



Semnan University



Research Article

HD-SEIRS Malware Propagation Model in Heterogeneous Complex Networks

Elham Asadi^a, Soodeh Hosseini^{a,*}

^a Department of Computer Science, Faculty of Mathematics and Computer, Shahid Bahonar University of Kerman, Kerman, Iran

PAPER INFO

Paper history:

Received: 2023-01-13

Revised: 2023-04-10

Accepted: 2024-04-03

Keywords:

Malware propagation modeling;
Basic reproductive ratio;
Scale-free networks (SFNs);
Heterogeneous networks;
Epidemic diseases.

ABSTRACT

In recent years, the Internet has become part of the requirements of human life. With the widespread use of the Internet, the Web, and online social networks, the number of vulnerabilities and security threats has increased significantly. Various types of malwares (worms and viruses) have become a major threat to the security of systems and networks. In this regard, researchers are looking for ways to identify malware and fight against them. One of the methods used in this field is to model the malware propagation in order to identify and combat malware by modeling its behavior. In this article, a malware propagation model based on the propagation of epidemic diseases in a heterogeneous network structure, considering the devices connected to the network and the Internet, is introduced. Modeling is done based on the Susceptible-Exposed-Infected-Recovered epidemic model for devices and Internet networks. The results show that the speed of malware propagation in the proposed HD-SEIRS model is significantly reduced compared to the SEIR model. Also, in this article, the basic reproduction ratio (R_0) is calculated for the proposed model and the effect of parameter changes on the proposed model is investigated.

DOI: <https://doi.org/10.22075/jme.2024.29591.2394>

© 2024 Published by Semnan University Press.

This is an open access article under the CC-BY 4.0 license. (<https://creativecommons.org/licenses/by/4.0/>)

* Corresponding author.

E-mail address: so_hosseini@uk.ac.ir

How to cite this article:

Asadi, E., & Hosseini, S. (2024). HD-SEIRS malware propagation model in heterogeneous complex networks. Journal of Modeling in Engineering, 22(79), 17-28. doi: 10.22075/jme.2024.29591.2394

مدل سازی انتشار بدافزار HD-SEIRS در شبکه های پیچیده ناهمگن

الهام اسدی^۱، سوده حسینی^{۱*}

| اطلاعات مقاله | چکیده |
|---|--|
| دریافت مقاله: ۱۴۰۱/۱۰/۲۳ | در سال های اخیر اینترنت جزئی از الزامات زندگی انسان شده است. با استفاده ی گسترده از اینترنت، وب و شبکه های اجتماعی برخط، تعداد آسیب پذیری ها و تهدیدات امنیتی به میزان قابل توجهی افزایش یافته است. انواع مختلف بدافزارها (کرم ها و ویروس ها) به یک تهدید بزرگ برای امنیت سیستم ها و شبکه ها تبدیل شده اند. در این راستا محققین به دنبال روش هایی برای شناسایی بدافزارها و مبارزه با آنها هستند. یکی از روش های مورد استفاده در این زمینه مدل سازی انتشار بدافزار است تا با مدل کردن رفتار بدافزارها به شناسایی و مبارزه با آنها بپردازیم. در این مقاله یک مدل انتشار بدافزار مبتنی بر انتشار بیماری های همه گیری در ساختار شبکه ای ناهمگن با در نظر گرفتن دستگاه های متصل به شبکه و شبکه ی اینترنت معرفی شده است. مدل سازی بر اساس مدل بیماری های همه گیری مستعد-در معرض آلودگی - آلوده-بهبودیافته برای دستگاه ها و شبکه اینترنت انجام می شود. نتایج نشان می دهد سرعت انتشار بدافزار در مدل پیشنهادی HD-SEIRS در مقایسه با مدل SEIR به طور قابل توجهی کاهش یافته است. همچنین در این مقاله نسبت باز تولید اولیه R_0 برای مدل پیشنهادی محاسبه شده است و اثر تغییرات پارامترها روی مدل پیشنهادی مورد بررسی قرار می گیرد. |
| بازنگری مقاله: ۱۴۰۲/۰۱/۲۱ | |
| پذیرش مقاله: ۱۴۰۳/۰۱/۱۵ | |
| واژگان کلیدی: | |
| مدل سازی انتشار بدافزار، نسبت باز تولید اولیه، شبکه های بی مقیاس، شبکه های ناهمگن، بیماری های همه گیری. | |

DOI: <https://doi.org/10.22075/jme.2024.29591.2394>

© 2024 Published by Semnan University Press.

This is an open access article under the CC-BY 4.0 license. (<https://creativecommons.org/licenses/by/4.0/>)

۱- مقدمه

برنامه های نرم افزاری ناخواسته استفاده می شود. این برنامه ها شامل ویروس ها، کرم ها، تروجان ها، جاسوس افزارها، ربات ها، باج افزارها و ... می باشند. مجرمان سایبری از بدافزارها به عنوان سلاح در دستیابی به اهداف خود استفاده می کنند. به ویژه، بدافزار برای راه اندازی طیف گسترده ای از حملات امنیتی، مانند به خطر انداختن رایانه ها، سرقت اطلاعات محرمانه، ارسال ایمیل های هرزنامه، از بین بردن سرورها، نفوذ به شبکه ها و فلج کردن زیرساخت های حیاتی استفاده شده است. این حملات اغلب منجر به خسارات شدید و خسارات مالی قابل توجهی می شود [۱]. انتشار بدافزارها می تواند به سرعت انجام شود

امروزه اکثر کارهای روزمره از طریق شبکه ی اینترنت صورت می گیرد و بر شمار افرادی که کارهای خود را با استفاده از رایانه و اینترنت انجام می دهند اضافه می شود. از این جهت بایستی بتوانیم بستری را فراهم کنیم که افراد دغدغه ی کمتری از الودگی شبکه داشته باشند. همانند دنیای فیزیکی، افرادی با اهداف مخرب (به عنوان مثال، مجرمان سایبری) در اینترنت وجود دارند. آنها سعی می کنند از کاربران قانونی استفاده کنند و از نظر مالی برای خود سود ببرند. بدافزار (مخفف نرم افزار مخرب)، یک اصطلاح عمومی است که به طور گسترده برای نشان دادن انواع مختلف

* پست الکترونیک نویسنده مسئول: so_hosseini@uk.ac.ir

۱. گروه علوم کامپیوتر، دانشگاه شهید باهنر کرمان، کرمان، ایران

استناد به این مقاله:

۲- کارهای مرتبط

همان‌طور که در بیماری‌های همه‌گیری انتقال آلودگی از فرد آلوده به افراد مستعد باعث انتشار بیماری می‌شود، انتشار ویروس‌ها و بدافزارها نیز به همین شکل است و مطالعاتی نیز بر این اساس انجام شده است [۷]. آلودگی در شبکه می‌تواند از طریق گره‌های آلوده به دیگر بخش‌های شبکه نفوذ پیدا کند و تبدیل به همه‌گیری در شبکه شود. برای جلوگیری از انتشار الودگی در شبکه می‌توان گره‌های آلوده را شناسایی کرد و مکانیسم‌های امنیتی را روی گره‌های آلوده در شبکه اعمال کرد تا از انتشار بدافزار در شبکه جلوگیری شود.

اینترنت در دسته‌ی شبکه‌های بی‌مقیاس قرار دارد که انتشار ویروس‌ها و بدافزارها در این شبکه موضوعی است که توسط محققان بسیاری مورد بررسی قرار می‌گیرد. برای اینکه اثر مکانیسم‌های دفاعی و روش مبارزه با بدافزارها را بتوانیم مورد بررسی قرار دهیم از روش‌هایی چون مدل‌سازی انتشار بدافزار استفاده می‌شود. در مدل‌سازی انتشار جمعیت به گروه‌هایی تقسیم می‌شود. کرمک مکندریک [۸] جمعیت را به سه گروه افراد مستعد، آلوده و بهبودیافته تقسیم کرد و مدل SIR را ارائه داد که در بسیاری موارد به‌عنوان مدل پایه برای مدل‌سازی بیماری‌های همه‌گیری استفاده می‌شود. پس از آن مدل‌های دیگری مثل SEIR ارائه شدند که در این مدل‌ها گروه‌های دیگری به مدل پایه اضافه شد. همچنان که در مدل SEIR گروه افراد با آلودگی نهان (E) نیز اضافه شده است [۹ و ۱۰]. مقالات بسیاری انتشار بدافزار را با استفاده از مدل‌های همه‌گیری گسسته و پیوسته زمان مورد بررسی قرار داده‌اند. در [۷] رفتار بدافزار توسط مدل گسسته زمان SEIRS بر روی دستگاه‌های موبایل مدل شده است. حسینی در [۱۱] به بررسی و مقایسه‌ی استراتژی‌های ایمن‌سازی مختلف مانند ایمن‌سازی تصادفی، ایمن‌سازی هدفمند، ایمن‌سازی آشنا و ایمن‌سازی پرخطر برای جلوگیری از شیوع بدافزار می‌پردازد. همچنین، سه معیار مرکزیت گره (درجه، نزدیکی و بینابینی) را در ایمن‌سازی هدفمند انجام می‌دهد تا روند انتشار بدافزار را کندتر کند. انتشار بدافزار در این مقاله بر اساس مدل همه‌گیری SEIRS-Q مدل شده است. ربرتو و

و منجر به آسیب‌های احتمالی شبکه و اختلال در خدمات آن شود. از این رو، یک گام مهم در جهت جلوگیری از چنین رویدادهایی، مطالعه‌ی رفتار انتشار بدافزار است.

شبکه‌های پیچیده در دو نوع همگن و ناهمگن مورد مطالعه قرار می‌گیرند. شبکه‌های دنیای کوچک و شبکه‌های تصادفی توزیع درجه‌ی همگن و شبکه‌های بی‌مقیاس توزیع درجه‌ی ناهمگن دارند. از دیگر ویژگی‌های شبکه‌های بی‌مقیاس ضریب خوشه‌بندی بالا و توزیع درجه توان و میانگین طول مسیر پایین است. شبکه‌های پیچیده را با ساختار گراف می‌توان نمایش داد. گره‌های شبکه رئوس گراف و ارتباط مابین گره‌ها را با یال‌های گراف می‌توان متناظر کرد [۲].

از دیگر خصوصیات مهم شبکه‌های پیچیده پویایی شبکه است. رفتارهای منحصر به فرد اعضا در کنار یکدیگر در یک شبکه منجر به ایجاد پدیده‌ای مثل انتشار می‌شود. مدل‌های انتشار بیماری‌های همه‌گیر [۳] انتشار شایعه [۴]، شکل‌گیری عقاید [۵] و بازاریابی ویروسی [۶] برای انواع انتشار در شبکه ارائه شده است. با توجه به شباهت‌های موجود بین نحوه‌ی انتشار اطلاعات و بیماری، می‌توان مدل‌های انتشار بیماری‌های همه‌گیری را برای مدل‌سازی رفتار بدافزار در شبکه استفاده کرد. در این شیوه‌ی مدل‌سازی انتشار جمعیت به گروه‌های مستعدین^۲ (S)، در معرض آلودگی^۳ (E)، آلوده^۴ (I) و بهبودیافته^۵ (R) بر اساس نوع مدل تقسیم می‌شود. مدل‌های پایه‌ای مدل‌های SI و SIR هستند.

در این مقاله مدل انتشار بدافزار مبتنی بر مدل SEIR در نظر گرفته شده است. هرکدام از گروه‌های مستعدین، در معرض آلودگی، آلوده و بهبودیافته برای دستگاه‌های متصل به شبکه و گره‌های شبکه‌ی اینترنت به‌صورت مجزا در نظر گرفته شده است (HD-SEIRS^۶). انتشار آلودگی در مدل پیشنهادی نسبت به مدل SEIR کاهش داشته است. بخش‌بندی ادامه‌ی مطالب به این صورت است که در بخش دوم کارهای مرتبط، بخش سوم مفاهیم مقدماتی، بخش چهارم مدل پیشنهادی انتشار بدافزار HD-SEIRS، بخش پنجم ارزیابی مدل پیشنهادی و بخش ششم نتیجه‌گیری آمده است.

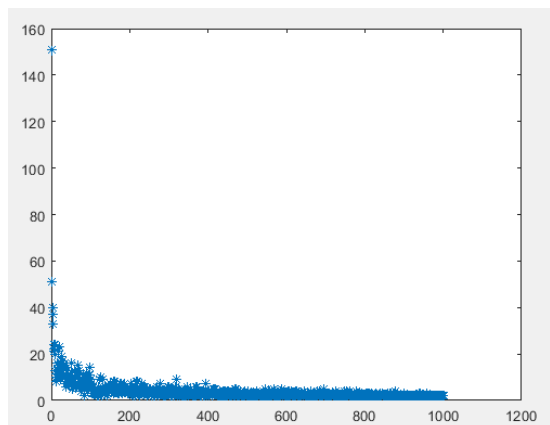
^۵ Recovered

^۶ Host Device-Susceptible Exposed Infected Recovered Susceptible

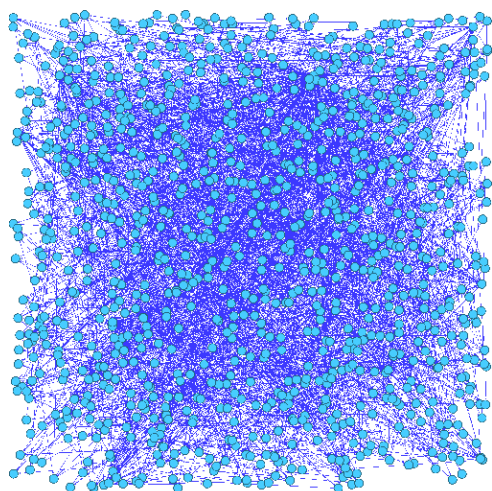
^۲ Susceptible

^۳ Exposed

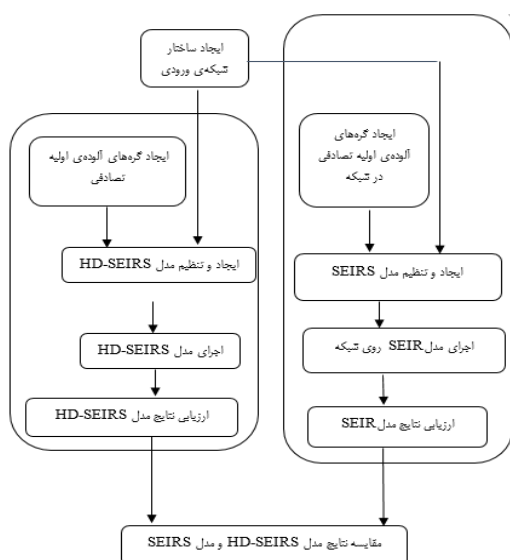
^۴ Infected



شکل (۱-الف) - نمودار توزیع درجه در شبکه



شکل (۱-ب) - شبکه ی باراباسی آلبرت با ۱۰۰۰ گره



شکل ۲- مراحل مدل پیشنهادی

همکاران در مقاله ای به مدل سازی انتشار در دو خوشه ی مستقل که یک کانال ارتباطی مشترک دارند، پرداختند [۱۲].

در زمینه مدل سازی های دو قسمتی کومار میسرا و همکاران [۱۳] یک مدل همه گیری که برای حمله DDoS از طریق دستگاه های اینترنت اشیا بر روی منابع هدف ایجاد شده و پویایی کلی آن تحلیل می شود، ارائه دادند. بخش اول مدل SIS روی گره های خارجی است. این بخش مربوط به چگونگی تشکیل ارتش زامبی هاست. بخش دوم مدل سازی یک حمله ی دیداس توسط زامبی ها روی یک هدف مشخص است که با مدل SIR مدل شده است. در جایی دیگر نیز مدل انتشار بدافزار مناسب برای شبکه های حسگر بی سیم مبتنی بر خوشه برای تجزیه و تحلیل پویایی انتشار بدافزار پیشنهاد شد. این مدل بر ویژگی های انتقال داده بین گره های مختلف در یک شبکه مبتنی بر خوشه تمرکز می کند و پارامترهای کاربردی واقعی شبکه های حسگر بی سیم، مانند شعاع ارتباط گره، چگالی توزیع شده گره و نرخ مرگ گره را در نظر می گیرد (ژو و همکاران [۱۴]). در مقاله ای نیز که در سال ۲۰۲۲ توسط یاداو و همکارش [۱۵] به چاپ رسید یک مدل همه گیری انتشار بدافزار SEIQR-V در شبکه های اینترنت اشیا مطرح شد که مدل مذکور یک مدل همه گیری SEIR با درج دو کلاس دیگر به نام های واکسیناسیون (V) و قرنطینه (Q) است. در اینجا، واکسیناسیون به عنوان یک مدافع فعال برای جلوگیری از شیوع بدافزار عفونی و قرنطینه به معنای جداسازی گره ها از شبکه در حین انجام فرآیند درمان برای حذف بدافزار است.

۳- مدل پیشنهادی انتشار بدافزار

در این بخش به مدل سازی انتشار بدافزار HD-SEIRS مبتنی بر مدل کلاسیک SIR [۸] پرداخته می شود. برای بررسی پویایی انتشار بدافزار بر روی شبکه های بی مقیاس سیستم مبتنی بر مدل HD-SEIRS تحت آزمایش بر روی شبکه ی بی مقیاس ناهمگن از نوع باراباسی آلبرت با ۱۰۰۰ گره و ۴۰۰۰ یال و توزیع توان (۱) قرار گرفته است و نتایج به دست آمده با مدل SEIRS مقایسه شده است. روند اجرای کار در شکل (۲) مشاهده می شود.

۳-۱- توصیف مدل

در این مقاله با استفاده از مدل بیماری‌های همه‌گیری SEIRS با در نظر گرفتن شبکه به دو دسته‌ی دستگاه‌های متصل به شبکه و گره‌های شبکه‌ی اینترنت به مدل‌سازی انتشار بدافزار در شبکه‌های بی‌مقیاس پرداخته می‌شود. نوآوری مدل پیشنهادی به این صورت است که گره‌ها به دودسته طبقه‌بندی می‌شوند. با توجه به طبقه‌بندی گره‌ها روند انتشار آلودگی در شبکه کاهش می‌یابد. طبقه‌بندی گره‌ها در شبکه‌های اینترنت اشیا منجر به شناسایی بهتر گره‌های آلوده و کاهش انتشار آلودگی می‌شود. آلودگی هر دستگاه روی دستگاه دیگر و همچنین روی گره‌های مجاورش در شبکه اینترنت اثر دارد. از طرفی اگر گرهی از شبکه‌ی اینترنت آلوده شود می‌تواند گره هم نوع خود یا دستگاه متصل به شبکه را آلوده کند. با این دیدگاه هر دسته به بخش‌های مستعدین- آلوده‌های نهان - آلوده - بهبود یافته (SEIRS) تقسیم می‌شود. دیاگرام مربوط به مدل پیشنهادی در شکل (۳) آمده است. براین اساس گروه‌های مربوط به مدل به شرح زیر می‌باشند.

مستعدین (S_D و S_H): گره‌هایی هستند که قادرند در تماس با گره‌های آلوده‌شده توسط بدافزار قرار گیرند. S_H گروه مستعدین تشکیل شده از گره‌های شبکه اینترنت و S_D گروه دستگاه‌های مستعد آلودگی است.

در معرض آلودگی (E_D و E_H): به ترتیب گره‌هایی از دسته‌ی گره‌های شبکه و دستگاه‌های متصل به شبکه هستند که به بدافزار آلوده‌اند ولی علائمی ندارد.

آلوده‌ها (I_D و I_H): به گره‌هایی از شبکه‌ی اینترنت یا دستگاه‌های متصل که به بدافزار آلوده شده‌اند و علائم‌دار هستند، گفته می‌شود.

بهبودیافته‌ها (R_D و R_H): گره‌هایی از شبکه یا دستگاه‌هایی هستند که تحت تاثیر نرم‌افزارهای از بین‌بردن بدافزار آلودگی آنها برطرف شده است.

هنگامی که بدافزار در شبکه منتشر می‌شود، گره‌ها طبق قوانین زیر تغییر حالت می‌دهند:

راس مستعدی که در حالت S_H قرار دارد زمانی که در مجاورت همسایه‌ی آلوده‌ی هم نوع خودش قرار گیرد با نرخ β_H آلوده می‌شود ولی هنوز علائم‌دار نشده است و وارد گروه E_H می‌شود. از طرفی این مستعدین می‌توانند آلودگی را با

نرخ ρ_D از دستگاه متصل آلوده‌ای که در مجاورت آنها است دریافت کنند.

گره‌های آلوده‌ای که آلودگی در آنها نهان است با نرخ δ_H علائم آلودگی در آنها ظاهر می‌شود و وارد گروه I_H می‌شوند.

گره‌های آلوده با نرخ γ_H تحت مکانیسم‌های امنیتی قرار گرفته و آلودگی آنها از بین می‌رود و وارد گروه R_H می‌شوند.

گره‌هایی که از آلودگی مصون شده‌اند مجدد امکان آلوده‌شدن توسط انواع دیگر بدافزار را دارند و با نرخ α_H وارد گروه S_H می‌شوند.

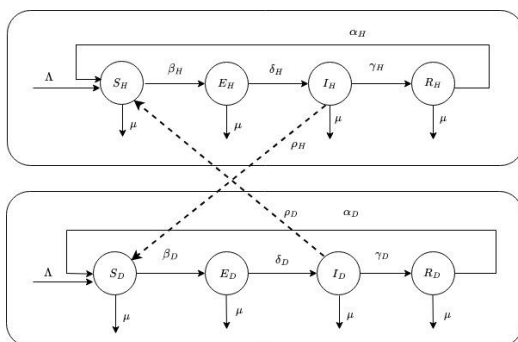
دستگاه متصل به شبکه‌ای که مستعد آلودگی به بدافزار است و در حالت S_D قرار دارد، زمانی که در مجاورت همسایه‌ی آلوده‌ی خودش قرار گیرد با نرخ β_D آلوده می‌شود ولی هنوز علائم‌دار نشده است و وارد گروه E_D می‌شود. از طرفی این مستعدین می‌توانند آلودگی را با نرخ ρ_H از گره‌های آلوده‌ای که جز دسته گره‌های شبکه‌ی اینترنت و مجاور با آنها هستند، دریافت کنند.

گره‌های آلوده‌ی E_D که آلودگی در آنها نهان است با نرخ δ_D علائم آلودگی در آنها ظاهر می‌شود و وارد گروه I_D می‌شوند.

گره‌های آلوده با نرخ γ_D تحت مکانیسم‌های امنیتی قرار گرفته و آلودگی آنها از بین می‌رود و وارد گروه R_D می‌شوند.

گره‌هایی که از آلودگی مصون شده‌اند مجدد امکان آلودگی توسط انواع دیگر بدافزار را دارند و با نرخ α_D وارد گروه S_D می‌شوند.

پارامترهای مدل و برخی جزئیات در جدول ۱ آورده شده است.



شکل ۳- مدل پیشنهادی HD-SEIRS

که $n_H + n_D = n$ و میانگین درجه دسته‌ی Λ_m که با $\langle k_i \rangle$ نشان داده می‌شود، برابر است با:

$$\langle k_i \rangle = \sum_{kj} p(j) \quad (3)$$

از طرفی $p(k) = k^{-\nu}$ برابر با احتمال اتصال نود شبکه به k نود دیگر، ν توان توزیع توان، m_i مینیمم درجه گروه Λ_m و γ_i ماکزیمم درجه‌ی گروه Λ_m است.

جدول ۱- نمادهای مدل

| نماد | توصیف نماد |
|-------------|--|
| Λ_i | نرخ اضافه شدن گره جدید به شبکه (گره‌ها در حالت مستعد قرار می‌گیرند). در دسته‌ی Λ_m که $0 \leq \Lambda_i \leq 1$ و $i = H, D$ |
| μ_i | نرخ خروج گره‌های دسته‌ی Λ_m از شبکه (نرخ مرگ و میر) که $0 \leq \mu_i \leq 1$ و $i = H, D$ |
| β_i | نرخ انتشار بدافزار در دسته‌ی Λ_m که $0 \leq \beta_i \leq 1$ و $i = H, D$ |
| δ_i | نرخ انتقال گروه گره‌های با آلودگی نهان به گروه گره‌های آلوده در دسته‌ی Λ_m که $0 \leq \delta_i \leq 1$ و $i = H, D$ |
| γ_i | نرخ انتقال گروه‌های با آلودگی به گروه بهبودیافته‌ها در دسته‌ی Λ_m که $0 \leq \gamma_i \leq 1$ و $i = H, D$ |
| α_i | نرخ انتقال از گروه بهبودیافته‌ها به گروه مستعدین در دسته‌ی Λ_m که $0 \leq \alpha_i \leq 1$ و $i = H, D$ |
| n_i | تعداد گره‌های دسته‌ی Λ_m و $i = H, D$ |

۳-۲- فرضیات مدل

در مدل‌سازی مدل پیشنهادی HD-SEIRS فرضیات زیر برای پیاده‌سازی در نظر گرفته شده است.

شبکه یک شبکه‌ی باراباسی آلبرت از نوع بی‌مقیاس و ناهمگن با $m=2$ است به‌طوری‌که $n = n_H + n_D = 1000$. از این ۱۰۰۰ گره در ابتدا ۱۰۰ گره به‌عنوان گره آلوده‌ی اولیه فرض شده‌اند و ۹۰۰ گره دیگر مستعد به آلودگی هستند. ۵۰ عدد از آلوده‌ها از نوع گره‌های شبکه اینترنت و ۵۰ آلوده‌ی دیگر مربوط به دستگاه‌های متصل به شبکه است. از طرفی

$$S_H^k(t) + E_H^k(t) + I_H^k(t) + R_H^k(t) = 1 \quad (4)$$

$$S_D^k(t) + E_D^k(t) + I_D^k(t) + R_D^k(t) = 1$$

نرخ تولد و نرخ مرگ و میر نیز با هم برابرند

$$\Lambda_H = \mu_H \cdot \Lambda_D = \mu_D$$

با توجه به جزئیات ذکر شده، معادلات شبکه به صورت زیر است:

$$\frac{dS_H^k(t)}{dt} = \Lambda_H - \beta_H S_H^k(t) \theta_H^k(t) - \mu_H S_H^k(t) + \alpha_H R_H^k(t) - \rho_D \theta_D^k(t) S_H^k(t) \quad (1)$$

$$\frac{dE_H^k(t)}{dt} = \beta_H \theta_H^k(t) S_H^k(t) - \mu_H E_H^k(t) - \delta_H E_H^k(t) + \rho_D \theta_D^k(t) S_H^k(t)$$

$$\frac{dI_H^k(t)}{dt} = \delta_H E_H^k(t) - \mu_H I_H^k(t) - \gamma_H I_H^k(t)$$

$$\frac{dR_H^k(t)}{dt} = \gamma_H I_H^k(t) - \mu_H R_H^k(t) - \alpha_H R_H^k(t)$$

$$\frac{dS_D^k(t)}{dt} = \Lambda_D - \beta_D \theta_D^k(t) S_D^k(t) - \mu_S S_D^k(t) + \alpha_D R_D^k(t) - \rho_H \theta_H^k(t) S_D^k(t)$$

$$\frac{dE_D^k(t)}{dt} = \beta_D \theta_D^k(t) S_D^k(t) - \mu_D E_D^k(t) - \delta_D E_D^k(t) + \rho_H \theta_H^k(t) S_D^k(t)$$

$$\frac{dI_D^k(t)}{dt} = \delta_D E_D^k(t) - \mu_D I_D^k(t) - \gamma_D I_D^k(t)$$

$$\frac{dR_D^k(t)}{dt} = \gamma_D I_D^k(t) - \mu_D R_D^k(t) - \alpha_D R_D^k(t)$$

در معادلات فوق $S_i^k(t)$, $E_i^k(t)$, $I_i^k(t)$, $R_i^k(t)$ که $i = H$ or D به ترتیب مستعدین، در معرض آلودگی، آلوده‌ها و بهبودیافته‌های با درجه k در گروه گره‌های شبکه اینترنت (H) یا دستگاه‌های متصل به شبکه (D) است. از طرفی $\theta_i^k(t)$ احتمال آلوده بودن گره همسایه با درجه k در خوشه Λ_m می‌باشد که می‌توان آن را به صورت معادله‌ی (۲) نوشت. بقیه‌ی پارامترهای مدل در جدول ۱ شرح داده شده‌اند.

$$\theta_i^k(t) = \frac{1}{\langle k_i \rangle} \sum_{k=m_i}^{y_i} k P(k) I_i^k(t) \quad (2)$$

تولید بعدی در شکل (۴) آورده شده است.

| الگوریتم به دست آوردن R_0 |
|--|
| ۱- پیدا کردن گروه‌های آلوده. |
| ۲- به دست آوردن ماتریس F با توجه به سرعت انتقال آلودگی در گروه‌های آلوده. |
| ۳- به دست آوردن ماتریس V با توجه به انتقال بین گروه‌های آلوده. |
| ۴- محاسبه ماتریس FV^{-1} . |
| ۵- محاسبه مقادیر ویژه ماتریس FV^{-1} و در نظر گرفتن بزرگترین مقدار ویژه به عنوان R_0 . |

شکل ۴- مراحل به دست آوردن نسبت بازتولید اولیه (R_0)

در مدل پیشنهادی گروه‌های آلوده، $E_H^k(t) \cdot I_H^k(t)$ ، $E_D^k(t) \cdot I_D^k(t)$ هستند که با توجه به این گروه‌ها ماتریس‌های F و V به شرح زیرند:

$$F = \begin{bmatrix} 0 & A_{H1} & 0 & -A_{H2} \\ 0 & 0 & 0 & 0 \\ 0 & -A_{D2} & 0 & A_{D1} \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (۸)$$

$$V = \begin{bmatrix} u_1 & 0 & 0 & 0 \\ -\delta_H & u_2 & 0 & 0 \\ 0 & 0 & u_3 & 0 \\ 0 & 0 & -\delta_D & u_4 \end{bmatrix} \quad (۹)$$

متغیرهای استفاده شده به همراه مقدار معادل آنها در جدول ۲ آورده شده‌اند.

ماتریس FV^{-1} با توجه به عبارات F و V به صورت زیر است:

$$G = FV^{-1} = \begin{bmatrix} \frac{\delta_H A_{H1}}{u_1 u_2} & \frac{A_{H1}}{u_2} & -\frac{\delta_D A_{H2}}{u_3 u_4} & -\frac{A_{H2}}{u_4} \\ 0 & 0 & 0 & 0 \\ -\frac{\delta_H A_{D2}}{u_1 u_2} & -\frac{A_{D2}}{u_2} & \frac{\delta_D A_{D1}}{u_3 u_4} & \frac{A_{D1}}{u_4} \\ 0 & 0 & 0 & 0 \end{bmatrix} \quad (۱۰)$$

مقادیر ویژه G عبارتند از:

$$\left\{ 0, \frac{(B_0 + \sqrt{(D_0 + D_1)})}{2u_1 u_2 u_3 u_4}, \frac{(B_0 - \sqrt{(D_0 + D_1)})}{2u_1 u_2 u_3 u_4} \right\}$$

۴- تحلیل مدل پیشنهادی

در این بخش به تحلیل پویایی مدل HD-SEIRS پرداخته می‌شود. نسبت بازتولید اولیه R_0 بیانگر میانگین تعداد آلودگی‌های ثانویه ناشی از آلودگی اولیه در طول زمان حیات آلودگی است. اگر R_0 کمتر از یک باشد انتشار بدافزار به شکل همه‌گیری نیست و همه‌گیری انتشار بدافزار در شبکه از بین رفته است ولی اگر بیشتر از یک باشد انتشار بدافزار در شبکه به صورت همه‌گیری خواهد بود [۱۶].

۴-۱- نقاط تعادل مدل پیشنهادی

در این بخش نقاط تعادل مدل پیشنهادی به دست آمده است. برای به دست آوردن نقاط تعادل مدل سمت راست معادلات (۱) را برابر صفر قرار می‌دهیم.

$$\frac{dS_H^k(t)}{dt} = 0, \quad \frac{dE_H^k(t)}{dt} = 0 \quad (۵)$$

$$\frac{dI_H^k(t)}{dt} = 0, \quad \frac{dR_H^k(t)}{dt} = 0$$

$$\frac{dS_D^k(t)}{dt} = 0, \quad \frac{dE_D^k(t)}{dt} = 0$$

$$\frac{dI_D^k(t)}{dt} = 0, \quad \frac{dR_D^k(t)}{dt} = 0$$

پس از حل معادلات (۵) و با توجه به اینکه در زمان قبل از همه‌گیری انتشار بدافزار تعداد گره‌های آلوده، در معرض آلودگی و بهبود یافته صفر است، نقطه‌ی تعادل ابتدایی^۸ به صورت زیر خواهد بود:

$$EQ_1 = \left(\frac{\Lambda_H}{\mu_H}, 0, 0, 0, \frac{\Lambda_D}{\mu_D}, 0, 0, 0 \right) \quad (۶)$$

و نقطه تعادل دیگر نیز به صورت زیر فرض می‌شود.

$$EQ_2 = (S_H^{k*}(t), E_H^{k*}(t), I_H^{k*}(t), \quad (۷)$$

$$R_H^{k*}(t), S_D^{k*}(t), E_D^{k*}(t), I_D^{k*}(t), R_D^{k*}(t))$$

۴-۲- نسبت بازتولید اولیه

در این بخش مقدار R_0 از روش تولید بعدی به دست آمده است [۱۷].
مراحل به دست آوردن نسبت باز تولید اولیه بر اساس روش

^۸ Malware Free Equilibrium

^۷ Basic Reproductive Ratio

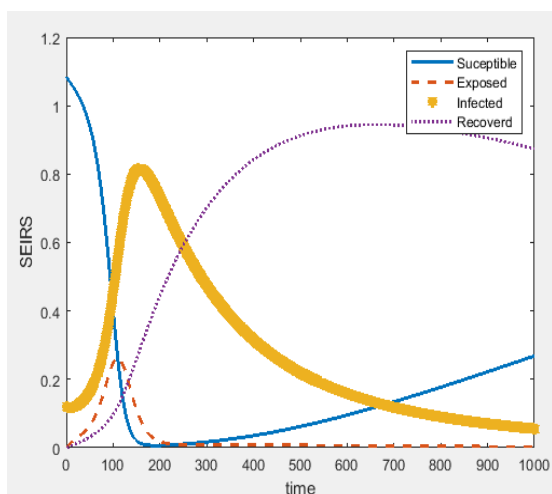
$$R_0 = \frac{B_0}{2u_1u_2u_3u_4} \quad (11)$$

اگر $R_0 < 1$ آلودگی هر گره از میزان آلودگی اولیه کمتر است در نتیجه مدل پیشنهادی به نقطه ای تعادل بدون آلودگی می رسد و اگر $R_0 > 1$ آلودگی در شبکه پخش می شود و انتشار بدافزار به صورت همه گیری خواهد بود.

۵- ارزیابی مدل پیشنهادی

در این بخش به ارزیابی مدل پیشنهادی HD-SEIRS پرداخته می شود. مدل پیشنهادی روی یک شبکه ی باراباسی آلبرت با ۱۰۰۰ گره که ۱۰۰ گره از این تعداد در ابتدای زمان شبیه سازی آلوده و ۹۰۰ گره دیگر مستعد آلودگی هستند، آزمایش شده است. پس از انجام آزمایشات روی مدل پیشنهادی در محیط متلب و نرم افزار Gephi، نتایج این بخش حاصل شده است.

شکل (۵) تغییرات مربوط به گروه های مستعد، در معرض آلودگی، آلوده و بهبود یافته را در مدل SEIRS در مدت زمان شبیه سازی نشان می دهد. شکل های (۶) و (۷) به ترتیب تغییرات مربوط به چهار گروه S، E، I و R را در مدل توسعه یافته HD-SEIRS نشان می دهد. هر یک از نمودارهای موجود در این شکل نشان دهنده ی تغییرات یکی از حالات گروه های مربوطه نسبت به زمان است. در ابتدا اکثریت گره ها در حالت مستعد قرار دارند و با گذشت زمان از چگالی گره های مستعد کم شده و به چگالی گره های آلوده اضافه می شود. بالاترین نقطه منحنی مربوط به گروه I بیشترین مقدار گره های آلوده را نشان می دهد.



شکل ۵- نمودار مدل SEIRS روی شبکه باراباسی آلبرت با ۱۰۰۰ گره

جدول ۲- مقادیر معادل برای متغیرهای استفاده شده

| نام متغیر | مقدار معادل برای متغیر |
|-----------|---|
| A_{H1} | $\frac{\beta_H}{\langle k_H \rangle} S_H^k(0)$ $\begin{bmatrix} 1 \\ 2 \\ \vdots \\ \gamma_H \end{bmatrix} [p(1). 2p(2). \dots \gamma_H p(\gamma_H)]$ $= \frac{\beta_H \langle K_H^2 \rangle \Lambda_H}{\langle k_H \rangle \mu_H}$ |
| A_{H2} | $\frac{\rho_D}{\langle k_D \rangle} S_H^k(0)$ $\begin{bmatrix} 1 \\ 2 \\ \vdots \\ \gamma_D \end{bmatrix} [p(1). 2p(2). \dots \gamma_D p(\gamma_D)]$ $= \frac{\rho_D \langle K_D^2 \rangle \Lambda_H}{\langle k_D \rangle \mu_H}$ |
| A_{D1} | $\frac{\beta_D}{\langle k_D \rangle} S_D^k(0)$ $\begin{bmatrix} 1 \\ 2 \\ \vdots \\ \gamma_D \end{bmatrix} [p(1). 2p(2). \dots n_2 p(\gamma_D)]$ $= \frac{\beta_D \langle K_D^2 \rangle \Lambda_D}{\langle k_D \rangle \mu_D}$ |
| A_{D2} | $\frac{\rho_H}{\langle k_H \rangle} S_D^k(0)$ $\begin{bmatrix} 1 \\ 2 \\ \vdots \\ \gamma_H \end{bmatrix} [p(1). 2p(2). \dots n_2 p(\gamma_H)]$ $= \frac{\rho_H \langle K_H^2 \rangle \Lambda_D}{\langle k_H \rangle \mu_D}$ |
| u_1 | $\mu_H + \delta_H$ |
| u_2 | $\mu_H + \gamma_H$ |
| u_3 | $\mu_D + \delta_D$ |
| u_4 | $\mu_D + \gamma_D$ |
| D_0 | $A_{D1}^2 \delta_D^2 u_1^2 u_2^2$ $- 2A_{D1} A_{H1} \delta_D \delta_H u_1 u_2 u_3 u_4$ $+ A_{H1}^2 \delta_H^2 u_3^2 u_4^2$ |
| D_1 | $4A_{D2} A_{H2} \delta_D \delta_H u_1 u_2 u_3 u_4$ |
| B_0 | $A_{D1} \delta_D u_1 u_2 + A_{H1} \delta_H u_3 u_4$ |

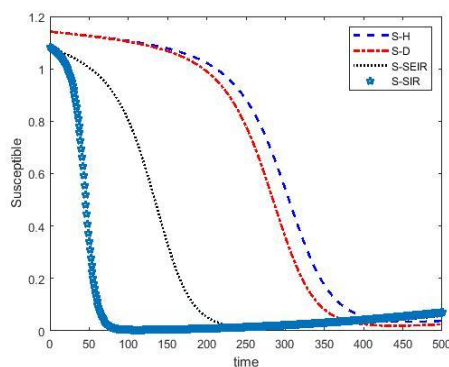
در نتیجه با توجه به متغیرهای معادل در جدول ۲ مقدار $R_0 = \rho(G)$ به صورت زیر خواهد بود:

0/05 مقایسه می‌کند. در شکل (۸-ب) گروه آلوده‌ها مقایسه‌ی بین مدل پیشنهادی و دو مدل SIRS و SEIRS انجام شده است. همان‌طور که در نمودارهای این دو قسمت مشخص است، با گذشت زمان از جمعیت مستعدین کم شده و به آلوده‌ها اضافه می‌شود. براساس تایید به دست آمده در نمودارهای ذکر شده روند کاهش مستعدین در مدل‌های SIRS و SEIRS سریع‌تر از مدل پیشنهادی است و همچنین روند انتشار بدافزار در مدل پیشنهادی کندتر از مدل SEIRS است. بنابراین مدل پیشنهادی با دو در دسته گرفتن گره‌های شبکه توانسته است روند انتشار بدافزار را کندتر کند.

در شکل (۸-ب) گروه در معرض آلودگی در مدل پیشنهادی با مدل SEIRS مقایسه شده است. از آنجایی که روند انتشار بدافزار در مدل پیشنهادی نسبت به مدل SEIRS کاهش دارد، در نمودار نیز به وضوح این کاهش در گروه گره‌های در معرض آلودگی دیده می‌شود.

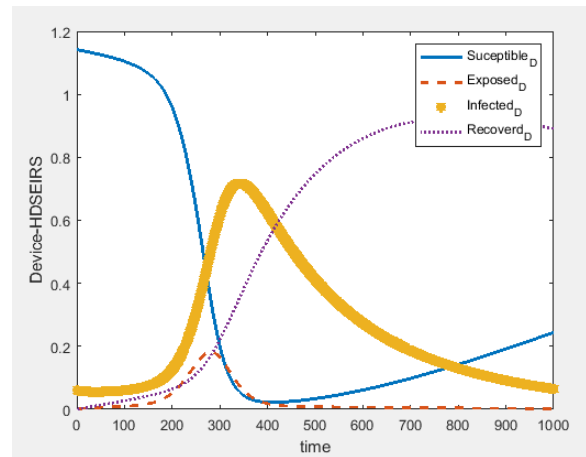
شکل (۸-ت) نیز گروه‌های بهبودیافته را در مدل پیشنهادی و مدل‌های SIRS و SEIRS بررسی می‌کند. از آنجایی که روند انتشار بدافزار در مدل پیشنهادی نسبت به دو مدل دیگر کاهش داشته است، بهبود گره‌ها نیز در این مدل نسبت به دو مدل ذکر شده از نظر زمانی همراه با تاخیر بوده است.

با توجه به موارد ذکر شده مدل پیشنهادی نسبت به مدل SEIRS و SIRS توانسته است روند انتشار بدافزار را کاهش دهد و با تاخیر مواجه سازد.



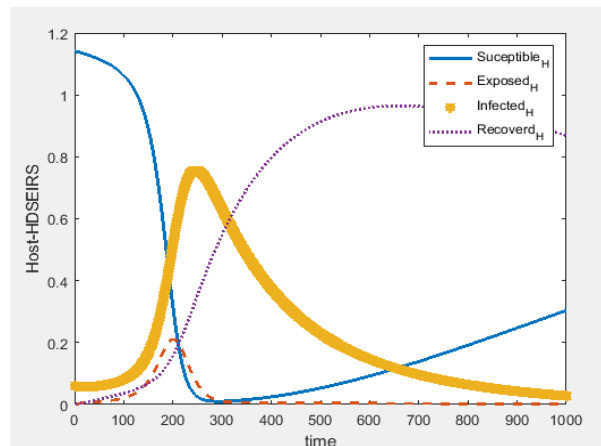
شکل (۸-الف) - مقایسه گروه مستعدین (S) مدل پیشنهادی با

مدل‌های SEIR و SIR. پارامترهای $\alpha_1 = 0$
 $0006 \cdot \alpha_2 = 0 \cdot 0005 \cdot \beta_1 = 0 \cdot 2 \cdot \beta_2 = 0 \cdot$
 $2 \cdot \gamma_1 = 0 \cdot 0006 \cdot \gamma_2 = 0 \cdot 005 \cdot \rho_1 = 0 \cdot$
 $006 \cdot \rho_2 = 0 \cdot 005 \cdot \mu_1 = 0 \cdot 0001 \cdot \mu_2 = 0 \cdot$
 $0002 \cdot \Lambda_1 = 0 \cdot 0001 \cdot \Lambda_2 = 0 \cdot 0002 \cdot \delta_1 =$
 $0 \cdot 06 \cdot \delta_2 = 0 \cdot 05$



شکل ۶- نمودار مدل HD-SEIRS توسعه یافته روی

دسته‌ی مربوط به دستگاه‌های متصل به شبکه $\alpha_D =$
 $0/0005 \cdot \beta_D = 0/2 \cdot \gamma_D = 0/005 \cdot \rho_D =$
 $0/005 \cdot \mu_D = 0/0002 \cdot \Lambda_D = 0/0002 \cdot \delta_D =$
 $0/05$



شکل ۷- نمودار مدل SEIR توسعه یافته روی دسته‌ی

مربوط به گره‌های شبکه‌ی اینترنت با پارامترهای $\alpha_H =$
 $0/0006 \cdot \beta_H = 0/2 \cdot \gamma_H = 0/006 \cdot \rho_H =$
 $0/006 \cdot \mu_H = 0/0001 \cdot \Lambda_H = 0/0001 \cdot \delta_H =$
 $0/06$

۵-۱- مقایسه مدل پیشنهادی HD-SEIRS با مدل‌های SEIRS و SIRS

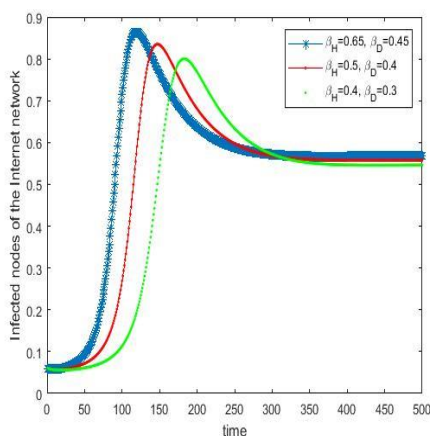
در این بخش گروه‌های S، E، I، R در مدل پیشنهادی HD-SEIRS با گروه‌های معادل در مدل‌های SEIRS و SIRS مقایسه شده‌اند.

شکل (۸) در بخش الف گروه مستعدین را در مدل پیشنهادی، مدل‌های SEIRS و SIRS به ازای مقادیر $\alpha_H = 0/0006 \cdot \alpha_D = 0/0005 \cdot \beta_H = 0/$
 $2 \cdot \beta_D = 0/2 \cdot \gamma_H = 0/006 \cdot \gamma_D = 0/$
 $005 \cdot \rho_H = 0/006 \cdot \rho_D = 0/005 \cdot \mu_H = 0/$
 $0001 \cdot \mu_D = 0/0002 \cdot \Lambda_H = 0/$
 $0001 \cdot \Lambda_D = 0/0002 \cdot \delta_H = 0/06 \cdot \delta_D =$

۵-۲- روند تغییرات R_0 و انتشار آلودگی با تغییر

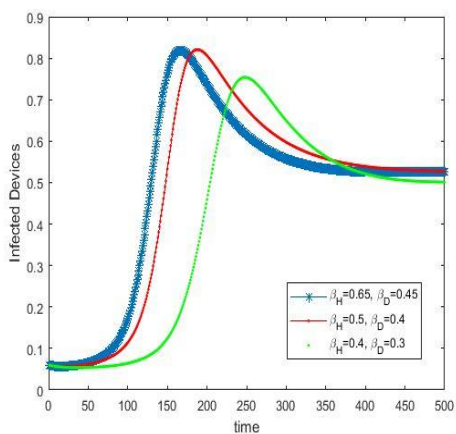
پارامترها در مدل HD-SEIRS

در این بخش انتشار بدافزار با تغییر پارامترهای مدل HD-SEIRS مورد بررسی قرار گرفته است. همان طور که در شکل (۹) دیده می شود با افزایش نرخ انتشار بدافزار $\beta_H \cdot \beta_D$ در هر دو بخش شبکه اینترنت و دستگاه های متصل به شبکه آلودگی افزایش یافته است و مقدار R_0 نیز افزایش پیدا کرده است.



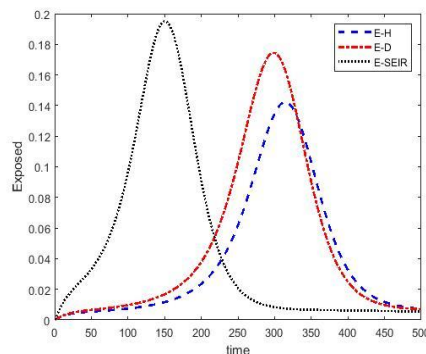
شکل (۹-الف) - مقایسه ی انتشار آلودگی در شبکه ی اینترنت در مدل HD-SEIRS با تغییر پارامترهای

$\beta_H \cdot \beta_D$ و پارامترهای ثابت $\alpha_D = 0/009$. $\alpha_H = 0/007$. $\gamma_H = 0/009$. $\gamma_D = 0/008$. $\rho_H = 0/005$. $\rho_D = 0/004$. $\mu_H = 0/001$. $\mu_D = 0/001$. $\Lambda_H = 0/001$. $\Lambda_D = 0/001$. $\delta_H = 0/1$. $\delta_D = 0/08$



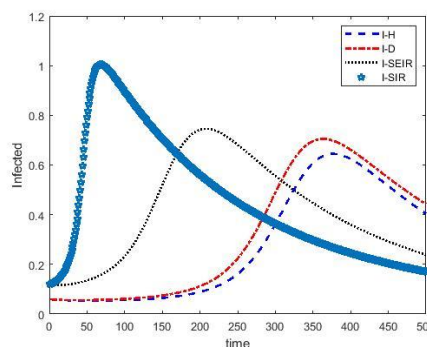
شکل (۹-ب) - مقایسه ی انتشار آلودگی در دستگاه های متصل به شبکه در مدل HD-SEIRS با تغییر

پارامترهای $\beta_H \cdot \beta_D$ و پارامترهای ثابت $\alpha_H = 0/009$. $\alpha_D = 0/007$. $\gamma_H = 0/009$. $\gamma_D = 0/008$. $\rho_H = 0/005$. $\rho_D = 0/004$. $\mu_H = 0/001$. $\mu_D = 0/001$. $\Lambda_H = 0/001$. $\Lambda_D = 0/001$. $\delta_H = 0/1$. $\delta_D = 0/08$



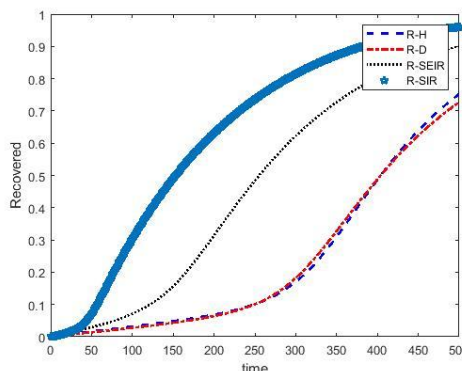
شکل (۸-ب) - مقایسه گروه گره های در معرض آلودگی (E)

مدل پیشنهادی با مدل SEIR . پارامترهای $\alpha_1 = 0$. $\alpha_2 = 0 \cdot 0005$. $\beta_1 = 0 \cdot 2$. $\beta_2 = 0 \cdot 0006$. $\gamma_1 = 0 \cdot 0006$. $\gamma_2 = 0 \cdot 0005$. $\rho_1 = 0 \cdot 0006$. $\rho_2 = 0 \cdot 0005$. $\mu_1 = 0 \cdot 00001$. $\mu_2 = 0 \cdot 0002$. $\Lambda_1 = 0 \cdot 00001$. $\Lambda_2 = 0 \cdot 00002$. $\delta_1 = 0 \cdot 06$. $\delta_2 = 0 \cdot 05$



شکل (۸-پ) - مقایسه گروه آلوده ها (I) مدل پیشنهادی با

مدل های SEIR و SIR . پارامترهای $\alpha_1 = 0$. $\alpha_2 = 0 \cdot 0005$. $\beta_1 = 0 \cdot 2$. $\beta_2 = 0 \cdot 0006$. $\gamma_1 = 0 \cdot 0006$. $\gamma_2 = 0 \cdot 0005$. $\rho_1 = 0 \cdot 0006$. $\rho_2 = 0 \cdot 0005$. $\mu_1 = 0 \cdot 00001$. $\mu_2 = 0 \cdot 0002$. $\Lambda_1 = 0 \cdot 00001$. $\Lambda_2 = 0 \cdot 00002$. $\delta_1 = 0 \cdot 06$. $\delta_2 = 0 \cdot 05$



شکل (۸-ت) - مقایسه گروه بهبودیافته ها (R) مدل پیشنهادی

با مدل های SEIR و SIR . پارامترهای $\alpha_1 = 0$. $\alpha_2 = 0 \cdot 0005$. $\beta_1 = 0 \cdot 2$. $\beta_2 = 0 \cdot 0006$. $\gamma_1 = 0 \cdot 0006$. $\gamma_2 = 0 \cdot 0005$. $\rho_1 = 0 \cdot 0006$. $\rho_2 = 0 \cdot 0005$. $\mu_1 = 0 \cdot 00001$. $\mu_2 = 0 \cdot 0002$. $\Lambda_1 = 0 \cdot 00001$. $\Lambda_2 = 0 \cdot 00002$. $\delta_1 = 0 \cdot 06$. $\delta_2 = 0 \cdot 05$

افزایش نرخ انتشار بدافزار مقدار R_0 افزایش پیدا کرده است. زمانی که $\beta_H = \beta_D = 0/012$ است $R_0 < 1$ و پایان همه‌گیری در شبکه را خواهیم داشت و برای مقدار $\beta_H = \beta_D \geq 0/02$ ، $R_0 > 1$ و همه‌گیری را در شبکه داریم.

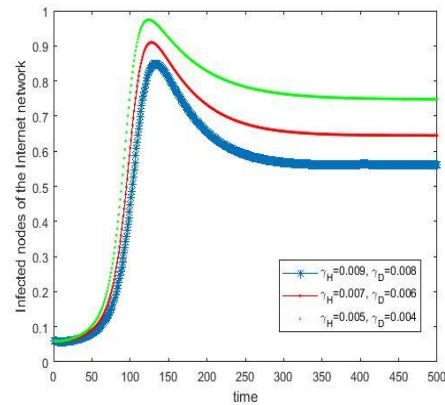
جدول ۳- مقادیر عددی R_0 به ازای نرخ‌های انتشار متفاوت و ثابت گرفتن بقیه‌ی پارامترها

| نرخ انتشار بدافزار ($\beta_1 \cdot \beta_2$) | نسبت بازتولید اولیه (R_0) |
|--|-------------------------------|
| $\beta_H = \beta_D = 0/008$ | 0/442932772204613 |
| $\beta_H = \beta_D = 0/01$ | 0/553665965255766 |
| $\beta_H = \beta_D = 0/012$ | 0/664399158306919 |
| $\beta_H = \beta_D = 0/02$ | 1/10733193051153 |
| $\beta_H = \beta_D = 0/022$ | 1/21806512356269 |

۶- نتیجه گیری

در این مقاله مدل HD-SEIRS برای شبکه‌ی بی‌مقیاس متشکل از دستگاه‌های متصل به شبکه و شبکه اینترنت ارائه شده است. در مدل پیشنهادی دستگاه‌های متصل به شبکه و گره‌های شبکه به صورت مجزا فرض شده‌اند به طوریکه هر گره شبکه یا دستگاهی متصل به اینترنت یا یک گره از شبکه‌ی اینترنت است. انتشار آلودگی در هر کدام از دسته‌ها بر اساس بیماری‌های همه‌گیری مستعد- در معرض آلودگی - آلوده - بهبودیافته مدل می‌شود. بر اساس نتایج به‌دست آمده انتشار آلودگی در مدل HD-SEIRS نسبت به مدل SEIRS کاهش پیدا کرده است. مقدار نسبت بازتولید اولیه در مدل پیشنهادی محاسبه شده و اثر تغییر پارامترهای نرخ انتشار بدافزار و نرخ بهبود در مدل پیشنهادی بررسی شده است. با توجه به آزمایشات انجام شده به این نتیجه رسیدیم که با افزایش مقدار نرخ انتشار بدافزار آلودگی در شبکه در هر دو دسته گره‌های شبکه اینترنت و دستگاه‌های متصل به شبکه افزایش می‌یابد ولی نسبت به مدل SEIRS آلودگی کمتر است. نسبت بازتولید اولیه در هر حالت به‌دست آمده است. از طرفی افزایش نرخ بهبود نیز کاهش آلودگی را در بر دارد در نتیجه تقسیم گره‌ها به دو دسته اثر مطلوبی روی کاهش میزان آلودگی و R_0 داشته است. طبق آزمایشات به‌عمل آمده با افزایش نرخ انتشار بدافزار آلودگی در شبکه افزایش می‌یابد و زمانی که $R_0 > 1$ همه‌گیری خواهیم داشت و با کاهش

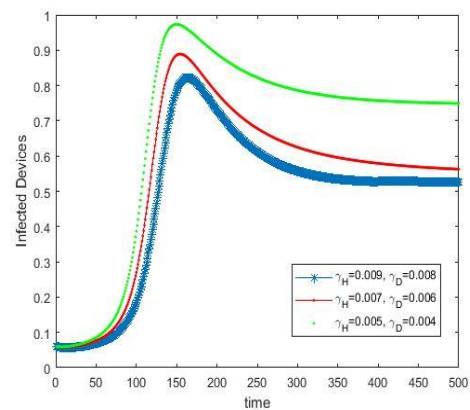
در شکل (۱۰) با تغییر پارامتر نرخ بهبود $\gamma_H \cdot \gamma_D$ انتشار بدافزار بررسی شده است. با کاهش نرخ بهبود، آلودگی در شبکه اینترنت و دستگاه‌های متصل به شبکه زیاد شده است و مقدار R_0 افزایش پیدا کرده است.



شکل (۱۰-الف)- مقایسه‌ی انتشار آلودگی در شبکه اینترنت

در مدل HD-SEIRS با تغییر پارامترهای $\gamma_H \cdot \gamma_D$ و

$$\alpha_H = 0/009 \quad \alpha_D = 0/007 \quad \beta_H = 0/6 \quad \beta_D = 0/5 \quad \rho_H = 0/005 \quad \rho_2 = 0/004 \quad \mu_H = 0/001 \quad \mu_D = 0/001 \quad \Lambda_H = 0/001 \quad \Lambda_D = 0/001 \quad \delta_H = 0/1 \quad \delta_D = 0/08$$



شکل (۱۰-ب)- مقایسه‌ی انتشار آلودگی در دستگاه‌های

متصل به شبکه در مدل HD-SEIRS با تغییر پارامترهای

$\gamma_H \cdot \gamma_D$ و پارامترهای ثابت

$$\alpha_H = 0/009 \quad \alpha_D = 0/007 \quad \beta_H = 0/6 \quad \beta_D = 0/5 \quad \rho_H = 0/005 \quad \rho_D = 0/004 \quad \mu_H = 0/001 \quad \mu_D = 0/001 \quad \Lambda_H = 0/001 \quad \Lambda_D = 0/001 \quad \delta_H = 0/1 \quad \delta_D = 0/08$$

جدول ۳ روند تغییر R_0 را با تغییر پارامترهای $\beta_1 \cdot \beta_2$ و

$$\alpha_H = 0/0005 \quad \alpha_D = 0/005 \quad \gamma_H = 0/05 \quad \gamma_D = 0/05 \quad \rho_H = 0/006 \quad \rho_D = 0/006 \quad \mu_H = 0/006 \quad \mu_D = 0/001 \quad \Lambda_H = 0/001 \quad \Lambda_D = 0/001 \quad \delta_H = 0/005 \quad \delta_D = 0/005$$

برای طبقه بندی گره ها در بخش شبیه سازی استفاده شده است. بهبود الگوریتم دسته بندی به کاهش زمان تمام شده شبیه سازی منجر می شود. در کارهای آینده کاهش زمان دسته بندی مورد مطالعه قرار خواهد گرفت.

نرخ انتشار بدافزار R_0 کاهش می یابد و زمانی که $R_0 < 1$ به پایان همه گیری در شبکه می رسیم. از معایب مدل پیشنهادی می توان به پیچیدگی زمانی الگوریتم دسته بندی گره ها اشاره کرد که در اینجا از الگوریتم دسته بندی طیفی

مراجع

- [1] Y. Ye, T. Li, D. Adjeroh, and S.S. Iyengar. "A survey on malware detection using data mining techniques." *ACM Computing Surveys (CSUR)* 50, no. 3 (2017): 1-40.
- [2] S. Boccaletti, V. Latora, Y. Moreno, M. Chavez, and D.U. Hwang. "Complex networks: Structure and dynamics." *Physics Reports* 424, no. 4-5 (2006): 175-308.
- [3] A. M. del Rey. "Mathematical modeling of the propagation of malware: a review." *Security and Communication Networks* 8, no. 15 (2015): 2561-2579.
- [4] L. Zhao, Q. Wang, J. Cheng, Y. Chen, J. Wang, and W. Huang. "Rumor spreading model with consideration of forgetting mechanism: A case of online blogging LiveJournal." *Physica A: Statistical Mechanics and its Applications* 390, no. 13 (2011): 2619-2625.
- [5] K. Sznajd-Weron, and J. Sznajd. "Opinion evolution in closed community." *International Journal of Modern Physics C* 11, no. 06 (2000): 1157-1165.
- [6] J. Yang, C. Yao, W. Ma, and G. Chen. "A study of the spreading scheme for viral marketing based on a complex network model." *Physica A: Statistical Mechanics and its Applications* 389, no. 4 (2010): 859-870.
- [7] M.T. Signes-Pont, A. Cortés-Castillo, H. Mora-Mora, and J. Szymanski. "Modelling the malware propagation in mobile computer devices." *Computers & Security* 79 (2018): 80-93.
- [8] W.O. Kermack, and A.G. McKendrick. "A contribution to the mathematical theory of epidemics." *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character* 115, no. 772 (1927): 700-721.
- [9] E. Kuhl, and E. Kuhl. "The classical SIR model." *Computational Epidemiology: Data-Driven Modeling of COVID-19* (2021): 41-59.
- [10] R. Almeida. "Analysis of a fractional SEIR model with treatment." *Applied Mathematics Letters*, 84 (2018): 56-62.
- [11] S. Hosseini. "Defense against malware propagation in complex heterogeneous networks." *Cluster Computing*, 24 (2021): 1199-1215.
- [12] J.R.C. Piqueira, M.A. Cabrera, and C.M. Batistela. "Malware propagation in clustered computer networks." *Physica A: Statistical Mechanics and its Applications*, 573 (2021): 125958.
- [13] B.K. Mishra, A.K. Keshri, D.K. Mallick, and B.K. Mishra. "Mathematical model on distributed denial of service attack through Internet of things in a network." *Nonlinear Engineering* 8, no. 1 (2019): 486-495.
- [14] X. Zhu, and J. Huang. "Malware propagation model for cluster-based wireless sensor networks using epidemiological theory." *PeerJ Computer Science* 7 (2021): 728-738.
- [15] C. Nwokoye, and I.I. Umeh. "The SEIQR-V model: On a more accurate analytical characterization of malicious threat defense." *Int. J. Inf. Technol. Comput. Sci* 9, no. 12 (2017): 28-37.
- [16] P. Van den Driessche. "Reproduction numbers of infectious disease models." *Infectious Disease Modelling* 2, no. 3 (2017): 288-303.
- [17] J.A. Wattis. "An introduction to mathematical models of coagulation-fragmentation processes: a discrete deterministic mean-field approach." *Physica D: Nonlinear Phenomena* 222, no. 1-2 (2006): 1-20.