
بسم الله الرحمن الرحيم

دانشکده علوم پایه
گروه ریاضی

پایان‌نامه

برای دریافت درجه کارشناسی ارشد در رشته
ریاضی کاربردی، گرایش آنالیز عددی

عنوان

پیش‌بینی انتشار بدافزار در یک شبکه رایانه‌ای با کمک روش‌های عددی

استاد راهنما

دکتر زهره دادی

استاد مشاور

دکتر حمیده نسب‌زاده

نگارنده

بنت‌الهدی ولی‌پور

شهریور ۱۴۰۱

باسمه تعالی

مشخصات پایان‌نامه تحصیلی دانشجویان

دانشگاه بجنورد

نام خانوادگی دانشجو: ولی‌پور نام: بنت‌الهدی

عنوان پایان‌نامه: پیش‌بینی انتشار بدافزار در یک شبکه رایانه‌ای با کمک روش‌های عددی

استاد راهنما: دکتر زهره دادی

استاد مشاور: دکتر حمیده نسب‌زاده

مقطع تحصیلی: کارشناسی ارشد رشته: ریاضی کاربردی گرایش: آنالیز عددی

دانشگاه: بجنورد دانشکده علوم پایه

تاریخ فارغ‌التحصیلی: شهریور ۱۴۰۱ تعداد صفحات: ۷۰

واژگان کلیدی: بدافزار، مدل انتشار، شبکه رایانه‌ای، روش‌های عددی.

چکیده

در این پایان‌نامه، ابتدا دینامیک نقاط تعادل یک مدل انتشار بدافزار در شبکه رایانه‌ای بر اساس گره‌های هدفمند و حمله‌کننده را با روش ژاکوبی و کدنویسی در نرم‌افزار متمتیکا مورد مطالعه قرار دادیم. سپس با پیاده‌سازی تقریب پده برای محاسبه جواب تقریبی تحلیلی یک مدل انتشار بدافزار پرداختیم و نمودارهای جواب دستگاه را بر اساس ضرایب بهینه به دست آمده در این روش را ارائه کردیم.

اصالت و مالکیت پایان‌نامه

اینجانب بنت‌الهدی ولی‌پور دانش‌آموخته کارشناسی‌ارشد رشته ریاضی کاربردی، گرایش آنالیز عددی دانشکده علوم پایه دانشگاه بجنورد پدیدآور پایان‌نامه با عنوان "دینامیک پیش‌بینی انتشار بدافزار در یک شبکه رایانه‌ای با کمک روش‌های عددی" با راهنمایی دکتر زهره دادی گواهی و تعهد می‌کنم که بر پایه قوانین و مقررات، از جمله «دستورالعمل نحوه بررسی تخلفات پژوهشی» و همچنین «مصادیق تخلفات پژوهشی» مصوب وزارت علوم، تحقیقات و فناوری (۲۵ اسفند ۱۳۹۳):

□ این پایان‌نامه دستاورد پژوهش اینجانب و محتوای آن از درستی و اصالت برخوردار است؛

□ حقوق معنوی همه کسانی را که در به دست آمدن نتایج اصلی پایان‌نامه تأثیرگذار بوده‌اند، رعایت کرده‌ام و هنگام کاربرد دستاورد پژوهشهای دیگران در آن، با دقت و به درستی به آنها استناد کرده‌ام؛

□ این پایان‌نامه و محتوای آن را تاکنون اینجانب یا کس دیگری برای دریافت هیچگونه مدرک یا امتیازی در هیچ جا ارائه نکرده‌ایم؛

□ همه حقوق مادی این پایان‌نامه از آن دانشگاه بجنورد است و آثار برگرفته از آن با وابستگی سازمانی دانشگاه بجنورد منتشر خواهد شد؛

□ در همه آثار برگرفته از این پایان‌نامه، نام استاد(ان) راهنما و اگر استاد راهنمای نخست تشخیص دهد، نام استاد(ان) مشاور و نشانی رایانامه سازمانی آنان را می‌آورم؛

□ در همه گام‌های انجام این پایان‌نامه، هرگاه به اطلاعات شخصی افراد یا اطلاعات سازمانها دسترسی داشته یا آن‌ها را به کار برده‌ام، رازداری و اخلاق پژوهش را رعایت کرده‌ام.

تاریخ امضا

حقوق دانشگاه بجنورد

تقدیم به

همسر عزیزم و

پسر گلم

سپاس‌گزاری...

پروردگارم! چگونه سپاست گویم که چرخش زبان به سپاس، خود نیازمند سپاسی دیگر است.

ضمن سپاس و ستایش به درگاه ایزد منان که به من توانایی داد که با استعانت از او بتوانم این پژوهش را انجام دهم، وظیفه خود می‌دانم از راهنمایی‌ها و زحمات بی‌دریغ سرکار خانم دکتر زهره دادی در به ثمر رسیدن این پایان‌نامه تشکر و قدردانی نمایم.
همچنین از سرکار خانم دکتر حمیده نسب‌زاده که زحمت مطالعه و مشاوره این پایان‌نامه را تقبل نمودند، کمال امتنان را دارم.

خدایا چنان کن سرانجام کار تو خشنود باشی و ما رستگار

بنت الهدی ولی‌پور
شهریور ۱۴۰۱

فهرست مطالب

فهرست اختصارات

گره‌های هدفمند مستعد یا آسیب‌پذیر ..... S_t
گره‌های هدفمند آلوده ..... I_t
گره‌های هدفمند بازیابی‌شده ..... R_t
گره‌های حمله‌کننده آسیب‌پذیر ..... S_a
گره‌های حمله‌کننده آلوده ..... I_a
گره‌های حمله‌کننده خارجی ..... E_a
نرخ تماس با آلودگی ..... β
نرخ بازیابی گره‌های هدفمند آلوده ..... γ
نرخ آسیب‌پذیری گره‌های هدفمند بازیابی‌شده ..... ε_t
نرخ آسیب‌پذیری گره‌های حمله‌کننده غیر آلوده ..... ε_a
نرخی که گره‌های حمله‌کننده خارجی به اینترنت متصل می‌شوند تا به گره‌های حمله‌کننده آسیب‌پذیر تبدیل شوند ..... σ
نرخ مرگ و میر و تولد گره‌های حمله‌کننده ..... μ
عدد تکثیر پایه ..... R_0
عدد تکثیر پایه برای جمعیت حمله‌کننده ..... R_{0a}
عدد تکثیر پایه برای جمعیت هدف ..... R_{0t}

فهرست شکل‌ها

فهرست جدول‌ها

مقدمه

در سال‌های اخیر مدل‌های انتشار که مبتنی بر مدل‌های اپیدمی بیولوژیکی می‌باشد در مدل‌سازی پدیده‌های متعددی مورد استفاده قرار گرفته است. یکی از پدیده‌ها حمله بدافزارها در شبکه رایانه‌ای است که به کمک مدل‌های دینامیکی انتشار به تجزیه و تحلیل این نوع از حمله‌ها و انتخاب مکانیسم دفاعی مناسب می‌توان پرداخت.

روش‌های متعددی برای مدل‌سازی این پدیده تاکنون استفاده شده است. یکی از روش‌های مرسوم استفاده از دستگاه‌های دیفرانسیل معمولی است که توسط محققین متعددی تاکنون به کار گرفته شده است.

محققین زیادی مانند علی و همکارانش [۱] در سال ۲۰۱۸، میشرا و همکارانش [۲] در سال ۲۰۱۹ و همچنین در سال‌های پیش از آن، مدل‌های غیر خطی انتشار ویروس را ارائه و تعمیم دادند. به طور نمونه میشرا و همکارانش در سال ۲۰۱۹ یک مدل بر اساس مدل‌سازی ریاضی در خصوص حمله‌های بدافزاری در حوزه اینترنت اشیا را ارائه نمودند و به تحلیل دینامیکی این مدل پرداختند. یکی دیگر از روش‌های مورد استفاده در مطالعه عددی مدل‌های انتشار بدافزاری در شبکه‌های رایانه‌ای استفاده از روش‌های عددی EP [۳] و NSFD [۴] است که علی و همکارانش در سال ۲۰۱۸ این روش‌ها را با پیاده‌سازی به روی یک مدل انتشار ویروس با یکدیگر مقایسه کردند. با توجه به عدم مطالعه مدل میشرا در سال ۲۰۱۹ با روش‌های عددی دیگر کامل‌تر دینامیک آن مدل از نظر

[۱] Ali and et al.
[۲] Mishra and et al.
[۳] Evolutionary Pade (EP)
[۴] Non Standard Finite Difference (NSFD)

عددی مورد توجه قرار گرفته است.

در این پژوهش در فصل اول، به ارائه پیشینه‌ای از اینترنت اشیا و مفاهیم مرتبط با آن می‌پردازیم. سپس در فصل دوم روش‌های ریاضی به کار گرفته شده در تحلیل مدل مورد نظر را توضیح خواهیم داد. سپس در فصل سوم مدل مورد مطالعه معرفی و دینامیک آن تحلیل می‌شود. سرانجام در فصل چهارم به حل مدل با استفاده از نرم‌افزار متمتیکا و به کارگیری روش تقریب پده می‌پردازیم.

فصل ۱
مفاهیم شبکه‌های رایانه‌ای

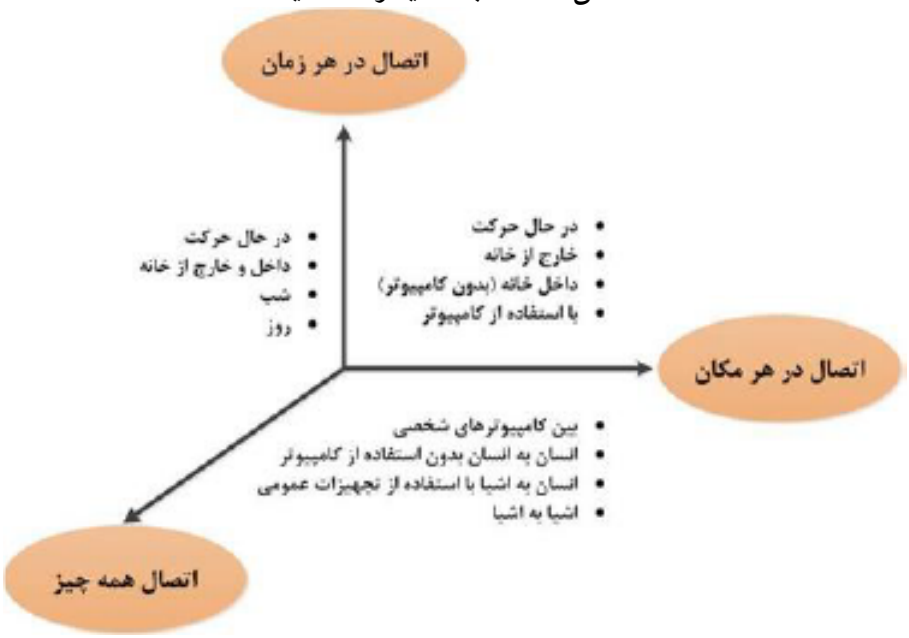
۱.۱ اینترنت اشیا

اینترنت اشیا (IoT)[۱] مفهومی جدید در دنیای فناوری و ارتباطات است که در آن برای هر موجودی (انسان، حیوان و یا شیء) قابلیت ارسال داده از طریق شبکه‌های ارتباطی، اعم از اینترنت یا اینترانت فراهم می‌گردد [۷].

شکل ۱.۱ ابعاد مختلف اینترنت اشیا را نشان می‌دهد. همه چیز باید بتوانند در هر لحظه از زمان و در هر نقطه از مکان به همدیگر مرتبط شوند. ارتباط رایانه‌های شخصی با همدیگر، تبادل اطلاعات انسان‌ها با یکدیگر، انسان‌ها با اشیا و خود اشیا با هم، بایستی در هر زمان از شبانه‌روز و در هر حالت و موقعیتی چه ثابت و چه در حال حرکت، (چه در خانه و اداره و محل کسب و کار و چه در زمان سفر و داخل قطار، اتوبوس شهری و هواپیما) امکان‌پذیر باشد. در واقع، برای برقراری ارتباط با شبکه، مهم نخواهد بود که آیا شیء متصل به اینترنت جاندار است و یا بی‌جان، ثابت است و یا متحرک، شب است و یا روز. هیچ محدودیتی و قید و بندی در برقراری ارتباط با شبکه گسترده و فراگیر اینترنت اشیا وجود نخواهد داشت.

[۱] Internet of Things (IoT)

شکل ۱.۱: ابعاد اینترنت اشیا.



تعریف ۱.۱.۱ (DoS). نوعی تهاجم رایانه‌ای، معمولاً برنامه‌ریزی شده، که هدف آن مختل کردن دستیابی به وب است. این تهاجمات به چندین شکل متصور هستند. متداول‌ترین شکل، ارسال درخواست‌های اتصال بسیار زیاد به یک سرویس‌دهنده اینترنت که قابل پاسخگویی نمی‌باشند. این امر سبب می‌شود تا سرویس‌دهنده آن‌قدر مشغول پاسخگویی به این درخواست‌ها گردد که درخواست‌های صحیح را نادیده می‌انگارد. مثالی از این نمونه تهاجمات، سیل SYN نام دارد که پورت‌های ورودی سرویس‌دهنده را با پیام‌های اتصال نادرست اشباع می‌کند. شکل دیگری از این تهاجمات که پینگ مرگ (PoD)[۲] نام دارد، فرمان پینگ را با بسته IP بسیار بزرگ ارسال می‌کند تا سرویس‌دهنده متوقف و یا دوباره راه‌اندازی شود. شکل دیگر این حملات، شامل تخریب یا تغییر در اطلاعات پیکربندی یک مثلاً اطلاعات مسیریابی می‌باشد. دستیابی غیرمجاز به اجزا فیزیکی یک سیستم و ارسال داده‌های نامعتبر و یا بسیار حجیم به منظور متوقف کردن یک سیستم، از دیگر اشکال این تهاجم هستند [۳].

[۲] Ping of Death (PoD)

تعریف ۲.۱.۱ (حمله انکار سرویس توزیع‌شده (DDoS)[۳]). شکلی از DoS[۴] که منشأ آن رایانه‌هایی است که هدفشان ایجاد اختلال در دستیابی به وب از طریق ارسال درخواست‌های اتصال بی‌شماری است که قابل انجام نمی‌باشند. هر تهاجم DDoS به گونه‌ای است که به تعدادی رایانه حمله می‌شود، برنامه‌هایی که در آن‌ها قرار می‌گیرند و آن‌قدر آن‌جا باقی می‌مانند تا سیگنالی به آن‌ها ارسال شود. وقتی سیگنال ارسال می‌شود، این رایانه‌ها جریان پیوسته‌ای از بسته‌های داده‌ای را به سایت وب مورد نظر آن‌قدر ارسال می‌کنند تا سرویس‌دهنده وب قادر به پاسخگویی نباشد. چون تهاجم از جانب چند رایانه صورت می‌گیرد، ویژگی‌های امنیتی که در شرایط عادی قادر به تشخیص و متوقف کردن روند پذیرش بسته‌های داده‌ای از یک منبع هستند، توانایی قطع تمام اتصالات مربوط به مهاجم‌ها را نخواهد داشت [۳].

تعریف ۳.۱.۱ (حمله نیمه باز[۵]). حمله نیمه باز، نوعی حمله DDoS است که هدف آن، از دسترس خارج ساختن سرور برای ترافیک قانونی، با مصرف تمامی منابع در دسترس سرور می‌باشد. یک مهاجم با ارسال درخواست‌های مکرر (SYN) قادر است تمامی پورت‌های روی سرور را مورد هدف قراردهد و باعث شود دستگاه مورد نظر قادر به پاسخگویی به ترافیک قانونی نباشد و یا بسیار کند پاسخ دهد.

با مصرف کردن تمام منابع سرور، این نوع حملات می‌توانند حتی سرورهای با ظرفیت بالا که قادر به پردازش میلیون‌ها ارتباط مختلف هستند را نیز از کار بیندازند [۷].

تعریف ۴.۱.۱ (پینگ مرگ (PoD)). نوعی حمله DoS است که در آن یک مهاجم با ارسال بسته‌های ناقص شکل یا بزرگ با استفاده از یک دستور Ping ساده سعی در خرابی، بی‌ثبات‌سازی یا مسدود کردن رایانه یا سرویس مورد نظر را دارد [۳].

[۳] Distributed Denial of Service Attack (DDoS)
[۴] Denial of Service Attack
[۵] SYN Flood

تعریف ۵.۱.۱ (پروتکل ارتباطی کاربر (UDP)[۶]). پروتکل بدون اتصالی در TCP/IP که با لایه transport مدل مرجع ISO/OSI متناظر است. UDP پیام‌های یک برنامه کاربردی را به بسته‌های قابل ارسال از طریق IP تبدیل می‌کند، اما چندان قابل اطمینان نیست، چرا که پیش از انتقال مسیر بین فرستنده و گیرنده را تعیین نمی‌کند و درستی تحویل پیام‌ها را نیز بررسی نمی‌کند. UDP از TCP کارآمدتر است، بنابراین برای مقاصد گوناگونی از جمله SNMP مورد استفاده قرار می‌گیرد؛ قابلیت اطمینان آن به برنامه کاربردی بستگی دارد که پیام را تولید می‌کند [۳].

تعریف ۶.۱.۱ (Zombie). رایانه‌ای که ناخواسته به میزبان یک برنامه مهاجم DDoS مبدل می‌شود و با سیگنال‌های راه دور مهاجم کنترل می‌گردد. کاوشگرها برای ایجاد یک zombie از ضعف‌های امنیتی برای وارد شدن به سرویس‌دهنده وب، پُست الکترونیکی یا برنامه کاربردی استفاده می‌کنند و ابزارهای DDoS پنهانی چون Trinoo و Tribal Flood Network را در آن‌ها قرار می‌دهند. این سرویس‌دهنده‌ها سپس با دریافت یک سیگنال از مهاجم به یک zombie مبدل می‌شوند و در تهاجم هماهنگ به سرویس‌دهنده‌های دیگر، شرکت می‌کنند [۳].

فناوری RFID

شناسایی خودکار و نگهداری داده‌ها (AIDC)[۷] روشی است که طی آن تجهیزات سخت‌افزاری یا نرم‌افزاری قادر به خواندن و تشخیص داده‌ها بدون کمک گرفتن از یک فرد هستند. فرض کنید در یک فروشگاه چندین قلم جنس خریداری کردید و در هنگام خروج، صندوق‌دار بارکد اجناس خریداری شده را تک تک قرائت نموده و در نهایت قبض خرید را صادر می‌کند. وقت شما علاوه بر صف مشتری‌ها در زمان قرائت نیز گرفته خواهد شد، همچنین اگر بارکد جنسی هم معیوب باشد، مشکل مضاعف می‌گردد. اما اگر به جای بارکد، از فناوری شناسایی مبتنی بر فرکانس رادیویی

[۶] User Datagram Protocol (UDP)
[۷] Automatic Identification and Data Capture (AIDC)

(RFID)[۸] استفاده گردد، مشکل حل خواهد شد و نیازی به صرف وقت زیادی برای فرآیند خرید به شرح مذکور نیست. هر کالا دارای برچسب الکترونیکی خواهد بود که موقع خروج از فروشگاه با فرستادن سیگنال‌های رادیویی همه مشخصات خود را به رایانه موجود در درب خروجی فروشگاه اعلام می‌کند و شما بدون صرف وقت و فقط با پرداخت هزینه، خرید خود را انجام می‌دهید.

در این روش، روی هر کالا و یا شیءای که قصد شناسایی و یا رصد آن وجود دارد، برچسب ویژه‌ای به نام تگ چسبانده می‌شود. این برچسب دارای دو جزء تراشه و آنتن است. تراشه، اطلاعات را از طریق آنتن ساطع می‌کند و آن‌گاه حسگرهای حساس موجود در محیط با دریافت سیگنال نسبت به شناسایی و یا رصد کالا و یا شیء اقدام می‌کنند. در حالت کلی یک سیستم RFID دارای بخش‌های زیر است:

۱ـ برچسب

۲ـ خوانشگر برچسب

۳ـ نویسنده اطلاعات

۴ـ آنتن و تقویت‌کننده سیگنال (در صورت لزوم)

۵ـ نرم‌افزار مدیریت اطلاعات

۶ـ بانک اطلاعاتی، ساختار شبکه اطلاعاتی [۷].

فناوری‌های بی‌سیم

از فناوری‌های بی‌سیم، امروزه همه به نوعی استفاده می‌شود. از موبایل‌ها تا شبکه‌های تلویزیونی و ادواتی که به صورت بی‌سیم کار می‌کنند، همگی از فناوری بی‌سیم بهره می‌گیرند. به طور کلی در شبکه‌های بی‌سیم، ارتباطات از طریق زنجیره امواج الکترومغناطیسی بوده که حاصل داده‌هایی است که در ارتباطات صوتی و تصویری با طول موج‌های مختلف صورت می‌گیرد.

[۸] Radio Frequency Identification (RFID)

در حالت کلی امواج به دو دسته تقسیم‌بندی می‌شوند:

۱ـ امواج مادون قرمز [۹]

۲ـ امواج رادیویی RF [۷].

۲.۱ امنیت در اینترنت اشیا

اینترنت اشیا از حسگرها و محرک‌ها استفاده می‌کند و آن‌ها حجم زیادی از داده‌ها را در مورد دما، رطوبت و نور برای بهینه کردن مصرف انرژی جمع‌آوری می‌کنند و از خطای عملیاتی که تأثیر واقعی بر محیط دارد، دوری می‌کنند. این مدل باید داده حسگر با نرخ بالا را در خود جای دهد تا اطلاعات را جذب و تحلیل نماید. در این پایگاه داده مفهومی، عملکرد خواندن و نوشتن بسیار مهم است، به ویژه وقتی نرخ داده بالا باشد. این پایگاه داده باید خواندن و نوشتن‌های با سرعت بالا را پشتیبانی کند و به طور مداوم در دسترس باشد تا این اطلاعات را در دوره‌های یکنواخت جمع‌آوری کند و مقیاس‌پذیر باشد تا کارایی هزینه را برای ذخیره داده‌ها در زمان حفظ نماید. سرویس‌ها و کاربردهای مقیاس بزرگ بر اساس اینترنت، به طور مستمر توسط اغتشاشات، حمله یا دزدی اطلاعات تهدید می‌شوند. در این بخش بهتر است مروری بر انواع حملات در حوزه فناوری اطلاعات داشته باشیم. حملات امنیتی ذاتاً به دو دسته فعال و غیر فعال تقسیم می‌گردند [۷].

۱.۲.۱ حملات غیرفعال

در این قبیل حملات، نفوذگر تنها به منبعی از اطلاعات به نحوی دست می‌یابد ولی اقدام به تغییر محتوای اطلاعات منبع نمی‌کند. این نوع حمله می‌تواند تنها به یکی از اشکال شنود ساده و یا آنالیز ترافیک باشد. اما منظور از شنود و آنالیز ترافیک چیست؟

[۹] Infrared

شنود: در این نوع حمله، نفوذگر تنها به پایش اطلاعات رد و بدل شده می‌پردازد. برای مثال، شنود ترافیک روی یک شبکه محلی یا یک شبکه بی‌سیم (که مدنظر ما است) نمونه‌هایی از این نوع حمله به شمار می‌آیند.

آنالیز ترافیک: در این نوع حمله، نفوذگر با کپی برداشتن از اطلاعات پایش شده، به تحلیل جمعی داده‌ها می‌پردازد. به عبارت دیگر بسته یا بسته‌های اطلاعاتی به همراه یکدیگر اطلاعات معناداری را ایجاد می‌کنند [۷].

۲.۲.۱ حملات فعال

در این نوع حملات، برخلاف حملات غیرفعال، نفوذگر اطلاعات مورد نظر را که از منابع به دست می‌آید، تغییر می‌دهد که تبعاً انجام این تغییرات مجاز نیست. از آن‌جایی که در این نوع حملات، اطلاعات تغییر می‌کنند، شناسایی رخداد حملات فرآیندی امکان‌پذیر است. درتقسیم بندی حملات دوموردزیرموردتوجه است.

تغییر هویت: در این نوع حمله، نفوذگر هویت اصلی را جعل می‌کند. این روش شامل تغییر هویت اصلی یکی از طرف‌های ارتباط یا قلب هویت و یا تغییر جریان واقعی فرآیند پردازش اطلاعات نیز است.

پاسخ‌های جعلی: در این نوع از حملات، نفوذگر، بسته‌هایی را که طرف گیرنده اطلاعات در یک ارتباط دریافت می‌کند، پایش می‌کند. البته برای اطلاع از کل ماهیت ارتباط یک اتصال از ابتدا پایش می‌گردد، ولی اطلاعات مفید تنها اطلاعاتی هستند که از سوی گیرنده برای فرستنده ارسال می‌گردند. این نوع حمله بیشتر در مواردی کاربرد دارد که فرستنده اقدام به تعیین هویت گیرنده می‌کند. لذا در صورتی که نفوذگر این بسته‌ها را ذخیره کند و در زمانی‌که یا گیرنده فعال نیست یا فعالیت یا ارتباط آن به صورت آگاهانه به روشی توسط نفوذگر قطع شده است، می‌تواند مورد سوء استفاده قرار گیرد. نفوذگر با ارسال مجدد این بسته‌ها خود را به جای گیرنده جا زده و

از سطح دسترسی مورد نظر برخوردار می‌گردد [۷].

تعریف ۱.۲.۱ (پچ[۱۰]). پچ یا وصله به مجموعه‌ای از تغییرات گفته می‌شود که به منظور به‌روزرسانی، تعمیر یا بهبود یک نرم‌افزار رایانه‌ای به کار می‌رود. این تغییرات ممکن است برای رفع آسیب‌پذیری‌های امنیتی و باگ‌های مختلف نرم‌افزار، بهبود نحوه استفاده یا کارایی و افزودن ویژگی‌های جدید به نرم‌افزار ایجاد شوند.

پچ‌ها معمولاً در فایل‌های اجرایی یا اجزای نرم‌افزار تغییراتی ایجاد می‌کنند یا به طور کامل آن‌ها را با نمونه‌های جدید جایگزین می‌کنند. حتی در برخی از نرم‌افزارهای منبع باز، وصله‌ها در قالب تغییرات سورس کد از طرف توسعه‌دهندگان مختلف منتشر می‌شوند که در این‌صورت وظیفه کامپایل آن‌ها بر عهده کاربر خواهد بود.
محتویات پچ‌ها بسته به میزان تغییرات در ابعاد مختلف (از چند کیلوبایت گرفته تا چند صد مگابایت) عرضه می‌شوند. در برخی موارد از اصطلاح سرویس پک [۱۱] برای پچ‌های بزرگ‌تر استفاده می‌شود. جالب است بدانید علاوه بر سیستم عامل‌ها، معمولاً وصله‌هایی که برای به‌روزرسانی و اعمال تغییرات در بازی‌های رایانه‌ای عرضه می‌شوند نیز به دلیل داشتن فایل‌های گرافیکی دارای حجم بالایی هستند.

تعریف ۲.۲.۱ (بات‌نت[۱۲]). botnet تشکیل شده از دو واژه Ro(bot) و work(Net) به معنای روبات و شبکه است که در اصطلاح رایج به شبکه‌ای گسترده از روبات‌ها اشاره دارد. فردی که مسئولیت هدایت این شبکه را بر عهده می‌گیرد به نام بات اصلی botMaster شناخته می‌شود که بیشتر منابع از اصطلاح بات مستر برای توصیف آن استفاده می‌کنند. [۷].
بات‌نت شبکه‌ای از تجهیزات الکترونیکی هوشمند است که توسط هکرها به بدافزارهایی آلوده شده‌اند و هکرها کنترل کاملی روی عملکرد این سامانه‌ها دارند. این سامانه‌ها می‌توانند رایانه‌های

[۱۰] Patch
[۱۱] Service Patch
[۱۲] Botnet

شخصی، سرورها، تجهیزات سیار و حتی دوربین‌های آی‌پی باشند.
به طور معمول، این بدافزارها در قالب کرم‌های خودتکثیری که از طریق اسکریپت‌ها یا روبات‌ها گسترش پیدا می‌کنند و به سرعت سامانه‌های کاربران را آلوده می‌کنند و ممکن است در کمتر از یک ساعت بالغ بر هزاران دستگاه را آلوده کنند.
مهم این است که رایانه‌های آلوده هیچ کار مخربی انجام نمی‌دهند و فایل‌های کاربران نیز در امنیت کامل قرار دارد؛ زیرا این سامانه‌ها قرار است برای هدف بزرگ‌تری استفاده شوند، بنابراین مهم است که بدافزار هیچ‌گونه فعالیت مخرب یا مشکوکی روی سامانه قربانیان انجام ندهد.

کاربرد بات‌نت

پژوهشی که چندی قبل توسط مؤسسه MIT انجام و گزارش آن منتشر شد نشان داد، روبات‌های فعال در شبکه‌های اجتماعی مثل اینستاگرام، توییتر، تلگرام، فیسبوک و نمونه‌های مشابه نقش مهمی در انتشار اخبار جعلی دارند. علاوه براین، بات‌نت‌ها می‌توانند از سخت‌افزار سامانه‌های قربانیان برای استخراج بیت‌کوین و سایر ارزهای دیجیتال استفاده کنند. از مهم‌ترین تأثیرات مخرب بات‌نت‌ها می‌توان به حمله به وب‌سایت‌ها، سرقت اطلاعات شخصی، ارسال هرزنامه‌ها، انتشار تبلیغات جعلی، بارگذاری بدافزار یا برنامه‌های مخرب روی دستگاه‌های مختلف و حمله به زیرساخت‌های بزرگ اشاره کرد.
آسیب‌پذیری برگ برنده بات‌نت‌هاست. بات‌نت‌ها می‌توانند هر دستگاه متصل به اینترنت را آلوده کنند. این دستگاه‌ها می‌توانند رایانه‌های شخصی، لپ‌تاپ‌ها، تلفن‌های همراه، ساعت‌های هوشمند، دوربین‌های آی‌پی، تلفن‌های آی‌پی، تجهیزات اینترنت اشیا و حتی دستگاه‌های DVR باشند. متأسفانه تولیدکنندگان تجهیزات اینترنت اشیا و به ویژه تولیدکنندگان یخچال، فریزر و تلویزیون‌های هوشمند از رمزهای عبور غیر ایمن برای محافظت از دستگاه‌های هوشمند استفاده می‌کنند که همین مسئله باعث شده تا هکرها به ساده‌ترین شکل قادر به آلوده کردن این دستگاه‌ها باشند.

با توجه به این‌که اینترنت اشیا به سرعت در حال پیشرفت است و دستگاه‌های آنلاین بیشتری به شبکه جهانی متصل می‌شوند، هکرها به راحتی می‌توانند شبکه‌های بات نت بزرگ‌تری را بر مبنای تجهیزات هوشمند خانگی ایجاد کنند. به‌طور مثال، در سال ۲۰۱۶ میلادی، یکی از بزرگ‌ترین حملات DDoS زیرساخت‌های اینترنتی شرکت داین [۱۳] را درهم نوردید. در این حمله از یک شبکه بات‌نت که متشکل از دوربین‌های امنیتی آلوده بود استفاده شد و در نهایت بخش‌های بزرگی از کاربران ساکن ایالات متحده امریکا برای چند ساعت به شبکه‌های بزرگی مثل توییتر، آمازون، نتفلیکس و.... دسترسی نداشتند.

[۱۳] Dyn

فصل ۲
مفاهیم ریاضی

در این فصل ابتدا به مطالعه مفاهیم ریاضی مورد نیاز می‌پردازیم. سپس روش آنالیز تقریب پده [۱] را بررسی می‌کنیم. پس از بیان تعاریف برای این روش تقریبی و نتایج حاصل از آن، مثال‌هایی از روش آنالیز تقریب پده در این فصل آورده شده است.

۱.۲ مقدمه

برای توصیف پدیده‌های زیستی، فیزیکی، شیمیایی و مهندسی از معادلات دیفرانسیل استفاده می‌کنیم؛ معادلات دیفرانسیل یکی از مهم‌ترین مباحث در ریاضیات است که به طور عمومی برای حل آن‌ها به سراغ روش‌های تحلیلی و پیدا کردن جواب دقیق [۲] و فرم تابعی جواب می‌رویم؛ از آنجا که در اکثر موارد پس از مدل‌سازی پدیده‌های دنیای واقعی با معادلات دیفرانسیل معمولی غیرخطی روبه‌رو هستیم، که البته بیشتر دستگاه‌های معادلات دیفرانسیل غیرخطی نمی‌توانند به صورت تحلیلی حل شوند، در این حالت به سراغ روش‌های عددی و پیدا کردن جواب عددی [۳] دستگاه معادلات دیفرانسیل غیرخطی می‌رویم یا از روش‌های تقریبی [۴] استفاده می‌کنیم؛ همان‌طور

[۱] Pade
[۲] Exact solution
[۳] Numerical solution
[۴] Approximate methods

که می‌دانید حل تحلیلی معادلات دیفرانسیل معمولی (ODEs)[۵] غیرخطی و معادلات دیفرانسیل با مشتقات جزئی (PDEs)[۶] غیرخطی سخت‌تر از حل تحلیلی ODEs و PDEs خطی است.

۲.۲ معادلات دیفرانسیل معمولی

تعریف ۱.۲.۲. فرض کنید F نگاشتی از $n+۲$ متغیر باشد و $y = y(x)$. معادله

$$F(x, y, y', y'', \ldots, y^{(n)}) = ۰ \qquad (۱.۲)$$

که رابطه‌ای است بین متغیر مستقل x و تابع $y(x)$ و مشتق‌های آن تا مرتبه n، یک معادله دیفرانسیل معمولی مرتبه n نامیده می‌شود [۷] [۵].

تعریف ۲.۲.۲. جواب معادله دیفرانسیل معمولی (۱.۲) در بازه $\alpha < x < \beta$ تابع $y = \phi(x)$ است به طوری‌که $\phi', \phi'', \ldots, \phi^{(n)}$ در این بازه موجود هستند و این توابع در (۱.۲) صدق می‌کند، یعنی [۵]

$$F(x, \phi(x), \phi'(x), \phi''(x), \ldots, \phi^n(x)) = ۰, \quad \forall x \in (\alpha, \beta).$$

۳.۲ دستگاه معادلات دیفرانسیل معمولی مرتبه اول

در اغلب مسائل ریاضیات کاربردی، چند متغیر وابسته وجود دارد که هر کدام تابعی از یک متغیر هستند، و این متغیر به طور عمومی زمان است. در بیشتر موارد، این نوع مسائل با روابط ریاضی توصیف می‌شوند و نتیجه یک دستگاه از معادلات دیفرانسیل می‌باشد که در آن تعداد معادلات برابر با تعداد متغیرهای وابسته است.

[۵] Ordinary Differential Equations
[۶] Partial Differential Equations
[۷] تعریف دقیق مفهوم معادلات دیفرانسیل مبتنی بر میدان‌های برداری است که در متون هندسه منیفلد به طور دقیق بیان شده است.

یک دستگاه مرتبه اول شامل n معادله و n متغیر وابسته $x_1, x_2, \ldots, x_n$ و یک متغیر مستقل t، به شکل زیر است [۵]

$$\begin{aligned}
\frac{dx_1}{dt} &= f_1(t, x_1, x_2, \ldots, x_n)\\
\frac{dx_2}{dt} &= f_2(t, x_1, x_2, \ldots, x_n)\\
&\vdots\\
\frac{dx_n}{dt} &= f_n(t, x_1, x_2, \ldots, x_n).
\end{aligned}$$

اکنون می‌توانیم قضیه اساسی وجود_یگانگی را برای دستگاه‌های غیرخطی بیان کنیم؛ در واقع برای هر دستگاه می‌توان شرط اولیه را در مبدأ در نظر گرفت، این امر به سادگی با یک تغییر متغیر امکان‌پذیر است.

قضیه ۱.۳.۲ (قضیه اساسی وجود_یگانگی). فرض کنید E یک زیرمجموعه باز از $\mathbb{R}^n$ و شامل x_0 باشد و فرض کنید $f \in C^1(E)$. آنگاه $a > 0$ چنان وجود دارد که مسأله مقدار اولیه

$$\dot{x} = f(x)$$

$$x(0) = x_0$$

روی بازه $[-a, a]$، جواب یگانه $x(t)$ دارد [۲].

تعریف ۲.۳.۲. فرض کنید E یک زیرمجموعه باز از $\mathbb{R}^n$ باشد و $f \in C^1(E)$ به طوری‌که $\begin{cases} \dot{x} = f(x) \\ x(t_0) = x_0 \end{cases}$ معرف یک دستگاه معادلات دیفرانسیل معمولی باشد اگر $\phi(t, x_0)$ جواب دستگاه فوق روی بازه $I(x_0)$ باشد، آنگاه به ازای هر $t \in I(x_0)$ مجموعه نگاشت $\phi_t : E \longrightarrow E$ که به صورت $\phi_t(x_0) = \phi(t, x_0)$ تعریف می‌شود را شار دستگاه می‌نامیم [۲].

تعریف ۳.۳.۲. نقطه تعادل x_0 نقطه هذلولوی دستگاه $\dot{x} = f(x)$ نامیده می‌شود هرگاه هیچ یک

از مقادیر ویژه نظیر به آن دارای قسمت حقیقی صفر نباشد. در ادامه فرض می‌کنیم نقطه تعادل مورد بحث هذلولوی باشد [۲].

تعریف ۴.۳.۲. شار دستگاه خطی $\begin{cases}\dot{x}= Ax \\ x(۰) = x_۰\end{cases}$ را شار هایپرپولیک می‌گوییم اگر A دارای مقادیر ویژه با بخش حقیقی صفر نباشد [۲].

تعریف ۵.۳.۲. یک مجموعه E زیرمجموعه $\mathbb{R}^n$ تحت شار دستگاه خطی $\begin{cases}\dot{x}= Ax \\ x(۰) = x_۰\end{cases}$ را پایا گوییم هرگاه $e^{At}E \subset E$ [۲].

تعریف ۶.۳.۲. فرض کنیم A یک ماتریس حقیقی $۲n\times ۲n$ با مقادیر ویژه مختلط، $\lambda_j = a_j+ib_j$ و $\bar{\lambda}_j = a_j - ib_j$، $i = ۱, ۲, \ldots, n$ با احتساب تکرار باشد. در این‌صورت بردارهای ویژه ساده و تعمیم‌یافته $w_j = u_j + iv_j$ و $\bar{w}_j = u_j - iv_j$ وجود خواهند داشت [۲].

قضیه ۷.۳.۲. فرض کنید $w_j = u_j + iv_j$ بردار ویژه تعمیم‌یافته یا ساده ماتریس مربعی A نظیر به مقدار ویژه $\lambda_j = a_j + ib_j$ باشد که اگر $b_j = ۰$، آن‌گاه $v_j = ۰$. به علاوه فرض کنید

$$B = \{u_۱, \ldots, u_k, u_{k+۱}, v_{k+۱}, \ldots, u_m, v_m\}$$

یک پایه برای $\mathbb{R}^n$ باشد. در این‌صورت زیرفضای پایدار و ناپایدار به صورت زیر تعریف خواهد شد

$$E^s = \text{Span}\left\{u_j, v_j | a_j < ۰,\ ۱ \le j \le n\right\},$$

$$E^u = \text{Span}\left\{u_j, v_j | a_j > ۰,\ ۱ \le j \le n\right\}.$$

که E^s و E^u زیرفضای $\mathbb{R}^n$ هستند [۲].

تعریف ۸.۳.۲. دستگاه غیرخطی

$$\begin{cases}\dot{x}= f(x) \\ x \in \mathbb{R}^n,\ x(۰) = x_۰\end{cases}$$

را در نظر می‌گیریم که $\bar{x}$ نقطه تعادل دستگاه می‌باشد و نگاشت

$$\phi_t : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

معرف شار (جریان‌ـ فلو) دستگاه می‌باشد. در این‌صورت منیفلد پایدار و ناپایدار را به صورت زیر تعریف می‌کنیم [۲]

$$W^s_{Loc}(\bar{X}) = \left\{x \in U \subseteq \mathbb{R}^n \middle| \phi_t(x)_{t\to+\infty} \longrightarrow \bar{X} \ , \ \phi_t(x) \in U, \ \forall\, t \geq ۰\right\},$$
$$W^u_{Loc}(\bar{X}) = \left\{x \in U \subseteq \mathbb{R}^n \middle| \phi_t(x)_{t\to-\infty} \longrightarrow \bar{X} \ , \ \phi_t(x) \in U, \ \forall\, t \leq ۰\right\}.$$

به علاوه توجه کنید که $\dim E^s = \dim W^s_{Loc}(\bar{X})$ و $\dim E^u = \dim W^u_{Loc}(\bar{X})$.

تعریف ۹.۳.۲. اکنون دستگاه $\dot{x}= f(x)$ را در نظر بگیرید و فرض کنید که $\phi(t,x)$ شار این دستگاه باشد و Ω بیانگر فضای حالتی باشد که از زیرمجموعه بازی از $\mathbb{R}^n$ است. در این‌صورت برای هر $x \in \mathbb{R}^n$، مسیر x را به صورت زیر تعریف می‌کنیم [۲]

$$P(x) = \{\phi(t,x) : t \in \mathbb{R}\}.$$

برای هر $x \in \mathbb{R}^n$، نیم مسیر مثبت x را به صورت زیر تعریف می‌کنیم

$$P^+(x) = \{\phi(t,x) : t \geq ۰\}$$

و به همین ترتیب برای $x \in \mathbb{R}^n$، نیم مسیر منفی را به صورت زیر تعریف می‌کنیم

$$P^-(x) = \{\phi(t,x) : t \leq ۰\}$$

می‌گوییم $M \subseteq \Omega$ تحت شار پایا است اگر برای هر $x \in M$،

$$P(M) = \{P(x) : x \in M\} \subseteq M$$

و می‌گوییم مجموعه $M \subseteq \Omega$ تحت شار به‌طور مثبت پایاست اگر برای هر $x \in M$،

$$P^+(M) = \{P^+(x) : x \in M\} \subseteq M.$$

و می‌گوییم که مجموعه $M \subseteq \Omega$ تحت شار به‌طور منفی پایاست اگر برای هر $x \in M$،

$$P^-(M) = \{P^-(x) : x \in M\} \subseteq M.$$

قضیه ۱۰.۳.۲. دستگاه غیرخطی $\dot{x} = f(x)$ دارای منیفلدهای پایدار و ناپایدار S و U است که در نقطه تعادل $X_\circ$ به زیر فضاهای پایدار و ناپایدار E^s و E^u از دستگاه خطی $\dot{X} = AX$ مماس می‌شود و اگر ϕ_t فلوی دستگاه غیرخطی $\dot{x} = f(x)$ باشد، آن‌گاه S و U به ترتیب مجموعه‌های پایای مثبت و منفی فلوی ϕ_t می‌باشند و در روابط زیر صدق می‌کنند [۲]

۱ـ به ازای هر $c \in S$، $\lim_{t\to\infty} \phi_t(c) = X_\circ$،

۲ـ به ازای هر $c \in U$، $\lim_{t\to-\infty} \phi_t(c) = X_\circ$.

۴.۲ پایداری دستگاه معادلات دیفرانسیل معمولی به عنوان یک سیستم دینامیکی پیوسته

برای توصیف پدیده‌های زیستی، فیزیکی و مهندسی از معادلات دیفرانسیل استفاده می‌کنیم. به ویژه پدیده‌های مرتبط با زمان را می‌توانیم به صورت دستگاه معادلات دیفرانسیل، که سیستم دینامیکی نیز نامیده می‌شود درآوریم؛ در اکثر موارد پس از مدل‌سازی پدیده‌های دنیای واقعی با معادلات دیفرانسیل معمولی غیرخطی روبرو هستیم و از آن‌جا که بیشتر دستگاه‌های غیرخطی معادلات دیفرانسیل نمی‌توانند حل شوند، توصیف رفتار کیفی مجموعه جواب دستگاه معادلات دیفرانسیل را در نزدیکی نقطه تعادل بررسی می‌کنیم که شبیه به رفتار کیفی مجموعه جواب دستگاه خطی‌سازی شده متناظر با آن در نزدیکی نقطه تعادل است [۲].

۱.۴.۲ پایداری

سیستمی پایدار محسوب می‌شود که اگر تغییراتی در ورودی آن اعمال کنیم، بعد از مدتی خروج به حالت اولیه خود بازگردد یا این‌که اگر هر مقدار تغییر محدودی که در ورودی یا شرط اولیه سیستم به وجود آوریم، حداکثر به همان مقدار تغییر محدود در خروجی یا جواب مسأله داشته باشیم [۲].

۲.۴.۲ نقطه تعادل

در دستگاه $\dot{X}= f(X)$ که $X \in \mathbb{R}^n$ و $f(X) = (f_1(X), \ldots, f_n(X))$، نقاط X^* را که در شرط $f(X) = 0$ صدق می‌کنند را نقاط تعادل دستگاه گوییم [۲].

یک نقطه تعادل، یک وضعیت ایستا از یک دستگاه است که متغیرهای سیستم دینامیکی در آن نقطه تعادل با گذشت زمان تغییر نمی‌کنند. در واقع ریشه های معادله $f(X^*) = 0$ همان نقاط تعادل هستند؛ یک دستگاه می‌تواند یک یا چند نقطه تعادل داشته باشد که هر یک از این تعادل‌ها می‌توانند پایدار یا ناپایدار باشند؛ هنگامی که مسیرهای موجود در همسایگی نقطه تعادل X^* با گذشت زمان $t \to \infty$ به طور موضعی به آن نقطه تعادل نزدیک شوند، آن‌گاه آن نقطه تعادل پایدار نامیده می‌شود؛ X^* ناپایدار است هرگاه $t \to \infty$ مسیرهای همسایگی از آن تعادل دور شود [۲].

۳.۴.۲ بررسی پایداری با استفاده از ماتریس ژاکوبی و مقادیر ویژه

در دستگاه $\dot{X}= f(X)$ اگر $X \in \mathbb{R}^n$ و $f(X) = (f_1(X), \ldots, f_n(X))$ یک تابع برداری روی $\mathbb{R}^n$ باشد، آن‌گاه

$$J := \frac{\partial f}{\partial X} = \left[\frac{\partial f_i}{\partial x_j}\right]_{n\times n} = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix}_{n\times n} \qquad (۲.۲)$$

را ماتریس ژاکوبی دستگاه $\dot{X}= f(X)$ می‌نامند؛ در ادامه برای بررسی رفتار سیستم، ماتریس ژاکوبی f را در هر یک از نقاط تعادل X^* محاسبه می‌کنیم و مقادیر ویژه آن‌ها را نیز به دست می‌آوریم؛

یعنی با استفاده از مقادیر ویژه ژاکوبی f در نقطه تعادل، می‌توان آن نقطه تعادل را طبقه‌بندی و رفتار سیستم را در نزدیکی هر نقطه تعادل شناسایی کرد؛ در واقع با جای‌گذاری نقطه تعادل X^* در ماتریس ژاکوبی داریم $A = J|_{X=X^*}$ که A یک ماتریس $n \times n$ است. با حل معادله مشخصه $\det(A - \lambda I) = ۰$، مقادیر ویژه λ_i، $i = ۱, ۲, \ldots, n$، از ماتریس A به دست می‌آید؛ طبقه‌بندی نقاط تعادل بر اساس مقادیر ویژه ماتریس A (ماتریس ژاکوبی دستگاه در هر یک از نقاط تعادل)، یعنی λ_i ها انجام می‌شود. حال اگر تمام مقادیر ویژه A دارای قسمت حقیقی منفی (مثبت) باشند، یک نقطه تعادل چاه یا پایدار (چشمه یا ناپایدار) برای دستگاه $\dot{X} = f(X)$ داریم، به‌علاوه اگر برخی از مقادیر ویژه A دارای قسمت حقیقی منفی باشند و بقیه آن‌ها دارای قسمت حقیقی مثبت باشند آن نقطه تعادل را نقطه تعادل زینی می‌نامند؛ همچنین نقطه تعادل X^* را پایدار موضعی نامند هرگاه همه مقادیر ویژه A دارای بخش حقیقی نامثبت باشد [۲].

در ادامه بخش‌های ۵.۲ و ۶.۲ را که از مرجع [۶] انتخاب شده است، خواهیم آورد.

۵.۲ چندجمله‌ای تیلور

می‌خواهیم یک چندجمله‌ای تقریب‌زننده را بررسی کنیم که از تابعی مانند f در نزدیکی نقطه مفروضی پیروی کند. انتخاب چندجمله‌ای را به عضوی از $\prod_n$ (مجموعه تمام چندجمله‌ای‌های از درجه نابیشتر از n) مقید می‌کنیم و ضرایب $c_۰, c_۱, \ldots, c_n$ را چنان می‌یابیم که چندجمله‌ای

$$P_n(x) = c_۰ + c_۱(x - a) + c_۲(x - a)^۲ + \ldots + c_n(x - a)^n \qquad (۳.۲)$$

تابع f را در نزدیکی نقطه $x = a$ تقریب کند، با این فرض که f در $x = a$ لااقل n بار مشتق‌پذیر است (در حالتی‌که a یکی از دو انتهای بازه باشد، آن‌گاه باید مشتق یک طرفه را در این نقطه در نظر داشته باشیم) ضرایب P_n را چنان انتخاب می‌کنیم که

$$P_n^j(a) = f^{(j)}(a), \qquad j = ۰, ۱, \ldots, n, \qquad (۴.۲)$$

$P_n^{\circ}(x) = P_n(x)$ و $f_n^{\circ}(x) = f(x)$. لذا P_n را چنان تعیین می‌کنیم که در $x = a$، توابع P_n و f دارای n مشتق اول برابر باشند، یعنی معادلات (۴.۲) عبارتند از

(۵.۲)
$$\begin{cases} P_n(x) = c_۰ + c_۱(x-a) + c_۲(x-a)^۲ + \ldots + c_n(x-a)^n \\ P_n'(x) = c_۱ + ۲c_۲(x-a) + ۳c_۳(x-a)^۲ + \ldots + nc_n(x-a)^{n-۱} \\ P_n''(x) = (۲)\cdot(۱)c_۲ + (۳)\cdot(۲)c_۳(x-a) + \ldots + n(n-۱)c_n(x-a)^{n-۲} \\ \vdots \\ P_n^n(x) = n(n-۱)\ldots(۲)\cdot(۱)c_n \end{cases}$$

که $n+۱$ معادله قطری بر حسب $n+۱$ مجهول از ضرایب $c_۰, c_۱, \ldots, c_n$ هستند. مشاهده می‌شود که می‌توان این ضرایب را از (۵.۲) به دست آورد. بدین ترتیب که آخرین معادله (۵.۲) مقدار c_n را به دست می‌دهد، سپس از معادله ما قبل آخر می‌توان $c_{n-۱}$ را به دست آورد و به همین طریق از پایین به بالا عمل می‌کنیم تا $c_۰, c_۱, \ldots, c_n$ به دست آیند. روش دیگر حل دستگاه (۵.۲)، محاسبه $P_n^j(a)$ برای $j = ۰, ۱, \ldots, n$ است که با استفاده از (۴.۲) خواهیم داشت

$$c_۰ = f(a),\ c_۱ = f'(a),\ c_۲ = \frac{f''(a)}{۲}, \ldots, c_n = \frac{f^n(a)}{n!}. \qquad (۶.۲)$$

با جایگزین کردن (۶.۲) در (۳.۲) داریم

$$P_n(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{۲}(x-a)^۲ + \ldots + \frac{f^n(a)}{n!}(x-a)^n \qquad (۷.۲)$$

که $P_n(x)$ را چندجمله‌ای تیلور f، از درجه n حول نقطه $x = a$ می‌گویند.

سری مک لورن

در بسیاری از کاربردهای قضیه تیلور، a را مساوی صفر اختیار می‌کنیم. در نتیجه سری به فرم زیر تبدیل می‌شود:

$$f(x) = f(۰) + \frac{f'(۰)}{۱!}x + \frac{f''(۰)}{۲!}x^۲ + \frac{f'''(۰)}{۳!}x^۳ + \ldots \qquad (۸.۲)$$

که معروف به سری مک لورن و حالت خاصی از سری توانی است.

۶.۲ تقریب پده

در این بخش، تقریب‌های گویا را برای توابع مطرح کرده و تابع $f(x)$ را روی قسمت کوچکی از دامنه‌اش تقریب خواهیم زد. برای مثال، اگر $f(x) = \cos x$ آن‌گاه داشتن یک فرمول برای تولید تقریب‌های بر روی بازه $[۰, \pi/۲]$ کافی خواهد بود؛ زیرا از اتحادهای مثلثاتی می‌توانیم استفاده کنیم و $\cos x$ را برای هر مقدار دیگر x واقع در خارج بازه $[۰, \pi/۲]$ حساب کنیم.

یک تقریب گویا برای $f(x)$ روی بازه $I = [a, b]$ خارج قسمت دو چندجمله‌ای $P_N(x)$ و $Q_M(x)$ است که به ترتیب از درجه N و M می‌باشند و از $R_{N,M}(x)$ برای نشان دادن این تابع کسری (تقریب) استفاده می‌کنیم

$$R_{N,M}(x) = \frac{P_N(x)}{Q_M(x)}, \quad x \in I. \tag{۹.۲}$$

هدف ما مینیمم کردن ماکسیمم خطاست. با انجام مقداری محاسبه، معمولاً می‌توان یک تقریب گویا ساخت که در سرتاسر I دارای خطای کمتری نسبت به یک چندجمله‌ای تقریبی باشد. بسطی که ارائه می‌دهیم یک مقدمه است و به تقریب پده محدود خواهد شد.

برای روش پده لازم است که $f(x)$ و مشتق‌های آن در $x = ۰$ پیوسته باشند. دو دلیل برای انتخاب دلخواه $x = ۰$ وجود دارد. اولاً محاسبات آن راحت‌تر است. ثانیاً از یک تغییر متغیر می‌توان استفاده کرد و محاسبات را به بازه‌ای که صفر را در بردارد انتقال داد. چندجمله‌ای‌های رابطه (۹.۲) عبارتند از

$$P_N(x) = p_۰ + p_۱x + p_۲x^۲ + \cdots + p_Nx^N \tag{۱۰.۲}$$

$$Q_M(x) = q_۰ + q_۱x + q_۲x^۲ + \cdots + q_Mx^M \tag{۱۱.۲}$$

چندجمله‌ای‌های (۱۰.۲) و (۱۱.۲) به طریقی ساخته می‌شوند که $f(x)$ و $R_{N,M}(x)$ در $x = ۰$ با هم برابر باشند و مشتق‌های آن‌ها تا درجه $N + M$ نیز در $x = ۰$ برابر باشند. در حالت $Q_۰(x) = ۱$

این تقریب دقیقاً بسط مک لورن برای $f(x)$ است. برای یک مقدار ثابت $N+M$ خطا کوچک‌ترین مقدار را دارا می‌باشد. اگر $P_N(x)$ و $Q_M(x)$ هم‌درجه باشند یا $P_N(x)$ یک درجه بالاتر از $Q_M(x)$ باشد [۴۰، ۴۳] توجه داشته باشید که جمله ثابت $Q_M(x)$ یعنی q_0 را می‌توان برابر ۱ در نظر گرفت. این مقدار مجاز است؛ زیرا q_0 نمی‌تواند صفر باشد و $R_{N,M}(x)$ هنگامی‌که $P_N(x)$ و $Q_M(x)$ هر دو بر یک عدد ثابت تقسیم شوند، تغییر نمی‌کند. بنابراین کسر گویای $R_{N,M}(x)$ دارای $N+M+1$ ضریب مجهول است $(n = N+M)$.

فرض کنید که $f(x)$ تحلیلی بوده و دارای بسط مک لورن زیر باشد

$$f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n + \cdots . \qquad (۱۲.۲)$$

تفاضل $f(x)Q_M(x) - P_N(x) = Z(x)$ را تشکیل می‌دهیم

$$\left(\sum_{j=0}^{\infty} c_j x^j\right)\left(\sum_{j=0}^{M} q_j x^j\right) - \left(\sum_{j=0}^{N} p_j x^j\right) = \sum_{j=N+M+1}^{\infty} a_j x^j \qquad (۱۳.۲)$$

اندیس پایینی $j = N+M+1$ برای جمع‌بندی طرف راست انتخاب شده است؛ زیرا $N+M$ مشتق اول $f(x)$ و $R_{N,M}(x)$ در $x = 0$ برابر هستند. در رابطه (۱۳.۲)، $N+1$ ضریب اول توان‌های x صفرند. بنابراین دستگاه معادلات زیر را بر حسب q_j $(j = 1, \ldots, M)$ و p_j $(j = 0, 1, \ldots, N)$ به صورت زیر می‌نویسیم

$$\sum_{j=0}^{M} q_j c_{N+s-j} = 0, \quad s = 1, 2, \ldots, M \qquad (۱۴.۲)$$

$$p_r = \sum_{j=0}^{r} c_{r-j} q_j, \quad r = 0, 1, \ldots, N \qquad (۱۵.۲)$$

توجه داشته باشید که در هر معادله مجموع اندیس‌های عامل‌های هر حاصل‌ضرب مقدار ثابتی است و این مجموع به تدریج از صفر تا $N+M$ افزایش می‌یابد. در معادله (۱۳.۲)، q_1، q_2، ...، q_M و از $N+1$ معادله (۱۵.۲) مقادیر p_1، p_2، ...، p_N را به دست می‌آوریم. سپس می‌توانیم تقریب

$f(x) = \frac{P_N(x)}{Q_M(x)}$ را بنویسیم. یکی از معایب این روش این است که خطا را به شکل یک فرمول صریح ارائه نمی‌دهد. هدف ما محاسبه بیشترین خطا روی بازه مورد نظر و سپس مینیمم کردن آن است.

برای حالتی که در این بخش آن را توضیح دادیم، ضرایب a_i برای $i = n+۱, n+۲, \ldots$ و q_j برای $j = ۱, ۲, \ldots, M$ چون سری همگراست در حال کاهش هستند. بنابراین یک تقریب خطا به وسیله اولین جمله در طرف راست (۱۳.۲)، $a_{N+M+۱}x^{N+M+۱}$ به دست می‌آید که داریم

$$a_{N+M+۱} = \sum_{j=۰}^{M} c_{N+M+۱-j}q_۱ \qquad (۱۶.۲)$$

این تقریب خطا بیان می‌کند ک با تقریب مک لورن f تقریب کسری که ما ارائه دادیم خطایش در نزدیک صفر کم است و هر چه از صفر دورتر می‌شویم، خطا بیشتر می‌شود.

لازم است که $f(x)$ با n مشتق اول تقریب سری در نقطه صفر با هم مساوی باشند. اگر $x = ۰$ وسط بازه‌ای نباشد که می‌خواهیم تقریب را روی آن بازه به دست آوریم با تغییر متغیر، $x = ۰$ را به وسط آن بازه انتقال می‌دهیم. یادآوری می‌کنیم که برای $M = N$ و $M = N + ۱$ ماکسیمم خطا، مینیمم می‌شود. البته این روش توسط کامپیوتر بررسی شده و دلیل تحلیلی ندارد.

مثال ۱.۶.۲. تقریب پده زیر را بررسی کنید.

$$\cos x = R_{۴,۴} = \frac{۱۵۲۱۰ - ۶۹۰۰x^۲ + ۳۱۳x^۴}{۱۵۱۲۰ + ۶۶۰x^۲ + ۱۳x^۴}$$

حل. اگر از بسط مک لورن برای $\cos x$ استفاده کنیم نه معادله و نه مجهول به دست می‌آوریم. از طرف دیگر، با توجه به این که $\cos x$ و $R_{۴,۴}$ هر دو توابع زوج هستند، توان‌های $x^۲$ را در بردارند. اگر با $f(x) = \cos(x^{۱/۲})$ شروع کنیم

$$f(x) = ۱ - \frac{x}{۲} + \frac{x^۲}{۲۴} - \frac{x^۳}{۷۲۰} + \frac{x^۴}{۴۰۳۲۰} - \cdots,$$

آن‌گاه می‌توانیم محاسبات را ساده‌تر کنیم. در این حالت رابطه (۱۳.۲) به صورت زیر به دست می‌آید

$$\left(۱ - \frac{x}{۲} + \frac{x^۲}{۲۴} - \frac{x^۳}{۷۲۰} + \frac{x^۴}{۴۰۳۲۰} - \cdots\right)\left(۱ + q_۱x + q_۲x^۲\right) - p_۰ - p_۱x - p_۲x^۲ =$$
$$۰ + ۰x + ۰x^۲ + ۰x^۳ + ۰x^۴ + c_۵x^۵ + c_۶x^۶ + \cdots$$

از مقایسه ضرایب پنج توان اول x دستگاه معادلات خطی زیر را به دست می‌آوریم

$$\begin{aligned}
&۱ - p_۰ = ۰\\
&-\frac{۱}{۲} + q_۱ - p_۱ = ۰,\\
&\frac{۱}{۲۴} - \frac{۱}{۲}q_۱ + q_۲ - p_۲ = ۰,\\
&-\frac{۱}{۷۲۰} + \frac{۱}{۲۴}q_۱ - \frac{۱}{۲}q_۲ = ۰,\\
&\frac{۱}{۴۰۳۲۰} - \frac{۱}{۷۲۰}q_۱ + \frac{۱}{۲۴}q_۲ = ۰.
\end{aligned}$$

از دو معادله آخر داریم

$$q_۲ = \frac{۱۳}{۱۵۲۱۰}, \quad q_۱ = \frac{۱۱}{۲۵۲}$$

و از سه معادله اول نیز $p_۰$، $p_۱$ و $p_۲$ را به دست می‌آوریم

$$p_۰ = ۱, \quad p_۱ = -\frac{۱۱۵}{۲۵۲}, \quad p_۲ = \frac{۳۱۳}{۱۵۲۱۰}.$$

در نتیجه $R_{۴,۴}$ به صورت زیر به دست می‌آید

$$R_{۴,۴} = \frac{۱۵۲۱۰ - ۶۹۰۰x^۲ + ۳۱۳x^۴}{۱۵۱۲۰ + ۶۶۰x^۲ + ۱۳x^۴}.$$

تقریب $R_{۴,۴}$ بسط مک لورن تابع $f(x)$ است.

اگر تقریب پده به دست آمده به اندازه کافی خوب نباشد، دو راه زیر توصیه می‌شود:

۱ـ بازه را به دو یا تعداد بیشتر تقسیم کرده و تقریب را بر روی این بازه‌ها می‌نویسیم.

۲ـ n را افزایش می‌دهیم تا دقت بیشتر شود $(n = N + M)$.

در روش دوم با افزایش n محاسبات بیشتر می‌شود و در روش اول نیز چون تقریبات مختلف را روی بازه‌های مختلف به کار می‌بریم احتیاج به وقت و حافظه بیشتری داریم. در حالت کلی، نمی‌توان n را به طور دقیق برای بهترین تقریب به دست آورد و تعداد زیربازه‌ها را طوری انتخاب کرد که به بهترین تقریب دست یابیم [۴۰]. در تقریب پده هر چه از مرکز بازه دورتر باشیم،افزایش خطا سریع‌تر می‌شود.

فصل ۳

مدل ریاضی عدم پذیرش حمله سرویس توزیع‌شده از طریق اینترنت اشیا در شبکه

اینترنت اشیا امکان تراکم انواع متفاوتی از ابزارها، اینترنت و عناصر انسانی (اشیاء فیزیکی) را برای بهبود ارتباط میان آن‌ها فراهم کرده است تا با بهبود ارتباط بین آن‌ها به یک اتصال کامل از جهان اشیا دست یابیم.

جریان اصلی سازگاری تکنولوژی اینترنت اشیا و کاربردهای گسترده آن یک سطح[۱] کاملاً جدید برای مجرمان سایبری را گشوده است که بیشتر برای حملات DDoS (حمله‌های انکار سرویس توزیع شده) مورد استفاده قرارمی‌گیرد.

در این فصل یک مدل اپیدمی دوبخشی ناشی از نفوذ به دو دسته گره‌های داخلی و خارجی ارائه شده است. این مدل ابتدا بر اساس حمله به ابزارهای اینترنت اشیا به دست آمده است و سپس حمله توزیع شده اشیا مخرب، بدافزار، مبتنی بر اینترنت اشیا روی منابع هدف در یک شبکه ایجاد شده است.

این مدل به صورت کلی بر پایه بات‌نت میرای[۲] که در سال ۲۰۱۶ شایع شد ساخته شده است. این مدل در نقاط تعادل برای پیدا کردن پایداری سراسری و موضعی‌شان بررسی شده است. رفتارهای

[۱] Platform
[۲] Mirai Botnet

بحرانی مدل ناشی از اثر گره‌های خارجی بررسی می‌شود. در این مطالعه از مدل‌سازی اپیدمی‌های زیستی برای طراحی و تحلیل حملات DDoS استفاده خواهیم کرد. ابتدا در زیست‌شناسی، شیوع بسیاری از بیماری‌های همه‌گیر مانند طاعون، آبله، مالاریا، ایدز و... موفقیت‌های بزرگی برای ریشه‌کن کردن آن‌ها از طریق ارائه مدل‌های اپیدمی صورت گرفت [۲۰، ۲۹].

در سال‌های اخیر، تعدادی از محققان، از مدل‌سازی اپیدمی برای تجزیه و تحلیل حمله و دفاع در مقابل اشیای مخرب و تأثیر آن بر روی شبکه‌های رایانه‌ای استفاده کرده‌اند تا چارچوبی برای مکانیزم دفاعی بهتر جدا از بهبود مشکل حمله ارائه کنند [۳۱، ۳۷]. مدل‌های اپیدمی در طبیعت پویا هستند که در آن کل جمعیت گره‌ها به بخش‌های مختلف مانندآسیب پذیر، واکسینه، در معرض خطر، آلوده، قرنطینه و بهبودیافته و غیره تقسیم می‌شوند. سپس حرکت گره‌ها از یک بخش محفظه به محفظه دیگر، با استفاده از معادلات دیفرانسیل معمولی نشان داده می‌شود. سیستم معادلات دیفرانسیل معمولی برای چنین مدل‌های اپیدمی از نقطه نظر نقاط تعادل و پایداری موضعی و سراسری آن‌ها تحلیل می‌شوند. در این مدل‌ها، ارزیابی آستانه اپیدمیک R_0 به ما کمک می‌کند تا تصمیم بگیریم که آیا اپیدمی ادامه خواهد یافت یا اینکه آلودگی از بین می‌رود.

اخیراً دو مدل اپیدمی بدافزار جدید توسط یانگ و یانگ[۳] ارائه شده است که اولین مورد [۵۲]، مبتنی بر مدل گسترش محاسبات دو ویروسی برای ارزیابی معیارهای انقراض هر دو ویروس‌ها و برای بقای تنها یک ویروس را ارزیابی کند و مدل دیگر [۵۳] بر اساس وصله‌هایی[۴] است (مدل آسیب پذیر وصله شده با آلودگی حساس) که می‌تواند در یک شبکه آسیب‌پذیر برای ارزیابی تأثیر آن بر شیوع ویروس رایانه‌ای منتشر شود.

در سال ۲۰۱۸، یک مدل شکار-شکارچی برای شبکه بی‌سیم نانو حسگری در برابر حملات اشیا

[۳] Yang and Yang
[۴] Patchs

مخرب توسط کشری[۵]، میشرا[۶] و مالیک[۷] برای تعیین این موضوع که آیا WNSN[۸] ها قادر به زنده ماندن در برابر حمله مخرب‌ها هستند یا نه، ارائه شده است [۲۳].

در این فصل، برای اولین بار، یک مدل اپیدمی ارائه و بررسی شده است که رابطه میان حمله‌های توزیع شده گره‌های هدفمند در یک شبکه و گره‌های خارجی را نشان می‌دهد.

در سال ۲۰۱۴، حوزه جدید اینترنت اشیا (IoT) توسط برندن اوبرین[۹] معمار ارشد و بنیان‌گذار سیستم‌های آریا به صورت زیر مطرح شد [۳۵].

"اگر فکر می کنید اینترنت زندگی شما را تغییر داده است دوباره بیندیشید. IoT قصد دارد دوباره آن را تغییر دهد! "

اینترنت اشیا یک الگوی شبکه جدید از به هم پیوستگی اشیا با هدف بهبود زندگی بشر توسط حضور فراگیرشان ایجاد می‌کند [۱۳]. این یک توسعه از اینترنت به دنیای فیزیکی برای بر همکنش با دستگاه‌های فیزیکی است. این می‌تواند یک وسیله خانگی، ابزار مراقبت سلامت، دوربین CCTV، دوربین رایانه‌ای، دو شاخه هوشمند، چراغ راهنما، ستاپ باکس تلویزیون و تقریباً هر چیزی که در برگیرنده سنسورها، محرک‌ها، واحدهای قدرت و سیستم‌های تعبیه شده هستند، باشد و مهم‌تر از همه این دستگاه باید با پروتکل اینترنتی کار کند [۸، ۱۰]. ملاحظه می‌شود که، اکثر دستگاه‌های IoT از طریق شبکه‌های بی‌سیم با استفاده از فناوری‌هایی مانند سیستم‌های شناسایی فرکانس رادیویی (RFID) و Wi-Fi به اینترنت متصل هستند که دارای ویژگی‌های امنیتی بسیار ضعیف به خاطر قدرت پایین و امکانات محاسباتی کم آن‌ها می‌باشد.

استفاده از دیواره آتش، به‌روزرسانی امنیتی و دستگاه‌های ضد بدافزار معمولاً برای چنین دستگاه‌های IoT کوچک‌تر و کم‌توان‌تر که دارای هیچ سیستم عامل کامل، پردازنده‌های قدرتمند یا حافظه

[۵] Keshri
[۶] Mishra
[۷] Mallick
[۸] Wireless Nano Sensor Network
[۹] Brenden O'Brien

مناسب نیستند، مناسب نبوده و حفاظت پیش‌فرض آن‌ها مانند حفاظت از طریق نام کاربری و کلمه عبور پیش فرض کارخانه، آن‌ها را تبدیل به اهداف نرم برای مجرمان می‌سازد و مهم‌تر از همه ابزارهای IoT می‌توانند نقاط ورودی را به نقاط بحرانی زیرساختی تبدیل کنند.

امروزه، مشاهده حمله همزمان هزاران گره به یک شبکه یا یک سرور، امری عادی است. این نوع حملات به حملات توزیع‌شده معروف هستند. عدم پذیرش حمله توزیع شده، یک حمله توزیع شده متداول است که ابتدا یک ارتش زامبی توسط یک کد زامبی جالب یا اسب تروجان روی گره‌های آلوده از روش‌های مختلف مانند نصب بازی‌های رایگان یا فایل‌های چند رسانه‌ای یا پیوست کردن به ایمیل، ایجاد می‌کند. اسب تروجان روشی مانند باز کردن یک اتصال برای ایجاد ارتباط با واحد کنترل‌کننده ایجاد می‌کند. در نهایت، به محض دریافت یک فرمان از واحد کنترل‌کننده، ارتش زامبی ورودی یک حمله بزرگ روی هدف مورد را حمله آغاز می‌کنند [۱۶، ۲۲]. حملات توزیع شده را می‌توان به دو بخش شبکه‌های سیمی و شبکه‌های بی‌سیم تقسیم کرد. از آنجا که به علت عدم وجود پروتکل‌های مناسب، گره‌های بی‌سیم آسیب‌پذیرتر از گره‌های سیمی هستند، بنابراین حملات توزیع‌شده از طریق گره‌های بی‌سیم رایج‌تر هستند.

مطابق گزارش روندهای DDoS سه ماهه چهارم ۲۰۱۵ Verisign [۵۱]، تقریباً ۷۵ درصد کل حمله‌های DDoS در سه ماهه چهارم سال ۲۰۱۵ مربوط به پروتکل UDP (دیتاگرام کاربر) از طریق شبکه‌های بی‌سیم بوده‌اند. خدمات ارائه شده توسط ارگان‌های مهمی مانند ارتش و مؤسسات دفاعی، شبکه برق، نصب هسته‌ای، بخش بانکی و سایر زیرساخت‌های مهم به طور نرمال به عنوان منابع هدفمند توسط مجرمان حملات خرابکارانه تلقی می‌شوند. طبق گزارشات Symantec [۴۷]، حمله به وب‌سایت بی بی سی در تاریخ اول ژانویه ۲۰۱۶، بزرگ‌ترین حمله DDoS است که به ۶۰۲ گیگابیت در ثانیه رسیده است (Gbps). همچنین، حمله سال ۲۰۱۰ توسط استاکس نت یک حمله هدفمند موفق علیه یک زیرساخت بحرانی و احتمالاً سازمان‌یافته بود و احتمالاً برای خرابکاری در برنامه هسته‌ای ایران طرح‌ریزی شده بود. سال ۲۰۱۶ سالی بیش از اندازه فعال برای

حمله‌های هدفمند بود. در این سال بات‌نت میرای ساخته شده از دستگاه‌های IoT مسئول سه حمله عمده DDoS بود. اولین حمله یک حمله بزرگ DDoS در وب سایت Brain Kreb بود که به ۶۲۰ *Gbps* رسید. سپس مورد دوم، حمله به شرکت میزبان فرانسوی OVH بود که به ۱ *Tbps* رسید. در نهایت سومین مورد حمله IoT که در کانون توجه قرارگرفت، حمله DDoS روی DSN ارائه‌دهنده DYN بود که PayPal، Twitter، Netflix و وب‌سایت‌های دیگر را مختل کرد [۴۸]. بات‌نت میرای تقریباً شامل ۱۲۰۰۰۰ و ۱۵۰۰۰۰ دستگاه IoT است که جهت اجرای حملات DDoS به ترتیب ۶۲۰ *Gbps* و ۱ *Tbps* مورد استفاده قرار می‌گیرد [۴۴]. به گفته گارتنر، ۸/۴ بیلیون IP، ابزارهای IoT را فعال کرد که این نرخ مورد استفاده در سراسر جهان در سال ۲۰۱۷، ۳۱ درصد بیشتر از سال ۲۰۱۶ بود و تا سال ۲۰۲۰ به ۲۰/۴ بیلیون خواهد رسید [۱۸]. علی‌رغم رشد مقبولیت IoT که چشم‌انداز بزرگی برای تأثیر اجتماعی دارد، با این وجود، به علت امنیت ضعیف آن، یکی از مخرب‌ترین فناوری‌ها است. همچنین، آسیب‌پذیری در برابر حملات DDoS با افزایش اتصال زیرساخت‌های بحرانی، مانند شبکه‌های بانکی، شبکه‌های برق، ترافیک هوایی یا سیستم کنترل راه آهن و غیره، به اینترنت افزایش می‌یابد.

حملات مخرب بر روی IP گره فعال شده یا شبکه آن آسیب قابل تصوری به افراد، سازمان‌ها و کشورها به یک اندازه وارد می‌کنند. درک بهتر انتقال پویای اشیای مخرب مطمئناً در طراحی راهکارهای محافظتی مفید برای محافظت و کنترل چنین حملات مخربی به ما کمک خواهد کرد. بنابراین یکی از اهداف این فصل، دستیابی به یک درک دقیق از حملات مخرب، ابتدا روی IP ابزارهای IoT فعال شده و سپس حملات DDoS روی منابع هدفمند در یک شبکه است که با استفاده از اعمال مدل‌سازی اپیدمیولوژیک امکان‌پذیر می‌شود. SIR (آسیب پذیر–آلوده–بازیابی شده) و SIS (آسیب پذیر–آلوده–آسیب پذیر) دو مدل اپیدمی کلاسیک ارائه شده توسط کرماک و مکِندریک[۱۰] برای تجزیه و تحلیل شیوع بیولوژیکی بیماری‌ها به ترتیب در سال ۱۹۲۷ و ۱۹۳۲

[۱۰] Mckendrick

هستند [۲۴، ۲۵]. مدل SIR برای دستیابی افراد مورد نیاز به مصونیت در برابر همان حمله، بسیار کابردی‌تر است. در حالی‌که مدل SIS برای افراد بهبود یافته‌ای است که هیچ مصونیتی ندارند.

در این فصل، مدل پیشنهادی ما دو بخش دارد: در بخش اول، مدل‌سازی برای حمله به دستگاه‌های IoT حاصل می‌شود که عمدتاً بر اساس مدل SIS ذکر شده و در طول بخش گره خارجی بنا می‌شود. در این بخش، بررسی می‌کنیم که چگونه مجرمان تعداد زیادی دستگاه IoT را برای تشکیل یک ارتش زامبی به خطر می‌اندازند. در قسمت آخر، مدل‌سازی برای حمله DDoS از طریق این ارتش زامبی به یک منبع هدفمند به دست می‌آید. این مدل‌سازی بر اساس مدل SIR فوق‌الذکر با مصونیت موقت به جای مصونیت دائم بنا نهاده شده است. ابزارهای آسیب‌پذیر IoT نه تنها تهدیداتی را برای خودشان ایجاد می‌کنند بلکه خودشان نیز تهدیدی جدی برای امنیت هر گونه زیرساخت های شبکه سیمی یا بی‌سیم ساخته شده از سایر دستگاه‌های فعال شده به اینترنت مانند رایانه، لپتاپ، تبلت، تلفن هوشمند و غیره به شمار می‌روند. مدل پیشنهادی ما نمونه‌ای از این مدل است.

تحرک یکی از ویژگی‌های اساسی بخش مهمی از گره‌های IoT در هر شبکه بی‌سیم است. با توجه به این تحرک، گره‌های بی‌سیم اغلب به اینترنت وصل یا قطع می‌شوند. به طور کلی به دلیل تحرک، اگر ابزارهای IoT از ناحیه پوشش محلی خارج شوند یا Wi-Fi قطع شود و یا دستگاه خاموش شود، آن‌گاه می‌توانیم گره IoT را به عنوان گره خارجی تلقی کنیم. حتی برای یک شبکه سیمی، فرضیه اتصال کامل به اینترنت با توپولوژی آن متناقض است [۱۷]. بنابراین، در حالت خاص، اگر یک گره به اینترنت متصل باشد به آن گره داخلی گویند. اگر به اینترنت متصل نباشد به این گره، گره خارجی می‌گویند.

در این فصل، گره‌های خارجی را به عنوان گره‌های IoT که به علت عدم اتصال به اینترنت قطع می‌شوند، در نظر می‌گیریم. از آن‌جا که میرای بات، مکانیزم پایداری ندارد، گره‌های آلوده IoT از طریق خاموش شدن و دوباره روشن شدن اینترنت به راحتی بازیابی می‌شوند [۴۴]. بنابراین، این گره‌های خارجی، گره‌های بازیابی شده هستند و راه‌اندازی مجدد، این گره‌های IoT را آسیب‌پذیر

می‌کنند.

بقیه این فصل به صورت زیر سازماندهی می‌شود:

بخش ۱.۳ مدل اپیدمی را فرمول‌بندی می‌کند. بخش ۲.۳ مدل را بررسی می‌کند. بخش ۳.۳ شبیه‌سازی را تحلیل می‌کند و در نهایت در بخش ۴.۳ به نتیجه‌گیری فصل می‌پردازد.

۱.۳ فرضیه ها و فرمول بندی مدل

در این فصل، یک مدل ریاضی بر اساس فرضیه‌های زیر ارائه می‌دهیم.

$(H۱)$: هر گره حمله‌کننده (آسیب پذیری یا آلوده)، به دلیل خاموشی، با نرخ ثابت $\alpha > ۰$ ازاینترنت قطع می‌شود تا به گره‌های حمله‌کننده خارجی، تبدیل شوند.

$(H۲)$: همان‌طور که در حمله میرای مشاهده شد، دستگاه‌های IoT آلوده می‌توانند با راه‌اندازی مجدد آن‌ها، تمیز شوند [۴۸]، فرض می‌گیریم که هر گره حمله‌کننده خارجی به اینترنت متصل است و تبدیل به گره حمله‌کننده آسیب‌پذیر در نرخ ثابت $\sigma > ۰$ می‌شود.

$(H۳)$: از آن‌جا که مدل ما شامل پویایی حیاتی است، هر گره حمله‌کننده (آسیب پذیر، آلوده یا خارجی) با احتمال $\mu > ۰$ از بین می‌رود.

$(H۴)$: همچنین μ نرخ افزایش از گره‌های جدید در قسمت گره خارجی می‌باشد.

$(H۵)$: هر گره آسیب پذیری (حمله‌کننده یا هدفمند) توسط یک گره حمله‌کننده با نرخ ثابت $\beta > ۰$ آلوده به شمار می‌رود.

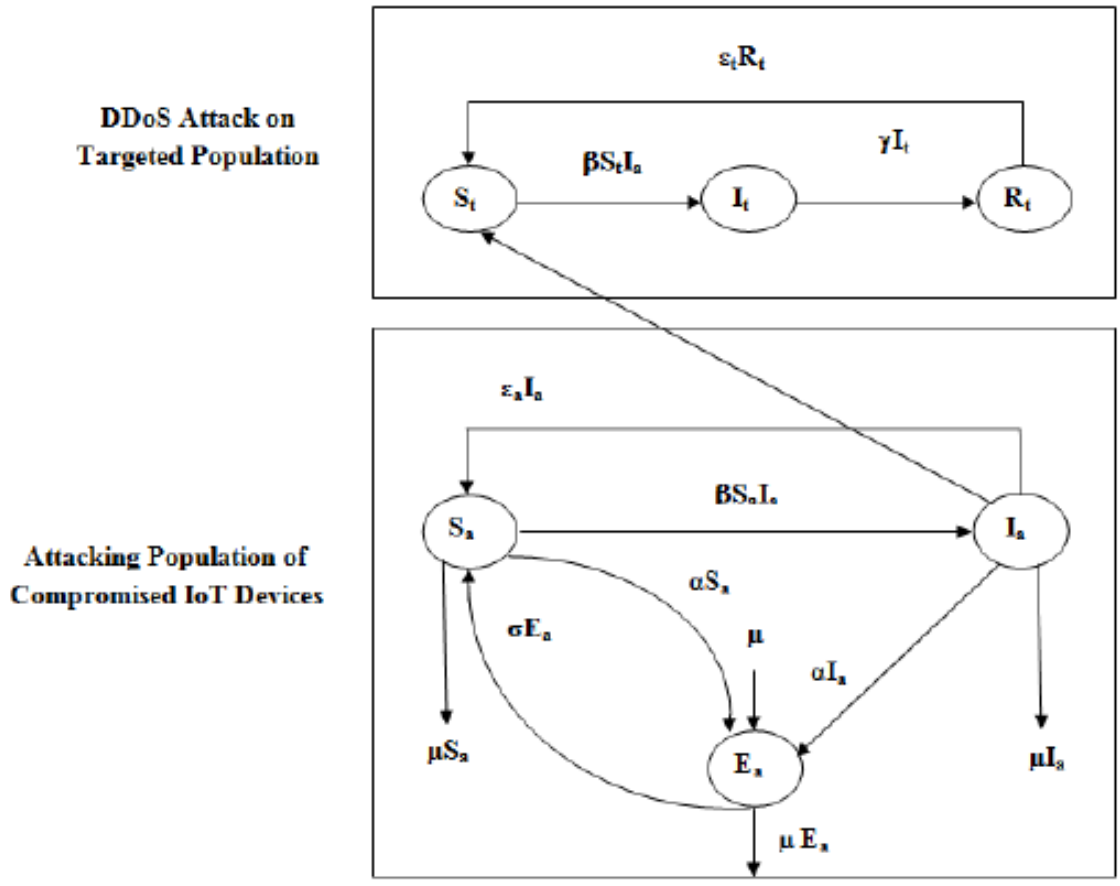
$(H۶)$: هر گره حمله‌کننده غیرآلوده دوباره تبدیل به گره حمله‌کننده آسیب‌پذیر با نرخ ثابت $\varepsilon_a > ۰$ می‌شود.

$(H۷)$: با توجه به اثر درمان مناسب، هر گره هدفمند آلوده تبدیل به گره هدفمند بازیابی شده با نرخ ثابت $y > ۰$ می‌شود.

$(H۸)$: به دلیل مصونیت موقت، گره هدفمند بازیابی شده دوباره تبدیل به گره آسیب‌پذیر هدفمند با نرخ ثابت $\varepsilon_t > ۰$ می‌شود.

بر اساس این فرضیه‌ها، یک مدل اپیدمی ارائه می‌دهیم که از پنج جنبه متفاوت مانند ابزارهای IoT، گره‌های خارجی و داخلی، شبکه بی‌سیم، حمله توزیع‌شده و منبع هدف‌گذاری شده مانند شکل ۱.۳ حاصل می‌شود.

شکل ۱.۳: نمایش شماتیک یک مدل از حمله توزیع‌شده روی منبع هدفمند از طریق گره IoT داخلی و خارجی در شبکه بی‌سیم.



ساختار مدل ارائه شده دارای دو بخش است. ابتدا، مجرمان، یک ارتش زامبی به دست می‌آورند که معمولاً به عنوان بات‌نت توسط گره‌های بی‌سیم هدفمند آسیب‌پذیر از جعیت حمله‌کننده شناخته می‌شوند. دوم، کل ارتش زامبی‌ها به صورت جمعی و همزمان، یک جمعیت هدف خاص تدارک می‌بیند.

برای جمعیت هدف، دستگاه معادلات دیفرانسیل معمولی که نرخ تغییرات بخش‌های مختلف طبق فرضیات بالا را توصیف می‌کنند، در شکل ۱.۳ نشان داده شده است که به صورت زیر فرمول‌بندی می‌شود

$$\begin{aligned} \frac{dS_t}{dt} &= -\beta S_t I_a + \varepsilon_t R_t, \\ \frac{dI_t}{dt} &= \beta S_t I_a - y I_t, \\ \frac{dR_t}{dt} &= y I_t - \varepsilon_t R_t \end{aligned} \tag{۱.۳}$$

که در آن $S_t(t) + I_t(t) + R_t(t) = ۱$.

مشابهاً، برای جمعیت حمله‌کننده، دستگاه معادلات دیفرانسیل معمولی که نرخ تغییرات بخش‌های مختلف را توصیف می‌کند، به صورت زیر فرمول‌بندی می‌شود

$$\begin{aligned} \frac{dS_a}{dt} &= -\beta S_a I_a - \mu S_a + \varepsilon_a I_a + \sigma E_a - \alpha S_a, \\ \frac{dI_a}{dt} &= \beta S_a I_a - \mu I_a - \varepsilon_a I_a - \alpha I_\alpha, \\ \frac{dE_a}{dt} &= \alpha S_a + \alpha I_a - \sigma E_a + \mu - \mu E_a \end{aligned} \tag{۲.۳}$$

که در آن $S_a(t) + I_a(t) + E_a(t) = ۱$.

دستگاه معادلات (۱.۳) و (۲.۳) را می‌توان به سیستم معادلات دیفرانسیل معمولی زیر کاهش

داد

$$\begin{aligned}
\frac{dS_t}{dt} &= -\beta S_t I_a + \varepsilon_t \left(۱ - S_t - I_t\right), \\
\frac{dI_t}{dt} &= \beta S_t I_a - y I_t, \\
\frac{dI_a}{dt} &= \beta \left(۱ - I_a - E_a\right) I_a - \mu I_a - \varepsilon_a I_a - \alpha I_a, \\
\frac{dE_a}{dt} &= \alpha \left(۱ - I_a - E_a\right) + \alpha I_a - \sigma E_a + \mu - \mu E_a.
\end{aligned} \tag{۳.۳}$$

ناحیه ممکن دستگاه (۳.۳) را می‌توان از رابطه زیر به دست آورد

$$\Psi = \{ (S_t, I_t, I_a, E_a) \in R^۴ : S_t > ۰,$$

$$I_t \geq ۰,\ I_a \geq ۰,\ E_a \geq ۰,\ S_t + I_t \leq ۱,\ I_a + E_a \leq ۱ \}$$

این ناحیه ممکن Ψ نسبت به دستگاه (۳.۳) به طور مثبت پایا هستند.

۲.۳ تجزیه و تحلیل ریاضیاتی مدل

۱.۲.۳ عدد تکثیر پایه

موفقیت یا عدم موفقیت هرگونه حمله سیگنال‌های مخرب بستگی به عدد تکثیر پایه $(R_۰)$ دارد. می‌توان این کمیت را به عنوان عدد میانگین از آلودگی ایجاد شده در یک جمعیت آسیب‌پذیر عمومی به وسیله یک گره آلوده در طی طول عمر آلودگی خود، تعریف نمود. $R_۰$ یک آستانه مهم است که می‌تواند تعیین کند که آیا آلودگی در شبکه بی‌سیم به صورت غیر متعارف ادامه دارد یا سرانجام با گذشت زمان پایان می‌پذیرد، یعنی اگر $R_۰ > ۱$ باشد، هر گره آلوده به طور متوسط بیش از یک گره مستعد را آلوده می‌کند و از این‌رو آلودگی همچنان ادامه دارد، در حالی‌که اگر $R_۰ \leq ۱$ باشد، هر کدام گره آلوده، به طور متوسط کمتر از یک گره مستعد را آلوده می‌کند و از این‌رو آلودگی از بین می‌رود [۲۱]. به عبارت دیگر، عدد تکثیر $R_۰$ به عنوان میانگین تعداد آلودگی‌های ثانویه هنگام ورود یک آلودگی جدید تعریف می‌شوند که باعث می‌شود شبکه به طور کامل مستعد آلودگی

شود.

در اکثر مدل‌ها، آلودگی می‌تواند در یک شبکه کاملاً مستعد شروع شود اگر و فقط اگر $R_۰ > ۱$ لذا عدد تکثیر $R_۰$ به عنوان مقدار آستانه تعیین می‌شود.

عدد تکثیر، متوسط گره‌هایی است که وقتی یک مورد آلوده به یک شبکه رایانه‌ای وارد می‌شود، به طور مستقیم به وسیله آن یک مورد آلوده در خلال دوره آلودگی آن، آلوده می‌شوند که معمولاً با $R_۰$ نمایش می‌دهند.

در واقع زمانی که هر گره آلوده به طور متوسط کمتر از یک گره مستعد را آلوده کند یعنی $R_۰ \leq ۱$ باشد، سرانجام آلودگی از بین خواهد رفت و اگر $R_۰ > ۱$ آن‌گاه تقریباً در تمامی اوقات به یک اندازه گره‌هایی آلوده خواهند بود که در واقع تعریف اندمیک است، یعنی هر گره آلوده به طور متوسط بیش از یک گره را آلوده کند، آلودگی رخ می‌دهد. در مدل‌های آلودگی شبکه‌های بی‌سیم، عدد تکثیر بیانگر میانگین تعداد گره‌هایی است که یک گره مستعد آلوده، عامل آلودگی را به گره‌های دیگر، زمانی که تقریباً تمام گره‌ها غیر آلوده هستند سرایت می‌دهد.

عوامل متعددی مانند نرخ تماس بین گره‌های حمله‌کننده و هدف‌دار، احتمال یا نرخ انتقال آلودگی در طول تماس و مدت آلوده بودن روی عدد تکثیر تأثیر می‌گذارند.

چون $\frac{dI_a}{dt} > ۰$ و $\frac{dI_t}{dt} > ۰$ شرایط اساسی برای ایجاد یک اپیدمی هستند، عدد تکثیر پایه برای جمعیت هدف $(R_{۰t})$ و برای جمعیت حمله‌کننده $(R_{۰a})$ به شرح زیر است

$$R_{۰t} = \frac{\beta}{y} \quad \text{و} \quad R_{۰a} = \frac{\beta}{(\mu + \varepsilon_a + \alpha)}.$$

با ادغام هر دو رابطه خواهیم داشت

$$R_۰ = \sqrt{\frac{\beta^۲}{(\mu + \varepsilon_a + \alpha)y}} \qquad (۴.۳)$$

مدل اپیدمی عمومی برای شبکه بی‌سیم می‌تواند این چنین باشد:

فرض کنید $x = (x_۱, x_۲, \ldots x_n)^T$ که در آن x_i تعداد گره‌ها در بخش iـاُم باشد و فرض می‌شود

بخش‌ها مرتب شده‌اند به طوری‌که m بخش اول آلوده می‌باشند (تمایز بین بخش‌های آلوده و غیرآلوده به کمک تغییر مدل صورت می‌گیرد و به تنهایی از ساختار معادلات نتیجه نمی‌شود).
X_s مجموعه همه حالت‌های غیر آلوده در نظر گرفته می‌شود

$$X_s = \{x \geq ۰ | x_i = ۰;\ i = ۱, ۲, \ldots, m\}.$$

فرض کنید $F_i(x)$ نرخ ظهور آلودگی‌های جدید در بخش iـاُم، $V_i^+(x)$ نرخ ورود گره‌ها به بخش iـاُم و $V_i^-(x)$ نرخ خروج گره‌ها از بخش iـاُم باشد. مدل انتقال آلودگی به صورت زیر می‌باشد که باید شرایط اولیه نامنفی به آن بیافزاییم

$$\dot{x_i} = f_i(x) = F_i(x) - V_i(x) \qquad (۵.۳)$$

که در آن $V_i = V_i^- - V_i^+$، $i = ۱, ۲, \ldots, m$ و فرض می‌شود V_i و F_i در ملزومات (۱) تا (۴) صدق کند:

(۱) اگر $x \geq ۰$، آنگاه $V_i^+, V_i^-, F_i \geq ۰$ برای $i = ۱, ۲, \ldots, m$.

اگر یک بخش خالی باشد، آنگاه گره‌ای برای انتقال به بیرون وجود ندارد تا بتوان آن را با آلودگی و دیگر ابزارها از آن بخش منتقل کرد. بنابراین

(۲) اگر $x_i = ۰$، آنگاه $V_i^-(x) = ۰$. به ویژه اگر $x \in X_s$، آنگاه $V_i^- = ۰$ برای $i = ۱, ۲, \ldots, m$.

چون از n بخش، mتای، آن‌ها آلوده هستند. با توجه به این‌که بروز آلودگی برای بخش‌های غیر آلوده صفر است، لذا

(۳) $F_i(x) = ۰$ اگر $i > m$.

همچنین فرض می‌شود اگر شبکه‌ای غیر آلوده باشد، همان‌طور غیر آلوده باقی می‌ماند. این‌گونه

زیرفضای عاری از آلودگی پایا باقی می‌ماند، یعنی در حالت‌های X_s، ورود و خروج و ظهور آلودگی در شبکه (یعنی در همه بخش‌ها) وجود ندارد. لذا

(۴) اگر $x \in X_s$، آنگاه $V_i^+(x) = ۰$. و $F_i(x) = ۰$ برای $i = ۱, ۲, \ldots, m$ طبق شرط (۲). لذا مدل انتقال آلودگی با توجه به رابطه (۵.۳)، بر اساس شرایط (۱) و (۲) به صورت زیر خواهد بود

$$f_i(x) = F_i(x) + V_i^+(x) - V_i^-(x) \xrightarrow{V_i^-(x)=۰} f_i(x) = F_i(x) + V_i^+(x) \geq ۰$$

و این بدان معناست که جواب‌های مدل (۵.۳) نامنفی هستند.

شبکه‌ای را نزدیک به نقطه تعادل در نظر بگیرید. آنگاه شبکه با توجه به سیستم خطی زیر به نقطه تعادل عاری از آلودگی بازخواهد گشت:

$$\bar{x} = Df(\bar{X})(x - \bar{X})$$

که در آن $Df(\bar{x})$ ماتریس ژاکوبی F نسبت به x، $\left[\frac{Df_i}{Dx_j}\right]$ در نقطه تعادل $\bar{X}$ است.
اگر $\bar{X}$ یک نقطه تعادل $\dot{x}_i = f_i(x) = F_i(x) - V_i(x)$ باشد و $f_i(x)$ در شرایط (۱) تا (۴) صدق کند، و F و V ماتریس‌های $m \times m$ باشند و به صورت $F = \left[\frac{\partial f_i}{\partial x_j}(\bar{X})\right]$ و $V = \left[\frac{\partial V_i}{\partial x_j}(\bar{X})\right]$ تعریف شوند که در آن $۱ \leq i$ و $j \leq m$. حال که ماتریس‌های F و V به دست آمدند، $FV^{-۱}$ را ماتریس نسل بعدی نامیدند و به صورت $R_۰ = FV^{-۱}$ تعریف کردند.
دستگاه (۳.۳) را به صورت زیر می‌نویسیم

$$\begin{bmatrix} \dot{I}_t \\ \dot{I}_a \\ \dot{E}_a \end{bmatrix} = \begin{bmatrix} \beta s_t I_a \\ \beta I_a \\ ۰ \end{bmatrix} - \begin{bmatrix} +yI_t \\ +\beta I_a^۲ + \beta E_a I_a + \mu I_a + \varepsilon_a I_a + \alpha I_a \\ -\alpha\,(۱ - I_a - E_a) - \alpha I_a + \sigma E_a - \mu + \mu E_a \end{bmatrix}$$

در این‌صورت داریم

$$F = \left[\frac{\partial f_i}{\partial x_j}(\bar{x})\right] = \begin{bmatrix} ۰ & \beta & ۰ \\ ۰ & \beta & ۰ \\ ۰ & ۰ & ۰ \end{bmatrix}$$

$$V = \left[\frac{\partial V_i}{\partial x_j}(\bar{x})\right] = \begin{bmatrix} ۰ & y & ۰ \\ \mu+\varepsilon_a+\alpha & ۰ & ۰ \\ ۰ & ۰ & \alpha+\sigma+\mu \end{bmatrix}$$

بنابراین

$$V^{-۱} = \frac{۱}{y(-\beta+\mu+\varepsilon_a+\alpha)(\alpha+\sigma+\mu)} \begin{bmatrix} ۰ & y(\alpha+\sigma+\mu) & ۰ \\ y(\mu+\varepsilon_a+\alpha)(\alpha+\sigma+\mu) & ۰ & ۰ \\ ۰ & ۰ & y(\mu+\varepsilon_a+\alpha) \end{bmatrix}$$

در نتیجه داریم

$$FV_t^{-۱} = \begin{bmatrix} ۰ & \beta & ۰ \\ ۰ & \beta & ۰ \\ ۰ & ۰ & ۰ \end{bmatrix} \begin{bmatrix} ۰ & \frac{۱}{\mu+\varepsilon_a+\alpha} & ۰ \\ \frac{۱}{y} & ۰ & ۰ \\ ۰ & ۰ & \frac{۱}{\alpha+\sigma+\mu} \end{bmatrix} = \begin{bmatrix} \beta/y & ۰ & ۰ \\ \beta/y & ۰ & ۰ \\ ۰ & ۰ & ۰ \end{bmatrix}$$

از طرف دیگر می‌دانیم

$$\begin{cases} \dot{s_t} = -\beta s_t I_a + \varepsilon_t(۱ - s_t - I_t) \\ \dot{I_a} = \beta I_a - \beta I_a^{۲} - \beta E_a I_a - \mu I_a - \varepsilon_a I_a - \alpha I_a \\ \dot{I_t} = \beta s_t I_a - y I_t \\ \dot{E_a} = \alpha\,(۱ - I_a - E_a) + \alpha I_a - \sigma E_a + \mu - \mu E_a \end{cases}$$

در نتیجه

$$\begin{bmatrix} \dot{I_a} \\ \dot{I_t} \\ \dot{E_a} \end{bmatrix} = \begin{bmatrix} \beta I_a \\ \beta s_t I_a \\ ۰ \end{bmatrix} - \begin{bmatrix} +\beta I_a^{۲} + \beta E_a I_a + \mu I_a + \varepsilon_a I_a + \alpha I_a \\ +y I_t \\ -\alpha\,(۱ - I_a - E_a) - \alpha I_a + \sigma E_a - \mu + \mu E_a \end{bmatrix}$$

$$F = \left[\frac{\partial f_i}{\partial x_j}(x)\right] = \begin{bmatrix} \beta & ۰ & ۰ \\ \beta & ۰ & ۰ \\ ۰ & ۰ & ۰ \end{bmatrix}$$

بنابراین

$$\left[\frac{\partial V_i}{\partial x_j}\right] = \begin{bmatrix} \mu+\varepsilon_a+\alpha & ۰ & ۰ \\ ۰ & y & ۰ \\ ۰ & ۰ & \alpha+\sigma+\mu \end{bmatrix}$$

$$\Rightarrow V^{-۱} = \begin{bmatrix} \frac{۱}{\mu+\varepsilon_a+\alpha} & ۰ & ۰ \\ ۰ & \frac{۱}{y} & ۰ \\ ۰ & ۰ & \frac{۱}{\alpha+\sigma+\mu} \end{bmatrix}$$

$$\Rightarrow V^{-۱} = \frac{۱}{y(\varepsilon_a+\alpha+\mu)(\mu+\sigma+\alpha)} \begin{bmatrix} y(\alpha+\sigma+\mu) & ۰ & ۰ \\ ۰ & (\mu+\varepsilon_a+\alpha)(\mu+\alpha+\sigma) & ۰ \\ ۰ & ۰ & y(\mu+\varepsilon_a+\alpha) \end{bmatrix}$$

در این‌صورت داریم

$$FV_a^{-۱} = \begin{bmatrix} \beta & ۰ & ۰ \\ \beta & ۰ & ۰ \\ ۰ & ۰ & ۰ \end{bmatrix} \begin{bmatrix} ۰ & \frac{۱}{\mu+\varepsilon_a+\alpha} & ۰ \\ ۰ & \frac{۱}{y} & ۰ \\ ۰ & ۰ & \frac{۱}{\alpha+\sigma+\mu} \end{bmatrix} = \begin{bmatrix} \frac{\beta}{\mu+\varepsilon_a+\alpha} & ۰ & ۰ \\ \frac{\beta}{\mu+\varepsilon_a+\alpha} & ۰ & ۰ \\ ۰ & ۰ & ۰ \end{bmatrix}$$

و این همان مقادیر مورد نظر است

$$R_{۰a} = \frac{\beta}{\mu+\varepsilon_a+\alpha},$$
$$R_{۰t} = \frac{\beta}{y}.$$

۲.۲.۳ وجود پایداری موضعی نقاط تعادل

قضیه ۱.۲.۳. دستگاه (۳.۳) یک نقطه تعادل عاری از آلودگی $E_۰(۱,۰,۰,۰)$[۱۱] و همچنین یک نقطه تعادل اندمیک $E^*\,(S_t^*, I_t^*, I_a^*, E_a^*)$ را قبول می‌کند، که تنها وقتی‌که $\beta > (\mu+\varepsilon_a+\alpha)$ باشد، موجود است.

برهان. برای محاسبه نقاط تعادل، داریم

$$\frac{dS_t}{dt} = ۰;\ \frac{dI_t}{dt} = ۰;\ \frac{dI_a}{dt} = ۰;\ \frac{dE_a}{dt} = ۰.$$

[۱۱] نقطه تعادل عاری از آلودگی $I_t = ۰,\ I_a = ۰$ و $E_a = ۰$.

یعنی

$$\begin{aligned}
&-\beta S_t I_a + \varepsilon_t(۱ - S_t - I_t) = ۰,\\
&\beta S_t I_a - y I_t = ۰,\\
&\beta(۱ - I_a - E_a) I_a - \mu I_a - \varepsilon_a I_a - \alpha I_a = ۰,\\
&\alpha(۱ - I_a - E_a) + \alpha I_a - \sigma E_a + \mu - \mu E_a = ۰.
\end{aligned} \tag{۶.۳}$$

پس از حل معادلات فوق، نقاط تعادل $E_۰(۱,۰,۰,۰)$ را برای حالت عاری از آلودگی و برای حالت تعادل اندمیک، نقطه تعادل $E^*\,(S_t^*, I_t^*, I_a^*, E_a^*)$ را داریم که در آن

$$E_a^* = \frac{(\alpha+\mu)}{(\alpha+\sigma+\mu)}.$$

با جایگزینی آن در رابطه (۶.۳) داریم

$$aI_a^{*۲} + bI_a^* + c = ۰ \tag{۷.۳}$$

که در آن

$$a = \beta, \quad b = -\frac{[(\beta-\mu-\varepsilon_a-\alpha)(\alpha+\sigma+\mu)-\beta(\alpha+\mu)]}{(\alpha+\sigma+\mu)}, \quad c = ۰.$$

فرض کنید تابع مبین (۷.۳) به صورت $\Delta = b^۲ - ۴ac$ باشد. اگر $b \geq ۰$، آنگاه (۷.۳) هیچ جواب مثبتی ندارد. همچنین اگر $\Delta < ۰$ آنگاه (۷.۳) هیچ جواب حقیقی ندارد. اما اگر $b < ۰$ و $\Delta > ۰$، آنگاه (۷.۳) دارای دو جواب مثبت است. توجه داشته باشید که اگر $\beta > (\mu+\varepsilon_a+\alpha)$ یا معادلاً $R_{۰a} > ۱$ باشد، آنگاه $b < ۰$ برقرار است.

بنابراین داریم

$$
\begin{aligned}
S_t^* &= \frac{\varepsilon_t}{\left[\frac{(\beta-\mu-\varepsilon_a-\alpha)(\alpha+\sigma+\mu)-\beta(\alpha+\mu)\pm\Delta}{۲(\alpha+\sigma+\mu)}+\left(۱+\frac{\beta}{y}\right)\varepsilon_t\right]}\\
I_t^* &= \frac{\varepsilon_t}{y\left[۱+\frac{۲\varepsilon_t(۱+\beta/y)(\alpha+\sigma+\mu)}{(\beta-\mu-\varepsilon_a-\alpha)(\alpha+\sigma+\mu)-\beta(\alpha+\mu)\pm\Delta}\right]}\\
I_a^* &= \frac{(\beta-\mu-\varepsilon_a-\alpha)(\alpha+\sigma+\mu)-\beta(\alpha+\mu)\pm\Delta}{۲\beta(\alpha+\sigma+\mu)} \qquad (۸.۳)\\
E_a^* &= \frac{(\alpha+\mu)}{(\alpha+\sigma+\mu)}.
\end{aligned}
$$

□

۳.۲.۳ پایداری موضعی نقطه تعادل عاری از آلودگی

قضیه ۲.۲.۳. اگر $R_{۰a} \leq ۱$، باشد، نقطه تعادل عاری از آلودگی $E_۰(۱,۰,۰,۰)$ سیستم (۳.۳) به طور موضعی و مجانباً پایدار در Ψ است و در صورتی‌که $R_{۰a} > ۱$ باشد، ناپایدار است.

برهان. در نقطه تعادل عاری از آلودگی $E_۰(۱,۰,۰,۰)$ از سیستم (۶.۳)، ماتریس ژاکوبین آن به شکل زیر است

$$
J_{IFE} = \begin{pmatrix}
-\varepsilon_t & -\varepsilon_t & -\beta & ۰\\
۰ & -y & \beta & ۰\\
۰ & ۰ & \beta-(\mu+\varepsilon_a+\alpha) & ۰\\
۰ & ۰ & ۰ & -(\alpha+\sigma+\mu)
\end{pmatrix} \qquad (۹.۳)
$$

معادله مشخصه ماتریس ژاکوبی فوق به شکل زیر محاسبه می‌گردد

$$
(\lambda+\varepsilon_t)(\lambda+y)(\lambda-\beta+\mu+\varepsilon_a+\alpha)(\lambda+\alpha+\sigma+\mu) \qquad (۱۰.۳)
$$

از این‌رو مقادیر ویژه رابطه (۹.۳)، برابر است با

$$
\lambda_۱ = -\varepsilon_t < ۰,\ \lambda_۲ = -y < ۰,\ \lambda_۳ = \beta-(\mu+\varepsilon_a+\alpha),\ \lambda_۴ = -(\alpha+\sigma+\mu) < ۰.
$$

از این چهار مقادیر ویژه $\lambda_۱, \lambda_۲$ و $\lambda_۴$ منفی و مقدار ویژه بعدی؛ یعنی $\lambda_۳$ نیز هرگاه شرط $\beta < (\mu + \varepsilon_t + \alpha)$ برقرار باشد، منفی می‌شود که معادل است با $R_{۰a} \leq ۱$. بنابراین، نقطه تعادل عاری از آلودگی $E_۰$ به صورت موضعی مجانباً در Ψ پایدار است. این نقطه تعادل می‌تواند ناپایدار باشد، یعنی $R_{۰a} > ۱$ اگر $\lambda_۳$ مثبت باشد. به عبارت دیگر، اگر $\beta > (\mu + \varepsilon_a + \alpha)$ برقرار باشد، نقطه تعادل $E_۰$ ناپایدار می‌شود و نقطه تعادل اندمیک یکتا E^* در درون Ψ ظاهر می‌شود و این نقطه به طور موضعی مجانباً پایدار است. از این‌رو اثبات می‌شود که $E_۰$ به طور موضعی مجانباً پایدار است اگر $R_{۰a} \leq ۱$ و ناپایدار است اگر $R_{۰a} > ۱$. □

۴.۲.۳ پایداری موضعی نقطه تعادل اندمیک

قضیه ۳.۲.۳. اگر $R_{۰a} > ۱$، آنگاه یک نقطه تعادل اندمیک یکتایی مانند $E^*(S_t^*, I_t^*, I_a^*, E_a^*)$ وجود دارد که به طور موضعی مجانباً در درون Ψ پایدار است.

برهان. در یک نقطه تعادل اندمیک $E^*(S_t^*, I_t^*, I_a^*, E_a^*)$ از دستگاه معادلات (۳.۳)، ماتریس ژاکوبی آن به شکل زیر است

(۱۱.۳)

$$J_{EE} = \begin{pmatrix} -(\beta I_a^* + \varepsilon_t) & -\varepsilon_t & -\beta S_t^* & ۰ \\ \beta I_a^* & -y & \beta S_t^* & ۰ \\ ۰ & ۰ & -\beta(۲ I_a^* E_a^*) + \beta - (\mu + \varepsilon_a + \alpha) & ۰ \\ ۰ & ۰ & ۰ & -(\alpha + \sigma + \mu) \end{pmatrix}$$

به واسطه مقادیر ویژه از رابطه (۱۱.۳)، $\lambda_۴ = -(\alpha+\sigma+\mu) < ۰$ منفی است که با شرط $R_{۰a} > ۱$ معادل است. دیگر مقدار ویژه $\lambda_۳ = -\beta(۲ I_a^* + E_a^*) + \beta - (\mu + \varepsilon_a + \alpha)$ است. بعد از انجام محاسبات داریم $\lambda_۳ < ۰$ اگر $\beta > (\mu + \varepsilon_a + \alpha)$ یا به طور معادل $R_{۰a} > ۱$.

دو مقدار ویژه دیگر، ریشه‌های معادله مشخصه زیر هستند

$$\lambda^۲ + [y - (\beta I_a^* + \varepsilon_t)]\lambda + [\beta I_a^*(y + \varepsilon_t) + \varepsilon_t y] = ۰. \qquad (۱۲.۳)$$

جمع و ضرب دو ریشه معادله (۱۲.۳) به ترتیب منفی و مثبت هستند. بنابراین هر دو ریشه منفی

هستند. بنابراین همه چهار مقدار ویژه منفی می‌شوند که این یعنی تعادل اندمیک $E^*\,(S_t^*, I_t^*, I_a^*, E_a^*)$ به طور موضعی مجانباً پایدار است اگر $R_{\circ a} < ۱$. □

۳.۳ شبیه‌سازی عددی و بحث درباره آن‌ها

نتیجه جالب مدل ما این است که موفقیت یا شکست حمله توزیع‌شده به منابع هدفمند، فقط بستگی به $R_{\circ a}$ دارد. بنابراین، در هر دو مثال ذکر شده در زیر، مدل ما بر اساس $R_{\circ a} < ۱$ یا $R_{\circ a} > ۱$ متناسب با کاربرد، شبیه‌سازی شده است.

مثال ۱.۳.۳. پایداری موضعی نقطه تعادل عاری از آلودگی که شبیه‌سازی عددی آن در شکل ۲.۳ به صورت گرافیکی نمایش داده شده است متناظر با داده‌های شبیه‌سازی شده برای حمله ناموفق بیان شده در جدول ۱.۳ است. در این‌جا نقطه اولیه به صورت زیر در نظر گرفته شده است

$$S_t = ۰/۹۷, I_t = ۰/۰۲, R_t = ۰/۰۱, S_a = ۰/۵۵, I_a = ۰/۲, E_a = ۰/۲۵$$

با مقادیر پارامتر

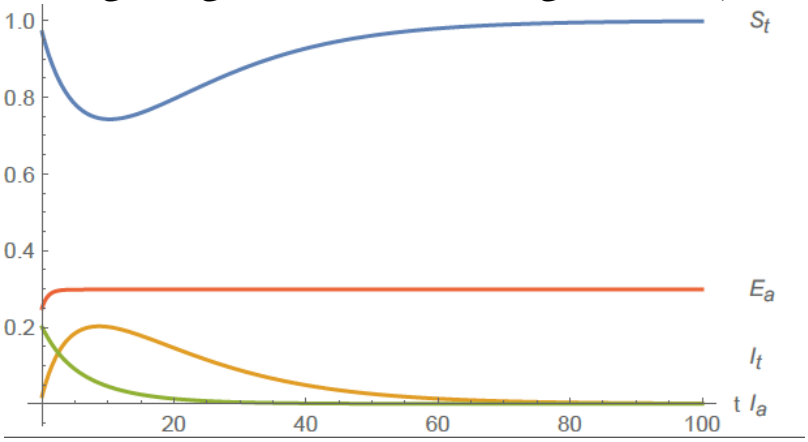
$$\beta = ۰/۳۵, \varepsilon_t = ۰/۲, y = ۰/۰۷, \mu = ۰/۱۲, \varepsilon_a = ۰/۰۲, \sigma = ۰/۸, \alpha = ۰/۲۲.$$

مقدار $R_{\circ a}$ برابر است با ۰/۹۷ و $R_{\circ a} < ۱$. که این یعنی نقطه تعادل $E_\circ$ پایدار می‌شود.
با استفاده از نرم‌افزار متمتیکا جواب دقیق دستگاه (۳.۳) به صورت زیر به دست آمده است

جدول ۱.۳ : جواب دقیق دستگاه (۳.۳)

زمان (t)	S_t	I_t	I_a	E_a
۰	۰/۹۷	۰/۰۲	۰/۲	۰/۲۵
۵/۳۸	۰/۷۷۵۶	۰/۱۸۸۱	۰/۰۸۵۳	۰/۲۹۸۱
۱۰/۴۷	۰/۷۴۲۶	۰/۱۹۹۵	۰/۰۴۲۷	۰/۲۹۸۲
۱۵/۵۲	۰/۷۶۲۷	۰/۱۷۴۷	۰/۰۲۲۷	۰/۲۹۸۲
۲۰/۱۸	۰/۷۹۷۳	۰/۱۴۴۶	۰/۰۱۲۹	۰/۲۹۸۲
۲۵/۱۲	۰/۸۳۶۷	۰/۱۱۳۸	۰/۰۰۷۲	۰/۲۹۸۲
۳۰/۲۵	۰/۸۷۴۰	۰/۰۸۶۴	۰/۰۰۳۹	۰/۲۹۸۲
۳۵/۴۵	۰/۹۰۵۴	۰/۰۶۴۰	۰/۰۰۲۱	۰/۲۹۸۲
۴۰/۲۷	۰/۹۲۸۷	۰/۰۴۷۸	۰/۰۰۱۲۵	۰/۲۹۸۲
۴۵/۰۳	۰/۹۴۶۷	۰/۰۳۵۵	۰/۰۰۰۷۲	۰/۲۹۸۲
۵۵/۴	۰/۹۷۲۴	۰/۱۸۱۹	۰/۰۰۰۲۲۱	۰/۲۹۸۲
۶۰/۳۶	۰/۹۸۰۱۱	۰/۰۱۳۰۹	۰/۰۰۰۱۲۵	۰/۲۹۸۲
۶۵/۴۱	۰/۹۸۵۷	۰/۰۰۹۳۳	۰/۰۰۰۰۷۰۵	۰/۲۹۸۲
۷۰/۵۸	۰/۹۸۹۹	۰/۰۰۶۵۷۷	۰/۰۰۰۰۳۹۰۵	۰/۲۹۸۲
۷۵/۷	۰/۹۹۲۹	۰/۰۰۴۶۳۹	۰/۰۰۰۰۲۱۷۴	۰/۲۹۸۲
۸۰/۲۱	۰/۹۹۴۷	۰/۰۰۳۴۰۶	۰/۰۰۰۰۱۲۹	۰/۲۹۸۲
۸۵/۷۴	۰/۹۹۶۴	۰/۰۰۲۳۲	$۶/۸۹ \times ۱۰^{-۶}$	۰/۲۹۸۲
۹۰/۰۹	۰/۹۹۷۳	۰/۰۰۱۷۲۳	$۴/۱۹ \times ۱۰^{-۶}$	۰/۲۹۸۲
۹۵/۰۲	۰/۹۹۸۱	۰/۰۰۱۲۲۵	$۲/۳۸ \times ۱۰^{-۶}$	۰/۲۹۸۲
۱۰۰	۰/۹۹۸۶	۰/۰۰۸۶۷۳	$۱/۳۴ \times ۱۰^{-۶}$	۰/۲۹۸۲

شکل ۲.۳ : پایداری موضعی نقطه تعادل عاری از آلودگی هنگامی که $R_{\circ a} < ۱$.



مثال ۲.۳.۳. پایداری موضعی نقطه تعادل عاری از آلودگی که شبیه‌سازی عددی آن در شکل ۳.۳ به صورت گرافیکی نمایش داده شده است متناظر با داده‌های شبیه‌سازی شده برای حمله

ناموفق بیان شده در جدول ۲.۳ است. در این‌جا نقطه اولیه به صورت زیر در نظر گرفته شده است $S_t = ۰/۹۷, I_t = ۰/۰۲, R_t = ۰/۰۱, S_a = ۰/۵۵, I_a = ۰/۲, E_a = ۰/۲۵$ با مقادیر پارامتر

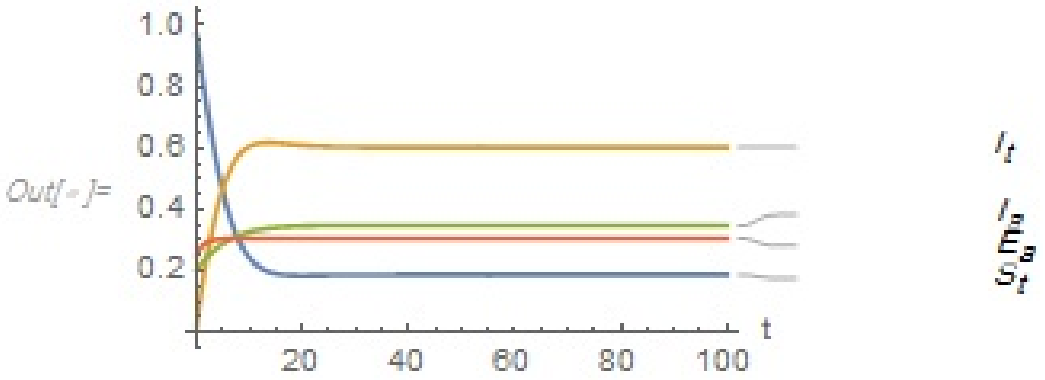
$$\beta = ۰/۶۵, \varepsilon_t = ۰/۲, y = ۰/۰۷, \mu = ۰/۱۲, \varepsilon_a = ۰/۰۰۵, \sigma = ۰/۵, \alpha = ۰/۱.$$

مقدار R_{oa} برابر است با ۲/۸۹ و $R_{oa} > ۱$. در شکل ۳.۳، مؤلفه I_t و I_a در مقادیر غیر صفر پایدار شده‌اند. این‌جا پایداری نقطه تعادل اندمیک نشان داده می‌شوند.

جدول ۲.۳: توزیع جمعیت از کلاس‌های مختلف گره‌ها برحسب زمان برای سناریوی یک حمله موفق ($R_{oa} > ۱$).

زمان (t)	S_t	I_t	I_a	E_a
۰	۰/۹۷	۰/۰۲	۰/۲	۰/۲۵
۱۰/۸۴	۰/۲۳	۰/۶۱	۰/۳۳	۰/۳
۲۰/۷۸	۰/۱۸	۰/۶۱	۰/۳۵	۰/۳
۳۱/۰۶	۰/۱۹	۰/۶	۰/۳۵	۰/۳
۴۰/۴۹	۰/۱۹	۰/۶	۰/۳۵	۰/۳
۵۰/۴۳	۰/۱۹	۰/۶	۰/۳۵	۰/۳
۶۰/۴۷	۰/۱۹	۰/۶	۰/۳۵	۰/۳
۷۰/۷۲	۰/۱۹	۰/۶	۰/۳۵	۰/۳
۸۰/۸۷	۰/۱۹	۰/۶	۰/۳۵	۰/۳
۹۱/۲۳	۰/۱۹	۰/۶	۰/۳۵	۰/۳
۱۰۰	۰/۱۹	۰/۶	۰/۳۵	۰/۳

شکل ۳.۳: پایداری موضعی نقطه تعادل اندمیک هنگامی‌که $R_{\circ a} > ۱$.



۴.۳ نتیجه‌گیری

در این فصل، یک مدل اپیدمی برای حمله DDoS از طریق دستگاه‌های IoT در منابع هدفمند توسعه داده شده است و همه دینامیک‌های آن مورد بررسی قرار گرفته است. اولین بخش از این مدل اپیدمی دو بخشی مبتنی بر IoT که توسعه داده شده است به فهم انتشار حملات مخرب در شبکه بی‌سیم مبتنی بر IoT که یک ارتش زامبی می‌سازد، می‌پردازد. در حالی‌که بخش دیگر این مدل برای درک یک حمله DDoS در شبکه هدفمند با کمک IoT باتنت توسعه‌یافته قبل، گسترش داده می‌شود.

مدل ارائه شده در این فصل از [۳۳] بیشتر مبتنی بر باتنت میرای است که از دستگاه‌های IoT بوده و با سه مورد اصلی حملات DDoS در سال ۲۰۱۶ در کانون توجه قرار گرفتند. نتایج به دست آمده به صورت زیر هستند:

(۱) نقطه تعادل عاری از آلودگی $E_\circ$ به صورت موضعی پایدار است هنگامی‌که $R_{\circ a} < ۱$.

(۲) نقطه تعادل اندمیک E^* به صورت موضعی پایدار است وقتی $R_{oa} > ۱$.

علاوه براین، ما مدل واقع‌بینانه‌تر [۳۳] با استفاده از گره‌های داخلی و خارجی بررسی کردیم. یک یافته مهم در این فصل این است که بیان می‌کند که موفقیت یا شکست حمله DDoS روی شبکه هدفمند تنها به عدد تکثیر پایه جمعیت حمله‌کننده بستگی دارد. در نهایت، موفقیت یا عدم موفقیت سناریوی حمله به کمک شبیه‌سازی نشان داده می‌شود. مدل ارائه شده نقش کلیدی و مهمی در ارزیابی احتمال خطر و سیاست‌گذاری در برابر حملات توزیع شده از طریق دستگاه‌های IoT در منابع هدفمند، ایفا می‌کند.

فصل ۴

حل عددی مدل غیر خطی انتشار ویروس در شبکه‌های رایانه‌ای به روش تقریب پده

ویروس رایانه‌ای یک کد مخرب، مضر، غیر مجاز را اجرا می‌کند؛ مانند پاک کردن فایل‌های ضروری و دسترسی به داده‌های محرمانه و اطلاعات شخصی مانند رمز عبور، شماره حساب، لیست تماس و غیره. بدافزارها بسته به نحوه انتشار، عملکرد و آسیب رساندن به سیستم/کاربران، به دسته‌های مختلفی طبقه‌بندی می‌شوند. این‌ها شامل ویروس‌های محاسباتی، کرم‌های رایانه‌ای، تروجان‌ها، روت‌کیت‌ها، نرم‌افزارهای جاسوسی هستند [۲۸، ۴۹]. انتشار ویروس‌های رایانه‌ای به سایر سیستم‌های متصل شباهت زیادی به رفتار ویروس‌های بیولوژیکی دارد [۹، ۱۱، ۴۶]. بنابراین، مدل‌های مختلف انتشار ویروس رایانه‌ای با استفاده از یک اپیدمیولوژیک ارائه شده است [۳۰، ۳۴، ۴۱، ۴۵]. تعدیل دینامیک انتشار ویروس رایانه‌ای به زبان ریاضی یک روش مؤثر برای درک و تجزیه و تحلیل رفتار انتشار است که در این راستا به روش تقریب پده، مدل را تجزیه و تحلیل می‌کنیم.

تقریب پده

ایده تقریب پده در پایان قرن نوزدهم در تئوری کلاسیک کسرهای مداوم فرموله شد [۳۶] که در بخش ۶.۲ به طور کامل در مورد آن توضیح داده شده است.

تقریب پده از مرتبه (N, M) تابعی گویا به فرم زیر است [۵۰]:

$$P_{N,M}(t) = \frac{\sum_{i=0}^{N} a_i t^i}{\sum_{j=0}^{M} b_j t^j}.$$

چندجمله‌ای‌های $\sum_{i=0}^{N} a_i t^i$ و $\sum_{j=0}^{M} b_j t^j$ تقریب‌های پده نامیده می‌شوند. طبق قاعده $b_0(\neq 0)$ رابطه زیر به دست می‌آید

$$P_{N,M}(t) = \frac{\sum_{i=0}^{N} a_i t^i}{1 + \sum_{j=0}^{M} b_j t^j}.$$

که شامل ضریب مجهول $(N + M + 1)$ است که باید به این ترتیب تعیین شود که بسط‌های سری مک لورن از $P_{N,M}(t)$ با برخی از تابع‌های هدف منطبق است [۱۲].

۱.۴ مدل ریاضی انتشار ویروس در شبکه‌های رایانه‌ای

مدل SEIR در نظر گرفته شده برای انتقال ویروس در یک شبکه رایانه‌ای که توسط می پنگ[۱] در [۳۸] پیشنهاد شده بود و در [۳۹] به آن اشاره شد، در شکل ۱.۴ توضیح داده شده است.

در زمان t' متغیرهای حالت مدل به شرح زیر است

$S(t)$: رایانه‌های آسیب پذیر ،

$E(t)$: رایانه‌های در معرض خطر،

$I(t)$: رایانه‌های آلوده،

$R(t)$: رایانه‌های بازیابی شده،

و پارامترهای مدل نیز به صورت زیر است

[۱] Mei Peng

N : کل جمعیت رایانه‌های موجود در شبکه،

p : نرخی که آنتی‌ویروس رایانه‌های آسیب پذیر را بازیابی می‌کند،

k : نرخی که آنتی‌ویروس رایانه‌های در معرض خطر را بازیابی می‌کند،

a : نرخی که آنتی‌ویروس می‌تواند رایانه‌های در معرض خطر را درمان کند،

$\beta_۱$: نرخ تماس رایانه های آسیب پذیر با رایانه‌های آلوده،

$\beta_۲$: نرخ تماس رایانه های آسیب پذیر با رایانه‌های در معرض خطر،

μ : نرخ حذف یک رایانه از شبکه،

r : نرخ بازیابی رایانه‌های آلوده که درمان می‌شوند.

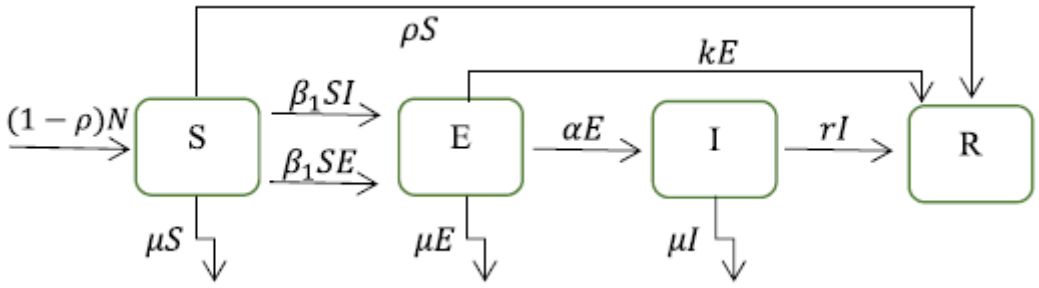
سیستم معادلات حاکم برای مدل به صورت زیر ارائه شده است

$$\begin{cases} S'(t) = (۱-p)N - \beta_۱ S(t)I(t) - \beta_۲ S(t)E(t) - pS(t) - \mu S(t), \\ E'(t) = \beta_۱ S(t)I(t) + \beta_۲ S(t)E(t) - kE(t) - \alpha E(t) - \mu E(t), \\ I'(t) = \alpha E(t) - rI(t) - \mu I(t), \\ R'(t) = pS(t) + kE(t) + rI(t). \end{cases} \quad (۱.۴)$$

در اینجا

$$S(t) + E(t) + I(t) + R(t) = N(t). \quad (۲.۴)$$

شکل ۱.۴ : مدل SEIR برای انتشار ویروس در یک شبکه رایانه‌ای.



فرض کنید

$$X_۱(t) = A - \beta_۱ S(t)I(t) - \beta_۲ S(t)E(t) - aS(t),$$

$$X_۲(t) = \beta_۱ S(t)I(t) + \beta_۲ S(t)E(t) - bE(t),$$

$$X_۳(t) = \alpha E(t) + cI(t),$$

$$A = (۱ - p)N,\ a = p + \mu,\ b = k + \alpha + \mu,\ c = r + \mu.$$

بنابراین طبق رابطه (۲.۴) و فرضیات بالا، مدل (۱.۴) را می‌توان به شکل زیر کاهش داد

$$\begin{cases} S'(t) = X_۱(t), \\ E'(t) = X_۲(t), \\ I'(t) = X_۳(t). \end{cases} \tag{۳.۴}$$

شرایط اولیه به صورت زیر هستند

$$S_۰ = S(۰) = ۵۰,\ E_۰ = E(۰) = ۴۰,\ I_۰ = I(۰) = ۲۰.$$

۲.۴ طرح عددی تقریبی پده

معماری محاسبات پیشنهادی بر اساس طرح تقریب پده که در فصل ۲ بیان شده است به صورت زیر ارائه می‌شود.

۱.۲.۴ ساخت تابعک مانده بر اساس تقریب پده

فرض کنید $S(t)$، $E(t)$ و $I(t)$ توسط توابع گویا پده از درجه N و M به صورت زیر تقریب زده شوند

$$S(t) \approx \frac{\sum_{i=۰}^{N} a_i t^i}{۱ + \sum_{j=۰}^{M} b_j t^j},\ E(t) \approx \frac{\sum_{i=۰}^{N} c_i t^i}{۱ + \sum_{j=۰}^{M} d_j t^j},\ I(t) \approx \frac{\sum_{i=۰}^{N} e_i t^i}{۱ + \sum_{j=۰}^{M} f_j t^j}. \tag{۴.۴}$$

با توجه به شرایط اولیه $S(t_۰) = S_۰,\ E(t_۰) = E_۰,\ I(t_۰) = I_۰$، اگر $t_۰ = ۰$، آن‌گاه داریم

$$a_۰ = S_۰,\ c_۰ = E_۰,\ e_۰ = I_۰ \tag{۵.۴}$$

که پیش‌تر مقادیر $S_۰ = ۵۰,\ E_۰ = ۴۰,\ I_۰ = ۲۰$ و با استفاده از نرم‌افزار کدنویسی در متمتیکا مقادیر $a_۱$، $a_۲$، $b_۱$، $b_۲$، $c_۱$، $c_۲$، $d_۱$، $d_۲$، $e_۱$، $e_۲$، $f_۱$ و $f_۲$ برای تقریب پده مرتبه $(۲, ۲)$ برای دستگاه (۱.۴) به دست می‌آیند.

با استفاده از نرم‌افزار متمتیکا، معادلات را به یک مسئله مینیمم‌سازی تبدیل می‌کنیم و مقادیر زیر به دست آمدند

i	a_i	b_i	c_i	d_i	e_i	f_i
۱	-۱۰۷۶	$-۱/۳۳۳۳$	۱۰۶۲/۴	$-۱/۳۳۳۳$	۱۲/۸	$-۰/۷۳۱۱۳۹$
۲	$-۰/۵۱۶۸۱۶$	۰/۳۳۳۳	۰/۴۱۵۷۶۴	۰/۳۳۳۳	$-۰/۰۴۰۱۸۴$	۰/۱۲۱۶۹۳

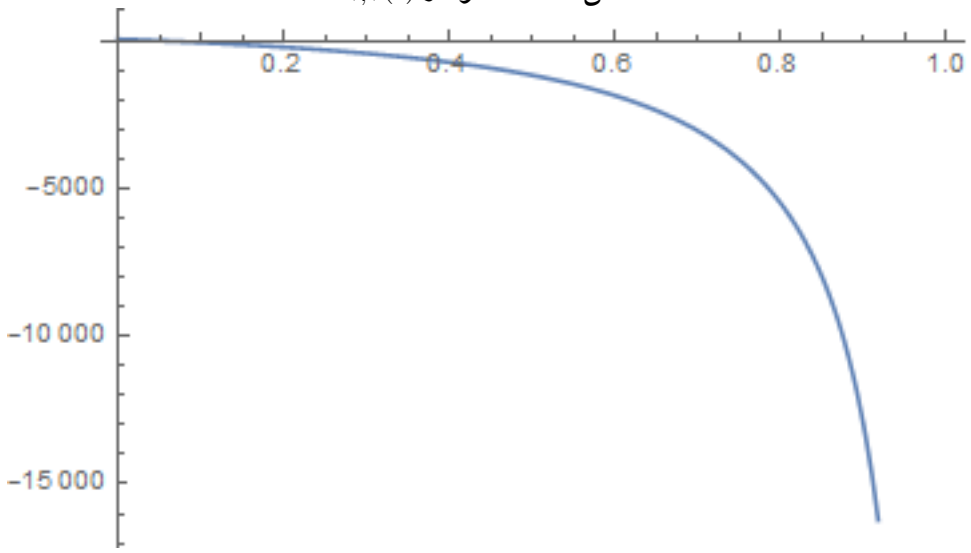
در نتیجه $P_{۲,۲}$ برای هر یک از روابط (۴.۴) به صورت زیر به دست می‌آید

$$S_{۲,۲}(t) \approx \frac{a_۰ + a_۱t + a_۲t^۲}{۱ + b_۱t + b_۲t^۲} = \frac{۵۰ - ۱۰۷۶t - ۰/۵۱۶۸۱۶t^۲}{۱ - ۱/۳۳۳۳t + ۰/۳۳۳۳t^۲},$$
$$E_{۲,۲}(t) \approx \frac{c_۰ + c_۱t + c_۲t^۲}{۱ + d_۱t + d_۲t^۲} = \frac{۴۰ + ۱۰۶۲/۴t + ۰/۴۱۵۷۶۴t^۲}{۱ - ۱/۳۳۳۳t + ۰/۳۳۳۳t^۲},$$
$$I_{۲,۲}(t) \approx \frac{e_۰ + e_۱t + e_۲t^۲}{۱ + f_۱t + f_۲t^۲} = \frac{۲۰ + ۱۲/۸t - ۰/۰۴۰۱۸۴t^۲}{۱ - ۰/۷۳۱۱۳۹t + ۰/۱۲۱۶۹۳t^۲}.$$

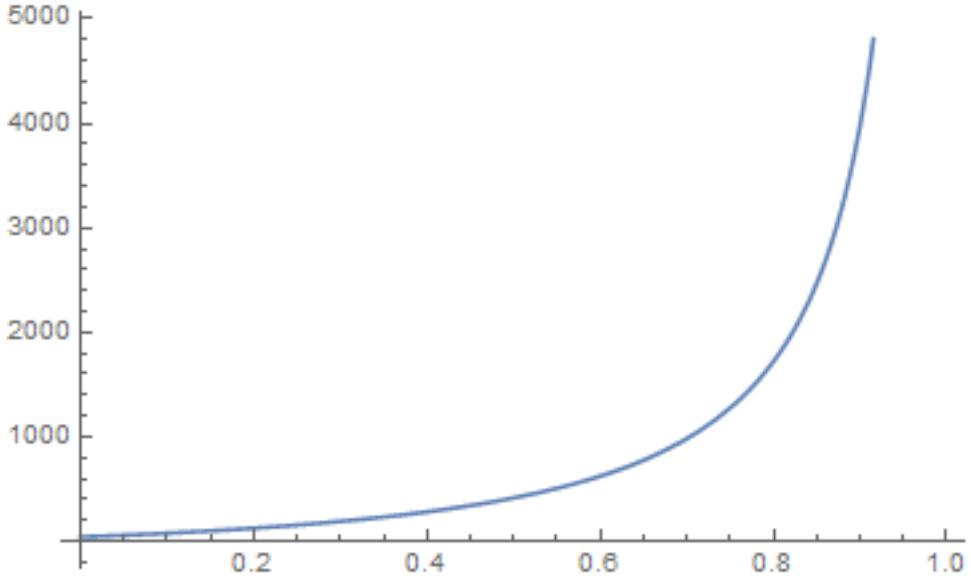
تقریب‌های $S_{۲,۲}(t)$، $E_{۲,۲}(t)$ و $I_{۲,۲}(t)$ بسط مک‌لورن تابع $f(t)$ هستند.

نمودارهای $S_{۲,۲}(t)$و $E_{۲,۲}(t)$ و $I_{۲,۲}(t)$ برای بازه $[۰, ۱]$ به ترتیب در شکل‌های ۲.۴، ۳.۴ و ۴.۴ به دست می‌آوریم.

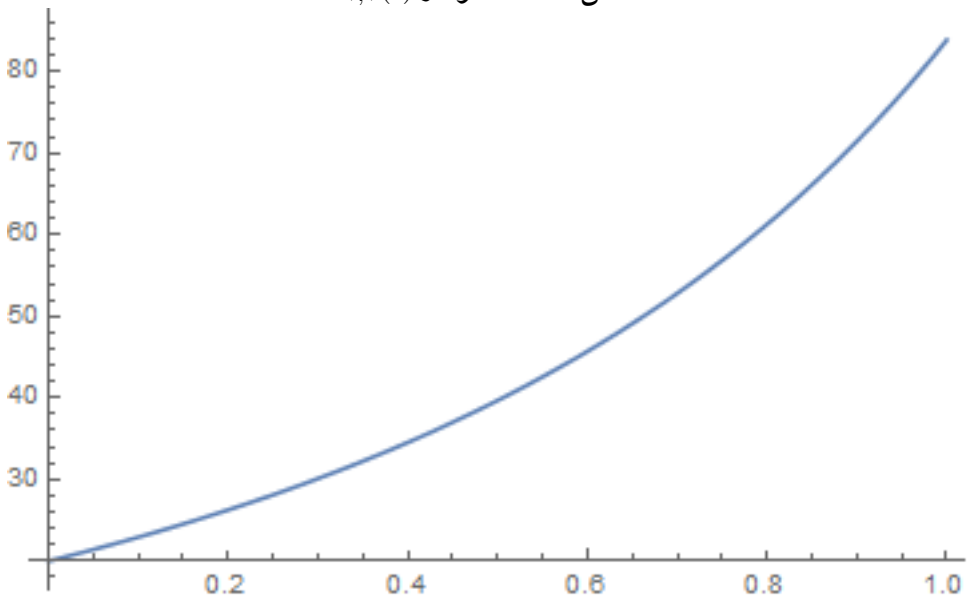
شکل ۲.۴: نمودار $S_{۲,۲}(t)$



شکل ۳.۴: نمودار $E_{۲,۲}(t)$



شکل ۴.۴: نمودار $I_{۲,۲}(t)$



پیوست

در حالت ۳.۲.۳ و با استفاده از دستور Nsolve سیستم دارای دو نقطه تعادل زیر است:

۱ ـ نقطه تعادل عاری از آلودگی $E_0(1,0,0,0)$؛

۲ ـ نقطه تعادل اندمیک $E^*\,(S_t^*, I_t^*, I_a^*, E_a^*)$.

رجوع کنید به زیربخش‌های ۱.۴.۲، ۲.۴.۲ و ۳.۴.۲.

حال هر یک از نقاط تعادل را در ماتریس ژاکوبین دستگاه (۲.۳) جایگذاری می‌کنیم و معادلات مشخصه مربوطه را به دست می‌آوریم

$$J = \begin{pmatrix} -\beta I_a - \varepsilon_t & -\varepsilon_t & -\beta S_t & 0 \\ \beta I_a & -y & \beta S_t & 0 \\ 0 & 0 & \beta(1 - 2I_a - E_a) - \mu - \alpha & -\beta I_a \\ 0 & 0 & 0 & -\alpha - \sigma - \mu \end{pmatrix}$$

۱ ـ محاسبه ماتریس ژاکوبی و معادله مشخصه در نقطه E_0:

$$J|_{E_0} = \begin{pmatrix} -\varepsilon_t & -\varepsilon_t & -\beta & 0 \\ 0 & -y & \beta & 0 \\ 0 & 0 & \beta - \mu - \alpha & 0 \\ 0 & 0 & 0 & -\alpha - \sigma - \mu \end{pmatrix}$$

معادله مشخصه:

$$(-\alpha - \mu - \sigma - \lambda)\,(-\alpha + \beta - \mu - \varepsilon_a - \lambda) \times \left(y\lambda + \lambda^2 + y\varepsilon_t + \lambda\varepsilon_t\right) = 0.$$

طبق فرضیه‌ها و فرمول‌بندی مدل، $\alpha > 0$، $\sigma > 0$، $\mu > 0$، $\beta > 0$، $\varepsilon_a > 0$، $y > 0$ و $\varepsilon_t > 0$. لذا مقادیر ویژه λ_1 تا λ_4 به صورت زیر بیان می‌شوند

$$\lambda_1 = -\varepsilon_t < 0,\ \lambda_2 = -y < 0,\ \lambda_3 = \beta - \alpha - \mu - \varepsilon_a,\ \lambda_4 = -\alpha - \mu - \sigma < 0$$

واضح است که مقادیر ویژه $\lambda_۱$، $\lambda_۲$ و $\lambda_۴$ منفی و برای مقادیر ویژه $\lambda_۳$ دو حالت داریم که اگر $\lambda_۳ = \beta - \alpha - \mu - \varepsilon_a < ۰$، در نتیجه $\beta < \alpha + \mu + \varepsilon_a$ که در نهایت $R_{۰a} \leq ۱$. بنابراین نقطه تعادل عاری از آلودگی $E_۰$ در ψ مجانباً پایدار است و اگر $\lambda_۳ = \beta - \alpha - \mu - \varepsilon_a > ۰$، آنگاه $\beta > \alpha + \mu + \varepsilon_a$ که $R_{۰a} > ۱$ و نقطه تعادل $E_۰$ ناپایدار می‌شود و نقطه تعادل اندمیک E^* در درون ψ ظاهر می‌شود و این نقطه به طور موضعی مجانباً پایدار می‌شود. از این‌رو می‌توان گفت $E_۰$ به طور موضعی مجانباً در ψ پایدار است اگر $R_{۰a} \leq ۱$ و ناپایدار است اگر $R_{۰a} > ۱$.

۲ـ محاسبه ماتریس ژاکوبی و معادله مشخصه در نقطه E^*:

$$J|_{E^*} = \begin{pmatrix} -\beta I_a^* - \varepsilon_t & -\varepsilon_t & -\beta S_t^* & ۰ \\ \beta I_a^* & -y & \beta S_t^* & ۰ \\ ۰ & ۰ & \beta(۱ - ۲I_a^* - E_a^*) - \mu - \alpha & -\beta I_a^* \\ ۰ & ۰ & ۰ & -\alpha - \sigma - \mu \end{pmatrix}$$

معادله مشخصه:

$$(-\beta I_a^* - \varepsilon_t - \lambda)(-y - \lambda)((\beta(۱ - ۲I_a^* - E_a^*) - \mu - \alpha) - \lambda)(-\alpha - \sigma - \mu - \lambda) = ۰.$$

$$\lambda_۱ = \frac{۱}{۲}\left(-y - \varepsilon_t - \beta I_a^* - \sqrt{(y + \varepsilon_t + \beta I_a^*)^۲ - ۴(y\varepsilon_t + y\beta I_a^* + \beta\varepsilon_t I_a^*)}\right),$$

$$\lambda_۲ = \frac{۱}{۲}\left(-y - \varepsilon_t - \beta I_a^* + \sqrt{(y + \varepsilon_t + \beta I_a^*)^۲ - ۴(y\varepsilon_t + y\beta I_a^* + \beta\varepsilon_t I_a^*)}\right),$$

$$\lambda_۳ = -\alpha - \mu + \beta - \varepsilon_a - \beta E_a^* - ۲\beta I_a^*,$$

$$\lambda_۴ = -\alpha - \mu - \sigma.$$

چهار مقدار ویژه $\lambda_۱$، $\lambda_۲$، $\lambda_۳$ و $\lambda_۴$ منفی هستند . با توجه به توضیحات ۳.۳، نقطه تعادل اندمیک E^* به طور موضعی مجانباً پایدار است اگر $R_{۰a} > ۱$.

برای وضوح بیشتر مطالب، می‌توانید در ادامه مثال ۱.۳.۳ را برای توضیحات داده شده حل کنید.

مراجع

[۱] اتکینسون، کندال. هان، ویمین و استوارت، دیوید. *حل عددی معادلات دیفرانسیل معمولی*، ترجمه حسین خیری و غلامرضا حجتی، دانشگاه تبریز، چاپ اول، ۱۳۹۳.

[۲] پرکو، لاورنس. *دستگاه‌های معادلات دیفرانسیل و سیستم‌های دینامیکی*، ترجمه سید احمد موسوی و محمد جهانشاهی، دانشگاه تربیت مدرس، چاپ اول، ۱۳۸۱.

[۳] تاتی بختیاری، داوود. *فرهنگ کامل و تشریحی لغات و اصطلاحات کامپیوتر*، تهران، انتشارات آراد کتاب، چاپ اول، ۱۳۸۸.

[۴] حسنوی، رضا و فرسایی، داریوش. *فرهنگ تشریحی کامپیوتر میکروسافت*، تهران، پیک علوم، چاپ پنجم، ۱۳۸۳.

[۵] کرایه‌چیان، اصغر. *معادلات دیفرانسیل و کاربرد آن‌ها*، دانشگاه فردوسی مشهد، چاپ بیست و پنجم، ۱۳۹۲.

[۶] طاهری نسب، یاسر. *حل عددی معادلات دیفرانسیل- جبری به روش تقریب پده*، دانشگاه یزد، ۱۳۸۳.

[۷] علوی‌نیا، سید مهدی. *اینترنت اشیا در هوشمندسازی شبکه‌ها*، تهران، انتشارات آوای قلم، چاپ اول، ۱۳۹۶.

[8] Abomhara, M. and Koien, G. M., *Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks*, Journal of Cyber Security, **4**, (2015) 65-88.

[9] Anderson, R.M. and May, R.M., *Infectious Diseases of Humans: Dynamics and Control*. Oxford University Press, Oxford, 1992.

[10] Atzori, L., Iera, A. and Morabito, G., *The internet of things: a survey*, Computer Networks, **54 (15)**, (2010) 2787-2805.

[11] Brauer, F., and Chavez, C.C., *Mathematical Models in Population Biology and Epidemiology*. Springer, New York, 2001.

[12] Bojdi, Z.K., Ahmadi-Asl, S. and Aminataei, A., *A new extended Padé approximation and its application*. Adv. Numer. Anal. 2013, Article ID 263467 (2013). https://doi.org/10.1155/2013/263467.

[13] Botta, A., De Donato, W., Persico, V., and Pescapé, A., *Integration of cloud computing and internet of things: a survey*, Future Generation Computer Systems, **56**, (2016) 684-700.

[14] Celic, E., Bayram, M., *On the numerical solution of differential algebraic equations by Pade series*, Applied Mathematics and Computation, **137**, (2003) 151-160.

[15] Celic, E., Bayram, M., *Arbitrary order numerical methd for solving differential-algebraic equations by Pade series*, Applied Mathematics and Computation, **137**, (2003) 57-65.

[16] Farraposo, S., Gallon, L. and Owezarski, P., *Network security and DoS Attacks*, Technical Report, LAAS-CNRS, France, 2005.

[17] Gan, C., Yang, X., Liu, W., Zhu, Q., Jin, J. and He, L., *Propagation of computer virus both across the Internet and external computers: a complex-network approach*, Communications in Nonlinear Science and Numerical Simulation, **19**, (2014) 2785-2792.

[18] Gartner, Inc, Gartner Says 8.4 Billion Connected Things Will Be in Use in 2017, Up 31 Percent From 2016, https://www.gartner.com/newsroom/id/3598917, 2017.

[19] Halder, K. and Mishra, B. K., *A mathematical model for a distributed attack on targeted resources in a computer network*, Communications in Nonlinear Science and Numerical Simulation, **19**, (2014) 3149-3160.

[20] Hethcote, H. W., *A thousand and one epidemic models, in: S. A. Levin (Ed.), Frontiers in Theoretical Biology, Lecture Notes in Biomathematics 100*, Springer, Berlin, p. 504, 1994.

[21] Jones, J. H., *Notes on* $R_\circ$,Technical Report, Stanford University, Stanford, 2007.

[22] Keshri, A. K., Mishra, B. K. and Mallick, D. K., *Library formation of known malicious attacks and their future variants*, International Journal of Advanced Science and Technology, **4**, (2016) 1-12.

[23] Keshri, A. K., Mishra, B. K. and Mallick, D. K., *A Predator- Prey Model on the Attacking Behavior of Malicious Objects in Wireless Nanosensor Networks, Nano Communication Networks*, Elsevier, **15**, (2018) 1-16. DOI: https://doi.org/10.1016/j.nancom.2018.01.002.

[24] Kermack, W. O. and McKendrick, A. G., *A contribution to the mathematical theory of epidemics*, In Proceedings of the Royal Society, London A, **115**, (1927) 700-721.

[25] Kermack, W. O. and McKendrick, A. G., *Contributions of mathematical theory to epidemics. II.-The problem of endemicity.* In Proceedings of the Royal Society, London A, **138**, (1932) 55-83.

[26] YLi, . and Muldowney, J. S., *A geometric approach to globalstability problems*, SIAM Journal, **27 (4)**, (1996) 1070-1083.

[27] Li, Y. and Muldowney, J. S., On Bendixson's criterion, Journal of Diferential Equations, **106**, (1994) 27-39.

[28] Martí n del Rey, A., *Mathematical modelling of the propagation of malware*, a review. Secur. Commun. Netw. **8(15)**, (2015) 2561-2579.

[29] Ma, Z. and Li, J., *Dynamical modelling and analysis of epidemics*, World Scientific, 2009.

[30] Meisel, M., Pappas, V. and Zhang, L.A., *Taxonomy of biologically inspired research in computer networking*. Comput. Netw. **54**, (2010) 901-916.

[31] Mishra, B. K. and Halder, K., *e-Epidemic Models on the Attack and Defense of Malicious Objects in Networks*, book chapter 9, V. Dabbaghian and V. K. Mago(eds.), *Theories and Simulations of Complex Social Systems, Intelligent Systems Reference Library 52*,Springer-Verlag Berlin Heidelberg, 2014.

[32] Mishra, B. K., Haldar, K. and Sinha, D. N., *Impact of Information based Classication on Network Epidemics*, Nature, Scientific Reports 6, Article number 28289, 2016. DOI:10.1038/srep28289

[33] Mishra, B. k., Keshri, A. K., Mallick„ D. K. and Mishra, B. K., *Mathematical model on distributed denial of service attack through Internet of things in a network*, Nonlinear Engineering, **8**, (2019) 486-495.

[34] Murray, W.H., *The application of epidemiology to computer viruses*. Comput. Secur. **7(2)**, (1988) 139-145.

[35] O'Brien, B., (2014, September 27). Aria Systems: Twitter, 2014, Retrieved from Twitter: https://twitter.com/ariasystemsinc/status/516022100872929280.

[36] Padé, H., *Sur la representation approche dúne fonction par des fractions rationelles*, Ann. Sci. Ec. Norm. Super. 9(suppl.), (1892) 1-93.

[37] Pastor-Satorras, Castellano, R., Van Mieghem, C., P., and Vespignani, A., *Epidemic processes in complex networks*. Reviews of modern physics, **87 (3)**, (2015), pp. 925.

[38] Peng, M., He, X., Huang, J. and Dong, T., *Modelling computer virus and its dynamics*, Math. Probl. Eng. **2013(5)**, Article ID 842614 (2013).

[39] Rafiq, M. and Raza, A., *Numerical modelling of transmission dynamics of vector-born plant pathogen*, In: Proceedings of 14th International Bhurban Conference on Applied Sciences and Technology (IBCAST-2017), (2017) 214-219.

[40] Ralston, A. and Rabinowitz P. h., *A first course in numerical analysis*, Mcgraw-Hill Internatioanal Edition, **8**th, 1986

[41] Ren, J., Yang, X., Yang, L.X, Xu, Y. and Yang, F., *A delayed computer virus propagation model and its dynamics*, Chaos Solitons Fractals, **45(1)**, (2012) 74-79.

[42] Richard, C., Robert, J. and Bishop, H., *Modern Control Systems*, Thelfth Edition, Prarson, 2010.

[43] Richard, L., Burden, J., *Douglas Faires*, Numerical Analysis, **PWS-KENT** Publishing Company, 4 ed. 1985.

[44] Said, N. B., Biondi, F., Bontchev, V., Decourbe, O., Given-Wilson, T., Legay, A., and Quilbeuf, J., *Detection of Mirai by Syntactic and Semantic Analysis*, 2017.

[45] Song, L.P., Jin, Z. and Sun, G.Q., *Modelling and analysing of botnet interactions*, Physica A **390(2)**, (2011) 347-358.

[46] Sun, C. and Hsieh, Y.H., *Global analysis of an SEIR model with varying population size and vaccination*, Appl. Math. Model. **34(10)**, (2010) 2685-2697.

[47] Symantec Corporation, Internet Security Thread Report, **21**, 2016.

[48] Symantec, Internet Security Threat Report (ISTR), **22**, 2017.

[49] Tipton, H.F. and Krause, M., *Information Security Management Handbook*, Auerbach Publications, Boca Raton (2010).

[50] Vijta, M., *Some remarks on the Padé -approximations*. In: Proceedings of the 3rd TEMPUS-INTCOM Symposium, (2000) 1-6.

[51] *Verisign Distributed Denial of Service Trends Report*, **2**, Issue 4, ۴^{th} Quarter, 2015.

[52] Yang, L. X., Yang, X., and Tang, Y. Y., *A bi-virus competing spreading model with generic infection rates*, IEEE Transactions on Network Science and Engineering, 2017.

[53] Yang, L. X., Yang, X., and Wu, Y., The impact of patch forwarding on the prevalence of computer virus: a theoretical assessment approach, Applied Mathematical Modelling, **43**, (2017) 110-125.

واژه‌نامه فارسی به انگلیسی

آلوده ..... Infected

ارتش زامبی ..... Zombie

اسب تروجان ..... Trojan horse

الگوریتم ..... Algoritm

اینترنت اشیا ..... Internet of thing

بدافزار مخرب ..... Malicious object

بسط مک لورن ..... Maclaurin expansion

به طور موضعی پایدار مجانبی ..... Locally asymptotically stable

به طور یکنواخت پایدار ..... Uniformly persistent

بندیکسون ..... Bandixon

پایداری ..... Stable

پایداری سیستم‌های دینامیکی ..... Stability of dynamical systems

پایداری مجانبی ..... Asymptotic Stability

پایداری موضعی ..... Local Stability

پچ ـ وصله ..... Patch

پروتکل ارتباطی کاربر ..... User Datagram Protocol (UDP)

تقریب اولیه ..... Intial approximation

تقریب پده ..... Pade approximation

نقطه تعادل اندمیک ..... Endemic equilibrium point

جواب تقریبی ..... Approxiation solution

جواب دقیق ..... Exact solution

چندجمله‌ای مشخصه ..... Characteristic polynomial

چندجمله‌ای تیلور ..... Taylor polynomial

حمله انکار سرویس توزیع‌شده ..... Distributed denial of service attack

حمله هدفمند ..... Targeted attack

خطا ..... Error

خودگردان ..... Autonomous

دستگاه معادلات دیفرانسیل ..... System of differential equations

روش‌های تقریبی ..... Approximate method

روش رانگ‌ـ کوتا ..... Rung-Kutta method

روش عددی ..... Numerical method

زینی ..... Saddle

سیستم‌های خطی ..... Linear system

سیستم‌های غیرخطی ..... Nonlinear system

شبکه‌های بی‌سیم ..... Wireless network

شرایط اولیه ..... Intial conditions

شرایط پایداری ..... Stationary conditions

عدد تکثیر پایه ..... Basic reproduction number

گره آلوده ..... Infectious node

گره خارجی ..... External node

گره مستعد (آسیب‌پذیر) ..... Susceptible node

گره هدفمند ..... Node targeted

فناوری شناسایی مبتنی بر فرکانس رادیویی ..... Radio Frequency Identification (RFID)

قضیه رُل ..... Rolle's theorem

قضیه وایراشتراس ..... Weiershtrass theorem

ماتریس ژاکوبی ..... Jacobian matrix

معادله مشخصه ..... Characteristic equation

معیار روت‌ـ هرویتس ..... Rout hurwitz criterion

مقدار ویژه ..... Eigen value

میرای بات نت ..... Mirai botnet

ناپایدار ..... Unstable

نقطه تعادل ..... Equilibrium point

نقطه تعادل عاری از آلودگی ..... Infected free equilibrium point

ویروس ..... Virus

همگرایی ..... Convergence

واژه‌نامه انگلیسی به فارسی

روش‌های تقریبی ..... Approximate method

جواب تقریبی ..... Approxiation solution

پایداری مجانبی ..... Asymptotic Stability

خودگردان ..... Autonomous

عدد تکثیر پایه ..... Basic reproduction number

بندیکسون ..... Bandixon

معادله مشخصه ..... Characteristic equation

چندجمله‌ای مشخصه ..... Characteristic polynomial

همگرایی ..... Convergence

حمله انکار سرویس توزیع‌شده ..... Distributed denial of service attack

نقطه تعادل اندمیک ..... Endemic equilibrium point

نقطه تعادل ..... Equilibrium point

خطا ..... Error

جواب دقیق ..... Exact solution

گره خارجی ..... External node

آلوده ..... Infected

نقطه تعادل عاری از آلودگی ..... Infected free equilibrium point

گره آلوده ..... Infectious node

اینترنت اشیا ..... Internet of thing

تقریب اولیه ..... Intial approximation

شرایط اولیه ..... Intial conditions

ماتریس ژاکوبی ..... Jacobian matrix

سیستم‌های خطی ..... Linear system

به طور موضعی پایدار مجانبی ..... Locally asymptotically stable

پایداری موضعی ..... Local Stability

بسط مک لورن ..... Maclaurin expansion

بدافزار مخرب ..... Malicious object

میرای بات نت ..... Mirai botnet

سیستم‌های غیرخطی ..... Nonlinear system

روش عددی ..... Numerical method

تقریب پده ..... Pade approximation

پچ ـ وصله ..... Patch

فناوری شناسایی مبتنی بر فرکانس رادیویی ..... Radio Frequency Identification (RFID)

قضیه رُل ..... Rolle's theorem

معیار روت ـ هرویتس ..... Rout hurwitz criterion

روش رانگ ـ کوتا ..... Rung-Kutta method

زینی ..... Saddle

پایداری سیستم‌های دینامیکی ..... Stability of dynamical systems

پایداری ..... Stable

شرایط پایداری ..... Stationary conditions

گره مستعد (آسیب‌پذیر) ..... Susceptible node

دستگاه معادلات دیفرانسیل ..... System of differential equations

چندجمله‌ای تیلور ..... Taylor polynomial

حمله هدفمند ..... Targeted attack

گره هدفمند ..... Targeted node

پروتکل ارتباطی کاربر ..... User Datagram Protocol (UDP)

به طور یکنواخت پایدار ..... Uniformly persistent

ناپایدار ..... Unstable

ویروس ..... Virus

قضیه وایراشتراس ..... Weiershtrass theorem

شبکه‌های بی‌سیم ..... Wireless network

ارتش زامبی ..... Zombie

Surname: Valipoure Name: Bentolhoda

Title: Predicting the malware propagation in a computer network using numerical methods

Supervisor: Dr. Zohreh Dadi
Advisor: Dr. Hamideh Nasabzadeh

Degree: M. Sc. Subject: Department of Mathematics
Field: Numerical Analysis

University of Bojnord Faculty of Basic Sciences
Date: August 2022 Number of pages: 70

Keywords: Malware, Propagation model, Computer network, Numerical methods.

Abstract

In this thesis, firstly, the study of the statuses and behaviors of a malware propagation model in the computer network and then the study of the dynamic states in that model are studied, analyzed and analyzed using the obtained numerical methods. We put the internet of things in a dynamic study. Then we solve the approximate Barouche model of the Pade approximation and get a solution for the differential equation.

University of Bojnord
Faculty of Basic Sciences

Dissertation Submitted in Partial

Fulfillment of the Requirements for the

Degree of Master of Science in Mathematics-Numerical Analysis

Title

Predicting the malware propagation in a computer network using numerical methods

Supervisor

Dr. Zohreh Dadi

Advisor

Dr. Hamideh Nasabzadeh

by

Bentolhoda Valipoure

August 2022