2018

Efficient Interconnectivity Among Networks Under Security Constraint

Pankaz Das
University of New Mexico

Rezoan A. Shuvro
University of New Mexico

Mahshid Rahnamay-Naeini
University of South Florida

Nasir Ghani
University of South Florida

Majeed M. Hayat
Marquette University, majeed.hayat@marquette.edu

MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM), (2018): 88-93. DOI.

Efficient Interconnectivity Among Networks Under Security Constraint

Pankaz Das
Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM
Rezoan A. Shuvro
Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM
Mahshid Rahnamay-Naeini
Department of Electrical Engineering, University of South Florida, Tampa, FL
Nasir Ghani
Department of Electrical Engineering, University of South Florida, Tampa, FL
Majeed M. Hayat
Department of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM

Abstract:

Interconnectivity among networks is essential for enhancing communication capabilities of networks such as the expansion of geographical range, higher data rate, etc. However, interconnections may initiate vulnerability (e.g., cyber attacks) to a secure network due to introducing gateways and opportunities for security attacks such as malware, which may propagate from the less secure network. In this paper, the interconnectivity among

subnetworks is maximized under the constraint of security risk. The dynamics of propagation of security risk is modeled by the evil-rain influence model and the SIR (Susceptible-Infected-Recovered) epidemic model. Through extensive numerical simulations using different network topologies and interconnection patterns, it is shown that the efficiency of interconnectivity increases nonlinearly and vulnerability increases linearly with the number of interconnections among subnetworks. Finally, parametric models are proposed to find the number of interconnections for any given efficiency of interconnectivity and vulnerability of the secure network.

SECTION I. Introduction

Many communication networks (e.g., military, private, commercial network) consist of a private and secure communication infrastructure, which requires interconnections with external networks for enhanced communication range, capacity, and redundancy, to name a few. In particular, interconnectivity between a small-sized network (consisting of a smaller number of nodes with lower link-bandwidth) and a large-sized network (comprising of a larger number of nodes with higher link-bandwidth) is required for expanding the communication range and data rate of the small network. For example, a wide range of commercial and non-commercial communication systems and networks are used to support the military communications [1].

An interconnected network that is composed of several interdependent subnetworks of varying sizes and security levels is termed as *multilevel network* [2]. Due to interconnections, these subnetworks become interdependent through the gateways due to the exchange of information among each other. However, different systems usually have distinct security policies, control structures, and infrastructural vulnerabilities, as in the case of military and commercial networks for example [3]. Therefore, interconnections in multilevel networks may increase the vulnerability of a secure subnetwork due to the propagation of security threats from less secure subnetworks. As a result, the composition of the individually secure systems with different security policies is not secure [4]. For instance, due to varying levels of securities, the inter-operation and data sharing between military and commercial systems through interconnections may increase the probability of breaching the security of the army node [3]. Moreover, in a multilevel network, if attackers compromise a node in a subnetwork, then there is a possibility that a node in the other subnetwork may be compromised through the interconnected gateways. As an example, interconnecting a highly secure network with the public Internet results in an increased vulnerability to the secure system by exposing it to cyber threats such as injection of malware (viruses, worms), packet sniffing, denial-of-service (DoS) attacks (Section 1.6, [5]). In wireless networks, the internetwork links can be eavesdropped along with a strong possibility of jamming and sniff [5], [6]. In fact, attackers may get access to the confidential data [4], analyze traffic [3], and may use the data for their benefit, such as extract critical information, locate the mobile nodes or military troops thus endanger their lives, etc.

Clearly, interconnectivity among subnetworks needs to be addressed in order to compose an efficient and resilient multilevel network. In this paper, we define the *efficiency of interconnectivity* of a multilevel network and model the *resiliency (1-vulnerability*) of a secure subnetwork due to the propagation of security risk (e.g., virus and worms) through interconnections. The dynamics of propagation of security risk are modeled by two models, namely the evil-rain influence model [7] and the SIR (Susceptible- Infected- Recovered) model [8]. In addition' we formulate two optimization problems that maximize the efficiency of interconnectivity with a constraint on the vulnerability/resiliency. We use different network topologies and interconnection patterns in our simulation and find the resiliency of a secure military network due to interconnections with less-secure commercial systems. Based on simulation data, we propose two parametric models to find the optimal number of interconnections that maximizes the efficiency of the interconnectivity of the multilevel network under security (resiliency or vulnerability) constraints.

This paper is organized as follows. The relevant literature is presented in Section II. In Section III, we use the SIR model and evil-rain model to model the risk propagation in a network. The efficiency of interconnectivity is

optimized in Section IV. In Section V, we propose the parametric models based on the numerical simulation data. Section VIconcludes the paper.

SECTION II. Related Work

The literature of interconnectivity among different networks has mainly been focused on military and commercial networks. In [9] the authors discussed the crucial differences between the commercial and military system. While interconnecting the military network with commercial networks, Shake *et al*. suggested using highly secure gateway nodes [3]. In [10] the authors proposed to overcome security issues by adding some overhead (IPSec protocol) to the military data packets that are routed through commercial networks. Surprisingly, the analytical modeling of the propagation of security risk through interconnections has not been studied much in literature. The authors in [11], [12] argued that the epidemic models could approximate the propagation of computer viruses in networks. Based on the SIR epidemic model, a relatively close work is [13], where the authors tested different network topologies (e.g., stars, cliques, cycles) to design the intra-connectivity structure of a network to maximize the resiliency and connectivity. In contrast, this work deals with the interconnection between different independent subnetworks, specifically, between a highly secure network and networks with a relatively low level of security. Further, we have formulated constrained optimizations for maximizing efficient interconnections among subnetworks.

On the other hand, there are analytical works on the propagation of failures in cyber-physical systems, where the interdependency between networks can lead to a cascading failure [14], [15]. Buldyrev *et al*. used percolation theory to model the propagation of node failure due to the interdependency between power and communication networks [16]. In [17] Rahnamay-Naeini optimized the interdependency in a cyber-physical network using the evil-rain influence model. The major departure in this work from [17]is that, rather than assuming all the nodes are vulnerable to attack, we have considered nodes in the less secure network are vulnerable, and the vulnerability is assumed to propagate to the secure network.

SECTION III. Vulnerability of a Secured Network

Figure 1 shows the physical architecture of a multilevel network introduced in [2], where we consider a 3-level network with low, medium and high securities to represent distinct security policies of the multilevel network. The level-l network (e.g., a military system) is used for sensitive tasks such as command and control. These networks are typically very well-protected but run at a low and intermittent bandwidth [9]. In contrast, level- 2 and level- 3 networks may consist of mobile cellular networks, ad-hoc networks, etc. These networks usually have high-bandwidth, but low levels of security compared to the level-l network [10]. Here the two nodes, namely “Attack” and “Repair-ability,” represent two sources of failures and healing capability of the network, respectively. The red question marks in Fig. 1 show the tentative interconnections (i.e., how different subnetworks should be connected?).

The dynamics of the propagation of security risk among subnetworks of a multilevel network can be well-approximated by the existing SIR epidemic model and evil-rain influence model as explained in [11], [12] and [7], [13], [17], respectively. Below we demonstrate how we exploit these two models to model the propagation of security risks among subnetworks.

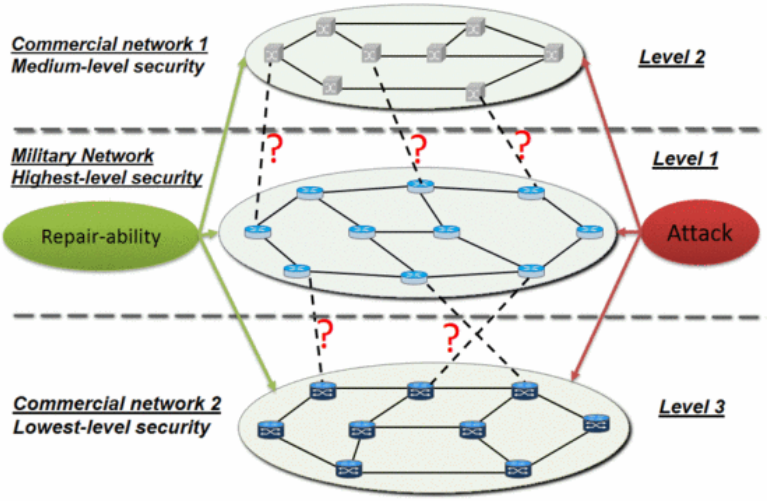


Fig. 1. A multilevel network infrastructure (e.g., 3 levels with military and commercial networks) with external attack and repair-ability in each network.

A. The Sir Epidemic Model

The epidemic model is a dynamical model that captures the spread of a disease in a network of large populations [8]. Among different versions of the epidemic model, we use the SIR model to characterize the dynamics of risk propagation in a network. In the SIR model, all the nodes are susceptible to attack initially, as such attackers can infect one or more nodes. The infected node compromises its neighbors with a transmission probability, denoted by τ (e.g., malware propagation). Further, as done in [13], the infected node is recovered/removed at the following time step by the recovery mechanism (the healing capability) of the SIR model. It implies that the vulnerability of the removed/recovered node is patched and the node will not be infected in future. In the SIR model, we define *resiliency* of a network G with N nodes as

$$R(G) = 1 - \frac{\mathbf{E}[N_f] - \mathbf{E}[N_i]}{N - \mathbf{E}[N_i]}, \quad (1)$$

where $\mathbf{E}[N_i]$ and $\mathbf{E}[N_f]$ are the expected number of nodes infected initially and eventually, respectively. Moreover, the difference $(\mathbf{E}[N_f] - \mathbf{E}[N_i])$ is the expected number of newly infected nodes at steady state due to the propagation of security risk from the initial compromised nodes. The steady state occurs when the propagation of risk stops and all nodes are in either susceptible state or recovered/removed state [13]. Here $\mathbf{E}[N_f]$ depends on τ as such $\mathbf{E}[N_f] = N$ if $\tau = 1$ and $\mathbf{E}[N_f] = \mathbf{E}[N_i]$ if $\tau = 0$. Hence, $0 \leq R(G) \leq 1$, where $R(G)$ is 0 if all nodes are compromised $(\mathbf{E}[N_f] = N)$. Finally, the vulnerability of the network is $(1 - R(G))$.

In the multilevel network, we take the different levels of securities of different subnetworks into account based on where the initial attack occurs. We assume the attack can only start at the less secure subnetwork by compromising some nodes; then the compromised nodes infect their neighbors with probability τ. Since the secure subnetwork is a part of the multilevel network, the attack also propagates to the secure network. For simplicity, we assume τ is equal for every node and network, where τ can be estimated from the real-world virus propagation data as done in [18].

B. The Evil-Rain Influence Model

The influence model is a networked Markov Chain (MC) framework for modeling interactions among nodes in a network, where the state evolution of a node depends on its MC, states of its neighbors and the influence from

neighbors. The influence received by a node from its neighbor is between 0 and 1, with the total influence received by a node from all its neighbors summing up to 1 [7]. A particular case of the binary influence model is the "evil-rain model," which has two autonomous nodes, named "source of failures" and "source of repairs" (e.g., the Attack and Repairability nodes shown in Fig. 1). The states of these autonomous nodes are fixed, and they are responsible for injecting failures and reparation (the healing capability) in the network, respectively. We model the risk propagation from one node to other nodes through influences between the nodes; i.e., the probability of propagation of risk between two nodes is equal to the influence among them.

In a network G of N nodes, we define the vulnerability as the expected number of compromised nodes at steady state [7]:

$$V(G) = \frac{1^T(\mathbf{I}-\mathbf{F})^{-1}\mathrm{u}}{N}, \quad (2)$$

where $\mathbf{u}$ is an N -dimensional vector that represents the external attack probability of each node, 1 is a column vector where all elements are 1, and $\mathbf{I}$ is an $N \times N$ identity matrix [7]. Moreover, $\mathbf{F}$ is the interconnection structure that represents influences between nodes. For 3 subnetworks, $\mathbf{F} = \begin{bmatrix} \mathbf{F}_{11}\mathbf{F}_{12}\mathbf{F}_{13} \\ \mathbf{F}_{21}\mathbf{F}_{22}\mathbf{F}_{23} \\ \mathbf{F}_{31}\mathbf{F}_{32}\mathbf{F}_{33} \end{bmatrix}$, where $\mathbf{F}_{ij}$ denotes the interconnection matrix between subnetwork i and j. In particular, $\mathbf{F}_{ij}(l,k) = c_{lk}^{ij}, 0 \leq c_{lk}^{ij} \leq 1$, implies that there is a connection of influence strength c_{lk}^{ij} between the $l$tb node of network i and kth node of network j. The higher the value of strength c_{lk}^{ij} the easier is the propagation of security risk from a compromised node to its neighbor, which could be, for instance, due to the lack of security solutions installed in their interface. Here we consider uniform influence $c_{lk}^{ij} = c$ for simplicity (similar to τ in the SIR model).

Similar to the resiliency in the SIR model, we define the resiliency as the fraction of nodes that are not compromised:

$$R(G) := 1 - V(G). \quad (3)$$

SECTION IV.Interconnectivity in Multilevel Networks

In this section, we maximize the efficiency of interconnectivity of the multilevel network under the security constraints.

A. Efficiency of Interconnectivity

Recall that the interconnectivity among different types of networks is essential for communicating outside their territories, redundant communication medium, etc., thus forming the multilevel network. The efficiency of connectivity among nodes for a network G with N nodes is [19]

$$W(G) = \frac{1}{N(N-1)} \sum_{u \in V} \sum_{v \in V-\{u\}} \frac{1}{d(u,v)^g}, \quad (4)$$

where V is the set of N nodes, $d(u,v)$ is the shortest path distance (i.e., number of edges in the shortest path) between node u and v, and g is the attenuation of the connection (here $g = 1$ **)**. In words, $W(G)$ is the efficiency of information exchange among nodes over the network. The efficiency of the connection between node u and v is inversely proportional to the shortest path distance between them. Note that, $d(u,v) = \infty$ implies there is no connection between node u and v, and $d(u,v) = 1$ implies there is a direct connection

between u and v. Moreover, with no connections among any nodes $W(G) = 0$, i.e., no node can communicate with other nodes in G. Interconnections enable communications among nodes (e.g., in a network where all nodes are directly connected with each other, $W(G) = 1$).

Since we are interested in the interconnectivity among subnetworks, we define the efficiency of interconnectivity of a multilevel network G_m as

$$\hat{W}(G_m) := W(G_m) - W(G_0), \quad (5)$$

where G_0 represents the multilevel network without any interconnections among the subnetworks.

B. Maximization of the Interconnectivity

Since different mathematical formulations are used in the SIR and evil-rain model for modeling the dynamics of risk propagation, we formulate two optimization problems based on these two models, which are described below.

First, for the SIR model, we maximize the efficiency of interconnectivity with a constraint on the resiliency as

$$\max_{e_{ij}, i \neq j} \hat{W}(G_m) \text{ subject to } R(G_s) \geq R_s, \quad (6)$$

where R_s is the minimum resiliency that is required for a secure subnetwork G_s, $e_{ij} \in \{0,1\}$ represents the connection between node i and j, and G_m is the multilevel network.

Similarly, using the evil-rain model we maximize the efficiency of interconnectivity under the vulnerability constraint,

$$\max_{\mathbf{F}_{ij}, i \neq j} \hat{W}(G_m) \text{ subject to } V(G_s) \leq V_s, \quad (7)$$

where V_s is the maximum vulnerability of the secure subnetwork G_s, $\mathbf{F}_{ij}$ is defined in the previous section, and here $i \neq j$ since we optimize interconnection between different networks.

Note that both optimization problems given by (6) and (7) are nonlinear and non-convex, for which no simple analytical solution or optimal algorithm exists. Here we recur to data from the numerical simulations to solve these optimization problems parametrically, which we demonstrate in the following section.

SECTION V. Numerical Simulation

In this section, we find the efficiency of interconnectivity and resiliency for different number and patterns of interconnections using both SIR and evil-rain model. Based on the simulation data, we propose our parametric models.

A. Network Topologies and Interconnection Patterns

We have considered different types of state-of-the-art network graphs to form a multilevel network, namely, Erdos-Renyi (**ER) graph** [8], **Barbasi and Albert (BA) graph** [8] and **Telia Carrier (TC) network**. Unlike ER and BA graph, the TC network is a real-world physical network topology with 21 nodes and 25 links, which are located over the USA [20].

Moreover, we have used the following link patterns to simulate the interconnectivity among subnetworks. **Assortative Link (AL):** Here the nodes with highest-degrees in one subnetwork connects to the nodes with highest -degree nodes in the other subnetwork, and so on. **Disassortative Link (DL):** The highest-degree nodes in one subnetwork connect to the nodes with the lowest-degree in the other subnetwork. **Random Link (RL):** Here connections among nodes are assigned randomly between two subnetworks. **1–1 Link (1-1):** Nodes are connected with shortest physical distances, i.e., a node in one subnetwork connects with the closest node in other subnetworks.

B. Multilevel Network Generation

We generate a 3-level network similar to the one shown in Fig. 1. When all three constituent subnetworks of the 3-level network are the ER graph, we denote it as the ER-ER-ER network. Similarly, we form the BA-BA-BA network and the ER-TC-BA network. Since the TC network has 21 nodes, we have used 21 nodes for generating the BA and ER network. Moreover, the TC network is a connected graph, and we generate the BA and ER networks so that these networks also form two connected graphs. In particular, for the ER network, we assign edges between nodes with probability p such that the generated graph is a connected graph (here we use $p = 0.18$ and check whether the graph is connected). A connected BA graph is formed by using the algorithm proposed in [21] with an average node-degree equal to 3.2, and the power-law exponent is 2.8. As shown in Fig. 1, we assume that the level-l network is the highly secure military network, whereas level-2 and level-3 networks are commercial networks with a lower level of security where the attack initiates. While interconnecting these subnetworks to form a 3-level network, we have used the same number of interconnections to connect the military network with two commercial networks. The connection patterns are AL, DL, RL, and 1–1. Here two commercial networks are used as two backup communication infrastructures for the military system, which can be scaled to any number of networks.

C. Simulation Results

We first discuss the simulation results of the SIR model. A node in the less secure subnetwork (commercial network) is attacked (compromised) initially, and then attack propagates with probability τ. Resiliency $(R(G))$ is calculated by using (1), where $\mathbf{E}[N_f]$ is computed by averaging over 1,000 realizations of the SIR model with one random initial failure $(\mathbf{E}[N_i] = 1)$.

Figure 2 shows the resiliency of the military network versus the number of interconnections for the ER-ER-ER, BA-BA-BA and ER-TC-BA network. Here the resiliency decreases as we increase the number of interconnections. This is because with more interconnections the risk easily propagates to the military system from commercial networks. Observe that the DL connection performs better than the AL connection, which is due to the fact that the military nodes with smaller degrees are connected to commercial nodes. Hence, even if an interconnected military node is compromised, due to its smaller degree the probability of compromising many neighbors is low.

Figure 3 shows the efficiency of interconnectivity of the 3-level network for different number of interconnections, which can be computed by (5). Here, as we increase the number of interconnections the efficiency of interconnectivity becomes high which is due to the new communication paths between subnetworks. Moreover, with AL connection the efficiency of interconnectivity of the 3-level network is higher than that for the DL connection, which is due to the higher node-degrees of the interconnected nodes.

The vulnerability versus the efficiency of interconnectivity for three multilevel networks is shown in Fig. 4. The vulnerability of the military network increases with the efficiency of the network. Moreover, for any given efficiency the higher the value of τ, the vulnerability becomes higher due to the larger propagation probability of risks from the compromised nodes.

Finally, Fig. 5 shows the results using the evil-rain model for the ER-ER-ER network due to space limitations. As described in the model, here commercial networks have the "source of failures" with a given probability (0.20 in the simulation); thus failures start from the commercial system and propagate to the military network. However, the military network has the "source of repairs" with a probability (0.20 in the simulation), which prevents the failure of the network entirely. We can observe the similar trend as in the SIR model. Thus we conclude that the interconnection increases the vulnerability of the secure military system. At the same time, the efficiency of interconnectivity among subnetworks also increases.

D. Parametric Model for the Resiliency and Efficiency

Motivated by the observed trends in the simulation data, we propose two parametric models for the efficiency of interconnectivity and resiliency for any given number of interconnection. From Fig. 2, observe that the resiliency is approximately linear with respect to the number of interconnections. We propose the following parametric expression for the resiliency $(R(\tau, G))$ with l number of interconnections,

$$R(\tau, G) = \alpha(\tau, G) + lb(\tau, G), \quad (8)$$

where $a(\tau, G), b(\tau, G)$ are two parameters estimated from simulation data, G represents the network graph, and τ is the transmission probability. We obtained the following values of the optimally fitted parameters $a = 0.997, b = -0.007$ (ER - ER - ER network); $a = 0.998, b = -0.017$ (BA - BA - BA network); $a = 1.001, b = -0.005$ (ER- TC-BA network); which were then used to generate the fitted lines in the Fig. 6(a).

Interestingly, as shown in Fig. 3, the efficiency of interconnectivity follows a nonlinear relationship with the number of interconnection (l), which we approximate as the following,

$$\hat{W}(\tau, G) = \alpha(\tau, G) l^{\beta(\tau, G)} + \gamma(\tau, G). \quad (9)$$

Here the values of optimally fitted parameters: $\alpha = 0.0828, \beta = 0.2984, \gamma = -4 \times 10^{-4}$ (ER-ER-ER network); $\alpha = 0.0959, \beta = 0.2678, \gamma = -3.2 \times 10^{-3}$ (BA-BA-BA network); $\alpha = 0.0854, \beta = 0.2678, \gamma = -4.7 \times 10^{-5}$ (ER - TC- BA network); which were then used to find the fitted lines in the Fig. 6(b).

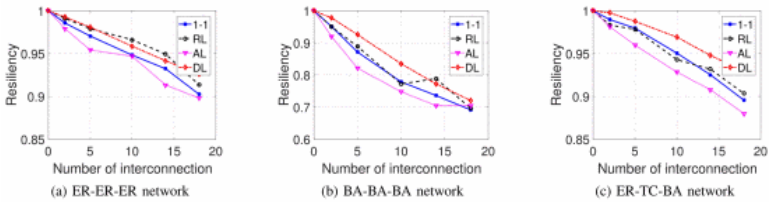


Fig. 2. Resiliency of the military network versus the number of interconnection for the ER-ER-er, BA-BA-ba, and ER-TC-ba networks with $\tau = 0.3$

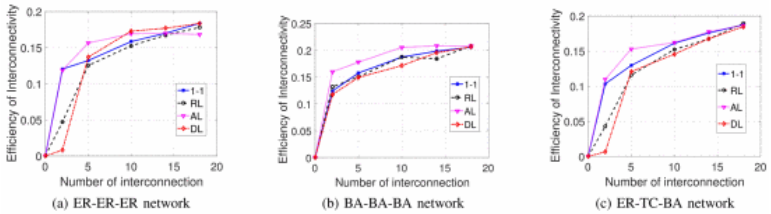


Fig. 3. The efficiency of interconnectivity versus the number of interconnection for the ER-ER-er, BA-BA-ba, and ER-TC-ba networks with $\tau = 0.3$

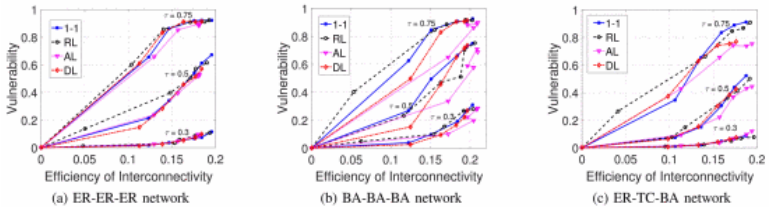


Fig. 4. The vulnerability of the military network versus the efficiency of interconnectivity for the ER-ER-er, BA-BA-ba, and ER-TC-ba networks

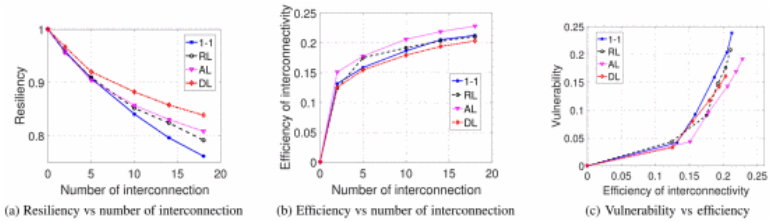
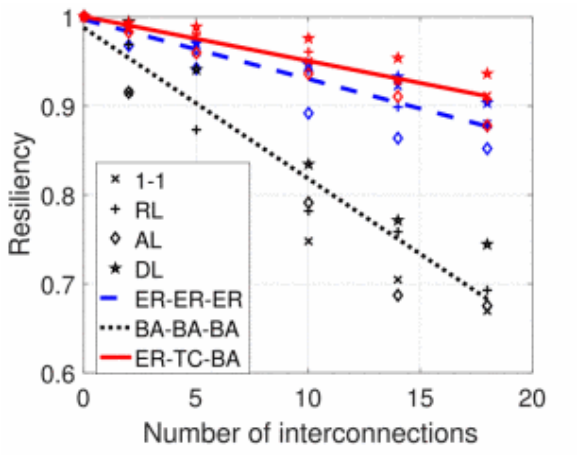
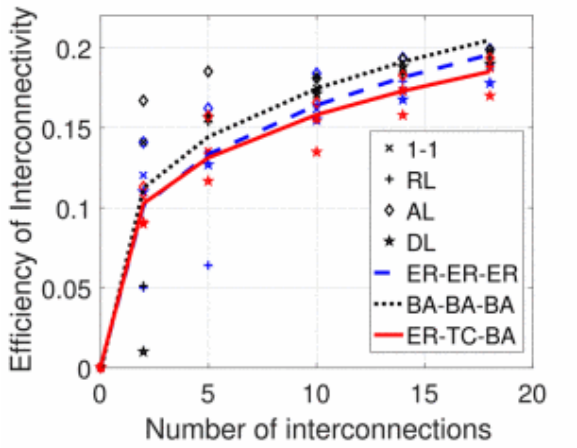


Fig. 5. Simulation results using the evil-rain influence model for the ER-ER-er network

The values of parameters in (8) and (9) are computed by fitting the simulation data so as to minimize the overall mean-square-error (MSE). Higher-order polynomials may yield more accurate fitting of the data with added complexities and also with a risk of over-fitting the data points [22]. Here we tradeoff the complexity with slight inaccuracy to keep the model simple and to avoid possible over-fitting error. We derive the parametric model for the SIR model due to space constraints. However, the model parameters may also be tuned for the evil-rain model as both models show qualitatively similar trends.



(a) Resiliency vs the number of interconnection



(b) Efficiency vs the number of interconnection

Fig. 6. Parametric fitting of the resiliency and efficiency of interconnectivity for different multilevel networks with four interconnection patterns. Here $\tau = 0.3$.

Note that, the parametric models have great importance in deriving key insights. For instance, based on the given constraints (resiliency or vulnerability), one can obtain the number of interconnections by (8) and corresponding efficiency of interconnectivity by (9), that solves both optimization problems. One can also compute the efficiency of the multilevel network and resiliency of a secure network provided the number of interconnections. Moreover, the solution is independent of interconnection patterns (AL, DL, RL, 1–1) assuming the MSE tolerance.

SECTION VI.Conclusion and Future Works

This paper has analyzed the dynamics of risk propagation in multilevel networks using the SIR epidemic model and evil-rain influence model. The assumptions used in the two models may represent all real-world risk propagation simplistically but enable an exact mathematical analysis of the dynamics of risk propagation in a multilevel network. We have proposed two parametric models to maximize the efficiency of interconnection under security (resiliency/vulnerability) constraints. These models can be used to find the number of interconnections for exchanging information within the multilevel network when some subnetworks are vulnerable to security attacks.

The analysis of the optimality of the proposed optimization problems and the trade-off between accuracy and complexity of the parametric model are left as future works. Besides, validating the parametric model with data from the real-world network is also a part of our future study. The generalization of this work for modeling the non-homogeneous propagation of security risks (i.e., τ and c may vary based on the types of security risks and links) would better capture the real-world threat propagation in the multilevel network.

ACKNOWLEDGMENT

This work was supported by the Defense Threat Reduction Agency's Basic Research Program under grant No. HDTRAl-13-1-0020 and NSFs grant No. 2GA11 NSF CRISP.

References

1. *Jie: How dod is building a bigger network that's also a smaller target*, [online] Available: https://defensesystems.com/Articles/2015/02/23/Joint-Information-Environment-JRSS-security.aspx?Page=l.

2. P. Das et al., "On the vulnerability of multi-level communication network under catastrophic attacks", *ICNC IEEE*, pp. 912-916, 2017.

3. T. H. Shake, "Security in military/commercial communication gateways", *Proceedings of MILCOM IEEE*, vol. 1, pp. 469-474, 1999.

4. S. Bistarelli et al., "Detecting and eliminating the cascade vulnerability problem from multilevel security networks using soft constraints", *AAAI*, pp. 808-813, 2004.

5. J. F. Kurose, K. W. Ross, Computer networking: A top-down approach, Addison-Wesley Reading, 2010.

6. V. Paruchuri et al., "Secure communications over hybrid military networks", *Proceedings of MILCOM IEEE*, pp. 1-7, 2008.

7. C. Asavathiratham, *The influence model:a tractable representation for the dynamics of networked markov chains*, 2000.

8. M. Newman, Networks: An introduction, Oxford university press, 2010.

9. M. S. Vassiliou et al., "Crucial differences between commercial and military communications technology needs: Why the military still needs its own research", *Proceedings of MILCOM IEEE*, pp. 342-347, 2013.

10. R. Di Pietro, G. Me, "Military secure communications over public cellular network infrastructure", *Proceedings of MILCOM IEEE*, vol. 1, pp. 400-405, 2002.

11. W. H. Murray, "The application of epidemiology to computer viruses", *Computers & Security*, vol. 7, no. 2, pp. 139-145, 1988.

12. J. O. Kephart, S. R. White, "Directed-graph epidemiological models of computer viruses", *Computation: The micro and the macro view World Scientific*, pp. 71-102, 1992.

13. A. Gutfraind, "Optimizing network topology for cascade resilience" in Handbook of optimization in complex net, Springer, pp. 37-59, 2012.

14. S. M. Rinaldi et al., "Identifying understanding and analyzing critical infrastructure interdependencies", *IEEE Control Systems*, vol. 21, no. 6, pp. 11-25, 2001.

15. M. Amin, "Toward secure and resilient interdependent infrastructures", *Journal of Infrastructure Systems*, vol. 8, no. 3, pp. 67-75, 2002.

16. S. V. Buldyrev et al., "Catastrophic cascade of failures in interdependent networks", *Nature*, vol. 464, no. 7291, pp. 1025-1028, 2010.

17. M. Rahnamay-Naeini, "Designing cascade-resilient interdependent networks by optimum allocation of interdependencies", *Int. conference on computing networking and comm.(ICNC) IEEE*, pp. 1-7, 2016.

18. H. Okamura, T. Dohi, "Estimating computer virus propagation based on markovian arrival processes", *IEEE 16th Pacific Rim Int. Symposium on Dependable Computing IEEE*, pp. 199-206, 2010.

19. V. Latora, M. Marchiori, "Efficient behavior of small-world networks", *Physical review letters*, vol. 87, no. 19, pp. 198, 2001.

20. J. P. Sterbenz et al., *The Univ. of Kansas*, 2010, [online] Available: http://www.ittc.ku.edu/resilinets/maps/.

21. K.-I. Goh et al., "Universal behavior of load distribution in scale-free networks", *Physical Review Letters*, vol. 87, no. 27, pp. 278, 2001.
22. D. A. Pados, P. Papantoni-Kazakos, "A note on the estimation of the generalization error and the prevention of overfitting", *1994 Int. conf. on neural networks IEEE*, vol. 1, pp. 321-326, 1994.