Reliability Evaluation by Expected Achievable Capacity in Stochastic Network Using Game Theory

Piyanan Satayapiwat, Kalika Suksomboon and Chaodit Aswakul

Department of Electrical Engineering, Faculty of Engineering,
Chulalongkorn University, Payathai Rd., Pathumwan, Bangkok 10330, Thailand
piyanan.satayapiwat@gmail.com, kmitmink@yahoo.com and chaodit.a@chula.ac.th

***Abstract*— To obtain a network with high fault tolerance, all possible characteristics of a failure event must be captured in the analysis. Also, an efficient method to identify and then upgrade vulnerable network components is required. A network game model between a router and intelligent attacker has been widely explored to overcome this challenge. In this paper, based on game theory framework, we have proposed a new vulnerability identification method to measure network reliability when the network is attacked by an intelligent adversary, who destroys network links to minimize capacity achieved between two network terminals. A new performance indicator– expected achievable capacity (EAC) has been proposed to help quantifying link vulnerability. To obtain EAC, a maximin problem is formulated and the method of successive averages is chosen to solve for the game solution. Numerical results show that the effect of worst-case failure on EAC can be thoroughly analyzed by the proposed framework.**

I. Introduction

Provision of highly reliable capacity for mission-critical data communications is the big issue for network planning. The disruption of a link or a node in the network can greatly worsen the normal pattern of network usages. Whenever possible, those links or nodes that are significant to the network performance must be made reliable. In the conventional analysis of network reliability and restoration design [1]-[5], the most common assumption is that link/node failure events occur either one at a time or in a simplified random manner. This assumption is well justified for failures occurring naturally. However, in recent years with the emergence of terrorist attempts, apart from natural failures, it is equally important that engineers must also be concerned with a new form of network reliability threat from intentional network attacks by hackers or terrorists. Building a robust network to overcome an intentional failure situation involves not only on protecting the critical network components but also to alleviate the failure's effects of any kind.

In the existing literature, the reliability issues based on an *intelligent* attacking entity have been widely investigated by using the framework of game theory. An interesting approach to cope with the worst case of failure scenario is to make use of game theoretic stochastic routing (GTSR) [6], [7]. GTSR selects a next hop beginning at a source towards its destination from the set of possible outgoing links in an optimal and random manner. Consequently, the number of eavesdropped/intercepted packets can be minimized by reducing the predictability of data transmission path.

The game theory has also been used in network reliability analysis of transportation systems. With game players being a dispatcher and a demon, the risk in transporting hazardous materials across a road network can be quantified [8]. The game objective is for the transport company to minimize the risk of exposing hazardous materials upon the road accidents which occur on purpose to maximize that risk. Likewise, when the system is a road network, the game players can be defined as the intelligent drivers that can optimally steer their vehicles to avoid the road congestion that is worsen by an imaginary network tester [9]-[11]. In a mobile ad hoc network (MANET), its reliability of communication has been modelled by a game competed between a router and an imaginary network tester [12]. This work has defined a new cost function to accommodate random link failure costs due to MANET wireless transmission nature. By solving this game, the relationship between mean link failure cost and optimal path selection scenarios can then be investigated.

As seen from the literature, the game theory is a powerful framework to analyze network reliability. This is especially true when the worst-case failure conditions are of major concern and, in response to failure events, the network has an intelligent mechanism to reroute necessary traffics away from the failed components. The existing literature relies on various definitions of cost function, depending on the system measures. These functions include the network delay or travel time [9]-[11] and the number of eavesdropped or intercepted packets [6].

In this work, the focus is steered towards a new cost function in terms of achievable flow capacity between two main terminals or nodes. The aim is in finding how much flow at most can be sent across a network. Indeed, this is inspired by the fundamental question in the well-known theory of maximum-flow, minimum-cut problem [13]. However, this work is aimed at finding how much *reliable* flow at most can be sent across a *stochastic* network whose components may fail randomly but in the most disruptive ways. The solution relies on a newly defined measure, called *expected achievable capacity (EAC)*, as to be further discussed in Section II. In addition, from the literature of vulnerability identification [9]-[11], vulnerable network components can be indicated by using the probability of equipment failure from attacker who invokes a particular link failure scenario to destroy links. The most vulnerable link can be identified by the link

978-1-4244-2036-0/08/$25.00

with highest chance of being attacked by attacker. However, the failure selection probability of the attacker can have more than one unique solutions leading to confusion when identifying the most vulnerable components. To overcome this drawback, this paper proposes a method to identify the links whose failure would affect the network achievable capacity the most. This method can be applied in helping network engineers sort out the vulnerability of links so that an efficient link backup plan can be well prepared.

The rest of this paper is organized as follows. In Section II, we define the EAC parameter. In Section III network game formulation, relevant assumptions, and methods to solve a game problem are given. Section IV proposes a new vulnerability identification method to indicate the most vulnerable link. Section V shows and discusses the numerical results. Section VI summarizes all findings from our work.

II. Expected Achievable Capacity

A network comprises of a set of nodes and links. Links are indexed by i with the total of I links. Assume that a link failure scenario j belongs to the failure scenario set of J possible cases. Also, the set of completely disrupted links, given the occurrence of link failure scenario j, is represented by Q_j. The functional capacity of link i is C_i, which is reduced to 0 if it fails. Let $C_{i,j}$ denote the achieved capacity from link i under failure scenario j. We then have

$$C_{i,j} = \begin{cases} 0, & i \in Q_j \\ C_i, & \text{otherwise.} \end{cases}$$

Note here that it is straightforward to extend from this formulation to partial link failure events where the failure does not disrupt the whole link capacity. A source node tries to send its data traffic towards its destination with the total of K possible paths. The set $L(k)$ of links along path k is chosen by the source node. There are two possibilities for the maximum capacity achieved from path k when link failure scenario j occurs. Firstly, if a link on path k fails, then the path cannot carry any data traffic. Secondly, if path k is not damaged under failure scenario j, then the achievable capacity equals the capacity of the bottleneck link on that path. Both cases bound the achievable capacity as

$$R_{k,j} = \min_{i \in L(k)} C_{i,j} \tag{1}$$

where $R_{k,j}$ defines the achievable capacity of path k under failure scenario j. For notational convenience, the payoff table of achievable capacity can be written in the matrix form

$$\mathbf{R} = \begin{bmatrix} R_{1,1} & \dots & R_{1,J} \\ \vdots & \ddots & \vdots \\ R_{K,1} & \dots & R_{K,J} \end{bmatrix} \tag{2}$$

In our formulated network game with mixed strategy, the sender selects path k with probability h_k and the failure scenario j occurs with probability q_j. The matrix form of these strategy selection probabilities are $\mathbf{H}^T = [h_1, \dots, h_K]$, $\mathbf{Q}^T = [q_1, \dots, q_J]$.

We define a new game cost function, *Expected Achievable Capacity* (EAC) as the maximum capacity achieved on average at the interval of data transmission when the worst-case link failure occurs. Given $\mathbf{H}$ and $\mathbf{Q}$, EAC can then be calculated from $\mathbf{R}$ directly:

$$EAC = \sum_{k=1}^{K} \sum_{j=1}^{J} h_k q_j R_{k,j} = \mathbf{H}^T \mathbf{R} \mathbf{Q}. \tag{3}$$

III. Game Formulation and Solution Methods

A. Player Strategy and Aim

In this section, network reliability analysis is visualized as a network game between two players, a router and an intelligent network attacker. Both players are assumed to be rational players. That is, the router objective is to maximize the achievable capacity by utilizing the optimal stochastic routing technique. Conversely, the network attacker objective is to minimize the achievable capacity by choosing to invoke random failure scenarios in an optimal manner. In this game, the objective cost function is directly computable from the proposed EAC, which is defined in (3). In the well-known maximin game formulation, the router seeks the best path selection strategy $\mathbf{H}$ by solving

$$\max_{\mathbf{H}} \min_{\mathbf{Q}} \mathbf{H}^T \mathbf{R} \mathbf{Q}. \tag{4}$$

and the attacker seeks the worst-case failure scenario $\mathbf{Q}$ by solving

$$\min_{\mathbf{Q}} \max_{\mathbf{H}} \mathbf{H}^T \mathbf{R} \mathbf{Q}. \tag{5}$$

Both (4) and (5) are optimized subject to the following constraints

$$\sum_{k=1}^{K} h_k = 1, \mathbf{H} \geq \mathbf{0}, \sum_{j=1}^{J} q_j = 1, \mathbf{Q} \geq \mathbf{0} \ . \tag{6}$$

From game theory literature, it is well known that we can transform (4)-(6) into a linear programming formulation [9]-[12]. J. V. Neumann [14] has shown that both optimal values obtained from (4) and (5) are the same and unique. Thus, the uniqueness of the EAC is guaranteed and the Nash equilibrium exists in this game. However, note that, path selection probabilities and link failure selection probabilities of both players at the Nash equilibrium may not be unique, as to be seen in Section V.

B. Solving Game by Method of Successive Averages

By updating selection probability for all possible strategies in each turn, the well-known method of successive averages (MSA) [11] has been here chosen to find a mixed-strategy Nash equilibrium solution to the maximin problem. An advantage of MSA over linear programming is that it can solve maximin and network reliability problems even when link costs are traffic dependent [11], [15]. For completeness, the solution method by MSA are summarized as follows.

1) At the beginning, set the turn index $n = 1$ and initialize the strategy selection probabilities for both

router player (h_k) and attacker player (q_j) by $h_k = \frac{1}{K}, q_j = \frac{1}{J}$.

2) Router calculates EAC, given each path selection strategy k ($k = 1, 2, \ldots, K$), from $E_k[R_{k,j}] = \sum_{j=1}^{J}[q_j R_{k,j}]$.
3) Router decides on the best path selection strategy $\hat{k}$ to maximize $E_k[R_{k,j}]$ from $\hat{k} = \arg\max_k E_k[R_{k,j}]$.
4) Router updates the new path selection probability (h_k) by MSA as

$$h_k \leftarrow (\frac{1}{n})x_k + (\frac{n-1}{n})h_k;\ x_k = \begin{cases} 1, & \text{if } k = \hat{k} \\ 0, & \text{otherwise .} \end{cases}$$

5) Attacker calculates EAC, given each failure scenario j ($j = 1, 2, \ldots, J$), from $E_j[R_{k,j}] = \sum_{k=1}^{K}[h_k R_{k,j}]$.
6) Attacker selects the best attacking strategy $\hat{j}$ to minimize $E_j[R_{k,j}]$ from $\hat{j} = \arg\min_j E_j[R_{k,j}]$.
7) Attacker updates failure selection probability (q_j) by using MSA:

$$q_j \leftarrow (\frac{1}{n})y_j + (\frac{n-1}{n})q_j;\ y_j = \begin{cases} 1, & \text{if } j = \hat{j} \\ 0, & \text{otherwise .} \end{cases}$$

8) Evaluate EAC from the game at iteration n

$$EAC = \sum_{k=1}^{K}\sum_{j=1}^{J} h_k q_j R_{k,j}.$$

9) If the selection probabilities h_k, q_j and EAC obtained are more different for the previous and current iterations than a tolerable threshold, then update $n \leftarrow n+1$ and go back to step 2. Otherwise, stop this recursion.

Note that, in steps 3 and 6, if there are at least two different strategies which yield the same EAC, then those strategies will be selected in a uniform random manner.

As the network grows in size and path alternatives increase, it is interesting to consider a more efficient algorithm apart from MSA in order to help reduce the burden of computational complexity. For example, the best-reply replicator dynamics in MSA can be replaced by a better-reply dynamics, where a player is allowed to opt for a better solution in each iteration, but not necessary the best. Not all actions need to be evaluated in each iteration. This results in an overall computational savings despite more iterations may be needed for a convergence. Such new iterative procedure warrants a worthy future investigation.

In the existing network game literature, the link vulnerability identification under the worst-case link-failure scenario relies on the attackers' link failure selection probability [9]-[11]. Nevertheless, it is possible to obtain multiple solutions from a network game and this may lead us to indicate an ambiguous set of vulnerable network links. Therefore, relying on failure selection probability is not reasonable for identification of link vulnerability. We need to change the vulnerability identification method to cope with this problem.

IV. Vulnerability Identification Method

Although failure selection probability can converge to multiple points of game solution, the proposed EAC always converges to a unique value. Therefore, we propose to use the EAC value to help identifying the network component vulnerability. The main concept of the proposed method is to quantify the effect of link capacity reduction on EAC. Hence, the proposed vulnerability identification begins with the removal of a certain amount of capacity from each link. Then, by using MSA, the remaining network with reduced capacity is analyzed for the EAC value of game. This value represents the obtainable maximum flow that can still pass through the remaining network when the worst-case link-failure scenario occurs. Let $EAC_i(\alpha)$ be the obtained EAC when link i is degraded by α capacity units. A link is said to be vulnerable if it causes the reduction of EAC once it is degraded. Therefore, the most vulnerable link $\hat{i}$ is defined by the link which gives the lowest EAC from

$$\hat{i} = \arg\min_i EAC_i(min(\alpha, C_i)). \tag{7}$$

V. Numerical Results

A. Comparison of Vulnerability Identification Methods

All numerical experiments throughout this paper are conducted to investigate a single link failure scenario, i.e. $Q_m = \{m\}; \forall m = 1, 2, \ldots, I$. In this part, the comparison of result characteristics from two different vulnerability identification methods are given, namely, the identification method in [9]-[11], and the newly proposed method in Section IV. Fig. 1 shows a network with each link capacity of 200 units. At the equilibrium, two different solutions of link failure selection probabilities are obtained (see Fig. 2). By [9]-[11], vulnerable network links can be indicated from the links with high failure selection probabilities. Fig. 2(a) indicates that links 2 and 5 are vulnerable links while Fig. 2(b) indicates that links 1, 2, 4, and 5 are vulnerable links. Both of these solution sets contradict each other because the vulnerable links indicated from Fig. 2(a) and Fig. 2(b) are not the same. Therefore, using link failure selection probability is not suitable to identify vulnerable links.

The proposed vulnerability identification method is now applied to analyze the same network. Fig. 3 shows the effect of link capacity degradation on the obtained EAC. Each graph represents the EAC when a link capacity is reduced. From the result, the proposed method produces *only one* solution set where links 1, 2, 4, and 5 are equally significant to the overall EAC. The result indicates that these four links must have the same level of protection because they give the same pattern of EAC reduction once they are degraded. In addition, this solution corresponds to the minimum-cut consisting of links 1, 2, 4, and 5. Because the solution is unique, looking for vulnerable network link by using EAC is more appropriate than using link failure selection probability.

B. Network Vulnerability Identification

The identification of link vulnerability to the overall EAC is investigated in this part. Fig. 4 represents a grid network

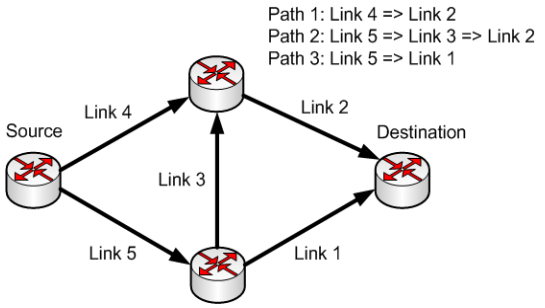

Fig. 1. A small network example.

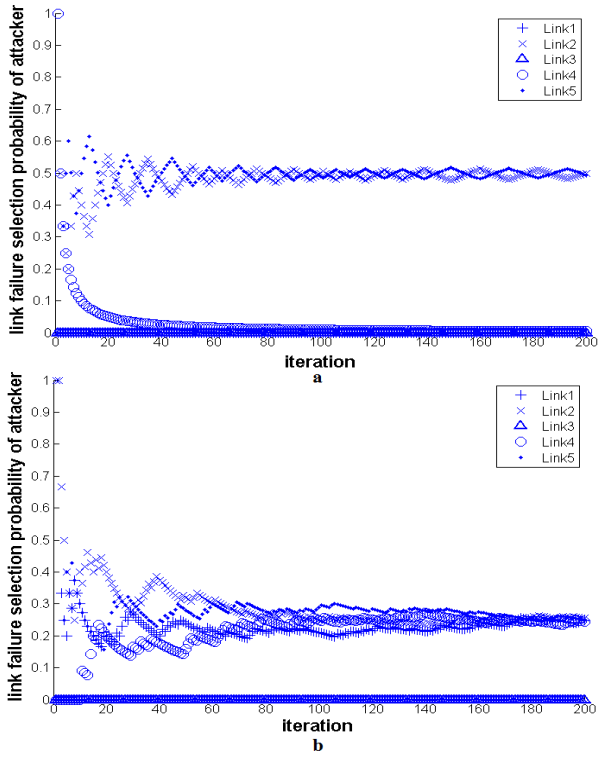

Fig. 2. Two different solutions of link failure selection probabilities from the game at the convergence point.

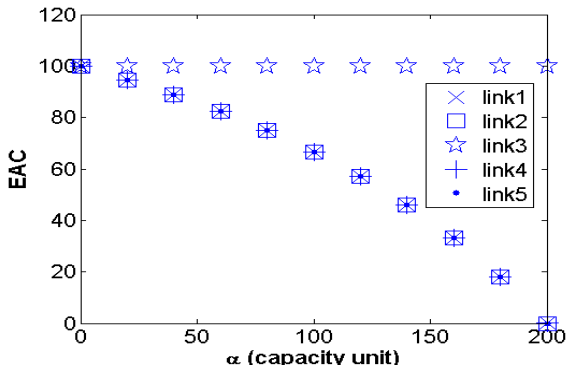

Fig. 3. Effect of capacity reduction on EAC for the small network.

with the capacity of links 1 to 12 of 11000, 6000, 2000, 15000, 31000, 1000, 32000, 7000, 28000, 17000, 22000, and 14000 units, respectively. This is also the network configuration used in [8]. Fig. 5 shows the effect of link capacity degradation on EAC. The most vulnerable link can then be identified using (7). If the target is on the overall system performance when a link is completely failed, then the link whose complete failure gives the lowest EAC must be protected first, i.e. links 1, 3, 10 and 12. Obviously, the remaining network without one of these four links cannot send any flows if it is attacked by an intelligent attacker. This is because both terminals in the remaining network can be disconnected by failing only one link. Consequently, the obtained EAC becomes 0 if any of these four links are removed.

When the target is to prevent the effect of partial capacity reduction, the link which yields the lowest EAC once its capacity is degraded must be protected first. To select α when a link is marginally degraded, the type of capacity degradation depends on the design criteria and severity of failure. For example, a complete link failure may be caused by fiber-cut from nuclear/terrorist attacks, or partial link degradation from occasional routine maintenance in which a fraction of link capacity might be disturbed. In practice, because the most vulnerable link can be changed depending on the value of α (see Fig. 5), network designers have to properly choose the level of α that closely reflects the severity of failure event which generally occurs in their network. Another approach to find the most vulnerable links can be done by setting the minimum requirement of EAC and varying the α value from 0 to the highest link capacity in the network. For the most vulnerable link, even gradual reduction of its capacity can sharply decrease the EAC to lower than the minimum EAC requirement. Therefore, one may sort the link vulnerability according to their minimum capacity needed be taken out to violate the network's minimum EAC requirement.

From Fig. 5, the vulnerable network components identified by (7) do not always correspond to links in the minimum-cut set. For instance, by minimum-cut set, links 1 and 3 are vulnerable links. However, apart from links 1 and 3, Fig. 5 shows that link 8 is another vulnerable link. For instance, if the capacity degradation α = 7,000 units, then our analysis suggests that link 8 is even *more* vulnerable than link 1. In this respect, one can conclude that the analysis via α is more refined than that of minimum-cut analysis because the link can be degraded at any level, not necessarily as a whole. Further, it can be noticed that links 4, 7, 8 and 11 have no effects on the overall EAC when their capacity is reduced. This is because the router can find a set of better alternative paths and then completely re-route all the traffic away from these links. As a result, reducing capacity of these links does not affect the obtained EAC.

The proposed vulnerability identification method can be applied to the real network configuration. Fig. 6 shows the Asia-Pacific Advanced Network (APAN) backbone network topology. The link number, capacity and connectivity of the

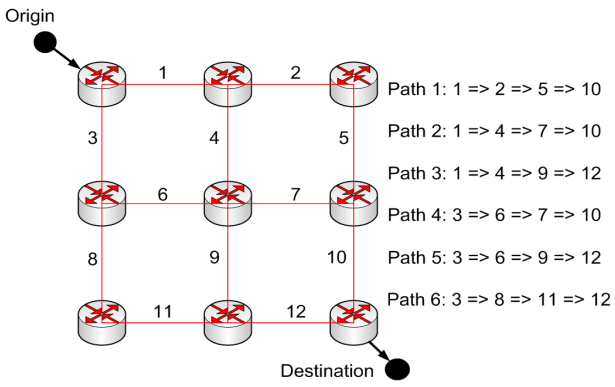

Fig. 4. Grid network with six possible paths for router player.

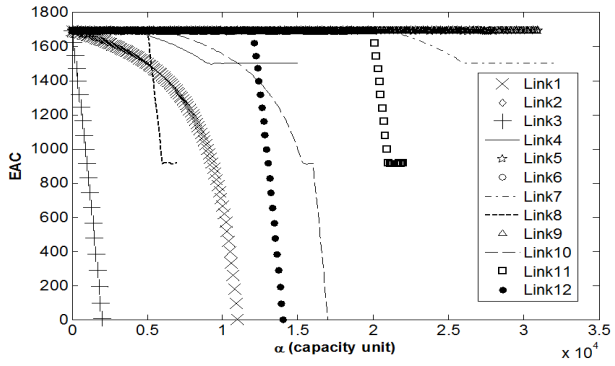

Fig. 5. Effect of link capacity reduction on EAC for a grid network.

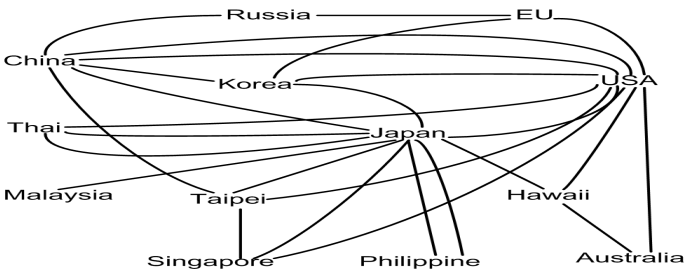

Fig. 6. Asia-Pacific Advanced Network (APAN) backbone network topology. The test used 25 paths to send data between China and Australia. All links are assumed to be bidirectional.

TABLE I

LINK CONNECTION CAPACITY

link	connection	capacity (Mbps)	link	connection	capacity (Mbps)
1	China-Russia	155	15	Thai-USA	155
2	Russia-EU	155	16	Malaysia-Japan	45
3	EU-USA	30000	17	Singapore-Japan	45
4	China-Korea	310	18	Taipei-Japan	622
5	Korea-EU	155	19	Singapore-Taipei	155
6	Korea-USA	1244	20	Philippine-Japan	45
7	Korea-Japan	2000	21	Philippine-Japan	155
8	China-USA	155	22	Singapore-USA	155
9	China-USA	45	23	Japan-Hawaii	155
10	China-Japan	2000	24	Taipei-USA	6600
11	Japan-USA	30000	25	Hawaii-USA	10000
12	China-Taipei	100	26	Hawaii-Australia	10000
13	Thai-Japan	44	27	Australia-USA	10000
14	Thai-Japan	45			

APAN network are given in Table I [16]. The effect of link capacity reduction is given in Fig. 7 where the considered demand pair is a connection between China and Australia. From Fig. 7, the proposed vulnerability identification method can identify the vulnerable network links which are links 4, 6, 10, 11, 25, 26, and 27. If preventing the complete link failure is the major concern, then links 26 and 27 must be protected most.

It is interesting to note that, after a link is degraded, the attacker would try to fail the remaining high-capacity links in order to leave the low-capacity links for data transmission. To avoid achieving low capacity between the considered demand pair, upgrading these low capacity links would eventually improve the obtained EAC at the occurrence of the worst-case link-failure event.

C. Effect of Different Failure Scenarios

Quantification of failure effect, in practice, needs to consider the relevant causes of network component failures i.e. (i) specific temporally-isolated failures each of which can always be restored before the next failure event occurs (SF), (ii) uniform random failures that randomly occur across the whole network (URF) and (iii) the worst-case random failures that are caused intentionally by attackers to minimize EAC (WCRF). The network topology in Fig. 4 is used to show the comparison of the EAC obtained from three different failure types where each link has 200 units of capacity (see Fig. 8). From Fig. 8, SF event has the least effect on the EAC reduction because a single link failure specifically occurs only on one link, and hence the router can eventually adapt the optimal stochastic routing policy to completely avoid the failed component. However, when a single link fails randomly, the routing attempts cannot successfully transmit the flow every time because of the randomness of failure events. This results in the reduction of EAC which gives the EAC lower than the SF case. At the Nash equilibrium, the WCRF event from game theoretical analysis can cause the transmission attempt to fail more frequently than the URF event, and WCRF event therefore gives the lowest EAC. To ensure that all types of possible failure events are prevented, reliability evaluation must be based on the worst-case result in order to analyze and protect the network in the most robust way.

VI. CONCLUSION

The contribution of this work is twofold. Firstly, we propose the EAC as a new network reliability indicator. Secondly, we propose a new method to identify link vulnerability from the EAC. The work scope is limited to only a single demand pair between two terminals. Previously, the multiple solution problem of strategies found at the game equilibrium introduces a difficulty in the identification of link vulnerability. This problem has been in this paper resolved by the proposed vulnerability identification method which

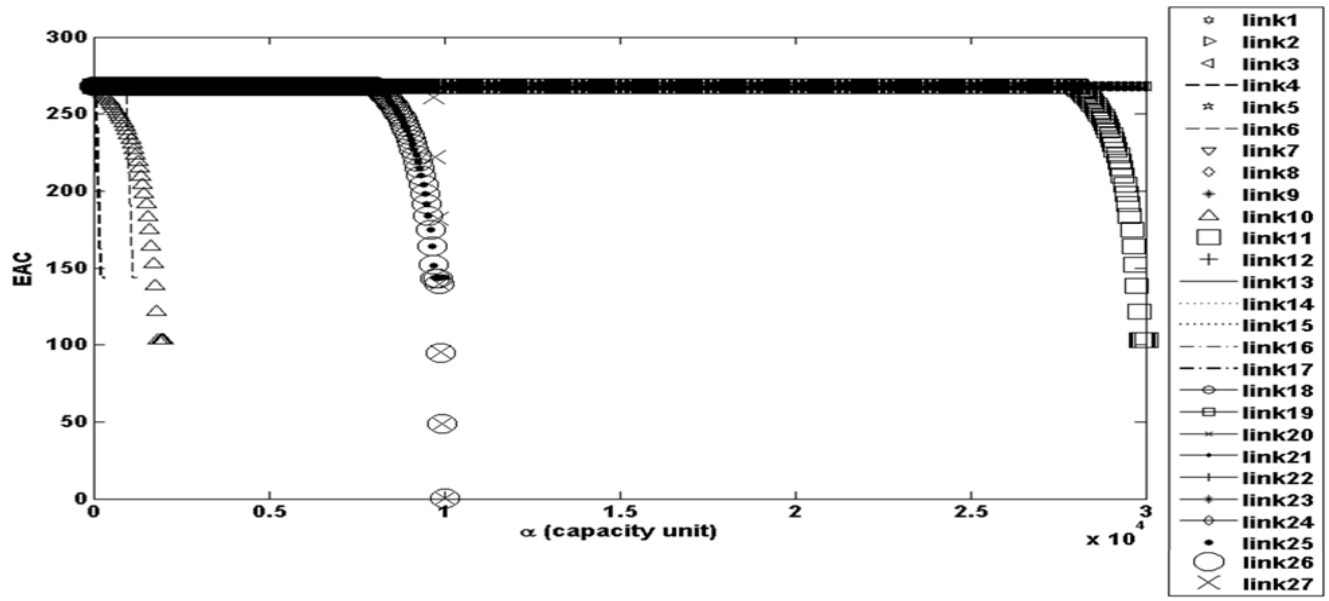

Fig. 7. Effect of link capacity reduction on EAC for the APAN network.

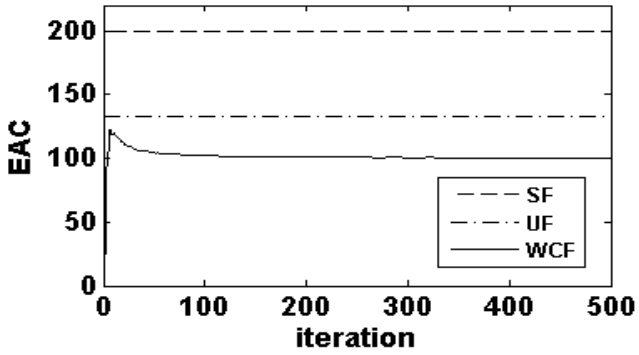

Fig. 8. EAC comparison for different failure scenarios. For SF case, the result of failing only one link is the same for every link.

can thoroughly sort out the vulnerable links in both aspects of failure (i.e. complete or partial link failure). To efficiently prevent a network from an intentional failure situation, the identification of system vulnerability, and reliability consideration must be based on the worst-case analysis. And, based on the obtained results, it is believed that the proposed EAC indicator via game theory framework could be most useful in such worst cases of failure analysis.

REFERENCES

[1] A. Chen, H. Yang, H. K. Lo, and W. Tang, "A capacity related reliability for transportation network" *Journal of Advanced Transportation*, vol. 33, no. 2, pp. 183-200, 1999.

[2] H. K. Lo, and Y. K. Tung, "Network with degradable links: capacity analysis and design" *Transportation Research Part B: Methodological*, vol. 37, no. 4, pp. 345-363, 2003.

[3] M. Pióro and D. Medhi, *Routing, Flow and Capacity Design in Communication and Computer Networks*, Morgan and Kaufman. June 2004.

[4] N. K. Singhal and B. Mukherjee, "Protecting multicast sessions in WDM optical mesh networks" *J. Lightw. Technol*, vol. 21, no. 4, pp. 884-892, 2003.

[5] N. K. Singhal, L. H. Sahasrabuddhe, B. Mukherjee, "Provisioning of survivable multicast sessions against single link failure in optical WDM mesh networks," *J. Lightw. Technol.*, vol. 21, no. 11, pp. 2587-2594, 2003.

[6] S. Bohacek, J. P. Hespanha, J. Lee, C. Lim, and K. Obraczka, "Game Theoretic Stochastic Routing for Fault Tolerance and Security in Computer Networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 18, no. 9, pp. 1227-1240, 2007.

[7] S. Bohacek, J. P. Hespanha, K. Obraczka, J. Lee, and C. Lim, "Enhancing Security via Stochastic Routing," *Proc. 11th IEEE Int'l Conf. Computer Comm. and Networks,*, 2002, pp. 58-62.

[8] M. G. H. Bell, "Mixed Route Strategies for the Risk-Averse Shipment of Hazardous Materials," *Netw. and Spat. Econ.*, vol. 6, no. 3, pp. 253-265, 2006.

[9] M. G. H. Bell "The measurement of reliability in stochastic transport networks," in *Proc. IEEE Int. Conf. Intell. Transp. Syst.*, Oakland, 2001, pp. 1183-1188.

[10] M. G. H. Bell, "A game theory approach to measuring the performance reliability of transport networks," *Transportation Research B*, vol. 34, no. 6, pp. 533-545, 2000.

[11] M. G. H. Bell, "The use of game theory to measure the vulnerability of stochastic networks," *IEEE Trans. Reliab.*, Vol. 52, no. 1, pp. 63-68, 2003.

[12] H. Karaa and J. Y. Lau, "Game Theory Applications in Network Reliability," in *Proc. Communications, 23rd Biennial Symposium*, 2006, pp. 236-239.

[13] L. R. Ford and D. R. Fulkerson, *Flows in Networks*. Princeton University Press, Princeton, NJ, 1962.

[14] J. V. Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*. Princeton University Press, 1944.

[15] Z. C. Li and H. J. Huang, "Fixed-Point Model and Schedule Reliability of Morning Commuting in Stochastic and Time-Dependent Transport Networks," in *LNCS*, vol. 3828, pp. 777-787, 2005.

[16] www.jp.apan.net.