Defense Threat Reduction Agency
8725 John J. Kingman Road, MS
6201 Fort Belvoir, VA 22060-6201

DTRA-TR-15-53

TECHNICAL REPORT

A Robust and Resilient Network Design Paradigm for Region-Based Faults Inflicted by WMD Attack

April 2016

HDTRA1-09-1-0032

Arunabha Sen et al.

Prepared by:
Arizona State University
Tempe, AZ 85287

DESTRUCTION NOTICE:

Destroy this report when it is no longer needed.
Do not return to sender.

PLEASE NOTIFY THE DEFENSE THREAT REDUCTION AGENCY, ATTN: DTRIAC/ J9STT, 8725 JOHN J. KINGMAN ROAD, MS-6201, FT BELVOIR, VA 22060-6201, IF YOUR ADDRESS IS INCORRECT, IF YOU WISH IT DELETED FROM THE DISTRIBUTION LIST, OR IF THE ADDRESSEE IS NO LONGER EMPLOYED BY YOUR ORGANIZATION.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
00-04-2016	Technical	April 8, 2009 - December 31, 2014

4. TITLE AND SUBTITLE

A Robust and Resilient Network Design Paradigm for Region-Based Faults Inflicted by WMD Attack

5a. CONTRACT NUMBER
HDTRA1-09-1-0032

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Arunabha Sen, Junshan Zhang (Arizona State)
Kannan Ramchandran (U. of Calf.)
Chunming Qiao (SUNY)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Arizona State University,Tempe, AZ 85287
University of California, Berkeley, CA 94720
SUNY Buffalo, Buffalo, NY 14260

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Threat Reduction Agency
8725 John J. Kingman Road, STOP 6201
Fort Belvoir, VA 22060-6201

10. SPONSOR/MONITOR'S ACRONYM(S)
DTRA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
DTRA-TR-15-53

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution Statement A. Approved for public released; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The goal of this project was to conduct basic research on the impact of region-based faults on networks and to develop techniques to mitigate their adverse effects with robust and resilient designs. In order to capture single/multiple WMD attack scenarios, our formalism included the single region fault model (sRFM) and the multiple region fault model (mRFM). The goal of this project was to answer several basic research questions in network science and advance the understanding and knowledge of robust and resilient network design under region-based failures.

15. SUBJECT TERMS

WMD; sRFM; single-layer network; data integrity; networks

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	SAR	20	Paul Tandy
Unclassified	Unclassified	Unclassified			**19b. TELEPHONE NUMBER** *(include area code)* 703-767-4663

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

UNIT CONVERSION TABLE

U.S. customary units to and from international units of measurement*

U.S. Customary Units	Multiply by → / ← Divide by†		International Units
Length/Area/Volume			
inch (in)	2.54	$\times 10^{-2}$	meter (m)
foot (ft)	3.048	$\times 10^{-1}$	meter (m)
yard (yd)	9.144	$\times 10^{-1}$	meter (m)
mile (mi, international)	1.609 344	$\times 10^{3}$	meter (m)
mile (nmi, nautical, U.S.)	1.852	$\times 10^{3}$	meter (m)
barn (b)	1	$\times 10^{-28}$	square meter (m^2)
gallon (gal, U.S. liquid)	3.785 412	$\times 10^{-3}$	cubic meter (m^3)
cubic foot (ft^3)	2.831 685	$\times 10^{-2}$	cubic meter (m^3)
Mass/Density			
pound (lb)	4.535 924	$\times 10^{-1}$	kilogram (kg)
unified atomic mass unit (amu)	1.660 539	$\times 10^{-27}$	kilogram (kg)
pound-mass per cubic foot (lb ft^{-3})	1.601 846	$\times 10^{1}$	kilogram per cubic meter (kg m^{-3})
pound-force (lbf avoirdupois)	4.448 222		newton (N)
Energy/Work/Power			
electron volt (eV)	1.602 177	$\times 10^{-19}$	joule (J)
erg	1	$\times 10^{-7}$	joule (J)
kiloton (kt) (TNT equivalent)	4.184	$\times 10^{12}$	joule (J)
British thermal unit (Btu) (thermochemical)	1.054 350	$\times 10^{3}$	joule (J)
foot-pound-force (ft lbf)	1.355 818		joule (J)
calorie (cal) (thermochemical)	4.184		joule (J)
Pressure			
atmosphere (atm)	1.013 250	$\times 10^{5}$	pascal (Pa)
pound force per square inch (psi)	6.984 757	$\times 10^{3}$	pascal (Pa)
Temperature			
degree Fahrenheit (^oF)	$[T(^oF) - 32]/1.8$		degree Celsius (^oC)
degree Fahrenheit (^oF)	$[T(^oF) + 459.67]/1.8$		kelvin (K)
Radiation			
curie (Ci) [activity of radionuclides]	3.7	$\times 10^{10}$	per second (s^{-1}) [becquerel (Bq)]
roentgen (R) [air exposure]	2.579 760	$\times 10^{-4}$	coulomb per kilogram (C kg^{-1})
rad [absorbed dose]	1	$\times 10^{-2}$	joule per kilogram (J kg^{-1}) [gray (Gy)]
rem [equivalent and effective dose]	1	$\times 10^{-2}$	joule per kilogram (J kg^{-1}) [sievert (Sv)]

*Specific details regarding the implementation of SI units may be viewed at http://www.bipm.org/en/si/.

†Multiply the U.S. customary unit by the factor to get the international unit. Divide the international unit by the factor to get the U.S. customary unit.

PROJECT TITLE: A ROBUST AND RESILIENT NETWORK DESIGN PARADIGM FOR REGION-BASED FAULTS INFLICTED BY WMD ATTACK

Award Number: HDTRA1-09-1-0032

Final Report – 22nd March 2015

Arunabha Sen	Junshan Zhang	Kannan Ramchandran	Chunming Qiao
Arizona State University Tempe, AZ 85287 asen@asu.edu	Arizona State University Tempe, AZ 85287 junshan.zhang@asu.edu	University of California Berkeley, CA 94720 kannanr@eecs.berkeley.edu	SUNY Buffalo Buffalo, NY 14260 drqiao01@gmail.com

I. PROJECT BACKGROUND – GOALS OF THE PROJECT

The goal of this project was to conduct basic research on the impact of *region-based faults* on networks and to develop techniques to mitigate their adverse effects with robust and resilient designs. In order to capture single/multiple WMD attack scenarios, our formalism included the single region fault model (sRFM) and the multiple region fault model (mRFM). The goal of this project was to answer several basic research questions in network science and advance the understanding and knowledge of robust and resilient network design under region-based failures.

Our research effort had two interdependent goals: (i) to maintain *network integrity* in the face of WMD attack, and (ii) to maintain *data integrity* in the face of WMD attack. By network integrity we imply that (a) the network will not easily succumb (e.g., get disconnected) to region-based faults, and (b) even in the unlikely event of a network disruption (i.e., the network does get disconnected), the network will still retain some useful structural (topological) properties. By data integrity we imply the ability of the network to recover lost data easily (in terms of redundant storage and network bandwidth). The yearly breakup of objectives that were achieved under the above mentioned goals are outlined below:

Year 1: (i) Fault-tolerant design principles for region-based faults

(ii) Utility maximization techniques with imprecise knowledge of network state

Year 2: (i) Protection/restoration schemes for region-based faults

(ii) Data storage and retrieval (storage vs. bandwidth trade-off) for region-based faults

Year 3: (i) Impact assessment of region-based faults

(ii) Integrations of research results of years 1, 2 and 3

After the evaluation of our performance for the first three years, the DTRA decided to exercise the option of increasing the Period of Performance by another two years. The goal of these two years of effort was to extend our focus from a single-layer network to *multi-layer interdependent networks* (MLIN). It was noted that the study of MLIN is of significant importance as critical infrastructures, such as electric power distribution networks, communication networks, transportation networks and financial networks, are highly interdependent and the failure of one

network has inevitable consequences in other networks. One of the objectives of this project was to understand and assess the damage caused by a WMD attack on a MLIN. By damage assessment, we not only imply *immediate damage* but also the damage as it *progresses over time*, involving first-order, second-order and third-order effects. In addition to studying the impact of WMD attack related to progressive failures, the objectives of this research included studies related to:

- MLIN hardening - i.e., strengthening of multi-layer network structures (subject to budget constraints) so that impact of progressive failure is minimized
- Progressive recovery from failure due to a WMD attack
- Data resiliency to a WMD attack

The major objectives in the additional years 4 and 5 of the project included:

Year 4: (i) Hardening of multi-layer networks

(ii) Impact assessment of progressive (cascading) failure in MLIN

Year 5: (i) Strategy development for progressive recovery from failure in MLIN

(ii) Strategy development for data protection and resilience

We now outline the summary of findings in this project.

II. SUMMARY OF FINDINGS UNDER THE PROJECT

In keeping with the goal of this research effort to ensure *network integrity* as well as *data integrity,* the project's research thrust was divided into two directions – one to ensure network integrity and the other to ensure data integrity. We now summarize our findings in these two areas from our work in Years 1-3 and Years 4-5.

II.A. ENSURING NETWORK INTEGRITY

II.A.1. SUMMARY OF FINDINGS FROM YEARS 1-3

Our approach to enhancing the robustness of a network (with the goal of maintaining Network Integrity) was (i) to identify the most "vulnerable" part of the network in the event of a region-based fault and (ii) to strengthen the most "vulnerable" part of the network. The vulnerability of network can be viewed from several different perspectives, e.g., (i) whether the graph remains connected or disconnected, (ii) whether network utility remains over a minimum threshold or not, and (iii) whether network virtualization is possible or impossible. We now discuss our findings under these perspectives:

II.A.1.1. FROM THE PERSPECTIVE OF CONNECTIVITY

Traditional graph connectivity metric fails to convey any information of the following form, when the number of faults exceeds the connectivity of the graph:

- If the network is connected or disconnected
- If disconnected, into how many components
- If disconnected, what is the size of the largest component
- If disconnected, what is the size of the smallest component

As part of this effort we introduced a set of new metrics to capture such information. The metrics that were introduced are as follows:

- *Component Decomposition Number* $\left(CDN = \alpha_X(G)\right)$: Defined as the maximum number of components in which G decomposes to, when any $\kappa(G) + X$ number of nodes of G fails, where $\kappa(G)$ is the connectivity of the graph G and X is an integer
- *Smallest Component Size* $\left(SCS = \beta_X(G)\right)$: Defined as the size of the smallest component among the components in which G decomposes to, when any $\kappa(G) + X$ number of nodes of G fails.
- *Largest Component Size* $\left(LCS = \gamma_X(G)\right)$: Defined as the size of largest component among the components in which G decomposes to, when any $\kappa(G) + X$ number of nodes of G fails.
- *Region-based Component Decomposition Number* $\left(RBCDN = \alpha_R(G)\right)$: Defined as the maximum number of components in which G decomposes to, when all nodes of a region R fails.
- *Region-based Smallest Component Size* $\left(RBSCS = \beta_R(G)\right)$: Defined as the size of the smallest component among the components in which G decomposes to, when all nodes of a region R fails.
- *Region-based Largest Component Size* $\left(RBLCS = \gamma_R(G)\right)$: Defined as the size of the largest component among the components in which G decomposes to, when all nodes of a region R fails.

Using these metrics various real-world problem settings were identified and solutions techniques were established. The following studies summarize theses problems studied:

II.A.1.1.1 BEYOND CONNECTIVITY - NEW METRICS TO EVALUATE ROBUSTNESS OF NETWORKS

Robustness or fault-tolerance capability of a network is an important design parameter in both wired and wireless networks. Connectivity of a network is traditionally considered to be the primary metric for evaluation of its fault-tolerance capability. However, connectivity $\kappa(G)$ (for random faults) or region-based connectivity $\kappa_R(G)$ (for spatially correlated or region-based faults, where the faults are confined to a region R) of a network G, does not provide any information about the network state, (i.e., whether the network is connected or not) once the number of faults exceeds $\kappa(G)$ or $\kappa_R(G)$. If the number of faults exceeds $\kappa(G)$ or $\kappa_R(G)$, one would like to know, (i) the number of connected components into which G decomposes, (ii) the size of the largest connected component, (iii) the size of the smallest connected component. In this study, we introduced a set of new metrics that computes these values. We focused on one particular metric called region-based component decomposition number (RBCDN), that measures the number of connected components in which the network decomposes once all the nodes of a region fail. We studied the computational complexity of finding RBCDN of a network. In addition, we studied the problem of least cost design of a network with a target value of RBCDN. We were able to show that the optimal design problem is NP-complete and presented an approximation algorithm with a performance bound of $O(log\ K + 4log\ n)$, where n denotes the number of nodes in the graph and K denotes a target value of RBCDN [40].

II.A.1.1.2 DESIGN AND ANALYSIS OF NETWORKS WITH LARGE COMPONENTS IN PRESENCE OF REGION-BASED FAULTS

In this study, we introduced a new metric called region-based largest component size (RBLCS), that provides the largest size of the component in which the network decomposes once all the nodes of a region fail. We studied the computational complexity of finding RBLCS for a given network. In addition, we also studied the problem of least cost design of a network with a target value of RBLCS. We proved that the optimal design problem is NP-complete and presented a heuristic to solve the problem [41].

II.A.1.1.3 IMPACT OF REGION-BASED FAULTS ON THE CONNECTIVITY OF WIRELESS NETWORKS

In this study we investigated the impact of region-based faults on the connectivity of wireless networks. Through analysis and simulation, we provided results relating the probability of a network being connected as transmission range and the size of fault-region are varied. If $d_{min}\ (G)$ denotes the minimum node degree of the network, we provide the analytical expression for $P(d_{min}\ (G) \geq\ k)$, which represents the probability of the minimum node degree being at least k, for $k\ =\ 1$. Moreover, we compute $P(\kappa(G) \geq\ k)$, where $\kappa(G)$ represents the connectivity of the graph G formed by the distribution of nodes in the deployment area and examine the relationship between $P(d_{min} \geq\ k)$ and $P(\kappa(G) \geq k)$ when $k\ =\ 1$ [44].

II.A.1.2. FROM THE PERSPECTIVE OF SURVIVABLE NETWORK DESIGN

From the perspective of survivable network design we primarily addressed (i) how best to defend an attack using limited resources, (ii) how to quantify the damage (in terms of "downtime") due to failures and (iii) development of a new survivable design paradigm which was based on the concept of mapping applications, or "services" with redundant (backup) resources, and migration of the services to the surviving part of the network after an attack.

In the following discussion we briefly describe the work done and summarize our findings. These findings have been reported in the following conference and journal papers.

In [1] we proposed a new service node migration strategy to combat failures. To ensure failure tolerance performance, redundant nodes and links are pre-determined and required computing and communication resources are pre-reserved. After failures occur which affect the primary (working) nodes, the services are migrated to the backup nodes which can still communicate with other survived service nodes using the redundant links. However, instead of performing direct (one-step) mapping of a (virtual) service requirement graph to the physical substrate network as done in the past, we proposed a two-step approach, whereby during the first step, the virtual graph is enhanced with built-in redundancy, and then in the second step, the enhanced virtual graph is mapped to the substrate network. Our results have shown that this two step approach is more cost-effective.

In [2], we applied a novel game-theoretical approach to the problem of protecting a network from deliberate attacks. Specifically, we have addressed the problem of defending wired networking infrastructures against deliberate attacks by formulating it as a two-player zero-sum game. In this work, both the defender and the malicious attacker are assumed to have limited defending and attacking resources, respectively, and accordingly must decide how to optimally allocate their resources. Since the network topology can be complex, and the attacks are unpredictable in that the adversaries may attack places that may be considered as "safe", e.g., the

non-Min-Cut links, it is impossible to formulate the maximum network flow that can be achieved after an attack using a closed-form function. In addition, given the infinite strategy spaces (how much resources on which link) for both the attacker and defender; it is also unrealistic to enumerate all possible solutions. To derive the optimal defending solution, we first used MP-LP (Multi-Parametric Linear Programming) to divide the entire strategy space into several critical regions such that, given any strategy pair from the defender and attacker over each critical region, the min-cut of the affected network will not change. In this way, we also transformed the network maximum flow into a piecewise function over the entire strategy space. We have thoroughly investigated its equilibrium solutions. One of the insights we have gained is that simply protecting the Min-Cut links in the original networks (as advocated by traditional approaches) are not effective.

In [3], we quantitatively evaluate the impact of failures and the two "check-pointing" strategies which directly translate to the fault-tolerance performance of the proposed migration approach. More specifically, we address a fundamental question of how to predict the downtime of provisioned server infrastructure for a given finite duration considering concurrent failures. Our work is the first of the kind that provides a closed form analytical solution of the pdf of the "downtime", and two distinct methods using sample path analysis to estimate the pdf – a computational method which utilizes the limiting behavior of a birth and death process and a more parsimonious statistical sampling approach.

In [4], we proposed an efficient resource allocation scheme which models a given application/service resource requirement as a virtual infrastructure (VI), and then maps to the physical (substrate) network based on the concept of the virtualization. The problem of efficiently mapping a VI is a key problem in provisioning Infrastructure (and Network) as a Service. In this paper, we studied the problem of cost efficient VI mapping and proposed a novel approach called the virtual infrastructure mapping algorithm (VIMA) that jointly considers node mapping and link mapping. Such a close coordination between the link and node mapping stages increases the efficiency of the VIMA algorithm. We compared the performance of our VIMA algorithm with other VI mapping algorithms such as NSVIM, vnmFlib and R-ViNE under various performance metrics using simulation. Our simulation results and analysis showed that the VIMA algorithm outperforms the other algorithms in terms of VI mapping costs and path length of VI links.

In [5], we took our earlier work a step further by addressing the problem of efficiently mapping a VI to a substrate while guaranteeing the VI's survivability in the event of failures in the substrate. In this paper, we studied the survivable VI mapping problem to protect against link failures in the substrate. We first proposed a solution based on traditional shared protection (survivable virtual infrastructure mapping algorithm, P-SVIMA), and then proposed a novel VI node migration protection-based algorithm (MP-SVIMA) to minimize the computing and communication resource costs. The MP-SVIMA scheme takes advantage of the flexibility in where VI nodes are mapped in the substrate by migrating a VI node from the originally mapped physical location to a different location after a physical link fails in order to recover from link failures. We compared the efficiency of our solutions using simulations under various performance metrics.

II.A.1.3. FROM THE PERSPECTIVE OF MULTILAYER INTERDEPENDENT NETWORKS

As part of this work it was observed that although most existing works have focused on networks in isolation, many real-world networks indeed interact and are interdependent. As a consequence,

there was a need to develop a new network science for modeling and quantifying the impact of *interdependence* between multiple networks. In this research, we considered a cyber-physical system consisting of two interacting networks, networks, e.g., a cyber-network overlaying a physical infrastructure network. It was envisioned that such a system is more vulnerable to attacks since node failures in one network may result in (due to the interdependence between the cyber-network and the physical infrastructure network) failures in the other network, causing a cascade of failures that would potentially lead to the collapse of the entire system. To enhance system robustness, we proposed a "regular" inter-edge allocation strategy. We showed that this strategy yielded better system resilience against random failures than all other existing strategies. In other related studies researchers have initiated studies on cascading failures across multiple interdependent networks. The model that is often used is the following: There are two interconnecting networks, say network A and network B, where each node in A supports one node in B and vice versa. The interdependence between two networks are represented by inter-edges connecting network A and network B. Specifically, a pair of nodes from network A and network B are connected by a bi-directional inter-edge when they provide support to each other. In some other proposed models the inter-edges are unidirectional. Furthermore, each node supports (and is supported by) a random number of nodes from the other network. Clearly, the robustness of interdependent systems hinges heavily on the allocation of the inter-edges that connect nodes in one network to nodes in the other network as well as the type of inter-edge (bi-directional or unidirectional). In our study, we considered a regular allocation strategy where all nodes have exactly the same number of bi-directional inter-edges ensuring a completely uniform support-dependent relationship. In our design, we made sure that each node supports (and is supported by) the same number of nodes from the other network. We analyzed this new model in terms of its robustness against random attacks characterizing the steady state size of the functioning parts of each network. From a design perspective, we showed analytically that the proposed method of regular inter-edge allocation helps improving the robustness of the system over the random allocation strategy studied by other researchers. Indeed, for a given expected number of inter-degree (the number of nodes supported plus the number of nodes dependent) per node, we showed that (i) it is better (in terms of robustness) to use bi-directional inter-links than unidirectional links since it ensures that for each node the amount of support being received and the amount of support provided are equal, (ii) it is better (in terms of robustness) to allocate each node exactly the same number of bi-directional inter-edges as opposed to allocating a random number of them to each node. To the best of our knowledge, this was the first study that characterized the robustness of interdependent networks under regular allocation of bi-directional inter-edges. Also, it was the first study that determined analytically the optimum inter-edge allocation strategy. We believe that our findings in this area allowed a new perspective on the design of interdependent systems.

II.A.2. SUMMARY OF FINDINGS FROM YEARS 4-5

II.A.2.1. IMPACT ASSESSMENT AND RECOVERY FROM WMD ATTACK ON VIRTUAL INFRASTRUCTURES

We investigated the effect of large-scale failures of physical (substrate) networks on the virtual infrastructures (VI) or virtual networks (VN) supporting certain applications or providing certain services. We also designed and evaluated algorithms that allocate necessary (i.e., minimal) and sufficient primary and redundant resources to a VI, as well as algorithms that migrate applications and services, such that the VI (and its applications and services) can survive a large-

scale failure. Finally, we examined correlated failures in a datacenter to come up with a downtime estimation of a service which will be useful for deciding how much redundant resources are needed to keep the availability of the service above a given threshold.

II.A.2.2. Advances in Robust Network Design with Probabilistic Models in WMD attack setting

It was observed that most of the existing research on robust network design assumed deterministic models of link failures. As part of this project we considered a probabilistic failure model and examined its impact on the network design. More specifically, we assumed that the link capacity is random due to a WMD attack, and took a stochastic approach to study network management against a WMD attack.

We also considered random failures in a cyber-physical system consisting of two interacting networks, i.e., a cyber-network overlaying a physical network. It was envisioned that these systems are more vulnerable to attacks since node failures in one network may result in failures in the other network (due to their interdependencies) causing a cascade of failures that would potentially lead to the collapse of the entire infrastructure. The robustness of interdependent systems against this sort of catastrophic failure hinges heavily on the allocation of the (interconnecting) links that connect nodes in one network to nodes in the other network. As part of this body of work, we characterized the optimum inter-link allocation strategy against random attacks in the case where the topology of each individual network is unknown. In particular, we analyzed the "regular" allocation strategy that allots exactly the same number of bidirectional internetwork links to all nodes in the system. We showed, both analytically and experimentally, that this strategy yields better performance (from a network resilience perspective) compared to all possible strategies, including strategies using random allocation, unidirectional interlinks, etc.

We also investigated dynamic security assessment (DSA) in smart grid – one of the most important infrastructures nationwide, aiming to provide system operators important information regarding the transient performance of power systems under various possible contingencies. Specifically, we studied online DSA in a data-mining framework by taking into account the operating condition (OC) variations and possible topology changes of power systems during the operating horizon. A robust scheme was proposed based on adaptive ensemble decision tree (DT) learning. To mitigate the impact of possibly missing PMU data, multiple small DTs were first trained off-line using a random subspace method. In particular, the developed random subspace method exploited the hierarchy of wide-area monitoring system (WAMS), the location information of attributes, and the availability of PMU measurements, so as to improve the overall robustness of the ensemble to missing data. Then, the performance of the trained small DTs was re-checked by using new cases in near real-time. In on-line DSA, viable small DTs were identified in case of missing PMU data, and a boosting algorithm was employed to quantify the voting weights of viable small DTs. The security classification decision for on-line DSA was obtained via a weighted voting of viable small DTs.

II.A.2.3. Analysis of PMU measurements for grid monitoring and control against possible WMD attacks

We investigated big data processing of PMU measurements for grid monitoring and control against possible WMD attacks. Big data processing and analytics of synchrophasor measurements, collected from multiple locations of power grids by phasor measurement units (PMUs), have the great potentials to enhance various power system operations and control.

Compared to SCADA data, the much finer temporal granularity and the precise synchronization make synchrophasor data the most promising tool for dynamic phenomenon monitoring and dynamic security analysis (DSA). The use of PMU measurements for wide area control also has significant potential in providing enhanced resilience against WMD attacks. The reliance on a suitable communication channel to transport the signal adds additional complexity in terms of reliability and resilience.

Since power system operating conditions become increasingly dynamic and unpredictable, we identified three major requirements for enhanced synchrophasor-based DSA, and developed technical approaches accordingly.

- *Accuracy and robustness:* Enhanced synchrophasor-based DSA should be accurate, and more importantly, should be robust to the operating condition variation and power system topology change and missing synchrophasor measurements.

  Technical approach: Small DTs and the ensemble learning algorithm developed in [6,7] can be utilized to efficiently update the predictive models and the critical decision rules by gracefully incorporating new cases to account for changed situations.

- *Scalability:* Enhanced synchrophasor-based DSA should accommodate and facilitate the growth of synchrophasor system. First, the new synchrophasor data from newly-deployed PMUs should be seamlessly incorporated. Second, enhanced synchrophasor-based DSA should provide guidance for the placement of new PMUs.

  Technical approach: For the first objective, the random subspace method developed in [7] can be utilized to build small DTs based on new synchrophasor measurements only, and then, these newly-built prediction models can be incorporated by using ensemble learning algorithms. For the second objective, via data-mining, enhanced synchrophasor-based DSA can provide the importance ranking of bus attributes, and thus new PMUs can be deployed at buses that have highest importance.

- *Distributed implementation and parallel computing:* Enhanced synchrophasor- based DSA should facilitate distributed implementation and parallel computing.

  Technical approach: Small DTs build from the random subspace method [7] can make decisions independently of each other by using subsets of synchrophasor measurements.

When PMU measurements are utilized for wide area control, the interdependence of the communication channel transporting the signal and the physical infrastructure incorporates a newer layer of complexity in terms of reliability and resilience. The wide area signal could provide enhanced control performance, however the failure of the communication channel could result in the system being vulnerable in terms of reliability.

System resiliency in such situations can be provided by making the physical infrastructure more resilient. This feature can be achieved through novel control designs which utilize multiple input signals including wide area and local signals. The control structure can be designed robustly using modern robust control techniques with multiple input signals. With the wide area signals being available the controller would have superior performance. When the communication channel is lost the controller would still be guaranteed to stabilize the system but the performance of the controller would be slightly degraded.

System resiliency can also be enhanced by having redundant communication channels which transmit multiple wide area signals and a hierarchical set of controllers using different wide area

signals can be designed robustly. When the channel carrying the control input which provides the best performance is lost a detection algorithm will have to be designed to detect the loss of the signal and when this occurs the controller would have to switched to the controller corresponding to the next wide area signal in the hierarchy which provides the next best performance.

These concepts to enhance resiliency will significantly improve power system reliability and performance and will also leverage the nation's large investment in synchrophasor technology.

II.A.2.4. IDENTIFICATION OF THE "*K*" MOST VULNERABLE ENTITIES OF MULTI-LAYER INTERDEPENDENT NETWORKS

In this study we investigated techniques to identify the "*K*" most vulnerable entities (the entities whose failure results in the maximum reduction of system utility) in a multi-layer interdependent network system. In multi-layer interdependent network, a failure has the propensity to "cascade", i.e. trigger additional failures due to the nature of the interdependencies between them. Although in recent years, a number of models have been proposed to analyze and to gain a deeper understanding of interdependency in a multi-layered network system, most of these models are over simplified and, as such, fail to capture the complex interdependency that exists between entities of these networks. To overcome the limitations of current models, we have recently proposed the *Implicative Interdependency Model*, which is able to capture such complex interdependency relations. We proposed techniques to identify the "*K*" most vulnerable entities of an interdependent network utilizing this model.

We showed that depending upon the interdependency relationships shared amongst the entities, the problem can be solved in polynomial time for some special cases, whereas for some others, the problem is NP-complete. We also established that this problem is equivalent to computation of a fixed point of a multilayered network system and proposed a technique for its computation utilizing Integer Linear Programming. Finally, we evaluated the efficacy of our technique using real data collected from the power grid and the communication network that span the Maricopa County of Arizona [30].

II.B. ENSURING DATA INTEGRITY

II.B.1. SUMMARY OF FINDINGS FROM YEARS 1-3

II.B.1.1. DISTRIBUTED STORAGE DESIGN

It was noted that distributed storage of data files in different nodes of a network enhances the reliability of the data by offering protection against node failure. In the $(N, K), N \geq K$ file distribution scheme, from a file F of size $|F|$, N segments of size $|F|/K$ are created in such a way that it is possible to reconstruct the entire file, just by accessing any segments. For the reconstruction scheme to work it is essential that the segments of the file are stored in nodes that are connected in the network. A network spanning across a large area might get disconnected due to such massive but localized failures, i.e., region-based faults. As a consequence, design of a data distribution scheme robust against such failures is extremely important. The problem we considered to ensure data integrity under such condition is, given:

- a storage network G of n nodes and topology of the network and the network layout on 2-dimensional plane,
- storage capacity of each node in the network,

- parameters N and K for data coding
- a region radius r

Find out the distribution of the coded data file segments in the network G, so that even if the network gets disconnected due a region-based fault, at least one large component in the network will have at least K distinct coded file segments with which original file can be reconstructed. The distribution scheme will also ensure that the total storage requirement is minimized. We proved that this problem is NP-complete, and provided techniques for solving this problem [36].

II.B.1.2. ASSESSING AND MANAGING DATA INTEGRITY CHALLENGES IN WMD ATTACK SCENARIOS

We developed a general mathematical framework for studying the data integrity problem in the case of a catastrophic and massive network failure, which is a characteristic of a WMD attack. We tackle this problem using recent novel results in Network Coding theory to provide optimal and efficient methods for coding and placing the data redundantly in the network to make it resilient to a WMD attack. Our study leads to a two-layered solution that takes into account the real-world vulnerabilities of distributed storage systems, namely disk failures and malicious virus attacks:

- *Pre-Attack Preparation*: Any implemented solution for protection against massive network failures can be jeopardized by two main vulnerabilities that characterize distributed data storage systems, which are node failures and adversarial attacks. These phenomena are not a rare occurrence, and treating them as a WMD attack would be a rather costly and infeasible solution. To deal with this situation, we have introduced and studied the concept of system maintenance. The system maintenance mechanism can be thought of as an inexpensive and efficient process running in the background that repairs the system from failures and cleans it from viruses in order to keep it ready to face a WMD attack.
- *Post-Attack Recovery*: A WMD attack results in destroying a large part of the network, and therefore the loss of all the data that was stored there. To guarantee that the data can still be recovered after such a catastrophic event, it must be placed redundantly in different parts of the network. To this end, we investigate the use of erasure codes to generate redundant coded forms of the data. Of particular interest is the class of Maximum Distance Separable (MDS) codes, which can guarantee data recovery as long as a specified minimum number of nodes survive the attack. We investigated the construction of such codes that can be optimally coupled with the maintenance system described above.

Our findings in this area are summarized as follows:

- *Exact Repair Codes Exist*: The existence of repair codes that can restore an exact copy of the data lost due to a node failure was an open problem that is deeply connected to the general network-coding problem commonly thought to be very hard. We were able to make important progress in this direction by showing that exact repair codes exist for the two important minimum bandwidth regime (MBR) and minimum storage regime (MSR). Our techniques use the novel interference alignment method from the seemingly unrelated field of wireless communications. In fact, the codes constructed not only suffice to prove achievability, but also are very practical and are easy to implement.

- *Minimizing Disk Reads*: While the total amount of download required for repairing failed nodes is certainly of great interest, a second and perhaps equally important metric is that of disk-reads. The amount of disk-reads (or disk-IO) performed during repair is defined as the amount of data that needs to be read from the disks in that process. Recognizing the importance of this metric, we designed explicit algorithms that not only minimize the amount of data downloaded during repair, but also simultaneously minimize the amount of data read. We term this "repair-by-transfer", i.e., wherein a node helping in the repair reads only the data it wants to pass. The property of repair-by-transfer also completely eliminates the need for any computations to be performed at the helping nodes, resulting in two major advantages. Firstly, the minimization of the amount of reading at the nodes and the elimination of repair operations clearly has the potential to significantly speed up the repair operation. Secondly, repair-by-transfer also allows for the use of dumb nodes (instead of smarter ones that have associated processors), thus allowing a much cheaper and more flexible storage system design.
- *Coding Reduces the Information Retrieval Delay*: The use of redundancy in the form of codes in a distributed storage system is traditionally motivated by the need of reliability storage in the face of node failures due to various reasons e.g., machine failures, power outage or adversarial attacks. In this work, we show that coding not only makes the storage system more reliable but also at the same time can provide a faster access to the stored data. By combining a simple linear code with a novel request-scheduling algorithm, which we call Blocking-one Scheduling (BoS), we show analytically that it is possible to use codes to reduce data retrieval delay by up to 17% over currently popular replication-based strategies. Although in this work we focus on a simplified setting where the storage system stores a single content, the methodology developed can be applied to more general settings with multiple contents.
- *Data Protection Against Eavesdropping and Malicious Attacks*: In the case of an emergency like post WMD attack it is crucial to be able to access the sensitive data stored in a distributed fashion in a network while simultaneously safeguarding it from unwanted intruders who may eavesdrop on, and possibly alter, the stored information. An important aspect of distributed storage systems is node failures over time, necessitating; thus, a repair mechanism in order to maintain desired high system reliability. For such dynamic settings, we characterized an upper bound on the maximum amount of information that can be stored safely on the system. Moreover, we also provide explicit code constructions that achieve these bounds and hence are capacity achieving.

II.B.2. SUMMARY OF FINDINGS FROM YEARS 4-5

II.B.2.1. ASSESSING AND MANAGING DATA INTEGRITY CHALLENGES IN WMD ATTACK SCENARIOS – EXTENSIONS

We extended the work done in this domain in Years 1-3 (as outlined above). We summarize the *key findings* in this area from years 4-5 as follows:

- *Efficient and Distributed Secret Sharing in General Networks*: Shamir's (n, k) threshold secret sharing is an important component of several cryptographic protocols, such as those for secure multiparty-computation, key management, and Byzantine agreement. These protocols typically assume the presence of direct communication links from the dealer to all participants; in which case, the dealer can directly pass the shares of the secret to each participant. In our study, we consider the problem of secret sharing when

the dealer does not have direct links to all the participants, and instead, the dealer and the participants form a general network. We have developed an efficient and distributed algorithm for secret sharing over general networks that satisfy what we call the *k*-propagating-dealer condition.

We have derived information-theoretic lower bounds on the communication complexity of secret sharing over any network, which may also be of independent interest. We have shown that for networks satisfying the *k*-propagating-dealer condition, the communication complexity of our algorithm is $\theta(n)$, and furthermore, is a constant factor away from the lower bounds. We have also shown that, in contrast, the existing solution entails a communication-complexity that is super-linear for a wide class of networks, and is $\theta(n^2)$ in the worst case. Moreover, the amount of randomness required under our algorithm is a constant, while that required under the existing solution increases with n for a large class of networks, and in particular, is $\theta(n)$ whenever the degree of the dealer is bounded. Finally, while the existing solution requires considerable coordination in the network and knowledge of the global topology, our algorithm is completely distributed and requires each node to know only the identities of its neighbors. Our algorithm thus allows for efficient generalization of several cryptographic protocols to a large class of general networks.

II.B.2.2. Fast and Efficient Data Reconstruction in Distributed Storage Systems

We were able to design a new erasure-coded storage system that reduces both network traffic and disk I/O by around 25% to 45% during reconstruction of missing or otherwise unavailable data, with no additional storage, the same fault tolerance, and arbitrary flexibility in the choice of parameters, as compared to common distributed storage systems. It is based on novel encoding and decoding techniques. We tested the new system in Facebook's warehouse datacenters and observed a 36% reduction in the computation time and a 32% reduction in the data read time, in addition to the 35% reduction in network traffic and disk IO. We were also able to reduce the latency of degraded reads and perform faster recovery from failed or decommissioned machines [13, 14].

II.B.2.3. Design and Analysis of Data Access Protocol in Distributed Storage Systems

While the use of codes for providing improved security and integrity of data in distributed storage systems, how fast such systems can provide data or how we should optimize data access protocols are not studied. We first studied data access performance of data storage systems based on codes through the lens of queueing theory, and analytically characterized the latency performance of distributed storage systems. Then, we designed superior data access protocol, which uses redundant requests to improve data access performance [15, 16].

II.B.2.4. Privacy-aware Information Retrieval and Sharing

We want to retrieve data from a public database without revealing to the server which record is being retrieved. We proposed new systems where one can retrieve data from coded distributed database systems. Moreover, we also designed systems where one can search database by providing multimedia data such as voices, faces, or locations instead of textual descriptions. We also studied how we can share private information across a network with low communication cost. With our proposed distributed algorithm, one can share secrets across a general network without worrying about reveal your secret [17, 18, 19].

III. TRAINING & PROFESSIONAL DEVELOPMENT OPPORTUNITIES PROVIDED

As a part of this project, several PhD (approximately 10) students at the three participating universities have been trained in the design of robust and resilient networks in presence of region faults. One student who was deeply involved in the project from its inception, successfully defended her PhD dissertation in May 2014. In addition, two post-docs, one at University of California, Berkeley and the other at Arizona State University have actively participated in the project and thereby trained through this research effort.

IV. RESULTS DISSEMINATION

The results have been disseminated in the scientific community through publications in scientific journals and presentations at conferences. In addition, the PIs of this project have given several invited talks at other research universities, such as the Kings College in London, U.K. and industrial research laboratories, such as Deutsche Telekom in Berlin, Germany.

V. PUBLICATION LIST

1. B. Guo, C. Qiao et al., "A Novel Virtual Node Migration Approach to Survive a Substrate Link Failure", IEEE/OSA OFC/NFOEC, Paper JTh2A, Los Angeles, CA, March 2012
2. X. Xun, M. Li, J. Wang and C. Qiao, "Optimal Resource Allocation to Defend against Deliberate Attacks in Fiber Infrastructures", IEEE Infocom, March, 2012
3. Y. Du et al., "Downtime Predictions for Virtual Servers: A Study under Two Checkpointing Scenarios", Conf. on Info. Systems and Technology (CIST), Phoenix, Arizona, Oct. 2012.
4. H. Yu, V. Anand, C. Qiao, H. Di, and X. Wei, "A Cost Efficient Design of Virtual Infrastructures with Joint Node and Link Mapping", Journal of Network and Systems Management, Springer, Vol. 20, Issue 1, pp 97-115, 2012
5. H. Yu, V. Anand and C. Qiao, "Virtual Infrastructure Design for Surviving Physical Link Failures", The Computer Journal, 55 (8), pp. 965-978, 2012
6. M. He, J. Zhang and V. Vittal, "Robust On-line Dynamic Security Assessment using Adaptive Ensemble Decision Tree Learning," IEEE Transactions on Power Systems, vol.28, no.4, in press, 2013.
7. M. He, V. Vittal and J. Zhang, "Online Dynamic Security Assessment of Power Systems with Missing PMU Measurements: A Data Mining Approach," IEEE Transactions on Power Systems, vol.28, no.2, pp.1969-1977, May, 2013.
8. Miao He, Sugumar Murugesan, Junshan Zhang: "A Multi-Timescale Scheduling Approach for Stochastic Reliability in Smart Grids With Wind Generation and Opportunistic Demand." IEEE Trans. Smart Grid 4(1): 521-529 (2013)
9. Osman Yagan, Dajun Qian, Junshan Zhang, Douglas Cochran: "Optimal Allocation of Interconnecting Links in Cyber-Physical Systems: Interdependence, Cascading Failures, and Robustness." IEEE Trans. Parallel Distrib. Syst. 23(9): 1708-1720 (2012)
10. M. He and L. Yang and J. Zhang and V. Vittal, "A Spatio-temporal Analysis Approach for Short-term Wind Generation Forecast, " IEEE Transactions on Power Systems, Volume (29), Issue(4), 2014, p. 1611 - 1622.
11. M. He and J. Zhang, "A Dependency Graph Approach for Fault Detection and Localization Towards Secure Smart Grid," IEEE Transactions on Smart Grid, special issue on Cyber, Physical and System Security of Smart Grid, pp.~342-351, June 2011.
12. M. He and S. Murugesan, and J. Zhang, "Multiple Timescale Dispatch and Scheduling for Stochastic Reliability in Smart Grids with Wind Generation Integration," INFOCOM 2011 (mini-symposium).
13. K. V. Rashmi, Nihar B. Shah, Dikang Gu, Hairong Kuang, Dhruba Borthakur, and Kannan Ramchandran, "A "Hitchhiker's" Guide to Fast and Efficient Data Reconstruction in Erasure-coded Data Centers", ACM SIGCOMM, Aug 2014.
14. K. V. Rashmi, Nihar B. Shah and Kannan Ramchandran, "A Piggybacking Design Framework for Read-and Download-efficient Distributed Storage Codes", IEEE International Symposium on Information Theory (ISIT), Istanbul, Jul. 2013.

15. Nihar B. Shah, Kangwook Lee and Kannan Ramchandran, "The MDS Queue: Analysing Latency Performance of Codes", ISIT 2014.
16. Nihar B. Shah, Kangwook Lee and Kannan Ramchandran, "When Do Redundant Requests Reduce Latency?", Allerton Conference on Control, Computing and Communication, Urbana-Champaign, Oct. 2013.
17. Nihar B. Shah, K. V. Rashmi and Kannan Ramchandran, "One Extra Bit of Download Ensures Perfectly Private Information Retrieval", ISIT 2014.
18. Giulia Fanti, Matthieu Finiasz, Gerald Friedland, Kannan Ramchandran, "Toward efficient, privacy-aware media classification on public databases", Proceedings of ACM International Conference of Multimedia Retrieval (ICMR), April 2014
19. Nihar B. Shah, K. V. Rashmi and Kannan Ramchandran, "Secret Sharing Across a Network with Low Communication Cost: Distributed Algorithm and Bounds", IEEE International Symposium on Information Theory (ISIT), Istanbul, Jul. 2013.
20. B. Guo, C. Qiao, J. Wang, H. Yu, Y. Zuo, J. Li, Z. Chen, and Y. He, "Survivable Virtual Network Design and Embedding to Survive a Facility Node Failure", IEEE JLT, 32(3), pp. 483-493, 2014.
21. Z. Ye, X. Li, A. N. Patel, P. N. Ji, X. Cao, C. Qiao, "Upgrade-aware Virtual Infrastructure Mapping in Software-Defined Elastic Optical Networks", Photonic Network Communications, accepted for publication.
22. Z. Ye, A. N. Patel, P. N. Ji, and C. Qiao, "Survivable Virtual Infrastructure Mapping over Transport Software-Defined Networks (T-SDN)", IEEE/OSA OFC, 2014 (invited for a special issue of OSA/IEEE JOCN)
23. L. Liu, J. Xu, H. Yu. L. Li, C. Qiao, "A Novel Performance Preserving VM Splitting and Assignment Scheme", IEEE ICC, June 2014
24. A. N. Patel, Z. Ye, P. N. Ji and C. Qiao "Survivable Virtual Infrastructure Mapping with Shared Protection in Transport Software-Defined Networks (T-SDNs)", OECC, 2014.
25. S. Shirazipourazad, A. Sen, S. Bandyopadhyay, "Fault-tolerant Design of Wireless Sensor Networks with Directional Antennas", 14th International Conference on Distributed Computing and Networking, **Best paper award,** Journal version appeared in Pervasive and Mobile Computing (PMC) Journal 2014.
26. A. Mazumder, A. Das, C. Zhou, A. Sen, "Region-based Fault-tolerant Distributed File Storage System Design Under Budget Constraint", International Workshop on Reliable Networks Design and Modeling (RNDM) IEEE, Barcelona, Spain, November 2014. **Best paper award.**
27. A. Mazumder, C. Zhou, A. Das, A. Sen, "Progressive Recovery from Failure in Multi-layered Interdependent Network Using a New Model of Interdependency", International Conference on Critical Information Infrastructures Security (CRITIS), Limassol, Cyprus, October, 2014.
28. A. Das, A. Banerjee, A. Sen, "Root Cause Analysis of Failures in Interdependent Power-Communication Networks", IEEE Military Communications Conference (MILCOM), Baltimore, Maryland, October 2014.
29. C. Zhou, A Mazumder, A. Sen, M. Reisslein and A. Richa, On Shortest Single/Multiple Path Computation Problems in Fiber-Wireless (FiWi) Access Networks, 15th IEEE International Conference on High Performance Switching and Routing, Vancouver, Canada in July 2014.
30. A. Sen, A. Mazumder, J. Banerjee, A. Das, and R. Compton, "Identification of K Most Vulnerable Nodes in a Multi-layered Network Using a New Model of Interdependency", 6th IEEE International Workshop on Network Science for Communication Networks, held in conjunction with IEEE Infocom in Toronto, Canada, May 2014
31. S. Banerjee, A. Das, A. Mazumder, Z. Derakhshandeh, A. Sen, On the Impact of Coding Parameters on Storage Requirement of Region-based Fault Tolerant Distributed File System Design, IEEE International Conference on Computing, Networking and Communications (ICNC) IEEE, Honolulu, Hawaii, January 2014.
32. A. Mazumder, A. Das, S. Gokalp, N. Kim, A. Sen, H. Davulcu, Spatio-Temporal Signal Recovery from Political Tweets in Indonesia , International Conference on Social Computing (SocialCom) ASE/IEEE, Washington, D.C., September 2013.
33. S. Shirazipourazad, C. Zhou, Z. Derakhshandeh, A. Sen, Analysis of On-line Routing and Spectrum Allocation in Spectrum-sliced Optical Networks, IEEE International Communication Conference (ICC), Budapest, Hungary, June 2013.
34. S. Shirazipourazad, C. Zhou, Z. Derakhshandeh, A. Sen, On Routing and Spectrum Allocation in Spectrum-sliced Optical Networks, IEEE Infocom Mini-Conference, Torino, Italy, April, 2013.
35. S. Shirazipourazad, A. Sen, S. Bandyopadhyay, Fault-tolerant Design of Wireless Sensor Networks with Directional Antennas, International Conference on Distributed Computing and Networking (ICDCN) 2013. **Best paper award**.
36. S. Banerjee, S. Shirazipourazad and A. Sen, On Region-based Fault Tolerant Design of Distributed File Storage in Networks, IEEE INFOCOM (Mini-Conference), Orlando, USA, 2012.

37. S. Shirazipourazad, P. Ghosh and A. Sen, On Connectivity of Airborne Networks with Unpredictable Flight Path of Aircrafts, ACM MobiHoc Workshop on Airborne Networks and Communications, Hilton Head Island, SC, 2012.
38. S. Shirazipourazad, B. Bogard, H. Vachhani, A. Sen and P. Horn, Influence Propagation in Adversarial Setting: How to Defeat Competition with Least Amount of Investment, in Proceedings of the 21st ACM International Conference on Information and Knowledge Management (CIKM), Maui, HI, USA, 2012.
39. S. Shirazipourazad, P. Ghosh and A. Sen, "On Connectivity of Airborne Networks in Presence of Region-based Faults", IEEE Milcom, Military Communications Conference, Baltimore, MD, 2011.
40. S. Banerjee , S. Shirazipourazad, P. Ghosh and A. Sen, "Beyond Connectivity - New Metrics to Evaluate Robustness of Networks", IEEE Conference on High Performance Switching and Routing (HPSR), Cartagena, Spain, 2011.
41. S. Banerjee, S. Shirazipourazad and A. Sen, "Design and Analysis of Networks with Large Components in Presence of Region-Based Faults" IEEE International Conference on Communication, Kyoto, Japan, 2011.
42. S. Banerjee and A. Sen, Impact of Region-Based Faults on the Connectivity of Wireless Networks in Log-normal Shadow Fading Model "IEEE International Conference on Communication , Kyoto, Japan, 2011.
43. S. Banerjee, S. Murthy and A. Sen, "On a Fault-tolerant Resource Allocation Scheme for Revenue Maximization in Data Centers", in IEEE ANTS, 2011.
44. A. Sen and S. Banerjee, "Impact of Region-based Faults on the Connectivity and Capacity of Wireless Networks, (Invited Paper), *47th Annual Allerton Conference on Communication, Control, and Computing*, University of Illinois, Urbana-Champaign, September 2009.

Under Review:

45. S. Banerjee, S. Shirazipourazad and A. Sen, "Design of Distributed Data Storage Networks Robust Against Region-Based Faults," IEEE Trans. on Networking.
46. A. Sen, S. Banerjee, B. H. Shen, L. Zhou, B. Hao, S. Murthy, "A New Evaluation Metric of Fault-tolerant Wireless Networks," IEEE Trans. on Networking.
47. S. Shirazipourazad, B. Bogard, H. Vachhani, A. Sen and P. Horn, "Influence Propagation in Adversarial Setting: How to Defeat Competition with Least Amount of Investment", Computational Social Networks (Springer)
48. S. Shirazipourazad, C. Zhou, Z. Derakhshandeh and A. Sen, "On Routing and Spectrum Allocation in Spectrum-sliced Optical Networks", IEEE Transactions on Networking
49. S. Shirazipourazad, P. Ghosh and A. Sen, "On Connectivity of Airborne Networks" AIAA Journal of Aerospace Information Systems (formerly known as Journal of Aerospace Computing, Information, and Communication)

DEPARTMENT OF DEFENSE

DEFENSE THREAT REDUCTION
AGENCY
8725 JOHN J. KINGMAN ROAD
STOP 6201
FORT BELVOIR, VA 22060
ATTN: P. TANDY

DEFENSE TECHNICAL
INFORMATION CENTER
8725 JOHN J. KINGMAN ROAD,
SUITE 0944
FT. BELVOIR, VA 22060-6201
ATTN: DTIC/OCA

DEPARTMENT OF DEFENSE CONTRACTORS

QUANTERION SOLUTIONS, INC.
1680 TEXAS STREET, SE
KIRTLAND AFB, NM 87117-5669
ATTN: DTRIAC