Integrating Control and Fault-Tolerant Wireless Network Design for Small Modular Nuclear Reactors

Wenchen Wang[1], Christopher D'Angelo[2], Daniel Mosse[1], and Daniel Cole[2]

[1]Computer Science Department, University of Pittsburgh, PA, USA
[2]Mechanical Eng and Materials Science Department, University of Pittsburgh, PA, USA
{*wew50,cjd66,mosse,dgcole*}*@pitt.edu*

***Abstract*—There has been an increasing number of cyber-physical systems (CPSs) in the last decade. CPSs sometimes include wireless networks that incur delay and errors. In this paper, we have developed an integrated design approach to combine control system and fault-tolerant wireless network design for an advanced, high-temperature, small, modular nuclear reactor (SMR). Our design approach is composed of two sub-problems: extracting network requirements from control systems and designing networks to meet such requirements. Focused on SMRs, our contributions are as follows: (1) we show how to derive a two-dimensional network performance requirement region in terms of network delay and error; (2) we propose a computation model to determine the network topology to meet network requirements with minimum energy consumption; (3) we conduct a case study with 12-hop and up to 78 nodes wireless sensor network to control a heat exchanger system in an SMR. The average difference between computation model results and simulation results is 4.1%, which confirms our computation model is accurate enough for such systems.**

I. Introduction

Real-time systems (RTSs) depend on the temporal and functional correctness of computations. In embedded systems in particular, a computing system typically controls a physical component, and therefore needs actuators that will effect change in the physical system. Nuclear Power Plants (NPPs) are examples of such embedded systems.

We focus on a particular class of embedded systems, namely small modular nuclear reactors (SMRs) that are controlled over a wireless network. SMRs are the next generation components in NPPs for efficient energy generation by nuclear fission, given that it does not require a large reactor to operate when small amounts of energy are needed, that is, it allows for incrementally bringing SMRs online as the need arises. We are loosely collaborating with Westinghouse in Pittsburgh to create realistic NPP scenarios. To the best of our knowledge, this is the first investigation of using a wireless network in an NPP to collect data, transmit it to the control room, and then to distribute control actions to the nodes that contain actuators. Wireless networks are not typically employed in NPPs due to regulatory bodies. This is exactly the reason for this study: exploring scenarios where wireless networks could be employed (e.g., cheaper nodes in a redundant network for abnormal scenarios or reducing cabling costs).

Work funded by the Department of Energy, Office of Nuclear Energy, under grant DE-NE000739.

The first two authors contributed equally to this work

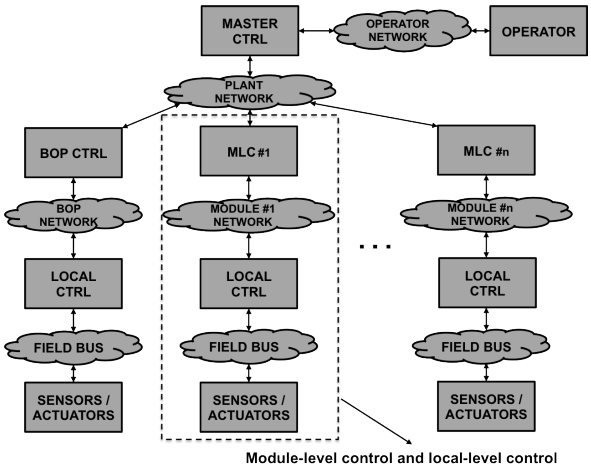


Figure 1: Supervisory Networked Control System Architecture for Advanced SMRs.

Given that NPPs have both sensors and actuators, data and commands have to travel to and from the control room, which is not co-located with the SMRs. It is well-known in control theory that time delays in a networked control system can degrade the performance of the system and lead to system instabilities [29]. Moreover, transmission errors can result in unwanted noise being processed by the control system leading to undesirable behavior. These facts lead to a need to investigate the real-time performance of a network and how network performance relates to the constraints and requirements of the control system.

Problem statement, assumptions, solution sketch: A typical SMR-based NPP will have multiple modules,

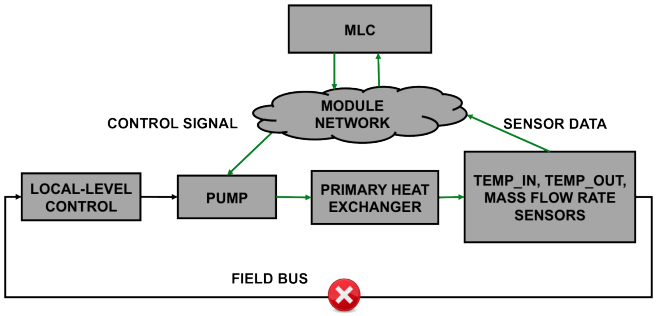


Figure 2: The subset of the dashed box in figure 1 "Module-level control and local-level control". Sensor data and control signal can be actively used through the wireless network when the field bus and/or local controller is deemed defective (red x)

each containing an integrated but smaller nuclear reactor [14, 26] whose energy output is a fraction of a traditional reactor. Ensuring SMR economic viability, however, requires addressing management and control, that is, creating a supervisory control system [8]. These integrated, complex systems are not typically co-located with one another, requiring even more cabling for the transmission of signals. Much research has gone into assessing the remaining useful life in cabling used for signal transmission in nuclear power plants [5]; with more cabling required for multiple SMRs in future NPPs, it is clear that more failure points are being introduced, leading to a necessity to add signal transmission and plant information redundancy; the use of wireless networks is one way to accomplish this. There are safety issues that must be addressed with the of wireless networks in NPPs, however, these issues are beyond the scope of this paper.

Figure 1 shows a hierarchical control system network architecture for monitoring and control of an NPP. This hierarchical controller has three layers: (a) the *master-level supervisory control* (master ctrl in Figure 1) coordinates and synchronizes the module-level controllers, each connected by a module network, as well as the balance of plant (BOP) (left part of Figure 1); (b) each *module-level control* (MLC) corresponds to one SMR; the MLC sets local controller setpoints and monitors the status of the SMR; and (c) the *local-level control* uses sensor data read from a (wired) field bus to regulate the system variables, and communicates with the MLC.

As a first step in SMR NPP control via wireless networks, we focus on one SMR module (see Figure 2). As a motivating example for this paper, we focus on the control of the primary heat exchanger (PHX), which is a non-linear system and principally used to remove heat from the reactor. Therefore, the control of the PHX influences both power produced by the SMR and the temperature of the reactor itself. This direct coupling to the reactor core makes this a good candidate for demonstrating the robustness of our integrated technique. Our wireless network would be useful as a backup network when the field bus or the local-level control fails.

Real-time delivery is important because spurious PHX system behavior induced by network error or delays could have the following implications on NPPs: (a) Thermal transients in system mechanical components, leading to fatigue or high thermal stresses; (b) Downstream effects on the core reactivity due to changes in coolant and fuel temperature and density [24]; (c) Taxing pump motors can lead to reduced reliability; and (d) Difficulty of monitoring and control of other systems in this highly coupled dynamic system.

During nominal operation we assume that time delays for the primary control loop can be ignored because the local-level controller is connected to sensors/actuators through a (wired) field bus. However, the delay in the secondary control loop is no longer negligible since the sensor data and control signal are sent over a wireless network. Co-location of MLC with all sensors/actuators in our system is not possible because the MLC is typically housed in the main NPP control room for safety and reliability reasons.

We assume that (a) links fail with a certain probability; we define *average link success ratio* (LSR) as the probability a message can be sent out successfully on that link and (b) Time Division Multiple Access (TDMA) [13, 23] is used for achieving real-time transmission; TDMA reserves slots for each node to transmit and therefore the network delay can be bounded.

Our TDMA network design that tolerates errors is combined with a control system design.

In this work, we developed a way to relate a controlled-system performance envelope to two metrics used in assessing wireless network performance: network transmission delay and error. Any network configuration that fits into the envelope derived for our particular controlled system will meet NPP performance requirements.

To save on the wireless network energy consumption (for reliability purposes), we place a certain number of nodes in the control area and wake up some nodes for transmission as needed. To meet the requirement and reduce network energy consumption, for a given LSR, we develop a computation model to determine the initial network topology with a minimum number of nodes. That is, we determine which nodes should be woken up to do transmission to satisfy the NPP network performance requirement, while saving energy.

We make the following three contributions: (1) We develop an integrated cyber-physical system performance envelope, which is a function of two network

performance variables, that describes the set of all wireless networks that will satisfy NPP controlled system performance requirements. When used as an inequality, a particular network topology's acceptability with respect to integrated cyberphysical system performance can be easily evaluated. (2) We propose a computation model to determine network initial topology to meet the network constraint and minimize network energy consumption. (3) As in [20], we evaluate our system through a case study; a 12-hop network with up to 78 nodes to control a heat exchanger system in an SMR. We verify our computation model by comparing with simulation results. Figure 3 shows our proposed design framework.

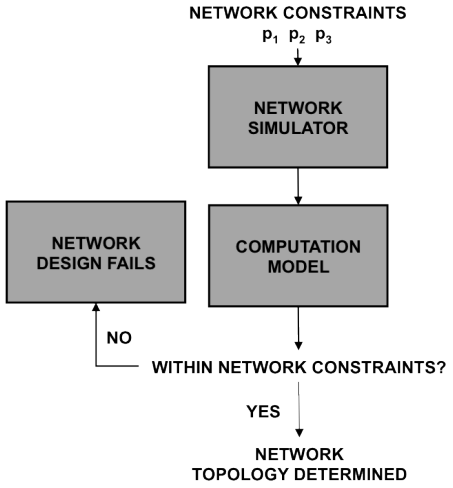


Figure 3: Iterative control and wireless network design framework.

II. Background and Related Work

A. Feedback Control Theory Primer

Current techniques for local control in commercial NPPs use classical feedback control theory, such as PI or PID control. Figure 4 shows a feedback control system where [r] is the reference or command input, [v] the sensor output, [u] the actuating signal, [d] the external disturbance, [y] the plant output and measured signal, and [n] the sensor noise. The exogenous input **d** is assumed to be zero in this paper. Block C refers to the controller, P is the plant, and F describes the feedback dynamics. The plant output is described by

$$y = \frac{PC(r - Fn)}{1 + PCF} \tag{1}$$

In this NPP we are most interested in how ranges of feedback delay and distortion affect the PHX and so we can define the auxiliary variable $e = r - Fn$ as the error. F is a network transmission delay of the form $\exp(-\Delta s)$ in the Laplace domain. We can therefore

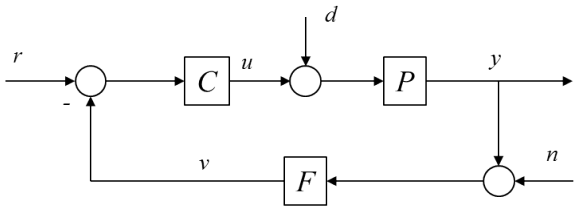


Figure 4: Elementary block diagram for a closed-loop dynamic system.

write the transfer function relating the system output y to e as:

$$\frac{y}{e} = \frac{PC}{1 + PCF}. \tag{2}$$

An elementary concept from feedback control theory is that of the Q-factor of a second-order system, which is related to a second-order system's damping ratio, ζ.

As $\zeta \to 0$ a system exhibits more oscillatory behavior. For $\zeta = 0$ the system is undamped. The characteristic equation of a second-order undamped system is:

$$s^2 + w_n^2 = 0 \tag{3}$$

in the Laplace domain. In the time domain and with nontrivial initial conditions (3), the systems time-domain behavior is $y(t) = \tilde{Y}\exp(jw_n t)$, which is purely oscillatory behavior and is unstable, where $\tilde{Y}$ is determined from initial conditions. A controlled PHX system can exhibit this type of behavior if network delay and error become overwhelming, which is clearly undesirable. Moreover, it is easily shown that if $\zeta < 0$ the time-domain behavior of the system will grow unbounded with time, which is unstable. The variable ζ is stressed in this context as it will be used in the analysis developed in section III. Network delay and errors could lead to a reduction in effective system damping ratio. These parameters are therefore used as input to the fault-tolerant wireless network design discussed in section IV.

B. Related Work

Networked control systems and performance requirements Delays and errors are unavoidable in any networked system. In [29, 31], the authors present two networked control system models with network-induced delay and with package loss and analyze system stability for each model. The authors do not examine the effect on performance, nor do they consider network delay and error *together* while providing a design strategy for both the network and control system. In [16], stability of a system with both network delay and error is considered simultaneously using a Lyapunov-based approach; the signal/system approach we use here not only guarantees a stable sys-

tem, but enables for seamless integration with network design and includes a way of evaluating the integrated cyber-physical system performance. In [12], the author derives a sufficient condition for the random access communication policy of shared wireless medium and design a control-aware random access communication policy. However, they did not specifically extract a network requirement from their control system.

Co-design of controller and wireless network To meet the requirements on system stability and performance, a few works present a systematic approach to integrate control systems and wireless networks, such as the water tank system [19, 20] and a smart water management system [17, 6]. In [20], the author incorporates emergency alarms of a coupled water tank system in wireless process control by delivering the emergency within their deadlines, but they do not emphasize how to balance the relation of errors and delay. The co-design of controllers and transmission schedules problem is divided into two sub-problems in [9]: schedule network to maximize the deadline-constrained reliability and to design a controller with optimum performance. However, they only consider a simple linear system and only provide deadlines for the network. We study a non-linear system with providing delay and packet loss relation, which gives more choices for network design, besides maximizing deadline-constrained reliability.

III. Nuclear Power Plant System

In this section we give a simplified description of the very complex nuclear power plant being controlled, and derive the delay and error requirements. We created a dynamic model of the Small Modular Advanced High Temperature Reactor (SmAHTR) [14] and implemented it in Simulink. SmAHTR is a fluoride-salt-cooled high temperature reactor whose molten-salt coolant ranges from 600 °C to 1000 °C. The reactor core dynamics are modeled using a 2-delayed neutron group spatial point kinetic model consisting of 3 axial core regions. This kinetic core model describes nuclear reactor physics, accounting for fissions in each region that are caused by the birth of neutrons in neighboring core regions. Fuel-coolant heat transfer is modeled using 2-state thermal hydraulic models for each axial region. Each integrated SmAHTR module has three primary (PHX) and emergency (EHX) heat exchangers. Figure 5 shows only one reactor model with one PHX and one EHX. The core outlet temperature is maintained by regulating the position of the control rods in the core using a PI controller and each PHX is independently controlled using a PI controller. Each PHX controller receives a power reference value from the supervisory control system and, the controller will

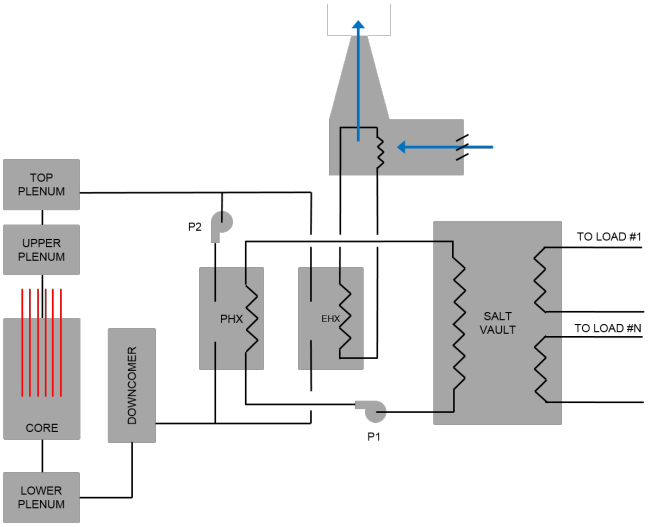


Figure 5: One SmAHTR reactor module coupled to the salt vault showing only one (out of three) PHX and EHX.

command pump P1 to vary the mass flow rate of molten salt through the secondary side of the PHX for meeting this reference power value. The SmAHTR plant couples multiple SMRs into a comparatively large energy repository, called a salt vault. (Additional details in [14].)

A. Controlled System in SmAHTR

In SmAHTR, each PHX has a variable-speed coolant pump (represented by P1 in Figure 5) as its primary actuator. PHX dynamics can be approximated by a first-order system with time delay [25, 28, 22]. Controller tuning for PHXs in NPPs is approached with special consideration to the dynamics of the reactor core. Core reactivity (i.e., the ratio of neutron production to loss) is sensitive to perturbations in inlet coolant temperature and flow as well as the rate of change in these parameters due to a nuclear-physical nonlinear temperature feedback effect. Considering the amount of overshoot associated with a small damping ratio, one can see the rippling effect on core flux distribution that large coolant flow and temperature variations can have, should the control system governing the PHX exhibit behavior with low damping characteristics. This is undesirable.

The internal time delay inherent to the SmAHTR PHX is described by a combination of physical and system measurement/control delays. System measurement and control delays arise from the calculation of the controller input, A/D conversion, D/A conversion, sensor delay, and network delays. The primary component for the internal time delay arises from the heat exchanger pipe residence time [22], which is a physical delay. The typical value of 1 second was used in our

analysis and simulations. The precise pipe residence time for a heat exchanger can be obtained through more exact modeling or via testing; the analytical approach developed herein is extensible to any heat exchanger pipe residence time. The transfer function relating secondary-side mass flowrate to primary-side outlet temperature for the PHX is given in the Laplace domain by:

$$P = k\frac{\exp(-\theta s)}{\tau s + 1} \tag{4}$$

where θ describes the process/internal time delay, τ is the characteristic time-constant of the approximated first-order system, and k is the open-loop system gain. In the analysis below, $k = 1$ for easier presentation.

Transmission of measurements and calculation of control signal over a wireless network will invariably lead to delays and signal errors/distortion, which must be considered when designing an NPP controller. The resulting PI-controlled closed-loop transfer function for the PHX system is the transfer function from the error e to the system output y

$$\frac{y(s)}{e(s)} = T(s) = \frac{\left(K_p + \frac{K_i}{s}\right)\left(\frac{\exp(-\theta s)}{\tau s + 1}\right)}{1 + \left(K_p + \frac{K_i}{s}\right)\left(\frac{\exp(-(\theta + \Delta) s)}{\tau s + 1}\right)}. \tag{5}$$

We take a signal and system norm approach to analyzing the effect that a distorted, delayed feedback signal has on a system's performance and stability. This linear combination of the reference and output (which is fed back) is the error, $e(s)$.

In the frequency domain, and from (5), we can see that the response of a system would be:

$$y(s) = T(s)e(s) \tag{6}$$

For brevity, we will drop the s in later derivations.

We use the 2-norm $\frac{||n||_2}{||y||_2}$, where $n = z - y$ is defined as the residual between the measured and true value. We define the following relationship:

$$\frac{||n||_2}{||y||_2} = R, \qquad R \in [0, 1) \tag{7}$$

Note that in (7) R is called the 2-norm measurement noise ratio and we assume that R is bounded by 1. Recall that a signal to noise ratio (SNR) is given by:

$$\text{SNR} = -20 \log \frac{||n||}{||y||} = -20 \log R \tag{8}$$

By bounding R as in Equation 7, we affirm the wireless network will not create a negative signal to noise ratio. Through taking a signal and system norm approach we can find a bounding worst-case response to any input

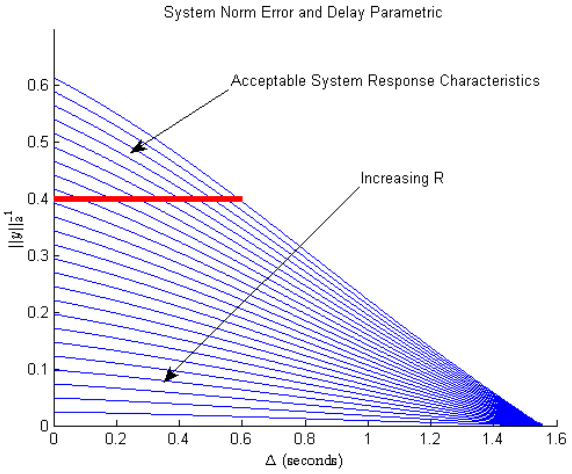


Figure 6: Parametric controlled PHX behavior as a function of network error and delay. Nuclear system considerations require that network performance fall within the bounded region shown.

through the following relationship [10]:

$$||y||_2 \leq ||T||_\infty ||u||_2 \tag{9}$$

where from the relationship given in (7) we can see that the system noise (which is a manifestation of error created by the wireless network) can be written as:

$$||n||_2 = R||y||_2 \tag{10}$$

We can find the bounded norm of the response of the system to a noisy input by: $||y||_2 \leq ||T||_\infty ||n||_2$, where $||n||_2$ represents the noisy input, which is recast through (10) to give us: $||y||_2 \leq \frac{1}{1-R}||T||_\infty$.

We define the delay in our feedback loop as Δ with the following relationship: $||y||_2 \leq \frac{1}{1-R}||T(\Delta)||_\infty$. It can be shown that $||y||_2 \to \infty$ as we approach some critical value for Δ, which we call Δ_{crit}. This is the point at which the effective damping ratio of our system is equal to zero. With no error introduced by the wireless network, $\Delta_{\text{crit}} = 1.554$s for our particular system. By varying the delay in the feedback loop and evaluating $||T||_\infty$ we can find the approximate system damping ratio by

$$2\zeta \approx ||y||_2^{-1} \tag{11}$$

We do not want our system to respond with a damping ratio of less than a threshold (we assume that the threshold of damping ratio is 0.2). In order words, if the system damping ratio is greater or equal to 0.2, we assume that network system meets the control system requirement. We develop the following criteria for the wireless network, see Figure 6.

Figure 6 is expressed in terms of parameters that can be extracted from a NPP wireless network performance criteria. The wireless network performance bounds

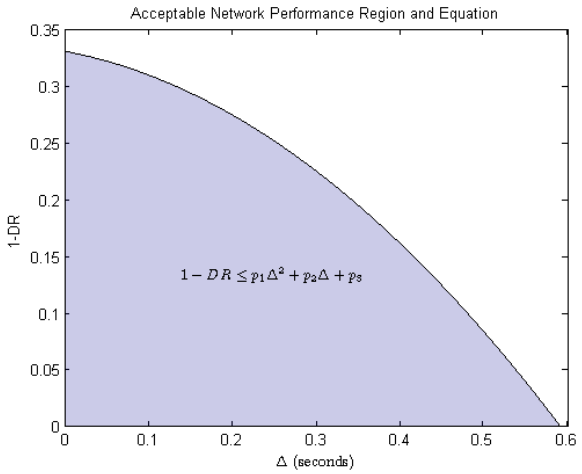


Figure 7: Acceptable network performance envelope for controlled PHX system design

come from the "acceptable system response characteristics" region of this figure. The 2-norm measurement noise ratio R, and delay, Δ, extreme for which a worst-case effective damping ratio of 0.2 will be achieved are: (1) R = 0.330, $\Delta = 0$; (2) for R = 0, $\Delta = 0.586$s.

From the analysis performed to generate Figure 6 and from (11), we extract the error values and network delay that traverse the stratum given by the boundary set at $||y||_2^{-1} = 0.4$. Note that the red line in Figure 6 represents $||y||_2^{-1} = 0.4$ and damping ratio = 0.2, and the region above the red line is the acceptable system response where damping ratio $\geq$ 0.2. The error and delay exactly on the boundary is $R = p_1\Delta^2 + p_2\Delta + p3$, where p_1, p_2 and p_3 are constants. It satisfies the requirement that the controlled system's effective damping ratio be equal to 0.2. Better performance is achieved if measurement noise ratio R and delay satisfy the inequality:

$$R \leq p_1\Delta^2 + p_2\Delta + p3 \tag{12}$$

where $p_1 = -0.714$, $p_2 = -0.138$, and $p_3 = 0.330$.

In our paper, we use network delivery ratio (DR), which was proposed [20] as the network reliability indicator, that is, the ratio of arrived messages ($DR \in [0,1]$). $1 - DR$ is the measurement noise induced to the control system from the network and both R and $1 - DR$ are in the same range $[0,1)$. Therefore, we can assert that $R = 1 - DR$. We derive the network delay and DR requirement as

$$1 - DR \leq p_1\Delta^2 + p_2\Delta + p3 \tag{13}$$

Any combination of $1 - DR$ and delay that satisfies the inequality above will fall into the region in Figure 7. The closer to $(0,0)$ in Figure 7, the better performance the control system will have. At the two extremes the NPP system and wireless network are fickle: (a) if the network delay exists at 0.586s, the network must have a perfect delivery ratio; (b) if 1-DR = 33%, the control system cannot withstand any delay in the feedback loop (which would be a physically impossible feat). The effect of the wireless network on controlled system performance is evaluated in the frequency domain, in this paper, through this signal/system norm approach for determining the worst-case effective system damping ratio. The wireless network design iteration is complete (i.e., acceptable delays) if $||y(R,\Delta)||_2^{-1} \geq 2\zeta$, where $\zeta \geq 0.2$ makes it for acceptable controlled-system behavior in the context of NPP operation.

IV. Meeting NPP Network Constraint

We focus on the wireless signal transmission for only the PHX system in an advanced SMR design. Three separate sensor signals are monitored and used for control input calculation, namely temperatures in and out (tin and tout, respectively), as well as mass flow rate of the primary heat exchanger (PHX). To tolerate sensor failures, each sensor has triple redundancy. We only consider link failures; node failures can be modeled by multiple link failures. To meet the NPP network constraint mentioned in Section III, we adjust the number of backup relay nodes, that is, add or reduce backup[1] nodes in the network.

In Figure 8, we use three redundant *duty sensors* for each measurement, located around the SMR (white nodes). A *Duty site* is the collective duty sensors for the same measurement. There are two data sinks (black nodes): (1) the MLC (top-right corner), and (2) the local actuator (LA), located in the bottom-left corner. The relay nodes (gray nodes) carry messages between sensors and the MLC.

There are two phases during operation: (1) in the *data collection phase*, duty sensors send their sensed values to the relay nodes towards the MLC, and (2) in the *forwarding phase*, after the MLC receives the measurements from the relay nodes, it makes a control decision about what action the LA should carry out and sends out the control signal to the LA. In this paper, similar to [20, 19], we assume the frequency of the above two phases is larger than the control system sample rate. Since the processes of data collection phase and forwarding phase are similar for the above assumption, we only consider one phase to simplify the presentation.

A. Fault Tolerant Network Protocol

Given that links may fail, to reduce the delivered result error, we use Bitvector fault-tolerant scheme [27]; we also assume that there is a single channel in these

[1]By "add backup relay nodes," we mean "to activate dormant nodes," not actually physically adding a node to the network.

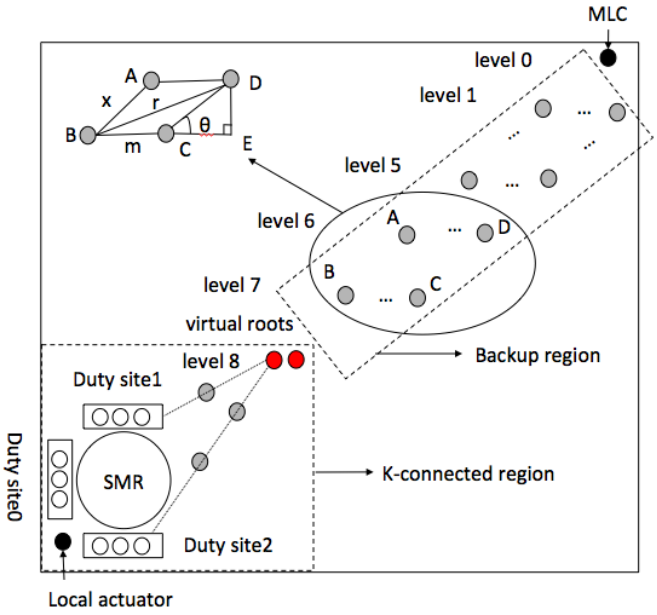


Figure 8: Fault tolerant relay nodes placement for PHX system within one SMR in NPP

simple, inexpensive sensor nodes. The bit vector contains 4 bits for each neighbor, to estimate the link quality of that neighbor; the bit vector is appended to the message sent by the node, in addition to the measurement value. A node has one primary parent and one or more backup parents. If the backup parent finds out (while overhearing and checking the bit vector) that the primary did not send out the values, the backup parent will compensate for it.

B. Network Node Placement

Optimal node placement in a wireless sensor network has been shown to be NP-hard [15]. Given that we only consider link failures, we apply k-edge disjoint algorithms [11, 15], instead of k-node disjoint algorithms [30, 7].

To gain more flexibility and efficiency in deploying relay nodes, we divide the network area into two regions, namely *k-connected region* and *backup region*. A *virtual root* (red node in Fig 8) demarcates the connection between the two regions. We determine the position (x, y) of the virtual root by calculating the geometric median [1] of data sinks, LA and MLC.

1) K-connected region: We define a *k-connected* region as the nodes and links having k-edge disjoint paths from each duty site to the virtual root. In the k-connected region, we apply Han's algorithm to place relay nodes [15].

To get k-edge disjoint paths from every duty sensor and the LA to the virtual root, we solve an optimization problem for finding a minimum-cost subgraph H of a digraph $G = (V, E)$ such that H contains k edge disjoint paths from a fixed node of G to any other node, which can be reduced to a weighted matroid intersection problem [11]. A common basis of these matroids corresponds to a subgraph that is the union of k disjoint spanning trees. Therefore, finding k-edge disjoint paths of a graph is to find the subgraph of k disjoint spanning trees with minimum cost. We also add $(k-1)$ backup nodes to the virtual root to improve reliability.

2) Backup region: In the backup region, primary relay nodes are placed in a "straight line" between the virtual roots and the MLC, called the *line of primary relay nodes*. The distance between two consecutive primary nodes is the same. In addition, there may be one or more *lines of backup nodes*, that is, each primary relay node may have one or more backup nodes. For example, in Figure 8, A and B are the primary nodes, and D and C are backups. Horizontally, the level located one primary node and its backup nodes is called one *level*. Each node in level l is able to listen to all the nodes in level $l-1$ and level $l+1$.

There are two reasons we have our network in two regions: (1) We add backup nodes[2] to each node in the primary line of relay nodes to improve network reliability ensuring each backup node is within the radio range of its neighbors (in fact, its primary node's neighbors). Adding k backup relay nodes for each relay node, yields $(k+1)^2$-edge disjoint paths, instead of $(k+1)$ as applying an k-edge disjoint algorithm. For example, in Figure 8, if we add one backup node (e.g., nodes D and C) for each primary relay node (e.g., nodes A and B), there will be 4-edge disjoint paths. (2) To ensure each node can hear all the nodes one hop from it, we place backup nodes as close as possible ("horizontally" right next to each other) in Figure 8. We assume the link between primary node and backup node (e.g., $A \rightarrow D$) never fails, given they are so close. The number of relay node in backup region is minimized, as shown below.

Theorem 1: Assuming faults are independent events, adding backup relay nodes as close as possible to each primary relay node minimizes the number of relay nodes in the backup region.

Proof: Referring to the inset in the upper left corner of Figure 8, note that the distance between two consecutive primary nodes (e.g., A and B) is x, which is a function the radio technology used and the power level each node transmits. We assume the primary relay sensors are fixed. The maximum distance between a primary node and its furthest backup node (e.g., B-C)

[2]In this paper, we use backup, backup nodes and backup relay nodes interchangeably

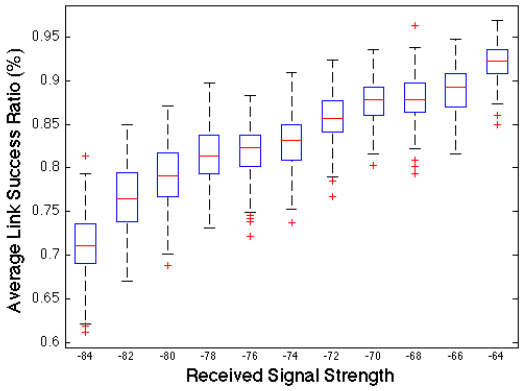


Figure 9: Average Link Success Ratio

is m. The maximum distance between sender and any backup receivers (e.g., B-D) is r.

We use an auxiliary imaginary point, E, that forms a right angle between D and the primary node B. θ is the angle DCE. Therefore,

$$(m + \cos\theta x)^2 + (\sin\theta)^2 x^2 = r^2 \tag{14}$$

Solving Equation 14, $x = \frac{\sqrt{4r^2 - 4(\sin\theta)^2 m^2} - 2\cos\theta m}{2}, r \geq \sin\theta m$. To minimize the number of primary nodes, we need to maximize x, the distance between two consecutive primary nodes. Therefore, m should be as small as possible since θ and r are constant, which means primary and backup nodes in the same level should be put as close as possible. ■

C. Delivery Ratio, Network Delay and Network Health Computation Model

In this section, we propose a computation model to determine the minimum number of nodes to have in the network, to meet the network constraint (Equation 13) and save energy. Our method is based on delay and network delivery ratio (defined in Section III-A the ratio of arrived messages).

1) Module-level controller delivery ratio: Based on our bitvector protocol, we compute the delivery ratio at the MLC, starting with the average LSR, p. We calculate the expected number of messages received by each primary relay node and its backup nodes (called a *level*) in an iterative way. Intuitively, each node sends messages that it has received to its parent nodes. The number of messages received varies (due to network errors) from 0 to the number of sensed values, but the total number of messages across a level cannot exceed the total number of messages (or sensed values), that is, there is no duplication of messages.

We introduce the concept of *state*, which represents the message-receiving situation of a level. A state of level l, s_l is $[c_{l,1}, c_{l,2}, ..., c_{l,n_l}, v_l, p_l]$, where n_l is the total number of nodes in level l, $c_{l,i}$ is the number of messages received by i^{th} node in level l, v_l is the total number of messages received over the level l, which is the summation of $c_{l,i}$, $\sum_1^{n_l} c_{l,i}$. s_l is calculated recursively from a state in previous level $l+1$, s_{l+1}. For example, let the previous level $l+1$ have n_{l+1} nodes, each node in level $l+1$ sends one message to the upper level l, which can be received (pending faults) by all the sensor nodes in the network.

Note that $v_l \leq v_{l+1}$, where v_{l+1} is the total number of messages received by level $l+1$. p_l is the probability of state s_l occurring and can be computed recursively as

$$\begin{aligned} p_l = \prod_{i=1}^{n_l} ((1-p_{l+1})^{i-1} p_{l+1})^{c_{l,i}} \\ \times ((1-p_{l+1})^{n_l})^{v_{l+1}-v_l} \end{aligned} \tag{15}$$

The above notation is a simplification of the problem, because there are many possible states at level l that can be derived from many possible states at level $l+1$. Therefore, strictly speaking, we should treat each element with another superscript, as follows. A state k of level l is represented as $s_l^k = [c_{l,1}^k, c_{l,2}^k, ..., c_{l,n_l}^k, v_l^k, p_l^k]$ computed from a state j of level $l+1$, s_{l+1}^j similarly defined. All the other definitions are also similar, but we omit the superscript k whenever no confusion arises.

To calculate the probability of all possible number of messages received by the MLC, we need to enumerate all possible states each level could have. For each level, we carry out the calculation with two phases, namely, a states-generating phase and states-combining phase. For the former, one/more states are generated by one of the states of the previous level. Formally, the new states of state k in level l are the combinations of all possible values of $c_{l,i}^k$ with the following conditions: $v_l^k \leq v_{l+1}^j$, $\forall i, 0 \leq c_{i,l}^k \leq v_{l+1}^j$. For the states-combining phase, the probability of states with the same total number of messages v_l^k are summed up and combined into one states. Since we compute each state's probability iteratively from the duty sites to the MLC, all possible number of messages will be accounted for at the MLC. The expected delivery ratio at the MLC is thus

$$DR = \sum_{i=1}^{m} (p_{MLC}(i) \times i), \tag{16}$$

where m is number of messages sent from duty sites, and $p_{MLC}(i)$ is the combined state probability that MLC receives exactly i messages.

2) Network health: Based on Equation 13, we define *network health* as a function of the delivery ratio (de-

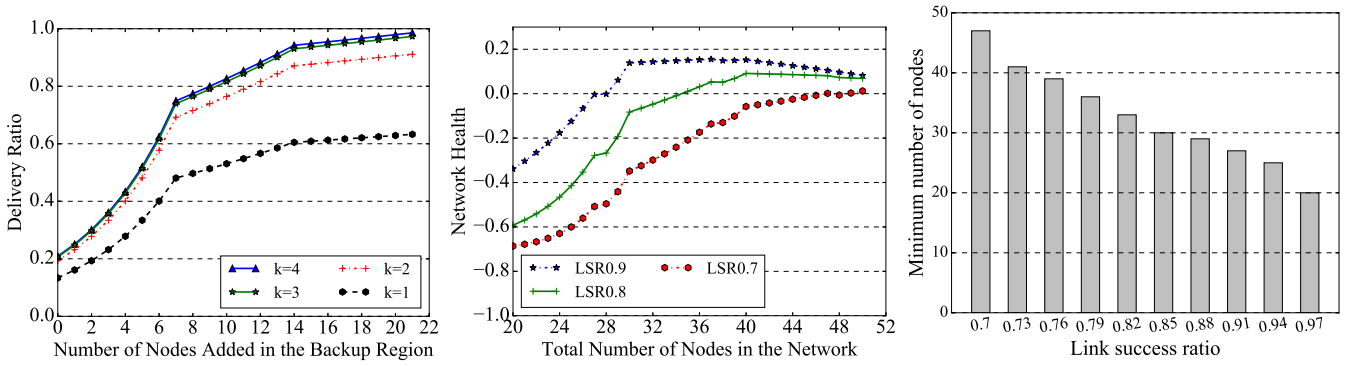


Figure 10: Computation model results (a) Delivery ratio at model-level controller; average link reliability =0.8 (b) Network health with link success ratio (LSR) 0.7, 0.8 and 0.9 (c) Computed minimum number of nodes needed to meet network constraint as a function of the network quality (LSR)

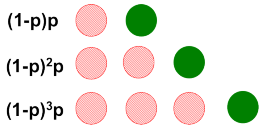


Figure 11: Illustration of the probability of all but one nodes failing when link success ratio is p. Red nodes do not receive messages and green nodes handle messages

fined in Equation 16), the error (or p, the probability of success of transmission for each link), and the worst-case network end-to-end delay $\Delta = N \times t_{slot}$, where N is the total number of nodes in the network and t_{slot} is the TDMA one time slot duration.

Note that the DR and the delay depend heavily on the number of nodes. Network health is formally shown in Equation 17 and is derived from the needs of the NPP for accuracy and timeliness.

$$NH = p_1\Delta^2 + p_2\Delta + p_3 - (1 - \text{DR}) \qquad (17)$$

When $NH \geq 0$, we say the network constraint is met. Therefore, we can estimate the minimum number of network nodes needed to satisfy $NH \geq 0$. The greater NH is, the better performance the control system will have.

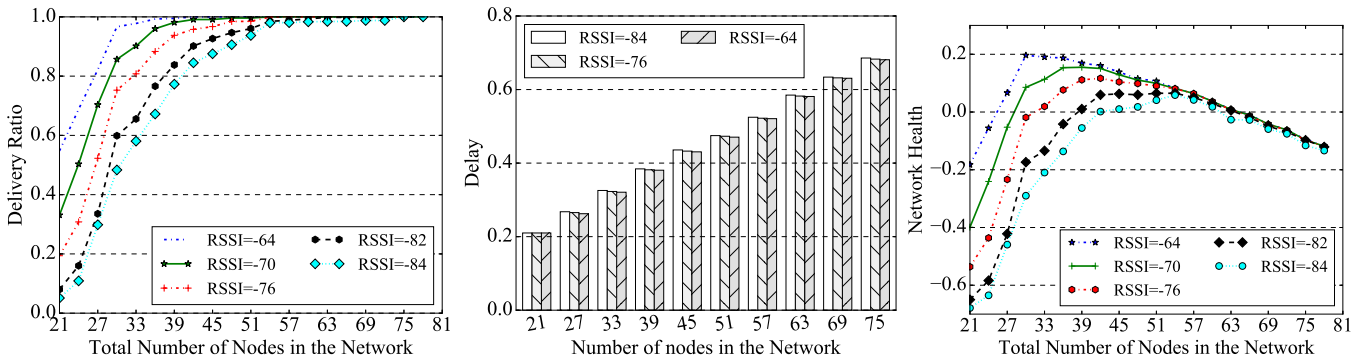
V. Case Study

We use MicaZ motes [2] to mimic cheaper, previous generation nodes with an indoor radio range of 20 m (65 ft). This distance necessitates 12 hops between the SMR and MLC (5 hops in the k-connected region and 7 levels in the backup region). Messages are sent hop by hop from duty sensors to MLC and then from the MLC to the local actuator with the commands to be executed. Typically, there are 2-3 lines of backup nodes (Section V-A), but we experiment with 7 lines, or 49 backup nodes for analysis purposes (Section V-B). We also assume the maximum connectivity degree of k-connected region is 4 (i.e., $k \leq 4$). We have up to 78 nodes in the network. We assume the same time slot duration, 10ms ($t_{slot} = 10ms$), of WirelessHART [3].

A. Computation Model Result

Starting with one line of primary nodes and fixed k-connected region, we add lines of backup nodes from virtual roots to MLC (i.e. add one node at a time in the first line of backup nodes from virtual roots to MLC, add one node at a time in the second line of backup nodes, etc.).

To show the trends clearly, we only show the results of adding up to 21 backup nodes, which means three lines of backup nodes. The delivery ratio at the MLC is shown in Figure 10a with average link success ratio 0.8 (other values for link reliability show the same trend; we choose one that is representative of NPPs and in range of [21]). Each line in Figure 10a represents the calculated delivery ratio as a function of the number of added backup nodes in the backup region for a fixed k-connected region. Three interesting observations follow. First, the inflection points happen when all primary relay nodes have the same number of backups (7 nodes or a complete line in this case). Second, while adding the first line of backup nodes, the delivery ratio exponentially increases due to the probability of sending messages from virtual root to MLC is $P_{virtual \to MLC} = ((1-p) \times p + p)^b \times p^{7-b}$, where b is the number of backup nodes added *in the first line of backup nodes*. As b increases, the $P_{virtual \to MLC}$ increases exponentially. Third, the slope decreases when adding more lines of backups. Figure 11 demonstrates the reason: the probability of using the last node in one level handling messages decreases as the number of backup nodes in each level increases, which explains why the slope of the first line of backup nodes is the steepest. From this result, we can decide how we add sensors to the network to gain the highest delivery ratio with the same number of nodes in the



(a) (b) (c)

Figure 12: Simulation results: (a) Delivery ratio for different nuber of nodes (b) Network delay for different number of nodes (c) Network health distribution for different number of nodes.

network. Figure 10b shows the average network health for different link success ratios. The system should operate above $NH \geq 0$, when network meets the control system requirements.

The estimated minimum number of nodes needed in the network to meet the error and delay constraints ($NH = 0$) required by the control algorithm is shown in Figure 10c as a function of the network quality (LSR). As the LSR decreases, more nodes needed in the network to meet control system requirement.

B. Simulation Result

In our simulation, we use the TOSSIM network simulator with wireless traces from a 21-node subset of the WUSTL Testbed [4]. Similar to [20], we use controlled Received Signal Strength with uniform gaps to simulate various wireless signal strength (RSSI) values. Figure 9 shows link success ratio statistics (out of 12,000 transmissions), where RSSI is between -64 dBm and -84dBm; note that at those values of RSSI, the average link success ratio is 0.93 and 0.71, respectively. We measured three metrics: average delivery ratio, average network delay and average network health.

Delivery Ratio (DR) is shown in Figure 12a for different RSSI values. The DR increases when the number of nodes increases, showing network gains in reliability. Obviously, the higher the RSSI, the higher the DR is; however, the difference decreases as a function of the number of nodes and RSSI becomes irrelevant for networks with many nodes (backups dominate then).

Network Delay shown in Figure 12b, increases as the number of nodes in the network increases; for each plotted value, we choose the topology with highest delivery ratio according to delivery ratio computation model to see where the boundary values are. This is because more backup nodes participate in passing the messages, which takes longer with TDMA protocols, that is, the backup nodes need slots in the schedule, and thus add to the network delay.

Network Health (NH) is shown in Figure 12c. Recall that the system should operate with $NH \geq 0$. It is interesting to see that the network health increases at first as the number of nodes in the network increases, because the delivery ratio increases faster than the network delay. But the network health then decreases as the number of nodes increases, because the network delay increases faster than the delivery ratio.

We also compare the computation results (CMR) with the simulation results (SR). Table I is the comparison of the minimum number of nodes of CMR (MinCMR) and minimum number of nodes of SR (MinSR) satisfying NPP requirements for various values of RSSI. *Diff* is defined as the percentage difference between MinCMR and MinSR, $Diff = (MinCMR - MinSR)/MinCMR$, indicating how much difference between our computation model and the realistic network simulation.

The MinCMR is different from MinSR due to the following two reasons: (1) CMR uses a uniform distribution of link success ratio to do the estimation of the minimum number of nodes in the network that would meet the network health constraints (see Eq 17), while the distribution of link success ratio in our simulation follows the CPM model [18] in Tossim. Figure 13 shows the histogram of the difference between LSR as a distribution, by subtracting with average value of LSR in the SR, for rssi=-64, rssi=-76 and rssi=-84. They are all different from uniform distributions. (2) In CMR, we estimate network health using the worst-case network delay. However, in the simulation, the network delay is typically smaller than the worst-case delay.

In addition, we observe that when the computation model we use for prediction has a higher standard deviation than the simulation model (see Table I), there is a higher difference in the number of nodes needed to keep $NH \geq 0$. The LSR dispersion degree (Figure 13) is highest for $rssi = -84$ and lowest for $rssi = -64$, which explains rssi=-84 shows the highest Diff.

Table I: Comparison of Model and Simulation results

rssi	LSR	LSR stdv	MinCMR	MinSR	Diff
-64	0.93	0.020	26	26	0%
-70	0.88	0.024	29	30	-3.4%
-76	0.82	0.031	33	32	3.0%
-82	0.77	0.035	37	39	-5.4%
-84	0.71	0.037	46	42	8.7%

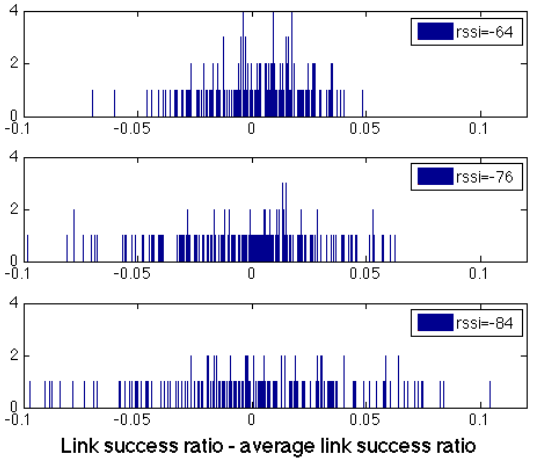


Figure 13: Histogram of LSR difference distribution for rssi=-64, rssi=-76 and rssi=-84

VI. Conclusions

In this paper, we design a controller for a Nuclear Power Plant system using wireless networks as an interactive solution with two parts: extract network requirements (delay and error) from the control system and then design network to meet the requirements with minimum energy consumption. Our simulation results verify our network design approach.

In the future, we will focus on dynamically redesigning the network at run time to adapt to the current system state.

References

[1] Geometric median: https://en.wikipedia.org/wiki/Geometric_median.

[2] Micaz mote: http://www.memsic.com/userfiles/files/Datasheets/WSN/micaz_datasheet-t.pdf.

[3] WirelessHart: http://www.hartcomm.org.

[4] Testbed: http://wan.cse.wustl.edu/index.php/Testbed.

[5] K. Anandakumaran, W. Seidl, and P. Castaldo. Condition assessment of cable insulation systems in operating nuclear power plants. *Dielectrics and Electrical Insulation*, 1999.

[6] K. Bhardwaj and R. Marculescu. Network-based modeling and analysis of cloud fraction and precipitation: A case study for the ohio river basin. In *CySWater 2015*.

[7] J. L. Bredin, E. D. Demaine, M. Hajiaghayi, and D. Rus. Deploying sensor networks with guaranteed capacity and fault tolerance. In *MobiHoc 2005*.

[8] D. Clayton and R. Wood. The role of instrumentation and control technology in enabling deployment of small modular reactors. In *American Nuclear Society Int'l Topical Meeting on Nuclear Plant Instrumentation, Control, and Human-Machine Interface Technologies*, 2010.

[9] B. Demirel, Z. Zou, P. Soldati, and M. Johansson. Modular co-design of controllers and transmission schedules in wirelesshart. In *CDC-ECC, 2011*, 2011.

[10] J. C. Doyle, B. A. Francis, and A. R. Tannenbaum. *Feedback control theory*. Courier Corporation, 2013.

[11] A. Frank and É. Tardos. An application of submodular flows. *Linear algebra and its applications*, 114:329–348, 1989.

[12] K. Gatsis, A. Ribeiro, and G. J. Pappas. Control-aware random access communication. In *ICCPS 2016*.

[13] S. Gobriel, D. Mosse, and R. Cleric. Tdma-asap: Sensor network tdma scheduling with adaptive slot-stealing and parallelism. In *ICDCS 2009*.

[14] S. Greene, J. Gehin, D. Holcomb, J. Carbajo, D. Ilas, A. Cisneros, V. Varma, W. Corwin, D. Wilson, G. Y. Jr., A.L.Qualls, F. Peretz, G. Flanagan, D. Clayton, E. Bradley, G. Bell, J. Hunn, P. Pappano, and M. Cetiner. Pre-conceptual design of a fluoride-salt-cooled small modular advanced high-temperature reactor (smahtr). Technical Report ORNL/TM-2010/199, Oak Ridge National Laboratory, 2010.

[15] X. Han, X. Cao, E. L. Lloyd, and C.-C. Shen. Fault-tolerant relay node placement in heterogeneous wireless sensor networks. *Mobile Computing, IEEE Transactions on*, 9(5):643–656, 2010.

[16] F. Jusuf and E. Joelianto. Stabilization of networked control system with time delay induced by network imperfections. In *ICCSII 2012*.

[17] S. Kartakis, E. Abraham, and J. A. McCann. Waterbox: A testbed for monitoring and controlling smart water networks. In *CySWater 2015*.

[18] H. Lee, A. Cerpa, and P. Levis. Improving wireless simulation through noise modeling. In *IPSN 2007*.

[19] B. Li, Y. Ma, T. Westenbroek, C. Wu, H. Gonzalez, and C. Lu. Wireless routing and control: a cyber-physical case study. In *ICCPS 2016*.

[20] B. Li, L. Nie, C. Wu, H. Gonzalez, and C. Lu. Incorporating emergency alarms in reliable wireless process control. In *ICCPS, 2015*.

[21] Z. Li, Z. Wu, Y. He, and C. Fulei. Hidden markov model-based fault diagnostics method in speed-up and speed-down process for rotating machinery. *Mechanical Systems and Signal Processing*, 19(2), 2005/03/.

[22] K. W. Mathisen, M. Morari, and S. Skogestad. Dynamic models for heat exchangers and heat exchanger networks. *Computers & chemical engineering*, 18, 1994.

[23] I. Rhee, A. Warrier, J. Min, and L. Xu. Drand: distributed randomized tdma scheduling for wireless ad-hoc networks. In *MobiHoc 2006*.

[24] J. K. Shultis and R. E. Faw. *Fundamentals of Nuclear Science and Engineering Second Edition*. CRC Press, 2007.

[25] S. Skogestad. Simple analytic rules for model reduction and pid controller tuning. *Journal of process control*, 13(4):291–309, 2003.

[26] J. Vujić, R. M. Bergmann, R. Škoda, and M. Miletić. Small modular reactors: Simpler, safer, cheaper? *Energy*, 45(1):288–295, 2012.

[27] W. Wang, D. Mosse, and D. G. Cole. Bitvector: Fault tolerant aggregation scheme for monitoring in nuclear power plants. In *ICESS 2015*.

[28] E. A. Wolff, K. W. Mathisen, and S. Skogestad. Dynamics and controllability of heat exchanger networks. *Proc. of Computer Oriented Process Engineering (COPE-91)*, pages 117–122, 1991.

[29] W. Zhang, M. S. Branicky, and S. M. Phillips. Stability of networked control systems. *Control Systems, IEEE*, 21(1):84–99, 2001.

[30] W. Zhang, G. Xue, and S. Misra. Fault-tolerant relay node placement in wireless sensor networks: Problems and algorithms. In *INFOCOM 2007*.

[31] W.-A. Zhang and L. Yu. Modelling and control of networked control systems with both network-induced delay and packet-dropout. *Automatica*, 44(12):3206–3210, 2008.