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 ـ کرمان ـ ایران ـ so_hosseini@uk.ac.ir

[2] گروه کامپیوتر ـ واحد شهربابک ـ دانشگاه آزاد اسلامی ـ شهربابک ـ ایران ـ asadi.cs@iau.ac.ir

چکیده: با تکامل شبکه‌ی بی‌سیم نسل پنجم، اینترنت اشیا (IOT) نیز تحول شگفتی در زندگی بشر ایجاد کرده است. از اینرو مطالعه‌ی دقیق‌تر فناوری اینترنت اشیا و حوزه‌های مختلف آن از جمله امنیت این حوزه ضروری خواهد بود. در زمینه‌ی 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- درمعرض 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 درجه‌ی گره میزان بااهمیت 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 آستانه‌ی اپیدمی انتشار بدفزار (R_0) در مدل پیشنهادی محاسبه شده است. مقایسه‌ی مدل با دو مدل SIRS و SEIRS نشان داد مدل پیشنهادی نسبت به دو مدل دیگر عملکرد بهتری داشته است.

واژه‌های کلیدی: **مدل‌سازی انتشار بدافزار - مدل‌سازی بیماری‌های همه‌گیری - عدد بازتولید اولیه - حد آستانه‌ی همه‌گیری - اینترنت اشیا.**

* نویسنده مسئول:سوده حسینی، **so_hosseini@uk.ac.ir**

VEIRV-A Malware Propagation Modeling in the Internet of Things Networks

Soodeh Hosseini [1*], Associate Professor, Elham Asadi [2], Assistant Professor

[1] Department of Computer Science, Faculty of Mathematics and Computer, Shahid Bahonar University of Kerman, Kerman, Iran, so_hosseini@uk.ac.ir

[2] Department of Computer, Shahrbabak Branch, Islamic Azad University, Shahrbabak, Iran, asadi.cs@iau.ac.ir

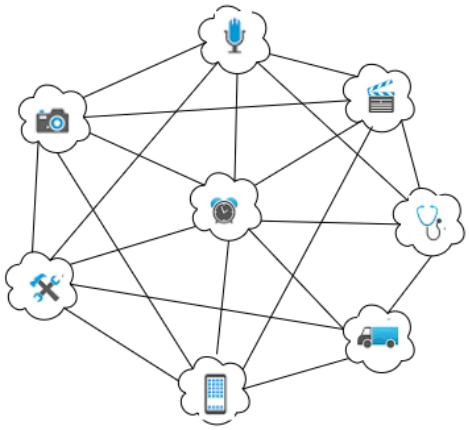
Abstract: With the evolution of the fifth generation wireless network, the Internet of Things (IoT) has also created a surprising transformation in human life. Therefore, a more detailed study of the Internet of Things technology and its various fields, including the security of this field, will be necessary. In the field of security of Internet of Things networks, one of the issues that has been raised is the spread of malware. In this paper, we have modeled the spread of malware in Internet of Things networks with the epidemic disease model of vulnerable - exposed to infection - infected - recovered - antidote. The effect of applying antidote to recovered and vulnerable nodes on the spread of malware in Internet of Things networks has been investigated. We have determined the importance of the node in the network based on the degree of the node and based on this rate, the vulnerable nodes in the network have been secured. Securing nodes based on the degree has led to a reduction in the spread of malware in the network. The epidemic threshold of malware spread (R_0) has been calculated in the proposed model. Comparing the model with the SIRS and SEIRS models showed that the proposed model performed better than the other two models.

Keywords: *Malware propagation modeling - Epidemic model- Basic reproduction number - Epidemic threshold limit - Internet of Things.*

*** Soodeh Hosseini**

۱. 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 [۱]. به عبارتی دیگر اینترنت اشیاء (IOT) یک فناوری است که اشیاء ممکن را به‌هم متصل می‌کند، به‌طوری که اشیاء شروع به برقراری ارتباط بین خود می‌کنند تا خدمات بهتری را برای کاربران به‌شکل غیرقابل تصوری ارائه دهند و زندگی آنها را آسان‌تر کنند. اشیاء هوشمند می‌توانند مجموعه‌ای از حسگرها، محرک‌ها، تلفن‌های هوشمند و غیره باشند [۲]. اینترنت اشیاء شهری امروزی سیستم‌های نرم‌افزار فشرده و مبتنی بر داده‌ها در مقیاس بزرگ هستند، که هزاران دستگاه هوشمند متصل به‌هم و دارای هوش محدود را شامل می‌شوند [۳]. شکل (۱) نمایی از اشیاء را در یک شبکه‌ی اینترنت اشیا نشان می‌دهد. این شبکه‌ها در حال حاضر در زمینه‌های مختلفی مانند پزشکی [۱, ۴]، بانکداری [۵]، حمل و نقل [۶]، کشاورزی [۷] و ... استفاده می‌شوند. باز بودن، پویایی و ناهمگونی شبکه‌ی اینترنت اشیاء، کاربران را در یک محیط بسیار ناامن قرار می‌دهد [۳]. هنگام ساخت یک دستگاه اینترنت اشیاء، سازندگان اغلب تاکید زیادی بر هزینه، اندازه و قابلیت استفاده دارند، در حالی که جنبه‌های امنیتی و پزشکی قانونی معمولا نادیده گرفته می‌شوند [۸]. بنابراین اشیاء ممکن است آسیب‌پذیری‌های زیادی داشته باشند و این دستگاه‌های آسیب‌پذیر قربانیان مناسبی برای ورود بدافزار یا نرم‌افزار مخرب به شبکه هستند. بدافزارها بانفوذ در شبکه و اختلال در سیستم‌ها سالیانه خسارات زیادی وارد می‌کنند. در سال‌های اخیر، مسائل امنیتی اینترنت اشیاء توجه گسترده‌ای را در محافل دانشگاهی و محافل صنعتی به خود جلب کرده است [۳]. حوزه دانشگاهی بر امنیت اینترنت اشیاء 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 تأثیر عوامل مختلف بر انتشار را تجزیه و تحلیل می‌کند [۹].



شکل (۱): نمایی از شبکه‌ی 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 آنهاست. 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 براساس بیماری‌های همه‌گیری است. این روش مدل‌سازی با توجه به شباهت بین ویروس‌ها و بدافزارها انجام می‌شود. در زمینه‌ی انتشار ویروس‌های بیولوژیک، به مدل‌سازی انتشار ویروس با روش بیماری‌های همه‌گیری تحقیقاتی صورت گرفته است [۱۰, ۱۱]. 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 دربین این سه گروه مدل کرد [۱۲]. مدل او به مدل SIR شهرت یافت و به‌عنوان مدل پایه مورد استفاده قرار گرفت. از آنجایی که دستگاه‌های اینترنت اشیاء آسیب‌پذیری‌های بیشتری نسبت به بقیه‌ی گره‌های شبکه‌ها دارند، بیشتر مستعد انتشار بدافزار هستند. در این مقاله با درنظر گرفتن پنج گروه آسیب‌پذیرها (Vulnerable)، در معرض آلودگی (Exposed)، آلوده‌ها (Infected)، بهبودیافته‌ها (Recovered) و پادزهر (Antidotal)، مدل VEIRV-A بر روی شبکه‌های اینترنت اشیاء ارائه شده است. در مدل ارائه شده گره‌های آسیب‌پذیر براساس درجه‌شان میزان بااهمیت بودن آنها تعیین و براساس نرخ اهمیت واکسینه شده‌اند. با توجه به صرفه‌جویی در زمان و هزینه‌ی اعمال پادزهر روی تمام گره‌های شبکه، ما این نرخ را به‌عنوان نرخ واکسیناسیون در نظر گرفته‌ایم. از طرفی در مدل ارائه شده طی دو مرحله پادزهر روی گره‌ها اعمال شده است. مرحله‌ی اول با توجه به درجه‌ی گره، گره‌های آسیب‌پذیر واکسینه شده‌اند و در مرحله‌ی دوم گره‌هایی که در مرحله‌ی اول پادزهر روی آنها اعمال نشده است و آلوده شده‌اند، پس از بهبود شانس ورود به مرحله‌ی اعمال پادزهر را پیدا کرده‌اند. بنابراین انتشار آلودگی در شبکه کاهش بیشتری داشته است. در زمینه‌ی تحلیل دینامیک شبکه حد آستانه‌ی همه‌گیری مدل ارائه شده به‌دست آمده است. بخش‌بندی ادامه‌ی مقاله به این صورت است که در بخش دوم کارهای انجام شده در زمینه‌ی انتشار بدافزار در شبکه‌های اینترنت اشیاء 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 نتیجه گیری مدل آمده است.

۲. کارهای مرتبط

باتوجه به پیشرفت تکنولوژی و استفاده از اشیاء 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 [۱۳] در مقاله‌ی خود مدل SLRP را مبتنی بر بیماری‌های همه‌گیری برای دستگاه‌های اینترنت اشیاء ناهمگن ارائه دادند به‌طوریکه 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 به‌طور جامع هزینه و میزان آلودگی کلی دستگاه را در نظر می‌گرفت. نتایج تجربی نشان داد که مدل انتشار پیشنهادی آنها می‌توانست به‌طور موثر دینامیک انتشار بدافزار را در چندین دستگاه ناهمگن منعکس کند. استراتژی دفاعی نرخ بازیابی پویا به‌دست‌آمده، بهتر از استراتژی استاتیک در رابطه با نتایج کلی عمل می‌کرد. لی و همکاران [۹] 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 درنظر 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 تأثیر قابل‌توجهی بر انتشار بدافزار دارد. چیا و همکارانش [۱۴] نیز یک مدل انتشار بات‌نت پویا (IOT-BSI) ارائه دادند تا تأثیرات 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 [۱۵] مدل SIRI را برای شبکه‌های ناهمگن پیشنهاد کردند. آنها تأثیر 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 [۱۶]، 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 به‌طور 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 [۱۷] مدل HSEIR-V را بر اساس بیماری‌های همه‌گیر ارائه کردند. آنها نشانه‌های گروه سیستم‌های حساس، آلوده، بهبود یافته و خارج از شبکه را در نظر گرفتند. پایداری، نقاط تعادل و نسبت بازتولید پایه برای WSN ها در مدل آنها به‌دست آمده است. آنها خروج سیستم از شبکه را به دو شکل آلودگی به‌بدافزار یا بدون آلودگی درنظر گرفتند. آنها پارامتری را برای نشان دادن ناهمگونی شبکه با توجه به اتصال ارتباطی تعیین کردند. کالام و همکارش [۱۸] 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 شبکه‌ی اینترنت اشیاء، می‌توانست میزان آلودگی را نیز کاهش دهد. ربرتو و همکاران [۱۹] رویکردی را برای افزایش امنیت اینترنت اشیاء با نصب به‌روزرسانی‌های امنیتی بر روی گره‌های اینترنت اشیاء پیشنهاد کردند. روش پیشنهادی از یک شبکه عصبی آگاه فیزیکی برای تخمین پارامترهای مربوط به انتشار بدافزار استفاده می‌کرد. یافته‌های انها نشان داد که تاکتیک کاهش انتشار بدافزار شامل انتخاب گره‌ها بر اساس ویژگی‌های شبکه موثرتر از انتخاب تصادفی گره است. یاداو و همکاران [۲۰] 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 به‌عنوان 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 به‌دست آوردند. علاوه بر آن پایداری مدل را برای نقطه تعادل بدون بدافزار و بدافزار محاسبه کردند. مدل‌های مطرح شده انتشار بدافزار را در شبکه مدل می‌کنند. در کارهای انجام شده‌ی قبل گره‌های غیر فعال ابتدا آلوده می‌شوند و سپس ایمن می‌شوند. در حالی ایمن‌سازی گره‌های اسیب‌پذیر 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 براساس درجه‌ی آن نرخ واکسیناسیون مجزایی را درنظر گرفته شده است. ضمنا در مدل ارائه شده شانس مجدد واکسیناسیون پس از آلوده شدن گره نیز درنظر گرفته شده است. گره‌های بااهمیتی که آسیب‌پذیر هستند ایمن شده‌اند و انتشار بدافزار در شبکه‌ی IOT مدل شده است. آستانه‌ی همه‌گیری در مدل پیشنهادی به‌دست آمده و در نهایت ارزیابی مدل در محیط متلب انجام شده است.

۳. مدل پیشنهادی

در این بخش مدل $VEIRV-A$ با در نظر گرفتن پادزهر روی گره‌های با اهمیت شبکه در شبکه‌های ناهمگن از جمله شبکه‌ی IOT ارائه شده است. از آنجایی که گره‌های با درجه‌ی 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.

۳-۱. توصیف مدل

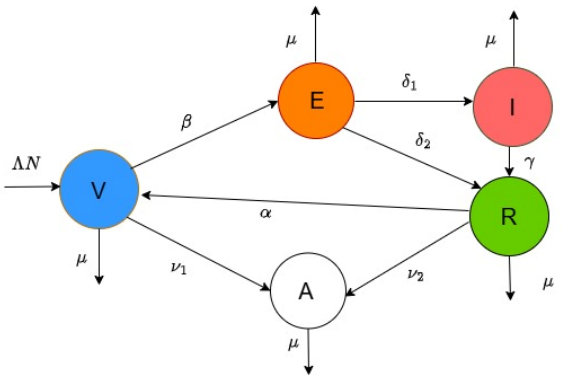
در مدل پیشنهادی گره‌های شبکه به پنج گروه آسیب‌پذیر (Vulnerable)، در معرض آلودگی(Exposed)، آلوده (Infected)، بهبودیافته (Recovered) و پادزهر (Antidotal) تقسیم شده‌اند. نمودار مربوط به گروه‌های مدل پیشنهادی در شکل (۲) آمده است. نمادهای به‌کار رفته در مدل نیز در جدول (۱) شرح داده شده‌اند.

گره آسیب‌پذیر زمانی‌که 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 بهبود یافته با نرخ α مجدد آسیب‌پذیر خواهند شد. با اعمال مکانیسم‌های امنیتی روی گره‌های بهبود یافته 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 درجه‌ی گره تعیین می‌شود. گره‌هایی که درجه‌ی بالاتری دارند نرخ واکسینه‌ی بیشتری خواهند داشت. باتوجه به اینکه در شبکه‌ای با N گره، درجه‌ی یک گره در بازه‌ی $[0..N]$ می‌تواند باشد، نرخ ν_1 برای گرهی با درجه‌ی k در بازه‌ی $[0..1]$ 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، رابطه‌ی (۱) بر اساس تغییر بازه‌ی k از $[0..N]$ به $[0..1]$ به دست آمده است. این رابطه نشان می‌دهد، هرچه درجه‌ی گره بیشتر باشد نرخ υ_1 نیز بیشتر خواهد بود و با کاهش درجه نرخ υ_1 نیز کمتر می‌شود. بنابراین υ_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.



شکل(۲): نمودار ارتباطات بین گروه‌های مدل پیشنهادی

جدول (۱): نمادهای به‌کار رفته در مدل به همراه توصیف آنها

نماد	توصیف نماد
ΛN	نرخ اضافه‌شدن گره‌های جدید به شبکه (گره‌ها در حالت آسیب‌پذیر قرار می‌گیرند.)
μ	نرخ خروج گره‌ها از شبکه (نرخ مرگ و میر).
β	نرخ انتشار بد افزار.
υ_1	نرخ واکسیناسیون گره‌های آسیب‌پذیر بر اساس اهمیت گره.
υ_2	نرخ واکسیناسیون یا اعمال پادزهر روی گره‌های بهبودیافته.
γ	نرخ بهبود از بدافزار.
δ_1	نرخ فعال شدن آلودگی در یک گره درمعرض آلودگی.
δ_2	نرخ بهبود گره بدون فعال شدن آلودگی.
α	نرخ انتقال گره‌های بهبود یافته به آسیب‌پذیر.
V^k	چگالی گره‌های آسیب‌پذیر با درجه‌ی k در شبکه
E^k	چگالی گره‌های در معرض آلودگی با درجه‌ی k در شبکه.
I^k	چگالی گره‌های آلوده با درجه‌ی k در شبکه.
R^k	چگالی گره‌های بهبودیافته از بدافزار با درجه‌ی k در شبکه .

A^k	چگالی گره‌های با درجه‌ی k در شبکه که پادزهر روی آنها اعمال شده است.
N	تعداد گره‌های شبکه.

با توجه به شرح مدل معادلات مدل به‌صورت زیر می‌باشند:

$$\begin{aligned}
\frac{dV^k(t)}{dt} &= \Lambda N - \beta V^k(t)\theta^k(t) - \mu V^k(t) \\
&\quad - \upsilon_1 V^k(t) + \alpha R^k(t) \\
\frac{dE^k(t)}{dt} &= \beta V^k(t)\theta^k(t) - (\mu + \delta_1 \\
&\quad + \delta_2)E^k(t) \\
\frac{dI^k(t)}{dt} &= \delta_1 E^k(t) - (\mu+\gamma)I^k(t) \\
\frac{dR^k(t)}{dt} &= \gamma I^k(t) - (\mu + \upsilon_2 + \alpha)R^k(t) \\
&\quad + \delta_2 E^k(t) \\
\frac{dA^k(t)}{dt} &= \upsilon_2 R^k(t) + \upsilon_1 V^k(t) - \mu A^k(t)
\end{aligned} \qquad (2)$$

در معادلات ذکر شده $\theta^k(\mathbf{t})$ احتمال آلوده بودن به بدافزار در گره همسایه با درجه k می‌باشد که می‌توان آن را به‌صورت معادله (۳) درنظر گرفت.

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

میانگین درجه‌ی شبکه نیز برابر است با $< K > = \sum_{j=1}^{n} j\,p(j)$

معمولا جهت ساده‌سازی روند کار شبیه‌سازی فرضیاتی برای شبیه‌سازی در نظر گرفته می‌شود . در این مقاله نیز فرضیات درنظر گرفته شده به شرح زیر می‌باشند.

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

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

۳- شبکه یک شبکه‌ی ناهمگن است.

۴- در ابتدای شبیه‌سازی۱۰ درصد گره‌ها آلوده به بدافزار هستند.

۲-۳. تحلیل دینامیک مدل

در تحلیل دینامیک مدل یکی از مواردی که انجام می‌شود، محاسبه‌ی مقدار عدد بازتولید اولیه یا R_0 است. این مقدار بیان‌کننده‌ی تعداد آلودگی‌های ثانویه‌ی ناشی از آلودگی اولیه در مدت زمان حیات بدافزار است [۲۱]. در حقیقت عدد باز تولید اولیه حد آستانه‌ی اپیدمی انتشار بدافزار در شبکه است که اگر مقدار آن کمتر از یک باشد همه‌گیری در شبکه وجود ندارد و بالعکس اگر مقدار آن از یک بیشتر باشد همه‌گیری انتشار بدافزار در شبکه وجود دارد. یکی از روشهای به‌دست آوردن مقدار R_0 روش تولید بعدی [۲۱] است. در این روش بردارهای f باتوجه به سرعت انتقال آلودگی و بردار v بر اساس نرخ انتقال آلودگی در گروه‌های آلوده به بدافزار به‌دست می‌آیند. در مدل پیشنهادی گروه‌هایی که در آنها آلودگی وجود دارد I و E هستند. در نتیجه بردارهای f و v به صورت زیر خواهند بود.

$$\mathrm{v}(x) = \begin{bmatrix} (\mu + \delta_1 + \delta_2)E^k(t) \\ (\mu+\gamma)I^k(t) - \delta_1 E^k(t) \end{bmatrix} \qquad (۴)$$

$$f(\mathrm{x}) = \begin{bmatrix} \beta\theta^k(\mathrm{t})\mathrm{V}(0) \\ 0 \end{bmatrix}$$

و در ادامه ماتریسهای F و V به‌صورت زیر محاسبه می‌شوند.

$$\mathrm{F} = \begin{bmatrix} \frac{\partial \mathrm{f}_1}{\partial \mathrm{E}} & \frac{\partial \mathrm{f}_1}{\partial \mathrm{I}} \\ \frac{\partial \mathrm{f}_2}{\partial \mathrm{E}} & \frac{\partial \mathrm{f}_2}{\partial \mathrm{I}} \end{bmatrix} = \begin{bmatrix} 0 & \beta\frac{< K^2 >}{< K >}\frac{\Lambda}{\mu} \\ 0 & 0 \end{bmatrix} \qquad (۵)$$

$$\mathrm{V} = \begin{bmatrix} \frac{\partial \mathrm{v}_1}{\partial \mathrm{E}} & \frac{\partial \mathrm{v}_1}{\partial \mathrm{I}} \\ \frac{\partial \mathrm{v}_2}{\partial \mathrm{E}} & \frac{\partial \mathrm{v}_2}{\partial \mathrm{I}} \end{bmatrix} = \begin{bmatrix} \mu + \delta_1 + \delta_2 & 0 \\ -\delta_1 & \mu + \gamma \end{bmatrix}$$

که $< K^2 > = \begin{bmatrix}1\\2\\\vdots\\\Delta\end{bmatrix}$ [p 2p ... Δp] و مقدار R_0 بر اساس رابطه $R_0 = \rho(FV^{-1})$ به‌دست می‌آید که ρ شعاع طیفی FV^{-1} یا بزرگترین مقدار ویژه‌ی ماتریس FV^{-1} است.

$$R_0 = \frac{\beta\delta_1}{(\gamma+\mu)(\mu+\delta_1+\delta_2)}\frac{< K^2 >}{< K >}\frac{\Lambda}{\mu} \qquad (۶)$$

با توجه به رابطه‌ی به‌دست آمده برای R_0 مشخص است که نرخ آلودگی و نرخ فعال شدن آلودگی با R_0 رابطه‌ی مستقیم و نرخ‌های بهبود δ_2 و γ با آن رابطه‌ی 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.

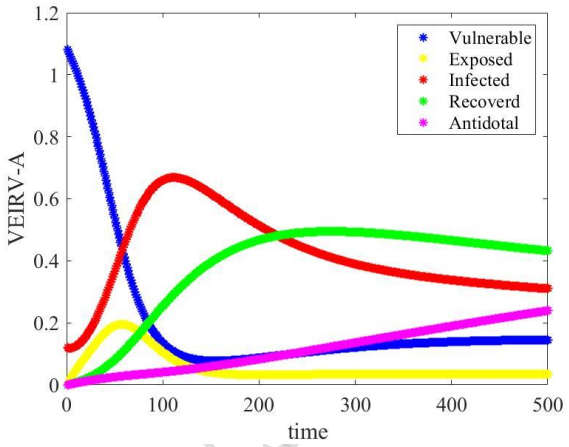
۴- نتایج شبیه‌سازی مدل

مدل پیشنهادی بر روی مجموعه داده‌ی استاندارد socfb-Amherst41 با ۲۲۳۵ گره و ۹۰۹۵۴ یال در محیط متلب شبیه‌سازی شده است و نتایج شبیه‌سازی در این بخش آمده است. شکل (۳) نمودار گروه‌های مختلف مدل VEIRV-A را به‌ازای مقادیر پارامترهای جدول (۲) روی مجموعه داده‌ی استاندارد در مدت زمان شبیه‌سازی (T) ۵۰۰ نشان می‌دهد. برآورد پارامترهای مدل در مدل‌سازی بسیار مهم است. با این حال، تخمین پارامتر یک مشکل چالش برانگیز است که می‌تواند زمان‌بر و گران باشد، به خصوص زمانی که پارامترهای تخمینی متعددی وجود داشته باشند. روش‌های مختلفی برای تخمین این پارامترها وجود دارد. یکی از روش‌های مؤثر، 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 [۲۲].

جدول (۲): مقدار عددی پارامترهای مدل در شبیه‌سازی روی مجموعه داده‌ی استاندارد socfb-Amherst41

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

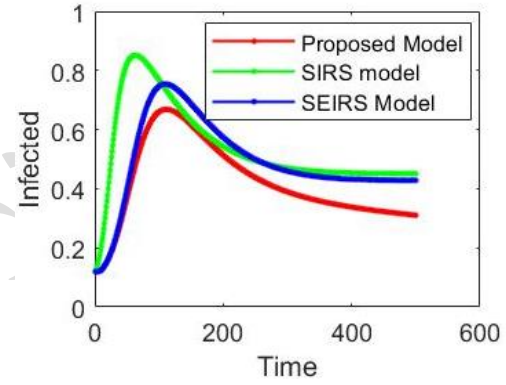
در ابتدای شبیه سازی از جمعیت آسیب‌پذیرها کم شده به گروه‌های درمعرض آلودگی و آلوده اضافه می‌شود و با گذشت زمان، چگالی گره‌های آلوده کاهش و چگالی گره‌های بهبود یافته افزایش می‌یابد. پس از ورود گره‌ها به گروه بهبود یافته با نرخ $\nu_2 = 0.001$ از چگالی گره‌های بهبود یافته کاسته شده و به چگالی گره‌های تحت تأثیر پادزهر اضافه می‌شود.



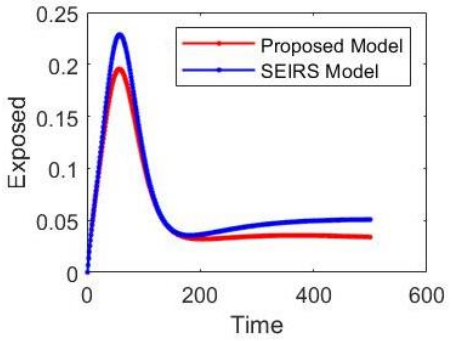
شکل(۳): گروه‌های V، E ، I ، R ، A و D در مدل پیشنهادی روی مجموعه داده‌ی استاندارد socfb-Amherst41

شکل (۴) گروه آلوده را در سه مدل SIRS ، SEIRS و مدل پیشنهادی VEIRV-A مقایسه می‌کند. همان‌طور که نتایج شبیه‌سازی شکل(۴) 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 درجه‌ی آنها از انتشار آلودگی در شبکه جلوگیری شده و سرعت انتشار نیز کاهش یافته است. روش پیشنهادی موجب شده است که چگالی آلوده‌های

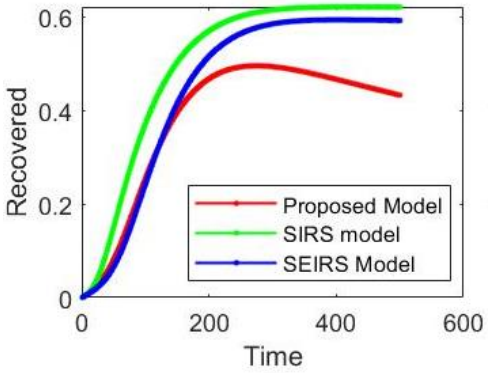
غیرفعال نیز کمتر شود. کاهش انتشار گروه در معرض آلودگی در مدل VEIRV-A نسبت به مدل SEIRS در شکل(۵) به وضوح مشخص است. شکل (۶) نیز به بررسی تغییرات گروه بهبودیافته‌ها در سه مدل می‌پردازد. در مدل پیشنهادی نرخ واکسیناسیون گره‌های آسیب‌پذیر بر اساس درجه تعیین شده و گره‌هایی که درجه‌ی بالاتری داشتند نرخ واکسیناسیون 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 (۶) این کاهش به وضوح دیده می‌شود.



شکل(۴): مقایسه‌ی گروه آلوده‌ها در سه مدل پیشنهادی و مدل‌های SIRS و SEIRS بر روی مجموعه داده‌ی استاندارد socfb-Amherst41



شکل(۵): مقایسه‌ی گروه در معرض آلودگی در دو مدل پیشنهادی و SEIRS بر روی مجموعه داده‌ی استاندارد socfb-Amherst41

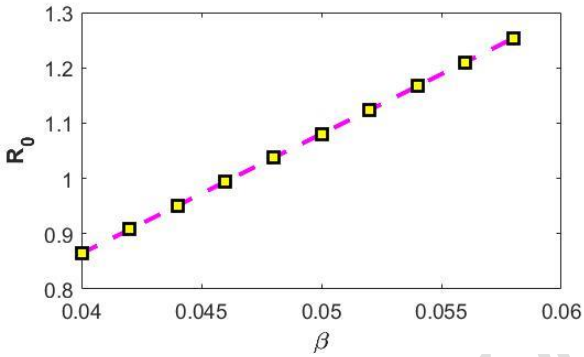


شکل (۶): مقایسه‌ی گروه بهبود یافته‌ها در سه مدل پیشنهادی و مدل‌های SIRS و SEIRS بر روی مجموعه داده‌ی استاندارد socfb-Amherst41

با توجه به رابطه‌ی (۶) برای R_0 پارامترهای β و δ_1 با R_0 رابطه‌ی مستقیم دارند و با افزایش آنها R_0 نیز افزایش می‌یابد که شکل‌های (۷) و (۸) تأییدی بر این رابطه هستند. از طرف دیگر رابطه‌ی معکوس R_0 با δ_2 و γ نیز در شکل‌های (۹) و (۱۰) نشان داده شده است. در جدول (۳) مقادیرعدد بازتولید اولیه (R_0) به ازای افزایش نرخ آلودگی (β) در بازه‌ی $[0.04,0.058]$ 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 رابطه‌ی ۶ مطابقت دارد. شکل (۷) نیز این نتایج را به صورت نمودار تحلیل کرده است. جدول (۴) نیز مقادیر R_0 را با افزایش مقدار نرخ فعال شدن آلودگی گره‌های در معرض آلودگی (δ_1) در بازه‌ی $[0.12,0.138]$ نشان می‌دهد. شکل (۸) 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 رابطه‌ی (۶) مطابقت دارد.

جدول(۳). مقادیر R_0 به ازای مقادیر مختلف β

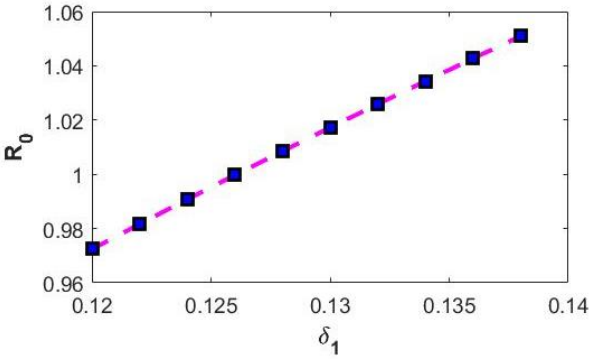
β	**0.040**	**0.042**	**0.044**	**0.046**	**0.048**
R_0	0.8644	0.9076	0.9508	0.9940	1.0372
β	**0.050**	**0.052**	**0.054**	**0.056**	**0.058**
R_0	1.0805	1.1237	1.1669	1.2101	1.2533



شکل(۷): روند تغییرات R_0 با تغییر β

جدول(۴). مقادیر R_0 به ازای مقادیر مختلف δ_1

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

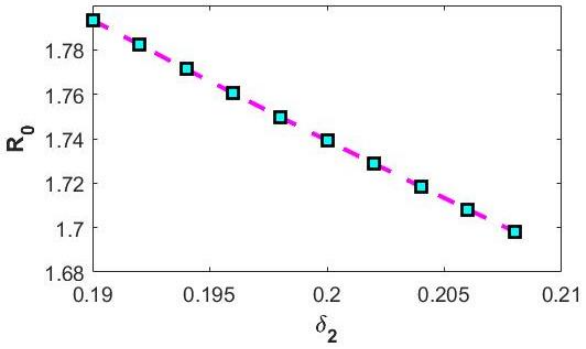


شکل(۸): روند تغییرات R_0 با تغییر δ_1

جدول (۵) نیز همان‌طور که در رابطه‌ی (۶) آمده است، روند کاهشی مقادیر R_0 را با افزایش نرخ بهبود گروه در معرض آلودگی (δ_2) در بازه‌ی $[0.19,0.208]$ 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 (۹) نتایج این تغییرات به صورت تصویری نشان داده شده است. نتایج به دست آمده در جدول (۶) و معادل تصویری آن در شکل (۱۰) بیانگر کاهش مقدار R_0 به‌ازای 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(۵). مقادیر R_0 به ازای مقادیر مختلف δ_2

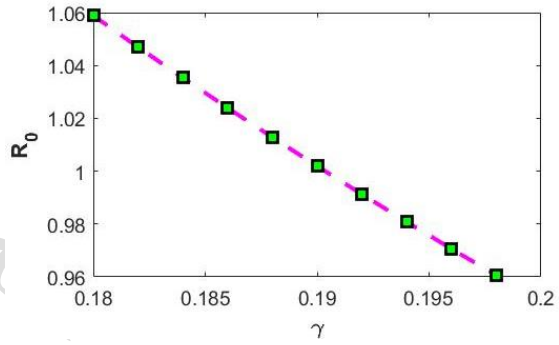
δ_2	**0.190**	**0.192**	**0.194**	**0.196**	**0.198**
R_0	1.7934	1.7823	1.7713	1.7605	1.7498
δ_2	**0.200**	**0.202**	**0.204**	**0.206**	**0.208**
R_0	1.7392	1.7288	1.7184	1.7082	1.6982



شکل(۹): روند تغییرات R_0 با تغییر δ_2

جدول(۶). مقادیر R_0 به ازای مقادیر مختلف γ

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(۱۰): روند تغییرات R_0 با تغییر γ

۵- نتیجه‌گیری

در این مقاله مدل $VEIRV-A$ بر اساس مدل‌سازی بیماری‌های همه‌گیری با در نظر گرفتن گروه پادزهر در شبکه‌ی اینترنت اشیاء ارائه شده است. در این مدل برای نرخ ورود گره‌های آسیب‌پذیر به گروه پادزهر بر اساس درجه‌ی گره یک میزان اهمیت تعیین می‌شود. گره‌های با اهمیت بیشتر شانس بیشتری برای واکسینه شدن دارند. بنابراین تأثیر پادزهر در شبکه بیشتر شده است. مدل پیشنهادی بر روی مجموعه داده‌ی 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 رابطه‌ی مستقیم دارند و پارمترهای γ و δ_2 رابطه‌ی عکس دارند که در نتایج شبیه‌سازی نیز این به‌وضوح مشاهده شده است. زمانی‌که مقدار R_0 کمتر از یک است انتشار بدافزار در شبکه متوقف شده است و همه‌گیری انتشاربدافزار 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 دربر داشته است. در کارهای آینده به بررسی چندین نوع آلودگی در شبکه‌های ناهمگن و همچنین تاثیر خوشه‌بندی در انتشار بدافزار خواهیم پرداخت.

مراجع

1. F. Sadoughi, A. Behmanesh, and N. Sayfouri, “Internet of things in medicine: A systematic mapping study,” *Journal of biomedical informatics,* vol. 103, pp. 103383, 2020. https://doi.org/10.1016/j.jbi.2020.103383.

2. C. Sobin, “A survey on architecture, protocols and challenges in IoT,” *Wireless Personal Communications,* vol. 112, no. 3, pp. 1383-1429, 2020. https://doi.org/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 of Things Journal,* vol. 7, no. 9, pp. 8036-8048, 2020. https://doi.org/10.1109/JIOT.2020.2990365.

4. J M. Javaid, and I. H. Khan, “Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic,” *Journal of oral biology and craniofacial research,* vol. 11, no. 2, pp. 209-214, 2021. https://doi.org/10.1016/j.jobcr.2021.01.015.

5. B. Ramphull, and S. D. Nagowah, “A Knowledge Model for IoT-Enabled Smart Banking,” *Journal of the Knowledge Economy,* vol. 15, no. 2, pp. 9174-9206, 2024. https://doi.org/10.1007/s13132-023-01434-2.

6. Moazzami, M., et al. *Internet of things architecture for intelligent transportation systems in a smart city*. in *2021 3rd Global Power, Energy and Communication Conference (GPECOM)*. 2021. IEEE, https://doi.org/10.1109/GPECOM52585.2021.9587692

7. J. Fan, Y. Zhang, W. Wen, S. Gu, X. Lu, and X. Guo, “The future of Internet of Things in agriculture: Plant high-throughput phenotypic platform,” *Journal of Cleaner Production,* vol. 280, pp. 123651, 2021.https://doi.org/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 Communications Surveys & Tutorials,* vol. 22, no. 2, pp. 1191-1221, 2020. https://doi.org/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. https://doi.org/10.1109/ACCESS.2020.2984668.

10. Akrami. A, Parsamanesh.M, "Investigation of a mathematical fuzzy epidemic model for the spread of coronavirus in a population", Soft Computing Journal, vol. 11, no.1- 21, pp. 2-9, 2022 . https://doi.org/10.22052/SCJ.2022.246053.1045.

11. Yadollahi. A, Sabaghian-Bidgoli. H, "A simulation model for the propagation of Covid-19 virus based on the discrete-time Markov chain", Soft Computing Journal, vol. 11, no.2- 22, pp. 88-103,

19. R. Casado-Vara, M. Severt, A. Díaz-Longueira, Á. M. d. Rey, and J. L. Calvo-Rolle, "Dynamic Malware Mitigation Strategies for IoT Networks: A Mathematical Epidemiology Approach," *Mathematics,* vol. 12, no. 2, pp. 250, 2024. https://doi.org/10.3390/math12020250.

20. Yadav, P. and A.K. Keshri. *The Dynamics of SEIQR-V Malware Propagation Model in IoT Networks*. in *2022 International Conference on IoT and Blockchain Technology (ICIBT)*. 2022. IEEE, https://doi.org/ 10.1109/ICIBT52874.2022.9807775 .

21. Z. Yu, H. Gao, D. Wang, A. A. Alnuaim, M. Firdausi, and A. M. Mostafa, "SEI2RS malware propagation model considering two infection rates in cyber–physical systems," *Physica A: Statistical Mechanics and its Applications,* vol. 597, pp. 127207, 2022.
https://doi.org/10.1016/j.physa.2022.127207.

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

2023,
https://doi.org/10.22052/SCJ.2023.246527.1076.

12. 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,* vol. 115, no. 772, pp. 700-721, 1927.

https://doi.org/10.1098/rspa.1927.0118.

13. Zhu, X., et al. *Modeling and Analysis of Malware Propagation for Cluster-based Wireless Sensor Networks*. in *2020 IEEE 6th International Conference on Dependability in Sensor, Cloud and Big Data Systems and Application (DependSys)*. 2020. IEEE. https://doi.org/ 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 of Things Journal,* vol. 7, no. 8, pp. 7470-7481, 2020. https://doi.org/ 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," *Journal of the Franklin Institute,* vol. 357, no. 7, pp. 4414-4436, 2020. https://doi.org/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.
https://doi.org/ 10.1109/ACCESS.2022.3213032.

17. S. Shen, H. Zhou, S. Feng, L. Huang, J. Liu, S. Yu, and Q. Cao, "HSIRD: A model for characterizing dynamics of malware diffusion in heterogeneous WSNs," *Journal of Network and Computer Applications,* vol. 146, pp. 102420, 2019. https://doi.org/10.1016/j.jnca.2019.102420.

18. Kalam, S. and A.K. Keshri. *Epidemic model on Denial of Service attack in IoT network*. in *2022 International Conference on IoT and Blockchain Technology (ICIBT)*. 2022. IEEE, https://doi.org/ 10.1109/ICIBT52874.2022.9807815 .