TOWER: Topology Optimization for netWork Enhanced Resilience

Enrique de la Hoz[1], Jose Manuel Gimenez-Guzman[1], German Lopez-Civera[1], Ivan Marsa-Maestre[1] and David Orden[2]

[1]*Computer Engineering Department, University of Alcala, Alcala de Henares, Madrid, Spain*

[2]*Physics and Mathematics Department, University of Alcala, Alcala de Henares, Madrid, Spain*

Keywords: Network Resilience, Critical Infrastructures, Graph Modelling, Network Reshaping.

Abstract: Nowadays society is more and more dependent on critical infrastructures. Critical network infrastructures (CNI) are communication networks whose disruption can create a severe impact on other systems including critical infrastructures. In this work, we propose TOWER, a framework for the provision of adequate strategies to optimize service provision and system resilience in CNIs. The goal of TOWER is being able to compute new network topologies for CNIs under the event of malicious attacks. For doing this, TOWER takes into account a risk analysis of the CNI, the results from a cyber-physical IDS and a multilayer model of the network, for taking into account all the existing dependences. TOWER analyses the network structure in order to determine the best strategy for obtaining a network topology, taking into account the existing dependences and the potential conflicting interests when not all requirements can be met. Finally, we present some lines for further development of TOWER.

1 INTRODUCTION

Since mid-90s, multiple events caused by natural disasters or by humans have brought to the fore the high level of dependency that our society has on what are known as critical infrastructures. If one of these infrastructures is compromised, it will have a serious impact in our life and disrupt the normal society order as a whole. Therefore, the protection of critical infrastructures is a top priority in the agendas of our governments and critical service operators.

Critical infrastructures are characterized by a high level of interconnection. Many physical, logical or virtual dependencies are not revealed until a crisis arises. This high level of interdependencies may lead to cascading failures. At the same time, small disruptions can be enough to unleash dramatic consequences in high complexity systems.

Critical network infrastructures (CNI) are one subset of this kind of systems. By CNI, we mean those communication network infrastructures whose disruption, intentional or accidental, has a high impact because of either its massive, even global, deployment (e.g., Internet, cell provider networks) or its supporting role for other critical infrastructures (e.g., the network for the internal communications of a control system in a nuclear facility, or the communication network for the electrical grid).

When addressing the challenge of offering robustness to CNI, the concept of network resilience emerges. We can define network resilience (Smith, 2011) as the ability of a network to defend itself and keep an acceptable service level in the presence of challenges such as malicious attacks, hardware failures, human mistakes (hardware or software misconfigurations) and large-scale natural disasters that may threat its normal operation.

In this work, we propose TOWER, a framework for the provision of adequate strategies to optimize service provision and system resilience in CNIs. For achieving this goal, TOWER will use as inputs a risk analysis and alert reports coming from different sources and will produce a proposal of a new network topology. This network topology should be able to tackle the malicious attack by isolating it and minimizing its impact in the whole network as the consequence of the potential cascading failure induced as a result of the attack. The new topology will be oriented to offer a robust answer to the threats that may impact the services at CNI or the network itself. Therefore, it has to take into account multiple and heterogeneous input data. We have identified three main sources: threat analysis, a

Hoz, E., Gimenez-Guzman, J., Lopez-Civera, G., Marsa-Maestre, I. and Orden, D.
TOWER: Topology Optimization for netWork Enhanced Resilience.
DOI: 10.5220/0006017101210128
In *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications (ICETE 2016) - Volume 1: DCNET*, pages 121-128
ISBN: 978-989-758-196-0

multi-layer model of the network and the results from a cyber-physical intrusion detection system. It is important to note that, although malicious attacks are not the only challenge to cope with in CNIs, this type of attacks use to be the most harmful ones as they are focused on the blockage of the network-provided network services. In fact, there are studies (Albert, 2000) that claim that network resilience obeys to different structural network properties in case of malicious attacks, human errors or natural disasters, due to the fact that these two last ones have a more random and distributed nature, while the first ones (malicious attacks) are usually focused on specific nodes that play an essential role in the network.

The rest of the paper is organized as follows. Section 2 presents a review of the state of the art. Section 3 introduces multilayer networks. In Section 4, the main components and challenges of TOWER are described. Section 5 discusses network resilience for CNI. Section 6 presents the main concepts on network topology adaptation that area applied in TOWER. Finally, some conclusions and future work are presented.

2 RELATED WORK

In the last decade, there has been a growing interest on maximizing the resilience of CNIs. Regarding the Internet, its vulnerability has been widely acknowledged (DHS, 2009) (Lin, 2007), and it has been shown in different global scale incidents, both accidental (Zmijewski, 2009) and as a result of malicious activities (Goldberg, 2014). Also, the role of communication networks in critical infrastructures has been studied, as there are interdependences between both (Rinaldi, 2001) (DHS, 2009). Electrical grids are one of the clearest examples of this. On the one hand, the communication networks rely on the power provided by the electrical grid to work. On the other hand, and increasingly, the electrical grid relies on the communication networks for its proper performance, as it is based on SCADA systems for its management.

There are some works in different areas that can be related to the study of resilience in complex networks. First, mobile ad-hoc networks and vehicular ad-hoc networks (MANET and VANET). In these networks, nodes are constantly moving, and, accordingly, the connectivity must evolve to deal with this. For these scenarios, it is critical to guarantee service continuity under this dynamicity (Landmark, 2015) (Su, 2015) (Dietzel, 2016). Second, delay tolerant networks (Fan, 2015), where service interruption after power failures, attacks or node dispersion are taken into account, has attracted much interest and its study has been promoted by DARPA. And last, wireless sensor networks, where it is necessary to create resilient network topologies able to provide connectivity even after some sensors stop contributing as a result of a battery outage (Younis, 2014) (Yao, 2015).

With this background, there are some works that face resilience in critical infrastructures by modelling them as complex networks. The closest works to our proposal are (Shao, 2015) and (Berezin, 2015). These works study the robustness of complex networks under attacks targeted to the most sensitive points of the network and are more theoretical than the ones that we propose. While they deal with generic complex networks, we want to include more realistic network models. Also, we propose to use a multi-layer network model, to capture the features of real-world networks. Finally, we employ optimization techniques based on negotiation to keep network resilience in a distributed and self-organized way.

As research on complex networks has evolved, it has been clearer the need of going further than monolayer graph modelling and exploring more realistic and complex models. Multiplex or multi-relational networks connect nodes using links that can express different kinds of relationships (Yagan, 2012). Multilevel networks and meta-networks enable also hierarchical structures and node and links of different types (Carley, 2007). Recently, (Kivelä, 2014) has presented a unified modelling for multi-layer networks that include these concepts in a unified manner that takes advantage of the different mathematical tools available in the state of the art.

In the last years, there have been significant advances on complex system optimization in domains that could be modelled as CNIs. Techniques potentially suited for these domains include auctions, optimization techniques, and negotiation protocols. Combinatorial auctions (Xia, 2005) (Sandholm, 2015) can enable large-scale collective decision-making in nonlinear domains, but only of limited type (i.e. negotiations consisting solely of resource/item allocation decisions). Multi-attribute auctions (Pham, 2015) are also aimed at a fundamentally limited problem –purchase negotiations– and require full revelation of preference information. Constraint-based and other optimization tools (Chechetka, 2006) (Davin, 2005) offer good solutions with interdependent issues, but

have not been applied to contexts with self-interested parties, thereby ignoring strategic issues derived from participant's selfish behaviour. In particular, the vast majority of these approaches assume that agreements will be honoured (e.g. after an auction, the winner will pay the agreed amount to the auctioneer). In many CNIs domains, however, this "agreement honouring" assumption cannot be made (e.g. you can suggest network reshapes to different network domains, but you cannot force them to accept them).

The distributed and adaptive nature of CNIs, along with the need to reach a consensus between conflictive individual goals to benefit a social goal, suggests the use of negotiation techniques. However, most negotiation research has focused on problems with one issue (typically price) or a few independent issues (Ren, 2013) and are demonstrably sub-optimal for negotiations with multiple interdependent issues (Klein, 2003). A number of research efforts (Marsa-Maestre, 2009) (Li, 2009) have attempted to address this challenge, facing serious limitations in terms of outcome optimality, strategic stability and scalability. These three performance indicators are key enablers for the success of optimization systems in large real-world CNIs infrastructures, due to their continuous increase in network size, structural complexity and dynamicity (Strogatz, 2001). If we want to keep relying on these exponentially growing infrastructures for our development as a society, new distributed optimization mechanisms should be devised for their management.

3 MULTILAYER NETWORKS

To achieve our purpose, and in order to take effectively into account the underlying complexity of CNI, the first step consists in modeling them by means of multilayer graphs. Graphs have shown to be a useful tool to model complex systems, as vertex or nodes can be employed to represent the functional elements of the system, while edges show the relationships between them. However, CNIs are usually complex networks that include intricate relations between their elements, so a simple graph can hardly capture these relations. For that reason, we use multilayer graphs to account for those relations in a more intuitive and powerful manner. As described in (Boccaletti, 2006) (Kivelä, 2014), multilayer networks incorporate multiple levels of connectivity and provide a natural framework to describe systems connected through different types of connections: each channel (relationship, activity or category) is represented by a layer and the same node or entity may have different kinds of interactions (different set of neighbors in each layer).

As shown in Fig. 1, and for example, a multilayer graph can be composed by different layers that express the physical location of the systems, the communication paths existing between them and also the functional and management dependencies. Apart from the more technical aspects, characteristics like the social or corporate dependencies present at any kind of critical infrastructure could be also easily modeled by means of new layers with their respective inter- and intra-layer dependencies.

4 TOPOLOGY OPTIMIZATION FOR NETWORK ENHANCED RESILIENCE (TOWER)

The main objective of TOWER is to provide adequate strategies to optimize service provision and system resilience by taking as input the risk analysis and alert reports and proposing a new network topology. This topology will be oriented to offer a robust answer to the threats that may impact the services at the critical infrastructure or the network that supports them. Therefore, it has to take into account multiple and heterogeneous input data that can be summarized into three main blocks:

1. Threat analysis: Before the TOWER module can be deployed a threat analysis and a contingency plan must be developed. These processes aim to create an initial status report for the system that provides enough information to TOWER to start working. This analysis must include a detailed analysis of the value, implicit risk and attack resilience of all the assets that must be protected.
2. A multilayer network model: As described in section 3, a multilayer network model is needed to represent the complex system underlying to the CNI. This transformation will enable to express hidden dependencies between assets that would not be covered otherwise. At the same time, this kind of model provides a wider perspective over the consequences of an attack as it can show how the malicious behavior or its consequences would spread throughout the network (e.g. a cascading failure). This data representation could be useful for an intrusion prevention system to take better decisions about

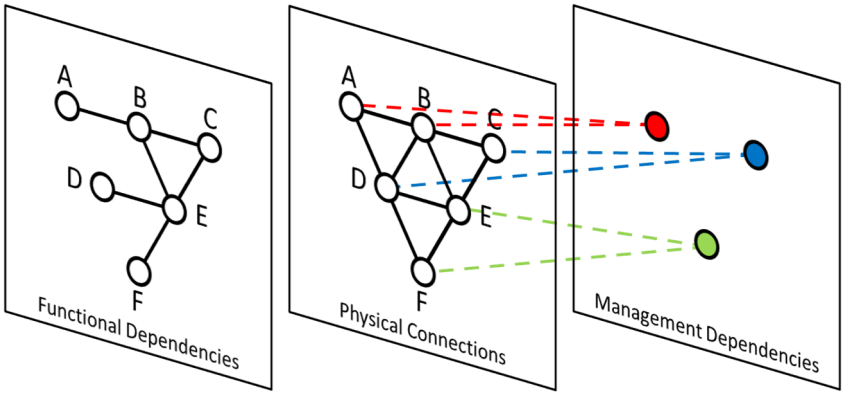

Figure 1: Example of three-layer graph.

how to isolate and protect the CNI in the event of an attack. All this process will be performed offline, that is, before the system is fully deployed. The model can be updated lately if new assets are introduced in the network but a first model must be created before the online process begins.

3. IDS alerts: These alerts contain information about the type of attack, its location and the assets involved. Based on this data, TOWER will be able to evaluate the overall status of the network and respond accordingly. Therefore, a consistent and meaningful communication channel must be developed to link the cyber-physical IDS and the recovery module.

After analyzing all this data, TOWER will compute a network topology intended to isolate the attack and minimize its impact. This topology will consider the required paths that must be always linked and make use of backup links or modified routing paths to create new ways to reach each point of the network. TOWER will offer a ranked list of different topologies, ordered by a score metric. This ranked list will provide different options for the rest of the recovery module. Therefore, if a particular topology cannot be deployed in the network, other options that will also reduce the impact of an attack should be available.

The purpose of the topology computation engine inside TOWER is to prevent not only the direct consequences of a loss of connectivity or a system failure (produced by an attacker or not), but also to avoid the cascading effects that it may produce. Consequently, TOWER will analyze the interdependencies that may emerge from the network elements and the risk analysis performed over them. All this information has to be translated into graph elements and this is when multilayer network modelling becomes useful for modelling all this complexity into multiple graphs for the representation of the existing different kinds of dependencies between network nodes. This relationship between the multiple layers of the network model provides an easier way to create a data structure for TOWER to find hidden consequences that cannot be directly traced to a failure in a network node.

The kind of network topology that TOWER will compute will be highly dependent on the type of attack detected. Different kinds of attacks will imply a particular type of topology modification, not only due to its location but also because of its inner characteristics. This implies that TOWER must take into account how the threat could spread through the network. For example, if the infrastructure is suffering a DDoS attack, TOWER may modify the network by cutting the paths under attack and reroute traffic through other alternative paths. On the other side, if a server gets compromised, TOWER will isolate the node and limit the communications made by all the computers that could have been reached from that server. Therefore, pivoting attacks that employ accessible servers to reach the internal network, that could not be attacked otherwise, are also covered by the TOWER approach.

One of the main challenges TOWER will face is the situation where updating the topology will protect part of the network but may introduce new threats or attack surface. Unfortunately, this is the most common case as computer networks tend to be highly coupled with some central nodes that manage a large amount of traffic. The existence of these nodes may create central points of failure which can originate a cascading effect if they are compromised. The purpose of the initial network topology deployment and all modifications made to it through TOWER is to minimize these interdependencies and maintain the network in a resilient state.

To achieve this purpose, different approaches are being studied, but the main efforts are focused on employing graph theory techniques to analyze the status of the network and compute how to react against an attack or a system malfunction. Apart from this data representation, the progress made in TOWER module is focused on finding relevant graph metrics that helps to characterize the network they model. These metrics are different than the characteristics modelled through the use of multiple layer networks. The layers are employed to show the dependencies present in the network at different levels, while these metrics describe the behavior of the dependencies. For example, if a layer of the network model is composed by the existing communications flows between the nodes, a metric, e.g. node degree, can help identifying the nodes that are the origin or destination of the majority of the traffic. One of the long-term purposes of our work is to study how the network structural properties of a problem influence the performance of optimization and the choice of the negotiation approaches best suited to it. To this end, we have selected a number of graph metrics from the literature, being the following:

1. **Graph order:** the number of nodes in the graph.
2. **Graph diameter:** the longest distance (number of traversed edges) between any pair of nodes in the graph (Newman, 2010).
3. **Wiener index:** gives a measure of graph complexity from the distances in the graph. It is computed as,

$$W(G) = \frac{1}{2}\sum_{i=0}^{|N|}\sum_{j=0}^{|N|} d(n_i, n_j)$$

   where $|N|$ are the number of vertices of the graph and $d(n_i, n_j)$ is the shortest distance between nodes (Wiener, 1947).
4. **Graph density:** the ratio between the number of edges in the graph and the maximum possible number of edges (that is, for a fully-connected graph).
5. **Clustering coefficient:** a measure of the degree to which nodes in a graph tend to cluster together. The cluster coefficient of a graph is computed as the average of the local clustering coefficient of its nodes, which is the ratio between the number of links between a node's neighbors and the maximum possible number of links between them (that is, if they were fully connected).

Another relevant type of metric are the centrality metrics. These metrics allow to identify the most important nodes inside a network, which can be critical to know the most vulnerable points at each ground station. There are a number of centrality metrics in the literature, such as degree centrality (Freeman, 1979), hub and authority centrality (Chakrabarti, 1999), PageRank centrality (Brin, 1998), Katz centrality (Katz, 1953) or betweenness centrality (Freeman, 1979) (Koschützki, 2005). In particular, betweenness centrality of a node is the ratio of shortest paths in the graph that traverse the node.

In particular, due to the need for TOWER to respond in a timely fashion to incidents, we are testing efficient methods to approximate these metrics, such as the ones in (Chierichetti, 2015) (Ohara, 2014) (Kimura, 2016).

We are studying the relevance of these and other metrics on the resilience of different kinds of networks, and we expect to be able to derive novel metrics and methods to detect the cascading effects of an attack and be able to react proactively to network intrusions. This way the system will not only react when an attack is made but also it will prevent the actual attacks strengthening the security measures or creating new backup paths if needed.

Finally, another set of techniques that allow to split a graph into multiple pieces are being studied during the design of TOWER module. These techniques allow to distribute the computational cost of running complex algorithms against big scale graphs. Clustering algorithms may be employed to detect sets of vertex that are more tied and therefore, should not be split when dividing the network. Particular cautions are needed here, since this kind of division may hide dependencies that could be relevant when deciding how to protect the network. Consequently, distributed computation algorithms will be evaluated against different use cases to explore how they impact the computation of new topologies compared to centralized algorithms.

5 NETWORK RESILIENCE

One of the main objectives of TOWER is being able to improve network resilience for CNI. For this to succeed, we need a way to identify and measure resilience in a network. In this section we will point out the most important points that should be taken into account.

To characterize a resilient network three levels of functional dependencies can be identified:

1. **System properties:** these entities represent the functions of the system that have to be protected and must be working permanently.

2. **System attributes:** they show the characteristics that tells us if a system property is robust enough to resist an attack. Some examples are the following:
    1. *Diversity:* It tells how much different kinds of elements are used in the network. The more diverse the system is, the more complex is to attack it as the adversary has to find vulnerabilities on multiple kind of systems. This attribute has to reach a point where the redundancy of the system is not compromised since redundant systems tend to be built using the same infrastructure employed for the replicated element.
    2. *Fault tolerance:* Is the system able to guarantee correct operation if the presence of a failure? This attribute is applied to distributed system where if a node fails, the remaining nodes must be able to continue working.
    3. *Deceptiveness:* It measures how much information can be manipulated about the infrastructure to fool the attacker.
    4. *Velocity/Fluidity:* this concept expresses the level of uncertainty offered to an attacker when he tries to attack the infrastructure. For example, the IP address of a system can change over time or there can be different ways to obtain the same information from different locations, making it harder to identify patterns or security measures.
    5. *Self-stability:* No matter how the system is compromised, the reaction performed has to lead to a stable state where the normal operation of the infrastructure is guaranteed.
3. **Metrics:** All the attributes described above cannot be measured directly (i.e. it does not exist a fault tolerance indicator on our systems). Therefore, specific observations must be performed on the infrastructure to determine the level of fulfillment of all these attributes. For example, to measure the diversity of the network, we may need a system inventory where the number of different operating systems and versions are described.

The metrics have to be carefully chosen as they generate the vision the system will have of the actual status of the network. They can also be modeled as part of the graph representation, showing the dependencies that exist between different attributes and metrics and the function they cover in the infrastructure.

6 ADAPTATION OF NETWORK TOPOLOGY

Up to this point, we have presented the main underlying concepts and technologies to TOWER for identifying and modelling the dependencies of a CNI. Using this information, and taking into account the threat model, TOWER will produce a proposal of new network topologies. These network topologies will be oriented to offer a robust answer to the threats that may impact the services at CNI or the network itself. In practice, this means that TOWER should be able to lead the CNI from a potentially harmful state, e.g. the preliminary steps of an attack or early signs of a system being compromised, to a new good state, ensuring or minimizing the impact for the whole network. It is when evaluating this impact, that the previous models reveal its importance: we ensure that no important dependence is missing. It can also be the case that it is not possible to ensure the safe operation of the whole network. For agreeing on the best outcomes for all the interesting parties, negotiation techniques, such as the one pointed out in section 2, can be used.

We also need to know how to reach a specific state. To do so, we need to model the viable transitions that exist between states, describing which methods or procedures have to be employed to get to that state. These transitions can also be modeled as a graph where the nodes represent the states the system can be and the edges show how to go from one state to another. To decide which path to follow inside this transition graph a decision system has to be developed. This system has to come up with the decision of which the best way is for protecting the network and the actions that have to be taken to reach a stable state that can guarantee the normal operation of the system.

To do so, first we need to perform an exhaustive enumeration of the states the system could be at. Since the computational cost of this enumeration process can exceed the time requirements of the platform, clustering techniques may be applied during offline pre-computation to reduce the number of nodes in the graph. Apart from the normal or working states of the system, we need also to model the states where the system is compromised. Therefore, we need to create also “bad” states that account for an attacker getting inside the network, with different degrees of success. These states must be based on the risk analysis used as input to the TOWER module. Using these compromised states, the system would be able to predict a malicious

behavior based on the preliminary states that can lead to the actual attack. For example, typically reconnaissance techniques are performed before launching an attack, thus if a port scan alert is received it can be mapped to a prior-attack state that can trigger preemptive security measures. Moreover, post-attack states will be also included in the enumeration as they can show how an attack could have cascading effects on multiple elements of the network. This analysis will help to choose the appropriate reaction method and also to determine the coverage of the response action.

Once these states are modeled, the next step consists on determining the current status of the system. In order to do so, a method that maps the information collected from the alerts to one of the states generated before has to be developed. To achieve this purpose, clustering techniques can also be employed, as they can compute the nearest or more similar state.

Once we know the condition of the system, we have translated it to an actual state node in our graph and we know the transitions we can employ to travel the graph from that node; we are ready to continue.

The final step is to compute the path we have to follow to a better state. Distributed agent-based decision systems are being studied to solve this problem. This kind of systems allow to get a response even in the case where a particular action may only benefit part of the infrastructure. This way the overall operation of the infrastructure is guaranteed even if part of it has to be partially harmed during the transition.

Game theory (Myerson, 2013) techniques are also being applied to model the behavior of an adversarial attack and predict how he can breach into the system, taking additional security measures at weak points. Therefore, we can also model the steps an attacker can take to compromise the systems and identify if the infrastructure actual state is leading to one of them, preventing further consequences. These techniques help also to reduce the amount of information that an attacker can obtain from the system, as this information is the input for the algorithm.

7 CONCLUSIONS

This paper presents TOWER (Topology Optimization for netWork Enhanced Resilience), a decision support system intended to provide topology alternatives in Critical Network Infrastructures (CNI), so that the impact of an attack on data communication is mitigated. The system operates from a multilayer network model of the asset inventory of the CNI, which specifies the dependencies between nodes and the associated risks, and is able to react to network incidents (modeled as perturbations in the network) by providing a ranked set of alternative topologies maximizing network resiliency. We discuss the most important design principles behind TOWER and finally, point out some research lines and ideas that will guide future TOWER development.

ACKNOWLEDGEMENTS

This work was partially supported by SCOUT, a research project supported by the European Commission under its 7th Framework Program (contract-no. 607019). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the SCOUT project or the European Commission.

REFERENCES

Albert, R. Error and attack tolerance of complex networks. *Nature*, *406*(6794), 378-382.

Berezin, Y. “Localized attacks on spatially embedded networks with dependencies,” *Scientific reports 5*.

Boccaletti, S., Latora, V., Moreno, Y., Chavez, M. and Hwang, D. U. Complex networks: Structure and dynamics. *Physics reports, 424(4),* 175-308. (2006).

Brin, S. and Page, L.: The anatomy of a large-scale hypertextual web search engine. *Computer Networks and ISDN Systems 30*, 107–117 (1998).

Carley, K.M. "Toward an interoperable dynamic network analysis toolkit." *Decis. Support Syst., 43*, 1324–1347. (2007).

Chakrabarti, S., Dom, B., Kumar, R., Raghavan, P., Rajagopalan, S., Tomkins, A., Gibson, and D., Kleinberg, J.: Mining the web’s link structure. *IEEE Computer 32*, 60–67 (1999).

Chechetka, A. and K. Sycara, No-commitment branch and bound search for distributed constraint optimization. *AAMAS International Conference. Hakodate*, Japan. (2006).

Chierichetti, F., Epasto, A., Kumar, R., Lattanzi, and S., Mirrokni, V.: Efficient algorithms for public-private social networks. In: *Proceedings of the 21st ACMSIGKDD International Conference on Knowledge Discovery and Data Mining (KDD’15)*. pp. 139–148 (2015).

Davin, J. and Modi, P.J. Impact of problem centralization in distributed constraint optimization algorithms. *AAMAS International Conference. (2005)*.

DHS, A Roadmap for Cybersecurity Research, Technical Report, *Department of Homeland Security (DHS). (2009)*.

Davin, K. Impact of problem centralization in distributed constraint optimization algorithms. In Proceedings of *The 4th International Conference on Autonomous Agents and Multiagent Systems AAMAS. (2005)*.

Dietzel, S. A resilient in-network aggregation mechanism for VANETs based on dissemination redundancy, *Ad Hoc Networks 37*, 101-109. (2016).

Fan, R. RobustGeo: A Disruption-Tolerant Geo-Routing Protocol, *24th International Conference on Computer Communication and Networks (ICCCN). (2015)*.

Freeman, L.: Centrality in social networks: Conceptual clarification. *Social Networks 1*, 215–239 (1979).

Goldberg, S. Why is it taking so long to secure internet routing? *Communications of the ACM*, *57*(10), 56-63. (2014).

Katz, L. A New Status Index Derived from Sociometric Index. *Psychometrika*, 39-43. (1953).

Kimura, M., Saito, K., Ohara, K., and Motoda, H.: Speeding-up node influence computation for huge social networks. *International Journal of Data Science and Analytics 1*, 1–14 (2016).

Kivelä, M. Multilayer networks, *Journal of Complex Networks*, 2(3), 203-271. (2014).

Klein, M., P. Faratin, H. Sayama and Y. Bar-Yam. Negotiating Complex Contracts. *Group Decision and Negotiation 12(2)*, 111 - 125. (2003).

Koschützki, D., Lehmann, K.A, Peeters, L., Richter, S. Tenfelde-Podehl, D. and Zlotowski, O.. Centrality indices. Network analysis. *Lecture Notes in Computer Science*. 3418:16–61, (2005).

Landmark, L. Resilient internetwork routing over heterogeneous mobile military networks, *IEEE Military Communications Conference (MILCOM)*, 388-394. (2015).

Li, M., Q. B. Vo and R. Kowalczyk Searching for fair joint gains in agent-based negotiation. *Autonomous Agents and Multi-agent Systems (AAMAS-09)*. (2009).

Lin, H. S. and Goodman S. E. Toward a Safer and More Secure Cyberspace, *National Academies Press (2007)*.

Marsa-Maestre, I., Lopez-Carmona, M. A., Velasco, J. R., and de la Hoz, E. Effective bidding and deal identification for negotiations in highly nonlinear scenarios. In *Proceedings of The 8th International Conference on Autonomous Agents and Multiagent Systems 2*, 1057-1064. (2009).

Myerson, Roger B. *Game theory*. Harvard university press, (2013).

Newman, M. Networks: an introduction. *Oxford University Press*, (2010).

Ohara, K., Saito, K., Kimura, and M., Motoda, H.: Resampling-based framework for estimating node centrality of large social network. In: *Proceedings of the 17th International Conference on Discovery Science (DS'14)*. pp. 228–239. LNAI 8777 (2014).

Pham, L., Teich, J., Wallenius, H., and Wallenius, J. Multi-attribute online reverse auctions: Recent research trends. *European Journal of Operational Research, 242(1)*, 1-9. (2015).

Ren, F., and Zhang, M. Bilateral single-issue negotiation model considering nonlinear utility and time constraint. *Decision Support Systems.* 60, 29-38. (2013).

Rinaldi, S.M. Identifying, understanding and analyzing critical infrastructures interdependencies, *IEEE Control Systems Magazine*, 21(6), 11-25. (2001).

Sandholm, T., and Likhodedov, A. Automated design of revenue-maximizing combinatorial auctions. *Operations Research*, 63(5), 1000-1025. (2015).

Shao, S. Percolation of localized attack on complex networks, *New Journal of Physics*, 17, 023049. (2015).

Smith, P. Network resilience: a systematic approach, *IEEE Communications Magazine*, 49(7), 88-97. (2011).

Strogatz, S. H. Exploring complex networks. *Nature*, 410(6825), 268-276. (2001).

Su, M.Y. A resilient routing approach for Mobile Ad Hoc Networks, *International Conference on High Performance Computing & Simulation (HPCS). (2015)*.

Wiener, H. Structural determination of paraffin boiling points. *Journal of the American Chemical Society*, 69(1):17–20, (1947).

Xia, M., Stallaert, J. and A. B. Whinston. Solving the combinatorial double auction problem. European *Journal of Operational Research* 164(1), 239-251. (2005).

Yağan, O. and Gligor, V. Analysis of complex contagions in random multiplex networks. *Physical Review E,* 86(3), 036103. (2012).

Yao,Y. EDAL: An Energy-Efficient, Delay-Aware, and Lifetime-Balancing Data Collection Protocol for Heterogeneous Wireless Sensor Networks, in *IEEE/ACM Transactions on Networking*, 23(3), 810-823. (2015).

Younis, M. Topology management techniques for tolerating node failures in wireless sensor networks: A survey, *Computer Networks*, 58, 254-283. (2014).

Zmijewski, Reckless Driving on the Internet, http://research.dyn.com/2009/02/the-flap-heard-around-the-world/ .(2009).