INL/CON-13-28681
PREPRINT

Resilient Plant Monitoring System: Design, Analysis, and Performance Evaluation

52nd IEEE Conference on Decision and Control

Humberto E. Garcia
Wen-Chiao Lin
Semyon M. Meerkov
Maruthi T. Ravichandran

December 2013

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

52nd IEEE Conference on Decision and Control
December 10-13, 2013. Florence, Italy

Resilient Plant Monitoring System: Design, Analysis, and Performance Evaluation

Humberto E. Garcia, Wen-Chiao Lin, Semyon M. Meerkov and Maruthi T. Ravichandran

Abstract— **Resilient monitoring systems are sensor networks that degrade gracefully under malicious attacks on their sensors, causing them to project misleading information. The goal of this paper is to design, analyze, and evaluate the performance of a resilient monitoring system intended to monitor plant conditions (normal or anomalous). The architecture developed consists of four layers: data quality assessment, process variable assessment, plant condition assessment, and sensor network adaptation. Each of these layers is analyzed by either analytical or numerical tools, and the performance of the overall system is evaluated using simulations. The measure of resiliency of the resulting system is evaluated using Kullback-Leibler divergence, and is shown to be sufficiently high in all scenarios considered.**

I. Introduction

This paper is devoted to the design, analysis, and performance evaluation of an autonomous decentralized monitoring system that degrades gracefully under malicious attacks on its sensors. We refer to such a system as *resilient*.

The sensor network addressed in this paper is intended to measure process variables, e.g., temperature, pressure, flow rate, etc., at various parts of a plant (e.g., power plant), and assess the plant's condition, e.g., normal or anomalous. When sensors are under attack, the sensor network must restructure itself, either by re-assigning some sensors or discounting measurements of others, or both, so that the best plant condition assessment is ascertained.

If the sensor malfunctioning were statistical, e.g., only the variance of the sensor measurement were maliciously changed, numerous statistical tools could be applied to evaluate the process variables and use them for plant assessment and subsequent sensor network adaptation. We assume, however, that the attacker may force a sensor to project misleading data, i.e., data, which are statistically unrelated to the process variable, and characterize the level of discrepancy by a scalar parameter referred to as data quality (*DQ*). In this situation, statistical methods become insufficient for process variable assessment, and, therefore, models of the attacker, *DQ*, and the effect of *DQ* on process variable identification must be introduced. This leads to a four-layer resilient monitoring system, designed and analyzed in this paper: data quality assessment layer; process variable assessment layer; plant condition assessment layer; and sensor network adaptation layer.

While the first three layers are based on the models and techniques introduced in this paper, the last one uses the so-called rational controllers developed in [1]–[3], which intend to select the sensor network state so that the plant assessment is optimized (as quantified by the entropy of the probability mass function (pmf) identified in the plant condition assessment layer). With the exception of our preliminary results reported in [4]–[6], and a different approach developed in [7] and [8], to the best of our knowledge, such systems are not described in the current literature.

The outline of the paper is as follows: Section II is devoted to modeling issues and problem formulation. The four layers mentioned above are described in Sections III-VI, respectively. Results of numerical evaluation of the resulting system are reported in Section VII. Finally, the conclusions and directions for future work are given in Section VIII. Due to space limitations, many details and all the proofs are omitted and can be found in [9].

II. Modeling and Problems Addressed

This section presents models of all components of the resilient monitoring system addressed in this paper, namely, process variables, sensors, attacker, plant, and sensor network. In addition, it describes problems addressed in the design and analysis of all the four layers of the monitoring system architecture. Finally, it introduces a measure of resiliency that quantifies the efficacy of monitoring systems under malicious attacks.

A. Process variable

Model: Let $\mathbf{V}$ denote a process variable, and $\tilde{V}$ be a continuous random variable that represents the values it takes according to the probability density function (pdf) $f_{\tilde{V}}(\tilde{v})$. In operations, process variables are often characterized as being normal or anomalous, for instance, low or high. To model this situation, introduce a discrete random variable V with outcomes Low (L), Normal (N), and High (H) defined by the following probabilities:

$$\begin{aligned} P_L^V &= \int_{V_{\min}}^{R_1} f_{\tilde{V}}(\tilde{v})\mathrm{d}\tilde{v},\ P_N^V = \int_{R_1}^{R_2} f_{\tilde{V}}(\tilde{v})\mathrm{d}\tilde{v}, \\ P_H^V &= \int_{R_2}^{V_{\max}} f_{\tilde{V}}(\tilde{v})\mathrm{d}\tilde{v}, \end{aligned} \tag{1}$$

where $V_{\min}$ and $V_{\max}$ are the minimum and maximum values of $\mathbf{V}$, respectively, and R_1 and R_2 are defined by technological considerations so that $V_{\min} < R_1 < R_2 < V_{\max}$. Thus, $\mathbf{V}$ is represented by a discrete random variable, V, with the universal set

$$\Sigma = \{\mathrm{L}, \mathrm{N}, \mathrm{H}\} \tag{2}$$

and the probability mass function (pmf), $P(V)$, given in (1).

The dynamics of $\mathbf{V}$ in each of its regions, L, N, and H,

H.E. Garcia and W.-C. Lin are with Idaho National Laboratory, P.O. Box 1625, Idaho Falls, ID 83415-3675, USA. Email: {Humberto.Garcia, Wen-Chiao.Lin}@inl.gov; S.M. Meerkov and M.T. Ravichandran are with Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI 48109, USA. Email: {smm, marutrav}@umich.edu

978-1-4673-5716-6/13/$31.00

are characterized by transfer functions denoted as $G_L^V(s)$, $G_N^V(s)$, and $G_H^V(s)$. In the simplest case, d.c. gains of these transfer functions, i.e.,

$$\alpha_{\rm L} \stackrel{\triangle}{=} G_L^V(0),\ \alpha_{\rm N} \stackrel{\triangle}{=} G_N^V(0),\ \alpha_{\rm H} \stackrel{\triangle}{=} G_H^V(0), \tag{3}$$

can be used to characterize the statics of $\mathbf{V}$ in regions L, N, and H.

Thus, the model of a process variable is defined by the pdf of $\tilde{V}$, pmf of V, and the transfer functions $G_L^V(s)$, $G_N^V(s)$, and $G_H^V(s)$.

B. Sensor

Model: Let $\mathbf{S}$ be a sensor assigned to monitor process variable $\mathbf{V}$, and $\tilde{S}$ a continuous random variable representing its projected data; the pdf of $\tilde{S}$ is denoted as $f_{\tilde{S}}(\tilde{s})$. As in the case of the process variable, the sensor measurements can be represented by a discrete random variable, S, with the outcomes low (L), normal (N), or high (H), and the pmf, $P(S)$, defined by

$$\begin{array}{rcl} P_L^S &=& \int\limits_{V_{\rm min}}^{R_1} f_{\tilde{S}}(\tilde{s}){\rm d}\tilde{s},\ P_N^S = \int\limits_{R_1}^{R_2} f_{\tilde{S}}(\tilde{s}){\rm d}\tilde{s}, \\ P_H^S &=& \int\limits_{R_2}^{V_{\rm max}} f_{\tilde{S}}(\tilde{s}){\rm d}\tilde{s}, \end{array} \tag{4}$$

where R_1 and R_2 are the same as in (1). Thus, S has the same universal set as V, but possibly a different pmf (given by (4)). The pmf's $P(V)$ and $P(S)$, may differ due to natural or malicious causes. For example, they may have different variances and/or expected values. We quantify the measure of discrepancy between $P(V)$ and $P(S)$ by a parameter referred to as Data Quality (*DQ*), which takes values on the interval $[0,\ 1]$, with $DQ = 0$ implying that the sensor is not trustworthy at all, and $DQ = 1$ indicating that it is perfectly trustworthy. While the issue of *DQ* assignment is addressed in Section III, we use it below to further define the sensor model.

Since *DQ* is not a statistical quantity, a model of its effect on the relationship between random variables V and S must be introduced. To accomplish this, define the quantity

$$B = \frac{2}{3}DQ + \frac{1}{3}, \tag{5}$$

referred to as the sensor *believability*. When DQ is close to 1, B is also close to 1; when DQ is close to 0, B is close to $\frac{1}{3}$, implying that each outcome of V is equally plausible. Using the believability, we define the conditional pmf of V given S as follows:

$$\begin{array}{rcl} P\{V = \sigma\ |S = \sigma\} &=& B, \\ P\{V \neq \sigma\ |S = \sigma\} &=& \frac{1-B}{2}, \end{array} \tag{6}$$

where $\sigma \in \Sigma$ (defined in (2)). Clearly, this implies that V has the same outcome as S with probability B, and two other outcomes with equal probabilities.

Thus, the model of a sensor is defined by the pdf of $\tilde{S}$, pmf of S, data quality DQ, believability B, and the coupling (6).

Problems:

1) Based on the models of the process variable and the sensor introduced above, develop a method for *DQ* assignment. This is carried out in Section III.
2) Given the sensor measurements $s_1, s_2, ..., s_n, ...,$ and its data quality *DQ*, develop a method for calculating an estimate of $P(V)$, denoted as $\hat{P}(V = \sigma)$, $\sigma \in \Sigma$, and specified by

$$\lim_{n\to\infty} P(V = \sigma | s_1, s_2, ..., s_n; DQ). \tag{7}$$

3) If multiple sensors, e.g., $\mathbf{S}_1$ and $\mathbf{S}_2$, monitor a process variable $\mathbf{V}$, develop a method to identify

$$\lim_{n\to\infty} P(V = \sigma | s_1^1, ..., s_n^1; DQ_1; s_1^2, ..., s_n^2; DQ_2). \tag{8}$$

This and the previous problem are considered in Section IV.

C. Attacker

Model: The attacker modifies sensor measurements in order to project misleading information. In formal terms, this implies that the attacker modifies $f_{\tilde{S}}(\tilde{s})$ by changing its variance or expected value, or both. Our preliminary investigation indicates that modifying expected values is more damaging for resilient monitoring than modifying variances. Therefore, the model of the attacker considered in this paper is that for a sensor under attack,

$$E[\tilde{S}] \neq E[\tilde{V}], \tag{9}$$

where $E[.]$ denotes the expected value. This implies, for example, that, while process variable $\mathbf{V}$ is in state N, sensor $\mathbf{S}$ may project a signal testifying that $\mathbf{V}$ is in state H or L.

The attacker model (9) is considered throughout this paper. In particular, it is used in Section III for data quality identification. We note, however, that other models of the attacker could be considered using the approach developed in this paper.

D. Plant

Model: Let $\mathbf{G}$ denote the monitored plant, and G be the discrete random variable representing its condition, which can be either normal, $\rm N_G$, or anomalous, $\rm A_1, A_2, ..., A_k$. However, to make the presentation more transparent, we assume that the anomalous states of the plant are analogous to those of the process variables, i.e., low ($\rm L_G$) and high ($\rm H_G$). Thus, the universal set of G is

$$G \in \Sigma_G = \{\rm L_G, N_G, H_G\}. \tag{10}$$

As far as the plant model is concerned, we assume that in the case of a single process variable it is specified by the conditional pmf of V given G, i.e.,

$$\mathbf{G}:\ P(V|G),\ V \in \Sigma,\ G \in \Sigma_G. \tag{11}$$

In the case of multiple process variables, $\mathbf{V}_1, \mathbf{V}_2, ..., \mathbf{V}_M$, the plant model is given either by a vector of conditional pmf's

$$\mathbf{G}: [P(V_1|G),\ P(V_2|G), ..., P(V_M|G)],\quad \begin{array}{rl} V_i & \in \Sigma, \\ G & \in \Sigma_G, \end{array} \tag{12}$$

or by a joint conditional pmf

$$\mathbf{G} : P(V_1, V_2, ..., V_M|G),\ V_i \in \Sigma,\ G \in \Sigma_G. \tag{13}$$

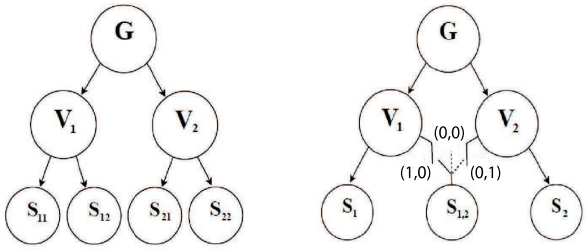
Problem: In the case of a single process variable monitored by a single or multiple sensors, given conditional pmf(s) (7) and the plant model (11), estimate the pmf of the plant state, $\hat{P}(G)$, $G \in \Sigma_G$. In the case of M process variables, $\hat{P}(G)$ must be identified based on either plant models (12) or (13) and the estimates of process variable pmf's, $\hat{P}(V_1), ..., \hat{P}(V_M)$. This problem is solved in Section V.

E. Sensor network

Model: Consider plant $\mathbf{G}$ with process variables $\mathbf{V}_1, ..., \mathbf{V}_M$. Assume that the sensor network, which monitors $\mathbf{G}$, consists of two types of sensors: *dedicated* and *free*. Each dedicated sensor monitors a specific process variable; in this situation, the only decision to be made in the framework of resilient monitoring is whether to use the measurements of this sensor for $\hat{P}(V)$ identification or not. Each free sensor is wired so that it can monitor any of the process variables to which it is connected. For example, thermocouples can be wired so that they could measure the temperature at either of two points on a boiler at a power plant. In this situation, the decision to be made is not only whether to use the measurements of a free sensor, but also which process variable this sensor should be monitoring.

The first of the above situations is referred to as *non-contentious* and the second as *contentious*. An example of each of these situations is given in Figure 1. Note that in the contentious case, the subscript of the free sensor lists all process variables to which it is connected.

The state of a dedicated sensor is denoted as either 1 or 0, with 1 implying that its measurements are used for the process variable pmf evaluation, and 0, that they are not. The state of a free sensor is denoted by a vector with elements 1 and 0, indicating to which process variable it is assigned to, if at all. For instance, the free sensor of Figure 1(b) has the states $(1,\ 0)$, $(0,\ 1)$, and $(0,\ 0)$, implying that it is assigned to $\mathbf{V}_1$, $\mathbf{V}_2$, and to neither, respectively.



(a) Non-contentious (b) Contentious

Fig. 1. Types of monitoring systems

Let X denote the state space of the sensor network and x a particular state in X. Let $\hat{P}_x(G = \sigma),\ \sigma \in \Sigma_G$, be the estimate of plant pmf when the network is in state x and let $\hat{I}_x(G)$ be the entropy of this pmf, i.e.,

$$\hat{I}_x(G) = -\sum_{\sigma \in \Sigma_G} \hat{P}_x(G = \sigma) \log_3 \hat{P}_x(G = \sigma). \tag{14}$$

Clearly, $\hat{I}_x(G)$ quantifies the measure of uncertainty in plant assessment – the smaller $\hat{I}_x(G)$, the more certain the assessment is. Using $\hat{I}_x(G)$, the problem of resilient monitoring can be defined as follows:

Problem: Autonomously (i.e., without any external interference) and in a decentralized manner (i.e., without communication among the sensors) determine the state of the network at which $\hat{I}_x(G)$ is minimized, i.e., find $x^* \in X$ such that

$$\hat{I}_{x^*}(G) = \min_{x \in X} \hat{I}_x(G), \tag{15}$$

and have the network operate in this state with the largest probability. An approach to solving this problem is outlined next.

F. Adaptation and measure of resiliency

Model: As mentioned above, in the non-contentious case, the decision to be made with regard to each sensor is whether to use its measurements for pmf (7) identification or not. In addition, in the contentious case, a decision must be made as to which process variable a free sensor should be assigned. In this work, these decisions are made by the so-called rational controllers.

The theory of rational behavior and rational controllers has been developed in [1] and further extended in [2], [3]. While the properties and behavior of rational controllers are described in Section VI, we note here that they are used in the current work to force the network to operate in the state x^* (i.e., the state resulting in the smallest entropy $\hat{I}_{x^*}(G)$) with the largest probability.

To characterize the efficacy of this adaptation procedure, we introduce the notion of *measure of resiliency*. Let $\hat{P}_x(G)$ be the estimate of the plant pmf when the network is in state $x \in X$. Let the probability of the network operating in state x be τ_x. Then, introduce the expected value of $\hat{P}_x(G)$, $x \in X$, given by

$$\bar{\hat{P}}(G) = \sum_{x \in X} \tau_x \hat{P}_x(G). \tag{16}$$

To quantify the measure of resiliency, we analyze the "distance" of $\bar{\hat{P}}(G)$ from the true pmf of the plant, $P(G)$. This is accomplished using the Kullback-Leibler divergence [11]:

$$D\left(P(G)||\bar{\hat{P}}(G)\right) = \sum_{\sigma \in \Sigma_G} P\{G = \sigma\} \log_3 \frac{P\{G = \sigma\}}{\bar{\hat{P}}\{G = \sigma\}}. \tag{17}$$

Based on this expression, we introduce the following measure of resiliency (*MR*):

$$MR = \frac{D\left(P(G)||\hat{P}_{\text{nr}}(G)\right) - D\left(P(G)||\bar{\hat{P}}(G)\right)}{D\left(P(G)||\hat{P}_{\text{nr}}(G)\right)}, \tag{18}$$

where $\hat{P}_{\text{nr}}(G)$ is the estimated plant pmf of the non-resilient system, i.e., when the monitoring system continuously operates assuming that $DQ_i = 1,\ \forall i$. Clearly, $MR \leq 1$, and the value 1 is attained when $\hat{P}(G) = P(G)$.

Based on the above, we formulate the following resilient adaptation problems:

Problems:

1) Design the structure and select the parameters of rational controllers appropriate for the resilient monitoring system.
2) For the system, thus designed, evaluate its performance as quantified by the measure of resiliency (18).

The first of these problems is solved in Section VI and the second one in Section VII.

III. Data Quality Assessment Layer

A. Approach

In the case of the mean-based attacker introduced in Subsection II-C, it could happen that a compromised sensor produces more self-consistent data (i.e., data with smaller entropy) than non-compromised ones. Since the resilient monitoring system uses entropy to quantify desirable sensor network states, this may lead to erroneous decisions as to which sensors should and which should not be taken into account. Clearly, this problem cannot be avoided by using traditional statistical tools, and non-statistical methods are necessary. In the current paper, this is accomplished using active identification based on *probing tests*: the process variable is probed by a rectangular signal, and the observed sensor responses are analyzed from the point of view of their consistency with the d.c. gains of the process variable, introduced in (3). The sensors with larger consistency are viewed as more trustworthy, and their *DQ* is assigned accordingly. This is the approach to *DQ* assignment developed in this section.

B. Probing signal

In general, any type of deterministic or random probing signals could be used. We utilize here the simplest probe – a rectangular pulse of amplitude A_0 and duration T, applied at the time instant t_0, i.e.,

$$u(t) = A_0 \text{rect}_{\text{T}}(t - t_0). \tag{19}$$

The value of A_0 should be selected sufficiently small so that the process variable remains in the same state (L, N, or H) before and during the probe. The value of T should be selected so that the process variable reaches a small vicinity of its steady state defined by the probe.

C. Probing inconsistency

Let $i \in \{1, 2, ..., N_{\text{S}}\}$, where N_{S} denotes the total number of sensors monitoring a given process variable $\mathbf{V}$. Further, let the mean value, $E[\tilde{S}_i]$, of the measurements of sensor $\mathbf{S}_i$ before the probe be μ_{S_i}, and at the end of the probe be $\tilde{\mu}_{\text{S}_i}$. Clearly, the difference between these two values should be equal to the d.c. gain of the process variable transfer function, which corresponds to its region (i.e., L, N, or H), multiplied by the amplitude of the probe, i.e.,

$$\tilde{\mu}_{\text{S}_i} - \mu_{\text{S}_i} = A_0 k_i(\mu_{\text{S}_i}), \tag{20}$$

where

$$k_i(\mu_{\text{S}_i}) = \begin{cases} \alpha_{\text{L}}, & \text{if } \mu_{\text{S}_i} \in \text{L} \\ \alpha_{\text{N}}, & \text{if } \mu_{\text{S}_i} \in \text{N} \\ \alpha_{\text{H}}, & \text{if } \mu_{\text{S}_i} \in \text{H} \end{cases} \tag{21}$$

and α_{L}, α_{N}, α_{H} are defined in (3). So, if a sensor is not attacked, the quantity $(\tilde{\mu}_{\text{S}_i} - \mu_{\text{S}_i}) - A_0 k_i(\mu_{\text{S}_i})$ is zero. If a sensor is attacked, it may be large. To discriminate between these two situations, we introduce the notion of *probing inconsistency* (PIC) of a sensor, as follows:

$$PIC_i \triangleq |(\tilde{\mu}_{\text{S}_i} - \mu_{\text{S}_i}) - A_0 k_i(\mu_{\text{S}_i})|, \tag{22}$$

where, $k_i(\mu_{\text{S}_i})$ is given in (21). When the attacker, being unaware of the probing signal, maintains the same average values of its signals before and during the probe, $PIC_i = A_0 k_i(\mu_{\text{S}_i})$. When the attacker is anticipating the probe, but does not exactly know A_0 or t_0, PIC_i again can be large. Only when the attacker is anticipating the probe and knows A_0 and t_0 exactly, PIC_i is small, and, thus, a sensor under attack may erroneously be recognized as a non-attacked one. To prevent this, a random A_0 can be used for each probing signal, although, in this paper, we do not address the issue of anticipating attackers with complete knowledge of the probe.

D. Data quality assignment

While various functions of PIC_i could be used for *DQ* assignment (see [5]), in this paper we assign it according to

$$DQ_i = e^{-F(PIC_i)}, \tag{23}$$

where $F(PIC_i)$ is a non-negative monotonically increasing function of PIC_i. Again, various types of such functions may be utilized. Our preliminary investigation indicates that a good choice of $F(PIC_i)$ is

$$F(PIC_i) = \gamma_i PIC_i^2,\ \gamma_i > 0. \tag{24}$$

Selecting an appropriate value of γ_i is of importance. Indeed, if this constant were too small, even sensors with large PIC_i would have relatively large DQ_i, which is undesirable; if it is too large, even sensors with small PIC_i would have relatively small DQ_i. Thus, this constant should be selected so that the largest tolerable PIC_i, denoted by PIC_{M_i}, results in the smallest DQ_i, which is a design parameter. If this parameter is selected as $\epsilon << 1$, the considerations based on (23) and (24) lead to the following γ_i:

$$\gamma_i = \gamma_i(\mu_{\text{S}_i}) = -\frac{\ln \epsilon}{PIC_{\text{M}_i}^2}, \tag{25}$$

where $PIC_{\text{M}_i}(\mu_{\text{S}_i})$ is

$$\begin{cases} |A_0(\alpha_{\text{L}} - \alpha_{\text{H}})|, & \text{if } \mu_{\text{S}_i} \in \text{L} \\ |A_0| \max\{|(\alpha_{\text{N}} - \alpha_{\text{L}})|, |(\alpha_{\text{N}} - \alpha_{\text{H}})|\}, & \text{if } \mu_{\text{S}_i} \in \text{N} \\ |A_0(\alpha_{\text{H}} - \alpha_{\text{L}})|, & \text{if } \mu_{\text{S}_i} \in \text{H}. \end{cases} \tag{26}$$

Equations (20)-(26) constitute the data quality assignment layer of the resilient monitoring system designed in this paper.

IV. Process Variable Assessment Layer

As indicated in Subsection II-B, the purpose of this layer is calculating $\hat{P}(V)$, i.e., the estimate of $P(V)$ based on sensor measurements $s_1, ..., s_n, ...$ and its data quality, DQ (see (7)). Below, we first carry this out for a single sensor and then for multiple sensors.

A. Process variable pmf estimation using data from a single sensor

Consider the process variable $\mathbf{V}$ monitored by sensor $\mathbf{S}$ with data quality DQ. Let $\hat{P}_n(V=\sigma)$, $\sigma \in \Sigma$ (see (2)), be the estimate of $P(V=\sigma)$ based on n sensor measurements and DQ, i.e.,

$$\hat{P}_n(V=\sigma) \triangleq P(V=\sigma|s_1, ..., s_n; DQ). \tag{27}$$

For convenience, denote $\hat{P}_n(V=\sigma)$ as $h_\sigma(n)$, $\sigma \in \Sigma$, $n \in \mathbb{N}$, and introduce the following recursive procedure for calculation of $h_\sigma(n)$:

$$h_\sigma(n+1) = h_\sigma(n) + \epsilon_h(n)\left[h^*_\sigma(s_{n+1}) - h_\sigma(n)\right], \tag{28}$$

with initial conditions

$$h_\sigma(0) = \frac{1}{3}, \forall \sigma. \tag{29}$$

In equation (28), ϵ_h is either a small parameter, i.e.,

$$0 < \epsilon_h << 1 \tag{30}$$

or a monotonically decreasing sequence, $\epsilon_h = \epsilon_h(n)$, satisfying the conditions:

$$0 < \epsilon_h(n) \leq 1, \sum_{n=1}^{\infty} \epsilon_h(n) = \infty, \sum_{n=1}^{\infty} \epsilon_h^2(n) < \infty. \tag{31}$$

As for the set point of (28), i.e., $h^*_\sigma(s_{n+1})$, it is defined, based on the sensor believability (5), as follows:

$$h^*_\sigma(s_{n+1}) \triangleq \begin{cases} B, & \text{if } s_{n+1} = \sigma \\ \frac{1-B}{2}, & \text{if } s_{n+1} \neq \sigma. \end{cases} \tag{32}$$

Thus, the dynamical system (28)-(32) defines the evolution of $\hat{P}_n(V)$ based on sensor $\mathbf{S}$ measurements and its DQ. The limit of this evolution is characterized as follows:

Theorem 4.1: 1) Under Assumption (30), there exists $0 < \epsilon_0 << 1$, such that for all $0 < \epsilon_h < \epsilon_0$, recursive procedure (28), (29), (32), converges in probability to the limit given by:

$$h_\sigma(n) \xrightarrow{\text{P}} DQ.P(S=\sigma) + \frac{1-DQ}{3} \text{ as } n \to \infty. \tag{33}$$

2) Under assumption (31), convergence to the same limit takes place with probability 1.

Proof: See [9]. □

Thus, according to this theorem, $\hat{P}(V)$ depends not only on sensor $\mathbf{S}$ measurements, but also on DQ. Observe that if DQ is close to 1, the estimated pmf of V is close to the pmf of S, which is identical to what is postulated by classical statistics. However, if DQ is close to 0, the same measurements result in $\hat{P}(V)$ being practically uniform and independent of the sensor measurements. For all intermediate values of DQ, $\hat{P}(V)$ is an affine function of DQ.

The recursive procedure (28)-(32), referred to as the *h-procedure*, is the basis of the process variable assessment layer using data from a single sensor.

B. Process variable pmf estimation using data from multiple sensors

Consider process variable $\mathbf{V}$ monitored by two sensors, $\mathbf{S}_1$ and $\mathbf{S}_2$, with data quality DQ_1 and DQ_2, respectively. Let $\hat{P}^{S_i}(V)$, $i \in \{1,2\}$, be the estimate of the pmf of V obtained from sensor $\mathbf{S}_i$ measurements and the recursive procedure (28), (29), (30), (32), i.e.,

$$\begin{aligned} \hat{P}^{S_1}(V=\sigma) &\triangleq \lim_{n\to\infty} P(V=\sigma|s_1^1, ..., s_n^1; DQ_1), \\ \hat{P}^{S_2}(V=\sigma) &\triangleq \lim_{n\to\infty} P(V=\sigma|s_1^2, ..., s_n^2; DQ_2). \end{aligned} \tag{34}$$

The question addressed here is: How can one obtain an estimate of the pmf of V, based on the measurements of both sensors, $\mathbf{S}_1$ and $\mathbf{S}_2$, simultaneously? To answer this question, we use the so-called Dempster-Shafer combination rule [12]. Namely, let $\hat{P}^{S_1S_2}(V=\sigma)$, $\sigma \in \Sigma$, denote the sought estimate, i.e.,

$$\lim_{n\to\infty} P(V=\sigma|s_1^1, ..., s_n^1; DQ_1; s_1^2, ..., s_n^2; DQ_2).$$

Then, according to the Dempster-Shafer rule,

$$\hat{P}^{S_1S_2}(V=\sigma) = \frac{\hat{P}^{S_1}(V=\sigma)\hat{P}^{S_2}(V=\sigma)}{\sum_{\sigma} \hat{P}^{S_1}(V=\sigma)\hat{P}^{S_2}(V=\sigma)}, \ \sigma \in \Sigma. \tag{35}$$

Clearly, rule (35) can be used for more than two process variables (by combining all pmf's simultaneously and normalizing by their sum). Note that the entropy of $\hat{P}^{S_1S_2}(V)$ is not necessarily smaller than that of $\hat{P}^{S_1}(V)$ and $\hat{P}^{S_2}(V)$. So, the pmf with the smallest of three entropies should be used in the plant assessment layer.

V. Plant Assessment Layer

The purpose of this layer is to estimate the pmf of G, i.e., $\hat{P}(G)$, $G \in \Sigma_G$, using the process variable pmf estimates, $\hat{P}(V_1), ..., \hat{P}(V_M)$, and either plant model, $\mathbf{G}$: $[P(V_1|G), ..., P(V_M|G)]$ or $\mathbf{G}$: $P(V_1, V_2, ..., V_M|G)$, $V_i \in \Sigma$, $G \in \Sigma_G$ (see Subsection II-D). With either of these models, $\hat{P}(G)$ is evaluated based on Jeffrey rule [10] and Dempster-Shafer rule [12], using the following procedure:

(a) Given $[P(V_1|G), P(V_2|G), ..., P(V_M|G)]$, assign the initial plant pmf as

$$P_0(G) = \left[\frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right]. \tag{36}$$

(b) Calculate the initial joint pmf of V_i and G,

$$P_0(V_i, G) = P_0(G)P(V_i|G), \ i = 1, 2, ..., M. \tag{37}$$

(c) Calculate the marginal probability

$$P_0(V_i) = \sum_{G \in \Sigma_G} P_0(V_i, G),\ i = 1, 2, ..., M. \quad (38)$$

(d) Apply Jeffrey's rule:

$$\hat{P}(V_i, G) = P_0(V_i, G)\frac{\hat{P}(V_i)}{P_0(V_i)},\ i = 1, 2, ..., M. \quad (39)$$

(e) Marginalize (39) to obtain the plant pmf estimate

$$\hat{P}^{V_i}(G) = \sum_{V_i \in \Sigma} \hat{P}(V_i, G),\ i = 1, 2, .., M. \quad (40)$$

(f) If $M > 1$, combine the pmf's obtained in (40) using Dempster-Shafer rule, as follows:

$$\hat{P}(G = \sigma_{\mathrm{G}}) = \frac{\prod_{i=1}^{M} \hat{P}^{V_i}(G = \sigma_{\mathrm{G}})}{\sum_{\sigma_{\mathrm{G}}} \prod_{i=1}^{M} \hat{P}^{V_i}(G = \sigma_{\mathrm{G}})},\ \sigma_{\mathrm{G}} \in \Sigma_G. \quad (41)$$

If the plant model is given as $P(V_1, V_2, ..., V_M|G)$, marginalize it to obtain

$$P(V_i|G) = \sum_{V_{j \neq i} \in \Sigma} P(V_1, V_2, ..., V_M|G), \quad (42)$$

$i, j \in \{1, 2, ..., M\}$. Then, follow steps (a)-(f) above.

VI. Sensor Network Adaptation Layer

The sensor network adaptation layer is based on rational controllers and temporal properties described in this section.

A. Rational Controller

Rational controllers, introduced in [1], are decision making devices that possess two properties: *ergodicity* and *rationality*. The ergodicity property implies that all states in the decision space are visited with a non-zero probability. The rationality property implies that the residence time in states with a smaller penalty function is larger than in those with a larger one. The degree to which this distinction is made is referred to as the *level of rationality*.

In the current work, we use the rational controller defined by the following residence time in state $x \in X$:

$$T_x = \begin{cases} T_{\max}, & \text{if } \hat{I}_x(G) \leq \beta \\ \left(\frac{\beta}{\hat{I}_x(G)}\right)^N T_{\max}, & \text{if } \hat{I}_x(G) > \beta, \end{cases} \quad (43)$$

where $\beta > 0$ is a small number (design parameter), $T_{\max}$ is the largest residence time (also a design parameter), and $\hat{I}_x(G)$ is, as before, the entropy of plant assessment pmf in sensor network state x. Thus, this controller resides in states with small entropy for at most $T_{\max}$ and less than that in other states. To ensure ergodicity, the rational controller defined by (43) visits all states of the sensor network in a deterministic, round-robin manner.

Let τ_x, defined as

$$\tau_x = \frac{T_x}{\sum_{x \in X} T_x}, \quad (44)$$

be the relative residence time in state $x \in X$, and let $\hat{P}_x(G)$ be the plant assessment pmf associated with this state. Then, the plant assessment pmf to be reported to the plant operator, is evaluated as

$$\bar{\hat{P}}(G) = \sum_{x \in X} \tau_x \hat{P}_x(G). \quad (45)$$

The rational controller, described in this subsection and the pmf $\bar{\hat{P}}(G)$ are used in Section VII for numerical performance evaluation of the resilient monitoring system designed in this work.

B. Temporal properties of adaptation

From the temporal point of view, the adaptation layer consists of *epochs*; K epochs (where K is the number of states in the sensor network) comprise a *cycle*; at the end of each cycle, $\bar{\hat{P}}(G)$ is reported to the plant operator.

For each $x \in X$, the epoch consists of three periods:

- DQ evaluation period, T_{DQ}
- Process variable(s) and plant pmf evaluation period, T_{eval}
- Residence period in state x, T_x.

Assuming that the sensor measurements are provided every 0.01 seconds, and using the procedure described in Section III, T_{DQ} is evaluated to be 5 seconds. Using the procedures described in Sections IV and V, the duration of process variable and plant assessment, T_{eval}, is about 6 seconds. The maximum residence period, $T_{\max}$, can be selected as desired. If $T_{\max}$ is selected to be 1 second, the duration of each epoch is less than or equal to 12 seconds.

As mentioned above, K epochs constitute a cycle, wherein each of K states of the sensor network is visited. So, the cycle duration is, at most, $12K$ seconds. Thus, the resilient monitoring system designed in this paper provides the plant assessment pmf, $\bar{\hat{P}}(G)$, within at most $12K$ seconds. This temporal organization is used in the next section to test the performance of the resilient monitoring system designed in this work.

VII. Performance Evaluation of the Four-Layer Resilient Monitoring System

This section presents the performance evaluation of the designed resilient monitoring system for two sensor network configurations, namely, non-contentious and contentious. The systems considered and their parameters are described in the following subsection.

A. Systems considered

Non-contentious sensor network: This system is shown in Figure 1(a). The plant $\mathbf{G}$ consists of two process variables, $\mathbf{V}_1$ and $\mathbf{V}_2$. Each process variable has two dedicated sensors, i.e., sensor $\mathbf{S}_{ij}$, $i, j \in \{1, 2\}$, monitors process variable $\mathbf{V}_i$. The random variable $\tilde{V}_i$, $i \in \{1, 2\}$, that characterizes $\mathbf{V}_i$, takes values on $[0,\ 10]$. This interval is divided into three regions, $[0,\ 10/3)$, $(10/3,\ 20/3]$, and $(20/3,\ 10]$, where the process variable is viewed as L, N, and H, respectively. Moreover, $\tilde{V}_i$ is assumed to be a Gaussian random variable, whose distribution is specified as $\mathcal{N}(\mu_{\mathrm{V}_i}, \sigma_{\mathrm{V}_i})$, with the

standard deviation being sufficiently small so that any realizations of $\tilde{V}_i$ outside $[0,\ 10]$ can be ignored. Similarly, the values taken by sensor $\mathbf{S}_{ij}$ is described by the random variable $\tilde{S}_{ij}$, whose distribution is given by $\mathcal{N}(\mu_{\mathrm{S}_{ij}}, \sigma_{\mathrm{S}_{ij}})$. All the sensors are assumed to possess a sampling period $T_S = 0.01$ seconds.

The d.c. gains (3) of the process variables are $\alpha_{\mathrm{L}}^{\mathrm{V}_1} = 2$, $\alpha_{\mathrm{N}}^{\mathrm{V}_1} = 1.8$, $\alpha_{\mathrm{H}}^{\mathrm{V}_1} = 1.62$, $\alpha_{\mathrm{L}}^{\mathrm{V}_2} = 1.5$, $\alpha_{\mathrm{N}}^{\mathrm{V}_2} = 1.3$, and $\alpha_{\mathrm{H}}^{\mathrm{V}_2} = 1.1$. Each process variable, $\mathbf{V}_i$, is probed by a rectangular signal (19). The magnitudes of the probe signals are $A_0^{\mathrm{V}_1} = 0.05$ and $A_0^{\mathrm{V}_2} = 0.1$. The parameter, ϵ, associated with the *DQ* assessment layer (see (25)), is assigned as 0.02.

Regarding the h-procedure, we choose ϵ_h to be 0.01. The stopping rule of this procedure is defined as follows: $|h_\sigma(n+1) - h_\sigma(n)| < 10^{-4}$. For the assumed sensor sampling period and stopping rule, convergence of the h-procedure is achieved in approximately 6 seconds.

The plant models are assumed to be

$$P(V_1|G) = \begin{bmatrix} 0.9 & 0.045 & 0.055 \\ 0.05 & 0.91 & 0.055 \\ 0.05 & 0.045 & 0.89 \end{bmatrix}, \quad P(V_2|G) = \begin{bmatrix} 0.8 & 0.095 & 0.0975 \\ 0.1 & 0.81 & 0.0975 \\ 0.1 & 0.095 & 0.805 \end{bmatrix}. \tag{46}$$

With respect to the sensor network adaptation layer, the measure of rationality of the rational controller is assigned as $N = 2$. The parameter β (see (43)) is chosen as 0.01, which is the entropy of a pmf wherein the largest element is approximately 0.998, and the remaining two elements are equal. The maximum residence time, $T_{\max}$, is chosen as 1 second. Given the parameters introduced above, it turns out that for all scenarios considered, the plant assessment pmf, $\bar{\hat{P}}(G)$, is reported to the operator in roughly 165 seconds.

Contentious sensor network: This system is shown in Figure 1(b). Each process variable has one dedicated sensor. Additionally, a free sensor is wired to monitor either of the two process variables. Sensor $\mathbf{S}_i$ refers to the dedicated sensor that monitors $\mathbf{V}_i$, $i \in \{1, 2\}$, while $\mathbf{S}_{1,2}$ denotes the free sensor. The sensor measurements are distributed according to $\mathcal{N}(\mu_{\mathrm{S}_i}, \sigma_{\mathrm{S}_i})$ and $\mathcal{N}(\mu_{\mathrm{S}_{1,2}}, \sigma_{\mathrm{S}_{1,2}})$, respectively. All other parameters of this system remain the same as in the non-contentious case. For all scenarios considered, the pmf $\bar{\hat{P}}(G)$ is reported in approximately 121 seconds.

B. Performance analysis in the non-contentious case

The performance of the resilient monitoring system, under various scenarios, is described below:

Scenario 1: The plant is actually in the low state, i.e., $P(G) = [1,\ 0,\ 0]$, with $\mu_{\mathrm{V}_1} = 1.6$, $\mu_{\mathrm{V}_2} = 1.7$, and $\sigma_{\mathrm{V}_i} = 0.01$, $i \in \{1, 2\}$. Sensors $\mathbf{S}_{21}$ and $\mathbf{S}_{22}$ are captured, and their mean shifted to show normal. The statistics of the sensors are characterized by $\mu_{\mathrm{S}_{11}} = 1.5$, $\mu_{\mathrm{S}_{12}} = 1.6$, $\mu_{\mathrm{S}_{21}} = 6.0$, $\mu_{\mathrm{S}_{22}} = 5.8$, $\sigma_{\mathrm{S}_{11}} = 0.1$, $\sigma_{\mathrm{S}_{12}} = 0.13$, $\sigma_{\mathrm{S}_{21}} = 0.15$, and $\sigma_{\mathrm{S}_{22}} = 0.11$. Based on these data, the *DQ*'s of the sensors are evaluated as $DQ_{11} = DQ_{12} = 1.0$, $DQ_{21} = DQ_{22} = 0.02$.

The resulting performance of the monitoring system is illustrated in Figure 2. As one can see, the rational controller forces the captured sensors to be disregarded. The plant assessment pmf, $\bar{\hat{P}}(G)$, is $[0.8807, 0.0559, 0.0634]$, which indicates that the plant is, indeed, in the low state.

For the non-resilient system, the plant assessment pmf, $\hat{P}_{\mathrm{nr}}(G)$, is $[0.6828, 0.2765, 0.0407]$. This leads to the measure of resiliency being $MR = 0.6671$, which testifies to the efficacy of the designed resilient monitoring system.

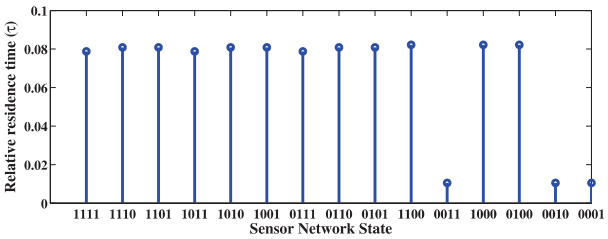


Fig. 2. Relative residence time for Scenario 1

Scenario 2: The plant and process variables are actually in the low state, and all four sensors are captured, with their means shifted to indicate high. The following statistics are assumed: $\mu_{\mathrm{V}_1} = 1.2$, $\mu_{\mathrm{V}_2} = 1.3$, $\sigma_{\mathrm{V}_i} = 0.01$, $i \in \{1, 2\}$, $\mu_{\mathrm{S}_{11}} = 8.2$, $\mu_{\mathrm{S}_{12}} = 8.3$, $\mu_{\mathrm{S}_{21}} = 9.1$, $\mu_{\mathrm{S}_{22}} = 9.2$, $\sigma_{\mathrm{S}_{11}} = 0.1$, $\sigma_{\mathrm{S}_{12}} = 0.15$, $\sigma_{\mathrm{S}_{21}} = 0.12$, and $\sigma_{\mathrm{S}_{22}} = 0.11$. The sensors *DQ*'s are identified as $DQ_{11} = DQ_{12} = DQ_{21} = DQ_{22} = 0.02$.

In this scenario, the rational controller resides in each state of the sensor network for roughly the same duration of time. The plant assessment pmf, $\bar{\hat{P}}(G)$, is $[0.3235, 0.3173, 0.3592]$, which implies that all plant states are almost equally plausible.

The non-resilient system obtains $\hat{P}_{\mathrm{nr}}(G) = [0.0069, 0.0059, 0.9872]$, which indicates erroneously that the plant is in the high state. The measure of resiliency is calculated to be $MR = 0.7733$, which, once again, reflects the advantages of the resilient monitoring system presented in this paper.

C. Performance analysis in the contentious case

Scenario 3: The process variables are actually high due to a plant anomaly, i.e., $P(G) = [0,\ 0,\ 1]$. The statistics of the process variables are assumed to be characterized by $\mu_{\mathrm{V}_1} = 9.1$, $\mu_{\mathrm{V}_2} = 9.0$, and $\sigma_{\mathrm{V}_i} = 0.01$, $i \in \{1, 2\}$. The sensor $\mathbf{S}_1$ is captured, and its mean shifted to show normal. The statistics of the sensors are characterized by $\mu_{\mathrm{S}_1} = 5.2$, $\mu_{\mathrm{S}_2} = 9.2$, $\mu_{\mathrm{S}_{1,2}} = 9.1$, $\sigma_{\mathrm{S}_1} = 0.1$, $\sigma_{\mathrm{S}_2} = 0.11$, and $\sigma_{\mathrm{S}_{1,2}} = 0.15$. Based on these data, we calculate sensor DQ's to be $DQ_1 = 0.0433$, $DQ_2 = 1.0$, and $DQ_{1,2} = 1.0$.

The most preferred states of the sensor network, with equal probability, are $(1(10)1)$ and $(0(10)1)$. The plant assessment obtained is $\bar{\hat{P}}(G) = [0.0130, 0.0120, 0.9750]$.

The non-resilient system reports

$$\hat{P}_{\mathrm{nr}}(G) = 0.5 \left(\hat{P}_{(1(10)1)}(G) + \hat{P}_{(1(01)1)}(G) \Big|_{DQ=1} \right). \tag{47}$$

Using (47), we obtain $\hat{P}_{\mathrm{nr}}(G) = [0.0219, 0.3214, 0.6567]$, which results in the measure of resiliency $MR = 0.94$.

Scenario 4: The plant is actually in the low state, i.e., $P(G) = [1,\ 0,\ 0]$, with $\mu_{\mathrm{V}_1} = 1.5$, $\mu_{\mathrm{V}_2} = 1.6$, and $\sigma_{\mathrm{V}_i} = 0.01$, $i \in \{1, 2\}$. The free sensor is captured, and its mean shifted to show high. When measuring $\mathbf{V}_1$, the statistics of $\mathbf{S}_{1,2}$ is characterized by $\mu_{\mathrm{S}_{1,2}} = 8.5$ and $\sigma_{\mathrm{S}_{1,2}} = 0.1$. When measuring $\mathbf{V}_2$, its mean and standard deviation are given by $\mu_{\mathrm{S}_{1,2}} = 8.7$ and $\sigma_{\mathrm{S}_{1,2}} = 0.1$, respectively. Moreover, the attacker's actions are such that sensor $\mathbf{S}_{1,2}$ does not reflect any shift in its expected value due to the probe signals, i.e., $\tilde{\mu}_{\mathrm{S}_{1,2}} = \mu_{\mathrm{S}_{1,2}}$. The statistics of the other sensors are characterized by $\mu_{\mathrm{S}_1} = 1.4$, $\mu_{\mathrm{S}_2} = 1.7$, $\sigma_{\mathrm{S}_1} = 0.13$, and $\sigma_{\mathrm{S}_2} = 0.1$. Based on these data, the sensors DQ's are identified as $DQ_1 = DQ_2 = 1.0$, and $DQ_{1,2} \approx 0$.

The resulting performance of the monitoring system is illustrated in Figure 3. The residence time is largest in states of the sensor network where both the dedicated sensors are active. The plant pmf assessment, $\hat{P}(G)$, is

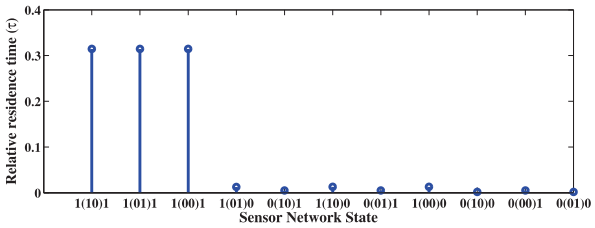


Fig. 3. Relative residence time for Scenario 4

$[0.9786, 0.0097, 0.0117]$.

The non-resilient system obtains $\hat{P}_{\mathrm{nr}}(G) = [0.4931, 0.4662, 0.0407]$. The question arises as to why this pmf takes place, given that the dedicated sensors indicate low, while the free sensor indicates high. This phenomenon can be explained as a manifestation of the *Zadeh counterexample* (see [13]): Assume we have two candidate pmf's of V, given by $P_1(V) = [0.95, 0.05, 0]$ and $P_2(V) = [0, 0.05, 0.95]$, i.e., indicating low and high, respectively. Combining them using Dempster-Shafer rule results in $P_{12}(V) = [0, 1, 0]$, which indicates normal. This conclusion was not obtained from either $P_1(V)$ or $P_2(V)$, which is paradoxical. In Scenario 4, the relatively large value of $\hat{P}_{\mathrm{nr}}(G = N)$ is precisely due to this phenomenon. Note that the resilient system prevents this aberration by appropriately assigning DQ, and adapting the sensor network according to the plant pmf's entropy in each state.

The measure of resiliency in this scenario is $MR = 0.97$, which, again, testifies to the efficacy of the resilient monitoring system designed in this work.

VIII. Conclusions and Future Research

This paper shows that the four-layer architecture developed is a viable approach to the design of resilient monitoring systems. Numerous problems, however, remain open. Some of them are as follows:

- Improving models of process variable, plant, and attacker by making them more general and practical. For example, attackers other than mean-based should be introduced and analyzed.
- Novel methods of active data quality assessment, which would be more effective and simpler than the probing technique developed in this paper.
- Improving the speed of convergence to the desirable sensor network state. This may be accomplished by using recursive versions of process variable and plant assessment estimates.
- Developing novel types of rational controllers that would lead to faster network adaptation.
- Fighting the "curse of dimensionality". An approach to combating this problem could be based on decomposition of the overall sensor network into smaller subsystems and adapting each of them separately.
- Most importantly, practical application of the developed resilient monitoring systems is a challenging task for future research.

Solutions to these problems will lead to a relatively complete and useful theory of resilient monitoring systems.

Acknowledgements

The University of Michigan students Naman Jhamaria and Heng Kuang are acknowledged for their participation in the initial stages of this research. Support for this research has been provided by the US Department of Energy under grant No. DE-AC07-05ID14517.

References

[1] S. M. Meerkov, "Mathematical Theory of Behavior," *Mathematical Biosciences*, Vol. 43, pp. 41-106, 1979.

[2] P. T. Kabamba, W.-C. Lin, and S. M. Meerkov, "Rational Probabilistic Deciders - Part I: Individual Behavior," *Mathematical Problems in Engineering*, Art. no. 35897, 31 pages, 2007.

[3] P. T. Kabamba, W.-C. Lin, and S. M. Meerkov, "Rational Probabilistic Deciders - Part II: Collective Behavior," *Mathematical Problems in Engineering*, Art. no. 82184, 34 pages, 2007.

[4] H. E. Garcia, N. Jhamaria, H. Kuang, W.-C. Lin, and S. M. Meerkov, "Resilient Monitoring System: Design and Performance Analysis," in *Proc. 4th Int. Symp. on Resilient Control Systems*, Boise, Idaho, USA, Aug. 9-11, 2011, pp. 61-68.

[5] H. E. Garcia, W.-C. Lin, S. M. Meerkov, and M. T. Ravichandran, "Data Quality Assessment: Modelling and Application in Resilient Monitoring Systems," in *Proc. 5th Int. Symp. on Resilient Control Systems*, Salt Lake City, Utah, USA, Aug. 14-16, 2012, pp. 124-129.

[6] H. E. Garcia, W.-C. Lin, and S. M. Meerkov, "A Resilient Condition Assessment Monitoring System," in *Proc. 5th Int. Symp. on Resilient Control Systems*, Salt Lake City, Utah, USA, Aug. 14-16, 2012, pp. 98-105.

[7] C. G. Rieger and K. Villez, "Resilient Control System Execution Agent (ReCoSEA)," in *Proc. 5th Int. Symp. on Resilient Control Systems*, Salt Lake City, Utah, USA, Aug. 14-16, 2012, pp. 143-148.

[8] C. G. Rieger, "Notional Examples and Benchmark Aspects of a Resilient Control System," in *Proc. 3rd Int. Symp. on Resilient Control Systems*, Idaho Falls, Idaho, USA, Aug. 10-12, 2010, pp. 64-71.

[9] H. E. Garcia, W.-C. Lin, S. M. Meerkov, and M. T. Ravichandran, "Resilient Plant Monitoring System: Design, Analysis, and Performance Evaluation," *Control Group Report No. CGR* 13-02, EECS Dept., University of Michigan, Ann Arbor, MI-48109, USA.

[10] Y. Peng, S. Zhang, and R. Pan, "Bayesian Network Reasoning with Uncertain Evidences," *International Journal of Uncertainty, Fuzziness, and Knowledge-based Systems*, Vol. 18, no. 5, pp. 539-564, 2010.

[11] S. Kullback, *Information Theory and Statistics*, John Wiley and Sons, NY, 1959.

[12] G. Shafer, *A Mathematical Theory of Evidence*, Princeton University Press, 1976.

[13] L. Zadeh, "A Simple View of the Dempster-Shafer Theory of Evidence and its Implication for the Rule of Combination," *AI Magazine*, Vol. 7, no. 2, pp. 85-90, 1986.