مجله محاسبات نرم، جلد 14، شماره 2 (پاییز و زمستان 1404)، صفحه 86_95
https://doi.org/10.22052/scj.2025.255570.1279

مجله محاسبات نرم
SOFT COMPUTING JOURNAL
تارنمای مجله: scj.kashanu.ac.ir

دانشگاه کاشان
University of Kashan

مدل‌سازی انتشار بدافزار VEIRV-A در شبکه‌های اینترنت اشیا✧

سوده حسینی[1*]، دانشیار، الهام اسدی[2]، استادیار

[1] گروه علوم کامپیوتر، دانشکده ریاضی و علوم کامپیوتر، دانشگاه شهید باهنر، کرمان، ایران.

[2] گروه کامپیوتر، واحد شهربابک، دانشگاه آزاد اسلامی، شهربابک، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت 14 آبان ماه 1403
پذیرش 25 دی ماه 1403

کلمات کلیدی:
مدل‌سازی انتشار بدافزار
مدل‌سازی بیماری‌های همه‌گیری
عدد بازتولید اولیه
حد آستانه همه‌گیری
اینترنت اشیا

چکیده

با تکامل شبکه بی‌سیم نسل پنجم، اینترنت اشیا (IOT) نیز تحول شگفتی در زندگی بشر ایجاد کرده است. از اینرو مطالعه دقیق‌تر فناوری اینترنت اشیا و حوزه‌های مختلف آن از جمله امنیت این حوزه ضروری خواهد بود. در زمینه امنیت شبکه‌های اینترنت اشیا، یکی از مواردی که مطرح شده انتشار بدافزار است. در این مقاله به مدل‌سازی انتشار بدافزار در شبکه‌های اینترنت اشیا با مدل بیماری‌های همه‌گیری آسیب‌پذیر – در معرض آلودگی - آلوده - بهبودیافته - پادزهر پرداخته‌ایم.اثر اعمال پادزهر روی گره‌های بهبودیافته و آسیب‌پذیر، در انتشار بدافزار شبکه‌های اینترنت اشیا مورد بررسی قرار گرفته است. ما بر اساس درجه گره میزان با اهمیت بودن گره را در شبکه تعیین کرده‌ایم و بر اساس این نرخ، گره‌های آسیب‌پذیر در شبکه ایمن شده‌اند. ایمن‌سازی گره‌های آسیب‌پذیر بر مبنای درجه منجر به کاهش انتشار بدافزار در شبکه شده است. حد آستانه اپیدمی انتشار بدفزار (R_0) در مدل پیشنهادی محاسبه شده است. مقایسه مدل با دو مدل SIRS و SEIRS نشان داد مدل پیشنهادی نسبت به دو مدل دیگر عملکرد بهتری داشته است.

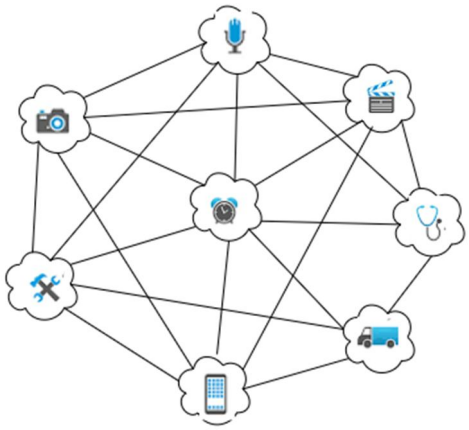
1. مقدمه

اینترنت اشیا (IOT) شبکه‌ای از اشیا فیزیکی است که از طریق اینترنت به یکدیگر مرتبط شده‌اند. این شبکه طیف وسیعی از سخت‌افزار و نرم‌افزار فناورانه از جمله حسگرها، محرک‌ها، دستگاه‌های پوشیدنی، فناوری اطلاعات و ارتباطات (ICT)، رایانش ابری و غیره را پوشش می‌دهد [1]. به عبارتی دیگر، اینترنت اشیا یک فناوری است که اشیا ممکن را به هم متصل می‌کند، به طوری که اشیا شروع به برقراری ارتباط بین خود می‌کنند تا خدمات بهتری را برای کاربران به شکل غیر قابل تصوری ارائه دهند و زندگی آنها را آسان‌تر کنند. اشیا هوشمند می‌توانند مجموعه‌ای از حسگرها، محرک‌ها، تلفن‌های هوشمند و غیره باشند [2]. اینترنت اشیا شهری امروزی سیستم‌های نرم‌افزار فشرده و مبتنی بر داده‌ها در مقیاس بزرگ هستند که هزاران دستگاه هوشمند متصل به هم و دارای هوش محدود را شامل می‌شوند [3]. شکل (1) نمایی از اشیا را در یک شبکه اینترنت اشیا نشان می‌دهد. این شبکه‌ها در حال حاضر در زمینه‌های مختلفی مانند پزشکی [1]، [4]، بانکداری [5]، حمل و نقل [6]، کشاورزی [7] و مانند آن استفاده می‌شوند. باز بودن، پویایی و

✧ نوع مقاله: پژوهشی
* نویسنده مسئول
پست(های) الکترونیک: so_hosseini@uk.ac.ir (حسینی)
asadi.cs@iau.ac.ir (اسدی)

نحوه ارجاع به مقاله: سوده حسینی، الهام اسدی، «مدل‌سازی انتشار بدافزار VEIRV-A در شبکه‌های اینترنت اشیا»، مجله محاسبات نرم، جلد 14، شماره 2، ص 86_95، پاییز و زمستان 1404.

ناهمگونی شبکه اینترنت اشیا، کاربران را در یک محیط بسیار ناامن قرار می‌دهد [3]. هنگام ساخت یک دستگاه اینترنت اشیا، سازندگان اغلب تاکید زیادی بر هزینه، اندازه و قابلیت استفاده دارند، در حالی که جنبه‌های امنیتی و پزشکی قانونی به طور معمول نادیده گرفته می‌شوند [8]. بنابراین اشیا ممکن است آسیب‌پذیری‌های زیادی داشته باشند و این دستگاه‌های آسیب‌پذیر قربانیان مناسبی برای ورود بدافزار یا نرم‌افزار مخرب به شبکه هستند. بدافزارها با نفوذ در شبکه و اختلال در سیستم‌ها سالیانه خسارات زیادی وارد می‌کنند. در سال‌های اخیر، مسائل امنیتی اینترنت اشیا توجه گسترده‌ای را در محافل دانشگاهی و محافل صنعتی به خود جلب کرده است [3]. حوزه دانشگاهی بر امنیت اینترنت اشیا از دیدگاه‌های زیر تمرکز دارد: فناوری تشخیص، تشخیص بدافزار بر اساس نظریه بازی، تجزیه و تحلیل و مدل‌سازی. دو دیدگاه اول، شناسایی بدافزار است. سومین دیدگاه پویایی انتشار بدافزار را شبیه‌سازی می‌کند و تاثیر عوامل مختلف بر انتشار را تجزیه و تحلیل می‌کند [9].



شکل (1): نمایی از شبکه اینترنت اشیا

تجزیه و تحلیل حالت انتشار ویروس و گسترش ویژگی‌ها از منظر پیشگیری برای کاهش خطرات و آسیب‌ها، یکی از روش‌های مبارزه با بدافزارها و جلوگیری از انتشار آنها است. با مدل‌سازی انتشار بدافزار در شبکه و پیش‌بینی‌های لازم در راستای کاهش انتشار بدافزار می‌توان شبکه را در برابر خطرات بدافزار مصون‌سازی نمود. مدل‌سازی انتشار بدافزار به روش‌های مختلفی انجام می‌شود. یکی از روش‌های آن مدل‌سازی انتشار بر اساس بیماری‌های همه‌گیری است. این روش مدل‌سازی با توجه به شباهت بین ویروس‌ها و بدافزارها انجام می‌شود. در زمینه انتشار ویروس‌های بیولوژیک، به مدل‌سازی انتشار ویروس با روش بیماری‌های همه‌گیری تحقیقاتی صورت گرفته است [10]، [11]. مدل‌های زیادی در مدل‌سازی انتشار بیماری‌های همه‌گیری جمعیت به گروه‌های متفاوتی تقسیم می‌شود که در مدل پایه آن کرمک مکندریک جمعیت را به سه گروه مستعدین (Susceptible)، آلوده‌ها (Infected) و بهبود یافته‌ها (Recovered) تقسیم و انتشار را در بین این سه گروه مدل کرد [12]. مدل او به مدل SIR شهرت یافت و به عنوان مدل پایه مورد استفاده قرار گرفت. از آنجایی که دستگاه‌های اینترنت اشیا آسیب‌پذیری‌های بیشتری نسبت به بقیه گره‌های شبکه‌ها دارند، بیشتر مستعد انتشار بدافزار هستند. در این مقاله با در نظر گرفتن پنج گروه آسیب‌پذیرها (Vulnerable)، در معرض آلودگی (Exposed)، آلوده‌ها (Infected)، بهبودیافته‌ها (Recovered) و پادزهر (Antidotal)، مدل VEIRV-A بر روی شبکه‌های اینترنت اشیا ارائه شده است. در مدل ارائه شده گره‌های آسیب‌پذیر بر اساس درجه‌شان میزان بااهمیت بودن آنها تعیین و بر اساس نرخ اهمیت واکسینه شده‌اند. با توجه به صرفه‌جویی در زمان و هزینه اعمال پادزهر روی تمام گره‌های شبکه، ما این نرخ را به عنوان نرخ واکسیناسیون در نظر گرفته‌ایم. از طرفی در مدل ارائه شده طی دو مرحله پادزهر روی گره‌ها اعمال شده است. مرحله اول با توجه به درجه گره، گره‌های آسیب‌پذیر واکسینه شده‌اند و در مرحله دوم گره‌هایی که در مرحله اول پادزهر روی آنها اعمال نشده است و آلوده شده‌اند، پس از بهبود شانس ورود به مرحله اعمال پادزهر را پیدا کرده‌اند. بنابراین انتشار آلودگی در شبکه کاهش بیشتری داشته است. در زمینه تحلیل دینامیک شبکه حد آستانه همه‌گیری مدل ارائه شده به دست آمده است.

بخش‌بندی ادامه مقاله به این صورت است که در بخش دوم کارهای انجام شده در زمینه انتشار بدافزار در شبکه‌های اینترنت اشیا آمده است. در بخش سوم مدل پیشنهادی و دینامیک مدل را آورده‌ایم. در بخش چهارم تجزیه و تحلیل مدل ارائه شده در

بخش آخر نیز نتیجه‌گیری مدل آمده است.

2. کارهای مرتبط

با توجه به پیشرفت تکنولوژی و استفاده از اشیا در راستای ساده‌سازی زندگی انسانی، همواره امنیت و جلوگیری از کاهش انتشار بدافزار در شبکه‌های IOT مورد توجه بسیاری از محققین بوده و هست.

ژو و همکاران [13]، در مقاله خود مدل SLRP را مبتنی بر بیماری‌های همه‌گیری برای دستگاه‌های اینترنت اشیا ناهمگن ارائه دادند به طوری که در مدل آنها نرخ بازیابی و نرخ آلودگی مجزایی برای هر دستگاه در نظر گرفته شده است. آنها یک استراتژی دفاعی بهینه با نرخ بازیابی پویا طراحی کردند که به طور جامع هزینه و میزان آلودگی کلی دستگاه را در نظر می‌گرفت. نتایج تجربی نشان داد که مدل انتشار پیشنهادی آنها می‌توانست به طور موثر دینامیک انتشار بدافزار را در چندین دستگاه ناهمگن منعکس کند. استراتژی دفاعی نرخ بازیابی پویا به دست آمده، بهتر از استراتژی استاتیک در رابطه با نتایج کلی عمل می‌کرد.

لی و همکاران [9]، بر اساس تفاوت ظرفیت انتشار دستگاه هوشمند و توانایی تشخیص، یک مدل انتشار بدافزار پویا (DDSEIR) ارائه دادند. در مدل آنها ابتدا دستگاه‌های هوشمند با توجه به سطح قابلیت انتشار با مکانیسم سلسله مراتبی و در نظر گرفتن توپولوژی شبکه به گروه‌های مختلفی طبقه‌بندی شده‌اند و سپس، توانایی تشخیص دستگاه هوشمند با ویژگی‌های هویت و اطلاعات فرستنده ارزیابی شده است. آزمایش‌های آنها نشان داد که ظرفیت انتشار و توانایی تشخیص دستگاه هوشمند تاثیر قابل‌توجهی بر انتشار بدافزار دارد.

چیا و همکارانش [14]، نیز یک مدل انتشار بات‌نت پویا (IOT-BSI) ارائه دادند تا تاثیرات دو ویژگی اجتماعی (یعنی قابلیت گسترش دستگاه و توانایی شناسایی دستگاه) را بر تشکیل بات‌نت بررسی کنند. آنها توانایی شناسایی دستگاه را به توانایی شناسایی منطقی و توانایی شناسایی غیرمنطقی بر اساس نظریه جامعه‌شناختی تقسیم کردند و خصوصیات دینامیکی انتشار بات‌نت را به صورت نظری تحلیل کردند. نتایج بررسی آنها نشان داد که مدل آنها با وضعیت واقعی سازگارتر است و بهتر از چهار مدل مقایسه شده عمل می‌کند.

لاهروز و همکاران [15]، مدل SIRI را برای شبکه‌های ناهمگن پیشنهاد کردند. آنها تاثیر توپولوژی شبکه و پارامترهای مدل را بر آستانه همه‌گیری بررسی کردند. آنها مفهوم مصونیت موقت و امکان آلودگی مجدد را در یک شبکه ناهمگن با انتقال از گروه بهبودیافته به گروه آلوده بررسی کردند. بدافزار از طریق پیوندهای ارتباطی مبتنی بر زیرساخت (INF) و اتصالات دستگاه به دستگاه (D2D) در شبکه‌های ناهمگن پخش می‌شد.

چن و همکاران [16]، مدل SIRD را برای بررسی ماهیت دینامیکی انتشار از طریق این اتصالات معرفی کردند. نتایج تجزیه و تحلیل و مدل‌سازی نشان داده است که تحرک و استفاده از هر دو اتصال INF و D2D به طور قابل توجهی به انتشار بدافزار در شبکه‌ها کمک می‌کند. آنها نشان دادند که افزایش آگاهی امنیتی در میان کاربران و بهبود نرخ بازیابی می‌تواند میزان و شدت انتشار بدافزار را کاهش دهد.

شن و همکاران [17]، مدل HSEIR-V را بر اساس بیماری‌های همه‌گیر ارائه کردند. آنها نشانه‌های گروه سیستم‌های حساس، آلوده، بهبودیافته و خارج از شبکه را در نظر گرفتند. پایداری، نقاط تعادل و نسبت بازتولید پایه برای WSN ها در مدل آنها به دست آمده است. آنها خروج سیستم از شبکه را به دو شکل آلودگی به بدافزار یا بدون آلودگی در نظر گرفتند. آنها پارامتری را برای نشان دادن ناهمگونی شبکه با توجه به اتصال ارتباطی تعیین کردند.

کالام و همکارش [18]، یک مدل اپیدمی با گروه قرنطینه در شبکه IOT توسعه دادند. مدل آنها حتی در صورت حمله، می‌توانست عملکرد خوبی داشته باشد. همچنین با کنترل انتشار حملات مخرب در شبکه اینترنت اشیا، می‌توانست میزان آلودگی را نیز کاهش دهد.

ربرتو و همکاران [19]، رویکردی را برای افزایش امنیت اینترنت اشیا با نصب به‌روزرسانی‌های امنیتی بر روی گره‌های اینترنت اشیا پیشنهاد کردند. روش پیشنهادی از یک شبکه عصبی آگاه

فیزیکی برای تخمین پارامترهای مربوط به انتشار بدافزار استفاده می‌کرد. یافته‌های آنها نشان داد که تاکتیک کاهش انتشار بدافزار شامل انتخاب گره‌ها بر اساس ویژگی‌های شبکه موثرتر از انتخاب تصادفی گره است.

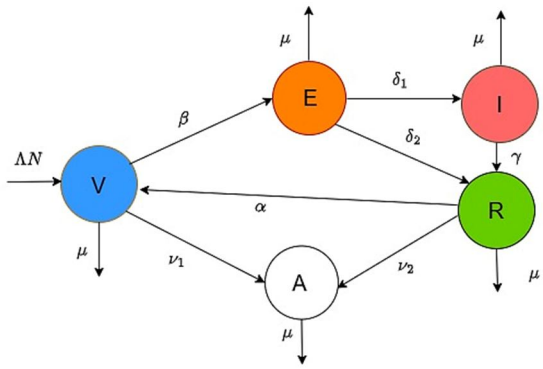
یاداو و همکاران [20]، یک مدل اپیدمی انتشار بدافزار SEIQR-V در شبکه‌های IOT پیشنهاد کردند. آنها به مدل اپیدمی SEIR دو کلاس به نام‌های واکسیناسیون (V) و قرنطینه (Q) اضافه کردند. در مدل آنها، واکسیناسیون به عنوان یک مدافع فعال برای جلوگیری از شیوع بدافزار و قرنطینه کلاسی به معنای جداسازی گره‌های آلوده در حین انجام فرآیند درمان برای حذف بدافزار مطرح شد. آنها نسبت بازتولید اولیه را برای مدلشان محاسبه کردند و نقاط تعادل مدل را به دست آوردند. علاوه بر آن پایداری مدل را برای نقطه تعادل بدون بدافزار و بدافزار محاسبه کردند. در کارهای انجام شده قبل گره‌های غیرفعال ابتدا آلوده می‌شوند و سپس ایمن می‌شوند. در حالی ایمن‌سازی گره‌های آسیب‌پذیر شبکه قبل از آلودگی کمک فراوانی به جلوگیری از انتشار آلودگی می‌کند. اعمال پادزهر روی کل گره‌ها هزینه و زمان زیادی را می‌طلبد. بنابراین برای هر گره بر اساس درجه آن نرخ واکسیناسیون مجزایی را در نظر گرفته شده است. در ضمن در مدل ارائه شده شانس مجدد واکسیناسیون پس از آلوده شدن گره نیز در نظر گرفته شده است. گره‌های بااهمیتی که آسیب‌پذیر هستند، ایمن شده‌اند و انتشار بدافزار در شبکه IOT مدل شده است. آستانه همه‌گیری در مدل پیشنهادی به دست آمده و در نهایت ارزیابی مدل در محیط متلب انجام شده است.

3. مدل پیشنهادی

در این بخش مدل VEIRV-A با در نظر گرفتن پادزهر روی گره‌های بااهمیت شبکه در شبکه‌های ناهمگن از جمله شبکه IOT ارائه شده است. از آنجایی که گره‌های با درجه بالا با گره‌های بیشتری در تماس هستند در صورتی که آلوده شوند آلودگی آنها منجر به آلودگی گره‌های بیشتری خواهد شد. از اینرو ایمن‌سازی آنها از انتشار آلودگی در شبکه جلوگیری می‌کند.

1.3. توصیف مدل

در مدل پیشنهادی گره‌های شبکه به پنج گروه آسیب‌پذیر (Vulnerable)، در معرض آلودگی (Exposed)، آلوده (Infected)، بهبودیافته (Recovered) و پادزهر (Antidotal) تقسیم شده‌اند. نمودار مربوط به گروه‌های مدل پیشنهادی در شکل (2) آمده است. نمادهای بکار رفته در مدل نیز در جدول (1) شرح داده شده‌اند.



شکل(2): نمودار ارتباطات بین گروه‌های مدل پیشنهادی

گره آسیب‌پذیر زمانی که در مجاورت گره آلوده به بدافزار قرار گیرد با نرخ β وارد گروه در معرض یا Exposed می‌شود. با گذشت زمان این گره با نرخ δ_1 آلوده می‌شود یا با نرخ δ_2 بهبود خواهد یافت. گره آلوده به بدافزار با نرخ γ به گره بهبودیافته تبدیل می‌شود و به وضعیت R می‌رود. از طرفی گره‌های بهبودیافته با نرخ α مجدد آسیب‌پذیر خواهند شد. با اعمال مکانیسم‌های امنیتی روی گره‌های بهبودیافته آنها با نرخ ν_2 ایمن می‌شوند. در این مدل گره‌های آسیب‌پذیر قبل از آلوده‌شدن با نرخ ν_1 وارد بخش پادزهر شده و پادزهر روی آنها اعمال می‌شود. این نرخ بر اساس درجه گره تعیین می‌شود. گره‌هایی که درجه بالاتری دارند، نرخ واکسینه بیشتری خواهند داشت. با توجه به اینکه در شبکه‌ای با N گره، درجه یک گره در بازه $[0..N]$ می‌تواند باشد، نرخ ν_1 برای گره با درجه k در بازه $[0..1]$ به صورت زیر تعیین خواهد شد.

$$\nu_1 = \frac{k}{N} \qquad (1)$$

با توجه به اینکه نرخ‌های موجود در شبکه مقادیر بین صفر و یک دارند، رابطه (1) بر اساس تغییر بازه k از $[0..N]$ به $[0..1]$ به دست آمده است. این رابطه نشان می‌دهد، هرچه درجه گره بیشتر باشد نرخ v_1 نیز بیشتر خواهد بود و با کاهش درجه نرخ v_1 نیز کمتر می‌شود. بنابراین v_1 تابعی از درجه است.

با گذشت زمان با اعمال مکانیسم‌های امنیتی روی گره‌ها چگالی گره‌های آلوده و در معرض کم می‌شود و به چگالی گره‌های پادزهر، بهبودیافته و آسیب‌پذیر اضافه می‌شود. در هر کدام از وضعیت‌ها برای یک گره امکان خروج از شبکه با نرخ μ وجود دارد.

جدول (1): نمادهای بکار رفته در مدل به همراه توصیف آنها

نماد	توصیف نماد
ΛN	نرخ اضافه شدن گره‌های جدید به شبکه (گره‌ها در حالت آسیب‌پذیر قرار می‌گیرند).
μ	نرخ خروج گره‌ها از شبکه (نرخ مرگ و میر).
β	نرخ انتشار بدافزار.
v_1	نرخ واکسیناسیون گره‌های آسیب‌پذیر بر اساس اهمیت گره.
v_2	نرخ واکسیناسیون یا اعمال پادزهر روی گره‌های بهبودیافته.
γ	نرخ بهبود از بدافزار.
δ_1	نرخ فعال شدن آلودگی در یک گره در معرض آلودگی.
δ_2	نرخ بهبود گره بدون فعال شدن آلودگی.
α	نرخ انتقال گره‌های بهبود یافته به آسیب‌پذیر.
V^k	چگالی گره‌های آسیب‌پذیر با درجه k در شبکه
E^k	چگالی گره‌های در معرض آلودگی با درجه k در شبکه.
I^k	چگالی گره‌های آلوده با درجه k در شبکه.
R^k	چگالی گره‌های بهبودیافته از بدافزار با درجه k در شبکه .
A^k	چگالی گره‌های با درجه k در شبکه که پادزهر روی آنها اعمال شده است.
N	تعداد گره‌های شبکه.

با توجه به شرح مدل معادلات مدل به صورت زیر می‌باشند:

$$\begin{aligned}
\frac{dV^k(t)}{dt} &= \Lambda N - \beta V^k(t)\theta^k(t) - \mu V^k(t) \\
&\quad - v_1 V^k(t) + \alpha R^k(t) \\
\frac{dE^k(t)}{dt} &= \beta V^k(t)\theta^k(t) - (\mu + \delta_1 + \delta_2)E^k(t) \\
\frac{dI^k(t)}{dt} &= \delta_1 E^k(t) - (\mu+\gamma)I^k(t) \\
\frac{dR^k(t)}{dt} &= \gamma I^k(t) - (\mu + v_2 + \alpha)R^k(t) \\
&\quad + \delta_2 E^k(t) \\
\frac{dA^k(t)}{dt} &= v_2 R^k(t) + v_1 V^k(t) - \mu A^k(t)
\end{aligned} \qquad (2)$$

در روابط ذکر شده، $\theta^k(t)$ احتمال آلوده بودن به بدافزار در گره همسایه با درجه k می‌باشد که می‌توان آن را به صورت رابطه (3) در نظر گرفت.

$$\theta(t) = \frac{1}{< K >} \sum_{k=m}^{n} kP(k)I^k(t) \qquad (3)$$

میانگین درجه شبکه نیز برابر است با $< K > = \sum_{j=1}^{n} j\, p(j)$ به طور معمول جهت ساده‌سازی روند کار شبیه‌سازی فرضیاتی برای شبیه‌سازی در نظر گرفته می‌شود. در این مقاله نیز فرضیات در نظر گرفته شده به شرح زیر می‌باشند:

1- تعداد کل گره‌ها در زمان ثابت می‌ماند، یعنی تولدها با مرگ‌ها متعادل می‌شوند، بنابراین $(\Lambda = \mu)$.

2- $V^k(t) + E^k(t) + I^k(t) + R^k(t) + A^k = 1$

3- شبکه یک شبکه ناهمگن است.

4- در ابتدای شبیه‌سازی 10 درصد گره‌ها آلوده به بدافزار هستند.

2.3. تحلیل دینامیک مدل

در تحلیل دینامیک مدل یکی از مواردی که انجام می‌شود، محاسبه مقدار عدد بازتولید اولیه یا R_0 است. این مقدار بیان‌کننده تعداد آلودگی‌های ثانویه ناشی از آلودگی اولیه در مدت زمان حیات بدافزار است [21]. در حقیقت عدد باز تولید اولیه حد

آستانه اپیدمی انتشار بدافزار در شبکه است که اگر مقدار آن کمتر از یک باشد همه‌گیری در شبکه وجود نـدارد و بـالعکس اگـر مقدار آن از یک بیشتر باشد همه‌گیری انتشار بدافزار در شـبکه وجود دارد. یکی از روش‌های به دست آوردن مقدار R_0 روش تولید بعدی [21]، است. در این روش بردارهای f با توجه بـه سرعت انتقال آلودگی و بردار v بر اساس نرخ انتقال آلودگی در گروه‌های آلوده به بدافزار به دست می‌آیند. در مدل پیشـنهادی گروه‌هایی که در آنها آلودگی وجود دارد E و I هستند. در نتیجه بردارهای f و v به صورت زیر خواهند بود:

$$v(x) = \begin{bmatrix} (\mu + \delta_1 + \delta_2)E^k(t) \\ (\mu + \gamma)I^k(t) - \delta_1 E^k(t) \end{bmatrix}$$
$$f(x) = \begin{bmatrix} \beta\theta^k(t)V(0) \\ 0 \end{bmatrix} \quad (4)$$

و در ادامه ماتریس‌های F و V به صورت زیر محاسبه می‌شوند:

$$F = \begin{bmatrix} \frac{\partial f_1}{\partial E} & \frac{\partial f_1}{\partial I} \\ \frac{\partial f_2}{\partial E} & \frac{\partial f_2}{\partial I} \end{bmatrix} = \begin{bmatrix} 0 & \beta\frac{< K^2 >}{< K >}\frac{\Lambda}{\mu} \\ 0 & 0 \end{bmatrix}$$
$$V = \begin{bmatrix} \frac{\partial v_1}{\partial E} & \frac{\partial v_1}{\partial I} \\ \frac{\partial v_2}{\partial E} & \frac{\partial v_2}{\partial I} \end{bmatrix} = \begin{bmatrix} \mu + \delta_1 + \delta_2 & 0 \\ -\delta_1 & \mu + \gamma \end{bmatrix} \quad (5)$$

که $< K^2 > = \begin{bmatrix} 1 \\ 2 \\ \vdots \\ \Delta \end{bmatrix} [p \quad 2p \quad \dots \quad \Delta p]$ و مقدار R_0 بر اساس رابطه $R_0 = \rho(FV^{-1})$ به دست می‌آید که ρ شعاع طیفی FV^{-1} یا بزرگترین مقدار ویژه ماتریس FV^{-1} است. پس داریم:

$$R_0 = \frac{\beta\delta_1}{(\gamma + \mu)(\mu + \delta_1 + \delta_2)}\frac{< K^2 >}{< K >}\frac{\Lambda}{\mu} \quad (6)$$

با توجه به رابطه به دست آمده برای R_0 مشخص است که نرخ آلودگی و نرخ فعال شـدن آلـودگی بـا R_0 رابطـه مسـتقیم و نرخ‌های بهبود δ_2 و γ با آن رابطه عکس دارند و همچنین نقش ساختار شبکه و نرخ مرگ و میر و تعداد گره‌های وارد شده به شبکه را در R_0 می‌توان دید.

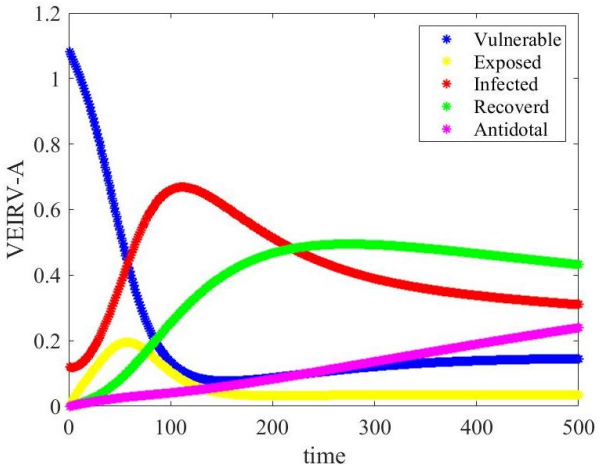
4. نتایج شبیه‌سازی مدل

مدل پیشنهادی روی مجموعه داده استاندارد socfb-Amherst41 با 2235 گره و 90954 یال در محیط متلـب شبیه‌سـازی شـده است و نتایج شبیه‌سازی در این بخش آمده اسـت. شـکل (3) نمودار گروه‌های مختلف مدل VEIRV-A را بـه ازای مقـادیر پارامترهای جدول (2) روی مجموعه داده اسـتاندارد در مـدت زمان شبیه‌سازی (T) 500 نشان می‌دهد. برآورد پارامترهای مدل در مدل‌سازی بسیار مهم است. با این حال، تخمین پارامتر یک مشکل چالش‌برانگیز است که می‌تواند زمانبر و گران باشد، بـه خصوص زمانی که پارامترهای تخمینی متعددی وجـود داشـته باشند. روش‌های مختلفی برای تخمین این پارامترها وجود دارد. یکی از روش‌های موثر، روش مونت کارلو است که برای تخمین پارامتر در مقیاس بزرگ مناسب است. در فرآیند مدل‌سازی، ما از روش مونت کارلو برای تخمین پارامترهای مدل با بهره‌گیری از کارایی و دقت آن استفاده کرده‌ایم [22].

جدول (2): مقدار عددی پارامترهای مدل در شبیه‌سازی روی مجموعه داده‌ی استاندارد SOCFB-AMHERST41

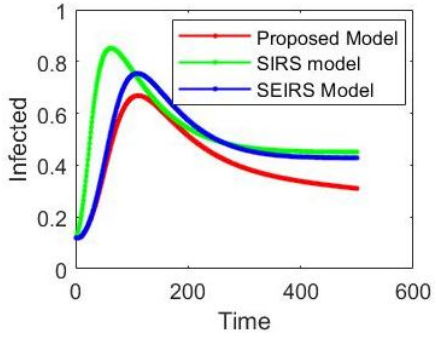
پارامتر	مقدار	پارامتر	مقدار
μ	0.0001	α	0.005
β	0.1	ν_2	0.001
γ	0.007	V	2012
δ_1	0.06	E	0
δ_2	0.004	I	223
A	0	R	0
T	500	Λ	0.0001

در ابتدای شبیه‌سازی از جمعیـت آسـیب‌پذیرها کـم شـده بـه گروه‌های در معرض آلودگی و آلوده اضافه می‌شود و با گذشت زمان، چگالی گره‌های آلوده کاهش و چگالی گـره‌هـای بهبـود یافته افزایش می‌یابد. پس از ورود گره‌ها به گروه بهبود یافته با نرخ $\nu_2 = 0.001$ از چگالی گره‌های بهبود یافته کاسته شده و به چگالی گره‌های تحت تاثیر پادزهر اضافه می‌شود.



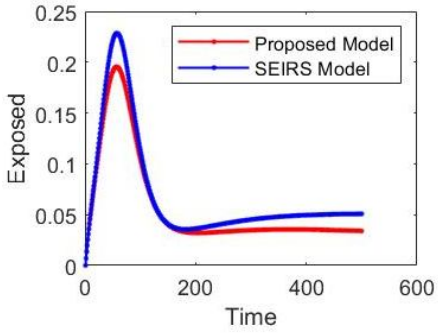
شکل(3): گروه‌های V، E، I، R، A و D در مدل پیشنهادی روی مجموعه داده استاندارد SOCFB-AMHERST41

شکل (4) گروه آلوده را در سه مدل SIRS، SEIRS و مدل پیشنهادی VEIRV-A مقایسه می‌کند. همان‌طور که نتایج شبیه‌سازی شکل(4) نشان می‌دهد در مدل پیشنهادی روند انتشار بدافزار نسبت به دو مدل دیگر کاهش داشته است. با توجه به واکسینه شدن گره‌های آسیب‌پذیر بر اساس درجه آنها از انتشار آلودگی در شبکه جلوگیری شده و سرعت انتشار نیز کاهش یافته است.

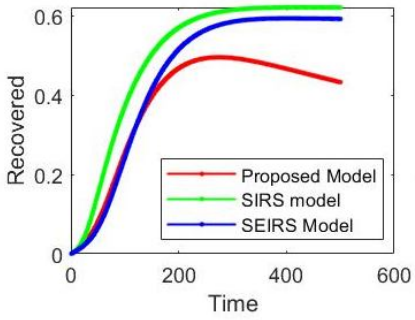


شکل(4): مقایسه گروه آلوده‌ها در سه مدل پیشنهادی و مدل‌های SIRS و SEIRS بر روی مجموعه داده استاندارد SOCFB-AMHERST41

روش پیشنهادی موجب شده است که چگالی آلوده‌های غیرفعال نیز کمتر شود. کاهش انتشار گروه در معرض آلودگی در مدل VEIRV-A نسبت به مدل SEIRS در شکل (5) به وضوح مشخص است. شکل (6) نیز به بررسی تغییرات گروه بهبود یافته‌ها در سه مدل مورد مقایسه می‌پردازد. در مدل پیشنهادی نرخ واکسیناسیون گره‌های آسیب‌پذیر بر اساس درجه تعیین شده و گره‌هایی که درجه بالاتری داشتند، نرخ واکسیناسیون آنها بیشتر شده است. در نتیجه چگالی گره‌های آلوده در این مدل کاهش یافته و به دنبال این کاهش، چگالی بهبود یافته‌ها نیز کمتر شده است. در شکل (6) این کاهش به وضوح دیده می‌شود.



شکل(5): مقایسه گروه در معرض آلودگی در دو مدل پیشنهادی و SEIRS بر روی مجموعه داده استاندارد SOCFB-AMHERST41



شکل (6): مقایسه گروه بهبودیافته‌ها در سه مدل پیشنهادی و مدل‌های SIRS و SEIRS بر روی مجموعه داده استاندارد SOCFB-AMHERST41

با توجه به رابطه (6) برای R_0 پارامترهای β و δ_1 با R_0 رابطه مستقیم دارند و با افزایش آنها R_0 نیز افزایش می‌یابد که شکل‌های (7) و (8) تاییدی بر این رابطه هستند. از طرف دیگر، رابطه معکوس R_0 با δ_2 و γ نیز در شکل‌های (9) و (10) نشان داده شده است. در جدول (3) مقادیر عدد بازتولید اولیه (R_0) به ازای افزایش نرخ آلودگی (β) در بازه [0.04,0.058] آورده شده است. با افزایش β مقادیر R_0 نیز افزایش یافته است. در مقادیر $\beta \geq 0.048$ همه‌گیری انتشار بدافزار در شبکه مشاهده می‌شود. این نتایج با رابطه (6) مطابقت دارد. شکل (7) نیز این نتایج را به صورت نمودار تحلیل کرده است. جدول (4) نیز مقادیر R_0

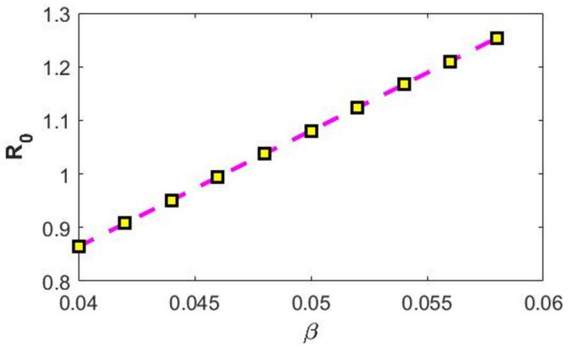
را با افزایش مقدار نرخ فعال شدن آلودگی گره‌های در معرض آلودگی (δ_1) در بازه [0.12,0.138] نشان می‌دهد. شکل (8) روند تغییرات را به صورت نمودار به تصویر می‌کشد. همان‌طور که انتظار می‌رود با افزایش نرخ δ_1 مقدار عدد باز تولید اولیه نیز افزایش می‌یابد و شبکه به سمت همه‌گیری انتشار بدافزار پیش می‌رود. این روند افزایشی R_0 نیز با رابطه (6) مطابقت دارد.

جدول(3): مقادیر R_0 به ازای مقادیر مختلف β

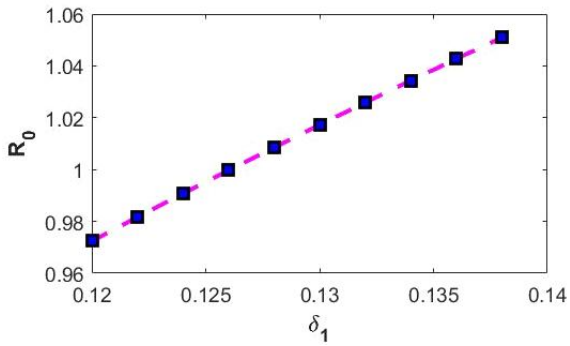
پارامتر	مقدار				
β	0.040	0.042	0.044	0.046	0.048
R_0	0.8644	0.9076	0.9508	0.9940	1.0372
β	0.050	0.052	0.054	0.056	0.058
R_0	1.0805	1.1237	1.1669	1.2101	1.2533

جدول(4): مقادیر R_0 به ازای مقادیر مختلف δ_1

پارامتر	مقدار				
δ_1	0.120	0.122	0.124	0.126	0.128
R_0	0.9724	0.9816	0.9907	0.9997	1.0172
δ_1	0.130	0.132	0.134	0.136	0.138
R_0	1.0085	1.0258	1.0343	1.0427	1.0509



شکل(7): روند تغییرات R_0 با تغیر β



شکل(8): روند تغییرات R_0 با تغیر δ_1

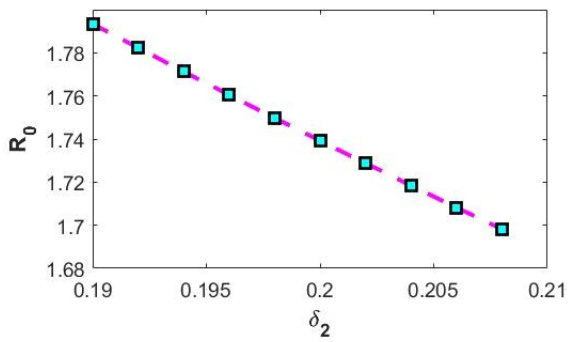
جدول (5) نیز همان‌طور که در رابطه (6) آمده است، روند کاهشی مقادیر R_0 را با افزایش نرخ بهبود گروه در معرض آلودگی (δ_2) در بازه [0.19,0.208] نشان می‌دهد. با افزایش نرخ بهبود δ_2 شاهد کاهش عدد بازتولید اولیه در شبکه هستیم. افزایش نرخ بهبود گره‌های درمعرض آلودگی در شبکه منجر به از بین رفتن همه‌گیری انتشار بدافزار در شبکه می‌شود. در شکل (9) نتایج این تغییرات به صورت تصویری نشان داده شده است. نتایج به دست آمده در جدول (6) و معادل تصویری آن در شکل (10) بیانگر کاهش مقدار R_0 به ازای افزایش مقدار نرخ بهبود گره‌های آلوده (γ) است. به ازای مقادیر $\gamma \geq 0.192$ همه‌گیری انتشار بدافزار در شبکه از بین رفته و مقدار R_0 از یک کمتر شده است.

جدول(5): مقادیر R_0 به ازای مقادیر مختلف δ_2

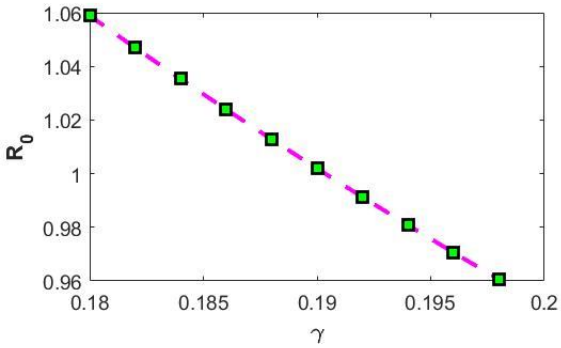
پارامتر	مقدار				
δ_2	0.190	0.192	0.194	0.196	0.198
R_0	1.7934	1.7823	1.7713	1.7605	1.7498
δ_2	0.200	0.202	0.204	0.206	0.208
R_0	1.7392	1.7288	1.7184	1.7082	1.6982

جدول(6): مقادیر R_0 به ازای مقادیر مختلف γ

پارامتر	مقدار				
γ	0.180	0.182	0.184	0.186	0.188
R_0	1.0588	1.0469	1.0353	1.0239	1.0128
γ	0.190	0.192	0.194	0.196	0.198
R_0	1.0019	0.9913	0.9808	0.9706	0.9606



شکل(9): روند تغییرات R_0 با تغیر δ_2



شکل(10): روند تغییرات R_0 با تغییر γ

5. نتیجه‌گیری

در این مقاله مدل VEIRV-A بر اساس مدل‌سازی بیماری‌های همه‌گیری با در نظر گرفتن گروه پادزهر در شبکه اینترنت اشیا ارائه شده است. در این مدل برای نرخ ورود گره‌های آسیب‌پذیر به گروه پادزهر بر اساس درجه گره یک میزان اهمیت تعیین می‌شود. گره‌های با اهمیت بیشتر شانس بیشتری برای واکسینه شدن دارند. بنابراین تاثیر پادزهر در شبکه بیشتر شده است. مدل پیشنهادی بر روی مجموعه داده استاندارد socfb-Amherst41 در محیط متلب پیاده‌سازی شده است. در تحلیل دینامیک مدل، مقدار R_0 محاسبه شده است. پارامترهای β، δ_1 با R_0 رابطه مستقیم دارند و پارمترهای γ و δ_2 رابطه عکس دارند که در نتایج شبیه‌سازی نیز این به وضوح مشاهده شده است. زمانی که مقدار R_0 کمتر از یک است انتشار بدافزار در شبکه متوقف شده است و همه‌گیری انتشار بدافزار در شبکه وجود ندارد. همچنین زمانی که R_0 از یک بیشتر است همه‌گیری انتشار بدافزار در شبکه دیده می‌شود. نتایج شبیه‌سازی نشان می‌دهد که مدل ارائه شده نسبت به مدل‌های SIRS و SEIRS کاهش انتشار آلودگی بیشتری داشته و عملکرد بهتری را در بر داشته است. در کارهای آینده به بررسی چندین نوع آلودگی در شبکه‌های ناهمگن و همچنین تاثیر خوشه‌بندی در انتشار بدافزار خواهیم پرداخت.

تعارض منافع: نویسندگان اعلام می‌کنند که هیچ تعارض منافعی ندارند.

مراجع

[1] F. Sadoughi, A. Behmanesh, and N. Sayfouri, “Internet of Things in Medicine: A Systematic Mapping Study,” J. Biomed. Inform., vol. 103, p. 103383, 2020, doi: 10.1016/j.jbi.2020.103383.

[2] C. Sobin, “A Survey on Architecture, Protocols and Challenges in IoT,” Wireless Pers. Commun., vol. 112, no. 3, pp. 1383-1429, 2020, doi: 10.1007/s11277-020-07108-5.

[3] H. Xia, L. Li, X. Cheng, C. Liu, and T. Qiu, “A Dynamic Virus Propagation Model Based on Social Attributes in City IoT,” IEEE Internet Things J., vol. 7, no. 9, pp. 8036-8048, Sept. 2020, doi: 10.1109/JIOT.2020.2990365.

[4] J. Javaid and I. H. Khan, “Internet of Things (IoT) Enabled Healthcare Helps to Take the Challenges of COVID-19 Pandemic,” J. Oral Biol. Craniofacial Res., vol. 11, no. 2, pp. 209-214, 2021, doi: 10.1016/j.jobcr.2021.01.015.

[5] B. Ramphull and S. D. Nagowah, “A Knowledge Model for IoT-Enabled Smart Banking,” J. Knowl. Econ., vol. 15, no. 2, pp. 9174-9206, 2024, doi: 10.1007/s13132-023-01434-2.

[6] M. Moazzami et al., “Internet of Things Architecture for Intelligent Transportation Systems in a Smart City,” in Proc. 3rd Global Power, Energy Commun. Conf. (GPECOM), 2021, pp. 330-335, doi: 10.1109/GPECOM52585.2021.9587692.

[7] J. Fan et al., “The Future of Internet of Things in Agriculture: Plant High-Throughput Phenotypic Platform,” J. Clean. Prod., vol. 280, p. 123651, 2021, doi: 10.1016/j.jclepro.2020.123651.

[8] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, “A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues,” IEEE Commun. Surveys Tuts., vol. 22, no. 2, pp. 1191-1221, 2020, doi: 10.1109/COMST.2019.2962586.

[9] L. Li, J. Cui, R. Zhang, H. Xia, and X. Cheng, “Dynamics of Complex Networks: Malware Propagation Modeling and Analysis in Industrial

Internet of Things," IEEE Access, vol. 8, pp. 64184-64192, 2020, doi: 10.1109/ACCESS.2020.2984668.

[10] A. Akrami and M. Parsamanesh, "Investigation of a Mathematical Fuzzy Epidemic Model for the Spread of Coronavirus in a Population," Soft Comput. J., vol. 11, no. 1, pp. 2-9, 2022, doi: 10.22052/SCJ.2022.246053.1045 [In Persian].

[11] A. Yadollahi and H. Sabaghian-Bidgoli, "A Simulation Model for the Propagation of COVID-19 Virus Based on the Discrete-Time Markov Chain," Soft Comput. J., vol. 11, no. 2, pp. 88-103, 2023, doi: 10.22052/SCJ.2023.246527.1076 [In Persian].

[12] W. O. Kermack and A. G. McKendrick, "A Contribution to the Mathematical Theory of Epidemics," Proc. Roy. Soc. Lond. Ser. A, vol. 115, no. 772, pp. 700-721, 1927, doi: 10.1098/rspa.1927.0118.

[13] X. Zhu et al., "Modeling and Analysis of Malware Propagation for Cluster-Based Wireless Sensor Networks," in Proc. IEEE 6th Int. Conf. Dependability Sensor, Cloud Big Data Syst. Appl. (DependSys), 2020, pp. 49-54, doi: 10.1109/DependSys51298.2020.00010.

[14] H. Xia, L. Li, X. Cheng, X. Cheng, and T. Qiu, "Modeling and Analysis Botnet Propagation in Social Internet of Things," IEEE Internet Things J., vol. 7, no. 8, pp. 7470-7481, 2020, doi: 10.1109/JIOT.2020.2984662.

[15] A. Lahrouz, A. Settati, H. El Mahjour, M. El Jarroudi, and M. El Fatini, "Global Dynamics of an Epidemic Model with Incomplete Recovery in a Complex Network," J. Franklin Inst., vol. 357, no. 7, pp. 4414-4436, 2020, doi: 10.1016/j.jfranklin.2020.03.010.

[16] B.-R. Chen, S.-M. Cheng, and M. B. Mwangi, "A Mobility-Based Epidemic Model for IoT Malware Spread," IEEE Access, vol. 10, pp. 107929-107941, 2022, doi: 10.1109/ACCESS.2022.3213032.

[17] S. Shen et al., "HSIRD: A Model for Characterizing Dynamics of Malware Diffusion in Heterogeneous WSNs," J. Netw. Comput. Appl., vol. 146, p. 102420, 2019, doi: 10.1016/j.jnca.2019.102420.

[18] S. Kalam and A. K. Keshri, "Epidemic Model on Denial of Service Attack in IoT Network," in Proc. Int. Conf. IoT Blockchain Technol. (ICIBT), 2022, pp. 1-6, doi: 10.1109/ICIBT52874.2022.9807815.

[19] R. Casado-Vara, M. Severt, A. Diaz-Longueira, A. M. del Rey, and J. L. Calvo-Rolle, "Dynamic Malware Mitigation Strategies for IoT Networks: A Mathematical Epidemiology Approach," Mathematics, vol. 12, no. 2, p. 250, 2024, doi: 10.3390/math12020250.

[20] P. Yadav and A. K. Keshri, "The Dynamics of SEIQR-V Malware Propagation Model in IoT Networks," in Proc. Int. Conf. IoT Blockchain Technol. (ICIBT), 2022, pp. 1-6, doi: 10.1109/ICIBT52874.2022.9807775.

[21] Z. Yu et al., "SEI2RS Malware Propagation Model Considering Two Infection Rates in Cyber-Physical Systems," Physica A: Stat. Mech. Appl., vol. 597, p. 127207, 2022, doi: 10.1016/j.physa.2022.127207.

[22] M. Severt, R. Casado-Vara, and A. Martin del Rey, "A Comparison of Monte Carlo-Based and PINN Parameter Estimation Methods for Malware Identification in IoT Networks," Technologies, vol. 11, no. 5, p. 133, 2023, doi: 10.3390/technologies11050133.