Journal of Electronical & Cyber Defence
Vol. 9, No. 4, 2022, Serial No. 36

The Presentation of an Active Cyber Defense Model for Application in Cyber Deception Technology

K. Dadashtabar Ahmadi, M. Mahmoudbabouei

*Assistant Professor Malek Ashtar University of Technology, Tehran, Iran

(Received: 22/08/2021, Accepted: 29/10/2021)

ABSTRACT

In recent years, the violation of the privacy of information and communication networks, which are more commonly known as cyber-attacks, has been increasing exponentially. These network breaches range from direct attacks on government infrastructure to populist activism and theft. This trend has increased the social and political awareness of users. The active cyber defense is a mechanism to protect computer devices, networks and digital devices against cyber-attacks and destructive intrusions. The function of active cyber defense is to actively seek to infiltrate or engage with the perpetrators of cyber incidents. The reaction of the defenders has always caused an imbalance between their activities and the attackers. Attackers have always used the network as a platform to strengthen their attacks to increase the intensity of attacks. In this study, we have used the Markov model to model and show the inherent difference in the performance of users and network intruders, with the distinction that the proposed model is different from the automatic patch and Moran trend and is more similar to the voter model. The proposed dynamic system model is based on the field average approximation, which purposefully determines the performance of active cyber defense. The imbalance between defenders and attackers in this proposed model is eliminated and according to the proposed dynamics and network conditions, we have provided a platform for the interaction of defenders and attackers to examine the performance of power functions in different situations. In the simulations, the performance of attackers and defenders is examined and according to the results obtained in the diagrams mentioned in the final part of the article, it is shown how to use the active cyber defense at the right time so that we can use this defensive approach in the right situation .

Keywords: : Active Cyber Defense, Cyber Security, Markov Chain, Cyber Dynamic

* Corresponding Author Email: dadashtabar@mut.ac.ir

نشریه علمی "پدافند الکترونیکی و سایبری"
سال نهم، شماره ۴، زمستان ۱۴۰۰، ص ۱۴۰- ۱۲۵

علمی– پژوهشی

ارائه مدلی برای دفاع سایبری فعال به‌منظور کاربرد در فناوری فریب سایبری

کوروش داداش‌تبار احمدی[1*]، محمد محمودبابویی[2]
۱- استادیار، ۲- کارشناسی ارشد، دانشگاه صنعتی مالک اشتر، تهران، ایران
(دریافت: ۱۴۰۰/۰۵/۳۱، پذیرش: ۱۴۰۰/۰۸/۰۷)

چکیده

در سال‌های اخیر نقض حریم شبکه‌های اطلاعاتی و ارتباطی که بیشتر بانام حملات سایبری شناخته می‌شوند، به‌صورت نمایی در حال افزایش است. این نقض‌های شبکه از حمله مستقیم به زیرساخت‌های دولت گرفته تا هکتیویسم پوپولیستی و سرقت را شامل می‌شود. این روند سبب افزایش آگاهی اجتماعی و سیاسی کاربران گردیده است. دفاع سایبری فعال مکانیزی جهت محافظت از دستگاه‌های کامپیوتری، شبکه و ابزارهای دیجیتال در برابر حملات سایبر و نفوذهای تخریب پذیر است. عملکرد دفاع سایبری فعال بدین‌صورت است که به دنبال نفوذ یا درگیر شدن با عاملان حوادث سایبر به‌صورت فعال خواهد بود. واکنشی عمل نمودن مدافعین همیشه سبب عدم توازن میان فعالیت‌های آن‌ها با مهاجمین بوده است. مهاجمین همیشه از شبکه به‌عنوان بستری جهت تقویت حملات خود بهره گرفته تا سبب افزایش شدت حملات شوند. در این تحقیق از مدل مارکوف برای مدل‌سازی و نمایش تفاوت ذاتی عملکرد کاربران و نفوذ گران شبکه بهره برده‌ایم، با این تفاوت که مدل ارائه‌شده با وصله خودکار و روند موران متفاوت بود و بیشتر به مدل رای دهندگان شباهت داشت. مدل سیستم دینامیکی ارائه‌شده بر اساس تقریب میانگین میدان است، که به‌طور هدفمند کارایی دفاع سایبری فعال را مشخص می‌نماید. عدم توازن بین مدافعین و مهاجمین در این مدل پیشنهادی از بین رفته و با توجه به دینامیک پیشنهادی و شرایط شبکه، بستری برای تعامل مدافعین و مهاجمین فراهم نموده‌ایم تا عملکرد توابع قدرت را در شرایط مختلف بررسی نماییم. در شبیه‌سازی صورت گرفته عملکرد مهاجمین و مدافعین بررسی گردید و با توجه به نتایج به‌دست‌آمده در نمودارهای مورداشاره در بخش پایانی مقاله نحوه استفاده از دفاع سایبری فعال در زمان مناسب نشان داده شد تا بتوانیم در موقعیت مناسب از این رویکرد دفاعی بهره‌گیری نماییم.

کلیدواژه‌ها: دفاع سایبری فعال، امنیت سایبری، زنجیره مارکوف، دینامیک سایبری

۱- مقدمه

امنیت سایبری یکی از مسائل مهم و حیاتی است که شامل تعدادی از فن‌ها و رویکردها برای ایمن‌سازی شبکه، زیرساخت‌های دیجیتالی و همچنین دستگاه‌های وابسته به آن‌ها را در برمی‌گیرد. به دنبال چندین حادثه مهم در سال‌های ۲۰۰۷ تا ۲۰۱۲ اقدام کنندگان بین‌المللی به یکی از جنبه‌های خاص امنیت سایبری توجه کرده‌اند که، دفاع سایبری نام دارد. درنتیجه در پی شدت یافتن این‌گونه حوادث و مطرح نمودن ادعاهایی مربوط به دخالت دولت‌ها و همچنین مطرح‌شدن در سطح سیاست‌های ملی سبب بررسی منافع دیجیتال گردید.

ACD[1] مفهومی است که مبتنی بر استفاده از ابزارهایی است که نه‌تنها حوادث سایبری را در هنگام وقوع شناسایی و متوقف می‌کند، بلکه اقدامات تهاجمی را برای به حداقل رساندن قابلیت‌های مهاجمان انجام می‌دهد. علاوه براین می‌تواند از طریق انواع راه‌حل‌های فنی مانند استقرار طعمه یا هک کردن شبکه مهاجم اقداماتی را جهت خنثی‌سازی فعالیت‌های صورت گرفته انجام دهد.

مفهوم دفاع سایبری فعال کمتر از یک دهه است که در ادبیات ما ظهور پیداکرده است برای مثال، کرم خوب[2](سفید) که برای شناسایی، مبارزه یا از بین بردن کرم بد مورداستفاده قرارگرفته است. بااین‌وجود مطالعات اولیه‌ای که انجام گرفت فقط بر روی مسائل قانونیپپ متمرکز بود [۸- ۱]. از سویی دیگر دفاع سایبری فعال به‌نوعی مورداستفاده قرارگرفته بود (کرم wechia که تلاش کرده بود تا کرم Blaster را از رایانه‌های آلوده بیرون کند [۴ و ۹])، و این‌گونه به نظر می‌آمد که دفاع سایبری فعال در آینده نزدیک اجتناب‌ناپذیر خواهد بود و باید به این سمت حرکت کرد [۶، ۱۰ و ۱۱]. بنابراین باید به‌طور سامانمند[3] کارایی دفاع سایبری فعال را مشخص کنیم.

۲- روش تحقیق

ما کارهای قبلی مرتبط را بر اساس دو منظر طبقه‌بندی می‌کنیم:

۱. مشکل عدم توازن بین مدافعین و مهاجمین
۲. رویکردهای به‌کار رفته جهت حل مشکل

*رایانامه نویسنده مسئول: dadashtabar@mut.ac.ir

[1] Active Cyber Defense
[2] White Worm
[3] Systematically

ناشر: دانشگاه جامع امام حسین (ع)

از منظر مشکل موردبررسی توجه داشته باشیم که همه مطالعات موجود در ریاضی در این تحقیق مدنظر ما هست. توصیف نتیجه دفاع واکنشی تحت شرایط مختلف پارامتری (برای مثال [۲۳- ۱۲]) بدین‌صورت هست. این مطالعات به‌طور اساسی کارهای پیشگامانِ را تعمیم می‌دهد [۲۴ و ۲۵] ، که مبتنی بر مدل‌های همه‌گیر همگن [1] در دستگاه‌های بیولوژیکی بود [۲۸- ۲۶]. برای مثال حتی برای کارهای اخیر [۲۱]، که دینامیک حمله - دفاع [2] بین یک مدافع و چند مهاجم که علیه یکدیگر می‌جنگند را نیز مورد مطالعه قرار می‌دهد، دفاع هنوز واکنشی است. در مقابل، تحقیق حاضر یک مشکل جدید را معرفی می‌کند، یعنی توصیف نتیجه دفاع فعال [3] در شرایط مختلف مدل پارامتر (که شامل گراف [4] و ساختار شبکه) بررسی می‌شود.

۳- کارهای مرتبط

سال‌هاست که بحث فنی پدافند سایبری فعال مطرح شده است [۸- ۱] با این وجود کمتر به مدل ریاضیاتی دفاع سایبری فعال توجه شده است، البته دفاع فعال ما را به یاد مدل رای دهندگان [5] می‌اندازد، (برای مثال می‌توان [۳۳- ۲۹] را نام برد)، که به‌موجب آن هر گره می‌تواند در هر مرحله از زمان وضعیت یکی از همسایگان خود را به‌طور تصادفی تصرف کند. بااین‌وجود، مدل رای‌دهنده موجود در مدل دفاع سایبری فعال ما با توابع رزمی [6] خطی قدرت مطابقت دارد (مفهوم تابع رزمی بعداً معرفی خواهد شد).

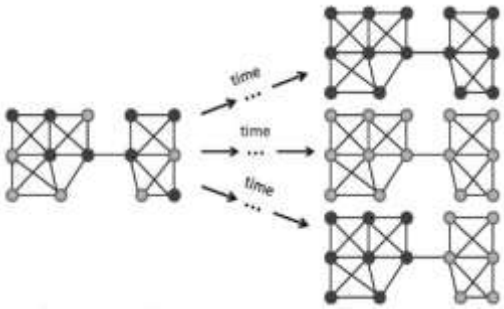
در مقابل، ما توابع رزمی غیرخطی عمومی را مطالعه می‌کنیم، که توضیح می‌دهد که چرا فنون تجزیه‌وتحلیل الگوی رای دهندگان نمی‌تواند با مدل دفاع اینترنتی فعال ما مقابله کند. سرانجام، گفتنی است دفاع سایبری فعال با پچ [7] خودکار متفاوت است [۳۴]، زیرا ممکن است مهاجم بسیاری از رایانه‌ها را به خطر بیاندازد و اینکه مدل دفاع سایبری فعال ما با روند موران [8] متفاوت است [۳۵ و ۳۶]، که پویایی جهش گره‌های همگن را در نظر می‌گیرد. از منظر فن‌هایی که برای مقابله با مشکل اپیدمی با ساختار شبکه بهره‌برداری می‌شود [۲۳- ۱۳]، عمدتاً دو رویکرد وجود دارد. اولین رویکرد استفاده از تقریب میانگین میدان [9] است (برای مثال [۲۸]). مدل سیستم دینامیکی ما نیز بر اساس تقریب میانگین میدانی مدل فرآیند تصادفی اختصاصی [10] است. تقریب میانگین میدان اولین قدم قابل‌قبول برای مطالعه مشکلاتی نظیر فرآیند دفاع فعال برای مدافع سایبری در تحقیق حاضر است. رویکرد دوم مقابله مستقیم با فرآیندهای اختصاصی است که در ساختار شبکه اتفاق می‌افتد. این روش سختگیرانِ تر از رویکرد تقریبی میانگین میدان است، اما غالباً پس از برقراری تفاهم مبتنی بر رویکرد میانگین میدانی دنبال می‌شود [۳۷]. به‌عنوان مثال، رفتار آستانه و نتیجه نهایی SIR [11] فرآیند اپیدمی در شبکه‌های تصادفی با خوشه‌ها (اجتماعات) که در آن بررسی می‌شوند [۱۹ و ۲۰]، در نظر بگیرید، روند اپیدمی SIR در دو مرحله: بیماری همه‌گیر SIR در خوشه‌ها گسترش می‌یابد (گسترش محلی) و سپس اپیدمی SIR در خوشه‌ها پخش می‌شود. برای آن مطالعات، استفاده از تخمین فرآیند شاخه‌ها امری منطقی است، زیرا لازم است فقط در مورد عفونت‌های اولیه کوچک توجه شود (به‌عنوان مثال، مرحله اولیه شیوع بیماری همه‌گیر) و ازآنجاکه مفهوم نسل، زادوولد در مدل SIR به‌خوبی تعریف‌شده است. نویسندگان یک قضیه دشوار حد مرکزی را تحت شرایط خاص به‌دست می‌آورند [۱۵]. در یک تحقیق دیگر، SIS [12] را بررسی می‌کند روند تماس [۳۸] در نمودارهای تصادفی که از طریق پیوست ترجیحی ایجاد می‌شوند [۳۹]. این مطالعه دقیق نتیجه آستانه را تائید می‌کند [۳۷] که از تقریب میانگین میدان به‌دست‌آمده، یعنی آستانه همه‌گیری شبکه‌ها بدون مقیاس صفر است. در [۱۸] نویسندگان هر دو مدل SIR و SIS را در نمودارهای تصادفی با قانون توزیع درجه قدرت را مطالعه نمودند. بهبود برخی از نتایج در [۱۸ و ۲۲] و [۲۳] نشان داده‌شده است که زمان انقراض همه‌گیری برای فرآیند تماس در گراف‌های تصادفی قانون - قدرت به‌صورت نمایی در تعداد گره‌ها رشد می‌کند، و در [۲۲]، حدهای به‌دست‌آمده در تراکم گره‌های آلوده به دست می‌آیند.

۳-۱- مدل دفاع سایبری فعال

سیستم سایبری موردمطالعه متشکل از کامپیوترهای شبکه‌ای / گره‌های جمعیت محدود است . یک کامپیوتر دو حالت دارد : به خطر افتاده یا در امنیت به سر می‌برد (برای مثال آسیب‌دیده اما امن نیست). ممکن است بگوییم که یک کامپیوتر درخطر افتاده توسط یک مهاجم اشغال‌شده است، و یک کامپیوتر امن توسط مدافع (اشغال‌شده) است. دشمن می‌تواند با بهره‌برداری از آن، کامپیوتر دیگری را نیز به خطر بیاندازد (به‌عنوان‌مثال Zero-Day یا Unpatched). حملات شبیه به بدافزار [13] هستند، به این معنی

[1] Homogeneous
[2] Attack-Defense
[3] Active Defense
[4] Graph
[5] Voter Model
[6] Combat Power
[7] Patch
[8] Moran Process
[9] Mean-Field Approximation
[10] Native
[11] Susceptible-infectious-removed
[12] Susceptible-infectious-susceptible
[13] Malware

که رایانه‌های به خطر افتاده می‌توانند به شیوه‌ای همه‌گیر و رایج به رایانه‌های آسیب‌پذیر حمله کنند. با دفاع سایبری فعال، مدافع می‌تواند مکانیزم‌های شبیه به (کرم[1] خوب) را در شبکه‌ها پخش کند (همان‌طور که کرم‌های مخرب گسترش می‌یابند) شناسایی و (پاک‌سازی) رایانه‌های به خطر افتاده را انجام دهد. تعامل بین حمله سایبری و دفاع سایبری فعال یک ساختار متقابل حمله و دفاعی را ایجاد می‌کند، یک توپولوژی گراف را نشان می‌دهد که چگونه گره‌های به خطر افتاده را به گره‌های امن و چگونگی استفاده از گره های ایمن در دفاع سایبری فعال برای تمیز کردن گره‌های به خطر افتاده را به نمایش می‌گذارد. ما می‌گوییم که یک مدافع (مهاجم) در صورتی استراتژیک است که در ابتدا گره‌های درجه بزرگ گراف با احتمالات بالاتر را اشغال کند. تعامل حمله- دفاع منجر به تکامل وضعیت امنیت سایبری کل سیستم سایبر می‌شود. ما نشان می‌دهیم که

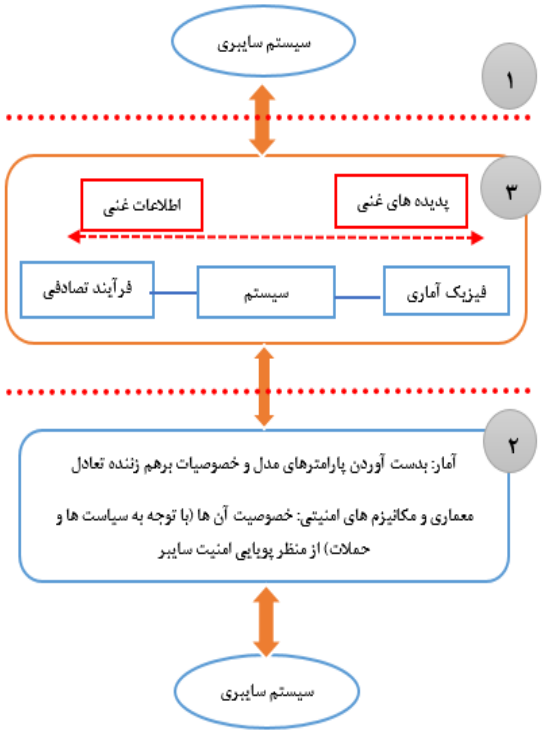


شکل(۱): سه حالت موجود در شبکه پیشنهادی

تکامل حالت در شکل (۱)، جایی که یک دایره توپر (مشکی) به معنای (امن) و یک دایره توخالی (خاکستری) به معنای (در معرض خطر) است. همان‌طور که در شکل ۱ نشان داده‌شده است، تکامل حالت می‌تواند پدیده‌های غنی را به نمایش بگذارد(برای مثال وجود انواع مختلف تعادل). در سطح بالا، هدف این پژوهش شناسایی این مسئله است که چگونه این تکامل توسط وضعیت اولیه، توپولوژی گراف، مؤلفه‌ها، و استراتژی‌های مهاجم / مدافع اداره می‌شود. ویژگی‌های موجود این امکان را به ما می دهد تا به برخی از سؤالات اساسی پاسخ دهیم، ازجمله اینکه در چه شرایطی وضعیت امنیت سایبر به سمت تعادل کاملاً امن حرکت خواهد کرد [۱۳،۱۴،۱۶،۱۷،۲۱].

۳-۲- مدل اختصاصی فرآیند مارکوف

زنجیره‌های مارکوف، از پراستفاده‌ترین فنون احتمالاتی درزمینه کشف نفوذ می‌باشند چراکه برحسب نرخ نفوذ و نرخ هشدارهای غلط، عملکردی بهتری را از خود نشان می‌دهند [۱]. دنیل فاوا در [۲۱] از مدل‌های مارکوف برای مدل‌سازی ترتیبی تجسم حملات استفاده نموده است. او با استفاده از یک درخت پسوندی، مدل‌های مارکوفی با مرتبه مختلف را پیاده‌سازی کرده و سپس در یک مدل مارکوف با طول متغییر تلفیق نمود. فاوا از یک مدل مارکوف با طول متغییر که شامل چندین رد حمله مشاهده‌شده است، رفتار و مراحل آتی حملات احتمالی را استنتاج می‌نماید [۱]. به‌طور کلی می‌توان گفت ما در حال بررسی حوزه جدید دینامیک امنیت سایبری هستیم، که پایه و اساس علم امنیت سایبری است. دینامیک امنیت سایبری اغلب چهارچوبی را ارائه می‌دهد که می‌تواند توصیف، تجویز و پیشگویی را در خود جای دهد و می‌تواند با استفاده از روش‌های مختلف ریاضی موردمطالعه قرار گیرد. برای مثال ما می‌توانیم پدیده‌های امنیت سایبری ارائه‌شده توسط دینامیک را مشخص کنیم و عوامل یا قوانین حاکم بر تکامل را مشخص کنیم. این مسئله عجیب نیست که دینامیک امنیت سایبری الهام گرفته از مدل‌های همه‌گیر دستگاه‌های زیستی باشد، چراکه محققان در تلاش برای طراحی و ساخت دستگاه‌های کامپیوتری هستند که می‌توانند ویژگی‌های ظریف دستگاه‌های زیستی (به‌ویژه بدن) را از طریق مفاهیمی مانند سیستم ایمنی مصنوعی تقلید کنند. این مفاهیم الهام گرفته شده از سامانه‌های تعاملی است، و توسط پایه مالی خرد در اقتصاد(یعنی پارامترهای اقتصاد کلان به‌طور ایدئال از برخی مدل‌های خرد اقتصاد استخراج می‌شوند) بیان می‌شود. در شکل زیر می‌توان نمایی کلی از دینامیک را مشاهده کنیم.



شکل (۲). دینامیک پیشنهادی کلی سیستم

[1] Worm

در ابتدا به بیان نمادها و علائم پرداخته می‌شود:

جدول(۱): علائم و فرمول‌ها

عنوان	علامت اختصاری
گراف/شبکه که چکیده سیستم سایبر است	$G = (v, E)$
	N_v
تعداد یال یک گره	$\deg(v)$
قدرت توان نمایی	γ
شاخص توان تابع مبارزاتی در دینامیک نوع اول و دوم	σ, τ
حالت یک گره در زمان t	$\xi_v(t)$
احتمال امن بودن یک گره در زمان t	$B_v(t)$
احتمال به خطر افتادن یک گره در زمان t	$R_v(t)$
متوسط تعداد میانگین گره‌های امن در زمان t	α ، $\alpha = \frac{1}{n}\sum_{v\epsilon V} B_v(0)$ ، به‌طور
حالت رندم گره‌های امن در زمان t=0	s
احتمال تغییر حالت گره امن به حالت به خطر افتاده در زمان t	θ_{vBR} (t)
احتمال تغییر حالت گره به خطر افتاده به حالت امن در زمان t	θ_{vRB} (t)

به‌طور کلی حمله/دفاع سایبری روی یک ساختار شبکه / گراف محدود صورت می‌گیرد. $G = (v, E)$، که $V = \{1,2, \dots, n\}$ حالت گره‌ها/ کامپیوترها و E شامل تنظیمات یال‌ها/قوس‌ها (u, v) زیرمجموعه E نمی‌باشند (برای مثال self-loop در این مسئله وجود ندارد). یک نقطه در هر زمان، $v\epsilon V$ دارای دو حالت هست : امن، بدین معنی است که (به‌عنوان‌مثال آسیب‌پذیر [1] اما به‌وسیله مهاجم در معرض خطر [2] نیست یا در حال حاضر به خطر نیفتاده است) یا در معرض خطر به این معنی است که توسط مهاجم به خطر افتاده است. گره‌ها حالت‌هایشان تغییر خواهد کرد و این مطلب اشاره به این موضوع دارد که یک گره امن دوباره به امن ساختن خود نمی‌پردازد و یک گره آسیب‌دیده دوباره برای در معرض خطر دادن خود اقدامی انجام نخواهد داد. ازآنجاکه مطالعه ما برای گراف‌های جهت‌دار و بدون جهت صورت می‌گیرد، ما تمرکز خود را بر روی گراف های بدون جهت می‌گذاریم. ما هیچ محدودیت قابل‌توجهی در G ایجاد نمی‌کنیم، چون در زندگی واقعی، G می‌تواند هر ساختاری داشته باشد. این به یک روش استاندارد در مطالعات توصیفی امنیت سایبری تبدیل‌شده است (برای مثال می‌توان به [۱۳،۱۴،۱۶،۱۷،۲۱] اشاره نمود). ساختار مدلسازی دینامیک ریاضی حاصله که نشان دهنده تعامل میان مدافعین و مهاجمین در ساختار شبکه گرافی بوده است بر اساس تئوری‌های بیان شده در [۳،۵] می‌باشد.

حالت گره $v\epsilon V$ به‌صورت تصادفی، متغیر است $\xi_v(t)\epsilon\{0,1\}$:

$$\xi_v(t) = \begin{cases} 1 & v \in V \text{ در زمان t امن است} \\ 0 & v \in V \text{ در زمان t در معرض خطر است} \end{cases} \quad (۱)$$

به همین ترتیب، ما تعریف می‌کنیم

$$B_v(t) = P\big(\xi_v(t)\big) = 1$$
$$R_v(t) = P\left(\xi_v(t)\right) = 0 \quad (۲)$$

همان‌طور که نشان داده می‌شود به‌وسیله $\tilde{\theta}_{v,BR}$ (t) نرخ [3] تغییر حالت v از حالت امن به حالت در معرض خطر متغییر هست که این مسئله نسبت به همسایگانش تنظیم می‌شود. شبیه همین مطلب نیز برای $\tilde{\theta}_{v,RB}(t)$ برقرار است، نرخ تغییر حالت گره به خطر افتاده به حالت امن به‌صورت تصادفی تعیین می‌شود. تغییر حالت $v\epsilon V$ به‌طور طبیعی به‌عنوان‌مثال فرآیند مارکوف توصیف می‌شود (که مکمل [4] مارکوف هست یا خود مارکوف هست) برای اهداف مرجع با احتمالات انتقال زیر:

$$P\left(\xi_v(t+\Delta t) = 1 \middle| \xi_v(t)\right) = \begin{cases} \Delta t.\tilde{\theta}_{v,RB}(t) + o(\Delta t) & \xi_v(t) = 0 \\ 1 - \Delta t.\tilde{\theta}_{v,BR}(t) + o(\Delta t) & \xi_v(t) = 1 \end{cases}$$
$$P\left(\xi_v(t+\Delta t) = 0 \middle| \xi_v(t)\right) = \begin{cases} \Delta t.\tilde{\theta}_{v,BR}(t) + o(\Delta t) & \xi_v(t) = 1 \\ 1 - \Delta t.\tilde{\theta}_{v,RB}(t) + o(\Delta t) & \xi_v(t) = 0 \end{cases} \quad (۳)$$

[1] Vulnerable
[2] Compromised
[3] Rate
[4] dubbed

همان‌طور که گفتیم $\Delta t \to 0$. نشان داده می‌شود که به‌وسیله $N_v\{u\epsilon V:(u,v)\epsilon E\}$ مجموعه همسایه‌های گره $v\epsilon V$. ازآنجاکه نرخ $\tilde{\theta}_{v,RB}(t)$ و $\tilde{\theta}_{v,BR}$ (t) به‌طور طبیعی توسط حالات تصادفی همسایه‌ی گره مشخص می‌شوند، ما از توابع تعیین‌کننده و احتمالاً غیرخطی استفاده می‌کنیم $f_{RB}(.): R \to [0,1]$ و $f_{BR}(.): R \to [0,1]$ که به ترتیب نرخ رندم را به‌صورت $\tilde{\theta}_{v,RB}(t)$ و $\tilde{\theta}_{v,BR}$ (t) تعریف می‌کنیم و در زیر بدین‌صورت نشان می‌دهیم:

$$\tilde{\theta}_{v,RB}(t) = f_{RB}\left(\frac{1}{\deg(v)}\sum_{u\epsilon N_v}\xi_v(t)\right) \qquad (۴)$$

$f_{BR}(.)$ و $f_{RB}(.)$، به‌عنوان تابع مبارزه در نظر گرفته می‌شود، زیرا این توابع خلاصه توانایی قدرت مبارزه را دارا می‌باشند. می‌توان توجه داشت که نتایج فوق یادآور مدل موسوم به رای دهندگان است [۲۹]، که در آن یک گره (حالت) خود را با توجه به همسایه تصادفی موجود و با بهره‌گیری از فرآیند پواسون[1] که دارای نرخ ثابت تغییر هست، تغییرات را انجام دهد. این کار به این مدل اجازه می‌دهد تا به یک فرآیند دوگانه[2] تبدیل شود که در زمان به عقب کار کند و به یک گام تصادفی تبدیل شود، که باعث قابل‌کنترل شدن آن می‌شود [۲۹]. متقابلاً در این مدل، حالت یک گره خود را مطابق با نرخی که ثابت نیست تغییر می‌دهد، اما در عوض به‌صورت غیرخطی به حالات همسایگان بستگی دارد. این غیرخطی بودن مانع از تبدیل‌شدن مدل فرآیند مارکوف اختصاصی به یک ولگشت[3] تبدیل می‌شود، و به معنی این است که فن مورداستفاده در مطالعات قبلی جواب گوی ما نخواهد بود. این مشکل ناشی از غیرخطی بودن هست بنابراین باید مدل فرآیند مارکوف اختصاصی را به‌عنوان مثال مدل سیستم دینامیکی قابل تجزیه و تحلیل ساده کنیم.

۳-۳- تنظیم مدل سیستم پویا از طریق توابع ویژه مبارزه خاص

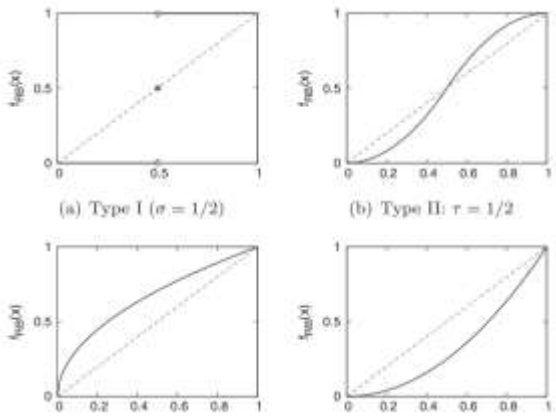
به یاد بیاورید که عملکرد توابع ویژه مبارزه $f_{RB}(.)$ ، هست و خلاصه قدرت مدافعین علیه مهاجمین نیز هست. باید خواص مورد انتظار را برآورده سازیم :

$f_{RB}(0) = 0$ (۱)

$f_{RB}(1) = 1$ (۲)

$f_{RB}(.)$ به‌صورت یکنواخت افزایش می‌یابد. (۳)

همانطور که در شکل نمایان است، بیشتر گره‌های امن در اطراف گره‌های به خطر افتاده هستند، این مسئله شانس بزرگی برای گره‌های آسیب‌دیده است چراکه دفاع فعال توسط مدافعین راه‌اندازی می‌شود. در این تحقیق ما چهار نوع تابع مبارزه داریم، به‌عنوان‌مثال ما در شکل زیر دو تابع مبارزه دارای آستانه را شاهد هستیم و دو شکل دیگر بدون آستانه می‌باشند.



شکل (۳): نمودار چهار نوع دینامیک پیشنهادی

نوع یک (a) دارای حد آستانه $\epsilon\sigma(0,1)$ و تعریف می‌شود:

$$\theta_{vRB}\,(\mathrm{t}) = f_{RB}\left(\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t)\right)$$

$$= \begin{cases} 1 & \frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t) > \sigma \\ 0 & \frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t) < \sigma \\ \frac{1}{2} & otherwise \end{cases} \qquad (۵)$$

به‌صورت شهودی، مدافع از مهاجم قوی‌تر است زمانی $\sigma < \frac{1}{2}$، و قدرتشان کمتر از مهاجم می‌شود زمانی که $\sigma > \frac{1}{2}$ ، و برابری قدرت زمانی با مهاجمان رخ می‌دهد که $\sigma = \frac{1}{2}$.

نوع دوم (b) دینامیک دارای آستانه $\tau\epsilon(0,1)$ ، ما تعریف می‌کنیم $f_{RB}(x)$ محدب و $f_{RB}(x) < x$ برای $x\epsilon[0,\tau)$ ، $f_{RB}(x)$ مقعر و $f_{RB}(x) > x$ برای $x\epsilon(\tau,1]$ ، $x = \tau$ برای $f_{RB}(x) = 0$ و $f_{RB}(x) = 1$. علاوه به راین، $f_{RB}(.)$ در فواصل $[0,\tau)$ و $(\tau,1]$در حال افزایش و پیوسته هستند. این‌گونه توابع سیگموید[4] نامیده می‌شوند. به‌طور شهودی مدافع قدرتش بیشتر است وقتی‌که $\tau < \frac{1}{2}$ و قدرتشان کمتر از مدافع است وقتی‌که $\tau > \frac{1}{2}$ ، و برابری قدرت زمانی با مدافع اتفاق می‌افتد که $\tau = \frac{1}{2}$. نوع سوم (c) دینامیک تابع مبارزه به‌صورت مقعر است و شامل افزایش در بازه $[0,1]$ ، $f_{RB}(x) > x$ برای$s\epsilon(0,1)$ و $f_{RB}(x) = 0$ و $f_{RB}(x) = 1$. به‌صورت شهودی مدافع پیش رفته‌تر از مهاجم است. (برای مثال مدافع دارد از برتری تابع مبارزه استفاده می‌کند). نوع چهارم (d) تابع مبارزه به شکل محدب است. و

[1] Poisson Process
[2] dual
[3] Random walk
[4] sigmoid

افـزایش دارد در بـازه $[0,1]$ ، $f_{RB}(x) < x$ بـرای $x\epsilon(0,1)$ و $f_{RB}(x) = 0$ ، $f_{RB}(x) = 1$. به‌صورت شهودی، مدافع نسبت بـه مهاجم پیش رفته‌تر نیست. توجه کنید که تابع نوع چهار دوگـان تابع نوع سوم است. اساس چهار نوع تابع مبارزه بالا را ما با تمرکز بر این موضوع باهم ترکیب می‌کنیم.

$$\theta_{vBR}(\mathrm{t}) = 1 - \theta_{vRB}(\mathrm{t}) \quad (۶)$$

با ترکیب معادله دینامیکی کلی و فرمول بالا، به بهینه شدن فرمول کلی دینامیکی برای یک نقطه می‌رسیم که بدین شرح است :

$$\frac{d}{dt}B_v(t) = \theta_{vRB}(\mathrm{t})\big(1 - B_v(t)\big) - \theta_{vBR}(\mathrm{t}).B_v(t) = \theta_{vBR}(\mathrm{t}) - B_v(t)$$

وظیفه اصلی ما توصیف این چهار نوع مدل دینامیکی هست، یعنی پویایی این چهار نوع تابع مبارزه را نشان دهد.

برای مثال ما برای تابع نوع یک داریم :

$$\theta_{vBR}(\mathrm{t}) = f_{BR}\left(\frac{1}{\deg(v)}\sum_{u\epsilon N_v}[1 - B_u(t)]\right) = \begin{cases} 1 & \frac{1}{\deg(v)}\sum_{u\epsilon N_v}[1 - B_u(t)] > 1 - \sigma \\ 0 & \frac{1}{\deg(v)}\sum_{u\epsilon N_v}[1 - B_u(t)] < 1 - \sigma \\ \frac{1}{2} & otherwise \end{cases} \quad (۷)$$

مـا مـی‌خـواهیم، در بـین مـوارد دیگـر، نقـش‌هـای آسـتانه مشخص شده در دینامیک های نوع ۱ و نوع دوم را مشخص کنیم، و نتایج ناشی از عدم وجود چنین آستانه‌هایی را در دینامیک انواع ۳ و ۴ را نشان دهیم.

۳-۴- شبکه گرافی پیشنهادی

ما برای شبیه‌سازی از دو شبکه گرافی ER و Power Law استفاده می‌کنیم. در شبکه ER ما توجهی به ساختار و توانایی ساختار شبکه نداریم و نتایج مستقل از نتایج احتمالاتی شبکه هست. در شبکه Power Law ما به توصیف منافع برای مدافع استراتژیک که در ابتدا گره‌های بزرگ با احتمالات بیشتر را اشغال می‌کند می‌پردازیم. به‌طور خاص پدیده ویژه مربوط به حداقل گسترش گره در خوشه‌ی گراف ER و احتمال بهینه پیوند میان گره‌ها در گراف Power Law به ترتیب به شرح زیر است:

$$\beta_k = inf\,\frac{|N_v \cap V_k|}{\deg(v)}\,, where\ N_v\{u\epsilon V : (u,v)\epsilon E\}$$
$$P_{vu}(n) = \frac{d_u(n)d_v(n)}{\sum_{k=1}^{n} d_k(n)} \quad (۸)$$

مستقل از مطالعات قبلی، جایی که $0 \le P \le 1$ به فرض $((d_{max}(n))^2 \le \sum_{k=1}^{n} d_k(n))$ [۴۰].

۳-۵- مشخصه‌های نوع اول دینامیک دفاع سـایبری فعال

در ایـن بخـش مـا ابتـدا دفـاع سـایبری فعـال را بـا مـدافع غیراستراتژیک در شبکه‌های دلخواه[1] عنوان می‌کنیم، که در ابتـدا با احتمال یکسان برای همه گره‌ها اشغال را انجـام مـی‌دهـد. مـا سپس بررسی می‌کنیم بیشتر موارد دشوار برای مدافع استراتژیک با درجه مسـتقل $B_v(0) \propto \deg(v)$ را مـدل تعمـیم‌یافتـه گـراف تصادفی که مدافع در ابتـدا بـه اشـغال گـره‌هـای بـا درجـه بـالا می‌پـردازد. (بـرای مثـال گـره‌هـای بـا درجـه بـالا کـه احتمـال حفاظتشان بهتر است).

۳-۵-۱- مشخصـه‌هـای نـوع اول دینامیـک بـا مـدافع غیراستراتژیک

دینامیک نوع اول برای مدافع غیراستراتژیک این مطالب را عنوان می‌کند که آیا دفاع سایبری فعال می‌تواند به‌صورت خودکار به پاک‌سازی شبکه داخلی بپردازد و همین‌طور روش‌های تصمیم‌گیری برای رسیدن به تعادل که ما نیاز داریم را نشان می‌دهد.

اصل کلی حاکم برای این نوع دینامیک، ما دارای یک شبکه خودسرانه‌ای هستیم که دارای حد آستانه معین و با توجه به معادله در شبکه گرافی داریم :

$$\frac{d}{dt}B_v(t) = \theta_{vRB}(\mathrm{t})\big(1 - B_v(t)\big) - \theta_{vBR}(\mathrm{t}).B_v(t) = \theta_{vBR}(\mathrm{t}) - B_v(t) \quad (۹)$$

اگر $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(0) > \sigma$ آن‌وقت برای گره‌های عضو شبکه ما داریم که، $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t) > \sigma$ که برای گره‌های عضو شبکه این نامساوی برقرار هست و گره‌های کوچک عضو شبکه که در اختیار مدافعین می‌باشند رفتار یکنواخت افزایشی را ادامه خواهند داد. اگر $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(0) < \sigma$ آن‌وقت برای گره‌های عضو شبکه ما داریم که، $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t) < \sigma$ که برای گره‌های عضو شبکه این نامساوی برقرار هست و گره‌های بزرگ عضو شبکه که در اختیار مدافعین هست رفتار یکنواخت کاهشی را از خود نشان خواهند داد.

[1] Arbitrary networks

۳-۵-۲- شرایط کافی برای آنکه مدافعین (مهاجمین) بتوانند شبکه را تحت اشغال خود دربیاورند

در این نوع از دینامیک که ما دارای یک شبکه خودسرانه با حد آستانه معین در شبکه گرافی هستیم اگر $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(0) > \sigma$ برای همه گره‌های عضو شبکه $\lim_{t\to\infty} B_v(t) = 1$. اگر $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(0) < \sigma$ برای همه گره‌های عضو شبکه $\lim_{t\to\infty} B_v(t) = 0$.

اثبات:

$$\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t) > \sigma \ \rightarrow \mathrm{t} \geq 0, \mathrm{v}\epsilon\mathrm{V}.$$

$$\theta_{vRB}(\mathrm{t}) = f_{RB}\left(\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t)\right)$$

$$= \begin{cases} 1 & \frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t) > \sigma \\ 0 & \frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t) < \sigma \\ \frac{1}{2} & otherwise \end{cases} \quad (۱۰)$$

$$\theta_{vRB}(\mathrm{t}) = 1 \rightarrow \mathrm{t} \geq 0, \mathrm{v}\epsilon\mathrm{V}.$$

از سیستم زیر چنین به دست می‌آید که :

$$\frac{d}{dt}B_v(t) = \theta_{vRB}(\mathrm{t})\big(1 - B_v(t)\big) - \theta_{vBR}(\mathrm{t}).B_v(t)$$
$$= \theta_{vBR}(\mathrm{t}) - B_v(t)$$

$$\frac{d}{dt}B_v(t) = \theta_{vRB}(\mathrm{t}) - B_v(t) = 1 - B_v(t).$$

و منجر به مطالب زیر می‌شود:

$$B_v(t) = \exp(-t)\,B_v(0) + 1 - \exp(-t) \text{ و } \lim_{t\to\infty} B_v(t) = 1 \quad (۱۱)$$

۳-۵-۳- شرایط کافی برای آنکه مدافعین (مهاجمین) نتوانند شبکه را تحت اشغال خود دربیاورند

در این دینامیک ما دارای شبکه خودسرانه خوشه‌ای هستیم که دارای حد آستانه معین در گراف تعیین‌شده هست. اگر ما $B_v(0) = \alpha_k$ برای هر گره عضو V_k باشد و β_k حداقل گسترش گره‌ها در فرمول $\beta_k = inf\frac{|N_v \cap V_k|}{\deg(v)}$ باشند. اگر $\alpha_k\beta_k > \sigma$ باشد برای همه گره‌های عضو V_k امنیت برقرار است و اگر $(1-\alpha_k)\beta_k > 1-\sigma$ گره‌های عضو V_k به خطر افتاده اند.

اثبات:

$$\alpha_k\beta_k > \sigma \quad for\ all\ nodes\ in\ V_k$$
$$\rightarrow \frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(0)$$
$$\geq \frac{1}{\deg(v)}\alpha_k.|N_v \cap V_k|$$
$$\geq \alpha_k\beta_k > \sigma.$$

$$\lim_{t\to\infty} B_v(t) = 1$$

$$(1-\alpha_k)\beta_k > 1-\sigma \quad for\ all\ nodes\ V_k$$
$$\rightarrow 1 - \frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(0) \quad (۱۲)$$
$$\geq \frac{\deg(v)}{\deg(v)} - \frac{\alpha_k.|N_v \cap V_k|}{\deg(v)} - \frac{\left|\frac{N_v}{V_k}\right|}{deg(v)}$$
$$= \frac{|N_v \cap V_k|}{\deg(v)}(1-\alpha_k)$$
$$\geq (1-\alpha_k)\beta_k$$
$$> 1-\sigma \quad \lim_{t\to\infty} B_v(t) = 0$$

با توجه به شرایط بیان‌شده برای به دست آوردن شبکه توسط مدافعین و مهاجمین می‌توان چنین استنباط نمود که همیشه شرایط مدنظر ما پیش نخواهد پس اگر حالت امنیت اولیه شبکه شرایط اصلی نوع اول دینامیک ما را برآورده نساخت، و همین‌طور مدافعین و مهاجمین نسبت به هم برتری نداشته باشند می‌توان این مسئله را عنوان نمود که در این شرایط ساختار شبکه نقش بسیار مهمی را برای ما ایفا می‌کند. در شبکه‌های خوشه‌ای دفاع سایبری فعال شاید بتواند به‌طور خودکار خوشه‌ها را پاک‌سازی نماید اما توانایی پاک‌سازی کل شبکه را دارا نیست. ما همیشه دو حالت را عنوان می‌کردیم یا در امنیت بودیم یا در معرض خطر قرار می‌گرفتیم، اما نوع دیگری از تعادل بیان شد که برخی از خوشه‌ها به خطر افتاده و برخی امن هستند. ازآنجایی‌که ثبات تعادل تعریف سطح بالاتری برای ما هست و این دینامیک گنجایش عنوان آن را ندارد، باید به تعادلی با توجه به برخی از روش‌ها و الگوریتم های کلی دست پیدا کنیم تا موضوع ما را حل نماید. قبل از ارائه این قضیه ما بیان می‌کنیم که تعادلی مدنظر ما است که اگر یک همسایگی داشته باشد پایدار است، به‌گونه‌ای که تعداد نقاط در اختیار مهاجمین در هرلحظه از زمان در ابتدا همسایگی واقع‌شده باشد و به تعادل مدنظر ما خواهد رسید. ما تعادلی را تعادل پایدار می‌نامیم که باهمگرایی نمایی اگر برای هرکدام از نقاط در اختیار مهاجمین در هرلحظه از زمان در همسایگی باشد پایداری مثبت ایجاد کند(در حالت امن باشد).

۳-۵-۴- روش و الگویی جهت رسیدن به تعادل پایدار

در الگو بیان‌شده در دینامیک نوع اول با مدافع استراتژیک که در یک شبکه خودسرانه گرافی با حد آستانه معلوم داریم :

$$B^* = [B_v^*]_{v\epsilon V}$$
$$\overline{B^*} = [1 - B_v^*]_{v\epsilon V}$$
$$B_v^* = \begin{cases} 1 & \frac{1}{\deg(v)} \sum_{u\epsilon N_v} B_u^* > \sigma \\ 0 & \frac{1}{\deg(v)} \sum_{u\epsilon N_v} B_u^* < \sigma \end{cases} \quad (۱۳)$$

برای همه گره‌های عضو شبکه برای هر دو B^* و $\overline{B^*}$ معادله تعادلشان به‌صورت تعادل پایدار مجانبی[1] هست که بدین‌صورت همگرایی اتفاق می‌افتد.

اگر $B_v^* = \sigma$ برای تعدادی از گره‌های عضو شبکه B^* و $\overline{B^*}$ ما به سمت ناپایداری می‌رویم. ما در شرایط گذشته بیان کردیم که دارای دو نوع تعادل امن و به خطر افتاده هستیم ولی در این الگوریتم به این مسئله رسیدیم که تعادل به‌صورت نمایی همگرا می‌شود[2].

۳-۵-۵- مشخصه‌های دینامیک نوع اول با مدافع استراتژیک

ما تحقیقاتمان را با مدافع استراتژیک ادامه می‌دهیم، در این نوع دینامیک که ما در ابتدا احتمال امن بودن گره V متناسب با درجه‌اش است. (برای مثال $B_v(0) \propto \deg(v)$) ما این وضعیت را در مدل توسعه‌یافته گراف رندم را در مطالعات خود بررسی نموده‌ایم. این بدان معنی است، که روش‌های پیشنهادی ما لزوماً برای شبکه‌های دلخواه صحیح نیست. ما این محدودیت را با نتایج تحلیلی مناسب پوشش می‌دهیم، که شامل تعیین مزایای ساختار حمله-دفاع [3] در شبکه گراف ER و گراف توان مبارزه است. پایه و اساس این نوع دینامیک، این را بیان می‌کند که تحت شرایطی مطمئناً $\frac{1}{\deg(v)} \sum_{u\epsilon N_v} B_u(t) > \sigma$ رخ می‌دهد. ما به‌طور تقریبی از توزیع نرمال [4] استفاده می‌کنیم، و با نشان دادن اینکه شرایط لیاپانوف[5] در قضیه حد مرکزی [6] و شرایط کولموگروف [7] در قانون قوی اعداد بزرگ [8] نیاز ما را برطرف خواهد نمود.

۳-۵-۶- دفاع سایبری فعال با مدافع استراتژیک

اگر $G(n) = (v(n), E(n))$ مثالی از n گره رندم در گراف توسعه‌یافته باشد بر طبق درجه به‌دست‌آمده از توالی $(d_1(n), \ldots . d_n(n))$ باشد. تعیین احتمال وابستگی درجه نقاط در اختیار مدافعین در لحظه صفر را ما تعیین می‌کنیم که حالت Vها(گره) را بر طبق مستقل بودن نقاط در اختیار مدافعین در لحظه صفر از هر چیز دیگری است، ما تنظیمات گره امن را چنین بیان می‌کنیم:

$$S = \{v: v\epsilon V(n) \wedge B_v(0) = 1\} \quad (۱۴)$$

تابع تعریف‌شده برای امن بودن در لحظه صفر

$$\phi(n) = \frac{\sum_{v\epsilon S} \deg(v)}{\sum_{v\epsilon V(n)} \deg(u)} \quad (۱۵)$$

که در آن درجه $\deg(v)$ ، $V(n)$ در $G(n)$ هست. قرار می‌دهیم:

$$S_{n,v}^2 = \sum_{u\epsilon V(n)} B_u(0)^2 P_{vu}(n)(1 - P_{vu}(n))$$
$$q_{n,v} = \sum_{u\epsilon V(n)} B_u(0)^3 P_{vu}(n)(1 - P_{vu}(n))[(1 - P_{vu}(n)^2 + P_{vu}(n)^2]$$
$$w_{n,v}^2 = \sum_{u\epsilon V(n)} P_{vu}(n)\,(1 - P_{vu}(n)) \quad (۱۶)$$
$$g_{n,v} = \sum_{u\epsilon V(n)} P_{vu}(n)\,(1 - P_{vu}(n))[(1 - P_{vu}(n)^2 + P_{vu}(n)^2]$$

فرض می‌کنیم :

$$\lim_{n\to\infty} sup_{v\epsilon V(n)} q_{n,v}/S_{n,v}^3 = 0.$$
$$\lim_{n\to\infty} sup_{v\epsilon V(n)} g_{n,v}/w_{n,v}^3 = 0.$$
$$\lim_{n\to\infty} \sqrt{\ln(n)}\,/d_{min}(n) = 0.$$
$$\lim_{n\to\infty} (\sum_{v\epsilon V(n)} g_{n,v})/(\sum_{v\epsilon V(n)} {w^2}_{n,v})^{3/2} = 0. \quad (۱۷)$$
$$\lim_{n\to\infty} (\sum_{v\epsilon V(n)} q_{n,v})/(\sum_{v\epsilon V(n)} {S^2}_{n,v})^{3/2} = 0.$$
$$\lim_{n\to\infty} \sum_{v\epsilon V(n)} \frac{1}{d_v^2} = 0.$$

اگر $\lim_{n\to\infty} \phi(n) > \sigma$ تقریباً مطمئن هستیم که $\lim_{n\to\infty} \lim_{t\to\infty} B_v(t) = 1$ برای همه گره‌های عضو شبکه به این اطمینان می‌رسیم که

$$\lim_{n\to\infty} P\left(\lim_{t\to\infty} B_v(t) = 1\right) = 1 \quad (۱۸)$$

[1] Asymptotically stable equilibria
[2] Exponential convergence
[3] Attack-defense
[4] Normal distribution
[5] Lyapunov condition
[6] Central limit theorem
[7] Kolmogorov condition
[8] Strong law numbers

اگر $\overline{\lim_{n\to\infty}\phi(n)<\sigma}$ تقریباً مطمئن هستیم که $\lim_{n\to\infty}\lim_{t\to\infty}B_v(t)=0$ برای همه گره‌های عضو شبکه به این اطمینان می‌رسیم که

$$\lim_{n\to\infty}P\left(\lim_{t\to\infty}R_v(t)=1\right)=1 \qquad (۱۹)$$

با توجه به این شرایط بیان‌شده در گراف رندم توسعه‌یافته (به‌جای شبکه‌های دلخواه) که در دسترس ما است لزوماً متراکم نیستند. برای این مطلب شرط کافی برای این فرض V هست $d_{min}\gg\sqrt{n}$ زیرا

$$\sum_{v\epsilon V(n)}\frac{1}{d_v^2(n)}\leq\frac{n}{d_{min}^2(n)}.$$

شرط لازم برای فرض V هست $n\ll\langle d_v^2(n)\rangle$ جایی که $\langle d_v^2(n)\rangle=\frac{1}{n}\sum_{v\epsilon V(n)}d_v^2(n)$ زیرا

$$\sum_{v\epsilon V(n)}\frac{1}{d_v^2(n)}\geq\frac{n}{\frac{1}{n}\sum_{v\epsilon V(n)}d_v^2(n)}=\frac{n}{d_v^2(n)} \qquad (۲۰)$$

این شرایط نشانگر آن نیست که گراف‌ها متراکم هستند. برای مثال دو شرط هست که راضی‌کننده به‌وسیله $d_v(n)=o(\sqrt{n}\log(n))$ برای همه گره‌هایی که عضو شبکه ما هست این مطلب را نشان می‌دهد که تراکم[1] گراف همگرا به صفر است مانند $n\to\infty$. مطالبی که بیان شد مربوط به مدافع استراتژیک با ارتباط مستقیم میان گره‌های امن با یال های گراف است. ویژگی مشخصه مزیت مدافع استراتژیک و ارتباط مستقیم آن با درجه گره : ازآنجایی‌که $B_v(0)\propto\deg(v)$ ما داریم:

$$B_v(0)=C_1\frac{\deg(v)}{\sum_{v\epsilon V(n)}\deg(u)} \qquad (۲۱)$$

برای تعدادی از ثابت‌ها $C_1>0$. سپس تعداد مورد انتظار گره‌های امن اولیه‌ای است که

$$\sum\nolimits_{v\epsilon V(n)}B_v(0)=C_1\frac{\deg(v)}{\sum_{v\epsilon V(n)}\deg(u)}=C_1 \qquad (۲۲)$$

با توجه به تعریف داریم:

$$\propto_{threshold}=\frac{\sigma}{n}\frac{\left[\sum_{v\epsilon V(n)}\deg(u)\right]^2}{\sum_{v\epsilon V(n)}\deg(v)^2} \qquad (۲۳)$$

جایی که $\deg(v)$ درجه گره $v\epsilon V(n)$ هست. با توجه به تنظیمات رندم گره‌های امن در لحظه صفر ما تغییر رندم را بدین‌صورت تعریف میکنیم:

$$\chi_v(S)=\begin{cases}1 & v\epsilon S\\ 0 & v\notin S\end{cases} \qquad (۲۴)$$

از آنجا که

$$\phi(n)=\frac{\sum_{v\epsilon S}\deg(u)}{\sum_{v\epsilon V(n)}\deg(v)}=\frac{\sum_{v\epsilon S}\deg(u)\chi_u(S)}{\sum_{v\epsilon V(n)}\deg(v)}\approx\frac{\sum_{v\epsilon S}\deg(u)B_u(0)}{\sum_{v\epsilon V(n)}\deg(v)}>\sigma \qquad (۲۵)$$

این مطالب به این امر دلالت می‌کند که اگر $\frac{|S|}{n}>\propto_{threshold}$ داریم که $\lim_{t\to\infty}B_v(t)=1$ برای هر گره که عضو مجموعه گره‌های شبکه ما باشد، و اگر $\frac{|S|}{n}<\propto_{threshold}$ داریم که $\lim_{t\to\infty}B_v(t)=0$ برای هر گره که عضو مجموعه گره‌های شبکه گرافی ما باشد. ازآنجایی‌که :

$$\frac{\left[\sum_{v\epsilon V(n)}\deg(u)\right]^2}{\sum_{v\epsilon V(n)}\deg(v)^2}\leq n \qquad (۲۶)$$

ما داریم که $\propto_{threshold}\leq\sigma$. این بدان معنی است که مدافع استراتژیک می‌تواند از دفاع سایبری فعال برای پاک‌سازی کل شبکه استفاده کند به‌صورت خودکار و زمانی این امر راحت‌تر صورت می‌پذیرد که تعدادی از نقاط در همان ابتدا بیش از مقدار آستانه در اختیار مدافع باشد. مشخصه مای مزیت مهاجم استراتژیک و ارتباط مستقیم آن با درجه گره : وقتی‌که $R_v(0)\propto\deg(v)$ و ما داریم $R_v(0)=C_2\frac{\deg(v)}{\sum_{v\epsilon V(n)}\deg(u)}$ برای تعدادی از ثابت‌ها $C_2>0$. بر طبق رابطه زیر ما داریم:

$$\theta_{vBR}(\mathrm{t})=f_{BR}\left(\frac{1}{\deg(v)}\sum_{u\epsilon N_v}[1-B_u(t)]\right)=\begin{cases}1 & \frac{1}{\deg(v)}\sum_{u\epsilon N_v}[1-B_u(t)]>1-\sigma\\ 0 & \frac{1}{\deg(v)}\sum_{u\epsilon N_v}[1-B_u(t)]<1-\sigma\\ \frac{1}{2} & otherwise\end{cases} \qquad (۲۷)$$

تابع مبارزه در $1-\sigma$ به‌صورت ناپیوسته هست. آستانه اشغال اولین گره بدین شرح است:

$$\frac{1-\sigma}{n}\frac{\left[\sum_{v\epsilon V(n)}\deg(u)\right]^2}{\sum_{v\epsilon V(n)}\deg(v)^2}$$

بنابراین آستانه اشغال اولیه گره امن ما بدین شرح است :

$$\beta_{threshold}=1-\frac{1-\sigma}{n}\frac{\left[\sum_{v\epsilon V(n)}\deg(u)\right]^2}{\sum_{v\epsilon V(n)}\deg(v)^2} \qquad (۲۸)$$

[1] dense

اگر $\frac{|S|}{n} > \beta_{threshold}$ ، بنابراین ما داریم $\lim_{t\to\infty} B_v(t) = 1$ و اگر $\frac{|S|}{n} < \beta_{threshold}$، ما خواهیم داشت $\lim_{t\to\infty} B_v(t) = 0$. ازآنجایی‌که $\beta_{threshold} > \sigma$ ما می‌توانیم نتیجه بگیریم که اگر گره‌های با درجه بالا توسط مهاجم آسیب ببینند، مدافع می‌تواند از دفاع فعال سایبری برای پاک‌سازی شبکه استفاده کند تنها بعدازاینکه مدافع یک نسبت از آستانه شبکه، گره در اختیار داشته باشد.

۳-۵-۷- مشخصه مزیت‌های مدافع استراتژیک با گراف ER

برای گراف ER[1] که دارای یال با احتمال P هست، توزیع درجه آن به‌صورت دوجمله‌ای هست : $B = (n, p)$

$$P(\deg(v) = k) = \binom{n}{p} p^k (n-p)^k, k = 0,1 \dots. \quad (۲۹)$$

با توجه به مطالب بالا ما نشان می‌دهیم:

$$\propto_{threshold} = \sigma \frac{P}{P + P(1-P)/n} \;, \beta_{threshold} = 1 - (1 - \sigma)\frac{P}{P + P(1-P)/n} \quad (۳۰)$$

از آنجایی‌که $n \to \infty$ هر دو آستانه آلفا و بتا همگرا به σ می‌شوند. به‌طور خاص:

$$\beta_{threshold} - \propto_{threshold} = 1 - \frac{P}{P + P(1-P)/n}$$

همگرا به صفر می‌شوند. درحالی‌که

$$\frac{\beta_{threshold}}{\propto_{threshold}} = 1 + \frac{1-P}{\sigma n} \quad (۳۱)$$

همگرا به یک هست. با توجه به معادلات بالا در شبکه گرافی مذکور منافع امنیتی به‌دست آمده توسط مدافع (مهاجم) استراتژیک قابل توجیه نیست، زیرا درجه های گره نسبتاً همگن هستند. می‌توان این مطلب را استنباط نمود در این نوع شبکه برای حذف گره‌های بزرگ، شبکه از خود مقاومت نشان می‌دهد. البته در مدل ما مهاجم قصد دارد گره‌ها را به خطر بیندازد اما هیچ گره‌ای را حذف نمی‌کند.

۳-۵-۸- مشخصه مزیت مدافع استراتژیک در power law گراف

در power law گراف با توان گاما داریم:

$$C = \int_{d_{min}(n)}^{d_{max}(n)} k^{-\gamma} dk = \frac{d_{max}(n)^{1-\gamma} - d_{min}(n)^{1-\gamma}}{1-\gamma}. \quad (۳۲)$$

با توجه به‌جایگذاری انتگرال در معادله ما داریم:

$$\propto_{threshold} = \frac{\sigma}{n}\frac{\left[\sum_{v\epsilon V(n)} \deg(u)\right]^2}{\sum_{v\epsilon V(n)} \deg(v)^2}$$

$$\propto_{threshold} = \frac{\sigma\left(\frac{n}{C}\int_{d_{min}(n)}^{d_{max}(n)} k^{1-\gamma} dk\right)^2}{\frac{n}{C}\int_{d_{min}(n)}^{d_{max}(n)} k^{2-\gamma} dk} =$$

$$= \frac{\sigma}{n}\left(\frac{n^2(d_{max}(n)^{2-\gamma} - d_{min}(n)^{2-\gamma})^2/(2-\gamma)^2}{(d_{max}(n)^{1-\gamma} - d_{min}(n)^{1-\gamma})^2/(1-\gamma)^2}\right) / \left(\frac{n(d_{max}(n)^{3-\gamma} - d_{min}(n)^{3-\gamma})/(3-\gamma))}{(d_{max}(n)^{1-\gamma} - d_{min}(n)^{1-\gamma})/(1-\gamma)}\right).$$

این امر منجر به چهار مورد می‌شود: $\gamma = 3$, $\gamma = 2$, $\gamma \notin \{1,2,3\}$, $\gamma = 1$ و قرار می‌دهیم $\mathcal{Z} = \frac{d_{max}(n)}{d_{min}(n)}$. برای $\gamma \notin \{1,2,3\}$ می‌توان نشان داد که:

$$\left(\frac{(d_{max}(n)^{2-\gamma} - d_{min}(n)^{2-\gamma})^2/(2-\gamma)^2}{(d_{max}(n)^{1-\gamma} - d_{min}(n)^{1-\gamma})^2/(1-\gamma)^2}\right) / \left(\frac{(d_{max}(n)^{3-\gamma} - d_{min}(n)^{3-\gamma})/(3-\gamma))}{(d_{max}(n)^{1-\gamma} - d_{min}(n)^{1-\gamma})/(1-\gamma)}\right)$$

$$\frac{\left(\mathcal{Z}^{2-\gamma} - 1\right)^2}{(\mathcal{Z}^{1-\gamma} - 1)(\mathcal{Z}^{3-\gamma} - 1)}\frac{(3-\gamma)(1-\gamma)}{(2-\gamma)^2}.$$

برای $\gamma = 1,2,3$ ما می‌توانیم به روشی مشابه استدلال کنیم. درنتیجه می‌توانیم تعریف کنیم :

$$h(\mathcal{Z},\gamma) = \begin{cases} \frac{\left(\mathcal{Z}^{2-\gamma} - 1\right)^2}{(\mathcal{Z}^{1-\gamma} - 1)(\mathcal{Z}^{3-\gamma} - 1)}\frac{(3-\gamma)(1-\gamma)}{(2-\gamma)^2} & \gamma \neq 1,2,3 \\ 2\frac{\mathcal{Z}-1}{\mathcal{Z}+1}\frac{1}{\ln \mathcal{Z}} & \gamma = 1 \\ \frac{\mathcal{Z}(\ln(\mathcal{Z}))^2}{(\mathcal{Z}-1)^2} & \gamma = 2 \\ 2\frac{\mathcal{Z}-1}{\mathcal{Z}+1}\frac{1}{\ln \mathcal{Z}} & \gamma = 3 \end{cases} \quad (۳۳)$$

اگر مدافع استراتژیک، دارای شرایط کافی برای $\lim_{t\to\infty} B_v(t) = 1$ هست اگر $\frac{|S|}{n} > \alpha_{threshold} = \sigma.h(\mathcal{Z},\gamma)$ ، اگر مهاجم استراتژیک باشد، شرایط کافی برای اینکه $\lim_{t\to\infty} B_v(t) = 1$ هست $\frac{|S|}{n} > \beta_{threshold} = 1 - (1-\sigma).h(\mathcal{Z},\gamma)$ ، بنابراین ما داریم:

$$\alpha_{threshold} - \beta_{threshold} = 1 - h(\mathcal{Z},\gamma),$$

$$\frac{\beta_{threshold}}{\alpha_{threshold}} = \frac{1-(1-\sigma).h(\mathcal{Z},\gamma)}{\sigma.h(\mathcal{Z},\gamma)} = 1 + \frac{1-h(\mathcal{Z},\gamma)}{\sigma.h(\mathcal{Z},\gamma)} \quad (۳۴)$$

[1] Erdos Renyi

با توجه به معادلات بالا توان گاما را برابر با ۲ در نظر می‌گیریم. نتایجی که از این شبکه به دست می‌آید بدین شرح است : تعریف مدافع (مهاجم) استراتژیک خیلی مهم است. به‌عنوان‌مثال در قانون قدرت شبکه‌ها[1] به‌آسانی با پاک شدن گره‌های بزرگ از بین می‌رود، بازهم در مدل ما مهاجم هدفش توافق است تا از بین بردن تعدادی از گره‌ها، علاوه بر این مزیت برای یک مدافع استراتژیک بزرگ شدن زیر کلاس[2] برای قدرت قانون شبکه‌ها برابر با $\gamma = 2$ هست.

۳-۶- مشخصه نوع دوم دینامیک دفاع سایبری فعال

دینامیک دوم بسیار شبیه به نوع اول است به‌جز در مواردی که بیان می‌کنیم. در دینامیک نوع یک تابع قدرت مبارزه در نزدیکی آستانه ناپیوسته بوده، درحالی‌که در دینامیک نوع دوم تابع مبارزه ما در نزدیکی آستانه پیوسته بوده و دیفرانسیل پذیر هست. برای مدافع غیراستراتژیک با گره مستقل ما همان قضایایی را که برای دینامیک نوع اول به دست آوردیم برای همین نوع از دینامیک به آن رسیدیم که از بیان آن می‌گذریم. در دینامیک نوع دوم ما شرایط کلی را بیان می‌کنیم :

نوع دوم دینامیک دارای حد آستانه معلوم در سیستم زیر در شبکه خودسرانه گرافی هست.

$$\begin{aligned}\frac{d}{dt}B_v(t) &= \theta_{vRB}\,(\mathrm{t})\big(1 - B_v(t)\big) \\ &\quad - \theta_{vBR}\,(\mathrm{t}).\,B_v(t) \\ &= \theta_{vBR}\,(\mathrm{t}) - B_v(t)\end{aligned} \qquad (۳۵)$$

اگر $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(0) > \tau$ برای همه گره‌های عضو شبکه‌داریم $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t) > \tau$ که برای تمام گره‌های عضو شبکه صادق است و احتمال امن بودن برای گره‌های کوچک در شبکه در طول زمان به‌صورت یکنواختی افزایش را نشان می‌دهد.

اگر $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(0) < \tau$ برای همه گره‌های عضو شبکه‌داریم $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(t) < \tau$ که برای تمام گره‌های عضو شبکه برقرار است و احتمال امن بودن گره‌های بزرگ در شبکه در طول زمان به‌صورت یکنواختی کاهش را نشان می‌دهد.

۳-۶-۱- شرایط کافی جهت اشغال شبکه توسط مدافع (مهاجم)

در نوع دوم این دینامیک شبکه خودسرانه ما دارای حد آستانه معین در گراف موردنظر شکل‌گرفته است.

اگر $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(0) > \tau$ برای همه گره‌های عضو شبکه ما به $\lim_{t\to\infty} B_v(t) = 1$ برای تمامی گره‌های عضو شبکه در طول زمان خواهیم رسید.

اگر $\frac{1}{\deg(v)}\sum_{u\epsilon N_v} B_u(0) < \tau$ برای همه گره‌های عضو شبکه ما به $\lim_{t\to\infty} B_v(t) = 0$ برای تمامی گره‌های عضو شبکه در طول زمان خواهیم رسید.

۳-۶-۲- شرایط کافی جهت عدم اشغال شبکه توسط مدافع(مهاجم)

در نوع دوم این دینامیک ما دارای یک شبکه خودسرانه با حد آستانه معلوم در گرافی که دارای ساختار خوشه‌ای است هستیم. اگر ما $B_v(0) = \alpha_k$ برای هر گره عضو V_k باشد و β_k حداقل گسترش گره‌ها در فرمول $\beta_k = inf\frac{|N_v \cap V_k|}{\deg(v)}$ باشند. اگر $\alpha_k\beta_k > \sigma$ باشد برای همه گره‌های عضو V_k امنیت برقرار است و اگر $(1-\alpha_k)\beta_k > 1-\sigma$ گره‌های عضو V_k به خطر افتاده‌اند.

۳-۶-۳- روش یا الگوریتمی برای رسیدن به معادله تعادل

در این روش ما دارای یک شبکه گرافی خود سرانه هستیم با حد آستانه تعیین‌شده هستیم. اگر ما معادله تعادل را برابر با:

$$B^* = [B_v^*]_{v\epsilon V} \qquad (۳۶)$$

و معادله تعادل گره‌های ناامن را برابر با:

$$\overline{B^*} = [1 - B_v^*]_{v\epsilon V} \qquad (۳۷)$$

در این صورت دو حالت پدید می‌آید:

اول اینکه دو حالت در شبکه ظهور پیدا می‌کند یا شبکه در امنیت است و یا در معرض خطر قرارگرفته است. دومین حالت نیز اگر $B^* = \tau$ برای تمامی گره‌های عضو شبکه، نقاطی که در اختیار مدافع(مهاجم) است به سمت ناپایداری خواهیم رفت.

۳-۷- مشخصه‌های نوع سوم و چهارم در دفاع سایبری فعال

عملکرد تابع مبارزه در دینامیک نوع سوم و چهارم بیانگر این مطلب است که مدافع (مهاجم) نسبت به حریف خود برتر یا پیشرفته‌تر است. به‌دلیل آنکه ما در این دو نوع از دینامیک آستانه‌ای نداریم، توابع قدرت رایانه‌ای[3]، نتیجه‌ای که به‌سرعت به دست می‌آید این است که هیچ تفاوتی میان استراتژیک یا غیراستراتژیک نیست.

[1] Power- Law Networks
[2] Subclass
[3] Computer-Power Function

۳-۸- ویژگی دینامیک نوع سوم

این دینامیک شامل یک شبکه خودسرانه در گراف تعیین‌شده هست. با توجه به این مدل سه حالت پدید می‌آید.

حالت اول اگر احتمال نقاط امنی که در اختیار مدافعین هست در لحظه صفر، از صفر بیشتر باشد برای همه گره‌های موجود در شبکه ما برای تمامی لحظات پیش رو شاهد امنیت شبکه خواهیم بود برای تمامی گره‌هایی که زیرمجموعه رئوس موجود در سیستم می‌باشند.

$$B_v(0) > 0 \rightarrow v\epsilon V \rightarrow \lim_{t\to\infty} B_v(t) = 1 \; for \; all \; v \; \epsilon V \quad (۳۸)$$

حالت دوم زمانی که $B_v(0) = [1, \dots, 1]$ ، تعادل پایدار مجانبی به‌صورت نمایی همگرا می‌شود. حالت سوم زمانی که $B_v(0) = [0, \dots, 0]$ ، ما شاهد ناپایداری هستیم.

۳-۹- ویژگی دینامیک نوع چهارم

ما در این نوع دینامیک دارای شبکه خودسرانه در گراف موردنظر هستیم. سه حالت پیش روی ما هست:

حالت اول اگر احتمال نقاط امنی که در اختیار مدافعین هست در لحظه صفر از صفر کمتر باشد برای همه گره‌های موجود در شبکه ما برای تمامی لحظات پیش رو شاهد ناامنی شبکه خواهیم بود برای تمامی گره‌هایی که زیرمجموعه رئوس موجود در سیستم می‌باشند.

$$B_v(0) < 0 \rightarrow v\epsilon V \rightarrow \lim_{t\to\infty} B_v(t) = 0 \; for \; all \; v \; \epsilon V \quad (۳۹)$$

حالت دوم زمانی که $B_v(0) = [0, \dots, 0]$، تعادل پایدار مجانبی به‌صورت نمایی همگرا می‌شود. حالت سوم زمانی که $B_v(0) = [1, \dots, 1]$ ، ما شاهد ناپایداری هستیم.

به‌طورکلی می‌توان چنین استنباط نمود که اگر مدافع ازلحاظ قدرت رزمی سایبری نسبت به مهاجم برتری داشته باشد، مدافع همیشه می تواند از دفاع فعال برای پاک کردن خودکار شبکه تا زمانی که چند رایانه وجود دارند که به خطر نیفتاده است، استفاده کند. در موردی که در آن مهاجم کل شبکه را به خطر انداخته است، مدافع باید قبل از شروع دفاع فعال، تنها چند کامپیوتر را به‌صورت دستی تمیز کند تا کل شبکه خود به‌طور خودکار پاک شود. این نشان می‌دهد که برتری رزمی سایبری می‌تواند به‌عنوان عامل بازدارندگی مؤثر عمل کند.

۳-۱۰- مقایسه برتری دفاع سایبری فعال نسبت به دفاع واکنشی

دفاع سایبری فعال که در حال حاضر مورداستفاده قرار می‌گیرد، به‌موجب آن مدافع به اجرای نرم‌افزار آنتی‌ویروس می‌پردازد که بر روی هر کامپیوتر برای اسکن و درمان آسیب‌پذیری وجود دارد، که به‌وسیله آن مدافع از نفوذ مهاجم یا بدافزار به محیط خود جلوگیری به عمل می‌آورد مانند فایروال‌ها که بدین گونه عمل می‌کنند. دفاع سایبری واکنشی به‌ناچار سبب عدم تقارن شده که موجب منفعت بردن مهاجم می‌شود چراکه مهاجم به‌صورت خودکار فعالیت‌های خود را توسط شبکه تقویت می‌کند. به‌طور خاص دفاع واکنشی شاید شبیه به مدل SIS[1] باشد این مدل بدین‌صورت است که خودش را سازگار می‌کند با ساختار شبکه خودسرانه مهاجم-مدافع[2] که شرط کافی برای از بین رفتن آسیب‌پذیری همه‌گیر است[۱۶].

$$\lambda_{1,A} < \frac{cure\ capability}{spreading\ capability} \quad (۴۰)$$

از آنجایی‌که $\lambda_{1,A}$ بزرگ‌ترین مقدار ویژه[3] ماتریس مجاورت[4] مربوط به ساختار دفاع-حمله است و این مفهوم به دست می‌آید که میانگین درجه گره یا اتصال، خلاصه توان درمان مدافع واکنشی، قدرت دفاع آن است (احتمال آسیب دیدن یک گره می‌شود حساسیت یک گره در یک‌زمان واحد)، و گسترش توانایی خلاصه‌ای از قدرت حمله مهاجم است (برای مثال آسیب دیدن یک گره به‌صورت موفقیت‌آمیز باید حمله به یک گره که دارای همسایگی مستعد و در یک مرحله زمانی هست انجام گیرد)، این بدان معنی است که مهاجم همیشه از اتصال باارزش بهره می‌برد، زیرا اثر مهاجم تقویت می‌شود با $\lambda_{1,A}$ ، که توضیح می‌دهد چرا پدیده عدم تقارن برای مهاجم سودمند است[۴۳،۴۴،۴۵]. از سویی در مدل دینامیکی که الگو/روش برای مدافع(مهاجم) غیراستراتژیک را جهت رسیدن به معادله تعادل را که بیان نمودیم، نشان می‌دهد که پدیده عدم توازن[5] با دفاع سایبی فعال از بین می‌رود زیرا $\lambda_{1,A}$ و مانند آن نقشی در نتایج تحلیلی ندارد. این بررسی‌ها ما را به‌طور خلاصه بدین نتیجه می‌رساند که دفاع فعال سایبری پدیده تقویت شدن حمله را از بین می‌برد، برای مثال عدم تقارن بین مهاجمین سایبری و مدافعین واکنشی سایبری را بیان نمود.

[1] Susceptible-infectious- susceptible
[2] Attack-defense
[3] Largest eigenvalue
[4] Adjacency matrix
[5] asymmetry

۳-۱۱- اعتبار سنجی مدل سیستم دینامیکی با شبیه‌سازی

ویژگی‌های بالا پویایی دفاع سایبری فعال مبتنی بر مدل سیستم دینامیکی را نشان داد، که تقریب میدان متوسط مدل فرآیند مارکوف است . بنابراین ، ما باید نشان دهیم که آیا نتایج تحلیلی به‌دست‌آمده از مدل سیستم دینامیکی ، در ذات خود مدل فرآیند مارکوف را دارا هست.

۳-۱۱-۱- اعتبارسنجی مدل

ما در اعتبار سنجی تمرکز خود را بر روی دقت سیستم دینامیکی گذاشته‌ایم. برای بررسی دقت دینامیک، ما به مقایسه میانگین احتمال امنیت گره‌های اشغال‌شده در مدل سیستم دینامیکی می‌پردازیم. برای مثال $B_v(t) = \frac{1}{|V|}\sum_{v\epsilon V} B_v(t)$ و شبیه‌سازی می‌کند بر اساس میانگین توابع امنیت گره‌های مدل مارکوف، برای مثال $\xi_v(t) = \frac{1}{|V|}\sum_{v\epsilon V} \xi_v(t)$. اگر $\xi_v(t)$ و $B_v(t)$ یک‌چیز مشابه ارائه دهند، اگر دقیقا یکسان نباشد در رفتار دینامیکی ما نتیجه می‌گیریم که نتایج تحلیلی حاصل از مدل سیستم دینامیکی برای مدل فرآیند مارکوف در آن مشهود است.

شبیه‌سازی مدل مارکوف بر اساس احتمال شرطی:

$$P\left(\xi_v(t+\Delta t)=1 \middle| \xi_v(t), v\epsilon N\right) = \begin{cases} \Delta t.\tilde{\theta}_{v,RB}(t) & \xi_v(t)=0 \\ 1-\Delta t.\tilde{\theta}_{v,BR}(t) & \xi_v(t)=1 \end{cases} \quad (۴۱)$$

جایی که نرخ رندم $\tilde{\theta}_{v,RB}(t)$ جایگزین می‌شود با $\theta_{v,RB}(t)$ نتایج شبیه‌سازی بعد از ۵۰ بار اجرا به دست می‌آید.

محاسبات عددی ما در مدل سیستم دینامیکی مبتنی بر معادله کلی دینامیکی بدین شرح است:

$$B_v(t+\Delta t) = B_v(t) + \left[\theta_{v,RB}(t) - B_v(t)\right]\Delta t \quad (۴۲)$$

که ما $\Delta t = 0.01$ را قرار داده‌ایم.

برای امتحان دقت آستانه، ما بررسی می‌کنیم که آستانه در مدل سیستم دینامیکی آیا در مدل سیستم دینامیکی مارکوف صحت لازم برقرار است؟ به‌منظور محاسبه حد آستانه مدل مارکوف، ما از روش عددی زیر استفاده می‌کنیم. ازآنجایی‌که همگرایی $\xi_v(t)$ در یک‌فاصله زمانی بسیار کوچک است که شامل حد آستانه می‌شود، ما تعریف می‌کنیم حد آستانه مدل مارکوف را به‌عنوان مقدار متوسط در آن بازه که به‌طور مشخص a_1 را کمترین مقدار قرار می‌دهیم به‌گونه‌ای که اشغال اولیه بزرگ‌تر از a_1 باعث شود که همه گره‌ها در ۵۰ اجرا امن شوند. و b_1 را به‌عنوان بزرگ‌ترین مقدار به‌طوری‌که اشغال اولیه کوچک‌تر از b_1 باعث شود همه گره‌ها در ۵۰ اجرا به خطر بیفتد. ما حد آستانه مدل مارکوف را بدین‌صورت بیان می‌کنیم و از دو نوع گراف ER و power law در شبیه‌سازی استفاده می‌کنیم.

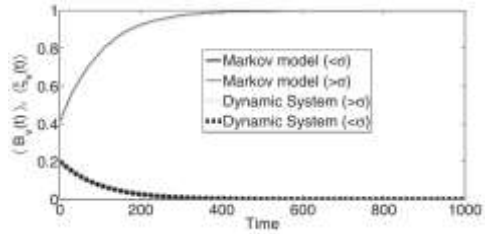
$$\sigma_{markov} = \frac{1}{2}(a_1 + b_1) \quad (۴۳)$$

ER : دارای ۲۰۰۰ گره و با احتمال پیوند مستقل $P = ۰/۰۲$

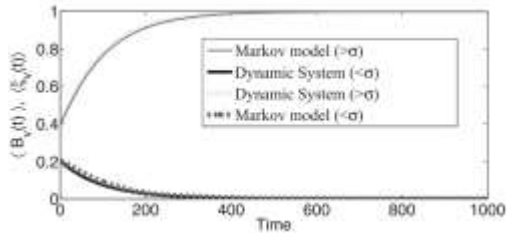
Power law : دارای ۲۰۰۰ گره و توان نمایی $\gamma = ۲/۵$ و حداقل درجه ۲ و حداکثر درجه ۱۲۰.

۳-۱۲- دقت کلی مدل سیستم دینامیکی

ما در دینامیک نوع اول با مدافع غیراستراتژیک با گره‌های مستقل همسان که در ابتدا با احتمال $B_v(0)$، اشغال‌شده است. به‌طور مشخص مدل سیستم دینامیکی ما که $B_v(t)$ متناظر است با $B_v(0) = ۰/۴ > \sigma = ۱/۳$ همه همگرا به ۱ هستند. و $B_v(0)$ متناظر است با $B_v(0) = ۰/۲ < \sigma = ۱/۳$ همگرا به صفر هستند.



شکل (۴): شبکه گرافی ER

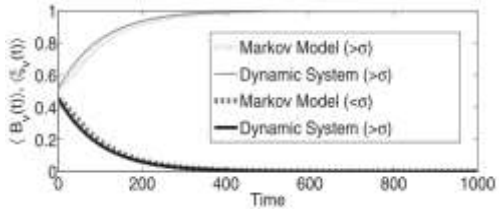


شکل (۵): شبکه گرافی power law

در مدل مارکوف $\xi_v(t)$ متناظر است با $P\{\xi_v(0)=1\} = ۰/۰۴$ همه همگرا به ۱ هستند و $\xi_v(t)$ متناظر است با $P\{\xi_v(0)=۱\} = ۰/۲$ همه همگرا به صفر هستند. بنابراین، تعریف دینامیک به ما نشان داده می‌شود به‌وسیله شرایط کافی برای تصرف کردن شبکه توسط مدافعین(مهاجمین)، و نیز توسط مدل فرآیند مارکوف به نمایش گذاشته می‌شود. با نگاهی به دینامیک نوع اول و مدافع استراتژیک احتمال نقاط امن در لحظه صفر با یال گره‌ها ارتباط مستقیم دارد و بدین‌صورت تعریف می‌شود:

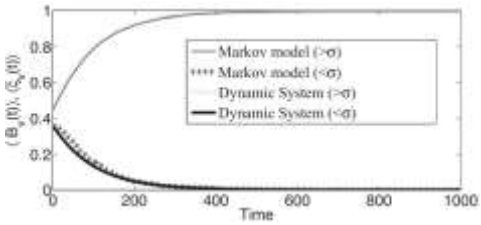
$$\eta = \frac{\sum_{u\epsilon S} deg(u)}{\sum_{v\epsilon V} deg(v)} \quad (۴۴)$$

جایی کـه S تنظـیم‌شـده بـرای گـره امـن در زمـان ۰ = t . نـابرابری کـه در شـرایط نتـایج دفـاع فعـال سـایبری بـا مـدافع استراتژیک بیان شد نشان می‌دهد کـه اگـر $\eta > \sigma$ ، پـس همـه گره‌ها امن می‌شود، درحالی‌که اگر $\eta < \sigma$ ، همـه گـره‌هـا نـاامن می‌شود. در شبیه‌سازی ما $\sigma = ۰/۵$ تنظیم کرده‌ایـم. شـکل زیـر نشان می‌دهد که در گراف ER ، هر دو مـدل سیسـتم دینـامیکی $B_v(t)$ و $\xi_v(t)$ همگرا به ۱ هستند وقتی‌کـه $\eta = ۰/۵۲ > ۰/۵$ $= \sigma$ و زمانی همگرا به صفر می‌شود که $\eta = ۰/۴۵ > \sigma = ۰/۵$.



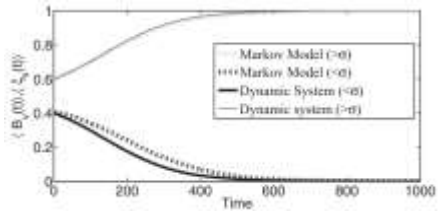
شکل (۶): شبکه گرافی ER

شکل۷ این مطلب را نشان می‌دهد که در شبکه power law هـر دو سیسـتم دینـامیکی $B_v(t)$ و $\xi_v(t)$ همگـرا بـه ۱ هسـتند، وقتی‌که $\eta = ۰/۴۵ < \sigma = ۰/۵$ و همگرا به صفر هستند زمـانی که $\eta = ۰/۳۵$ (خیلی کوچک‌تر از $\sigma = ۰/۵$) باشد. ایـن پدیـده به‌وسیله شرایط نتایج دفاع سایبری فعـال بـا مـدافع اسـتراتژیک نشان داده‌شده است. برای مثال اثر مـدافع اسـتراتژیک در گـراف ER مهم نیست ولی اثر مـدافع اسـتراتژیک در power law مهـم است. درهرصورت نتایج شبیه‌سـازی پدیـده‌ای کـه توسـط مـدل سیستم دینامیکی ما نشـان داده‌شـده اسـت در ذات خـود مـدل مارکوف را دارا است.

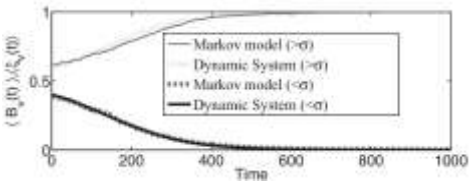


شکل (۷): شبکه گرافی power law

دینامیک نوع دوم تـابع مبـارزه‌اش بـا $\tau = 0.5$ ، $f_{RB}(x) = 2x^2$ برای $x\epsilon[0,0.5]$ و $f_{RB}(x) = -2x^2 + 4x - 1$ بـرای $x\epsilon[0.5,1]$. برای مدل سیستم دینامیکی، شکل (۸ و ۹) نشان می‌دهـد کـه $B_v(0) = 0.4 < \tau = 0.5$ دلالت دارد به اینکه همه گـره‌هـا بـه خطر افتاده اند و $B_v(0) = 0.6 > \tau = 0.5$ اشاره دارد به اینکـه همه گره‌ها امن خواهند شد.

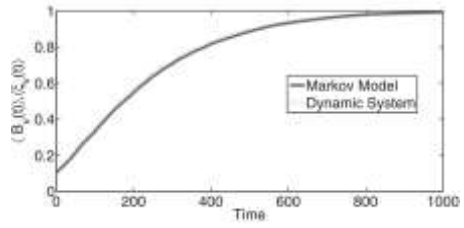


شکل (۸): شبکه گرافی ER

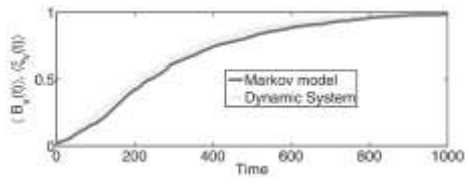


شکل (۹): شبکه گرافی power law

بـرای نـوع سـوم تـابع مبـارزه بـا $f_{RB}(x) = 2x^{1/2}$، شـکل (۱۰ و ۱۱) نشـان مـی‌دهـد کـه $B_v(t)$ متنـاظر اسـت بـا $B_v(0) = ۰/۰۲$ همگرا به ۱ هست. همین پدیده در مدل فرآینـد به نمایش گذاشته‌شده است. ویژگی دینامیک نوع سوم این قضیه را تائید می‌کند.

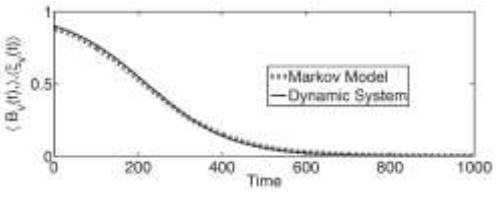


شکل (۱۰): شبکه گرافی ER

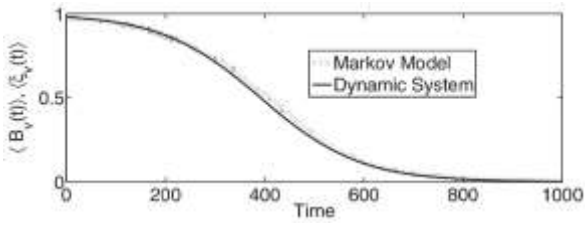


شکل (۱۱): شبکه گرافی power law

برای نوع چهارم تابع مبارزه $f_{RB}(x) = x^2$، شکل ۱۲و۱۳ اثبات می‌کند که $B_v(t)$ متناظر است با $B_v(0) = 0.98$ همگرا به صفر است. همین پدیده مدل مارکوف را نشان می‌دهد. برای شبکه power law و مدافع استراتژیک، احتمال گره‌های امن در لحظه صفر ارتباط مستقیمی با یال گره دارد.



شکل (۱۲): شبکه گرافی ER



شکل (۱۳): شبکه گرافی power law

مـــا شـــرط کـــافی را بـــا $\frac{|S|}{n} > \sigma.h(\mathcal{Z},\gamma)$ بـــرای $\lim_{t\to\infty} B_v(t) = ۰$ به دست آوردیم. بدین معنـی کـه مـدافع برای آنکه از دفاع فعال سایبری استفاده کند تا شـبکه بـه‌صـورت خودکار پاک‌سازی شود، نیاز به اشغال تعداد بیشـتری از قسـمت مای گره $\sigma.h(\mathcal{Z},\gamma)$ دارد، وقتی‌که $h(\mathcal{Z},\gamma)$ حداقل هست.

با توجه به اشکال شماره (۴) تا (۱۳)، که نتایج شـبیه سـازی تعامل میان مدافعین و مهاجمن را نشـان مـی دهـد ایـن نتیجـه حاصل می گردد که، دفاع سایبری فعال تقویـت شـده و حمـلات تحت اثر شبکه که مهاجمین از این نقطه ضعف بهره می برده اند و حاصل عدم توازن با مدافعین بود را خنثی نمـوده اسـت. بـرای اثبات صحت عملکرد مدل توابع نیز باید نشان دهیم که عملکـرد توابع پیشنهادی همانند مـدل مـارکوف بـوده کـه بـه وضـوح در اشکال مورد اشاره با یکدیگر هم پوشانی دارند.

۴- نتیجه‌گیری

در این تحقیق طرحی ارائه شد که عدم تـوازن میـان مـدافعین و مهاجمین را از بین برد، و به نقاط ضعف مدافعین پرداخته شد. در دفاع سنتی یا واکنش محور، به اجـرای آنتـی‌ویـروس و ابزارهـای گوناگون بسنده می‌کردیم که این کار سبب نفوذ مهاجم یا بدافزار در محیط مدافع شده، که این عدم توازن سبب عملکرد منفعلانـه مدافعین شده و اثرات مهاجم توسـط شـبکه بـه‌صـورت خودکـار تقویت‌شده که به یک نوع تأثیر شـبکه معـروف اسـت. در تئـوری بیان‌شده ما تعامل بین مدافعین و مهاجمین را هدف قـرار داده و با توجه به استراتژیک بودن طرف مقابل در دینامیک‌های مختلف که در بستر شبکه‌های مختلف شبیه‌سـازی مـی‌شـود. ایـن نکتـه بسیار مهم است که در هر شبکه باید چگونه و در چه زمانی عمل نماییم تا بتوانیم از دفاع سایبری فعال استفاده کنیم. با توجـه بـه فرضیات مسئله مهاجم قصد حذف گره را نخواهد داشت، بنابراین باید ساختار شبکه طوری طراحی شود تا مهاجم هزینه زیـادی را برای اقدامات خود بپردازد این همان بازدارنـدگی دفـاع سـایبری فعال است.

۵- مراجع

[1] K. M. Aghaei, S. Farshchi, en H. Shirazi, “A new architecture for impact projection of cyber-attacks based on high level information fusion in cyber command and control”, 2015.

[2] D. Aitel, “Nematodes--beneficial worms”, Black Hat Federal, vol 33, bll 39–44, 2006. [3] N. Weaver and D. Ellis, “White worms don’t work,” ;login: The USENIX Magazine, vol. 31, no. 6, pp. 33–38, 2006.

[3] Q. Zhang, C. Zhou, N. Xiong, Y. Qin, X. Li, en S. Huang, “Multimodel-based incident prediction and risk assessment in dynamic cybersecurity protection for industrial control systems”, IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol 46, no 10, bll 1429–1444, 2015.

[4] J. Aycock en A. Maurushat, “‘ Good’ worms and human rights”, Acm Sigcas Computers and Society, vol 38, no 1, bll 28–39, 2008. [5] H. Lin, “Lifting the veil on cyber offense,” IEEE Security & Privacy, vol. 7, no. 4, pp. 15–21, 2009.

[5] S. Xu, “Emergent behavior in cybersecurity”, in Proceedings of the 2014 Symposium and Bootcamp on the Science of Security, 2014, bll 1–2.

[6] W. Matthews, “Us said to need stronger, active cyber defenses”. 2010.

[7] J. P. Kesan en C. M. Hayes, “Mitigative counterstriking: Self-defense and deterrence in cyberspace”, Harv. JL & Tech., vol 25, bl 429, 2011.

[8] H. S. N. Wire, “Active cyber-defense strategy best deterrent against cyber-attacks”. 2011.

[9] W. Lu, S. Xu, en X. Yi, “Optimizing active cyber defense”, in International Conference on Decision and Game Theory for Security, 2013, bll 206–225.

[10] L. Shaughnessy, “The internet: Frontline of the next war”. 2011.

[11] J. Wolf, “Update 2-us says will boost its cyber arsenal”. 2011.

[12] R. Albert, H. Jeong, en A.-L. Barabási, “Error and attack tolerance of complex networks”, nature, vol 406, no 6794, bll 378–382, 2000.

[13] Y. Wang, D. Chakrabarti, C. Wang, en C. Faloutsos, “Epidemic spreading in real networks: An eigenvalue viewpoint”, in 22nd International Symposium on Reliable Distributed Systems, 2003. Proceedings., 2003, bll 25–34. [14] A. Ganesh, L. Massoulié, en D. Towsley, “The effect of network topology on the spread of epidemics”, in Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies., 2005, vol 2, bll 1455–1466.

[15] N. Berger, C. Borgs, J. T. Chayes, en A. Saberi, “On the spread of viruses on the internet”, 2005.

[16] D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, en C. Faloutsos, “Epidemic thresholds in real networks”, ACM Transactions on Information and System Security (TISSEC), vol 10, no 4, bll 1–26, 2008.

Series A, Containing papers of a mathematical and physical character, vol 115, no 772, bll 700–721, 1927.

[28] H. W. Hethcote, "The mathematics of infectious diseases", SIAM review, vol 42, no 4, bll 599–653, 2000.

[29] R. Durrett, Random graph dynamics, vol 200. Cambridge university press Cambridge, 2007.

[30] N. Masuda, N. Gibert, en S. Redner, "Heterogeneous voter models", Physical Review E, vol 82, no 1, bl 010103, 2010.

[31] E. Pugliese en C. Castellano, "Heterogeneous pair approximation for voter models on networks", EPL (Europhysics Letters), vol 88, no 5, bl 58004, 2009.

[32] V. Sood, T. Antal, en S. Redner, "Voter models on heterogeneous networks", Physical Review E, vol 77, no 4, bl 041121, 2008.

[33] F. Schweitzer en L. Behera, "Nonlinear voter models: the transition from invasion to coexistence", The European Physical Journal B, vol 67, no 3, bll 301–318, 2009.

[34] M. Vojnovic en A. J. Ganesh, "On the race of worms, alerts, and patches", IEEE/ACM Transactions on Networking, vol 16, no 5, bll 1066–1079, 2008.

[35] P. A. P. Moran en Others, "The statistical processes of evolutionary theory", The statistical processes of evolutionary theory., 1962.

[36] M. A. Nowak, Evolutionary dynamics: exploring the equations of life. Harvard university press, 2006.

[37] R. Pastor-Satorras en A. Vespignani, "Epidemic spreading in scale-free networks", Physical review letters, vol 86, no 14, bl 3200, 2001.

[38] T. M. Liggett, Stochastic interacting systems: contact, voter and exclusion processes, vol 324. springer science & Business Media, 2013.

[39] A.-L. Barabási en R. Albert, "Emergence of scaling in random networks", science, vol 286, no 5439, bll 509–512, 1999.

[40] F. Chung, F. R. K. Chung, F. C. Graham, L. Lu, K. F. Chung, en Others, Complex graphs and networks. American Mathematical Soc., 2006.

[17] P. Van Mieghem, J. Omic, en R. Kooij, "Virus spread in networks", IEEE/ACM Transactions On Networking, vol 17, no 1, bll 1–14, 2008.

[18] S. Chatterjee en R. Durrett, "Contact processes on random graphs with power law degree distributions have critical value 0", The Annals of Probability, vol 37, no 6, bll 2332–2356, 2009.

[19] F. Ball, D. Sirl, en P. Trapman, "Threshold behaviour and final outcome of an epidemic on a random network with household structure", Advances in Applied Probability, vol 41, no 3, bll 765–796, 2009.

[20] F. Ball, D. Sirl, en P. Trapman, "Analysis of a stochastic SIR epidemic on a random network incorporating household structure", Mathematical Biosciences, vol 224, no 2, bll 53–73, 2010.

[21] D. Fava, "Characterization of cyber attacks through variable length markov models", 2007.

[22] T. Mountford, J.-C. Mourrat, D. Valesin, en Q. Yao, "Exponential extinction time of the contact process on finite graphs", Stochastic Processes and their Applications, vol 126, no 7, bll 1974–2013, 2016.

[23] T. Mountford, D. Valesin, en Q. Yao, "Metastable densities for the contact process on power law random graphs", Electronic Journal of Probability, vol 18, bll 1–36, 2013.

[24] J. O. Kephart en S. R. White, "Directed-graph epidemiological models of computer viruses", in Computation: the micro and the macro view, World Scientific, 1992, bll 71–102.

[25] J. O. Kephart en S. R. White, "Measuring and modeling computer virus prevalence", in Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy, 1993, bll 2–15.

[26] A. G. M'Kendrick, "Applications of mathematics to medical problems", Proceedings of the Edinburgh Mathematical Society, vol 44, bll 98–130, 1925.

[27] W. O. Kermack en A. G. McKendrick, "A contribution to the mathematical theory of epidemics", Proceedings of the royal society of london.