International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:9, No:12, 2015

System Survivability in Networks in the Context of Defense/Attack Strategies: The Large Scale

A. Ben Yaghlane, M. N. Azaiez, M. Mrad

***Abstract*—**We investigate the large scale of networks in the context of network survivability under attack. We use appropriate techniques to evaluate and the attacker-based- and the defender-based-network survivability. The attacker is unaware of the operated links by the defender. Each attacked link has some pre-specified probability to be disconnected. The defender choice is so that to maximize the chance of successfully sending the flow to the destination node. The attacker however will select the cut-set with the highest chance to be disabled in order to partition the network. Moreover, we extend the problem to the case of selecting the best p paths to operate by the defender and the best k cut-sets to target by the attacker, for arbitrary integers p,k>1. We investigate some variations of the problem and suggest polynomial-time solutions.

***Keywords*—**Defense/attack strategies, large scale, networks, partitioning a network.

I. Introduction

IN this paper, we treat the case of attacks on large networks. We will provide optimal policies both for the attacker and defender of the network in a game-theoretic spirit. Networks are considered as good targets for intelligent threats including terrorism, wars, and rebellions. Many of the oil pipeline networks have been attacked in various places in the world such as Iraq, Saudi Arabia, and Libya in the last few years. Road networks as well as computer systems have been also attacked. Consequently, it is important to develop defense tools to protect our homeland infrastructure. One should not however under-estimate the skills and the destruction capacities of potential attackers. Therefore, defensive strategies should be devised in anticipation of intelligent attacks suggesting the determination of optimal attack strategies.

II. Literature Review

Some important literature in defense/attack strategies has been developed in the last decade. Interested readers may refer to [1] and [2]. Two nice papers on attacks on telecommunication and transportation networks are given respectively in [3] and [4]. Reference [5] discusses least-cost attack strategies on networks and provides a variety of operations research techniques to assess the network least-cost cut sets in a branch and bound fashion.

A. Ben Yaghlane, M. N. Azaiez are with the Université de Tunis, Institut Supérieur de Gestion, Tunis Business School, Tunis, Tunisia (e-mail: asma_benyaghlane@yahoo.fr, naceur.azaiez@tbs.rnu.tn).

M. Mrad is with the King Saud University, Department of Industrial Engineering, College of engineering, Riadh, Saudi Arabia (e-mail: mradmehdiisg@yahoo.fr).

Reference [6] defines network survivability both for the case of perfect information, in which the attacker may observe the operated paths and hence attack those of interest, and absence of information where the attacker would select the links to target independently of the defender strategy of operating the network. In the latter case, they distinguish two types of network survivability; namely the defender-based- and the attacker-based- network survivability. They provide tools for assessing network survivability and compare the defender-based-network survivability against the attacker-based-network survivability as well as against network reliability. All the assessments are made for relatively small networks. For this paper to be self-contained, we will display in Section III the main developments by [6].

In this paper, we extend [6] to the large scale and suggest some interesting generalizations.

III. Background

We will start by discussing the case of perfect information in which both types of network survivability coincide. Then, we will display the main findings for the case of absence of information. We assume that the defender of the network is interested in sending some flow (in sufficient capacity) from a source node to a destination node. The attacker's objective is to prevent the flow from reaching the destination; in which case the attack succeeds. Else, the attack is considered as failing. We assume that the attacker may target any link of the network. Each attacked link has a pre-defined survival probability. A link can be attacked only once. Attacks are made sequentially. The attacker is interested in determining the set of links to target in order to disable the network. The attack resources are limited so that the attacker would only consider a limited number of links in a specific order.

In the case of perfect information, the network survivability is defined to be the highest probability of a breakthrough path to survive an attack.

The case of absence of information is assumed to be the case where the attacker need not know the breakthrough path that has been effectively used by the defender. The attacker would opt for a conservative approach by disabling an entire cut set to make sure that the flow cannot reach its destination no matter what breakthrough path is used. The corresponding network probability to survive is referred to as the attacker-based-network survivability. In contrast, the defender-based-network survivability coincides with the one given in the case of perfect information.

Determining the attacker-based-network survivability suggests solving a min-cut problem (by duality) which can

easily be modeled as a linear program. Reference [6] investigates the relationship between the defender-based- and the attacker-based-network survivability as well as their relationships with network reliability. Let Sp (respectively Sc) be the defender-based-network survivability (attacker-based-network survivability). Also, let R be the network reliability. Then, the following results apply.

Proposition 1. $S_p \leq R \leq S_c$

Proposition 2. Except when the network is reduced to a series system (or a single breakthrough path), the following inequality holds:

$$S_p < R$$

Proposition 3. Except when the network is reduced to a single link joining the source to the destination, the following inequality holds:

$$S_p < S_c$$

IV. Case of Large Scale Networks

When the size of the network becomes reasonably large, one may wonder about the ability to assess the network survivability. We will briefly show that both types of network survivability may be approached using some efficient techniques.

A. Defender-Based-Network-Survivability

In order to assess the defender-based-network survivability of large networks, we can easily show that the problem is equivalent to the shortest-path formulation.

In fact, let $\mathcal{P}$ be the set of all breakthrough paths and consider a breakthrough path $P \in \mathcal{P}$. Let p_{ij} be the survivability of a link (i, j) of P. Then,

$$S_P = \prod_{(i,j)\in P} p_{ij} \quad (1)$$

The problem is to solve:

$$Max_{P\in\mathcal{P}}\, S_P \quad (2)$$

Set $w_{ij} = -Ln(p_{ij})$. Then, optimization problem (2) is equivalent to:

$$Min_{P\in\mathcal{P}} \sum_{(ij)\in P} w_{ij} \quad (3)$$

Clearly, (3) is the shortest-path problem that can efficiently be solved through the corresponding standard techniques such as Dijkstra's algorithm or Floyd's Algorithm.

B. Attacker-Based-Network-Survivability

The problem has to do with identifying the cut-set with the lowest probability to survive. This is clearly a min-cut problem or equivalently (by duality) a flow-max problem. Both equivalent types of problems have been extensively studied in the literature and many polynomial-time algorithms are suggested to efficiently treat them.

V. Extensions

We investigate a number of interesting extensions in which we attempt to derive the network survivability. The extensions involve networks with multiple sources and/or sinks instead of single ones, the case of attacking nodes instead of arcs, and the case where the defender seeks to have all nodes of the network connected instead of sending flow from a source to a sink.

A. Multiple Sources and/or Sinks

If the network consists of a number of sources and/or sinks, then we may add a virtual source and/or sink (as appropriate). The virtual source/sink will be linked to the original sources/sinks with arcs having a survival probability of one. This brings us to a special case among those treated above. Applications may include attacking water pipelines that feed different cities from different dams. Another application could be to attack roads to prevent military troops from reaching battle fields from different barracks.

B. Attacking Nodes Instead of Arcs

In this case, we may virtually split each node into two nodes with a link having a survival probability equals the one corresponding to the node of interest. The remaining original arcs will have survival probabilities equal one. Again, this will be another special case of those treated above. Applications may include attacking boosters instead of oil pipelines in an oil-distribution network.

C. Connecting All Nodes of the Network

If the network operation consists on linking all the nodes of the network rather than sending flow from a source to a destination, then the defender-based-network survivability will be assessed as a minimum-spanning-tree problem for which the solution methodology is well-known and computationally efficient. In the case of perfect information, the attacker should simply attack the same path as to be chosen by the defender (i.e., the one solving the minimum-spanning-tree problem). For the case of absence of information; or say when the defender moves next to the attack and hence may deviate from the "destroyed path", then the attacker would opt for a conservative approach to make sure that the attack would disconnect the network. This corresponds to the concept of the attacker-based-network survivability. In this case, the problem is modified to a one in which the attacker seeks to partition the network into two disconnected sub-networks. This can be seen as the minimum bisection problem which consists on separating the vertices of an undirected graph into two clusters, such that the weight of the edges crossing between clusters is minimized. In the attacker-based-network survivability, we consider that the weight of each edge *{i,j}* is equal to $-ln(1 - p_{ij})$.

The following mathematical formulation models the problem by maximizing the weights of arcs inside the two clusters which is equivalent to minimizing the total weight of arcs linking the two clusters.

Let *G(V,E)* be an undirected graph where *V* is the set of vertices and *E* is the set of edges.

S_1 and S_2 denote respectively the first and the second cluster of the bisection where $S_1 \cup S_2 = V$, $S_1 \cap S_2 = \emptyset$ and $|S_1| \geq 1$. Let $x_j = \begin{cases} 1 \text{ if node } j \in S_1 \\ 0 \text{ otherwise} \end{cases} \forall j \in V$. Also, let

$$y_{ij} = \begin{cases} 1 \text{ if edge } \{i,j\} \text{ is not selected in the bisection} \\ 0 \text{ otherwise} \end{cases} \quad \forall \{i,j\} \in E$$

Then, the problem can be formulated as:

$$Max \sum_{\{i,j\} \in E} -\ln(1 - p_{ij}) y_{ij} \quad (4)$$

Subject to

$$\sum_{j \in V} x_j \geq 1 \quad (5)$$

$$\sum_{j \in V} x_j \leq |V| - 1 \quad (6)$$

$$y_{ij} \leq 1 + x_j - x_i \; \forall \{i,j\} \in E \quad (7)$$

$$y_{ij} \leq 1 + x_i - x_j \forall \{i,j\} \in E \quad (8)$$

$$y_{ij} \in \{0,1\} \; \forall \{i,j\} \in E \quad (9)$$

$$x_j \in \{0,1\} \; \forall j \in V \quad (10)$$

After solving this integer linear program all edges that have ($y_{ij} = 0$) should be attacked.

In order to make an efficient attack, we can require that the minimum number of separated nodes after the attack be larger than or equal to a given threshold value D.

In this case, the same formulation still remains valid by replacing constraints (5) and (6) by:

$$\sum_{j \in V} x_j \geq D \quad (11)$$

$$\sum_{j \in V} x_j \leq |V| - D \quad (12)$$

Example 1. Consider the network displayed in Fig. 1 where each edge is labeled by the probability to survive after an attack.

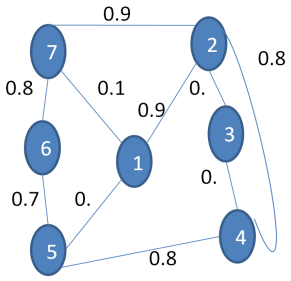

Fig. 1 Network of example 1

In order to separate the network into two disconnected sub-networks, we solve the above integer program.

In case of $D = 1$, the solution is to attack the edges $\{2,3\}$ and $\{3,4\}$ and the probability to succeed the attack is $0.6*0.5 = 0.3$. Therefore, the network will be divided into two clusters $\{3\}$ and $\{1,2,4,5,6,7\}$. If however $D = 2$, the solution is to attack the edges $\{5,4\}$, $\{5,1\}$, and $\{6,7\}$ and the probability to succeed the attack is $0.2*0.2*0.7 = 0.28$. Therefore, the network will be divided into two clusters $\{5,6\}$ and $\{1,2,3,4,7\}$.

When the size of the network gets reasonably large, we should make sure that the solution procedure is efficient. We conduct the following experiment. The survival probabilities upon attack are generated between 0.1 and 0.9 for all the links in the network. The number of nodes n is taken to be equal to 10, 20, 30,…, 500. The degree of each node is randomly generated in the set $\{2,3,4\}$. Finally, m is the number of arcs in each instance.

The proposed Integer Linear Program (5.1)-(5.7) is solved using CPLEX 12.6. All the computational experiments are carried out on an Intel(R) Core(TM) i7 2.00 GHz Personal Computer with 16 GB RAM. The results are displayed in Table I. The following notation is used:

Sol: The optimal solution of each instance that gives the value of the probability to break successfully all the links of the best bisection.

Time: The computational time spent by the solver to find the optimal solution.

D: The minimum number of nodes that should include each cluster.

We have tested the proposed mathematical formulation with three different values of *D*: 1, 5 and $\lfloor n/3 \rfloor$ on each instance.

The empirical results show that the problem becomes harder to solve when the value of *D* increases especially for the large instances. In fact, the mathematical formulation is able to solve to optimality instances with a number of nodes larger than 320 in case of $D = \lfloor n/3 \rfloor$ knowing that the maximum allowable computation time is fixed to 3600 second. On the other hand, the same formulation was able to solve all instances in less than one second in case of $D = 1$ and the largest instance has taken less than 3.5 seconds in case of $D = 5$.

It seems logical that the solution of most of instances is equal to zero in case of $D = \lfloor n/3 \rfloor$. In fact, the minimum number of nodes to separate from the network increases with the number of links to attack. Since the probability of a successful attack is the product of probabilities of the links to attack and given that the number of these links is large, then the resulting probability will converge to zero.

In some instances, we have seen that the solution is equal to 1 and this is due to the fact that the related networks are initially not connected.

VI. Conclusion

In this work, we extend the study by [6] to large networks. We provide a variety of tools to tackle reasonably sized networks. These tools include the shortest-path problem, the min-cut problem, the minimum-spanning-tree problem, the minimum bisection problem as well as integer programming. Our approach also extends to consider a variety of networks other than the one with a single source and a single destination that has been previously investigated. We illustrate, through

an example, the efficiency of our suggested methodology. In addition, we provide examples of interesting applications.

TABLE I
THE RESULTS OF THE EMPIRICAL STUDY

		D = 1		D = 5		D= ⌊n/3⌋	
n	m	Sol	Time	Sol	Time	Sol	Time
10	18	0.604	0.202	0.008	0.052	0.033	0.156
20	38	0.660	0.009	0.012	0.024	0.006	0.020
30	62	0.354	0.011	0.023	0.023	0.001	0.028
40	83	0.291	0.015	0.004	0.031	0.000	0.059
50	112	0.516	0.018	0.010	0.045	0.000	0.043
60	133	0.325	0.056	0.013	0.130	0.000	0.143
70	152	0.428	0.032	0.026	0.175	0.000	0.184
80	177	0.501	0.039	0.039	0.154	0.000	0.571
90	199	0.494	0.058	0.009	0.188	0.000	0.697
100	219	1.000	0.000	0.014	0.238	0.000	0.825
110	246	0.591	0.053	0.036	0.256	0.000	1.524
120	262	0.714	0.111	0.032	0.340	0.000	0.762
130	284	0.606	0.072	0.038	0.489	0.000	1.634
140	307	1.000	0.001	0.031	0.285	0.000	1.119
150	333	0.609	0.095	0.053	0.414	0.000	6.899
160	352	1.000	0.001	0.113	0.496	0.000	2.560
170	379	0.592	0.112	0.039	0.693	0.000	10.444
180	397	1.000	0.001	0.051	0.677	0.000	10.541
190	430	0.423	0.235	0.017	0.909	0.000	20.849
200	435	0.757	0.132	0.106	0.678	0.000	36.884
210	467	0.757	0.178	0.111	0.506	0.000	26.514
220	499	0.740	0.164	0.051	1.172	0.000	155.960
230	510	0.712	0.163	0.067	0.888	0.000	27.995
240	529	0.616	0.313	0.072	0.919	0.000	60.732
250	574	0.790	0.193	0.092	0.876	0.000	141.352
260	572	0.720	0.201	0.064	0.841	0.000	112.663
270	617	0.792	0.200	0.040	1.710	0.000	304.846
280	627	0.587	0.286	0.062	1.451	0.000	1811.413
290	661	0.602	0.448	0.082	1.259	0.000	411.580
300	669	0.533	0.241	0.052	1.459	*	>3600
310	698	0.559	0.221	0.092	1.563	0.000	1469.318
320	720	0.632	0.330	0.033	2.013	0.000	822.296
330	735	0.697	0.183	0.065	2.398	*	>3600
340	765	0.684	0.217	0.065	1.890	*	>3600
350	780	0.660	0.367	0.080	1.758	*	>3600
360	816	0.697	0.441	0.064	1.964	*	>3600
370	840	0.688	0.398	0.052	3.426	*	>3600
380	844	0.688	0.533	0.070	2.080	*	>3600
390	877	0.670	0.349	0.073	2.496	*	>3600
400	891	0.668	0.614	0.102	2.323	*	>3600
410	918	0.801	0.468	0.142	1.875	*	>3600
420	947	0.679	0.380	0.112	1.228	*	>3600
430	969	0.756	0.427	0.151	1.560	*	>3600
440	975	0.729	0.316	0.148	0.916	*	>3600
450	991	0.705	0.574	0.093	1.255	*	>3600
460	1041	0.659	0.488	0.075	2.321	*	>3600
470	1037	0.740	0.748	0.129	1.499	*	>3600
480	1056	0.613	0.475	0.085	2.226	*	>3600
490	1095	0.765	0.660	0.115	2.369	*	>3600
500	1122	0.880	0.484	0.127	3.420	*	>3600

REFERENCES

[1] Bier, Vicki M., M. N. Azaiez. 2009. Game theoretic risk analysis of security threats (ed.). International Series in Operations Research and Management Science 128 Springer.

[2] Azaiez, M. N., Vicki. M. Bier. 2007. Optimal resource allocation for security in reliability systems. European Journal of Operational Research, 181, 773–786.

[3] Cox, L. A. Jr., (2009). Making telecommunications network resilient against terrorist attacks, In Bier, V.M. and Azaiez, M. N. (ed.), Game theoretic risk analysis of security threats (pp. 175-197). New York: Springer: The International Series of Operations Research and Management Science, 128.

[4] Kanturska, U., Schmöcker, J.D., Fonzone, A., Bell, M., G., H., (2009). Improving reliability through multi-path routing and link defence, an application of game theory to transport. In Bier, V.M. and Azaiez, M. N. (ed.), Game theoretic risk analysis of security threats (pp. 199-227). New York: Springer: The International Series of Operations Research and Management Science, 128.

[5] Gharbi, A., Azaiez, M. N., Kharbech, M. (2010), "Minimizing Expected Attacking Cost in Networks", Electronic Notes in Discrete Mathematics,36, 947–954.

[6] Ben Yaghlane A., Azaiez M.N., Mrad M., 2015. System survivability in networks: submitted for publication