مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"
سال ششم، شماره ۳، پاییز ۱۳۹۷، ص ۱۴۰-۱۳۱

مدل‌سازی انتشار بدافزار با در نظر گرفتن رویکرد تنوع نرم‌افزاری در شبکه بی‌مقیاس وزن‌دار

سوده حسینی[1*] ، محمد عبداللهی ازگمی[2]

۱- استادیار، دانشکده ریاضی-کامپیوتر، بخش علوم کامپیوتر، دانشگاه شهید باهنر کرمان، کرمان،

۲- دانشیار، دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران، تهران

(دریافت:۹۶/۰۹/۰۷، پذیرش: ۹۶/۱۰/۲۲)

چکیده

امروزه انتشار بدافزارها، یک تهدید امنیتی بزرگ در فضای سایبری محسوب می‌شود. مدل‌سازی انتشار بدافزارها منجر می‌شود تا محققان بتوانند رفتار انتشاری آن‌ها را شناسایی و پیش‌بینی نموده و سازوکارهای دفاعی مناسبی را برای دفاع در برابر آن‌ها به‌کار گیرند. در این راستا تنوع نرم‌افزاری به عنوان یک سازوکار دفاع سایبری مورد توجه قرار گرفته است. در این مقاله، یک مدل همه‌گیری از انتشار بدافزار در شبکه‌های بی‌مقیاس وزن‌دار با در نظر گرفتن رویکرد تنوع نرم‌افزاری پیشنهاد شده است. تنوع نرم افزاری به عنوان یک سازوکار دفاعی باعث کاهش انتشار آلودگی بدافزار در شبکه می‌شود. نتایج شبیه‌سازی عددی، تاثیر متغیرهای مختلف بر فرآیند انتشار بدافزار را نشان می‌دهد. همچنین ما نشان دادیم با تخصیص بسته‌های نرم‌افزاری متنوع به گره‌های شبکه، نسبت باز تولید کاهش می‌یابد که باعث کاهش سرعت انتشار همه‌گیری در شبکه می‌شود. بعلاوه تاثیر نمای وزن، در سرعت انتشار بدافزار مورد مطالعه قرار گرفته است.

واژگان کلیدی: انتشار بدافزار، تنوع نرم‌افزاری، شبکه بی‌مقیاس وزن‌دار.

۱- مقدمه

بدافزارها (نظیر کرم‌ها[1]، ویروس‌ها[2] وبات‌نت‌ها[3])، تهدیدات شناخته شده امنیتی برای شبکه‌ها هستند که اثرات تخریبی بسیاری از خود به‌جای می‌گذارند و حداقل یکی از سه اصل امنیتی را تحت حمله قرار می‌دهند (محرمانگی[4]، جامعیت[5] و دسترس‌پذیری[6]) [۱]. برای ابداع تدابیر دفاعی و پیشگیرانه، مطالعه رفتار انتشاری بدافزارها الزامی است. در این راستا مدل‌های همه‌گیری شناختی مطرح شده در حوزه بیماری‌های واگیردار مانند مستعد-آلوده (SI[7])، مستعد-آلوده- مستعد (SIS[8]) و مستعد-آلوده-بازیابی‌شده (SIR[9]) جهت مطالعه رفتار پویای انتشار بدافزارها مورد استفاده قرار گرفته است [۳،۲]. در مدل‌های همه‌گیری شناختی موجود از انتشار بدافزار، اثر تنوع نرم‌افزاری[10] در نظر گرفته نشده است. تنوع نرم‌افزاری هزینه حمله کننده را افزایش می‌دهد و باعث کاهش نرخ انتشار آلودگی می‌شود.

آسیب‌پذیری‌های مشترک در نرم‌افزارهای مشابه، منجر به گسترش انتشار بدافزارها می‌شود. تنوع نرم‌افزاری به‌عنوان یک سازوکار دفاعی مؤثر مورد توجه واقع شده است. تنوع نرم‌افزاری عبارت است از تولید انواع مختلفی از نرم‌افزار که از نظر رفتاری (معنایی) معادل هستند، ولی از لحاظ ساختاری با یکدیگر متفاوتند [۴]. اغلب شبکه‌ها به اجرای نرم‌افزارهای مشابه می‌پردازند که این موضوع به عنوان عدم تنوع (تک‌محصولی[11]) شناخته می‌شود [۵]. تنوع نرم‌افزاری منجر به کاهش آسیب‌پذیری‌های مشترک و کاهش اثرات عدم تنوع می‌شود. این روش همچنین، مقاومت شبکه‌ها را در

* رایانامه نویسنده مسئول: so_hosseini@uk.ac.ir

1- Worm
2- Virus
3- Botnet
4- Confidentiality
5- Integrity
6- Availability
7- Susceptible–Infected
8- Susceptible–Infected–Susceptible
9- Susceptible–Infected–Recovered
10- Software Diversity
11- Monoculture

برابر حملات بدافزارها افزایش می‌دهد و منجر به پایداری شبکه می‌شود.

مطالعات اخیر نشان داده است که اکثر شبکه‌های دنیای واقعی مانند اینترنت، شبکه‌های اجتماعی، بیولوژیکی و سامانه‌های ارتباطی دارای خصوصیات ساختاری مشترکی مانند توزیع درجه بی‌مقیاس، خاصیت دنیای کوچک[1] و خاصیت غیریکنواختی[2] هستند [۷-۶]. این شبکه‌ها اغلب به عنوان شبکه‌های بی‌مقیاس[3] شناخته می‌شوند. در بسیاری از شبکه‌های دنیای واقعی، یکی از مهم‌ترین خصوصیات، وزن است. به عنوان نمونه در اینترنت، وزن، به وسیله جریان ترافیک و یا پهنای باند مسیریاب‌ها معین می‌شود [۸]. در مطالعات همه گیری شناختی، وزن به عنوان میزان ارتباط بین گره‌ها تعیین می‌شود. همبندی شبکه نقش مهمی در انتشار آلودگی دارد. همچنین غیریکنواختی در شبکه بی‌مقیاس در تعداد ارتباطات و در وزن پیوندها مشاهده می‌شود.

مدل‌سازی انتشار بدافزارها در شبکه‌های بی‌مقیاس به ما کمک می‌کند تا فهم دقیق‌تری از پویایی انتشار بدافزارها داشته باشیم و روش‌های دفاعی مناسبی را ارائه دهیم. اکثر کارهای انجام‌شده به مدل‌سازی انتشار بدافزارها، بدون در نظر گرفتن سازوکارهای دفاعی مؤثر پرداخته‌اند و روش تنوع نرم‌افزاری در شبکه‌ها، به عنوان یک سازوکار دفاعی مؤثر لحاظ نشده است. اکثر کارهای انجام شده با معین نمودن نقاط دفاعی و استفاده از راهبردهای مصون‌سازی انجام شده است [۹].

در این مقاله، بر اساس مدل همه‌گیری مستعد- در معرض آلودگی- آلوده- بازیابی شده- مستعد (SEIRS[4]) به مدل‌سازی انتشار بدافزار در شبکه بی‌مقیاس وزن‌دار می‌پردازیم. و تاثیر وزن روی مدل انتشار بدافزار را مورد مطالعه قرا می‌دهیم. همچنین با اعمال سازوکار دفاعی تنوع نرم‌افزاری روی گره‌های شبکه، قصد کنترل و توقف انتشار بدافزارها را در شبکه وزن‌دار داریم. مدل پیشنهاد شده به صورت تحلیلی حل می‌شود و رفتار پویای مدل مورد ارزیابی قرار می‌گیرد.

در ادامه مقاله، در بخش دوم، کارهای انجام‌شده شرح داده می‌شوند. در بخش سوم، مدل پیشنهادی انتشار بدافزار در شبکه بی‌مقیاس وزن‌دار با اعمال تنوع نرم‌افزاری معرفی می‌شود. همچنین تحلیل پویایی انتشار بدافزار بررسی می‌شود. در بخش چهارم، نتایج شبیه‌سازی‌های عددی نشان داده شده است و در نهایت در بخش پنجم به جمع‌بندی و کارهای آتی می‌پردازیم.

۲- کارهای مرتبط

با توسعه سریع اینترنت و شبکه‌های ارتباطی، انتشار بدافزارها به یک چالش جدی امنیتی تبدیل شده است. مالکان داده‌ها و مدیران شبکه‌ها برای پیشگیری از انتشار بدافزارها و مبارزه با آن‌ها هزینه‌های سنگینی می‌پردازند. انواع بدافزارها مانند بات‌نت‌ها از لحاظ تعداد و پیچیدگی رو به رشد هستند. بات‌نت‌ها امروزه به یکی از تهدیدهای جدی برای امنیت رایانه‌ها در فضای سایبری شناخته می‌شوند [۱۰]. آن ها شامل شبکه‌ای از میزبان‌های آلوده و در معرض خطر هستند که تحت کنترل یک حمله‌کننده یا نفوذگر قرار دارند و ریشه اولیه بسیاری از حملات و فعالیت‌های مخرب در سطح شبکه هستند. در [۱۰]، سیر مراحل تکامل این بدافزارها نشان داده شده است همچنین روش‌هایی برای تحلیل و شناسایی این بدافزارها در سطح شبکه معرفی شده است تا از اثرات مخرب آن‌ها جلوگیری نمایند. در [۱۱]، راهکاری برای تحلیل فایل‌های مخرب و مشکوک ارائه شده است تا بتواند رفتار داخلی بدافزارها را به‌طور خودکار تعیین نماید و سرعت انتشار آن‌ها را در سطح شبکه کاهش دهد.

با رشد مداوم تهدیدات بدافزارها، تامین امنیت به موضوع بسیار مهمی تبدیل شده است. نگرانی‌های امنیتی به‌واسطه به‌اشتراک‌گذاری آسیب‌پذیری‌های مشترک در نرم‌افزارهای مشابه و در نتیجه گسترش بدافزارها باعث شده است تا تنوع نرم‌افزاری به عنوان یک اصل دفاع سایبری در شبکه‌های کلان مقیاس مورد توجه قرار گیرد [۱۲].

هنگامی‌که رویکردهای مبتنی بر تنوع نرم‌افزاری برای مسائل امنیتی مطرح می‌شود، به دنبال کاهش آسیب‌پذیری‌های مشترک در شبکه هستیم. در نتیجه، برای حمله کننده، طراحی یک حمله منحصربه‌فرد که قادر به بهره‌برداری از آسیب‌پذیری‌های مشترک بین گره‌های شبکه باشد، بسیار دشوار می‌شود. بنابراین، مقاومت این سامانه‌ها در برابر حملات اینترنتی افزایش می‌یابد. یکی از اولین فنون تنوع نرم‌افزاری، برنامه نویسی N-نگارشی است که N نگارش مختلف از یک نرم‌افزار مشابه توسط N تیم برنامه‌نویسی مختلف با الگوریتم‌های متفاوت پیاده‌سازی می‌شود تا آسیب‌پذیری‌های مشترک به حداقل برسد [۱۳]. اما از آنجایی‌که توسعه و نگهداری نگارش‌های مختلف هزینه بسیار بالایی دارد این روش عملا قابل

1- Small-World
2- Heterogeneity
3- Scale-Free Network
4- Susceptible–Exposed–Infected–Recovered–Susceptible

استفاده نیست.روش‌هایی که تنوع را به‌طور خودکار اعمال می‌کنند مطلوب‌تر هستند. بنابراین امروزه تبدیل برنامه به‌طور خودکار مانند تصادفی سازی کد[1]، تصادفی‌سازی مجموعه دستورالعمل‌ها[2] و تصادفی‌سازی فضای آدرس[3] به عنوان روش‌های تنوع نرم‌افزاری مورد توجه قرار گرفته است [۱۴]. تنوع نرم‌افزاری را می‌توان در بسته‌های نرم‌افزاری، سیستم عامل و یا سکوهای سخت‌افزاری اعمال کرد [۱۲]. تنوع نرم‌افزاری به عنوان یک سازوکار دفاعی موثر در کاهش انتشار همه‌گیری نقش دارد [۱۲]. در کارهای انجام شده برای مدل‌سازی انتشار بدافزار بر اساس مدل‌های همه‌گیری شناختی، سازوکار دفاعی تنوع نرم‌افزاری در نظر گرفته نشده است.

اکثر مطالعات، مدل‌سازی انتشار بدافزار را بر اساس مدل‌های همه‌گیری شناختی انجام داده‌اند. در این مدل‌ها، طی فرآیند انتشار همه‌گیری، گره‌ها در یکی از حالات مستعد[4] (S)، در معرض آلودگی[5] (E)، آلوده[6] (I) و بازیابی شده[7] (R) قرار می‌گیرند [۱۵-۱۷]. در حالت مستعد، گره‌ها آسیب‌پذیر به آلودگی هستند ولی هنوز آلوده نشده‌اند. در حالت در معرض آلودگی، گره‌های مستعد بوسیله همسایه آلوده خود، آلوده شده‌اند ولی آلودگی را منتشر نکرده‌اند به عبارتی غیرفعال هستند. در حالت آلوده، گره‌های آلوده شده قادر به حمله به همسایگان مستعد خود هستند و آلودگی را منتشر می‌کنند. در حالت بازیابی شده، با اعمال نرم‌افزارهای ضد ویروس و سامانه‌های تشخیص نفوذ، گره‌های آلوده بازیابی می‌شوند و دیگر قادر به آلوده‌سازی نیستند. بنابراین، اغلب مدل‌های همه‌گیری شناختی رایج عبارتند از مدل SI، مدل SIS و مدل SIR.

انتشار بدافزارها در شبکه‌های پیچیده، مخصوصاً شبکه‌های بی‌مقیاس تهدید بزرگی برای امنیت این شبکه‌ها محسوب می‌شوند. شبکه بی‌مقیاس به عنوان مدلی عمومی برای بسیاری از شبکه‌های اجتماعی، فناورانه و سامانه‌های زیستی استفاده می‌شوند. این شبکه‌ها دارای خصوصیات ساختاری مشترکی مانند توزیع درجه بی‌مقیاس، خاصیت دنیای کوچک (ضریب خوشه‌بندی بالا و میانگین فاصله کم) و ساختار انجمنی هستند [۱۸]. این شبکه‌ها با تعیین تعاملات بین گره‌ها روی روند انتشار آلودگی در شبکه بی‌مقیاس تأثیر می‌گذارند. در[۱۹]، رفتار انتشار بدافزارها در شبکه بی‌مقیاس مورد مطالعه قرار گرفته است. نتایج نشان می‌دهد که شبکه‌های بی‌مقیاس نسبت به انتشار بدافزارها آسیب‌پذیری بیشتری دارند.

در شبکه‌های بی‌مقیاس وزن‌دار، جزئیات فرآیند انتشار همه‌گیری در شبکه‌های بی‌مقیاس، با وزنی که به پیوندها داده می‌شود مورد بررسی قرار می‌گیرد. مدل‌های شبکه‌ای وزن‌دار گوناگونی برای توصیف رفتار سامانه‌های پیچیده پیشنهاد شده است[۲۰-۲۳]. در [۲۰]، سه مدل اصلاح شده SIS در شبکه‌های بی‌مقیاس وزن‌دار معرفی شده است. پویایی و تکامل وزن و درجه به‌طور سراسری در طول زمان در نظر گرفته شده است. در [۲۱]، انتشار همه‌گیری در مدل SIR روی شبکه بی‌مقیاس وزن‌دار با در نظر گرفتن آلودگی‌های غیرخطی پیشنهاد شده است. در [۲۲]، پویایی وزن در شبکه بی‌مقیاس وزن‌دار مورد مطالعه قرار گرفته است. پویایی وزن به‌طور محلی در طول زمان در نظر گرفته می‌شود به‌عبارتی وزن یال‌های مرتبط با گره مورد نظر افزایش داده می‌شود و وزن بقیه یال‌ها تغییر نمی‌کند که اصطلاحاً تکامل وزن به‌طور محلی انجام شده است. در [۲۳]، رفتار پویای مدل همه‌گیری SIRS در شبکه پیچیده وزن‌دار مطالعه شده است. نتایج نشان داده است که غیریکنواختی توزیع وزن تاثیر قابل توجهی روی آستانه همه‌گیری و سرعت انتشار بدافزار دارد.

۳- مدل پیشنهادی انتشار بدافزار در شبکه بی‌مقیاس وزن‌دار

در این بخش به مدل‌سازی و تحلیل مدل انتشار همه‌گیری پیشنهاد شده در شبکه بی‌مقیاس وزن‌دار با تخصیص تنوع نرم‌افزاری به گره‌های شبکه می‌پردازیم. برای بررسی پویایی انتشار بدافزارها در شبکه‌های کلان مقیاس، سیستم را مبتنی بر یک مدل تحت آزمایش قرار می‌دهیم. برای این منظور، یک مدل ریاضی از سیستم ایجاد کرده و سپس به حل تحلیلی و شبیه‌سازی آن پرداخته می‌شود. با مقایسه نتایج حل عددی مدل تحلیلی و خروجی مدل شبیه‌سازی، صحت مدل تحقیق می‌شود. در مدل پیشنهادی انتشار بدافزار، گرافی را با N گره از C نوع مختلف (C>=1) در نظر می‌گیریم. به عبارتی با تخصیص C بسته نرم‌افزای متنوع به گره‌های شبکه، گره‌هایی با انواع متفاوت داریم، بسته‌های نرم‌افزاری متنوع دارای عملکرد یکسان هستند ولی کدهای دودویی متفاوتی دارند که مانع از انتشار بدافزارها می‌شوند. در C=1 تنوع نرم‌افزاری وجود

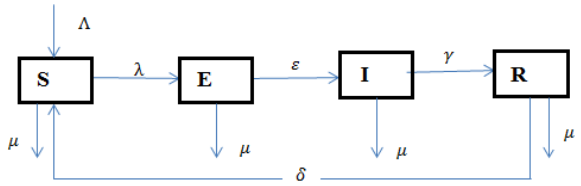
1- Code Randomization
2- Instruction Set Randomization(ISR)
3- Address Space Randomization(ASR)
4- Susceptible
5- Exposed
6- Infected
7- Recovered

ندارد به‌عبارتی، گره‌هایی که نوع یکسان دارند آسیب‌پذیری‌های مشترک در آنها مانند سرریز بافر[1] منجر به گسترش بدافزارها می‌شود. C به‌عنوان معیار تنوع در نظر گرفته شده است $c=1,2,3\ldots,C$. هر گره آلوده از نوع c، همسایه مستعد خود از همان نوع را آلوده می‌کند. تخصیص بسته‌های نرم‌افزاری متنوع به گره‌های شبکه بر اساس الگوریتم رنگ‌آمیزی تصادفی انجام شده است [۲۴]. هر رنگ تخصیص داده شده به گره‌ها معادل با یک بسته نرم‌افزاری متنوع است.

در چارچوب مدل‌سازی پیشنهادی، گره‌ها در طی انتشار بدافزها (کرم‌ها یا ویروس‌ها) در یکی از حالت‌های مستعد، در معرض آلودگی، آلوده و بازیابی شده قرار می‌گیرند:

- $S_{k,c}(t)$ برابر است با چگالی افراد مستعد با درجه k و نوع c در زمان t. ($k=1,2,\ldots n$ که n برابر با حداکثر درجه شبکه است.)
- $E_{k,c}(t)$ برابر است با چگالی افراد در معرض آلودگی با درجه k و نوع c در زمان t.
- $I_{k,c}(t)$ برابر است با چگالی افراد آلوده با درجه k و نوع c در زمان t.
- $R_{k,c}(t)$ برابر است با چگالی افراد مصون و یا بازیابی شده با درجه k و نوع c در زمان t.

نمودار انتقال آلودگی بین حالت‌های S, E, I و R در مدل جدید پیشنهاد شده مطابق شکل زیر است:



شکل (۱): نمودار انتقال حالت مدل انتشار بدافزار SEIRS

همان‌طور که در شکل (۱) نشان داده شده است، زمانی‌که گره مستعد از نوع c، تحت حمله همسایه آلوده خود از همان نوع قرار می‌گیرد مستقیماً به حالت آلوده نمی‌رود بلکه ابتدا به حالت در معرض آلودگی می‌رود و پس از آن بعد از سپری شدن زمان معین، آلوده می‌شود. گره آلوده با استفاده از نرم‌افزارهای ضد ویروس بازیابی می‌شود و دیگر قادر به آلوده‌سازی نیست. همچنین گره‌های بازیابی شده با نصب مجدد سیستم عامل می‌توانند مجدداً به حالت مستعد وارد شوند و این روند ادامه داده می‌شود.

1- Buffer-overflow

متغیرهای مدل به صورت زیر تعریف می‌شوند:

λ: متناسب با نرخ انتشار آلودگی است

ε: نرخ از بین رفتن زمان نهفتگی برای گره‌های نهفته و یا در معرض آلودگی است.

γ: متناسب با نرخ بازیابی از آلودگی است.

δ: نرخ از بین رفتن گره‌های بازیابی شده است.

Λ : نرخ الحاق گره جدید به شبکه است. گره جدید در حالت مستعد قرار می‌گیرد.

μ: برابر است با نرخ مرگ (نرخ ترک کردن از شبکه) که در هریک از حالات S,E,I و R ممکن است رخ دهد.

C: تعداد بسته‌های نرم‌افزاری متنوع است هرچه تعداد بسته‌های نرم‌افزاری تخصیص داده شده به گره‌های شبکه بیشتر باشد احتمال آلودگی کمتر است.

مدل جدید پیشنهاد شده بر اساس معادلات دیفرانسیل به صورت زیر است:

$$\begin{aligned}
\frac{dS_{k,c}(t)}{dt} &= \Lambda - kS_{k,c}(t)\theta(t) + \delta R_{k,c}(t) - \mu S_{k,c}(t).\\
\frac{dE_{k,c}(t)}{dt} &= -\varepsilon E_{k,c}(t) + kS_{k,c}(t)\theta(t) - \mu E_{k,c}(t).\\
\frac{dI_{k,c}(t)}{dt} &= \varepsilon E_{k,c}(t) - \gamma I_{k,c}(t) - \mu I_{k,c}(t).\\
\frac{dR_{k,c}(t)}{dt} &= \gamma I_{k,c}(t) - \delta R_{k,c}(t) - \mu R_{k,c}(t).
\end{aligned} \qquad (۱)$$

که $\theta(t) = \frac{\sum_{k=m}^{\infty}(k/c)\varphi(k)P(k)\ \lambda_{hk} I_{k,c}(t)}{<k>/c} = \frac{\alpha}{c<k>}\sum_k k\,P(k)\,\lambda_{hk} I_{k,c}(t)$

$kS_{k,c}(t)\theta(t)$ برابر با گره‌های آلوده شده جدید با درجه k در واحد زمان است. $\theta(t)$: احتمال انتقال آلودگی از طریق ارتباط با گره آلوده است. $\varphi(k) = \alpha k$ برابر با آلودگی گره‌ای با درجه k است. که α آلودگی گره‌های آلوده با درجه‌های مختلف را نشان می‌دهد و مقدار آن بین صفر و یک است. λ_{hk} نرخ انتقال آلودگی از گره آلوده با درجه h به گره مستعد با درجه k است. از آنجاکه گره آلوده از نوع c فقط می‌تواند گره مستعد از همان نوع را آلوده کند (به دلیل آسیب‌پذیری مشترک)، نرخ انتشار آلودگی برابر است با λ/c.

در این مقاله، به مدل‌سازی انتشار بدافزار در شبکه بی‌مقیاس وزن‌دار می‌پردازیم. با توجه به الگوهای متفاوت وزن در شبکه‌های پیچیده، استفاده از درجه گره‌ها برای توصیف وزن یک یال، مورد توجه قرار گرفته است. به عبارتی وزن بین دو گره با درجه k و h به صورت تابعی از درجه آنها تعریف می‌شود $w_{kh} = w_0\,(kh)^{\beta}$. متغیر w_0 و نمای β وابسته به نوع شبکه پیچیده است. به عنوان نمونه، در شبکه متابولیک $\beta = 0.5$، در شبکه فرودگاه‌های آمریکا $\beta = 0.8$

است [۲۵]. به طور کلی β یک متغیر قابل تنظیم است. در اینجا $w_0 = 1$ در نظر گرفته شده است. همان‌طور که ذکر شد وزن w_{kh} مرتبط با یک یال است، به طور مشابه برای یک گره با درجه k، قدرت آن برابر با مجموع وزن یال‌های متصل به آن گره است. به عبارتی قدرت گره با درجه k برابر است با $\chi_k = \sum_{h\epsilon v(k)} w_{kh} = k\sum_h P(h|k)w_{kh}$. در این مقاله $P(h|k) = \frac{hP(h)}{<k>}$ است.

برای هر گره با درجه k، نرخ انتقال آلودگی برابر با $\frac{\lambda k}{c}$ است . با تخصیص c بسته نرم‌افزاری متنوع به گره‌های شبکه، انتشار آلودگی کاهش می‌دهیم. با در نظر گرفتن متنوع‌سازی، انجام حمله برای حمله‌کننده بسیار دشوار است زیرا حمله‌کننده قادر به بهره‌برداری از آسیب‌پذیری‌های مشترک بین گره‌ها نیست. همچنین نرخ انتقال برای یک یال، از یک گره با درجه k به گره دیگر با درجه h، متناسب است با وزن آن یال به قدرت گره با درجه k است.

از آنجاکه $w_{kh} = w_0\,(kh)^{\beta}$ و $\chi_k = k\sum_h P(h|k)w_{kh}$

بنابراین:

$$\lambda_{hk} = \frac{\lambda h}{c}\,\frac{w_{hk}}{\chi_h} \qquad (۲)$$

احتمال این‌که گره مستعد با درجه k در زمان t به‌وسیله همسایه آلوده‌اش (v_h) با درجه h، آلوده شود برابر است با: $\rho(t) = 1 - \prod_{h\epsilon v_h^{infectious}}(1-\lambda_{hk})$.

با در نظرگرفتن معادله (۲)، معادلات دیفرانسیل مدل (۱) مجدداً بازنویسی می‌شوند.

$$\begin{aligned}
&\frac{dS_{k,c}(t)}{dt} = \\
&\Lambda - \lambda_{hk}\alpha\, S_{k,c}(t)\theta(t) + \delta R_{k,c}(t) - \mu\, S_{k,c}(t).\\
&\frac{dE_{k,c}(t)}{dt} = -\varepsilon E_{k,c}(t) + \lambda_{hk}\alpha\, S_{k,c}(t)\,\theta(t) - \\
&\mu E_{k,c}(t).\\
&\frac{dI_{k,c}(t)}{dt} = \varepsilon E_{k,c}(t) - \gamma\, I_{k,c}(t) - \mu\, I_{k,c}(t). \qquad (۳)\\
&\frac{dR_{k,c}(t)}{dt} = \gamma\, I_{k,c}(t) - \delta\, R_{k,c}(t) - \mu R_{k,c}(t).
\end{aligned}$$

که $\theta(t) = \frac{1}{<k>}\sum_k k\,P(k)\,I_{k,c}(t)$.

شرایط اولیه برای مدل همه‌گیری پیشنهاد شده شامل:

$$0 \le S_{k,c}(0), E_{k,c}(0), I_{k,c}(0), R_{k,c}(0) \le 1, \qquad (۴)$$

شرایط مدل‌سازی برابراست با:

$$\begin{aligned}
&S_{k,c}(0) = 1 - E^0_{k,c} - I^0_{k,c} - R^0_{k,c} \ge 0\,,\\
&E_{k,c}(0) = E^0_{k,c} \ge 0,\; I_{k,c}(0) = I^0_{k,c} \ge 0, \qquad (۵)\\
&R_{k,c}(0) = R^0_{k,c} \ge 0
\end{aligned}$$

۳-۱- مفروضات مدل

مسئله مهم در انواع مدل‌ها، پیش‌فرض‌هایی است که برای ساده‌نمودن مسئله و قابل حل نمودن آن‌ها صورت می‌پذیرد. هنر مدل‌سازی در حذف متغیرهایی است که کمترین تاثیر را بر رفتار سامانه داشته و حذف آن‌ها در ساده‌سازی معادلات مدل نقش اساسی دارد. پیش‌فرض‌ها عموما مانع از ورود به مباحث حل معادلات دیفرانسیل غیرخطی در مدل‌های زمان پیوسته و معادلات تفاضلی غیرخطی در مدل‌های زمان گسسته می‌شود.

در مدل‌سازی انتشار بدافزار در شبکه بی‌مقیاس وزن‌دار مبتنی بر متنوع‌سازی نرم‌افزار می‌توان فرضیات زیر را در نظر گرفت:

- همبندی شبکه بر اساس شبکه بی‌مقیاس باراباسی-آلبرت با در نظر گرفتن ویژگی خوشه‌بندی است.
- تخصیص بسته‌های نرم‌افزاری متنوع به گره‌های گراف بر اساس الگوریتم رنگ‌آمیزی تصادفی انجام می‌شود.
- بسته‌های نرم‌افزاری متنوع بر اساس روش تبدیل برنامه به طور خودکار ایجاد شده‌اند.
- جمعیت کل گره‌های شبکه، ثابت و برابر با هزار گره است (N=1000).
- در ابتدا، تمام گره‌ها آسیب‌پذیر هستند ($S_{k,c}(0)$=900) به غیر از تعدادی گره آلوده اولیه ($I_{k,c}(0)$=100)، انتخاب گره‌های آلوده اولیه، راهبرد حمله را معین می‌کند. اگر به صورت تصادفی انتخاب شوند تا فرآیند انتشار را آغاز نمایند یعنی راهبرد حمله به صورت پیش‌فرض تصادفی است.
- تغییر پویایی همبندی شبکه در طول فرآیند انتشار در نظر گرفته می‌شود و نرخ مرگ برابر با نرخ تولد است ($\Lambda = \mu$).
- برای افزایش دقت شبیه‌سازی، هر آزمایش ده بارتکرار شده است و میانگین نتایج آنها به عنوان جواب نهایی در نظر گرفته شده است.

۳-۲- تحلیل مدل پیشنهادی *SEIRS*

در این بخش به تحلیل پویایی مدل انتشار همه‌گیری SEIRS می‌پردازیم. یکی از مفاهیم مهم در همه‌گیری، نسبت باز تولید[1] (R_0) است که برابر با میانگین تعداد آلودگی‌های ثانویه ناشی شده از یک آلودگی اولیه، در طول چرخه حیات آلودگی است [۲۶]. با توجه به آستانه نسبت بازتولید، رفتار پویای مدل بررسی می‌شود و

1- Reproductive Ratio

معین می‌کنیم که آیا همه‌گیری در شبکه رخ داده است یا خیر. به‌طور کلی، اگر مقدار R_0 کمتر از یک باشد آنگاه آلودگی بدافزار در شبکه از بین رفته است. در غیر این صورت، اگر مقدار R_0 بزرگتر از یک باشد آنگاه آلودگی بدافزار در شبکه پایدار است و همه‌گیری رخ داده است [۲۷].

قضیه ۱:

اگر $R_0<1$ باشد آنگاه آلودگی هر گره جدید از میانگین تعداد آلودگی‌های ثانویه کمتر است و مدل (۳) به یک نقطه تعادل فاقد آلودگی بدافزار می‌رسد در وضعیت $E_0\{(S_{k,c}^{\infty}, E_{k,c}^{\infty}, I_{k,c}^{\infty}, R_{k,c}^{\infty}) =$ $\{(1,0,0,0)$ یک نقطه تعادل فاقد بدافزار[1] داریم.

اگر $R_0>1$ باشد آنگاه آلودگی در مدل (۳) منتشر می‌شود و به یک تعادل در همه‌گیری می‌رسیم (حالت پایدار در همه‌گیری[2]) $E_1\{(S_{k,c}^{\infty}, E_{k,c}^{\infty}, I_{k,c}^{\infty}, R_{k,c}^{\infty}) = (S_{k,c}^{*}, E_{k,c}^{*}, I_{k,c}^{*}, R_{k,c}^{*})\}$

اثبات:

برای پیدا کردن نقاط تعادل، حالت پایدار مدل (۳) را در نظر می‌گیریم و سمت راست معادلات مدل (۳) را برابر با صفر قرار می‌دهیم.

$$\frac{dS_{k,c}(t)}{dt}=0, \frac{dE_{k,c}(t)}{dt}=0, \frac{dI_{k,c}(t)}{dt}=0, \frac{dR_{k,c}(t)}{dt}=0, \quad (۶)$$

در وضعیت فاقد آلودگی بدافزار و در حالت پایدار مقادیر $E_{k,c}^{\infty}, I_{k,c}^{\infty}, R_{k,c}^{\infty}$ برابر با صفر است و از آنجاکه نرخ مرگ برابر با نرخ تولد است $(\Lambda = \mu)$ بنابراین، $S_{k,c}^{\infty}=1$ است. همچنین با محاسبات ساده، نقاط تعادل در حالت پایدار در همه‌گیری نیز به‌دست می‌آید.

$$\begin{aligned} E^{\infty} &= \frac{(\gamma+\mu)}{\varepsilon} I^{\infty}, \\ I^{\infty} &= \frac{\frac{\lambda_{hk}}{c<k>}\alpha \sum_k k\, p(k) I^{\infty}}{(\mu+\varepsilon)\times\frac{(\gamma+\mu)}{\varepsilon}+[1+\frac{(\gamma+\mu)}{\varepsilon}+\frac{\gamma}{\delta+\mu}]\frac{\lambda}{c<k>}\alpha \sum_k k\, p(k) I^{\infty}}, \\ R^{\infty} &= \frac{\gamma}{\delta+\mu} I^{\infty}. \\ S^{\infty} &= 1 - E^{\infty} - I^{\infty} - R^{\infty}. \end{aligned} \quad (۷)$$

بعد از پیدا کردن نقاط تعادل در دو حالت فاقد آلودگی بدافزار و پایدار در همه‌گیری، حال باید نسبت بازتولید یا R_0 را محاسبه نماییم. در این مقاله، برای محاسبه R_0 از روش نسل-بعد[3] استفاده می‌کنیم [۲۸]. نسبت بازتولید یا R_0 بوسیله شعاع طیفی عملگر نسل-بعد به‌دست می‌آید $R_0 = \rho(FV^{-1})$. شعاع طیفی ماتریس G برابر با $\rho(G)$ است. ماتریس F، حالت آلوده جدید را معین می‌کند و ماتریس V برابر با انتقال آلودگی و از بین رفتن آلودگی، بین دو حالت آلوده و در معرض آلودگی را نشان می‌دهد.

$$F=\left[\frac{\partial F_i(E_0)}{\partial x_j}\right], \qquad V=\left[\frac{\partial V_i(E_0)}{\partial x_j}\right]. \quad (۸)$$

برای محاسبه نسبت بازتولید یا R_0 براساس ماتریس نسل-بعد، باید دو حالت در معرض آلودگی و آلوده از مدل (۳) را در نظر بگیریم.بنابراین معادلات دیفرانسیل دو حالت $E_{k,c}(t)$ و $I_{k,c}(t)$ از مدل (۳) برابر است با:

$$\begin{aligned} &\frac{dE_{k,c}(t)}{dt} = \\ &-\varepsilon E_{k,c}(t) + \frac{\lambda_{hk}}{c<k>}\alpha k S_{k,c}(t)\sum_k k\, p(k)\, I_{k,c}(t) - \\ &\mu E_{k,c}(t). \\ &\frac{dI_{k,c}(t)}{dt} = \varepsilon E_{k,c}(t) - \gamma\, I_{k,c}(t) - \mu\, I_{k,c}(t). \end{aligned} \quad (۹)$$

با توجه به معادلات (۸) و (۹) ماتریس F و V در نقطه تعادل فاقد آلودگی بدافزار (E_0) محاسبه می‌شوند:

$$F=\begin{bmatrix}0 & 0\\ A & 0\end{bmatrix}_{E_0} \quad V=\begin{bmatrix}\mu+\varepsilon & -\varepsilon\\ 0 & \gamma+\mu\end{bmatrix}_{E_0}. \quad (۱۰)$$

که $A=\frac{\lambda_{hk}\,\alpha}{c<k>} S_{k,c}^{\infty} \begin{bmatrix}1\\2\\\vdots\\n\end{bmatrix}[1\,P(1),\quad 2\,P(2),\quad \ldots,\quad n\,P(n)]$

و در E_0، $S_{k,c}^{\infty}=1$ است.

سپس به محاسبه ماتریس معکوس V می‌پردازیم که برابر است با:

$$V^{-1}=\begin{bmatrix}\frac{-1}{\mu+\varepsilon} & \frac{\varepsilon}{(\gamma+\mu)(\mu+\varepsilon)}\\ 0 & \frac{1}{\gamma+\mu}\end{bmatrix}. \quad (۱۱)$$

در نهایت ماتریس نسل-بعد $G=FV^{-1}$ محاسبه می‌شود:

$$G=FV^{-1}=\begin{bmatrix}0 & 0\\ \frac{-A}{(\mu+\varepsilon)} & \frac{A\,\varepsilon}{(\gamma+\mu)(\mu+\varepsilon)}\end{bmatrix}. \quad (۱۲)$$

از آنجاکه محاسبه نسبت بازتولید یا R_0 برابر با شعاع طیفی ماتریس G است بنابراین:

$$R_0=\rho(FV^{-1})=\frac{\varepsilon A}{(\gamma+\mu)(\mu+\varepsilon)}. \quad (۱۳)$$

با جایگزینی مقدار A در (۱۳)، مقدار R_0 بدست می‌آید.

$$\begin{aligned} R_0 &= \\ &\frac{\varepsilon\,\alpha}{(\gamma+\mu)(\mu+\varepsilon)}\frac{\lambda_{hk}}{c<k>}\begin{bmatrix}1P(1) & 2P(2) & \ldots. & nP(n)\\ 2P(2) & 2^2P(2) & \ldots.. & 2nP(n)\\ \vdots\ \vdots & \vdots\ \vdots & \vdots\ \vdots & \vdots\ \vdots\\ nP(1) & 2nP(2) & \ldots\ \ldots & n^2P(n)\end{bmatrix}, \\ \Rightarrow\ R_0 &= \frac{\varepsilon\,\alpha}{(\gamma+\mu)(\mu+\varepsilon)}\frac{\lambda<g(k)k^2>}{c<g(k)k>}. \end{aligned} \quad (۱۴)$$

■

1- Malware-Free Equilibrium
2- Endemic Equilibrium
3- Next-generation

بر اساس قضیه ۱ و با توجه به معادله (۱۴)، تعداد بسته‌های نرم‌افزاری متنوعی که مورد نیاز است تا همه‌گیری در شبکه رخ ندهد برابر است با :

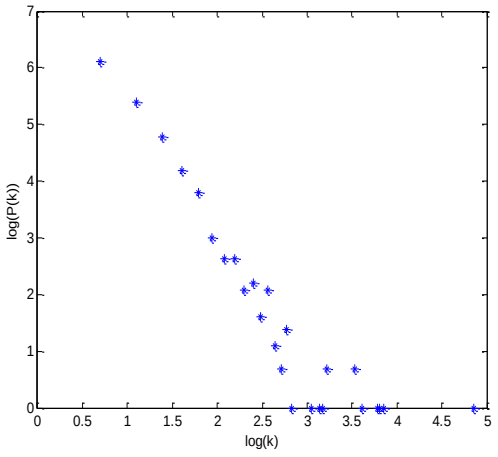
$$R_0 = \frac{\varepsilon\,\alpha}{(\gamma+\mu)(\mu+\varepsilon)}\ \frac{\lambda<g(k)k^2>}{c<g(k)k>} < 1,$$

$$\Rightarrow C_{critical} = \left[\frac{\varepsilon\,\alpha}{(\gamma+\mu)(\mu+\varepsilon)}\ \frac{\lambda<g(k)k^2>}{c<g(k)k>}\right], \qquad (۱۵)$$

با تخصیص بسته‌های نرم‌افزاری متنوع $(C_{critical})$ به گره‌های شبکه بی‌مقیاس وزن دار، از انتشار آلودگی بدافزار به بخش‌های دیگر جلوگیری کرده و تضمین می‌کنیم که آلودگی بدافزار تبدیل به همه‌گیری در شبکه نشود.

۴- شبیه‌سازی عددی

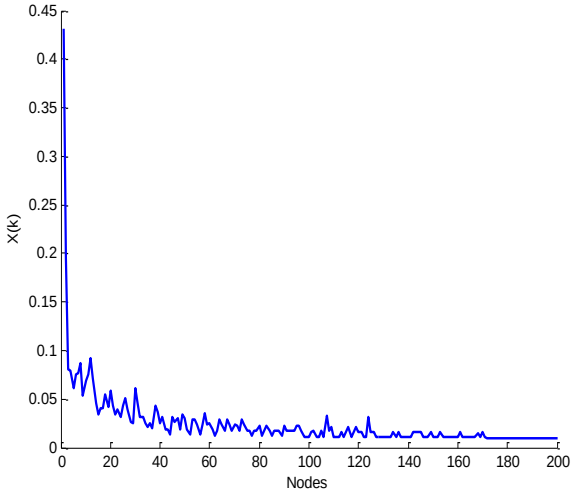
در این بخش با استفاده از نتایج شبیه‌سازی عددی، پویایی مدل انتشار همه‌گیری نمایش داده می‌شود. با استفاده از الگوریتم رشد و اتصال ترجیهی، مدل شبکه ای باراباسی-آلبرت ایجاد می‌شود [۲۹]. با هدف کاهش انتشار همه‌گیری، بسته‌های نرم‌افزاری متنوع به گره‌های شبکه بی‌مقیاس وزن‌دار تخصیص داده شده است. در شبکه‌هایی با ساختار بی‌مقیاس وزن‌دار، اتصال ترجیحی قدرت و پویایی وزن را در نظر می‌گیریم. گره جدید با اتصال ترجیحی به گره‌ای با قدرت بیشتر، به شبکه اضافه می‌شود، به گونه‌ای که توزیع درجه، توزیع قدرت و توزیع وزن به صورت توزیع قانون توان است. شبیه‌سازی‌های انجام شده مبتنی بر مدل شبکه‌ای وزن دار باراباسی-آلبرت با ۱۰۰۰ گره است. حداقل درجه برابر با ۳ و حداکثر درجه ۱۴۹ است. شبیه‌سازی‌ها توسط نرم‌افزار متلب انجام شده است. شکل (۲) توزیع درجه قانون توان را در شبکه بی‌مقیاس باراباسی آلبرت نشان می‌دهد.



شکل (۲): توزیع قانون توان در شبکه بی مقیاس باراباسی-آلبرت با ۱۰۰۰ گره

همانطور که در شکل (۲) نشان داده شده است، احتمال اینکه گره جدید به گره i متصل شود برابر با $p(k_i) = \frac{k_i}{\sum_j k_j}$ است. که k_i برابر با درجه گره i و سیگمای مخرج برابر با جمع درجه همه گره‌هایی است که از قبل موجود هستند. در این مدل گره‌های جدید با احتمال بالاتر به گره‌های موجود با درجه بالا متّصل می‌شوند. بدین ترتیب با قانون اتّصال ترجیحی[1] درجه‌ی گره‌هایی که درجه‌ی بیشتر دارند سریع‌تر، و درجه‌ی گره‌هایی که درجه‌ی پایین‌تر دارند کندتر، رشد می‌کند لذا تعداد گره‌ها با درجه‌ی بالا بسیار کم و تعداد گره‌ها با درجه‌ی پایین بسیار زیاد خواهد شد. بنابراین نوسانات اتصالات در این شبکه‌ها بسیار بالاست و این شبکه‌ها مستعد به انتشار آلودگی بدافزار هستند.

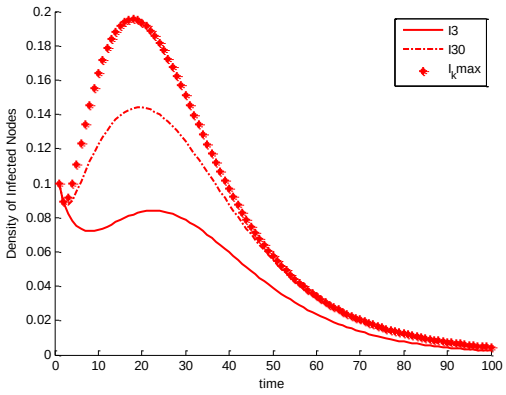
در شبکه بی مقیاس وزن دار با فرض اینکه ۲۰۰ گره داشته باشیم قدرت هر گره مطابق با شکل (۳) است. چنانچه در شکل (۳) نشان داده شده است، قدرت هر گره تابعی از درجه آن گره است (χ_k). زمانی‌که درجه یک گره بالا باشد قدرت آن نیز افزایش می‌یابد.



شکل (۳): قدرت هر گره در شبکه باراباسی-آلبرت

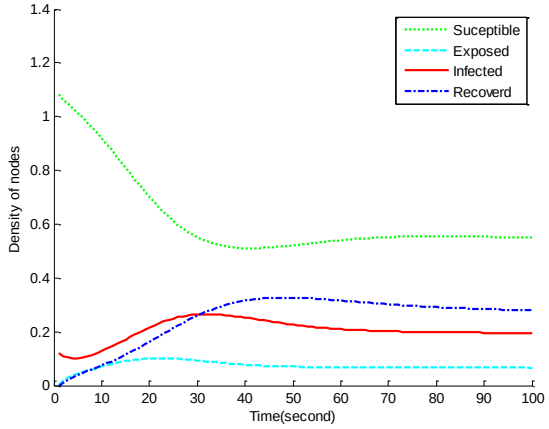
شکل (۴)، رفتار پویای گره‌ها با درجه‌های مختلف را نشان می‌دهد. همانطور که در شکل (۴) نشان داده شده است گره‌ها با درجه بالا، قدرت بالاتری دارند و بیشتر در معرض آلودگی قرار می‌گیرند و آلودگی بدافزار را با سرعت بیشتری منتشر می‌کنند. بنابراین منجر به افزایش چگالی گره‌های آلوده می‌شوند.

1- Preferential attachment



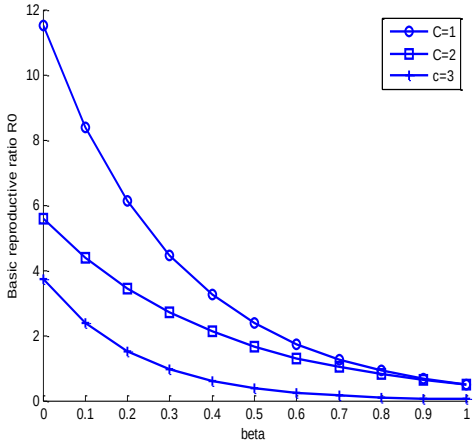
شکل (۴): چگالی گره‌های آلوده تحت درجه‌های مختلف.
$\lambda = 0.2, \varepsilon = 0.3, \gamma = 0.1, \delta = 0.01, \mu = 0.01$ و $C = 1$.

در شکل (۵) رفتار پویای مدل (۱) در شبکه بی‌مقیاس مورد بررسی قرار می‌گیرد. با در نظر گرفتن مقادیر $\lambda = 0.2, \varepsilon = 0.3, \gamma = 0.1, \delta = 0.01, \mu = 0.01$ و $C = 1$ مقدارهای $R_0 = 12.7589$ و $C_{critical} = 13$ بر اساس معادله (۱۵) به‌دست می‌آید. طبق قضیه (۱) چنانچه مقدار R_0 بزرگتر از یک باشد آلودگی بدافزار در شبکه همه‌گیر می‌شود و به حالت پایدار در آلودگی می‌رسیم. همانطور که محاسبات عددی نشان می‌دهد نیاز به تخصیص سیزده بسته نرم‌افزاری متنوع به گره‌های شبکه داریم تا بتوانیم آلودگی بدافزار را در شبکه از بین ببریم و مانع از انتشار بدافزار به گره‌های دیگر شویم.



شکل(۵): چگالی افراد مستعد، در معرض آلودگی، آلوده و مصون در شبکه بی‌مقیاس وزن دار بدون در نظر گرفتن تنوع نرم‌افزاری.
$\lambda = 0.15, \varepsilon = 0.3, \gamma = 0.1, \delta = 0.01, \mu = 0.01$ و $C = 1$.

شکل (۶) بر اساس مدل (۳) مقدار R_0 را تحت مقادیر مختلف β به ازای تعداد بسته‌های نرم‌افزاری متفاوتی که به گره‌های شبکه وزن‌دار تخصیص داده شده است را نشان می‌دهد. مقادیر متغیرها همانند شکل (۵) است. همان‌طور در شکل (۶) نشان داده شده است با افزایش مقادیر β و C مقدار R_0 کاهش می‌یابد که این نتیجه، تاثیر متغیر β و متنوع‌سازی را در کاهش انتشار آلودگی بدافزار در شبکه بی‌مقیاس وزن‌دار نشان می‌دهد.

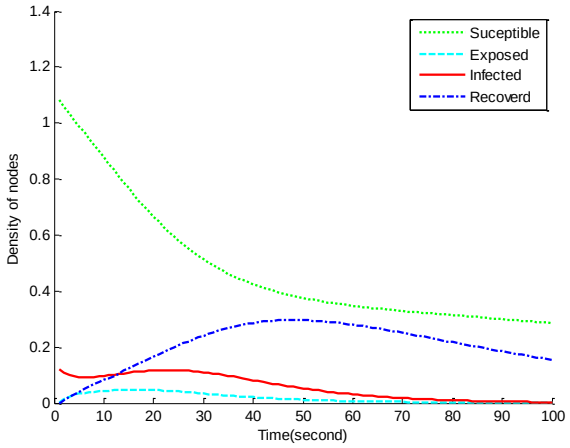


شکل(۶): نسبت بازتولید اولیه R_0 در برابر β به ازای بسته‌های نرم‌افزای مختلف $C = 1,2,3$ ، متغیرها $\lambda = 0.2, \varepsilon = 0.3, \delta = 0.01, \gamma = 0.1$ $\mu = 0.01$

همان‌طور که در شکل (۶) نشان داده شده است در حالت $C = 1$ که هیچ بسته نرم‌افزاری متنوعی به گره‌های شبکه بی‌مقیاس وزن‌دار تخصیص داده نشده است مقدار R_0 به ازای همه مقادیر β به جز $\beta = 1$، بزرگتر از یک است که طبق قضیه (۱) آلودگی بدافزار در شبکه به حالت همه‌گیری می‌رسد. با جایگزینی مقادیر متغیرها در معادله (۱۵) در $\beta = 0.3$ با عدم تنوع نرم‌افزاری ($C = 1$)، نیاز به تخصیص شش بسته نرم‌افزاری متنوع به گره‌های شبکه وزن‌دار داریم ($C_{critical} = 6$) تا تعادل فاقد آلودگی بدافزار طبق قضیه (۱) نتیجه شود. در $\beta = 0.3$ و $C = 2$ نیاز به تخصیص دو بسته نرم‌افزاری دیگر داریم تا $R_0 < 1$ شود به عبارتی $C_{critical}$ برابر چهار بسته نرم‌افزاری محاسبه شده است. در $\beta = 0.3$ و $C = 3$ مقدار R_0 برابر با ۰/۹۲۴۳۸ محاسبه شده است از آنجاکه مقدار R_0 کوچکتر از یک شده است بنابراین طبق قضیه (۱) آلودگی بدافزار در شبکه از بین می‌رود.

در شکل (۷) رفتار پویای انتشار همه‌گیری در شبکه بی مقیاس وزن دار با در نظر گرفتن تنوع نرم افزاری نشان داده شده است. با تخصیص سیزده بسته نرم افزاری متنوع ($C = 13$) به گره‌های شبکه بی‌مقیاس وزن دار، مانع از انتشار آلودگی بدافزار در شبکه می‌شویم. با جایگزینی مقادیر متغیرها مشابه شکل (۵)، $\lambda = 0.2, \varepsilon = 0.3, \gamma = 0.1, \delta = 0.01, \mu = 0.01$ و در نظر گرفتن

تنوع نرم‌افزاری $(C = 13)$، مقدار R_0 محاسبه می‌شود $(R_0 = 0.9365)$. طبق قضیه ۱، زمانی‌که R_0 کوچکتر از یک است یعنی آلودگی هر گره جدید از میانگین تعداد آلودگی‌های ثانویه کمتر است و سیستم (۳) به یک نقطه تعادل فاقد آلودگی بدافزار می‌رسد. همان‌طور که در شکل (۷) نشان داده شده است چگالی گره‌های آلوده بعد از گذشت ۹۰ ثانیه به صفر می‌رسد و آلودگی بدافزار در شبکه از بین می‌رود.



شکل (۷): چگالی افراد مستعد، در معرض آلودگی، آلوده و مصون در شبکه بی‌مقیاس وزن دار با در نظر گرفتن تنوع نرم‌افزاری $\lambda = 0.2, \varepsilon = 0.3, \gamma = 0.1, \delta = 0.01, \mu = 0.01$ و $C = 13$.

۵- نتیجه‌گیری

در این مقاله، بر اساس مدل همه‌گیری SEIRS پویایی انتشار بدافزار در شبکه بی‌مقیاس وزن‌دار مورد مطالعه قرار گرفت. همچنین تاثیر تنوع نرم‌افزاری به عنوان یک راهبرد دفاعی در مدل‌سازی انتشار بدافزار در نظر گرفته شد و بسته‌های نرم‌افزاری متنوع به گره‌های شبکه تخصیص داده شد تا از انتشار همه‌گیری در شبکه بی‌مقیاس وزن دار جلوگیری شود. رفتار پویای مدل بر اساس نسبت بازتولید (R_0) بررسی شد که معین می‌کند آیا همه‌گیری در شبکه رخ داده است یا خیر. با استفاده از حل تحلیلی و شبیه‌سازی‌های عددی، تاثیر متغیرهای مختلف روی فرآیند انتشار بدافزار مورد مطالعه قرار گرفت. همچنین نشان دادیم گره‌ها با درجه بالا و قدرت بالاتر، آلودگی بدافزار را سریعتر منتشر می‌کنند و معین کردیم با افزایش مقادیر β و C مقدار R_0 کاهش می‌یابد که این نتیجه، تاثیر متغیر β و متنوع‌سازی را در کاهش انتشار آلودگی بدافزار در شبکه بی‌مقیاس وزن‌دار نشان می‌دهد.

در آینده ما قصد داریم به تحلیل پویایی سراسری در شبکه بی‌مقیاس وزن‌دار در حالت تعادل فاقد آلودگی بدافزار بپردازیم و همچنین به بررسی سازوکارهای دفاعی مانند مصون‌سازی گره‌ها با هدف کاهش انتشار آلودگی در شبکه وزن‌دار بپردازیم.

۶- منابع

[1] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11-33, 2004.

[2] J. Li, J. Lou, and M. Lou, "Some Discrete SI and SIS Epidemic Models, "Applied Mathematics and Mechanics, vol. 29, pp. 113–119, 2008.

[3] F. Zhang, J. Li, and J. Li, "Epidemic characteristics of two classic SIS models with disease-induced death," Journal of Theoretical Biology, vol. 424, pp. 73-83, 2017.

[4] Y. Yang, S. Zhu, and G. Cao, "Improving sensor network immunity under worm attacks: A software diversity approach," Ad Hoc Networks, vol. 47, pp. 26-40, 2016.

[5] A. Gherbi, R. Charpentier, and M. Couture, "Software Diversity for Future Systems Security," Journal of Defense Software Engineering, vol. 25, no. 5, pp. 10-13, 2011.

[6] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.-U. Hwang, "Complex Networks: Structure and Dynamics," Physics Reports, vol. 424, no. 4, pp. 175-308, 2006.

[7] L. Zhang, M. Small, and K. Judd, "Exactly scale-free scale-free networks," Physica A: Statistical Mechanics and its Applications, vol. 433, pp. 182-197, 2015.

[8] R. Pastor-Satorras and A. Vespignani, "Evolution and Structures of the Internet: A Statistical Physics Approach," Cambridge University Press, Cambridge, 2004.

[9] R. Pastor-Satorras and A. Vespignani, "Epidemics and Immunization in Scale-Free Networks," Handbook of Graphs and Networks: From the Genome to the Internet, pp. 111-130, 2005.

[10] M. R. Hasani Ahangar and R. Jalaei, "A Analytical Survey on Botnet and Detection Methods," Journal of Electronical & Cyber Defence, vol. 4, no. 4, pp. 25-46, 2017. (In Persian)

[11] S. Parsa and A. Gooran Oorimi, "An Optimal and Transparent Framework for Automatic Analysis of Malware," Advanced Defence Science and Technology, vol. 6, pp. 71-80, 2016. (In Persian)

[12] A. Gherbi and R. Charpentier, "Diversity-based Approaches to Software Systems Security," Communications in Computer and Information Science, vol. 259, pp. 228–237, 2011.

[13] D. V. Gruzenkin, A. S. Chernigovskiy, and R. Y. Tsarev, "N-version Software Module Requirements to Grant the Software Execution Fault-Tolerance," in Proceedings of the Computational Methods in Systems and Software, pp. 293-303, 2017.

[14] T. Jackson, B. Salamat, G. Wagner, C. Wimmer, and M. Franz, "On the Effectiveness of Multi-Variant Program Execution for Vulnerability Detection and Prevention," In Proc. of the 6th International Workshop on Security Measurements and Metrics, pp. 1-7, 2010.

[15] D. Wanduku, "Complete global analysis of a two-scale network SIRS epidemic dynamic model with distributed delay and random perturbations," Applied Mathematics and Computation, vol. 294, pp. 49-76, 2017.

[16] F. Zhang, J. Li, and J. Li, "Epidemic characteristics of two classic SIS models with disease-induced death," Journal of Theoretical Biology, vol. 424, pp. 73-83, 2017.

[17] J. Ren and Y. Xu, "A compartmental model for computer virus propagation with kill signals," Physica A: Statistical Mechanics and its Applications, 2017.

[18] J. Jiang, S. Wen, S. Yu, Y. Xiang, W. Zhou, and H. Hassan, "The structure of communities in scale- free networks," Concurrency and Computation: Practice and Experience, vol. 29, 2017.

[19] S. Koochaki and M. A. Azgomi, "A Method for Fluid Modeling of the Propagation Behavior of Malware in Scale-Free Networks," Journal of Electronical & Cyber Defence, vol. 4, no. 4, pp. 1-10, 2017. (In Persian)

[20] M. Sun, H. Zhang, H. Kang, G. Zhu, and X. Fu, "Epidemic spreading on adaptively weighted scale-free networks," Journal of mathematical biology, vol. 74, pp. 1263-1298, 2017.

[21] X. Chu, Z. Zhang, J. Guan, and S. Zhou, "Epidemic spreading with nonlinear infectivity in weighted scale-free networks," Physica A: Statistical Mechanics and its Applications, vol. 390, pp. 471-481, 2011.

[22] M. Junfen, H. Sun, J. Pan, and J. Zhou, "Weighted Scale-Free Network with Widely Weighted Dynamics," In: Proceedings of the 30th Chinese Control Conference, pp. 904-909, 2011.

[23] Q. Wu and F. Zhang, "Dynamical behavior of susceptible–infected–recovered–susceptible epidemic model on weighted networks," Physica A: Statistical Mechanics and its Applications, vol. 491, pp. 382-390, 2018.

[24] A J. O'Donnell and H. Sethu, "On Achieving Software Diversity for Improved Network Security Using Distributed Coloring Algorithms," In: Proceedings of the 11th ACM Conference on Computer and Communications Security, pp. 1-11, 2004.

[25] P. Macdonald, E. Almaas, and A. L. Barabási, "Minimum Spanning Trees of Weighted Scale-Free Networks," EPL (Europhysics Letters), vol. 72, no. 2, pp. 1-5, 2005.

[26] P. Driessche, "Reproduction numbers of infectious disease models," Infectious Disease Modeling, vol. 2, pp. 288-303, 2017.

[27] Y. Wang and J. Cao, "Global Dynamics of a Network Epidemic Model for Waterborne Diseases Spread," Applied Mathematics and Computation, vol. 237, pp. 474-488, 2014.

[28] M. Roberts and J. Heesterbeek, "Characterizing the next-generation matrix and basic reproduction number in ecological epidemiology," Journal of mathematical biology, vol. 66, pp. 1045-1064, 2013.

[29] R. M. Ferreira, R. M. de Almeida, and L. G. Brunnet, "Analytic solutions for links and triangles distributions in finite Barabási–Albert networks," Physica A: Statistical Mechanics and its Applications, vol. 466, pp. 105-110, 2017.

Journal of Electronical & Cyber Defence
Vol. 6, No. 3, 2018, Serial No. 23

Malware Propagation Modeling Considering Software Diversity Approach in Weighted Scale-Free Network

S. Hoseini*, M. Abdollahi Azgomi

*Shahid Bahonar University of Kerman

(Received: 28/11/2017, Accepted: 12/01/2018)

ABSTRACT

Nowadays, malware propagation has become a major threat in cyber space. Modeling malware propagation process allows us to get a better understanding of the dynamics of malware spreading as well as helping us to find effective defense mechanisms. Due to the security concerns, software diversity has received much attention as a cyber-defense mechanism. In this paper, considering software diversity approach, an epidemic model of malware propagation in scale-free networks is proposed. Software diversity as a defense mechanism reduces the malware propagation process in the network. Simulation results show the effect of different parameters on the malware propagation process. Also, we demonstrate that the assignment of diverse software packages to network nodes reduces the basic reproductive ratio and malware propagation speed in the network. Moreover, the effect of weight's exponent on the speed of malware propagation is investigated.

Keywords: Malware Propagation, Software Diversity, Weighted Scale-Free Network

* Corresponding Author Email: so_hosseini@uk.ac.ir