مجله علمی - پژوهشی "پدافند الکترونیکی و سایبری"
سال چهارم، شماره ۴، زمستان ۱۳۹۵، ص ۱۰-۱

روشی برای مدل‌سازی سیّال رفتار انتشاری بدافزارها در شبکه‌های بی‌مقیاس

سارا کوچکی[۱]، محمد عبداللهی ازگمی*[۲]

۱- دانشجوی کارشناسی ارشد،۲- دانشیار دانشگاه علم و صنعت ایران

(دریافت: ۹۳/۱۲/۰۹، پذیرش: ۹۵/۰۲/۱۴)

چکیده

شبکه بی‌مقیاس یک مدل انتزاعی برای شبکه‌های اجتماعی برخط یا شبکه‌های نظیر به نظیر است که دارای ویژگی تبعیت از توزیع درجه قانون توان هستند. به سبب این ویژگی‌ها، این شبکه‌ها نسبت به انتشار بدافزارها (نظیر ویروس و کرم) آسیب‌پذیری بیشتری دارند. از روش‌های مدل‌سازی و شبیه‌سازی برای ارزیابی رفتار انتشاری بدافزارها در شبکه‌های بی‌مقیاس و تحلیل راهبردهای دفاع در برابر انتشار بدافزارها استفاده می‌شود. اما زیاد بودن تعداد رخدادهایی که باید پردازش شوند و همچنین در نظر گرفتن جزئیات گره‌های شبکه، روش‌های شبیه‌سازی گسسته- رخداد موجود را برای اجرا بر روی این شبکه‌های بزرگ و پیچیده نامناسب کرده است. از این‌رو، برای مدل‌سازی رفتار انتشاری بدافزارها، مدل‌های سیّال، که در آن‌ها نیازی به دانستن جزئیات شبکه نیست، مناسب‌تر به نظر می‌رسند.

در این مقاله، برای مدل‌سازی سیّال انتشار بدافزارها، یک شبکه بی‌مقیاس را به‌طور انتزاعی در قالب یک شبکه ستون فقرات متشکل از ابرگره‌هایی نمایش داده می‌شود که هر کدام شامل چندین گره شبکه هستند. هر ابرگره در صورت آلوده بودن، می‌تواند آلودگی را به‌صورت یک جریان سیّال به گره‌های همسایه خود منتشر سازد. به این ترتیب مدل‌سازی فرآیند اصلی انتشار بدافزارها، بدون در نظر گرفتن وضعیت آلودگی هر گره و جزئیات دیگر صورت می‌گیرد. برای ارزیابی روش پیشنهادی، از روش شبیه‌سازی عامل‌مبنا استفاده شده است. نتایج ارزیابی نشان می‌دهند که شبکه‌های بی‌مقیاس بزرگ را می‌توان با استفاده از روش پیشنهادی مدل‌سازی نموده و انتشار بدافزارها را در این شبکه‌ها مورد مطالعه قرار داد. همچنین، به‌عنوان مطالعه موردی، تاثیر مصون‌سازی‌های تصادفی و هدفمند گره‌ها در مدل‌های پیشنهادی ارزیابی شده‌اند.

واژه‌های کلیدی: شبکه‌های بی‌مقیاس، مدل‌سازی انتشار، انتشار بدافزار، مدل‌سازی سیّال، شبیه‌سازی عامل‌مبنا، نت‌لوگو.

۱- مقدمه

گراف ویژه اکثر شبکه‌های دنیای واقعی همچون اینترنت، شبکه جهانی وب، ارتباطات میان انسان‌ها با استفاده از شبکه‌های بی‌مقیاس[۱] مدل‌سازی می‌شود. از این‌رو، امنیت در این شبکه‌ها و بهبود آن یکی از مسائل مهم به شمار می‌آید. از سوی دیگر با توجه به ویژگی‌های خاص این شبکه‌ها، همچون دارا بودن گره‌های مرکزی (هاب)[۲]، کوتاه بودن طول مسیر و ضریب خوشه‌بندی[۳] بالا، در برابر انتشار بدافزارها، رفتار ویژه‌ای از خود نشان می‌دهند. این شبکه‌ها در برابر حملات تصادفی مقاومت زیادی از خود نشان می‌دهند [۱]. این در حالی است که در برابر حملات هدفمند به شدت آسیب‌پذیر است. یعنی در صورتی که بتوان در این شبکه‌ها، گره‌های مهم و حساس را شناخت و بر روی آن‌ها حمله صورت داد، احتمال شکست نسبت به زمانی که حمله به‌صورت تصادفی انجام می‌شود، بسیار بالاتر است [۲].

در دنیای امروز اینترنت، خسارت‌های ناشی از حملات بدافزارها[۴] به مشکلی جدی تبدیل شده است. از جمله مهم‌ترین بدافزارها، کرم‌ها[۵] هستند. از زمان پیدایش کرم موریس[۶]، که اولین کرم کامپیوتری به حساب می‌آید، تهدیدات امنیتی حاصل از بدافزارها در حال افزایش بوده و هر ساله خسارت‌های زیادی را به بار می‌آورند [۳]. با استفاده از مدل‌سازی می‌توان نحوه تهدیدها و حمله‌ها را آسان‌تر درک کرد. همچنین به کمک مدل‌سازی و شبیه‌سازی، فهم تکنیک‌های جدید انتشار نیز ساده‌تر خواهد بود. علاوه براین می‌توان مدل‌هایی را برای کاهش خسارت‌های ناشی از فعالیت بدافزارها ارائه داد [۳].

با وجود سودمندی‌های متصور برای مدل‌سازی و شبیه‌سازی شبکه، با افزایش پیچیدگی‌ها و همچنین اندازه شبکه، روش‌های

* رایانامه نویسنده مسئول: azgomi@iust.ac.ir

1- scale-free networks
2- hub
3- clustering coefficient
4- malware
5- worm
6- Morris

شبیه‌سازی گسسته- رخداد[1] موجود، کارایی خود را از دست داده و مدل‌سازی سیّال[2] که در آن نرخ جریان ترافیک شبکه مهم است، کاراتر به نظر می‌رسد. در واقع در گذشته برای مدل کردن رفتار ترافیک در سطح بسته‌ها، مدل‌های گسسته- رخداد شبکه، به‌طور گسترده مورد استفاده قرار گرفته‌اند. در این مدل‌ها ورود یا از بین رفتن یک بسته به‌عنوان یک رخداد در نظر گرفته می‌شد. این مدل‌ها بعضی از سناریوها را به خوبی نمایش می‌دادند و نتایج دقیقی تولید می‌کردند. اما در مورد اینترنت که شبکه‌ای گسترده با پهنای باند بالا و ترافیک شبکه بالاست، این مدل‌ها نمی‌توانند مورد استفاده قرار گیرند، چرا که در این مدل‌ها هنگامی که بخواهیم به وجود آمدن و از بین رفتن همه بسته‌ها را محاسبه کنیم، هزینه محاسباتی بسیار بالا می‌رود. در واقع روش‌های سیّال برای مدل کردن شبکه‌های آزمایشی و کوچک مناسب هستند، اما برای شبکه‌های بزرگ دنیای واقعی، هزینه محاسباتی به شدت بالا می‌رود [۳].

برای رفع مشکل محدودیت اندازه شبکه، روش مدل‌سازی گسسته- رخداد موازی پیشنهاد شده است. اما مشکل دیگر درباره اینترنت این است که اینترنت علاوه بر این که شبکه بزرگی است، ترکیب پیچیده‌ای از اتصالات دارای پهنای باند بسیار بزرگ است و جریان بسته‌هایی که درگاه‌های مسیریاب‌ها وارد می‌شوند، به‌طور دائمی است. بنابر این موازی‌سازی برای مدل کردن رفتار اینترنت مناسب به نظر نمی‌رسد [۴].

با توجه به توضیحات ارائه شده، برای مدل‌سازی رفتار ترافیک اینترنت، مدل جریان سیّال معرفی شده است. در این مدل به جای کار کردن با بسته‌ها، با جریانی از بسته‌ها روبرو هستیم. تغییر نرخ جریان از معدود رخدادهایی است که در این نوع مدل‌سازی مطرح است. از این رو مدل‌سازی با سرعت بیشتری انجام می‌شود و علاوه براین نیازی به دانستن جزئیات ویژگی‌های تک تک گره‌ها نیست. در واقع هرچه تغییر میزان جریان کمتر باشد، تعداد رخدادهای تولید شده کمتر است [۴].

با توجه به شباهت رفتار انتشاری کرم‌های کامپیوتری و رفتار انتشاری ویروس‌های بیماری‌های مختلف در دنیای واقعی از یک سو و مدل‌سازی ارتباطات میان انسان‌های مختلف توسط شبکه‌های بی‌مقیاس از سوی دیگر، مدل‌سازی انتشار کرم‌ها در شبکه‌های بی‌مقیاس می‌تواند از این جنبه نیز امری مهم تلقی شود.

در ادامه مقاله، در بخش دوم، مقدمه‌ای بر کار انجام شده در این مقاله خواهد آمد. در بخش سوم، به معرفی مفاهیم اولیه پرداخته خواهد شد. در ادامه در بخش چهارم، روش پیشنهادی معرفی خواهد شد. در بخش پنجم، نحوه شبیه‌سازی روش پیشنهادی، ارائه خواهد شد. در بخش ششم، به ارزیابی روش پیشنهادی پرداخته می‌شود. در نهایت در بخش هفتم نتیجه‌گیری انجام می‌شود.

۲- مفاهیم پایه

در سال‌های اخیر به منظور تحلیل رفتار شبکه‌های دنیای واقعی، تحقیقاتی درباره نحوه چینش گره‌ها در این شبکه‌ها، انجام شده است. نتایج این تحقیقات نشان می‌دهد که بسیاری از شبکه‌ها از شبکه جهانی وب گرفته تا شبکه‌هایی همچون سامانه‌های متابولیسمی سلول‌ها، دارای گره‌هایی هستند که نقش بسیار مهمی را در همبندی شبکه ایفا می‌نمایند. این گره‌ها معمولاً به گره‌های زیادی از شبکه اتصال دارند.

چنین شبکه‌هایی که دارای گره‌هایی از این نوع هستند به شبکه‌هایی که بی‌مقیاس می‌خوانیم گرایش دارند. به این نوع گره‌ها، گره‌های مرکزی یا هاب گفته می‌شود. در این شبکه‌ها بعضی از هاب‌ها دارای اتصالات بی‌شمار بوده و هیچ گره‌ای لزوماً شبیه گره دیگر نیست. این شبکه‌ها معمولاً به‌صورت قابل پیشگویی قطعی رفتار می‌کنند. برای مثال این شبکه‌ها در برابر خرابی‌های تصادفی به‌طور قابل ملاحظه‌ای مقاوم هستند، اما در برابر حملات هدفمند بسیار آسیب‌پذیر هستند. اطلاعاتی که از نتایج این تحقیقات به‌دست آمده است تصور ما را نسبت به دنیای پیچیده اطرافمان تغییر داده است. برخلاف نظریه‌های شبکه قدیمی، هاب‌ها تأییدکننده این امر هستند که شبکه‌های پیچیده، معماری‌های مشخصی دارند که از قوانین بنیادی که برای ارزیابی سلول‌ها، کامپیوترها و زبان‌ها مطرح شده‌اند پیروی می‌کنند [۱].

تاریخچه معرفی شبکه‌های بی‌مقیاس به سال ۱۹۹۸ برمی‌گردد. هنگامی که باراباسی و همکارانش سعی در مدل کردن گراف شبکه وب داشتند، نوع خاصی از شبکه‌ها موسوم به شبکه‌های بی‌مقیاس پدیدار شد. اصلی‌ترین ویژگی این شبکه‌ها آن است که توزیع اتصالات گره‌ها در آن‌ها از تابع توزیع توان[3] پیروی می‌کند [۵]. معرفی این نوع شبکه، باعث شد درباره شبکه‌هایی که قبلاً معرفی شده بوند، ابهاماتی پیش آید. دانشمندان با پی بردن به ویژگی‌های خاص این شبکه‌ها، به این موضوع پی بردند که نحوه شکل‌گیری و همبندی شبکه‌های دنیای واقعی به عامل خاصی بستگی ندارد و تقریباً همه شبکه‌های دنیای واقعی مشابه این همبندی هستند [۵].

از جمله حملاتی که بر روی شبکه‌های دنیای واقعی که با شبکه‌های بی‌مقیاس مدل می‌شوند صورت می‌گیرد، حملات بدافزاری است. واژه بدافزار به ویروس[4]، کرم، تراوا[5] و هر

1- discrete-event
2- fluid modeling

3- power-law distribution
4- virus
5- Trojan

برنامه دیگری که با نیت اعمال خرابکارانه ایجاد شود، اطلاق می‌شود [۶].

با توجه با ویژگی‌های خاص کرم‌های کامپیوتری، در این مقاله به ارائه روشی برای مدل‌سازی نحوه انتشار این نوع بدافزارها بر روی شبکه‌های بی‌مقیاس پرداخته می‌شود. کرم کامپیوتری به برنامه‌ای اطلاق می‌شود که توانایی بازتولید خود را داراست و با استفاده از شبکه نسخه‌های خود را به دیگر کامپیوترهای موجود در شبکه می‌فرستد. برخلاف ویروس، کرم‌ها خود را به برنامه‌های دیگر نمی‌چسبانند. همچنین کرم‌ها عموماً با اشغال پهنای باند به شبکه آسیب می‌رسانند در حالی که ویروس‌ها در بیشتر اوقات باعث خرابی برنامه‌های موجود در کامپیوتر آلوده و از دست رفتن اطلاعات موجود در آن می‌شوند. مهمترین ویژگی مشترک آن‌ها این است که کرم‌ها نیز خودهمانندساز[1] هستند، اما تکثیر[2] آن‌ها از دو جهت متفاوت است. اول این‌که، کرم‌ها مستقل و متکی به خود هستند و محتاج به کد اجرایی دیگری نیستند. دوم، کرم‌ها از طریق شبکه‌ها، از ماشینی به ماشین دیگر منتقل و پخش می‌شوند [۶].

۳- کارهای مرتبط

برای افزایش قدرت دفاعی این شبکه‌ها، کارهای مختلفی انجام شده است که در ادامه این بخش مورد بررسی قرار می‌گیرند.

اولین کار مرتبط پیشین، آن بوده است که تحمل‌پذیری شبکه در برابر آسیب‌پذیری‌های امنیتی به طریقی بیشتر شود. برای این کار دو روش مطرح شده است. در روش اول می‌توان به شبکه یال‌هایی اضافه کرد. اساس این کار این است که تعداد مشخصی یال به شبکه اصلی اضافه می‌شود تا در صورت مورد حمله قرار گرفتن شبکه، ساختار اصلی آن به هم نریزد. تعداد یال‌های اضافه‌شونده و گره‌های مربوط به آن با استفاده از یک فرمول ویژه قابل محاسبه است. نتایج به دست آمده نشان‌دهنده افزایش قدرت دفاعی با استفاده از این روش است [۲].

روش دیگر برای افزایش تحمل‌پذیری در برابر خطا، پنهان‌کردن ویژگی‌های حساس شبکه است. در حمله‌هایی که تاکنون بر روی این شبکه‌ها صورت گرفته، در ابتدا ویژگی‌ها و ساختار این شبکه‌ها مورد بررسی قرار گرفته، تا گره‌های حساس شناسایی شوند. به همین دلیل در صورت پنهان‌کردن ویژگی‌های شبکه به ویژه خصوصیت‌های مختلف یال‌ها می‌توان از شناسایی و دسترسی به یال‌ها و در نتیجه حمله بر روی شبکه جلوگیری کرد [۲].

پیشنهاد دیگری که برای افزایش قدرت دفاعی این شبکه‌ها وجود دارد این است که از مصون‌سازی[3] استفاده شود. مصون‌سازی بر روی شبکه‌های بی‌مقیاس به دو روش انجام می‌شود [۷].

در روش اول که مصون‌سازی یکنواخت[4] نامیده می‌شود، گره‌هایی که برای مصون‌سازی انتخاب می‌شوند به‌صورت تصادفی از میان گره‌های موجود در شبکه انتخاب می‌شوند. این روش برای شبکه‌های بی‌مقیاس کارایی پایینی دارد؛ چرا که در این شبکه‌ها توزیع درجه به‌صورت یکنواخت نیست و در صورت انتخاب گره‌ها به‌صورت یکنواخت احتمال آن که گره‌های دارای درجه پایین انتخاب شوند، بسیار بالاست. در صورتی که بتوان به طریقی گره‌ها دارای اتصالات زیاد را شناسایی کرد و آن‌ها را مصون نمود، مصون‌سازی بر روی شبکه بی‌مقیاس از کارایی بیشتری برخوردار خواهد بود. چرا که در صورتی که به عنوان مثال بتوان گره‌های هاب را که دارای بالاترین درجه در گراف هستند را مصون نمود، می‌توان انتشار آلودگی در شبکه را تا حد زیادی کنترل کرد. به این نوع مصون‌سازی، که با عنوان روش دوم مطرح است، مصون‌سازی هدفمند[5] گفته می‌شود [۷].

از حملات دیگری که بر روی شبکه‌های بی‌مقیاس انجام می‌شود، حمله به کمک بدافزارهاست. از جمله راه‌کارهای موجود برای تعریف نحوه رفتار کرم‌ها بر روی شبکه‌ها، استفاده از مدل‌سازی است. با استفاده از مدل‌سازی می‌توان روش‌هایی را برای پاک کردن شبکه آلوده‌شده یافت. همچنین در صورت تعریف کرم‌های جدید می‌توان آن‌ها را شناسایی کرد. مدل‌های همه‌گیری شناختی که رفتار انتشاری بدافزارها را همانند نحوه انتشار بیماری‌ها میان انسان‌ها توصیف می‌کنند، مبنای بسیاری از مدل‌سازی‌های انجام شده در زمینه انتشار بدافزارها در شبکه‌ها هستند. در شبکه‌های بی‌مقیاس نیز مدل‌سازی‌های مختلفی در زمینه انتشار بدافزار با استفاده از این روش‌ها صورت گرفته است. در سال ۲۰۰۱ برای اولین بار به مدل‌سازی انتشار بدافزار بر روی شبکه‌های بی‌مقیاس صورت گرفت. این پژوهش به منظور تحلیل آستانه همه‌گیری در این شبکه‌ها انجام شد. نتایج حاصل از این پژوهش نشان‌دهنده آن بود که در شبکه‌های بی‌مقیاس با اندازه نامتناهی، حد آستانه برای همه‌گیری وجود ندارد. اساس این مدل‌سازی مدل SIS[6] بود [۸].

در پژوهشی که در سال ۲۰۱۱ انجام شد، مدل‌سازی انتشار با توجه به ترافیک جریان بر روی شبکه‌های بی‌مقیاس با اندازه متناهی انجام شد [۹]. در مدل‌سازی انجام شده در سال

1- self-replicate
2- propagate

3- immunization
4 -uniform immunization
5 -targeted immunization
6- susceptible-infected-susceptible

۲۰۱۴ به بررسی اثر مصون‌سازی‌های مختلف بر روی شبکه‌های بی‌مقیاس پرداخته شد [۱۰]. در پژوهشی که در سال ۲۰۱۲ به منظور بررسی تأثیر مراقبت از گره‌های آلوده صورت گرفت از مدل‌سازی SIR[1] استفاده شد. نتایج حاصل از این مدل‌سازی نشان‌دهنده آن بود که مراقبت از گره‌های آلوده در آستانه آلودگی تأثیری ندارد [۱۱].

در [۱۲]، یک روش تحلیلی برای مدل‌سازی انتشار بدافزارها در شبکه‌های بی‌مقیاس با در نظر گرفتن تنوع نرم‌افزاری به عنوان یک تکنیک دفاع سایبری ارائه شده است. در [۱۳]، از شبیه‌سازی عامل‌مبنا و نرم‌افزار نت‌لوگو برای شبیه‌سازی پویایی انتشار بدافزارها در شبکه‌های بی‌مقیاس استفاده شده و نتایج حاصله با مدل تحلیلی مقایسه شده است. در [۱۴]، بر مبنای یک فرآیند انتشار شایعه، مدلی برای انتشار بدافزارها در شبکه‌های بی‌مقیاس ارائه شده است.

در واقع مدل‌سازی انتشار بدافزار در شبکه‌های بی‌مقیاس به‌صورت گسسته- رخداد و سطح بسته بارها مدل‌سازی شده است؛ اما مشکل آن این است که برای مدل کردن انتشار سریع مناسب نیست؛ چرا که باید رخدادهای زیادی در آن محاسبه شوند. برای غلبه بر این مشکل یک راه‌حل متصور، حذف جزئیات از مدل‌سازی و ارائه یک مدل سیّال و فشرده است که رفتار کرم را به‌صورت کلی مدل می‌نماید. در روش پیشنهادی، این رهیافت مورد توجه قرار گرفته است.

۴- روش پیشنهادی

نوآوری مورد نظر در این پژوهش، مدل‌سازی انتشار کرم در شبکه‌های بی‌مقیاس به‌صورت سیّال است که تحلیل رفتاری انتشار بدافزارها را به‌صورت سریع ممکن می‌سازد. برای این منظور، برای افزایش سرعت مدل‌سازی انتشار کرم در شبکه‌های بی‌مقیاس مدل‌سازی سیّال استفاده می‌شود. مزیت این روش آن است که در آن نیازی نیست همه جزئیات در نظر گرفته شوند و پیچیدگی‌های مدل‌سازی در آن کاهش می‌یابد. از این‌رو، هنگامی که اندازه شبکه بزرگ می‌شود، این نوع مدل‌سازی کارایی بالایی از خود نشان می‌دهد.

در روش پیشنهادی با توجه به این که فرض بر این است که هنگام انتشار کرم بر روی شبکه، همبندی آن تغییری نمی‌کند، ابتدا نیاز است که شبکه اولیه ساخته شود. برای ساخت شبکه بی‌مقیاس از الگوریتم باراباسی- آلبرت (BA) [۱۵] استفاده می‌شود. این الگوریتم که توسط باراباسی و آلبرت ارائه شده است، اولین و در عین حال پرکاربردترین روش ساخت این شبکه‌ها است. این روش دارای دو شرط اساسی در ساخت شبکه است:

۱) رشد مرحله به مرحله اندازه شبکه ۲) انتخاب اولویت‌دار گره‌ها برای اضافه کردن یال. برای ایجاد شبکه‌ای که همبندی آن به‌صورت بی‌مقیاس باشد، رعایت هر دو شرط ضروری است. الگوریتم ساخت این شبکه در شکل (۱) نشان داده شده است.

```
Algorithm 1: Making scale-free network topology
Input: N=Network size, P0= Number of initial nodes in topology,
m=Number of joining node's neighbors, G= Topology
graph
G Function MakeNetwork()
Begin
  LotteryList = Array of tickets
  For i=1 to N - P0
    Foreach CurrentPeers as Node
      NodeID = ID of Node
      NodeDegree = Degree of Node
      For j=1 to NodeDegree
        Add NodeID to LotteryList
      End For
    End Foreach
    SelectedNeighbors = Select randomly m of LotteryList elements
    Create_Links_With SelectedNeighbors
End For
End
```

شکل (۱). نحوه ساخت شبکه اولیه [۱۵]

در این الگوریتم در ابتدا با تعداد محدودی گره و یال‌های بین آن‌ها، گراف اولیه ساخته می‌شود. در واقع در ابتدا به اندازه تعداد مشخصی گره وجود دارد که گراف کامل آنها رسم می‌شود. در ادامه، در هر مرحله یک گره به شبکه افزوده می‌شود. این گره توسط یک یال به گره‌های قبلی اضافه می‌شود. نحوه اضافه شدن گره به صورتی است که برای گره‌های قدیمی، احتمال این که گره بتواند سر دیگر یال گره جدید باشد، با درجه گره متناسب است. این امر بدان معناست که گره‌های دارای درجه بیشتر از شانس بیشتری برای کسب یال جدید برخوردارند و به این ترتیب درجه گره‌هایی که درجه بزرگتری دارند، بزرگ و بزرگ‌تر می‌شوند تا تبدیل به گره‌های هاب شوند. نحوه پیاده‌سازی این الگوریتم به گونه‌ای است که در ابتدا تعداد گره‌های اولیه و گره‌های نهایی مشخص است و گراف بر مبنای این شبکه‌ها ساخته می‌شود.

پس از ساخت شبکه بی‌مقیاس، باید انتشار بدافزار بر روی آن مدل شود. هدف، مدل‌سازی روش انتشار همه‌گیری SIR است. در این روش هرکدام از گره‌ها در یکی از وضعیت‌های مستعد آلودگی[2]، آلوده[3] یا مصون‌شده[4] قرار دارند. در ابتدای انتشار وضعیت همه گره‌ها به‌صورت مستعد است. پس از آلوده کردن تعداد بسیار محدودی از گره‌ها، انتشار آلودگی آغاز می‌گردد. گره‌های آلوده با شناسایی همسایه‌های مستعد خود، آلودگی را انتشار داده و با توجه به نرخ انتشار، گره‌های مستعد را به حالت آلوده درمی‌آورند. سپس گره‌ها با یک نرخ تعریف‌شده از حالت

1- susceptible-infected- removed

2- susceptible
3- infected
4- removed

آلوده به حالت مصون‌شده تغییر حالت می‌دهند. این روند تا هنگامی ادامه پیدا می‌کند که همه گره‌ها به‌صورت مصون‌شده درآیند. در واقع حالت پایدار[1] مدل هنگامی حاصل می‌شود که همه گره‌ها در وضعیت مصون‌شده قرار داشته باشند.

با توجه به این که مدل‌سازی انتشار به‌صورت سیّال مورد نظر است، روش پیشنهادی باید به گونه‌ای عمل کند که در آن نیازی به حفظ تمامی جزئیات نباشد. به عنوان مثال در شبیه‌سازی، این که هر کدام از گره‌ها در هر لحظه در چه حالتی است مهم نیست و تنها مقدار کلی حالت‌های مختلف گره‌ها در شبکه اهمیت دارد. به عنوان مثال در یک لحظه خاص، وضعیت آلودگی یک گره در روند مدل‌سازی اهمیتی ندارد، اما مجموع گره‌های آلوده موجود در شبکه برای مدل‌سازی دارای اهمیت است. اصولاً در مدل کردن اینترنت، وب یا هر شبکه بی‌مقیاس دیگر، به دلیل مقیاس بسیار بزرگ و پیچیدگی شبکه، مدل‌سازی به‌صورتی که هر گره نمایان‌گر یک کاربر یا سامانه باشد، کاری غیرممکن است. از سوی دیگر در مدل‌سازی برای ما مهم نیست که به عنوان مثال دقیقاً کدام گره آلوده است. از سوی دیگر باید تأکید کنیم که یکی از اهداف اصلی مطرح در این مدل‌سازی، سرعت اجرای مدل است. همچنین، با توجه به این که اندازه شبکه می‌تواند بسیار بزرگ باشد، هدف ما در این پژوهش بررسی نحوه انتشار در کل شبکه است. در نتیجه، جزئیات وضعیت گره‌ها در هر لحظه در روند کلی شبیه‌سازی تأثیر چندانی ندارد. لذا، در مرحله بعد برای بالا بردن سرعت شبیه‌سازی از گراف به دست آمده در مرحله قبل، گراف فشرده دیگری ساخته می‌شود.

برای شبیه‌سازی نحوه انتشار در ابتدا شبکه به ابرگره‌هایی[2] تقسیم می‌شود که هر کدام شامل چندین گره از شبکه اصلی هستند. برای تقسیم شبکه به ابرگره‌ها، بر اساس [۱۶] شبکه به سه بخش سیّال، *همه‌گیری* و *بسته* تقسیم می‌شود. نحوه انتشار آلودگی در گره‌های اصلی که به نوعی ستون فقرات[3] شبکه را تشکیل می‌دهند توسط شبکه سیّال مدل می‌شود. در آن دسته از گره‌های شبکه که در همبندی شبکه به عنوان برگ در نظر گرفته می‌شوند و در روند انتشار تاثیر کمتری می‌گذارند، شبکه به‌صورت همه‌گیری در نظر گرفته شده است. تعامل بین دو شبکه همه‌گیری و سیال به کمک شبکه بسته‌ها صورت می‌گیرد. با تقسیم کردن ستون فقرات شبکه اصلی به ابرگره‌های دیگر، شبکه سیّال به دست می‌آید. ویژگی‌های مختلف گره‌هایی که درون یک ابرگره هستند به یکدیگر شباهت زیادی دارد. در این شبکه سیّال برای هر گره هر یال بین گره‌ها نرخ ورود و نرخ خروج تعیین می‌شود.

اگر در یک ابرگره، گره‌ای وجود داشته باشد که با گره‌ای از یک ابرگره دیگر در شبکه اولیه یال داشته باشد، دو ابرگره توسط یالی به هم متصل می‌شوند. گراف حاصل از اتصال این ابرگره‌ها نشان‌دهنده ستون فقرات شبکه اولیه است. تعداد گره‌های گراف فشرده توسط کاربر تعیین می‌شود. الگوریتم ساخت گراف فشرده در شکل (۲) نشان داده شده است.

```
Algorithm 2: Making backbone of the network
Input: Net=initial scale-free network graph, N=network size
Begin
  For i=1 to N
    Find MAX degree of Net
    Size of node =MAX degree
    Add to newNodes
    Remove from Net
  End for
 n= The number of new graph's nodes
 For i=1 to n
    Find links of newNodes
    Links's Weight= The number of links between old nodes
 End for
```

شکل (۲). نحوه ساخت گراف فشرده ستون فقرات شبکه

اگر در گراف فشرده، گره‌ای آلوده باشد، بر روی همسایه‌های خود تأثیر خواهد گذاشت و آلودگی را به‌صورت سیّال و پیوسته انتشار خواهد داد. برای شبیه‌سازی نحوه انتشار کرم‌ها به‌صورت سیّال، هر گره جریانی از آلودگی را به همسایه‌های خود ارسال می‌کند. این جریان دارای یک نرخ ارسال و یک نرخ دریافت است. هر گره با توجه به نرخ‌های مشخص، به گره‌های همسایه خود حمله می‌کند. این امر به معنی آن است که در روند انتشار، به‌صورت سیّال عمل خواهد می‌کند.

برای مدل‌سازی انتشار فرض می‌شود که گره v در ابتدا توسط کرم آلوده می‌شود و سپس در هر مرحله زمانی هر گره آلوده می‌تواند تعداد i گره دیگر را آلوده کند. در صورتی که هر گره آلوده شود به رنگ قرمز در می‌آید و شروع به آلوده کردن گره‌های دیگر می‌نماید. نحوه انتشار به این گونه است که گره آلوده شده در ابتدا گره‌هایی را که با آن در یک ابرگره قرار دارند را آلوده می‌کند و در صورتی که این ابرگره با ابرگره‌های دیگر رابطه‌ای داشته باشد شروع به آلوده کردن گره‌های ابرگره دوم می‌کند. به این صورت کرم در میان ابرگره‌ها انتشار می‌یابد. اما در صورتی که ابرگره آلوده شده با گره‌های موجود در ابرگره‌های دیگر اتصال نداشته باشد، تنها می‌تواند ابرگره خود را آلوده نماید که در مدل مطرح در این پروژه با توجه به این که همبندی شبکه مدل‌سازی شده به‌صورت بی‌مقیاس است، این حالت اتفاق نمی‌افتد. در مرحله بعد با توجه به تعداد اتصالات ابرگره، ابرگره‌های دیگر آلوده می‌شود.

در گراف فشرده هر گره نشان‌دهنده مجموعه‌ای از سامانه‌هاست. در مورد وضعیت گره‌ها در این گراف در هر لحظه نمی‌توان گفت به طور صد در صد آلوده بوده یا مستعد آلودگی

1- steady-state
2- super-node
3- backbone

است. در واقع هر گره ترکیبی از این سه وضعیت است. به‌عنوان مثال برای هر گره می‌توان گفت سی درصد از گره آلوده، چهل درصد مستعد آلودگی و سی درصد در حالت پاک‌شده قرار دارد. این امر نشان می‌دهد به عنوان مثال سی درصد از گره‌های اولیه تشکیل‌دهنده گره دوم در حالت آلوده قرار داشته‌اند. در حالت کلی نسبت مجموع گره‌های آلوده به کل گره‌ها در گراف‌های اولیه و فشرده با هم برابر است. به این ترتیب بستری فراهم می‌شود که در آن بتوان میزان آلودگی را برای هر گره به‌صورت جریانی پیوسته در نظر گرفت و شبیه‌سازی را به‌صورت پیوسته انجام داد.

فرض می‌شود میزان آلوده بودن در هر گره به عوامل زیر بستگی دارد:

۱) مقدار اولیه آلودگی گره
۲) نرخ انتشار آلودگی گره
۳) نرخ پاک‌سازی از آلودگی گره
۴) تعداد همسایه‌های گره
۵) میزان آسیب‌پذیری گره از گره‌های همسایه

در گراف فشرده به دست آمده، نحوه انتشار آلودگی در هر گره به‌صورت SIR پیاده‌سازی شده است. برای این کار از رابطه‌های پایه اصلی موجود برای این نوع انتشار استفاده می‌شود. برای مدل‌سازی SIR از فرمول‌های (۱)، (۲) و (۳) استفاده می‌شود [۱۷]:

$$\frac{dS(t)}{dt} = -\langle k \rangle \beta\, i(t)\, S(t) \quad (۱)$$

$$\frac{di(t)}{dt} = -\delta\, i(t) + \langle k \rangle \quad (۲)$$

$$\frac{dr(t)}{dt} = -\delta\, i(t) \quad (۳)$$

در این فرمول‌ها S نشان دهنده میزان گره‌های مستعد آلودگی، i نشان دهنده میزان گره‌های آلوده و r نمایش‌دهنده گره‌های پاک شده و $\langle k \rangle$ میانگین درجه گره‌ها در شبکه است. همچنین β نشان‌دهنده نرخ انتشار آلودگی و δ نشان‌دهنده نرخ پاک‌سازی گره‌هاست.

این فرمول‌ها نشان‌دهنده میزان تغییر هر کدام از متغیرهای تعداد گره‌های مستعد آلودگی، آلوده مصون‌شده در گره هستند. از آنجایی که گره‌های گراف فشرده هرکدام نشان‌دهنده یک مجموعه از گره‌های گراف اولیه هستند، تغییر هر کدام از این متغیرها در گراف فشرده نشان‌دهنده تغییر تعداد گره‌های آلوده و یا مستعد و مصون‌شده از شبکه است.

در مدل‌سازی انجام شده در گراف فشرده، مقدار δ به اندازه مقداری که از ابتدا تعیین‌شده است، باقی خواهد ماند. اما مقدار β با توجه به تعداد همسایه‌های گره و با توجه به میزان آلوده بودن همسایه‌ها قابل تغییر است. فرض می‌شود این میزان تأثیرپذیری به عوامل زیر بستگی دارد:

۱) اندازه ابرگره همسایه
۲) درصد آلودگی ابرگره همسایه
۳) نرخ انتشار در ابرگره همسایه
۴) معکوس اندازه ابرگره
۵) وزن یال بین دو ابرگره

تغییرات β علاوه بر میزان تأثیری که از گره‌های همسایه می‌گیرد، به نرخ آلوده‌سازی خود ابرگره نیز وابسته است. بنابراین موارد گفته‌شده میزان تغییرات β به ازای هر یک از همسایه‌های آن با توجه به فرمول (۴) تغییر می‌کند:

$$\frac{d\beta}{dt} = \beta * \mathrm{c} * \frac{neighbor's\ size}{current\ node's\ size} * link's\ weight * neighbore'\beta * infected\ \ of\ neighbor \quad (۴)$$

این فرمول نشان‌دهنده میزان تأثیرپذیری هر گره از گره همسایه خود است. توجه به این نکته ضروریست که در این فرمول فرض شده است که همه عوامل به یک اندازه تأثیرگذارند. در این فرمول C یک مقدار ثابت کوچکتر از یک است که ثابت تأثیرپذیری است. این فرمول تغییرات β را تنها به ازای یکی از همسایه‌های آن نمایش می‌دهد. از این‌رو، برای به دست آوردن تغییرات کلی آن، باید میزان تأثیرات همه گره‌های همسایه را با یکدیگر جمع نمود. الگوریتم میزان تاثیرپذیری هر گره از گره‌های همسایه آن در شکل (۳) نشان داده شده است.

این الگوریتم بر اساس اصول شبیه‌سازی سیّال عمل می‌کند. برای این منظور ابرگره‌های موجود در گراف ستون فقرات شبکه مبنای کار قرار داده می‌شوند و جریال انتشار آلودگی از یک ابرگره به سایر ابرگره‌ها در نظر گرفته می‌شود. در حلقه اصلی این الگوریتم، به ازای هر ابرگره موجود در گراف ستون فقرات (ND)، جریان سیّال ورودی آن محاسبه می‌شود. سپس برای هر ابرگره همسایه با ND، جریان سیّال ورودی آنها به ND محاسبه شده و به عنوان جریان سیّال خروجی، به جریان سیّال ورودی ابرگره ND اضافه می‌شود و با توجه به تغییرات جریان‌های سیّال ورودی و خروجی، درصد مستعد بودن، آلوده بودن و پاک بودن ابرگره ND بروزرسانی می‌شود.

هر چه تعداد گره‌ها در گراف فشرده کمتر باشد، اندازه گره‌ها بزرگتر می‌شود، و معیارهای درونی در نظر گرفته‌شده برای هر گره تأثیر بیشتری در روند انتشار خواهند داشت. هر چه تعداد گره‌ها بیشتر شود، معیارهای خارجی که همان جریان آلودگی است، تأثیر بیشتری در میزان آلودگی خواهند گذاشت.

Algorithm 3: Fluid propagation modeling
Input: *Backbone Graph ,initial value of susceptible,infected and removed of each node*
Begin
Foreach node *ND in Backbone Graph*
Begin
Calculate internal fluid flow
Foreach neighbor *NEIGH of ND*
Begin
Calculate fluid flow of NEIGH on ND
Add to external fluid flow
End
Update percent of ***susceptible of ND***
Update changes of percent of ***infected of ND***
Update changes of percent of ***removed of ND***
Define new state of ND
End
End

شکل (۳). شبه‌کد نحوه انتشار آلودگی در گره‌های مختلف

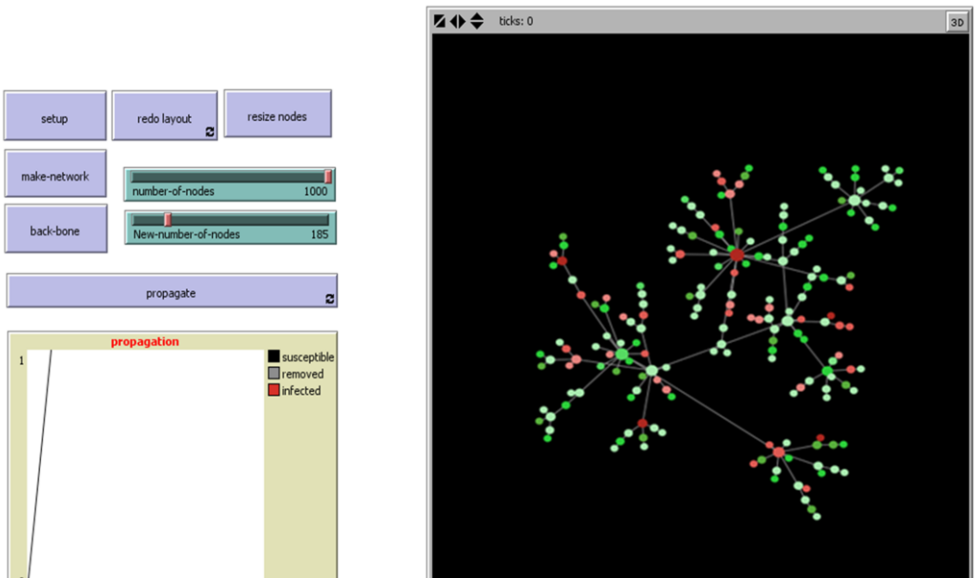
۵- شبیه‌سازی عامل‌مبنای روش پیشنهادی

در محیط‌های بزرگ که موجودیت‌های زیادی حضور دارند و دائما در حال تعامل با یکدیگرند، استفاده از شبیه‌سازی عامل‌مبنا[1] سودمند است. این نوع مدل‌سازی به برنامه‌نویسی شئ‌گرا شباهت زیادی دارد، با این تفاوت که در آن، عامل در تعیین نحوه تعاملش با دیگر موجودیت‌ها، تأثیرگذار است و نحوه برخورد با ورودی‌های مختلف را خودش تعیین می‌کند. لذا پیچیدگی‌های شبیه‌سازی موجود در شبکه مورد بحث، از این طریق کاهش می‌یابد [۱۸]. لذا در این پژوهش از این روش شبیه‌سازی استفاده شده است. ابزار شبیه‌سازی مورد استفاده، نت‌لوگو[2] است.

دلیل انتخاب این ابزار آن است که نت‌لوگو یک محیط قابل برنامه‌ریزی چند عامله است که به‌صورت رایگان قابل دریافت است. برنامه‌نویسی در نت‌لوگ با زبان لوگو[3] قابل انجام است. ساخت یک مدل در محیط نت‌لوگو با استفاده از عامل‌ها صورت می‌پذیرد. عامل‌ها به‌صورت ترتل[4] و ارتباطات بین آن‌ها با پیوندها[5] مشخص می‌شوند. در مدل پیشنهادی ما هر ترتل در شبکه نشان‌دهنده یک گره است. یال‌های بین گره‌ها نیز با پیوند شبیه‌سازی شده‌اند [۱۸]. در برنامه‌های نوشته‌شده به زبان لوگو به‌جای اجرای توابع و حلقه‌های تکرار معمول، از عامل‌ها خواسته می‌شود که کاری انجام دهند. به این ترتیب می‌توان الگوهای پیچیده را در زمانی کوتاه بدون در نظر گرفتن جزئیات پیاده‌سازی (مگر در مواردی که در کاربرد مهم هستند) پیاده‌سازی نمود. برای پیاده‌سازی مدل پیشنهادی با توجه به الگوریتم‌های ارائه شده، ابتدا یک شبکه بی‌مقیاس ایجاد می‌شود. سپس گراف فشرده ستون فقرات شبکه اولیه استخراج می‌شود. تعداد گره‌های گراف فشرده بستگی به نظر کاربر دارد. در مرحله بعد انتشار آلودگی بر روی شبکه به‌صورت سیّال مدل می‌شود. در شکل (۴) واسط کاربری ابزار نت‌لوگو نشان داده شده است.

۶- ارزیابی

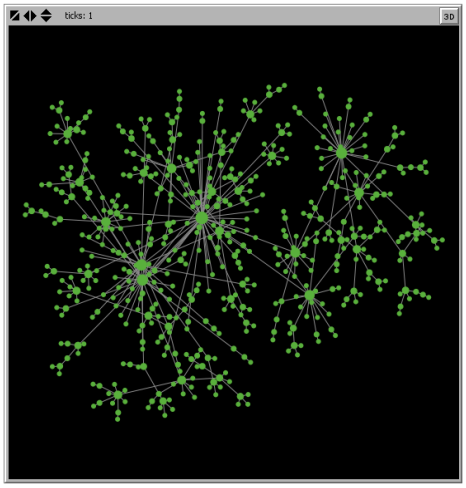
در اینجا در ابتدا یک ارزیابی از تأثیر فشرده‌سازی گره‌ها ارائه می‌دهیم. شکل (۵)، نشان‌دهنده یک گراف شبکه بی‌مقیاس اولیه، ساخته‌شده توسط برنامه است. تعداد گره‌های این گراف برابر ۵۵۰ است. در شکل (۶) نمایش‌دهنده گراف فشرده به‌دست آمده از گراف شکل (۵) است. تعداد گره‌های این گراف برابر ۱۸۰ است (کاهش ۶۷ درصدی گره‌ها).



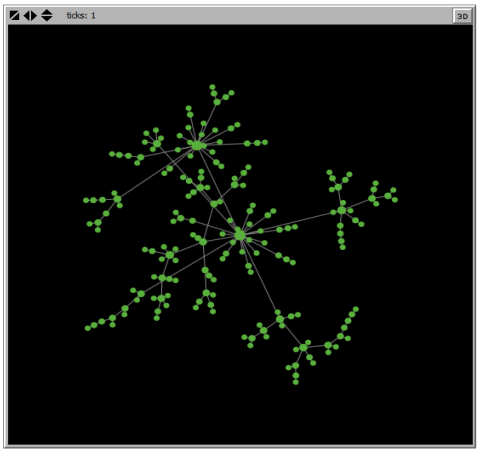
شکل (۴). نمایی از واسط کاربری محیط شبیه‌سازی شده

1- agent-based simulation
2- NetLogo

3- Logo
4- turtle
5- links



شکل (۵). نمونه‌ای از گراف شبکه بی‌مقیاس اولیه ساخته شده توسط برنامه

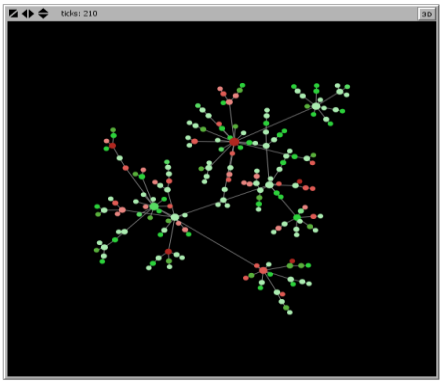


شکل (۶). گراف فشرده ستون فقرات متناظر با گراف شبکه اولیه ساخته شده توسط برنامه

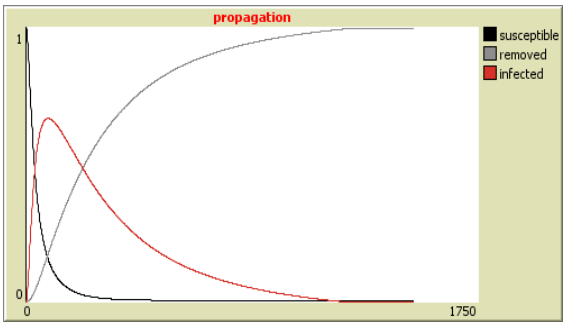
در شکل (۷) گراف مدل‌سازی شده نشان شده است. در این گراف گره‌های قرمز پررنگ‌تر، میزان آلودگی بیشتری را نمایش می‌دهند. در واقع در ابتدای مدل‌سازی، همه گره‌ها سبز رنگ هستند چرا که میزان آلودگی در آن‌ها صفر است. سپس با گذشت زمان و با انتشار کرم در گره‌های مختلف، رنگ هر گره بر مبنای میزان آلودگی موجود در آن تغییر می‌کند و به رنگ قرمز در می‌آید.

حال نشان می‌دهیم که امکان شبیه‌سازی سیاست‌های مصون‌سازی بر روی گراف فشرده حاصله وجود دارد.

در شکل (۸)، نمودار حاصل از مدل‌سازی سیّال انجام شده برای انتشار کرم آورده شده است. هر کدام از منحنی‌های شکل نشان‌دهنده میزان تغییرات یکی از حالت‌های مستعد آلودگی، آلوده یا مصون‌شده نسبت به زمان است. همان‌گونه که در شکل (۸) مشخص است، هنگامی که شبیه‌سازی به حالت پایدار می‌رسد، میزان گره‌های آلوده و مستعد به سمت صفر میل می‌کند و گره‌ها در حالت مصون‌شده قرار دارند.



شکل (۷). نمونه‌ای از گراف فشرده نشان‌دهنده چگونگی انتشار در سطح شبکه



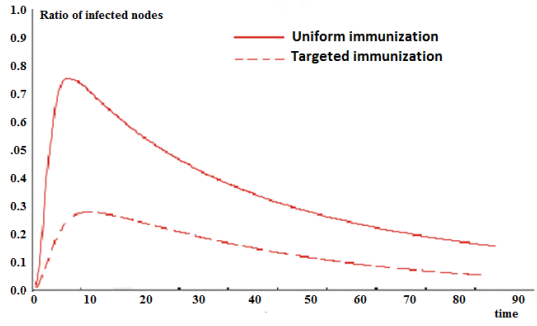
شکل (۸). نمودار میزان تغییرات حالت‌های مختلف

در ابتدا تمامی گره‌ها در حالت مستعد آلودگی قرار دارند که با گذشت زمان از مقدار آن‌ها کاسته شده و در نهایت به سمت صفر میل می‌کند. این میزان کاهش در ابتدای منحنی از شیب بسیار زیادی برخوردار است. دلیل این امر آن است که با گذشت زمان با کاهش میزان گره‌های مستعد، نرخ اصابت کرم کاهش پیدا کرده و از این رو سرعت انتشار کاهش پیدا کرده و گره‌های مستعد با سرعت کمتری به گره‌های آلوده تبدیل می‌شوند. با شروع انتشار به تدریج از میزان گره‌های مستعد کاسته شده و به گره‌های آلوده اضافه می‌شود. منحنی نمایش‌دهنده تغییرات گره‌های آلوده دارای یک قله است که نشان‌دهنده بیشینه مقدار ممکن گره‌های آلوده است. در واقع در شروع انتشار با توجه به نرخ اصابت بالا میزان گره‌های آلوده با سرعت بیشتری اضافه می‌شود، از طرفی با توجه به آن که مقدار گره‌های آلوده کم است، تغییر گره‌های آلوده به مصون‌شده به کندی صورت می‌گیرد. در نقاط پس از قله منحنی با وجودی که انتقال از حالت مستعد به حالت آلوده اتفاق می‌افتد اما به دلیل افزایش سرعت انتقال از حالت آلوده به حالت مصون شده، از میزان گره‌های آلوده کاسته می‌شود.

با مقایسه نمودار حاصل از مدل‌سازی و نمودارهای موجود، حاصل از شبیه‌سازی گسسته- رخداد، اعتبار نتایج مشاهده می‌شود. در منحنی میزان گره‌های مصون شده، مقدار آن در ابتدا

صفر است. با گذشت زمان با تغییر حالت گره‌ها از مستعد به آلوده و سپس مصون‌شده به مقدار آن‌ها اضافه می‌شود و در نهایت در حالت پایدار تمامی گره‌ها در حالت مصون‌شده قرار دارند.

همان‌گونه که در قسمت مقدمه عنوان شد، از آن‌جایی که شبکه‌های بی‌مقیاس، ناهمگن هستند، مصون‌سازی گره‌های مختلف تأثیرات متفاوتی در انتشار خواهد گذاشت. در این شبکه‌ها با توجه به آن که گره‌های هاب اتصالات زیادی را به خود اختصاص داده‌اند، مصون کردن آن‌ها تأثیر بسیار بیشتری از مصون کردن گره‌های غیرهاب بر روند انتشار خواهد گذاشت. برای ارزیابی نحوه انجام مصون‌سازی در روند انتشار، با توجه به این قاعده که در شبکه‌های بی‌مقیاس، بیست درصد از گره‌ها، هشتاد درصد از اتصالات را به خود اختصاص داده‌اند، در ابتدا به مصون کردن بیست‌درصد از گره‌ها به‌صورت تصادفی پرداخته شده است. سپس این بیست درصد به‌صورت هدفمند از میان گره‌های هاب انتخاب شده‌اند و در نهایت نمودار حاصل از هر دو نوع مصون‌سازی رسم شده است. نمودار شکل (۹) مقایسه‌ای میان این دو روند مصون‌سازی را به نمایش گذاشته است. در این نمودار، منحنی بالا نشان‌دهنده روند انتشار در صورت مصون‌سازی تصادفی بیست درصد از گره‌های شبکه است. منحنی پایین نشان‌دهنده روند انتشار در صورت مصون‌سازی هدفمند بیست درصد از گره‌های هاب شبکه است. همان‌طوری که در شکل مشخص است، در صورت مصون‌سازی گره‌های هاب، میزان آلودگی شبکه به شدت کاهش پیدا خواهد کرد.



شکل (۹). مقایسه روند انتشار درصورت مصون‌سازی تصادفی و هدفمند

۷- نتیجه‌گیری

در شبکه‌های بی‌مقیاس با توجه به این که گاه اندازه شبکه بسیار بزرگ می‌شود، مدل‌سازی با استفاده از روش‌های سنتی پیچیده و زمان‌بر خواهد بود. از این رو برای افزایش سرعت مدل‌سازی، از مدل‌سازی سیّال استفاده شد.

از این‌رو، در این مقاله روشی پیشنهاد شده است که در آن نیازی به مدل‌سازی جزئیات شبکه و همه گره‌های آن نیست. در واقع در این روش با توجه به نحوه اتصال گره‌ها، گره‌هایی که در مجاورت یکدیگر هستند در دسته‌های یکسانی به‌طور فشرده قرار می‌گیرند که به آن‌ها ابرگره گفته می‌شود. سپس به جای در نظر گرفتن جزئیات آلودگی در تک‌تک گره‌ها، میزان آلودگی و نحوه انتشار آلودگی در این ابرگره‌ها در نظر گرفته می‌شود. در حالت کلی در این نوع مدل اهمیتی ندارد که در یک لحظه خاص وضعیت هر کدام از گره‌ها به چه صورت است و تنها کافی است که بدانیم وضعیت کلی شبکه به چه صورت است. به عنوان مثال، چند درصد از گره‌ها در یک لحظه آلوده هستند. برای مدل‌سازی چگونگی انتشار، در صورتی‌که یک گره آلوده باشد، می‌تواند با نرخ خاصی آلودگی را به گره‌های همسایه خود به صورت پیوسته و سیّال منتقل کند. این روش با توجه به این که برای انجام مدل‌سازی دانستن جزئیات مولفه‌های مختلف ضروری نیست، پیچیدگی محاسباتی اجرای مدل شبیه‌سازی را به‌طور چشمگیر کاهش خواهد داد. زیرا، تعداد گره‌های شبکه به شدت کاهش پیدا نموده‌اند.

مدل پایه شبیه‌سازی سیّال مورد استفاده، روش SIR است که در آن گره‌ها در ابتدا به‌صورت مستعد آلودگی هستند. سپس به حالت آلوده و در نهایت پاک‌شده تغییر حالت می‌دهند. برای هر کدام از این تغییر حالات نرخ تعیین‌شده‌ای وجود دارد. برای انجام مدل‌سازی از ابزار شبیه‌سازی نت‌لوگو استفاده شده است. در نت‌لوگو مدل‌سازی به‌صورت عامل‌مبنا است. در این نوع از مدل‌سازی در ابتدا عامل‌ها تعریف می‌شوند. سپس بر اساس معیارهای مختلف نحوه رفتار این عامل‌ها را به‌گونه‌ای مشخص می‌شوند که به رفتار آن‌ها در دنیای واقعی نزدیک باشد.

به‌دلیل این که هدف این پژوهش نشان دادن امکان استفاده از شبیه‌سازی سیّال و فواید آن بوده است، اندازه ابرگره‌ها که حاصل چکیده‌سازی گراف اولیه شبکه و متأثر از مشخصات آن هستند، در طراحی سناریوهای شبکه اولیه و آزمایش‌های انجام شده لحاظ نشده‌اند. از این‌رو، پرداختن به این موضوع به عنوان یکی از کارهای آتی پیشنهاد می‌شود.

در ادامه این پژوهش در آینده می‌توان به مدل‌های دیگر شبکه‌های بی‌مقیاس، غیر از مدل باراباسی- آلبرت، توجه نمود و آنها را به‌صورت سیّال مدل‌سازی نمود. همچنین، مدل‌های همه‌گیری شناختی دیگر به جای مدل SIR می‌توانند مورد استفاده قرار گیرد. در نهایت، تعمیم مدل پیشنهادی با در نظر گرفتن نحوه پویش کرم (در مورد کرم‌های فعال) می‌تواند موضوع پژوهش دیگری باشد.

۸- مراجع

[1] W. Yu, S. Chellappan, X. Wang, and D. Xuan, "Peer-to-peer system-based active worm attacks: modeling, analysis and defense," Computer Communications, vol. 31, no. 17, pp. 4005-4017, 2008.

[2] Y. Zhuo, Y. Peng, C. Liu, Y. Liu, and K. Long, "Improving the attack tolerance of scale-free networks by adding and hiding edges," Physica Scripta, vol. 83, p. 025801, 2011.

[3] G. Yong-Wang, S. Yu-Rong, and J. Guo-Ping, "Epidemic spreading in scale-free networks including the effect of individual vigilance," Chinese Physics B, vol. 21, p. 010205, 2012.

[4] E. G. Im, J. S. Kim, I. W. Noh, and H. J. Jang, "A hybrid model for worm simulations in a large network," In Proceedings of the Intelligence and Security Informatics, Springer, pp. 301-306, 2007.

[5] A.-L. Barabási and R. Albert, "Emergence of scaling in random networks," Science, vol. 286, pp. 509-512, 1999.

[6] R. Harrison, the Bitdefender, 2004. Website. [Online]. http://www.bitdefender.com/files/KnowledgeBase/file/Antivirus_Defense-in-Depth_Guide

[7] M. Boguná, R. Pastor-Satorras, and A. Vespignani, "Absence of epidemic threshold in scale-free networks with degree correlations," Physical Review Letters, vol. 90, p. 028701, 2003.

[8] H. Trottier and P. Philippe, "Deterministic modeling of infectious diseases: theory and methods," The Internet Journal of Infectious Diseases, vol. 1, p. 3, 2001.

[9] S. Meloni, A. Arenas, and Y. Moreno, "Traffic-driven epidemic spreading in finite-size scale-free networks," In Proceedings of the National Academy of Sciences, vol. 106, pp. 16897-16902, 2009.

[10] C. M. Macal and M. J. North, "Tutorial on Agent-based Modelling and Simulat ion," Journal of Simulation, vol. 4, no. 3, pp. 151-162, 2010.

[11] E. G. Im, J. S. Kim, I. W. Noh, and H. J. Jang, "A hybrid model for worm simulations in a large network," In Proceedings of the Intelligence and Security Informatics, Springer, pp. 301-306, 2007.

[12] S. Hosseini, M. Abdollahi Azgomi, and A. Torkaman Rahmani, "Malware propagation modeling considering software diversity and immunization," Journal of Computational Science, vol. 13, Elsevier, pp. 49-67, March 2016.

[13] S. Hosseini, M. Abdollahi Azgomi, and A. Torkaman Rahmani, "Agent-based simulation of the dynamics of malware propagation in scale-free networks," Simulation: Transactions of the Society for Modeling and Simulation International, vol. 92, no. 7, SAGE, pp. 709-722, July 2016.

[14] S. Hosseini and M. Abdollahi Azgomi, "A model for malware propagation in scale-free networks based on rumor spreading process," Computer Networks, vol. 108, Elsevier, pp. 97-107, Oct. 2016.

[15] A. Barabasi and E. Bonabeau, Scale-Free Networks. Scientific American, 2003.

[16] E. G. Im, J. T. Seo, D.-S. Kim, Y. H. Song, and Y. Park, "Hybrid modeling for large-scale worm propagation simulations," In Proceedings of the Conference on Intelligence and Security Informatics, Springer, pp. 572-577, 2006.

[17] C. C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling and analysis," In Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 138-147, 2002.

[18] C. M. Macal and M. J. North, "Tutorial on Agent-based Modelling and Simulat ion," Journal of Simulation, vol. 4, no. 3, pp. 151-162, 2010.

A Method for Fluid Modeling of the Propagation Behavior of Malware in Scale-Free Networks

S. Koochaki, **M. Abdollahi Azgomi***

*Iran University of Science and Technology

(Received: 28/02/2015, Accepted: 03/05/2016)

ABSTRACT

Scale-free network (SFN) is a conceptual model for online social networks and peer-to-peer networks, which exhibit a power-law degree distribution. Due to these characteristics, these networks are more vulnerable to the spread of malware (such as virus and worm). Modeling and simulation methods are used to evaluate the propagation behavior of malware in scale-free networks and analyze the defense strategies against malware propagation. To do so, a high number of events should be processed and details of network nodes should be considered. This makes the existing discrete-event simulation methods inappropriate for running on large and complex networks. Hence, for modeling the propagation behavior of malware, fluid models, which need not know the details of network, seems to be more appropriate. In this paper, for fluid simulation of malware propagation, a scale-free network is conceptually represented as a backbone network including supernodes, any one of which includes several nodes of the network. Each supernode in the case of infection can propagate pollution as a fluid flow to its neighboring nodes. Therefore, the main process of malware propagation can be modeled without considering the details of every node. To evaluate the proposed method, an agent-based simulation method has been used. The evaluation results show that large scale-free networks can be modeled and the propagation of malware can be studied using the proposed approach. In addition, the effect of random and targeted immunization of nodes on the proposed models is evaluated as a case study.

Keywords: Scale-Free Networks, Propagation Modeling, Malware Propagation, Fluid Modeling, Agent-Based Simulation, NetLogo

* Corresponding Author Email: azgomi@iust.ac.ir