مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
ویژه‌نامه کنفرانس بین‌المللی ترکیبیات، رمزنگاری و محاسبات، ص ۱۲۵ -۱۱۷

بهینه‌سازی محافظت از شبکه در برابر خط‌مشی‌های ممانعتی متنوع از طریق الگوریتم‌های تکاملی

وحید خرازی*

دانشگاه علم و صنعت ایران

(دریافت: ۹۵/۰۷/۰۵، پذیرش: ۹۶/۰۳/۰۶)

چکیده

هدف ما در این مقاله ارائه یک قالب بهینه‌سازی شبکه است که پایداری شبکه را برای یک جریان مورد نیاز عرضه و تقاضا بیشینه می‌کند. در قالب ارائه‌شده یال حالت تصادفی دارد که با درنظرگرفتن آسیب‌پذیری یال با استفاده از تابع میزان موفقیت مهاجم- مدافع مشخص می‌شود. در این قالب، هدف ممانعت‌کننده کاهش بیشینه جریان مورد انتظار شبکه از طریق تخریب یال‌های شبکه است. به‌علاوه، فرض می‌شود ممانعت‌کننده دارای منابع محدودی برای ممانعت از عناصر شبکه باشد. در این مطالعه به‌دنبال پیداکردن احتمال تخریب یک عنصر شبکه بوده و سپس می‌خواهیم منابع دفاعی در بین اقدامات دفاعی مختلف مثلاً جدایی، حفاظت و افزونگی به طور مطلوب توزیع کنیم به نحوی که پایداری سامانه حداکثر شود. رویکردهای متفاوتی که برای حل این قالب ممانعت مطرح شده‌اند غالباً برای شبکه‌های با ابعاد کوچک محدود می‌شوند. ما در این مقاله یک الگوریتم تکاملی برای حل این مسائل ارائه می‌دهیم. نتایج عددی به دست آمده نشان می‌دهد که این الگوریتم تکاملی فضای جواب را به طور قابل توجهی محدود می‌کند و بنابراین می‌توان آن را در شبکه‌های با ابعاد بزرگ به کار برد.

واژه‌های کلیدی: ممانعت در شبکه، محافظت از سیستم، پایداری شبکه، بهینه‌سازی تکاملی

۱- مقدمه

یک شبکه با پیکربندی معلوم و ثابت، تعدادی مصرف‌کننده محصول یا تحویل‌گیرنده خدمات را در نظر بگیرید به‌عنوان مثال در موارد قانونی، برق و ارتباطات و در موارد غیرقانونی مواد مخدر یا قاچاق اسلحه چنین شبکه‌ای را تشکیل می‌دهند. در این تحقیق تأثیر رویدادهای خارجی (به‌عنوان مثال، ۱۱ سپتامبر ۲۰۰۱ در مورد حمل و نقل و ۲۰۰۳ در مورد خاموشی در شبکه برق شمال غرب ایالات متحده) بر از کار افتادن اجزا در سطح شبکه بررسی می‌شود. زیر ساخت‌های حیاتی می‌توانند به‌عنوان شبکه‌های ارتباطی یا خدماتی تعریف شوند که برای اقتصاد و رفاه اجتماعی یک ملّت حیاتی هستند. به‌عنوان مثال، زیرساخت انرژی یکی از زیر ساخت‌های حیاتی است، بدون یک منبع انرژی پایدار، بهداشت و رفاه مورد تهدید است و اقتصاد کشور نمی‌تواند موثر باشد. بدیهی است برای بخش انرژی، عملکرد مناسب شبکه برق باید به‌طور مداوم بالا نگه داشته شود که این امر در مورد نگهداری و ایمنی شبکه حمل و نقل نیز درست است. در خارج از آمریکا، اتحادیه اروپا همراه با دیگر مدیران ملی و فرا ملی، درحال حاضر به اهمیت مهندسی قابلیت اطمینان و امنیت سیستم[1] که مرتبط با زیرساخت‌های حیاتی است پی برده و از طریق پیاده‌سازی سیاست‌ها و برنامه‌های خاص، (به خصوص برنامه اروپا برای حفاظت از زیرساخت‌های حیاتی) سعی در اجرای آن دارد. به‌طور خلاصه، از دیدگاه امنیتی، اختلال یا تخریب زیرساخت‌ها می‌تواند ضربه شدید و ناتوان‌کننده‌ای بر دفاع، امنیت اقتصادی و رفاه روانی کشور تحمیل کند. با توجه به این زیرساخت‌ها، می‌توان شبکه را قالب‌بندی کرد. به‌عنوان مثال، زیر ساخت‌های انرژی می‌تواند به‌عنوان جریان شبکه یا مخابرات به‌عنوان شبکه ارتباطی قالب‌بندی شود. تحقیق در زمینه قابلیت اطمینان و تجزیه و تحلیل خطر از طریق پیاده‌سازی خط‌مشی‌های محافظتی برای کاهش عدم جریان شبکه می‌تواند از اتفاقات ناخواسته در سطح شبکه که توسط شکست منابع داخلی ایجاد می‌شود جلوگیری کند.

مسائل ممانعت در شبکه تنوع بسیاری دارند و تعداد زیادی از این قالب‌ها تاکنون مطرح شده‌اند. تمامی قالب‌ها براساس سه رویکرد اصلی: بهینه‌سازی ترکیباتی، برنامه‌ریزی تصادفی و نظریه بازی می‌باشند. دراین قالب ممانعت که ما در این مقاله بررسی می‌کنیم ممانعت از هر یال به احتمال $p \leq 1$ موفق خواهد بود و هدف مهاجم کمینه کردن بیشینه جریان مورد انتظار است. برای این نوع مسائل، مک مسترز و ماستین[2] در [۱] یک روش حل مربوط به شبکه‌های مسطح (شبکه‌هایی که یال‌ها هم‌دیگر را قطع

* رایانامه نویسنده مسئول: kharazi@comp.iust.ac.ir

1- Reliability Engineering and System Safety

2- Mc Master and Mustin

نمی‌کنند) را براساس برنامه‌ریزی خطی ارائه کرده‌اند. این روش به شمارش مجموعه‌ای از اجزا نیاز دارد که شکست شبکه را تضمین می‌کنند و فقط در شبکه‌های با اندازه کوچک کاربرد دارد. برای این نوع شبکه‌ها، هلم بولد[1] [۲] یک روش برنامه‌ریزی پویا را پیاده‌سازی کرده که در آن مسطح‌بودن شبکه فرض شده است. بنابراین، قابلیت کاربرد آن به شبکه‌های با ابعاد کوچک محدود می‌شود. بویل[2] [۳] یک روش دوگان بسط‌یافته براین قالب در نظر گرفته است. این شیوه تمام مسیرهای s – t را که از بین می‌روند را می‌شمارد. هم‌چنین، وود[3] [۴] نشان داد که DNIP[4] یک NP- کامل است و یک قالب تازه از LP را ارائه کرد که توسط برنامه‌ریزی عدد صحیح حل می‌شود. با این‌حال این رویکرد در شبکه‌های با اندازه تقریباً کوچک اجرا شده بود. دای و پو[5] [۵] برای مواجه‌شدن با این محدودیت‌ها نخستین روش بهینه‌سازی تکاملی را برای حل مسائل DNIP ارائه کرده‌اند. این الگوریتم ژنتیک GA[6] می‌تواند جواب‌هایی برای شبکه‌های بزرگ تولید کند. با این‌حال، بایستی از مفاهیم مربوط به عملگر پیوند، جهش، جریمه و هم‌چنین پیش‌زمینه مناسبی در GA استفاده کرد. اخیراً راکو و رامیرز مارکز[7] در [۶]، PSDA[8] را ارائه کرده‌اند که یک الگوریتم تکاملی برای حل مسائل DNIP است. این الگوریتم فضای جواب را در یک جستجوی احتمالی مورد کاوش قرار می‌دهد.

۱-۱- تعریف مساله

اگرچه یکی از بی‌نهایت خط‌مشی‌های حمله‌ای توسط ممانعت‌کننده را می‌توان در نظر گرفت. در این تحقیق فرض بر این است که مهاجم منابع‌اش را به‌طور مساوی در میان تمام اجزای شبکه توزیع می‌کند. این فرض در مورد توزیع مساوی منابع در موارد زیر قابل توجیه است:

(a) مهاجم هیچ اطلاعی درباره ساختار شبکه و اهمیت یال‌های خاص ندارد و برای از بین‌بردن تمامی عناصر شبکه تلاش می‌کند.

(b) مهاجم هیچ توانایی برای هدایت حمله به یال‌های خاص را ندارد. به‌عنوان مثال، در استفاده از آلات موشکی با دقت پایین، مهاجم تلاش می‌کند به کل منطقه آسیب برساند و تنها بر حسب تصادف می‌تواند یالی را تخریب کند که تجهیزات زیادی در آن قرار گرفته است.

(c) سیستم نیازمند حفاظت در برابر بلایای طبیعی از قبیل سیل، طوفان و غیره است که کل منطقه را تخریب می‌کنند.

مفروضات این قالب به صورت زیر است:

- ظرفیت تمام یال‌ها مشخص است.
- تقاضای شبکه و پیکربندی- شبکه ثابت و مشخص است.
- بودجه مدافع و مهاجم معلوم است.
- بودجه حمله به‌طور مساوی در میان همه یال‌ها توزیع شده است.
- مهاجم یال‌های بدون محافظت را با احتمالی برابر با یک تخریب می‌کند.

جدول (۱): فهرست علائم و اختصارات استفاده‌شده در مقاله

$G(N,A)$	شبکه ظرفیت دار
$\boldsymbol{x}$	بردار خط‌مشی دفاعی= $\boldsymbol{x}=(x_{s1},\dots,x_{st},x_{12},\dots,x_{1n},\dots,x_{ij},\dots,x_{nt})$
x_{ij}	متغییر تصمیم‌گیری باینری، اگر یال شبکه بین گره‌های i و j دفاع شود $(x_{ij}=1)$ و در غیر این صورت $(x_{ij}=0)$
$\mathbf{x_u^h}$	h امین خط‌مشی دفاعی در چرخه u ام $\boldsymbol{x_u^h}=(x_{s1u}^h,\dots,x_{snu}^h,\dots,x_{12u}^h,\dots,x_{1nu}^h,\dots,x_{jhu}^h,\dots,x_{ntu}^h)$
$\boldsymbol{\gamma_u}$	بردار احتمال $\boldsymbol{\gamma_u}=(\gamma_{s1u},\dots,\gamma_{snu},\gamma_{12u},\dots,\gamma_{1nu},\dots,\gamma_{iju},\dots,\gamma_{ntu})$
γ_{ij}	احتمال این‌که از یال بین گره‌های i و j دفاع شود $P(x_{ij}=1)$
$\boldsymbol{k_{ij1}}$	مولفه جریان بین گره‌های i و j
v_{ij}	احتمال تخریب یال بین گره‌ها i و j
t_{ij}^m	منابع دفاعی اختصاص‌یافته برای هر یال بین گره‌های i و j
T_{ij}^m	منابع تهاجمی اختصاص‌یافته برای هر یال بین گره‌های i و j
m	پارامتر میزان درگیری
a	بردار وضعیت $\boldsymbol{a}=(a_{s1},\dots,a_{st},a_{12},\dots,a_{ij},\dots,a_{nt})$
b	بودجه تدافعی
B	بودجه تهاجمی
$\boldsymbol{\varphi(a)}$	جریان شبکه تحت بردار وضعیت a
$R(\boldsymbol{a}\|\boldsymbol{x'},d,v_{ij})$	پایداری شبکه تحت بردار خط‌مشی x' برای جریان داده شده d
d	جریان مورد نیاز شبکه
u	اندیس دور
S	اندازه مجموعه جواب
$\boldsymbol{x^*}$	بردار خط‌مشی دفاعی بهینه
$\vee$	عملگر یای منطقی

1- Helmbold
2- Boyle
3- Wood
4- Deterministic Network Interdiction Problem
5- Dai and Poh
6- Genetic Algorithm
7- Rocco and Ramirez-Marquez
8- Probabilistic Solution Discovery Algorithm

۱-۲- پیش‌زمینه حفاظت از شبکه‌ها

$G(N,A)$ را یک شبکه ظرفیتی با گره منبع s و گره تقاضا t در نظر بگیرید که N مجموعه‌ای از گره‌ها است و $A = A_1 \cup A_2$ که $A_1 = \{(s,i),(j,t)|1 < i,j < n\}$ و $A_2 = \{(i,j)|1 < i,j < n\}$ مجموعه‌ای از یال‌ها هستند. شبکه به ترتیب دارای بودجه تدافعی و تهاجمی b و B است. به علاوه، k_{ijv} یک عضو از $\boldsymbol{k_{ij}}$ است که بردار ظرفیت یال (i,j) را نمایش می‌دهد. برای این بردارها داریم $v = 0,1$ و $0 = k_{ij0} < k_{ij1}$. بردار وضعیت شبکه $\boldsymbol{a} = (a_{s1}, \dots, a_{st}, a_{12}, \dots, a_{ij}, \dots, a_{nt})$ ظرفیت جریان برای هر یال از شبکه است.

۱-۳- آسیب‌پذیری یال

آسیب‌پذیری یک یال شبکه v_{ij} (یعنی همان احتمال تخریب) به صورت نسبت تابع موفقیت [۸-۷] در رقابت مهاجم- مدافع به شکل:

$$v_{ij} = \frac{T_{ij}^m}{T_{ij}^m + t_{ij}^m}$$

تعریف می‌شود که در آن t_{ij}^m و T_{ij}^m به ترتیب بودجه تدافعی و تهاجمی اختصاص‌یافته به یال است و پارامتر m میزان درگیری به شرح زیر است:

۱) اگر $m = 0$، تلاش مهاجم و مدافع تأثیر یکسانی بر آسیب‌پذیری دارد.

۲) اگر $0 < m < 1$، نشان از یک عدم تناسب برتری ناشی از سرمایه‌گذاری کم‌تر از حریف دارد.

۳) اگر $1 < m < \infty$، نشان از یک عدم تناسب برتری برای سرمایه‌گذاری بیش‌تر از منابع حریف دارد.

۴) اگر $m = 1$، هر سرمایه‌گذاری تأثیر متناسب با آسیب‌پذیری اجزا دارد.

بنا بر توضیحات داده شده، در این قالب فرض بر این است که مهاجم منابعش را به طور مساوی در میان همه یال‌ها به طور مساوی توزیع می‌کند. بنابراین، $T_{ij} = B/|A|$. به‌علاوه بردار $\boldsymbol{x} = (x_{s1}, \dots, x_{st}, x_{12}, \dots, x_{1n}, \dots, x_{ij}, \dots, x_{nt})$ یک خط‌مشی دفاعی است به‌طوری‌که عنصر x_{ij} مقداری برابر با یک $(x_{ij} = 1)$ دارد اگر یال (i,j) به‌عنوان بخشی از خط‌مشی دفاعی تعریف‌شده باشد و مقدار صفر $(x_{ij} = 0)$ اگر دفاع نشود. در نتیجه، بردار خط‌مشی دفاعی مشخص می‌کند از کدام یال‌ها دفاع شود و چون در مفروضات این قالب بودجه دفاعی‌اش را به‌طور مساوی در میان یال‌های انتخاب‌شده برای دفاع پخش می‌کند، بنابراین داریم:

$$t_{ij}^m = \begin{cases} 0 & x_{ij} = 0 \\ \dfrac{b}{\sum_{ij} x_{ij}} x_{ij} & x_{ij} = 1 \end{cases}$$

جدول (۲): احتمال دقیق جریان s-t برای خط‌مشی‌های دفاعی مختلف

Defense strategy no.	Defense strategy (x_{s2}, x_{st}, x_{2t})	$(P(\varphi(a) = f\|x, v_{ij}\|)$				Expected flow
		$f = 0$	$f = 10$	$f = 100$	$f = 110$	
1	(0,0,0)	1	0	0	0	0
2	(1,0,0)	1	0	0	0	0
3	(0,1,0)	0.20	0.80	0	0	8
4	(0,0,1)	1	0	0	0	0
5	(1,1,0)	0.33	0.67	0	0	6.7
6	(1,0,1)	0.55	0	0.45	0	45
7	(0,1,1)	0.33	0.67	0	0	6.7
8	(1,1,1)	0.28	0.39	0.14	0.19	38.8

۱-۴- پایداری شبکه

تابع $\varphi(a): Z^{|A|} \to Z^+$ یک بردار حالت شبکه را به یک جریان شبکه بین $s-t$ می‌نگارد. بنابراین، پایداری شبکه تحت خط‌مشی دفاعی بردار x'، جریان داده‌شده d و آسیب‌پذیری‌های v_{ij} به‌صورت زیر تعریف می‌شود:

$$R(\boldsymbol{a}|\boldsymbol{x}', d, v_{ij}) = P(\varphi(\boldsymbol{a}) \geq d|\boldsymbol{x}', v_{ij})$$

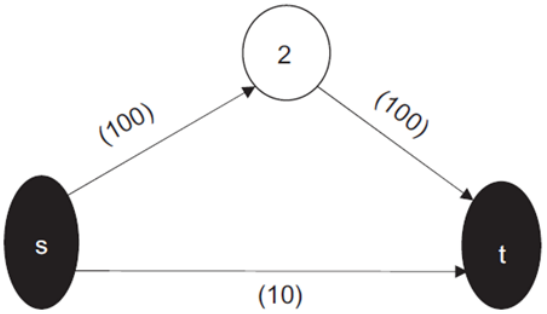
۱-۵- مثال تشریحی

برای روشن‌نمودن مفاهیم ذکرشده، همان‌طور که در شکل (۱) مشاهده می‌شود یک مثال در نظر گرفته‌ایم که در اصل توسط کرمیکن[1] و همکارانش در [۹] ارائه شده است. این شبکه ساده شامل یک گره منبع s و یک گره تقاضا t و گره میانی 2 است. مقدار بالای هر یال نشان‌دهنده ظرفیت آن یال است. فرض کنید برای این شبکه میزان درگیری $m = 1$ و بودجه تدافعی و تهاجمی به ترتیب b = ۴۰ و B = ۳۰ است.

برای این مثال، احتمال این‌که شبکه جریانی برابر با f داشته باشد را برای هر یک از خط‌مشی‌ها دفاعی ممکن نمایش می‌دهد.

1- Cormican

توجه داشته باشید که جریان شبکه تابعی از آسیب‌پذیری هریک از یال‌ها و نیز خط‌مشی دفاعی است. به‌عنوان مثال، برای خط‌مشی دفاعی نخست $T_{ij}^{m}=10$ و $t_{ij}^{m}=0$ به‌طوری‌که $v_{ij}=1$ برای هر یال (i,j) است. به طور مشابه در ششمین خط‌مشی دفاعی فقط دو یال حفاظت شده‌اند. در این دفاع، $T_{ij}^{m}=10$ و $t_{ij}^{m}=40/2=20$ به‌طوری‌که $v_{ij}=1/3$ برای یال‌های دفاع شده $(s,t$ و $2,t)$ و $v_{ij}=1$ برای یال دفاع نشده (s,t) است. در این مثال احتمال این‌که شبکه نتواند هیچ جریانی را انتقال دهد با درنظرگرفتن احتمال تخریب یال‌های x_{s2} و x_{2t} برابر با $1/3+1/3-1/9=0.55$ است. هم‌چنین احتمال این‌که جریان انتقالی برابر با ۱۰۰ واحد باشد را می‌توان به‌عنوان احتمال این‌که هر دو یال بعد از حمله باقی بمانند به دست آورد.



شکل (۱): مثال تشریحی

به‌علاوه، نتایج به ما اجازه مقایسه خط‌مشی‌های دفاعی مختلف و معیارهای بهینه‌سازی متفاوت را می‌دهد. به‌عنوان‌مثال، جواب بهینه می‌تواند s امین خط‌مشی باشد اگر هدف ماکزیمم کردن جریان مورد انتظار شبکه از گره منبع به گره مقصد باشد. بااین‌حال، اگر مدافع بخواهد خط‌مشی را انتخاب کند که جریان شبکه بیش‌تر یا مساوی ۱۰ واحد (به عنوان یک سطح اطمینان) باشد آن‌گاه سومین خط‌مشی، جواب بهینه است.

برای این قالب شبکه، محاسبه پایداری شبکه برای خط‌مشی دفاعی بردار x و جریان مورد نیاز شبکه d در $G(N,A)$ از طریق روش تحلیلی مشخص کرده مجموعه‌های مسیر/ برش کمینه ظرفیت‌دار [۱۱-۱۰] و یا یکی از روش‌های شبیه‌سازی [۱۳-۱۲] انجام می‌گیرد. چون محاسبه دقیق همه مجموعه‌های مسیر/ برش کمینه NP- سخت است و پیچیدگی محاسباتی با افزایش تعداد یال‌ها و گره‌های شبکه به طور نمایی افزایش می‌یابد. در این مقاله از شبیه‌سازی مونت‌کارلو برای تخمین $R(\boldsymbol{a}|\boldsymbol{x}',d,v_{ij})=P(\varphi(\boldsymbol{a})\geq d|\boldsymbol{x}',v_{ij})$ استفاده شده است.

به‌علاوه، نتایج به ما اجازه مقایسه خط‌مشی‌های دفاعی مختلف و معیارهای بهینه‌سازی متفاوت را می‌دهد. به‌عنوان‌مثال، جواب بهینه می‌تواند s امین خط‌مشی باشد اگر هدف ماکزیمم کردن جریان مورد انتظار شبکه از گره منبع به گره مقصد باشد. بااین‌حال، اگر مدافع بخواهد خط‌مشی را انتخاب کند که جریان شبکه بیش‌تر یا مساوی ۱۰ واحد (به عنوان یک سطح اطمینان) باشد آن‌گاه سومین خط‌مشی، جواب بهینه است.

۱-۶- قالب حفاظت بهینه از شبکه

تابع هدف در این قالب عبارت است از یک خط‌مشی دفاعی که پایداری شبکه را برای یک جریان به خصوص $s-t$ مورد نیاز شبکه در $G(N,A)$ به شکل:

$$\text{Max } R(\boldsymbol{a}|\boldsymbol{x}',d,v_{ij})$$
$$s.t.$$
$$(1)\ \ C(x)=b$$
$$(2)\sum_{i|x_{ij}}a_{ij}-\sum_{h|x_{jh}}a_{jh}=0\ \ \forall j\in N$$
$$(3)\ \ x_{ij}\in Bin(0,1)$$

را بیشینه می‌کند به طوری که:

۱) مجموعه هزینه دفاعی برای خط‌مشی دفاعی $\boldsymbol{x}$ برابر با بودجه دفاعی می‌باشد.

۲) جریان ورودی و خروجی هر گره تحت خط‌مشی دفاعی $\boldsymbol{x}$ باید برابر با صفر باشد.

۳) طبیعت دودویی متغیر تصمیم‌گیری $\boldsymbol{x}$ را نشان می‌دهد.

۲- روش تحلیل و ارائه نتایج

رویکرد تحقیق در این مسئله بر اساس سه گام زیر است:

۱) شبیه‌سازی مونت‌کارلو[1] برای به وجود آوردن خط‌مشی ممانعتی بالقوه؛

۲) الگوریتم فورد فولکرسون[2] [۱۴] برای ماکزیمم جریان $s-t$ شبکه؛

۳) الگوریتم تکاملی که ناحیه‌ای از فضای جواب را در هر چرخه براساس جستجوی احتمالی مورد کاوش قرار می‌دهد که از متناسب‌کردن جواب‌های تولیدشده به دست می‌آید؛

۲-۱- الگوریتم تکاملی PSDA

رویکرد بهینه‌سازی ارائه‌شده در این مقاله یک الگوریتم تکاملی (EA[3]) است که شباهت‌هایی با الگوریتم ژنتیک (GA) و بهینه‌سازی الگوریتم مورچگان (ACO[4]) دارد. در رابطه با الگوریتم ژنتیک،

1- Monte-Carlo Simulation
2- Ford-Fulkerson
3- Evolutionary Algorithm
4- Ant Colony Optimization Algorithms

تفاوت اساسی این است که الگوریتم حول محور مراحل مربوط به تولید نسل (انتخاب والدین، پیوند و جهش) نیست. در این الگوریتم ناحیه‌ای از فضای جواب براساس جستجوی احتمالی مورد کاوش قرار می‌گیرد که این احتمال از متناسب‌کردن جواب‌های تولیدشده در هر دور به دست می‌آید. هم‌چنان که روند الگوریتم پیش می‌رود ناحیه مورد جستجو به سمت جواب‌های بهتر سوق پیدا می‌کند. به عنوان تفاوت با الگوریتم مورچگان، الگوریتم ارائه‌شده فضای جواب را با استفاده از تابع جریمه و بهترین جواب‌های به‌دست‌آمده در هر دور به‌روزرسانی می‌کند. مانند دیگر الگوریتم‌های تکاملی PSDA برای تمامی مسائل هم‌گرا نیست [۱۵]. با این حال، طبیعت احتمالی PSDA باعث می‌شود ناحیه‌ای از فضای جواب را جستجو کند که جواب‌هایی با کیفیت بالا دارد. این الگوریتم تکاملی ثابت شده است که جواب‌هایی با کیفیت بالا برای انواع مختلف ممانعت در شبکه‌ها [۱۶]، تخصیص قابلیت اطمینان [۱۷]، بازرسی محتوا [۱۸] و شبکه‌های بی‌سیم [۱۹] دارد. در این رابطه برونز[1] [۲۰] یک شیوه مشابه برای کاوش فضای جواب از طریق تراکم مرزی برای حل مسائل بهینه‌سازی مقید ارائه کرده است. امتیاز PSDA این است که تنها به سه پارامتر برای به دست آوردن جواب بهینه نیاز دارد.

۲-۲- ایجاد خط‌مشی

در این گام، یک تعداد به خصوص (SAMPEL) از خط‌مشی‌های دفاعی $\boldsymbol{x_u^h} = (x_{s1u}^h, \dots, x_{snu}^h, \dots, x_{12u}^h, \dots, x_{1nu}^h, \dots, x_{jhu}^h, \dots, x_{ntu}^h)$ را با استفاده از شبیه‌سازی مونت کارلو و براساس احتمال دیکته‌شده توسط بردار احتمال:

$$\boldsymbol{\gamma_u} = (\gamma_{s1u}, \dots, \gamma_{snu}, \gamma_{12u}, \dots, \gamma_{1nu}, \dots, \gamma_{iju}, \dots, \gamma_{ntu})$$

تولید می‌کنیم. مؤلفه $\boldsymbol{\gamma_u}$ از γ_{iju} برابر با احتمال این است که یال (i,j) به عنوان بخشی از خط‌مشی دفاعی انتخاب شود، $\gamma_{iju} = p(x_{iju}^h = 1)$. این گام هم‌چنین تعیین می‌کند که الگوریتم چه موقع خاتمه یابد.

الگوریتم زمانی متوقف می‌شود که بردار γ_u دیگر نمی‌تواند به‌روزرسانی شود، یعنی همه مؤلفه‌های γ_u صفر یا یک هستند. شبه کد الگوریتم برای این گام به‌صورت زیر است:

Step 1—Strategy development:
For $h = 1, \dots,$ SAMPLE
{For $i = 1, \dots, n$ and $j = 1, \dots, n$ implement MC simulation and as dictated by γ_u generate a network defense design $\mathbf{x}_u^h = (x_{s1u}^h, \dots, x_{snu}^h, x_{12u}^h, \dots, x_{1nu}^h, \dots, x_{iju}^h, \dots, x_{ntu}^h)$
$h \to h+1$;}
if $(\gamma_{iju} = 1 \vee \gamma_{iju} = 0 \ \forall\ i, j) \vee u = U$, then Stop, $x^* = \arg\max\{K\}$.
else go to step 2.

۲-۳- تجزیه و تحلیل خط‌مشی

در گام دوم، الگوریتم تعداد یال‌ها دفاع‌شده برای هر $\mathbf{x_u^h}$ را بررسی می‌کند و سپس پایداری شبکه $R(\boldsymbol{a}|\boldsymbol{x_u^h}, d, v_{ij})$، را برای هر خط‌مشی دفاعی $\boldsymbol{x_u^h}$ بر اساس بردارهای k_{ij} و v_{ij} تخمین می‌زند. تعداد زیادی از روش‌ها برای به دست آوردن $R(\boldsymbol{a}|\boldsymbol{x_u^h}, d, v_{ij})$ وجود دارد. در این مقاله از روش شبیه‌سازی مونت کارلو همراه با الگوریتم فورد فولکرسون براساس مقاله [۱۴] برای تخمین پایداری یک خط‌مشی دفاعی استفاده شده است.

برای یک خط‌مشی دفاعی به خصوص $\mathbf{x_u^h}$، بردار تصادفی $\mathbf{x_u'^h}$ را با درنظرگرفتن این‌که کدام یال‌ها برای دفاع انتخاب شده‌اند و آسیب‌پذیری آن‌ها تولید می‌کنیم. سپس این بردار توسط الگوریتم فورد فولکرسون برای مشخص‌کردن ماکزیمم جریان مورد ارزیابی قرار می‌گیرد. وقتی‌که ماکزیمم جریان بیش‌تر یا برابر با مقدار جریان مورد نیاز برای پایداری شبکه d باشد، $\mathbf{x_u'^h}$ به عنوان یک وضعیت موفق محسوب می‌شود و شمارنده تعداد وضعیت‌های موفق سیستم یک واحد افزایش می‌یابد، در غیر این صورت، شمارنده بدون تغییر باقی می‌ماند. این روند $NSIMUL$ بار تکرار می‌شود. برای تخمین پایداری شبکه تعداد وضعیت‌های موفق سیستم را بر $NSIMUL$ تقسیم می‌کنیم. بعد از به‌دست‌آوردن پایداری شبکه برای هر خط‌مشی دفاعی، جواب‌های به‌دست‌آمده را از بزرگ به کوچک مرتب می‌کنیم. شبه کد الگوریتم برای این گام به‌صورت زیر است:

Step 2—Strategy Analysis and Penalization:
For $h = 1, \dots,$ SAMPLE
Obtain $t_{ij}^m = b/\Sigma_{ij}x_{ij}$ and estimate $R(\mathbf{a}|\mathbf{x}_u^h, d, v_{ij})$
List $R(\mathbf{a}|\mathbf{x}_u^h, d, v_{ij})$ by decreasing order of magnitude:
$R(\mathbf{a}|\mathbf{x}_u^{(1)}, d, v_{ij}) \geq R(\mathbf{a}|\mathbf{x}_u^{(2)}, d, v_{ij}) \geq \dots \geq R(\mathbf{a}|\mathbf{x}_u^{(\text{SAMPLE})}, d, v_{ij})$.

۲-۴- کاوش جواب

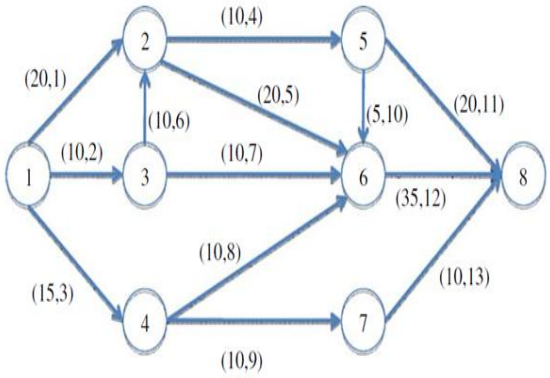
در سومین و آخرین گام از الگوریتم PSDA، یک زیرمجموعه مرتب از خط‌مشی‌های دفاعی برای به‌روز رسانی بردار احتمال γ_u مورد استفاده قرار می‌گیرد. این بردار جدید به گام نخست برای بررسی‌نمودن خاتمه الگوریتم یا برای هدایت کاوش تکاملی به سمت جواب‌های با کیفیت بالاتر فرستاده می‌شود. هم‌چنین در این گام تعداد به خصوص S از بهترین جواب‌های به‌دست‌آمده در چرخه در مجموعه K ذخیره می‌شود. شبه کد الگوریتم برای این گام به صورت زیر است:

Step 3—Solution Discovery
$\dots K \to K \cup R(\mathbf{a}|\mathbf{x}_u^{(1)}, d, v_{ij}) \geq R(\mathbf{a}|\mathbf{x}_u^{(2)}, d, v_{ij}) \geq \dots \geq R(\mathbf{a}|\mathbf{x}_u^{(\text{TOP})}, d, v_{ij}) \dots$
$u \to u+1$;
For $i = s,1, \dots, n$ and $j = 1, \dots, n$, t update vector γ_u as follows:
$\gamma_{iju} = (\Sigma_{k=1}^{S} x_{iju-1}^{(k)})/S$ where $S \ll$ SAMPLE;
Go to Step 1.

1- Berrones

۳- نتایج محاسباتی

برای نشان‌دادن رفتار PSDA برای مسئله حفاظت از شبکه از یک مثال استفاده می‌کنیم. شبکه‌ای که آن‌ها را مورد تجزیه و تحلیل قرار می‌دهیم در شکل (۲) مشاهده می‌شود، مقادیر بالای هر یال به ترتیب ظرفیت و اندیس آن‌ها نشان می‌دهد. برای مثال، یال بین گره‌های ۱ و ۲ دارای ظرفیت ۲۰ واحد و اندیس ۱ است. در این پیکربندی شبکه ماکزیمم جریانی که از گره منبع ۱ به گره چاهک ۲ می‌توان فرستاد ۴۵ واحد است. در این مثال فرض بر این است که مهاجم منابعش را میان تمام یال‌ها به طور مساوی تقسیم می‌کند و هیچ اطلاعی از پیکربندی شبکه و اهمیت یال‌های به خصوص ندارد. برای تشریح بهینه‌سازی قالب و راه‌حلش، سه جریان $d = (10,20,40)$، دو بودجه تهاجمی $B = (260,520)$، سه بودجه تدافعی $b = (130,650,1300)$ و سه میزان درگیری $m = (./3,1,3)$ در نظر گرفته شده است. برای این مثال پارامترهای مورد نیاز برای PSDA به صورت $SAMPEL = 50$، $U = 20$ و $S = 7$ در نظر گرفته شده است.



شکل (۲): یک مثال عددی برای تجزیه و تحلیل شبکه

نتایج به‌دست‌آمده از شرایط متفاوت در نظر گرفته‌شده در شکل (۲) نمایش داده شده است. این نتایج درک مناسبی از خط‌مشی دفاعی برای بیشینه‌کردن پایداری شبکه را فراهم می‌کنند. برای سه تقاضای شبکه نتایج به‌دست‌آمده بینش زیر را ارائه می‌دهند:

برای تقاضای ۱۰ واحد، پیکربندی شبکه افزونگی زیادی دارد و به مسیرهای گوناگون عرضه و تقاضا اجازه می‌دهد تا تقاضای شبکه را برآورده سازند. در این حالت، نتایج شکل (۲) نشان می‌دهند زمانی که بودجه تدافعی کم است، انتخاب خط‌مشی دفاعی بهینه براساس انتخاب یک مسیر عرضه و تقاضا (با اختصاص تمام منابع تدافعی به یال‌های این مسیر) و یا توزیع منابع در یال‌های گوناگون شبکه برای افزایش مختصر پایداری هریک از مسیرهای افزونه دیگر می‌باشد.

برای تشریح استدلال بالا سه حالت برای $B = 260$ در نظر می‌گیریم، اگر از تمام یال‌های شبکه حفاظت شود و $m = 1$ فرض شود. احتمال این‌که هر یال حفاظت‌شده تخریب نشود $(1 - v_{ij})$ به ترتیب بایستی برابر با ۰/۳۳۳۳، ۰/۷۱۴۳ و ۰/۸۳۳۳ باشد. براساس این آسیب‌پذیری‌ها، پایداری شبکه زمانی که از تمام یال‌های حفاظت شود به ترتیب برابر با ۰/۱۷۸۶، ۰/۸۵۸۹ و ۰/۹۶۹۸ است. طبق جدول (۳) پایداری شبکه برای خط‌مشی‌های دفاعی به ترتیب ۰/۳۳۱۵، ۰/۸۸۸۶ و ۰/۹۷۹۸ است. بنابراین جواب‌های به‌دست‌آمده توسط PSDA نشان می‌دهند که وقتی منابع تدافعی برای ایجاد افزونگی محدود هستند، منابع بایستی برای ماکزیمم‌کردن پایداری در یک مسیر عرضه- تقاضا (مسیر انتخابی شامل یال‌های شماره ۱، ۵ و ۱۲ برای b=۱۳۰) مورد استفاده قرار گیرند. هم‌چنان که منابع افزایش می‌یابند، چون آسیب‌پذیری عناصر (یال‌ها) کاهش می‌یابد، افزونگی پایداری تدافعی را بهبود می‌بخشد (همان‌طورکه مشاهده می‌کنید برای $b = 1300$ فقط از یال شماره ۱۰ حفاظت نشده است).

این استدلال هم‌چنین برای میزان بالای درگیری $m = 3$ نیز برقرار است. در این حالت وقتی منابع دفاعی یال افزایش می‌یابد، آسیب‌پذیری یال به‌سرعت کاهش می‌یابد. درنهایت برای حالتی که میزان درگیری پایین است، $m = 0.3$، زمانی که فقط از یک مسیر (به‌عنوان‌مثال ۱، ۵ و ۱۲) استفاده می‌کنیم آسیب‌پذیری یال‌ها بین ۰/۲۸۸۸ در بهترین حالت و ۰/۴۹۴۶ در بدترین حالت متغیر است، همواره از تخصیص منابع به یال‌های گوناگون به‌منظور ایجاد افزونگی استفاده می‌کنیم. در حقیقت وقتی میزان درگیری پایین است افزایش تلاش برای حفاظت از هر یال به خصوص تأثیر ناچیزی در کاهش آسیب‌پذیری آن یال دارد. بنابراین، فراهم‌نمودن افزونگی برای حفاظت از مسیرها (حفاظت از تعداد زیادی از یال‌ها) بسیار کاراتر از تخصیص منابع به تعداد کمی از یال‌ها است.

جدول (۳): نتایج محاسباتی به دست آمده در شرایط متفاوت

d	B	b	$m=1$			$m=0.3$			$m=3$	
			Non-defended links	Net.surv		Non-defended links	Net.surv		Non-defended links	Net.surv
۴۰	۵۲۰	۱۳۰	۸ ،۶	۰,۰۰۲۴		۴، ۶، ۸، ۱۰، ۱۱	۰/۰۰۲۴		NS*	۰,۰۰۰۰
		۶۵۰	۱۰ ،۶	۰,۰۲۷۴		۱۰	۰,۰۱۱۷		۴، ۶، ۸، ۱۰، ۱۱	۰,۴۱۹۹
		۱۳۰۰	۴، ۶، ۸، ۱۰، ۱۱	۰,۱۸۷۵		۱۰	۰,۰۲۲۵		۴، ۶، ۸، ۱۰، ۱۱	۰,۸۹۵۰
	۲۶۰	۱۳۰	۴، ۶، ۸، ۱۰، ۱۱	۰,۰۰۲۹		۱۰	۰,۰۰۴۶		NS*	۰,۰۰۰
		۶۵۰	۴، ۶، ۸، ۱۰، ۱۱	۰,۱۸۰۶		۱۰	۰,۰۲۴۱		۴، ۶، ۸، ۱۰، ۱۱	۰,۸۹۶۴
		۱۳۰۰	۴، ۶، ۸، ۱۰، ۱۱	۰,۴۰۶۲		۱۰	۰,۰۴۴۰		۴، ۶، ۸، ۱۰، ۱۱	۰,۹۸۹۳
۲۰	۵۲۰	۱۳۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۱۵۲۰		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۱۳۹۱		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۱۸۲۸
		۶۵۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۶۰۸۶		۴، ۶، ۹، ۱۰، ۱۱ ، ۱۳	۰,۲۲۹۰		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۹۸۵۱
		۱۳۰۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۷۷۷۶		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۳۰۵۵		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۹۹۸۹
	۲۶۰	۱۳۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۳۲۷۰		۶، ۹، ۱۰، ۱۱، ۱۳	۰,۱۴۶۱		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۷۶۷۰
		۶۵۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۷۸۴۱		۱۰	۰,۳۰۲۶		۶، ۸، ۱۰	۰,۹۹۴۱
		۱۳۰۰	۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۸۸۰۰		۴، ۶، ۹، ۱۰، ۱۱ ، ۱۳	۰,۳۷۷۵		۲، ۳، ۴، ۶، ۷، ۸، ۹، ۱۰، ۱۱، ۱۳	۰,۹۹۹۸
۱۰	۵۲۰	۱۳۰	۱، ۲، ۴، ۵، ۶، ۷، ۹ ، ۱۰، ۱۱، ۱۳	۰,۱۴۱۲		۱۰	۰,۲۹۵۹		۱، ۲، ۴، ۵، ۶، ۷، ۹، ۱۰، ۱۱، ۱۳	۰,۱۸۲۳
		۶۵۰	۱۰ ،۶	۰,۶۴۲۶		۱۰	۰,۵۲۲۹		۱، ۲، ۴، ۵، ۶، ۷، ۹، ۱۰، ۱۱، ۱۳	۰,۹۸۴۶
		۱۳۰۰	۱۰ ،۶	۰,۸۸۶۴		۱۰	۰,۶۲۶۳		۱۰ ،۸ ،۶ ،۵	۰,۹۹۹۸
	۲۶۰	۱۳۰	۲، ۳، ۴، ۶، ۷، ۸، ۹ ، ۱۰، ۱۱	۰,۳۳۱۵		۱۰	۰,۳۸۶۸		۱، ۳، ۴، ۵، ۶، ۸، ۹، ۱۰، ۱۱،۱۳	۰,۷۶۳۰
		۶۵۰	۱۰ ،۶	۰,۸۸۸۶		۱۰	۰,۶۲۶۳		۱۰ ،۸ ،۶ ،۵	۰,۹۹۹۶
		۱۳۰۰	۱۰	۰,۹۷۸۷		۱۰	۰,۷۲۳۰		۱۰	۰,۹۹۹۹

زمانی‌که تقاضای شبکه ۲۰ واحد در نظر گرفته شود، تعداد مسیرهای افزونه برای تأمین این جریان کاهش می‌یابد. فقط دو مسیر مستقل وجود دارد که تقاضای شبکه را برآورده می‌سازند - اولی مسیر شامل یال‌های ۱، ۵ و ۱۲ درحالی‌که دومی شامل یال‌های ۲، ۳، ۴، ۶، ۹، ۱۱ و ۱۳ است. بنابراین خط‌مشی دفاعی یا بایستی یکی از این دو مسیرهای منبع- مقصد حفاظت کند و یا حول هر یک از آن‌ها افزونگی ایجاد کند.

نتایج به‌دست‌آمده برای هر یک از بودجه‌های تدافعی و تهاجمی زمانی که $m = 1,3$ است، رفتاری مشابه با بحث قبلی دارد. درنتیجه، بهترین خط‌مشی دفاعی مسیر ۱، ۵ و ۱۲ است، چون شامل تعداد کمی یال است و بنابراین آسیب‌پذیری یال‌ها کم است. تنها جوابی که از این رفتار تبعیت نمی‌کند یال‌های ۶، ۸ و ۱۰ را تعریف می‌کند که برای ایجاد افزونگی ضروری نیستند.

برای تقاضای $d = 40$ واحد تنها مسیر تأمین‌کننده جریان، شامل یال‌های ۱، ۲، ۳، ۵، ۷، ۹، ۱۲ و ۱۳ است. همان‌طورکه قبلاً بحث شد، بودجه منابع بایستی به این مسیر اختصاص یابد تا آسیب‌پذیری این مسیر کاهش یابد. جواب‌های بهینه برای $m = 1$ و $m = 3$ نشان می‌دهند که تنها از یال‌های ۴، ۶، ۸، ۱۰ و ۱۱ حفاظت نشده است.

برای این تقاضا، بالابردن افزونگی حداقل نیازمند سه یال اضافی دیگر است. بنابراین، به طور قابل توجهی منابع تخصیص‌یافته به سایر یال‌ها را کاهش می‌دهد. با این حال، در این مورد هنگامی‌که بودجه دفاعی کم است، منابع تهاجمی دفاع را در هم می‌شکنند. چون در شبیه‌سازی انجام‌شده مقادیر بسیار نزدیک به صفر بودند هیچ خط‌مشی دفاعی برای تأمین جریان موردنیاز وجود ندارد و PSDA جواب NS[1] را نمایش می‌دهد.

۳-۱- نتایج دای و پو

شبکه در نظر گرفته‌شده برای این مثال در واقع از دای و پو [۶] گرفته شده است. همان‌طور که در شکل (۲) مشاهده می‌کنید مقادیر بالای هر یال به ترتیب ظرفیت و اندیس آن یال را نشان می‌دهد. برای این پیکربندی شبکه ماکزیمم جریان از s به t برابر ۴۴ واحد است، زمانی که هیچ حمله‌ای وجود ندارد. جدول (۴) نتایج حاصل از حالت‌های مختلف قالب آسیب‌پذیری شبکه را نشان می‌دهد.

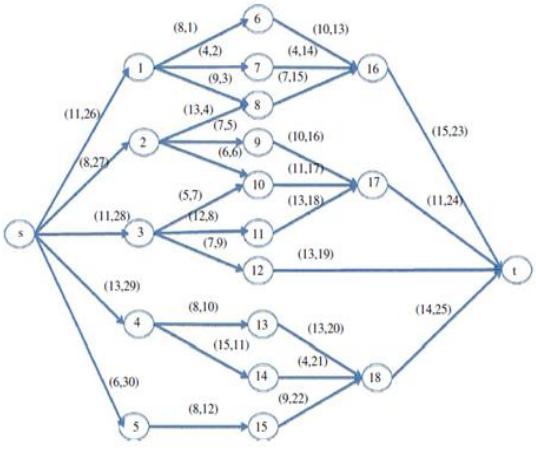
1- No Solution

جدول (۴). نتایج حاصل از حالت‌های مختلف قالب آسیب‌پذیری شبکه (دای و پو)

Net.surv	$m=5$ Non-defended links	Net.surv	$m=0.2$ Non-defended links	Net.surv	$m=1$ Non-defended links	b	B	d
۰,۷۲۳۵	۲، ۵، ۸، ۱۱، ۱۴، ۱۶، ۱۸، ۲۱	۰,۰۰۰۰	NS	۰,۰۰۵	۱۷	۱۰۰۰		
۰,۹۹۷۵	۲، ۶، ۷، ۱۱، ۱۴، ۱۷، ۲۱	۰,۰۰۰۵	۱۷، ۱۵	۰,۰۶۱۵	۲، ۱۱، ۱۴، ۲۱	۳۰۰۰	۶۰۰	
۰,۹۹۹۰	۵، ۱۴، ۱۶، ۲۱	۰,۰۰۱۰	۸، ۲	۰,۳۷۰۵	۲، ۱۱، ۱۴، ۲۱	۹۰۰۰		۴۴
۰,۹۹۵۰	۳، ۵، ۸، ۱۱، ۱۶، ۱۸، ۲۱	۰,۰۰۰۰	NS	۰,۰۴۹۰	۲، ۱۱، ۱۴، ۲۱	۱۰۰۰		
۰,۹۹۸۵	۶، ۱۱، ۱۴، ۱۷	۰,۰۰۱۵	۲۰	۰,۳۵۰۵	۲، ۱۱، ۱۴، ۲۱	۳۰۰۰	۲۱۰	
۰,۹۹۹۰	۱۴	۰,۰۰۳۰	۲۱، ۱۱	۰,۷۱۵۰	۲۱، ۱۱	۱۳۰۰		
0.9915	۲، ۴، ۶، ۸، ۱۲، ۱۴، ۱۸، ۲۲، ۳۰	۰,۰۰۶۵	۵، ۲	۰,۰۴۰۰	۶، ۷، ۱۷	۱۰۰۰		
۰,۹۹۹۵	۱۴، ۲	۰,۰۱۵۰	۶	۰,۴۹۱۰	۵، ۸، ۱۶، ۱۸	۳۰۰۰	۶۰۰	
۰,۹۹۹۵	۵، ۶، ۱۴، ۱۶، ۲۱، ۳۰	۰,۳۵۵۰	۶	۰,۹۱۸۵	۷	۹۰۰۰		۲۹
۰,۹۹۹۰	۷، ۱۱، ۲۱	۰,۰۱۵۰	۱۲، ۲۲، ۳۰	۰۴۷۷۰	۲، ۵، ۱۴، ۱۷	۱۰۰۰		
۰,۹۹۹۵	۱۵، ۱۶، ۱۸، ۲۱	۰,۰۳۲۵	۶	۰۹۱۲۰	۱۴، ۲	۳۰۰۰	۲۱۰	
۰,۹۹۹۸	۲۲، ۱۶	۰,۰۷۴۰	۱۶، ۵	۰,۹۹۳۵	۷	۹۰۰۰		
۰,۹۹۸۵	۲، ۵، ۶، ۷، ۱۲، ۱۴، ۱۶، ۱۷، ۲۲، ۳۰	۰,۲۸۳۵	۱۲، ۲۲، ۳۰	۰,۷۱۷۵	۴، ۵، ۶، ۷، ۹، ۱۰، ۱۱، ۱۲، ۱۶، ۱۷، ۱۹، ۲۰، ۲۱، ۲۲، ۲۵، ۲۷، ۲۹، ۳۰	۱۰۰۰		
۰,۹۹۹۰	۴، ۶، ۱۳، ۱۹، ۲۲، ۲۷، ۲۹	۰,۴۰۷۵	۶	۰,۹۷۵۵	۱۶، ۵	۳۰۰۰	۶۰۰	
۰,۹۹۹۵	۲، ۷، ۹، ۱۰، ۱۳، ۱۴، ۱۵، ۲۲، ۲۵، ۲۶، ۲۹	۰,۵۶۰۰	۶	۰,۹۹۵۰	۷، ۵	۹۰۰۰		۱۱
۰,۹۹۵۰	۵، ۶، ۷، ۱۱، ۱۲، ۱۳، ۱۵، ۱۶، ۳۰	۰۴۰۱۰	۲۱، ۱۱	۰,۹۷۱۰	۲، ۵، ۱۴، ۱۶	۱۰۰۰		
۰,۹۹۹۰	۱، ۲، ۳، ۱۱، ۱۳، ۱۴، ۱۶، ۱۷، ۲۱، ۲۲، ۲۶، ۲۷	۰,۵۵۰۵	۶	۰,۹۹۹۰	۷، ۵	۳۰۰۰	۲۱۰	
۰,۹۹۹۵	۱، ۱۰، ۱۳، ۱۴	۰,۶۸۹۰	۶	۰,۹۹۹۵	۸، ۶، ۳	۹۰۰۰		

در این جدول در کل ۱۸ حالت مختلف، برای میزان درگیری‌های $m=0.2,1,3$، سه جریان متفاوت $(d=44,29,11)$، سه بودجه تدافعی $(b=1000,3000,9000)$ و دو بودجه تهاجمی $(B=210,600)$ وجود دارد. برای این مثال پارامترهای مورد نیاز برای PSDA به صورت $SAMPEL=500$، $U=10$ و $S=71$ در نظر گرفته شده است.

تجزیه و تحلیل نتایج به‌دست‌آمده (جدول ۴) برای این شبکه بزرگ‌تر مانند مثال پیشین است. خط‌مشی دفاعی بهینه برای $m=1$، زمانی که بودجه تدافعی کم‌ترین $(b=1000)$ و بودجه تهاجمی بیش‌ترین $B=600$ مقدار است، فقط از ۱۲ یال حفاظت می‌شود با این امید که این یال‌ها افزونگی لازم برای فرستادن جریان مورد نیاز را فراهم کنند. هم‌چنان که بودجه تدافعی افزایش می‌یابد یا بودجه تهاجمی کاهش می‌یابد، یال‌های بیش‌تر می‌توانند برای فراهم‌نمودن افزونگی اضافه شوند و پایداری شبکه را افزایش دهند. به طور مشابه، وقتی تقاضا نیازمند یال‌های بیش‌تری است تا جریان مورد نیاز شبکه $d=40$ را تأمین کند. خط‌مشی دفاعی منابعش را به طور مساوی در میان یال‌های با اهمیت بیش‌تر توزیع می‌دهد.



شکل (۳): شبکه دای و پو

۴- نتیجه‌گیری و تحقیقات آینده

این مقاله قالب تدافعی از شبکه را نشان می‌دهد که مهاجم تلاش می‌کند جریان عرضه- تقاضا را با اختصاص منابع تخریبی به طور مساوی در میان یال‌های ظرفیت‌دار شبکه کاهش دهد. تحت این تهدید حمله، مدافع منابع‌اش را برای حفاظت از یال‌های شبکه اختصاص می‌دهد به طوری‌که احتمال تامین جریان مورد نیاز شبکه (همان پایداری شبکه) بیشینه شود. قالب بهینه‌سازی براساس آسیب‌پذیری یال‌ها با استفاده از تابع میزان موفقیت مهاجم- مدافع برای هر یال تعیین می‌شود. جواب‌های به دست آمده برای این قالب بر روی شبکه‌های مختلف نشان می‌دهد که موقعی که مدافع با توزیع مساوی منابع تهاجمی روبروست، خط‌مشی دفاعی بایستی براساس انتخاب میان بهبود قابل توجه پایداری یک مسیر عرضه- تقاضا به خصوص (با تخصیص تمام منابع دفاعی به یال‌های این مسیر)، یا توزیع منابع در میان یال‌های گوناگون شبکه برای افزایش مختصر پایداری چندین مسیر و بنابراین ایجاد افزونگی باشد. نتایج به دست آمده هم‌چنین نشان می‌دهد وقتی میزان درگیری افزایش می‌یابد انتخاب نخست سودمندتر است.

اگرچه این مقاله نخستین گام در فهمیدن رفتار خط‌مشی دفاعی می‌باشد، با این‌حال اگر به مدافع اجازه دهیم منابع‌اش را به طور نامساوی تقسیم کند، شاید موجب تخصیص بهتر و در نتیجه پایداری شبکه را در برابر سناریوهای متفاوت حمله‌ای افزایش دهد. هم‌چنین ممکن است مهاجم منابع‌اش را به طور بهینه در میان یال‌ها پخش کند تا بیش‌ترین آسیب را برای هر خط‌مشی دفاعی محتمل برساند. بنابراین، هریک از این موارد در تحقیقات آینده می‌تواند مورد بررسی قرار گیرد.

۵- مراجع

[1] A. W. McMasters and T. M. Mustin, “Optimal interdiction of a supply network,” Nav. Res. Logist. Q., 1970.

[2] R. L. Helmbold, “A countercapacity network interdiction model,” 1971.

[3] M. R. Boyle, “Partial-enumeration for planar network interdiction problems,” 1998.

[4] R. K. Wood, “Deterministic network interdiction,” Math. Comput. Model., 1993.

[5] Y. Dai and K. Poh, “Solving the network interdiction problem with genetic algorithms,” In Proceedings of the fourth Asia-Pacific conference on industrial engineering and management system, Taipei, pp. 18–20, 2002.

[6] J. E. Ramirez-Marquez, C. M. Rocco S, and G. Levitin, “Optimal protection of general source-sink networks via evolutionary techniques,” Reliab. Eng. Syst. Saf., 2009.

[7] G. Levitin and K. Hausken, “False targets vs. redundancy in homogeneous parallel systems,” Reliab. Eng. Syst. Saf., 2009.

[8] G. Levitin and K. Hausken, “Redundancy vs. protection vs. false targets for systems under attack,” IEEE Trans. Reliab., vol. 58, no. 1, pp. 58–68, 2009.

[9] K. J. Cormican, D. P. Morton, and R. K. Wood, “Stochastic Network Interdiction,” Oper. Res., 1998.

[10] B. A. Gebre and J. E. Ramirez-Marquez, “Element substitution algorithm for general two-terminal network reliability analyses,” IIE Trans. (Institute Ind. Eng.), 2007.

[11] J. E. Ramirez-Marquez and B. A. Gebre, “A classification tree based approach for the development of minimal cut and path vectors of a capacitated network,” IEEE Trans. Reliab., 2007.

[12] C. M. Rocco S and J. A. Moreno, “Network reliability assessment using a cellular automata approach,” Reliab. Eng. Syst. Saf., 2002.

[13] C. M. Rocco S and E. Zio, “Solving advanced network reliability problems by means of cellular automata and Monte Carlo sampling,” Reliab. Eng. Syst. Saf., 2005.

[14] L. R. Ford Jr and D. R. Fulkerson, “Flows in networks,” Princeton university press, 2015.

[15] Y. Rabinovich and A. Wigderson, “Techniques for bounding the convergence rate of genetic algorithms,” Random Struct. Algorithms, 1999.

[16] C. M. Rocco S and J. E. Ramirez-Marquez, “Deterministic network interdiction optimization via an evolutionary approach,” Reliab. Eng. Syst. Saf., 2009.

[17] J. E. Ramirez-Marquez, “New approaches for reliability design in multistate systems,” In Handbook of Performability Engineering, Springer, pp. 465–476, 2008.

[18] J. E. Ramirez-Marquez, “Port-of-entry safety via the reliability optimization of container inspection strategy through an evolutionary approach,” Reliab. Eng. Syst. Saf., 2008.

[19] J. L. Cook and J. E. Ramirez-Marquez, “Optimal design of cluster-based ad-hoc networks using probabilistic solution discovery,” Reliab. Eng. Syst. Saf., 2009.

[20] A. Berrones, “Stationary probability density of stochastic search processes in global optimization,” J. Stat. Mech. Theory Exp., 2008.