INL/CON-12-24440
PREPRINT

Improving Control System Cyber-State Awareness Using Known Secure Sensor Measurements

7th International Conference on Critical Information Infrastructures Security

Ondrej Linda
Milos Manic
Miles McQueen

September 2012

The INL is a
U.S. Department of Energy
National Laboratory
operated by
Battelle Energy Alliance

This is a preprint of a paper intended for publication in a journal or proceedings. Since changes may be made before publication, this preprint should not be cited or reproduced without permission of the author. This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, or any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for any third party's use, or the results of such use, of any information, apparatus, product or process disclosed in this report, or represents that its use by such third party would not infringe privately owned rights. The views expressed in this paper are not necessarily those of the United States Government or the sponsoring agency.

Improving Control System Cyber-State Awareness using Known Secure Sensor Measurements

Ondrej Linda, Milos Manic, Miles McQueen

Abstract. This paper presents design and simulation of 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. The KSSM concept relies on physical measurements to detect malicious falsification of the control systems state. The KSSM method can be incrementally integrated with already installed control systems for enhanced resilience. This paper reviews the previously developed theoretical KSSM concept and then describes a simulation of the KSSM system. A simulated control system network is integrated with the KSSM components. The effectiveness of detection of various intrusion scenarios is demonstrated on several control system network topologies.

Keywords: Cyber-Security, Critical Control Systems, State-Awareness

1 Introduction

Resiliency and enhanced state-awareness are crucial properties of modern control systems. Especially critical infrastructures, such as energy production and industrial systems, would significantly 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. During system state falsification, 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 crypto graphic 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 KSSM 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]-[10].

This paper describes the design and simulation of the KSSM method. First, 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.

The rest of the paper is organized as follows. Section 2 reviews the previously proposed KSSM concept, followed by description of the design and simulation of the KSSM enabled control system in Section 3. Experimental testing is presented in Section 4 and the paper is concluded in Section 5.

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 after 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 was targeted for critical infrastructure control systems that lack robust crypto graphic 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.

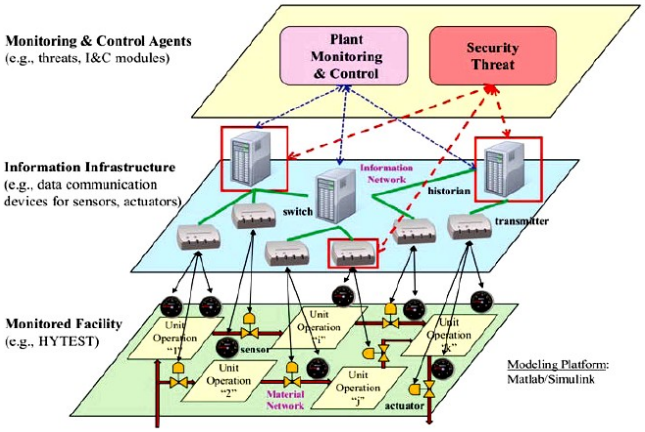


Fig. 1. Hybrid energy production facility [5].

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. Fig. 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 measurements 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.

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 harden the detection mechanism because which

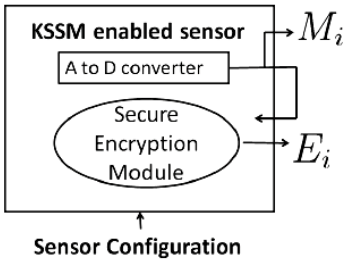


Fig. 2. Schematic of a KSSM-enabled sensor [5].

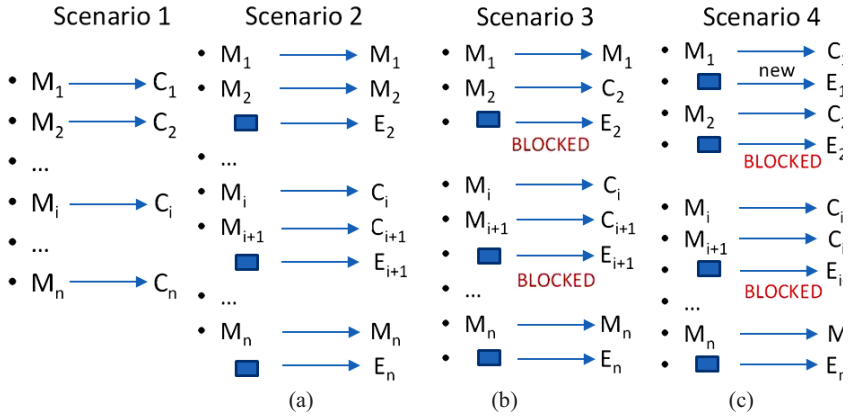


Fig. 3. Communication scenarios.

sensor measurements are being secured at particular time cannot be predicted by the attacker. 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.

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 Fig. 2. The cryptographic sensor may be KSSM enabled with software or hardware as a means 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.

Fig. 3 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 Fig. 3(a). 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 Fig. 3(b), 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 Fig. 3(c). 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 Fig. 3(d), where the values C_1 and E_1 from the newly selected

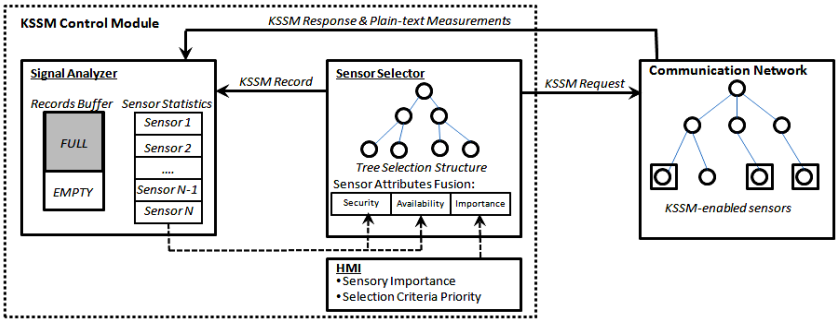


Fig. 4. Architecture of the KSSM system.

KSSM-enabled sensor would produce a mismatch and indicate a presence of system state falsification.

3 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.

3.1 KSSM System Architecture

The overall KSSM system architecture is depicted in Fig. 4. 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 the 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.

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 unencrypted and the KSSM encrypted network messages. Everytime 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.

3.2 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 particular node are assigned a specific selection probability, which guides the random descending process. This method is repeated until the 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:

Step 1: Initialize the sensor selection probabilities p_{ij} of each branch in the selection tree.

Step 2: Repeat for all k KSSM sensors.

Step 2.1: Set current node n_i as root.

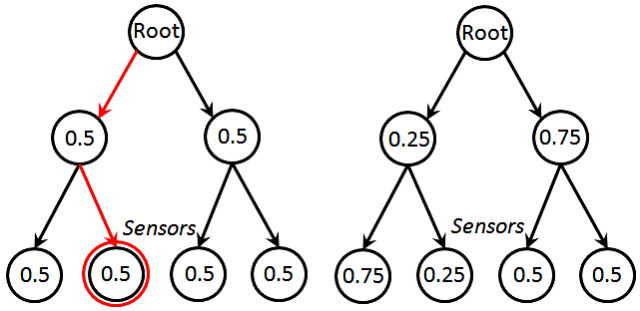
Step 2.2: Repeat, until current node n_i is a leaf.

Step 2.2.1: Randomly select j^{th} branch of current node n_i based on branch selection probabilities p_{ij}.

Step 2.2.2: 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.

Step 2.3: Return the index of the sensor in the selected leaf.

Step 2.4: Repeat until current node n_i is a root



(a) (b)

Fig. 5. Sensor selection tree before (a) and after selection (b). The sensor selection is denoted by red color.

Step 2.4.1: For all siblings of current node n_i compute the new branch selection probability from their parent as:

$$p_{kj} = \begin{cases} p_{kj} = p_{kj}(1-\alpha), & k = i \\ p_{kj} = p_{kj} + \dfrac{\alpha\, p_{ij}}{(K-1)}, & k \neq i \end{cases} \tag{1}$$

Step 2.4.2: Ascent to the parent of node n_i.

Coefficient α used in **Step 2.4.1** 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 Fig. 5. 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 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.

3.3 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 sensors 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 than 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 above 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.

4 Simulation 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.

4.1 Network Emulator

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 through-put 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 has been constructed. The network gathers measurements from 9 sensors, which are grouped into 3 sub-networks as depicted in Fig. 6.

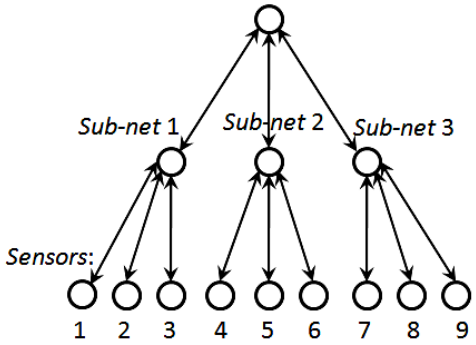


Fig. 6. Testing network topology.

4.2 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 are gathered once every second. In addition, k=2 KSSM 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.

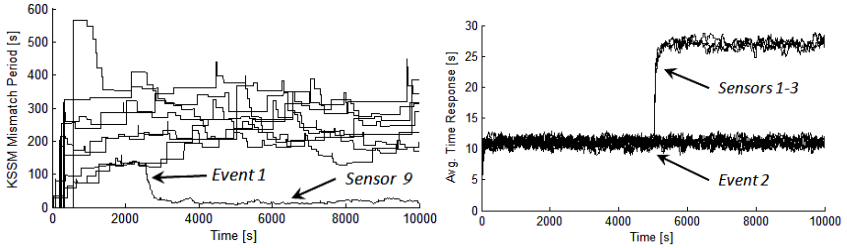
Event 1: At time t = 2500*s* a possible cyber-attack is simulated on sensor 9. This attack is implemented as an increased packet corruption rate for the communication node of sensor 9, leading to increased number of mismatched plain-text and KSSM messages from sensor 9.

Event 2: At time t = 5000*s* the network traffic in sub-network 1 becomes congested, which is implemented as decreased through-put of particular communication nodes. Hence, the availability of sensors 1-3 is decreased.

Event 3: At time t = 7,500*s* 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 5 to its maximum value of 1.0.

Event 1 affects the security of sensor 9. The increased probability of obtaining an incorrect KSSM message from sensor 9 causes the time interval of receiving two mismatching plain-text and KSSM messages from sensor 9 to decrease. Hence, the security of this sensor is increased. This fact can be clearly observed in Fig. 7(a).

Event 2 affects the availability of sensors 1-3. After the time delay for messages from sub-network 1 was increased, the response time of the KSSM messages from sensors 1-3 were increased. This resulted in decreased availability of sensors 1-3 as shown in Fig. 7(b).



(a) (b)

Fig. 8. KSSM values mismatch period (a) and average time response for various KSSM sensors (b).

Fig. 8 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 increased security of compromised sensor 9 when event 1 occurs leads to its increased selection weight. It can also be seen that the decreased availability of sensors 1-3 when event 2 occurs leads to their lower selection weight.

Finally, Event 3 at time 7,500*s* can be observed when the operator overrides the selection criteria importance and modifies the selection weight, which increases the weight of sensor 5 due to its higher importance.

To verify the influence of the sensor selection weight on the KSSM sensor sampling process, Fig. 9 shows histograms of sensor selection for the four quarters of the simulation. It can again be observed that the increased value of the security parameter leads to more frequently selecting sensor 9 in Fig. 9(b) and the decreased availability of sensors 1-3 leads to their less frequent selection in Fig. 9(c). Finally, the higher importance of sensor 5 results in its more frequent sampling together with sensor 9, which was likely compromised by an attacker, as shown in Fig. 9(d). In summary, Fig. 9 demonstrates that the KSSM system adjusts the sensor selection algorithm to

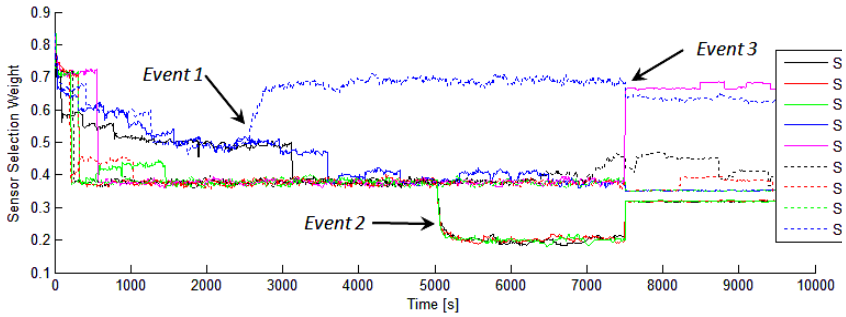


Fig. 7. Selection weight for different sensors during the test scenario.

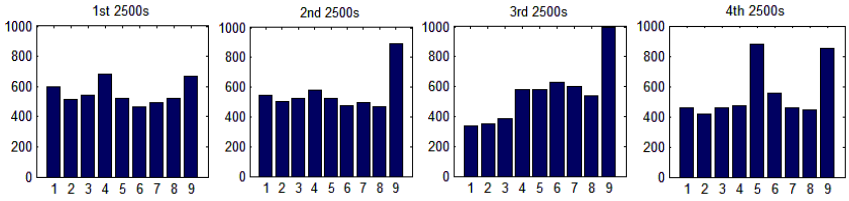


Fig. 9. Sensor selection histograms for different intervals of the simulation.

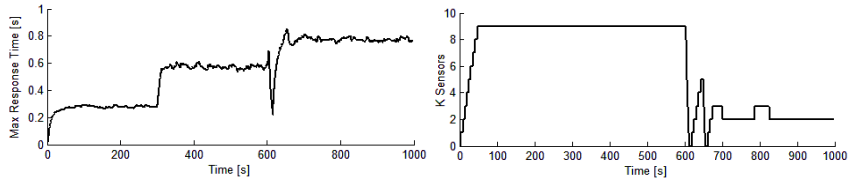
obtain more samples from likely compromised sensors and to obtain less samples from congested parts of the network.

4.3 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 Fig. 6 was used. The network was simulated for 1,000s 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, a maximum desired response for plain-text measurement was set to 0.8s. For the initial 300s, the network was simulated with low average time-delay for individual network nodes (0.05s average latency of network node per packet). At time 300s the average time delay on the network nodes was increased to 0.1s. Finally, at time 600s the average time delay was increased to 0.15s. 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.

Fig. 10 demonstrates this behavior of the system. First, Fig. 10(a) depicts the maximum observed response time of the plain-text measurements. It is apparent how this maximum response time increases at times 300s and 600s. Next, Fig. 10(b) 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



(a) (b)

Fig. 10. Maximum response time of plain-text measurements (a) and the number of selected KSSM values (b).

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 300s increased the maximum response time (~0.6s) but did not yet exceed the desired performance. However, when the time-delay was again increased at time 600s, some of the plain-text measurements were not reported in the desired time and the KSSM system quickly decreased the number k of KSSM sensors, in order not to compromise the real-time response of the control system. Next, the KSSM control module attempted to increase the number of KSSM samples and observe its impact on network response time. Eventually, the number of KSSM values stabilized at k=2, which provided the maximum level of cyber-state awareness given the available communication bandwidth.

5 Conclusion

This paper presented a design and simulation of a low cost, low false and high reliability alarm rate method for improved cyber-state awareness of critical control systems - the Known Secure Sensor Measurements mechanism. The KSSM method relies on the physical measurements to detect malicious falsification of the control system's state. The KSSM technique can be incrementally integrated with already installed control systems for enhanced resilience.

First, the previously developed theoretical KSSM concept was reviewed and then its simulation was described. A virtual control system communication network was used to demonstrate the performance of the system. It was shown that the KSSM system can adapt its parameters to specific network behavior including the operator's request. Furthermore, it was demonstrated that the number of selected KSSM sensors can be automatically adapted to provide the maximum amount of cyber-state awareness while minimizing the impacts on the real-time performance of the control system.

The presented work constitutes a first step towards successful demonstration of the feasibility of the KSSM concept. The future work will be focused on additional experimental testing and implementation of the KSSM concept and on improving the sensor selection algorithm via computational intelligence techniques.

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, T. Vollmer, M. Manic, 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&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.