مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"

سال اول، شماره ۴، زمستان ۱۳۹۲، ص ۸-۱

افزایش اثربخشی رفتار کاربران شبکه‌های نظیر به نظیر در انتشار کرم‌واره‌های غیرفعال

محمدرضا حسنی آهنگر[۱]، محمود فروغی[۲*]

۱- استادیار، دانشگاه جامع امام حسین (ع)، ۲- دانشجوی دکتری دانشگاه جامع امام حسین (ع)

(دریافت: ۹۲/۰۶/۰۳ ، پذیرش: ۹۲/۱۰/۱۴)

چکیده

در این مقاله روش‌های مختلف مدل‌سازی کرم‌واره‌های غیرفعال در شبکه‌های نظیر به نظیر مورد بررسی و مطالعه قرار گرفته است. هدف این مدل‌ها مشخص کردن چگونگی و سرعت انتشار این بدافزارها در بستر شبکه است. در این راستا ابتدا چند مدل مطرح از انتشار کرم‌واره‌های غیرفعال معرفی گردیده و ویژگی‌های هر مدل مورد بررسی قرار گرفته، و به تفاوت‌ها و برتری‌های آنها نسبت به یکدیگر اشاره می‌شود. سپس با افزودن پارامترهایی نحوه تاثیر رفتار کاربران بر سرعت انتشار کرم‌واره‌ها در مدل اعمال گردید و با شبیه‌سازی مدل، نشان داده شده که نحوه رفتار کاربران بر افزایش سرعت انتشار آلودگی در این شبکه‌ها حداقل ۳ برابر تاثیر مستقیم دارد.

واژه‌های کلیدی: مدل انتشار، شبکه نظیر به نظیر، کرم‌واره غیرفعال

۱. مقدمه

کرم‌واره‌ها یکی از تهدیدات مهم امنیتی در شبکه‌های کامپیوتری هستند. مدل‌سازی و ارزیابی رفتار و نحوه گسترش آنها در شبکه راه خوبی برای شناخت آنها و طراحی اقدام دفاعی در برابر آنها می‌باشد. هر چند کرم‌واره‌های فعال به دلیل قابلیت جستجو و گسترش خودبخودی و سرعت انتشار بالا بیشتر مورد مطالعه قرار گرفته‌اند ولی در سال‌های اخیر با گسترش شبکه‌های نظیر به نظیر در بستر اینترنت و حجم بالای مبادله اطلاعات در آنها برای کرم‌واره‌های غیر فعال نیز این امکان به وجود آمده تا با چسبیدن به ترافیک این شبکه‌ها با سرعت بیشتری در بین گره‌های یک شبکه نظیر به نظیر گسترش یابند. بنابراین این نوع از کرم‌واره‌ها نیز کم‌کم مورد توجه محققین قرار گرفتند. به دلیل شباهت‌های موجود، برای مدل‌سازی انتشار کرم‌واره‌ها در شبکه معمولاً از مدل‌های انتشار بیماری‌های بیولوژیک استفاده می‌شود [۱]. شبکه نظیر به نظیر یک الگو برای تعامل عضوهای شبکه با یکدیگر است به صورتی که هر دو گره‌ای بدون یک کنترل مرکزی می‌توانند با یکدیگر ارتباط برقرار کرده و اطلاعات را بین یکدیگر به اشتراک گذارده و مبادله نمایند.

این الگو در مقابل معماری سرویس‌گیرنده/ سرویس‌دهنده قرار می‌گیرد. در این شبکه یک نظیر می‌تواند هم تأمین کننده یک یا چند منبع باشد و هم مصرف کننده مستقیم و بدون واسطه منابعی که نظیرهای دیگر فراهم کرده‌اند باشد [۲]. برخی از مزایای این شبکه‌ها عبارتند از:

- این سامانه‌ها با اجتناب از وابسته کردن سامانه به یک مدیریت متمرکز، باعث افزایش مقیاس‌پذیری سامانه می‌شوند.
- گره‌ها به طور مستقیم با یکدیگر ارتباط دارند و بنابراین نیاز به یک ساختار پرهزینه برای برقراری ارتباط بین گره‌ها و مدیریت آن نخواهیم داشت.
- به‌دلیل مقیاس‌پذیری بالای آن، امکان افزایش تعداد گره‌های سامانه و در نتیجه افزایش منابع در دسترس سامانه فراهم شده و سامانه قدرتمندی ایجاد خواهد شد.

این شبکه‌ها روش مناسبی برای به اشتراک‌گذاری اطلاعات بین مردم در بستر اینترنت فراهم می‌کنند. به همین دلیل امروزه به‌صورت گسترده برای مبادله اطلاعات در بستر اینترنت به‌کار می‌روند و برخی از آنها با داشتن میلیون‌ها عضو بخش عمده‌ای از ترافیک اینترنت را به خود اختصاص داده‌اند. از شبکه‌های نظیر به نظیر

* رایانامه نویسنده پاسخگو: mforooghy@ihu.ac.ir

معروف می‌توان به آی‌مش[1]، کازا[2]، نپستر[3]، ناتلا[4] و فری‌نت[5] اشاره کرد[۲]. کرم‌واره یک نرم‌افزار بدخواه (بدافزار) است که می‌تواند نسخه‌های متعددی از خودش را تکثیر کرده و در فضای شبکه گسترش یابد. کرم‌واره‌های فعال برنامه‌های خودمختاری هستند که از طریق شبکه‌های کامپیوتری با انجام جستجو، حمله و آلوده کردن رایانه‌ها از راه دور پخش می‌شوند.

کرم‌واره‌های غیرفعال معمولا خودشان را به پوشه‌های اشتراکی می‌چسبانند، و با دانلود و اجرای این فایل‌ها توسط سایر نظیرها انتشار پیدا می‌کنند. این کرم‌واره‌ها در پوشه‌های اشتراکی نظیرهای آلوده، تحت چندین نام مختلف مقیم می‌شوند. هنگامی که سایر نظیرها یکی از آن فایل‌ها را دانلود می‌کنند، کرم‌واره‌ها در این میزبان گسترش پیدا می‌کنند و هنگامی که کاربر، فایل را اجرا می‌کند کرم خودش را با چندین نام مختلف و فریبنده در پوشه‌های به اشتراک گذاشته شده قربانی جدید کپی می‌کند و منتظر قربانی‌های بعدی می‌ماند. در مقایسه با کرم‌واره‌های فعال، کرم‌واره‌های غیرفعال به آرامی در اینترنت انتشار پیدا می‌کنند اما شبکه‌های نظیر به نظیر با میلیون‌ها کاربر (مثل بیت تورنت[6]) بستر مناسبی برای انتشار آنها هستند. به عنوان نمونه در سال ۲۰۰۱ کرم‌واره کد- رد[7] در کمتر از ۱۴ ساعت ۳۵۹۰۰۰ رایانه متصل به اینترنت را آلوده کرد. بر خلاف کرم‌واره‌های فعال، کرم‌واره‌های غیرفعال در حین انتشار رفتار غیر- طبیعی عمده‌ای ندارند و این امر تشخیص آنها را دشوار می‌کند.

در این مقاله ابتدا سابقه کارهای انجام شده روی کرم‌واره‌ها مرور می‌شود. در بخش بعدی برخی مدل‌های قبلی معرفی و بررسی شده و نیز به اقداماتی که برای بهبود وضعیت این مدل‌ها انجام گردیده اشاره می‌گردد و سرانجام در بخش پایانی با افزودن پارامترهایی به مدل‌های موجود، اثر رفتار کاربران در مدل اعمال گردیده و نتایج مورد انتظار از طریق شبیه‌سازی نمایش داده شده است.

۲. سابقه

اولین کرم‌واره شناخته شده رایانه‌ای در سال ۱۹۸۸ با عنوان موریس به رایانه‌های با سامانه عامل یونیکس حمله کرد و حدود پنج تا ده درصد از فضای اینترنت را آلوده کرد [۳]. در ۱۱ جولای ۲۰۰۱ کرم‌واره‌ی کد- رد حدود ۳۶۰۰۰۰ رایانه متصل به اینترنت را ظرف مدت کمتر از ۱۴ ساعت اشغال کرد. خسارت ناشی از این حمله در آن زمان بالغ بر دو و نیم میلیارد دلار برآورد گردید [۴]. در سال ۲۰۰۲ استنی فورد[8] در یک کار تحقیقاتی با حمایت مالی دارپا[9] یک مدل کلاسیک ریاضی برای نحوه‌ی انتشار کد- رد ارائه کرد [۵]. اولین بار نمایش ریاضی انتشار بیماری‌ها بنام مدل اپیدمیک توسط کندریک[10] و با عنوان کاربردهای ریاضیات در مسائل پزشکی حدود صد سال پیش ارائه شد [۶]. در مدل دیگری که در سال ۲۰۰۲ توسط زو[11] ارائه شد تأثیر ترافیک شبکه و اقدامات پیشگیرانه انسانی نیز در نظر گرفته شده بود [۷]. در ۲۰۰۳ چن[12] یک مدل گسسته زمان برای کرم‌واره‌ها ارائه کرد [۸]. در این مدل برای عواملی مثل ترمیم و پاک‌سازی ایستگاه‌های کاری هم پارامترهایی تعریف شده بود. در همان سال سندین[13] یک روش برای تشخیص کرم‌واره‌ها با استفاده از شبکه‌های نظیر به نظیر ارائه کرد [۹].

در سال‌های ۲۰۰۴ و ۲۰۰۵ یو و همکارانش نتیجه تحقیقاتشان بر روی انتشار کرم‌واره‌های غیرفعال در بستر شبکه‌های نظیر به نظیر را منتشر کردند[۱۰ و ۱۱].

سه مدل انتشار برای کرم‌واره‌ها توسط چائوشنگ فنگ[14] و همکارانش در سال ۲۰۰۸ ارائه شد [۱۲]. این مدل‌ها (SIR,SIS,SI) که هر کدام برای مرحله‌ای از فرآیند انتشار کرم‌واره‌ها تعریف شده بودند نسبت به سایر مدل‌ها معروف‌تر شده و مبنای بسیاری از تحقیقات بعدی قرار گرفتند. به عنوان مثال، در همان سال بوژان و همکارانش با استفاده از مدل SI چند روش دفاعی در برابر کرم‌واره‌ها ارائه کردند [۱۳]. یک مدل پیشنهادی دیگر برای انتشار کرم‌ها در شرایط وجود اقدامات تدافعی در سال ۲۰۰۹ و توسط توتونجی[15] ارائه گردید [۱۴]. در ۲۰۱۲ آقای خنجری و همکارانش یک مدل بهبود یافته بر پایه مدل‌های SI, SIS و SIR ارائه کردند [۱۵]. ما در ادامه این مدل‌های اخیر را مورد بررسی قرار می‌دهیم.

۳. مدل‌های SI, SIS و SIR

همان طور که قبلاً اشاره شد این مدل‌ها در سال ۲۰۰۸ ارائه شدند و مبنای بسیاری از کارهای بعدی بوده‌اند [۱۲]. به دلیل آنکه شبکه‌های نظیر به نظیر سامانه‌های پیچیده‌ای هستند برای امکان- پذیر شدن مدل‌سازی و تحلیل آنها، معمولاً از پیش‌فرض‌هایی برای ساده کردن مسئله استفاده می‌شود.

1- iMesh
2- KaZaa
3- Napster
4- Gnutella
5- FreeNet
6- BitTorrent
7- Code-Red
8- Staniford
9- DARPA
10- M.Kendrick
11- Zou
12- Chen
13- J.Sandin
14- ChaoshengFeng
15- OssamaToutonji

پیش فرض‌های این مدل به شرح زیر می‌باشند:

- توپولوژی شبکه استاتیک و تعداد کل اعضای آن (نظیرها) عدد ثابتی است که در مدل با N(t) نشان داده شده است. تعداد فایل‌ها نیز ثابت بوده و هیچ فایلی به فایل‌های به اشتراک گذارده، اضافه نمی‌شود.
- هر کاربر تمام فایل‌هایی را که می‌خواهد با دیگران به اشتراک بگذارد را در یک پوشه‌ی مشترک[1] قرار می‌دهد.
- تمام کاربران، فایل‌ها را در پوشه‌ی مشترکشان دانلود می‌کنند.
- پس از اتمام دانلود یک فایل یک بار اجرا می‌شود.
- زمان جستجو، اتصال، دانلود و اجرای یک فایل برای همه فایل‌ها عدد ثابتی بوده و با عنوان واحد زمانی[2] شناخته می‌شود. یک واحد زمانی طول می‌کشد که دانلودکننده فایل، آلوده شده یا مصون بماند.
- وقتی یک نظیر (ایستگاه کاری) آلوده می‌شود C عدد فایل آلوده با نام‌های مختلف در پوشه‌ی مشترک مستقر می‌شوند. تمام نظیرهای آلوده همان C عدد فایل را به اشتراک می‌گذارند. پارامترها و نمادهای مورد استفاده در مدل در جدول ۱ آمده‌اند.

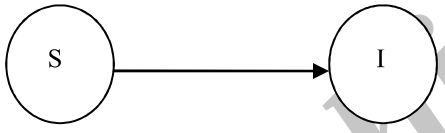
جدول ۱. پارامترها و نمادهای مدل

نماد پارامتر	شرح پارامتر
N(t)	تعداد تمام اعضای شبکه که در اینجا عدد ثابتی‌است.
S(t)	تعداد نظیرهای مستعد در زمان t
I(t)	تعداد نظیرهای آلوده شده در زمان t
R(t)	تعداد نظیرهای بازیابی شده در زمان t
K(t)	تعداد فایل‌های آلوده شده در زمان t
M(t)	تعداد فایل‌های آلوده نشده در زمان t
h(t)	احتمال دانلود فایل‌های آلوده در زمان t $h(t)=\alpha\frac{K(t)}{M(t)+K(t)}$
λ_d	نرخ دانلود فایل جدید توسط هر نظیر
λ_{is}	نرخ تبدیل یک نظیر آلوده به نظیر مستعد پس‌از بازیابی
λ_{sr}	نرخ تبدیل یک نظیر مستعد به نظیر بازیابی شده
λ_{ir}	نرخ تبدیل یک نظیر آلوده شده به نظیر بازیابی‌شده

۱.۳. مدل SI

در این مدل هر نظیر در شبکه دو حالت دارد: یا مستعد آلودگی است (S) و یا آلوده شده است (I). نظیرهای مستعد هیچ فایل آلوده‌ای را به اشتراک نمی‌گذارند ولی در معرض خطر دانلود فایل‌های آلوده هستند و وقتی فایل آلوده‌ای را دانلود و اجرا می‌کنند بلافاصله آلوده می‌شوند.

احتمال دانلود کردن فایل‌های آلوده متناسب با نسبت فایل های آلوده به کل فایل‌های شبکه است که با h(t) نمایش داده شده است. پارامتر ثابت α تنظیم کننده‌ای است که با تنظیم مقدار آن می‌توان احتمال انتشار را به عدد واقعی نزدیک‌تر کرد. در یک واحد زمانی یک نظیر مستعد λ_d فایل را دانلود می‌کند، احتمال اینکه فایل‌ها آلوده باشند برابر h(t) است. بنابراین احتمال آنکه یک نظیر مستعد آلوده شود $\lambda_d h(t)$ برابر است. در نتیجه آهنگ تغییر S برابر $-\lambda_d h(t)S(t)$ است. کاملاً واضح است که آهنگ تغییر I برخلاف آهنگ تغییر S است. هنگامی که یک نظیر مستعد آلوده می‌شود، تعداد فایل های آلوده C عدد افزایش می‌یابد. بنابراین آهنگ تغییر K برابر با $\lambda_d h(t)S(t).c$ است. برای مدل SI فرض می‌کنیم یک گره‌ی مستعد پس از آلوده شدن در همان وضعیت باقی می‌ماند بنابراین نمودار پیشرفت حالت آن به صورت شکل ۱ خواهد بود:



شکل ۱. نمودار پیشرفت حالت مدل SI

درنتیجه معادلات دیفرانسیل مدل SI به‌شرح زیر خواهد بود:

$$\frac{ds(t)}{dt} = -\lambda_d . h(t) . S(t) \qquad (۱)$$

$$\frac{dI(t)}{dt} = \lambda_d . h(t) . S(t) \qquad (۲)$$

$$\frac{dk(t)}{dt} = \lambda_d h(t) . S(t) . c \qquad (۳)$$

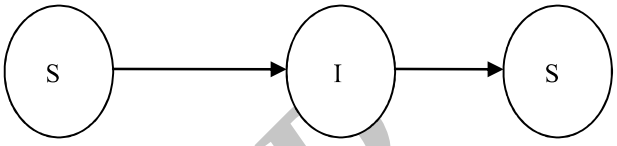
$$\frac{dM(t)}{dt} = \lambda_d N\left(1 - h(t)\right) \qquad (۴)$$

$$N(t) = S(t) + I(t)$$

1- Share Folder
2- Time Unit

۲.۳. مدل SIS

نمودار پیشرفت حالت در این مدل برابر شکل ۲ است. یعنی وقتی تمام فایل‌های آلودهٔ یک نظیر آلوده به‌صورت طبیعی از بین برود یا پاک شود آن نظیر دوباره به حالت مستعد باز می‌گردد. به‌نظر مؤلف شکل ۳ نمودار پیشرفت حالت این مدل را به نحو واقعی تری نشان می‌دهد.



شکل ۲. نمودار پیشرفت حالت مدل SIS

شکل۳. نمودار پیشرفت حالت اصلاح شده برای مدل SIS

بر این اساس معادلات دیفرانسیل مدل SIS را می‌توان به صورت زیر نوشت:

$$\frac{ds(t)}{dt} = -\lambda_d h(t)S(t) + \lambda_{is} I(t) \quad (۵)$$

$$\frac{dI(t)}{dt} = \lambda_d h(t)S(t) - \lambda_{is} I(t) \quad (۶)$$

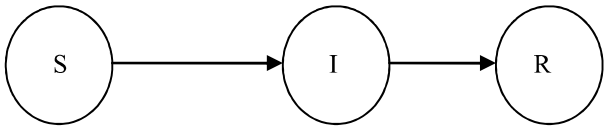
$$\frac{dk(t)}{dt} = c\lambda_d h(t)S(t) - c\lambda_{is} I(t) \quad (۷)$$

$$\frac{dM(t)}{dt} = \lambda_d N\left(1 - h(t)\right) \quad (۸)$$

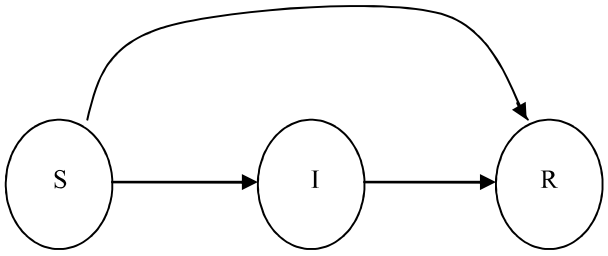
$$N(t) = S(t) + K(t)$$

۳.۳. مدل SIR

همچنان که آلودگی کرم‌واره‌ها افزایش می‌یابد کاربران متوجه حضور آنها در شبکه شده و تدابیری مثل ترمیم سامانه ها و به‌روزآوری آنتی‌ویروس‌ها را اتخاذ می‌کنند که نتیجه آن ایمن شدن بخشی از ایستگاه‌های کاری است. این ایستگاه‌ها را با عنوان نظیرهای بازیابی شده (R) می‌شناسیم و فرض می‌کنیم که آنها دیگر آلوده نخواهند شد. با فرض آنکه نظیرهای مستعد و نظیرهای آلوده به ترتیب به نسبت $\lambda_{ir}I(t)$ و $\lambda_{sr}S(t)$ پاک‌سازی شوند، آهنگ تغییر نظیرهای پاک‌شده برابر $\lambda_{sr}S(t)+\lambda_{ir}I(t)$ خواهد بود. در همان زمان فایل‌های آلوده با نرخ $C\lambda_{ir}I(t)$ کاهش می‌یابند. نمودار پیشرفت حالت این مدل به صورت شکل ۴ خواهد بود که با توجه به آنکه بر اساس فرضیات مدل برخی نظیرها مستقیما از حالت مستعد به حالت بازیابی تغییر وضعیت می‌دهند شکل ۵ تناسب بیشتری با این فرضیات دارد (مؤلف).



شکل ۴. نمودار پیشرفت حالت مدل SIR



شکل ۵. نمودار پیشرفت حالت اصلاح شده برای مدل SIR

با توجه به نکات فوق معادلات دیفرانسیل مدل SIR را می‌توان به‌صورت زیر نوشت:

$$\frac{ds(t)}{dt} = -\lambda_d h(t)S(t) - \lambda_{sr} S(t) \quad (۹)$$

$$\frac{dI(t)}{d(t)} = \lambda_d h(t)S(t) - \lambda_{ir} I(t) \quad (۱۰)$$

$$\frac{dR(t)}{d(t)} = \lambda_{sr} S(t) + \lambda_{ir} I(t) \quad (۱۱)$$

$$\frac{dk(t)}{d(t)} = C\lambda_d h(t)S(t) - C\lambda_{ir} I(t) \quad (۱۲)$$

$$\frac{dM(t)}{dt} = \lambda_d N\left(1 - h(t)\right) \quad (۱۳)$$

$$N(t) = S(t) + I(t) + R(t)$$

۴.۳. بررسی مدل

اگر چه مدل‌های فوق کارایی خوبی داشتند و مدل‌های نسبتا مناسبی برای انتشار بودند اما برخی فرضیات موجود در آنها با فضای واقعی تطابق نداشت. در این بخش به برخی از این موارد اشاره می‌کنیم.

- ثابت فرض کردن تعداد نظیرهای برخط، (تعداد ایستگاه‌های کاری) و تعداد فایل‌های به اشتراک گذارده شده که این با طبیعت شبکه‌های نظیر به نظیر سازگار نیست و در عمل محیط این شبکه‌ها در مدل به یک محیط ایستا تبدیل شده است.
- غفلت از متوسط اندازه فایل به عنوان یک پارامتر تأثیرگذار در سرعت انتشار، واضح است که هر چه اندازهٔ فایل بزرگ‌تر باشد زمان انتقال بیشتر شده و نرخ انتشار کاهش می‌یابد.
- در نظر نگرفتن پهنای باند شبکه به‌عنوان عاملی که بر روی سرعت فرآیند انتشار اثر می‌گذارد به‌طور طبیعی پهنای باند بیشتر به معنای سرعت انتشار بیشتر خواهد بود[۱۶].

۵.۳. مدل بهبود یافته

در مرجع [۱۵] تلاش شده برخی کاستی‌های بیان‌شده در مدل‌های فوق برطرف شود. این کار با افزودن چند پارامتر به‌عنوان عوامل تأثیرگذار در فرایند انتشار انجام شده است. در جدول ۲ لیست پارامترهای اضافه شده به مدل اولیه مشاهده می‌شود.

جدول ۲. پارامترهای جدید در مدل بهبود یافته

پارامتر	شرح
S_i	اندازه میانگین فایل‌های آلوده شده
S_{ui}	اندازه میانگین فایل‌های غیر آلوده
b_w	میانگین پهنای باند نظیرها (ایستگاه‌های کاری) در اینجا برای همه ثابت فرض شده است.
λ_{di}	متوسط نرخ دانلود به وسیله هر نظیر، معادل λ_d در مدل پایه است با این تفاوت که در اینجا به نسبت پهنای باند و اندازه فایل‌های آلوده محاسبه می‌شود. $\lambda_{di}=\frac{bw}{si}$
λ_{dui}	متوسط نرخ دانلود فایل‌های غیرآلوده به وسیله هر نظیر $\lambda_{dui}=\frac{b_w}{S_{ui}}$

علاوه بر پارامترهای جدید در فرضیات ابتدایی مدل نیز اصلاحاتی صورت گرفته است. از جمله آنکه تعداد نظیرهای شبکه و نیز تعداد فایل‌ها عدد ثابتی نبوده و می‌تواند در طی شبیه‌سازی تغییر کند. مدل بهبود یافته SI که با عنوان DSI نام‌گذاری شده است دارای همان نمودار پیشرفت حالت و معادلات دیفرانسیل(۱) الی(۴) است. با این تفاوت که در معادلات (۱) الی (۳)، λ_{di} جایگزین λ_d و در معادلهٔ (۴)، λ_{dui} جایگزین λ_d شده است و بدین ترتیب اثر پهنای باند و اندازهٔ فایل‌ها در مدل اعمال گردیده است. بدین ترتیب معادلات (۱۴) الی (۱۷) را می‌توان برای مدل DSI نوشت:

$$\frac{ds(t)}{dt} = -\lambda_{di}.h(t).S(t) \qquad (۱۴)$$

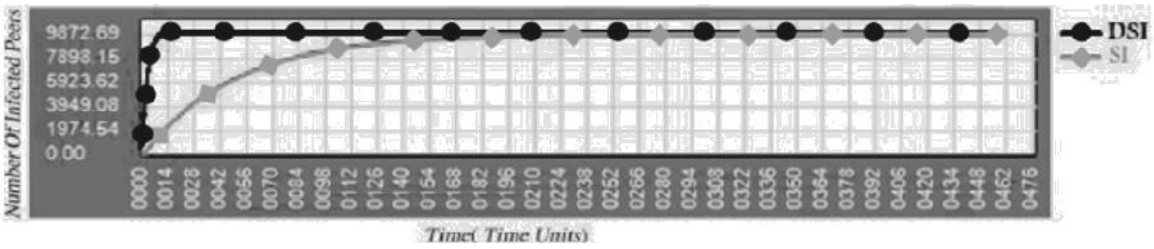
$$\frac{dI(t)}{dt} = \lambda_{di}.h(t).S(t) \qquad (۱۵)$$

$$\frac{dk(t)}{dt} = \lambda_{di}h(t).S(t).c \qquad (۱۶)$$

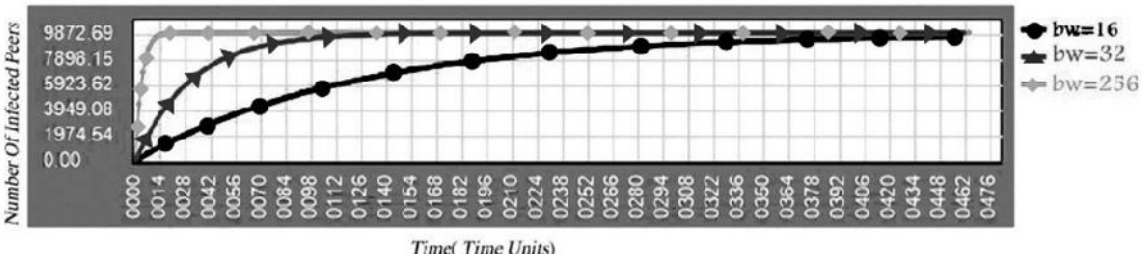
$$\frac{dM(t)}{dt} = \lambda_{dui}N\big(1-h(t)\big) \qquad (۱۷)$$

$$N(t) = S(t) + I(t)$$

به همین طریق می‌توان مدل‌های SIS و SIR را بهبود داده و این مدل‌های بهبودیافته را به ترتیب با نماد DSIS و DSIR نمایش می‌دهیم. در این مدل‌ها تنها با جایگزین کردن دو پارامتر λ_{di}و λ_{dui}، اثر پهنای باند و اندازه‌ی فایل‌ها روی مدل اعمال شد. بر اساس نتایج شبیه‌سازی‌های انجام شده در مرجع [۱۵] می‌توان اختلاف عملکرد این مدل بهبود یافته با مدل پایه را مشاهده نمود. به‌عنوان نمونه در شکل ۶، نمودار مقایسه حاصل از شبیه‌سازی دو مدل SI و DSI آمده است. همچنان‌که از شکل پیداست، هرچند با گذشت زمان مقادیر به‌دست آمده از دو مدل به هم نزدیک می‌شوند اما در ابتدای کار اختلاف قابل توجهی بین دو مقدار مشاهده می‌شود و این اختلاف ناشی از دخالت دادن پهنای باند و اندازه‌ی فایل در مدل DSI است.



شکل ۶. اختلاف خروجی مدل SI با DSI



شکل ۷: تأثیر پهنای باند بر انتشار کرم‌واره‌ها

علاوه بر این در همان مرجع اثر پهنای باند به صورت مستقل بر انتشار کرم‌واره‌ها مورد بررسی قرار گرفت که نتیجه آن در شکل ۷ مشخص شده است.

همان‌طور که اشاره شد با ارائه یک رابطه برای محاسبه‌ی نرخ دانلود فایل‌های آلوده و غیرآلوده برای هر نظیر(λ_{di} و λ_{dui}) اثر پهنای باند و اندازه فایل‌ها در مدل اعمال گردیده است. به نظر می‌رسد عوامل دیگری نیز بر روی نرخ دانلود فایل‌ها موثر باشند که اعمال آنها می‌تواند به واقعی‌تر شدن مدل کمک کند.

به‌عنوان مثال در اختیار داشتن یک الگوی رفتاری از کاربران هنگامی در مورد دانلود یا رها کردن فایل‌ها تصمیم می‌گیرند، می‌تواند در سرعت انتشار آلودگی موثر باشد. البته تهیه چنین الگویی با توجه به آنکه مدل‌سازی رفتار انسانی است چالش‌های خاص خود را دارد.

۴. مدل پیشنهادی

همان‌طوری که قبلا اشاره شد سرعت انتشار کرم‌واره‌های غیر-فعال به نحوه‌ی رفتار کاربران وابسته است و تصمیم‌گیری آنها برای بارگذاری یا رهاکردن یک فایل می‌تواند به روند انتشار یک آلودگی کمک کند و یا سرعت آن را کاهش دهد. برای اعمال الگوی رفتار کاربران در مدل‌های فوق می‌توان یک ضریب λ_{dx} را جایگزین λ_{di} کرد. این ضریب جدید بر اساس رابطه زیر تعریف می‌شود:

$$\lambda_{dx} = \frac{bw}{si} p \qquad (۱۸)$$

در این رابطه p احتمال بارگذاری فایل توسط کاربران از شبکه را نشان می‌دهد. به‌عنوان نمونه اگر کاربران یک شبکه در ۷۵٪ مراجعات به شبکه اقدام به دریافت فایل نمایند آنگاه مقدار p برابر با ۰/۷۵ خواهد بود. بدین ترتیب در مدل جدید علاوه بر پهنای باند و اندازه فایل‌ها عامل موثر رفتار کاربران نیز دخالت داده می‌شود. با تحلیل رابطه فوق به‌سادگی می‌توان به‌این نتیجه رسید که با افزایش احتمال دانلود فایل توسط کاربران مقدار λ_{dx} نیز افزایش خواهد یافت و افزایش این مقدار بر اساس معادله دیفرانسیل (۱۹) می‌بایست باعث افزایش نرخ رشد گره‌های آلوده شود.

$$\frac{dI(t)}{dt} = \lambda_{dx} . h(t) . S(t) \qquad (۱۹)$$

به همین ترتیب با کاهش احتمال بارگذاری فایل و ضریب λ_{dx}، می‌توان انتظار داشت نرخ رشد گره‌های آلوده کاهش یابد. همان‌طور که از مقایسه معادله دیفرانسیل (۱۹) با معادله دیفرانسیل (۲) مشخص است، مدل پیشنهادی که ما نام آن را XSI انتخاب کرده‌ایم، دارای همان نمودار پیشرفت حالت و معادلات دیفرانسیل (۱) الی (۴) است. با این تفاوت که در معادلات (۱) الی (۴)، λ_{dx} جایگزین λ_{d} شده است. برای مدل پیشنهادی XSIS و XSIR که به ترتیب بهبود یافتهٔ مدل‌های DSIS و DSIR هستند نیز دقیقاً همین شرایط وجود دارد.

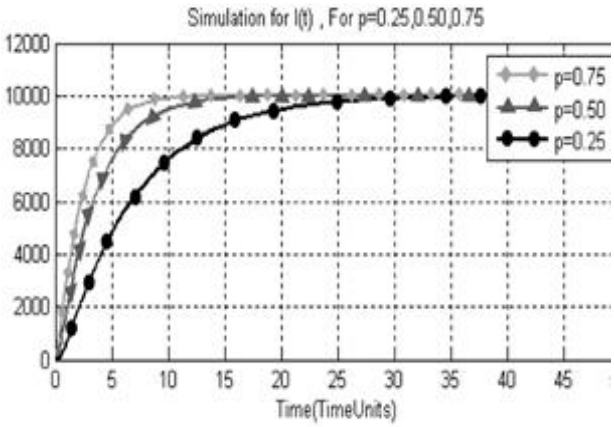
۱.۴. نتایج شبیه‌سازی و ارزیابی

بر اساس فرضیات مسئله، افزایش احتمال بارگذاری فایل از یک نظیر هنگام مراجعه به آن توسط یک کاربر می‌بایست باعث افزایش سرعت انتشار آلودگی در شبکه شود. برای بررسی این مسئله با استفاده از نرم‌افزار MATLAB و با شرایط اولیه جدول ۳ با در نظر

جدول ۳. شرایط اولیه شبیه‌سازی

پارامتر	مقدار	شرح
S(0)	۱۰۰۰۰	تعدادکل میزبان‌های شبکه
I(0)	۱۰	تعداد میزبان‌های آلوده در ابتدا
Bw	۶۴ kbps	پهنای باند
Si	۱۰۰	اندازه میانگین فایل‌های آلوده شده
C	۱۰	تعداد تکثیر فایل آلوده در هر مرحله
α	۱	ضریب اصلاح
K(t)	۱۰	تعداد فایل‌های آلوده شده در زمان t
M(t)	۱۰۰۰	تعداد فایل‌های آلوده نشده در زمان t

گرفتن سه مقدار ۰/۲۵ ، ۰/۵۰ و ۰/۷۵ برای مدل p اجرا شد و به عنوان نمونه برای مدل XSI نتایج شکل ۸ بدست آمد. همچنین از مقایسه شکل ۸ با شکل‌های ۶ و ۷ که مربوط به مدل‌های قبلی هستند ملاحظه می‌شود که در اینجا به‌ازای شرایط ثابت مثل اندازه متوسط فایل‌ها و پهنای باند شبکه، تنها به‌ازای تغییر رفتار کاربران ۳ الگوی انتشار برای کرم‌واره به‌دست آمده است.



شکل۸. تاثیر رفتار کاربران بر سرعت انتشار آلودگی

این در حالی است که مدل‌های قبلی به‌ازای این تغییرات و ثابت ماندن بقیه شرایط تنها یک الگوی انتشار ارائه می‌نمایند، زیرا در تعریف آنها چنین پارامتری در نظر گرفته نشده است. همان‌طور که از نمودار مشاهده می‌شود وقتی کاربران تنها در ۲۵٪ موارد تصمیم به دریافت فایل از یک نظیر می‌گیرند سرعت انتشار کمتر بوده و حدود ۳۰ واحد زمانی طول می‌کشد تا کرم‌واره تمام گره‌های شبکه را آلوده کند. در حالی‌که اگر کاربران در ۷۵٪ موارد اقدام به دریافت و اجرای فایل نمایند کل شبکه در طی ۱۰ واحد زمانی آلوده خواهد شد. به عبارت دیگر سرعت انتشار در این حالت ۳ برابر حالت قبل است. بنابراین همان‌طور که مشاهده می‌شود با فرض ثابت بودن بقیه شرایط الگوی رفتاری کاربران در یک شبکه نظیر به نظیر می تواند سرعت گسترش آلودگی ناشی از کرم‌واره‌ها را تا چندین برابر افزایش دهد.

۵. نتیجه‌گیری

رفتار کرم‌واره‌های غیرفعال برخلاف کرم‌واره‌های فعال برای گسترش در بستر یک شبکه کاملا وابسته به نقل و انتقال فایل‌ها توسط کاربران می‌باشد. بنابراین در مدل‌سازی آنها باید نحوه رفتار کاربران در کنار سایر پارامترهای موثر مثل پهنای باند و اندازه فایل‌ها ، دخالت داده شود. در مدل بهبود یافته با در نظر گرفتن احتمال دانلود فایل در هنگام مراجعه به شبکه، به‌عنوان نماد رفتار کاربران، افزودن این پارامتر به مدل نشان داد که افزایش آن به‌طور مستقیم می‌تواند باعث افزایش سرعت انتشار آلودگی شود. میزان افزایش پارامتر مربوط به رفتار کاربران، به خروجی مدل که میزان انتشار آلودگی است وابسته است. لذا وقتی کاربران تنها در ۲۵٪ موارد که از یک نظیر فایل دریافت می‌کنند سرعت انتشار حدود ۳۰ واحد زمانی طول می‌کشد تا کرم‌واره تمام گره‌های شبکه را آلوده کند. در حالی‌که اگر کاربران در ۷۵٪ موارد اقدام به دریافت و اجرای فایل نمایند کل شبکه در طی ۱۰ واحد زمانی آلوده خواهد شد. به عبارت دیگر سرعت انتشار در این حالت ۳ برابر حالت قبل است. بنابراین با فرض ثابت بودن شرایط معمول، الگوی رفتاری کاربران در یک شبکه نظیر به نظیر با سرعت گسترش آلودگی ناشی از کرم‌واره‌ها یک ارتباط مستقیم خطی دارد.

۶. مراجع

[1] Daley. D. J and Gani. J, Epidemic Modeling: An Introduction, Cambridge, Studies in Mathematical Biology, 2001.

[2] Ramman. M, "P2P Network:onlinepriacy of music,films and computer software", journal of intellectuall property rights,Vol 9, pp 440-461, september 2004.

[3] Guanling. C, Robert S. G, Proceeding InfoScale '06 Proceedings of the 1st international conference on Scalable information systems, Article No. 29 New York, NY, USA ©2006.

[4] Moore, Colleen. S," Code-Red: a case study on the spread and victims of an internet worm", http://www David.caida.org /publications/papers/codered/codered.pdf, 2002.

[5] Staniford. S, Paxson. V, and Weaver. N, How to Own the Internet inYour Spare Time. In Proceedings of the 11th USENIX Security.

[6] Fred. B, "The Kermack–McKendrick epidemic model revisited" ,ELSEVIER,MathematicalBiosciencesVolume 198, Issue 2, Pages 119–131, December 2005.

[7] Zou. C. C, Gong. W, and Towsley. D, "Code Red Worm PropagationModeling and Analysis", In Proceedings of9-th ACM Conference onComputer and Communication Security(CCS), Washington DC,November 2002.

[8] Chen. Z, Gao. L, and Kwiat. K, "Modeling the Spread of Active Worms", IEEE INFOCOM, 2003.

[9] Sandin. J, "P2P systems for worm detection," inDIMACS Workshop on large scale attacks,Piscataway, NJ, USA, September 2003.

[10] Wei. Y, "Analyze the Worm-Based Attack in Large Scale P2PNetworks", In Proceedings of8th IEEE International Symposium on High Assurance Systems Engineering (HASE'04) , 2004.

[11] Wei. Y, Corey. B, SriramChellappan and Dong Xuan, "Peer-to-Peer System-based Active Worm Attacks:Modeling and Analysis", In Proceedings ofIEEE International Conference on Communications (ICC), May 2005.

[12] Feng. C, Qin. Z, Cuthbet. L, and Tokarchuk. L, "Propagation modeling of passive worms in P2P networks," 2008, pp. 1027-1031.

[13] Bo. Z, Laurissa. T, ChaoshengFeng , Zhiguang Qin ," Defense against Passive Worms in P2P Networks" Proceedings of Networking & Electronic Commerce Research Conference (NAEC 2008).

[14] Ossama T. and Seong-Moo Y.," Passive Benign Worm Propagation Modeling with Dynamic Quarantine Defense", KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 3, NO. 1, FEBRUARY 2009

[15] Khanjari. N, S. Ehsan, Azgomi. M.A, A Novel Dynamic Modeling Method of Passive Worms Propagation in Peer to Peer Networks, J. Basic. Appl. Sci. Res., 2(10) 10130-10136, 2012.

[16] Khanjari. N, Present a method for modeling the propagation of passive pollutants in Peer to Peer Networks, Master's thesis, Zanjan Islamic Azad University, 2012 (In Persian).