection for SCADA Systems,’ 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC and HMIT 05) , Albuquerque, NM, Nov 12-16, 2006.
10. S. Zhong, T. Khoshgoftaar, N. Seliya, ‘Clustering-based network intrusion detection,’ In Intl. Journal of Reliability, Quality and Safety, Vol. 14, No. 2, 2007, pp. 169-187.
11. A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, K. Poolla, ‘Smart Grid Data Integrity Attacks: Characterizations and Countermeasures,’ In Proc. of Smart Grid Comm 2011.
12. , ‘Cryptographic Protection of SCADA Communications, Part 1: Background, Policies and Test Plan, Draft 5’ American Gas Association, April 2005
13. ‘Cryptographic Protection of SCADA Communications, Part 2: Retrofit Link Encryption for Asynchronous Serial Communications’ American Gas Association, April 2005
14. C. Tsang , ‘Multi-agent intrusion detection system in industrial network using ant colony clustering approach and unsupervised feature extraction,’ IEEE International Conference on Industrial Technology, 2005. ICIT 2005
15. S. Cheung, B. Dutertre, M. Fong, U. Lindqvist, K. Skinner, A. Valdes, ‘Using Model-based Intrusion Detection for SCADA Networks, ’ in Proc. of the SCADA Security Scientific Symposium, 2007.

16. M. McQueen, ‘Deception used for cyber defense of control systems,’ 2nd Conference on Human System Interactions, 2009.
17. D. Wei , ‘An integrated security system of protecting Smart Grid against cyber attacks,,’ Innovative Smart Grid Technologies (ISGT), 2010.

Glossary

Use the template *glossary.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style your glossary in the Springer layout.

glossary term Write here the description of the glossary term. Write here the description of the glossary term. Write here the description of the glossary term.

glossary term Write here the description of the glossary term. Write here the description of the glossary term. Write here the description of the glossary term.

glossary term Write here the description of the glossary term. Write here the description of the glossary term. Write here the description of the glossary term.

glossary term Write here the description of the glossary term. Write here the description of the glossary term. Write here the description of the glossary term.

glossary term Write here the description of the glossary term. Write here the description of the glossary term. Write here the description of the glossary term.

Index