

صلى الله عليه وسلم



دانشکده علوم پایه
گروه ریاضی

پایان نامه

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 پایان نامه تحصیلی دانشجویان
دانشگاه بجنورد

نام خانوادگی دانشجو: ولی پور

نام: بنت الهدی

عنوان پایان نامه: پیش بینی 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: ۶۸

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 ممتیکا 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 پایان نامه

اینجانب بنت الهدی ولی پور دانش آموخته کارشناسی ارشد رشته ریاضی کاربردی، گرایش آنالیز عددی دانشکده علوم پایه دانشگاه بجنورد پدیدآور پایان نامه با عنوان "دینامیک پیش بینی انتشار بدافزار در یک شبکه رایانه ای با کمک روش های عددی" با راهنمایی دکتر زهره دادی گواهی و تعهد می کنم 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 پایان نامه دستاورد پژوهش اینجانب و محتوای آن از درستی و اصالت برخوردار است؛
□ حقوق معنوی همه کسانی را که در به دست آمدن نتایج اصلی پایان نامه تأثیرگذار بوده اند، رعایت کرده ام و هنگام کاربرد دستاورد پژوهش های دیگران در آن، با دقت و به درستی به آنها استناد کرده ام؛

□ این پایان نامه و محتوای آن را تاکنون اینجانب یا کس دیگری برای دریافت هیچ گونه مدرک یا امتیازی در هیچ جا ارائه نکرده ایم؛

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

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

□ در همه گام های انجام این پایان نامه، هرگاه به اطلاعات شخصی افراد یا اطلاعات سازمان ها دسترسی داشته یا آنها را به کار برده ام، رازداری و اخلاق پژوهش را رعایت کرده ام.

تاریخ امضا

حقوق دانشگاه بجنورد

این گزارش و همه حقوق مادی و محصولات آن (مقاله ها، کتاب ها، پروانه های اختراع، برنامه های رایانه ای، نرم افزارها، تجهیزات ساخته شده و مانند آنها) بر پایه «قانون حمایت حقوق مؤلفان و مصنفان و هنرمندان» مصوب سال ۱۳۴۸ و اصلاحیه های بعدی آن و همچنین آیین نامه های اجرایی این قانون از آن دانشگاه بجنورد است و هرگونه استفاده از همه یا پاره ای از آن شامل نقل قول، تکثیر، انتشار، کاربرد نتایج، تکمیل و مانند آنها به صورت چاپی، الکترونیکی یا وسایل دیگر، تنها با اجازه نوشتاری دانشگاه بجنورد شدنی است. نقل قول محدود در انتشارات علمی مانند کتاب و مقاله یا پایان نامه ها و رساله های دیگر با نوشتن اطلاعات کامل کتاب شناختی، نیازی به مجوز دانشگاه بجنورد ندارد.

تقدیم بہ

مجلس عزیزم و

سپرگرم

سپاس گزارمی...

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.

خدا یا چنان کن سرانجام کار
تو خوشنودباشی و ما رسگار

بنت الهدی ولی پور
شهریور ۱۴۰۱

فهرست مطالب

خ	فهرست اختصارات
د	فهرست شکل‌ها
ذ	فهرست جدول‌ها
۱	مقدمه
۳	۱ مفاهیم شبکه‌های رایانه‌ای
۳	۱.۱ اینترنت اشیا
۸	۲.۱ امنیت در اینترنت اشیا
۸	۱.۲.۱ حملات غیرفعال
۹	۲.۲.۱ حملات فعال
۱۳	۲ مفاهیم ریاضی
۱۳	۱.۲ مقدمه
۱۴	۲.۲ معادلات دیفرانسیل معمولی
۱۴	۳.۲ دستگاه معادلات دیفرانسیل معمولی مرتبه اول
	۴.۲ پایداری دستگاه معادلات دیفرانسیل معمولی به عنوان یک سیستم دینامیکی
۱۸	پیوسته
۱۸	۱.۴.۲ پایداری
۱۹	۲.۴.۲ نقطه تعادل
۱۹	۳.۴.۲ بررسی پایداری با استفاده از ماتریس ژاکوبی و مقادیر ویژه
۲۰	۵.۲ چندجمله‌ای تیلور
۲۲	۶.۲ تقریب پده

۲۶	مدل ریاضی عدم پذیرش حمله سرویس توزیع شده از طریق اینترنت اشیا در شبکه
۳۲	۱.۳ فرضیه ها و فرمول بندی مدل
۳۵	۲.۳ تجزیه و تحلیل ریاضیاتی مدل
۳۵	۱.۲.۳ عدد تکثیر پایه
۴۰	۲.۲.۳ وجود پایداری موضعی نقاط تعادل
۴۲	۳.۲.۳ پایداری موضعی نقطه تعادل عاری از آلودگی
۴۲	۴.۲.۳ پایداری موضعی نقطه تعادل اندمیک
۴۳	۳.۳ شبیه سازی عددی و بحث درباره آنها
۴۶	۴.۳ نتیجه گیری
	۴ حل عددی مدل غیر خطی انتشار ویروس در شبکه های رایانه ای به روش تقریب
۴۸	پده
۴۹	۱.۴ مدل ریاضی انتشار ویروس در شبکه های رایانه ای
۵۱	۲.۴ طرح عددی تقریبی پده
۵۱	۱.۲.۴ ساخت تابعک مانده بر اساس تقریب پده
۵۵	پیوست
۵۷	مراجع
۶۱	واژه نامه فارسی به انگلیسی
۶۴	واژه نامه انگلیسی به فارسی

فهرست اختصارات

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

فهرست شکل‌ها

۴	۱.۱	ابعاد اینترنت اشیا.
	۱.۳	نمایش شماتیک یک مدل از حمله توزیع‌شده روی منبع هدفمند از طریق گره
۳۳		IoT داخلی و خارجی در شبکه بی‌سیم.
۴۵	۲.۳	پایداری موضعی نقطه تعادل عاری از آلودگی هنگامی که $R_{oa} < 1$.
۴۶	۳.۳	پایداری موضعی نقطه تعادل اندمیک هنگامی که $R_{oa} > 1$.
۵۰	۱.۴	مدل SEIR برای انتشار ویروس در یک شبکه رایانه‌ای.
۵۳	۲.۴	نمودار $S_{۲,۲}(t)$.
۵۳	۳.۴	نمودار $E_{۲,۲}(t)$.
۵۴	۴.۴	نمودار $I_{۲,۲}(t)$.

فهرست جدول‌ها

۴۴	۱.۳	جواب دقیق دستگاه (۳.۳)
		۲.۳	توزیع جمعیت از کلاس‌های مختلف گره‌ها برحسب زمان برای سناریوی یک
۴۶		حمله موفق ($R_{oa} > 1$)

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، میسرا 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 میسرا 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 میسرا 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

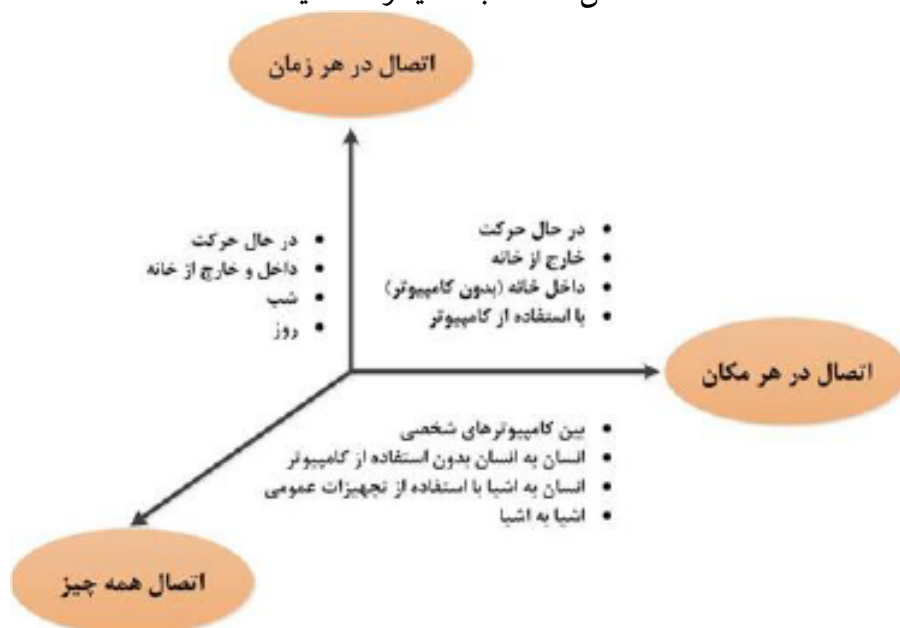
۱.۱ اینترنت اشیا

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 اینترنت فراهم می‌گردد [۴].

شکل ۱.۱ ابعاد مختلف اینترنت اشیا را نشان می‌دهد. همه چیز باید بتواند 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.

^۱Internet 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].

^۲Ping of Death (PoD)

تعریف ۲.۱.۱ (حمله انکار سرویس توزیع شده (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 قرار دهد 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 [۴].

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].

^۳Distributed Denial of Service Attack (DDoS)

^۴Denial of Service Attack

^۵SYN Flood

تعریف ۵.۱.۱ (پروتکل ارتباطی کاربر (UDP) ^۶). پروتکل بدون اتصالاتی 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

^۶User Datagram Protocol (UDP)

^۷Automatic Identification and Data Capture (AIDC)

(RFID)[^] 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:

- ۱- برچسب
- ۲- خوانشگر برچسب
- ۳- نویسنده اطلاعات
- ۴- آنتن و تقویت کننده سیگنال (در صورت لزوم)
- ۵- نرم افزار مدیریت اطلاعات
- ۶- بانک اطلاعاتی، ساختار شبکه اطلاعاتی [؟].

فناوری‌های بی سیم

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

[^]Radio Frequency Identification (RFID)

در حالت کلی امواج به دو دسته تقسیم‌بندی می‌شوند:

۱- امواج مادون قرمز^۹

۲- امواج رادیویی RF [؟].

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 [؟].

۱.۲.۱ حملات غیر فعال

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؟

^۹Infrared

شود: در این نوع حمله، نفوذگر تنها به پایش اطلاعات رد و بدل شده می‌پردازد. برای مثال، شود 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 [۴].

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. در تقسیم بندی حملات دو مورد زیر مورد توجه 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 زمانی که 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 [۹].

تعریف ۱۰.۲.۰۱ (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 این صورت 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 ۲۰.۲.۰۱ (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. [۹].

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 بر این، 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 این که 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 بات نت که متشکل از دوربین‌های امنیتی آلوده بود استفاده شد و در نهایت بخش‌های بزرگی از کاربران ساکن ایالات متحده آمریکا 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

^۱Pade

^۲Exact solution

^۳Numerical solution

^۴Approximate 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

$$F(x, y, y', y'', \dots, y^{(n)}) = 0 \quad (۱.۲)$$

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 [۵].

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

$$F(x, \phi(x), \phi'(x), \phi''(x), \dots, \phi^{(n)}(x)) = 0, \quad \forall x \in (\alpha, \beta).$$

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.

یک دستگاه مرتبه اول شامل n معادله و n متغیر وابسته x_1, x_2, \dots, x_n و یک متغیر مستقل t ، به

^۵Ordinary Differential Equations

^۶Partial Differential Equations

^۷تعریف دقیق مفهوم معادلات دیفرانسیل مبتنی بر میدان‌های برداری است که در متون هندسه منیفلد به طور دقیق بیان شده است.

شکل زیر است [۵]

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

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 طوری که 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 $\phi_t : E \rightarrow E$ 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 $\begin{cases} \dot{x} = Ax \\ x(0) = x_0 \end{cases}$ 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 $\begin{cases} \dot{x} = Ax \\ x(0) = x_0 \end{cases}$ را پایا می‌گوییم هرگاه $e^{At}E \subset E$ [۲].

تعریف ۶.۳.۲. فرض کنیم A یک ماتریس حقیقی $2n \times 2n$ با مقادیر ویژه مختلط، $\lambda_j = a_j + ib_j$ و $\bar{\lambda}_j = a_j - ib_j$ با $i = 1, 2, \dots, n$ با احتساب تکرار باشد. در این صورت 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 $b_j = 0$ ، آن‌گاه $v_j = 0$. به علاوه فرض کنید

$$B = \{u_1, \dots, u_k, u_{k+1}, v_{k+1}, \dots, u_m, v_m\}$$

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

$$E^s = \text{Span} \{u_j, v_j | a_j < 0, 1 \leq j \leq n\},$$

$$E^u = \text{Span} \{u_j, v_j | a_j > 0, 1 \leq j \leq n\}.$$

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

تعریف ۸.۳.۲. دستگاه غیرخطی

$$\begin{cases} \dot{x} = f(x) \\ x \in \mathbb{R}^n, x(0) = x_0 \end{cases}$$

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

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

معرف شار (جریان-فلو) دستگاه می‌باشد. در این صورت منیفلد پایدار و ناپایدار را به صورت زیر

تعریف می‌کنیم [۲]

$$W_{Loc}^s(\bar{X}) = \{x \in U \subseteq \mathbb{R}^n \mid \phi_t(x)_{t \rightarrow +\infty} \rightarrow \bar{X}, \phi_t(x) \in U, \forall t \geq 0\},$$

$$W_{Loc}^u(\bar{X}) = \{x \in U \subseteq \mathbb{R}^n \mid \phi_t(x)_{t \rightarrow -\infty} \rightarrow \bar{X}, \phi_t(x) \in U, \forall t \leq 0\}.$$

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

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 این صورت

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

$$P^+(x) = \{\phi(t, x) : t \geq 0\}$$

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

$$P^-(x) = \{\phi(t, x) : t \leq 0\}$$

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_0 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]

$$1 - \lim_{t \rightarrow \infty} \phi_t(c) = X_0, \quad c \in S$$

$$2 - \lim_{t \rightarrow -\infty} \phi_t(c) = X_0, \quad c \in U$$

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 $f(X) = (f_1(X), \dots, f_n(X))$ ، 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 ریشه‌های 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 $t \rightarrow \infty$ به طور موضعی به آن نقطه تعادل نزدیک شوند، آن‌گاه آن نقطه تعادل پایدار نامیده می‌شود؛ X^* ناپایدار است هرگاه $t \rightarrow \infty$ 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 $f(X) = (f_1(X), \dots, f_n(X))$ یک تابع برداری روی \mathbb{R}^n باشد، آن‌گاه

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

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 $\det(A - \lambda I) = 0$ ، مقادیر ویژه λ_i ، $i = 1, 2, \dots, n$ ، 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 Π_n (مجموعه تمام چندجمله‌ای‌های از درجه نابیشتر از n) مقید می‌کنیم و ضرایب c_0, c_1, \dots, c_n را چنان می‌یابیم که چندجمله‌ای

$$P_n(x) = c_0 + c_1(x-a) + c_2(x-a)^2 + \dots + c_n(x-a)^n \quad (۳.۲)$$

تابع f را در نزدیکی نقطه $x = a$ تقریب کند، با این فرض که f در $x = a$ لاقلاً n بار مشتق‌پذیر است (در حالتی که 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

$$P_n^j(a) = f^{(j)}(a), \quad j = 0, 1, \dots, n, \quad (۴.۲)$$

$f_n^\circ(x) = f(x)$ و $P_n^\circ(x) = P_n(x)$ 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

$$\begin{cases} P_n(x) = c_0 + c_1(x-a) + c_2(x-a)^2 + \dots + c_n(x-a)^n \\ P_n'(x) = c_1 + 2c_2(x-a) + 3c_3(x-a)^2 + \dots + nc_n(x-a)^{n-1} \\ P_n''(x) = (2) \cdot (1)c_2 + (3) \cdot (2)c_3(x-a) + \dots + n(n-1)c_n(x-a)^{n-2} \\ \vdots \\ P_n^n(x) = n(n-1)\dots(2) \cdot (1)c_n \end{cases} \quad (5.2)$$

که $n+1$ معادله قطری بر حسب $n+1$ مجهول از ضرایب c_0, c_1, \dots, 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-1} را به دست آورد و به همین طریق از پایین به بالا عمل می‌کنیم تا c_0, c_1, \dots, c_n به دست آیند. روش دیگر حل دستگاه (۵.۲)، محاسبه

$P_n^j(a)$ برای $j = 0, 1, \dots, n$ است که با استفاده از (۴.۲) خواهیم داشت

$$c_0 = f(a), c_1 = f'(a), c_2 = \frac{f''(a)}{2}, \dots, c_n = \frac{f^n(a)}{n!}. \quad (6.2)$$

با جایگزین کردن (۶.۲) در (۳.۲) داریم

$$P_n(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2}(x-a)^2 + \dots + \frac{f^n(a)}{n!}(x-a)^n \quad (7.2)$$

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:

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \dots \quad (8.2)$$

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 $[0, \pi/2]$ کافی خواهد بود؛ زیرا از اتحادهای مثلثاتی می‌توانیم استفاده کنیم و $\cos x$ را برای هر مقدار دیگر x واقع در خارج بازه $[0, \pi/2]$ 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

$$R_{N,M}(x) = \frac{P_N(x)}{Q_M(x)}, \quad x \in I. \quad (9.2)$$

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 $x = 0$ پیوسته باشند. دو دلیل برای انتخاب دلخواه $x = 0$ 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

$$P_N(x) = p_0 + p_1x + p_2x^2 + \dots + p_Nx^N \quad (10.2)$$

$$Q_M(x) = q_0 + q_1x + q_2x^2 + \dots + q_Mx^M \quad (11.2)$$

چندجمله‌ای‌های (۱۰.۲) و (۱۱.۲) به طریقی ساخته می‌شوند که $f(x)$ و $R_{N,M}(x)$ در $x = 0$ با هم برابر باشند و مشتق‌های آن‌ها تا درجه $N + M$ نیز در $x = 0$ برابر باشند. در حالت $Q_0(x) = 1$ 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 $R_{N,M}(x)$ هنگامی که $P_N(x)$ 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

$$f(x) = c_0 + c_1x + c_2x^2 + \dots + c_nx^n + \dots \quad (۱۲.۲)$$

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

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

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 ($j = 1, \dots, M$) و p_j ($j = 0, 1, \dots, N$) به صورت زیر می‌نویسیم

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

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

توجه داشته باشید که در هر معادله مجموع اندیس‌های عامل‌های هر حاصل ضرب مقدار ثابتی است و این مجموع به تدریج از صفر تا $N + M$ افزایش می‌یابد. در معادله (۱۳.۲)، q_1, q_2, \dots, q_M و از $N + 1$ معادله (۱۵.۲) مقادیر p_1, p_2, \dots, 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 $i = n + 1, n + 2, \dots$ و q_j برای $j = 1, 2, \dots, M$ چون سری همگراست در حال کاهش هستند. بنابراین یک تقریب خطا به وسیله اولین جمله در طرف راست (۱۳.۲)، $a_{N+M+1}x^{N+M+1}$ به دست می‌آید که داریم

$$a_{N+M+1} = \sum_{j=0}^M c_{N+M+1-j} q_j \quad (۱۶.۲)$$

این تقریب خطا بیان می‌کند که 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 $x = 0$ وسط بازه‌ای نباشد که می‌خواهیم تقریب را روی آن بازه به دست آوریم با تغییر متغیر، $x = 0$ را به وسط آن بازه انتقال می‌دهیم. یادآوری می‌کنیم که برای $M = N$ و $M = N + 1$ ما کسیم خطا، مینیمم می‌شود. البته این روش توسط کامپیوتر بررسی شده و دلیل تحلیلی ندارد.

مثال ۱۰.۶.۲. تقریب پده زیر را بررسی کنید.

$$\cos x = R_{f,4} = \frac{15210 - 6900x^2 + 313x^4}{15120 + 660x^2 + 13x^4}$$

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 $R_{f,4}$ هر دو توابع زوج هستند، توان‌های x^2 را در بردارند.

اگر با $f(x) = \cos(x^{1/2})$ شروع کنیم

$$f(x) = 1 - \frac{x}{2} + \frac{x^2}{24} - \frac{x^3}{720} + \frac{x^4}{40320} - \dots,$$

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

$$\left(1 - \frac{x}{2} + \frac{x^2}{24} - \frac{x^3}{720} + \frac{x^4}{40320} - \dots\right) (1 + q_1x + q_2x^2) - p_0 - p_1x - p_2x^2 = \\ 0 + 0x + 0x^2 + 0x^3 + 0x^4 + c_5x^5 + c_6x^6 + \dots$$

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

$$\begin{aligned} 1 - p_0 &= 0 \\ -\frac{1}{2} + q_1 - p_1 &= 0, \\ \frac{1}{24} - \frac{1}{2}q_1 + q_2 - p_2 &= 0, \\ -\frac{1}{720} + \frac{1}{24}q_1 - \frac{1}{2}q_2 &= 0, \\ \frac{1}{40320} - \frac{1}{720}q_1 + \frac{1}{24}q_2 &= 0. \end{aligned}$$

از دو معادله آخر داریم

$$q_2 = \frac{13}{15210}, \quad q_1 = \frac{11}{252}$$

و از سه معادله اول نیز p_0 ، p_1 و p_2 را به دست می‌آوریم

$$p_0 = 1, \quad p_1 = -\frac{115}{252}, \quad p_2 = \frac{313}{15210}.$$

در نتیجه $R_{4,4}$ به صورت زیر به دست می‌آید

$$R_{4,4} = \frac{15210 - 6900x^2 + 313x^4}{15120 + 660x^2 + 13x^4}.$$

تقریب $R_{4,4}$ بسط مک لورن تابع $f(x)$ است.

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

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

۲- 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 توزیع شده 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 قرار می‌گیرد.

در این فصل یک مدل اپیدمی دویخشی 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

^۱Platform

^۲Mirai 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 مانند آسیب‌پذیر، 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 آسیب‌پذیر 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

^۳Yang and Yang

^۴Patches

مخرب توسط کشری^۵، میشر^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 می‌کنید 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 برهم‌کنش 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

^۵Keshri

^۶Mishra

^۷Mallick

^۸Wireless Nano Sensor Network

^۹Brenden O'Brien

مناسب نیستند، مناسب نبوده و حفاظت پیش فرض 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 توزیع شده 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 کنترل کننده ایجاد می‌کند. در نهایت، به محض دریافت یک فرمان از واحد کنترل کننده، 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 توزیع شده از طریق گره‌های بی‌سیم رایج‌تر هستند.

مطابق گزارش روندهای DDoS سه ماهه چهارم ۲۰۱۵ Verisign [۵۱]، تقریباً ۷۵ درصد کل حملات 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 سازمان یافته 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 بات نت 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 620 Gbps رسید. سپس مورد دوم، حمله به شرکت میزبان فرانسوی OVH بود که به 1 Tbps رسید. در نهایت سومین مورد حمله IoT که در کانون توجه قرار گرفت، حمله DDoS روی DSN ارائه‌دهنده DYN بود که PayPal، Twitter، Netflix و وبسایت‌های دیگر را مختل کرد [۴۸].

بات نت میرای تقریباً شامل 120000 و 150000 دستگاه IoT است که جهت اجرای حملات DDoS به ترتیب 620 Gbps و 1 Tbps مورد استفاده قرار می‌گیرد [۴۴]. به گفته گارتنر، $8/4$ بلیون IP، ابزارهای IoT را فعال کرد که این نرخ مورد استفاده در سراسر جهان در سال 2017 ، 31 درصد بیشتر از سال 2016 بود و تا سال 2020 به $20/4$ بلیون 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 قابل‌تصور 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 (آسیب‌پذیر-آلوده-بازیابی شده) و SIS (آسیب‌پذیر-آلوده-آسیب‌پذیر) دو مدل اپیدمی کلاسیک ارائه شده توسط کرماک و مک‌کندریک^{۱۰} برای تجزیه و تحلیل شیوع بیولوژیکی بیماری‌ها به ترتیب در سال 1927 و 1932

^{۱۰} Mckendrick

هستند [۲۴، ۲۵]. مدل SIR برای دستیابی افراد مورد نیاز به مصونیت در برابر همان حمله، بسیار کاربردی تر است. در حالی که 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 عمده‌تاً 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.

تحرك یکی از ویژگی‌های اساسی بخش مهمی از گره‌های IoT در هر شبکه بی‌سیم است. با توجه به این تحرك، گره‌های بی‌سیم اغلب به اینترنت وصل یا قطع می‌شوند. به طور کلی به دلیل تحرك، 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

می کنند.

بقیه این فصل به صورت زیر سازماندهی می شود:

بخش ۱.۳ مدل اپیدمی را فرمول بندی می کند. بخش ۲.۳ مدل را بررسی می کند. بخش ۳.۳ شبیه سازی را تحلیل می کند و در نهایت در بخش ۴.۳ به نتیجه گیری فصل می پردازد.

۱.۳ فرضیه ها و فرمول بندی مدل

در این فصل، یک مدل ریاضی بر اساس فرضیه های زیر ارائه می دهیم.

(H۱): هر گره حمله کننده (آسیب پذیری یا آلوده)، به دلیل خاموشی، با نرخ ثابت $\alpha > 0$ از اینترنت قطع می شود تا به گره های حمله کننده خارجی، متصل شوند.

(H۲): همان طور که در حمله میرای مشاهده شد، دستگاه های IoT آلوده می توانند با راه اندازی مجدد آنها، تمیز شوند [۴۸]، فرض می گیریم که هر گره حمله کننده خارجی به اینترنت متصل است و تبدیل به گره حمله کننده آسیب پذیر در نرخ ثابت $\sigma > 0$ می شود.

(H۳): از آن جا که مدل ما شامل پویایی حیاتی است، هر گره حمله کننده (آسیب پذیر، آلوده یا خارجی) با احتمال $\mu > 0$ از بین می رود.

(H۴): همچنین μ نرخ افزایش از گره های جدید در قسمت گره خارجی می باشد.

(H۵): هر گره آسیب پذیری (حمله کننده یا هدفمند) توسط یک گره حمله کننده با نرخ ثابت $\beta > 0$ آلوده به شمار می رود.

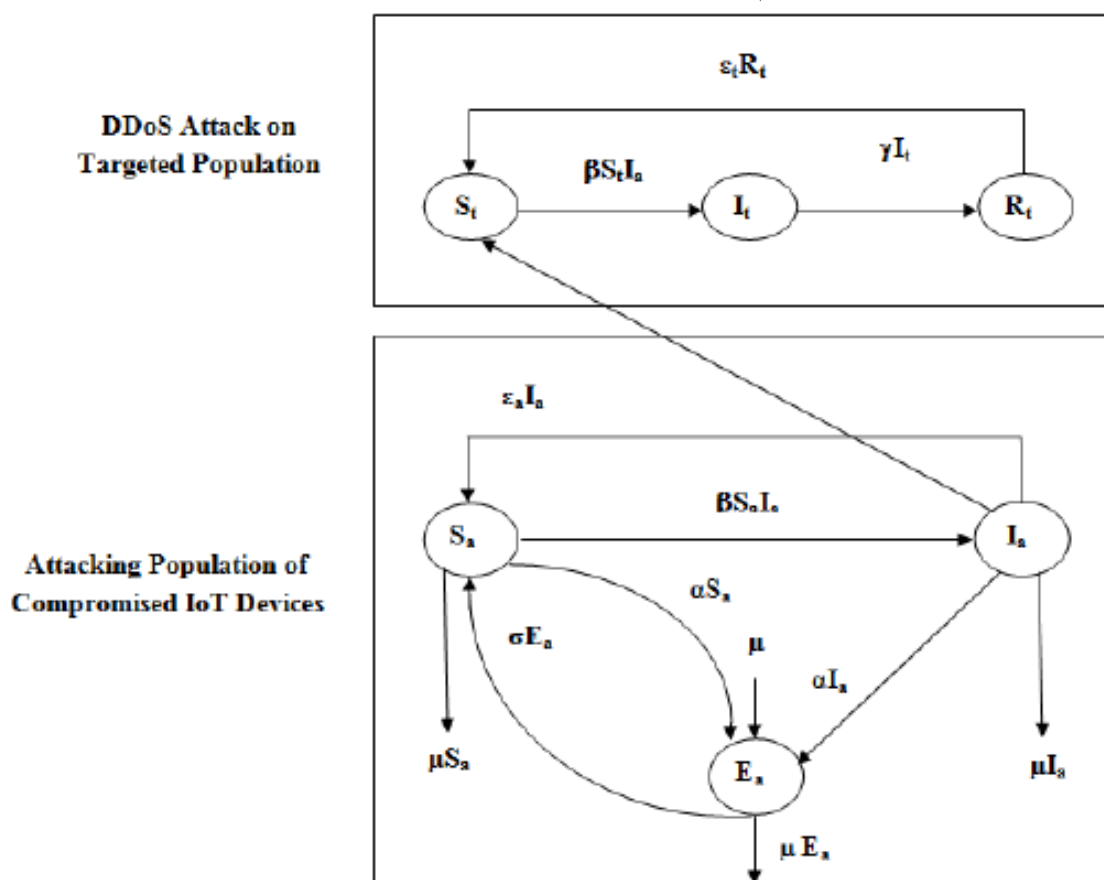
(H۶): هر گره حمله کننده غیر آلوده دوباره تبدیل به گره حمله کننده آسیب پذیر با نرخ ثابت $\varepsilon_a > 0$ می شود.

(H۷): با توجه به اثر درمان مناسب، هر گره هدفمند آلوده تبدیل به گره هدفمند بازیابی شده با نرخ ثابت $y > 0$ می شود.

(H۸): به دلیل مصونیت موقت، گره هدفمند بازیابی شده دوباره تبدیل به گره آسیب پذیر هدفمند با نرخ ثابت $\varepsilon_t > 0$ می شود.

بر اساس این فرضیه ها، یک مدل اپیدمی ارائه می دهیم که از پنج جنبه متفاوت مانند ابزارهای IoT، گره های خارجی و داخلی، شبکه بی سیم، حمله توزیع شده و منبع هدف گذاری شده مانند شکل ۱.۳ حاصل می شود.

شکل ۱.۳: نمایش شماتیک یک مدل از حمله توزیع شده روی منبع هدفمند از طریق گره IoT داخلی و خارجی در شبکه بی سیم.



ساختار مدل ارائه شده دارای دو بخش است. ابتدا، مجرمان، یک ارتش زامبی به دست می آورند که معمولاً به عنوان بات نت توسط گره های بی سیم هدفمند آسیب پذیر از جمعیت حمله کننده شناخته می شوند. دوم، کل ارتش زامبی ها به صورت جمعی و همزمان، یک جمعیت هدف خاص تدارک می بیند.

برای جمعیت هدف، دستگاه معادلات دیفرانسیل معمولی که نرخ تغییرات بخش های مختلف طبق فرضیات بالا را توصیف می کنند، در شکل ۱.۳ نشان داده شده است که به صورت زیر فرمول بندی می شود

$$\begin{aligned}\frac{dS_t}{dt} &= -\beta S_t I_a + \varepsilon_t R_t, \\ \frac{dI_t}{dt} &= \beta S_t I_a - \gamma I_t, \\ \frac{dR_t}{dt} &= \gamma I_t - \varepsilon_t R_t\end{aligned}\quad (1.3)$$

که در آن $S_t(t) + I_t(t) + R_t(t) = 1$.

مشابهاً، برای جمعیت حمله کننده، دستگاه معادلات دیفرانسیل معمولی که نرخ تغییرات بخش های مختلف را توصیف می کند، به صورت زیر فرمول بندی می شود

$$\begin{aligned}\frac{dS_a}{dt} &= -\beta S_a I_a - \mu S_a + \varepsilon_a I_a + \sigma E_a - \alpha S_a, \\ \frac{dI_a}{dt} &= \beta S_a I_a - \mu I_a - \varepsilon_a I_a - \alpha I_a, \\ \frac{dE_a}{dt} &= \alpha S_a + \alpha I_a - \sigma E_a + \mu - \mu E_a\end{aligned}\quad (2.3)$$

که در آن $S_a(t) + I_a(t) + E_a(t) = 1$.

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

داد

$$\begin{aligned} \frac{dS_t}{dt} &= -\beta S_t I_a + \varepsilon_t (1 - S_t - I_t), \\ \frac{dI_t}{dt} &= \beta S_t I_a - \gamma I_t, \\ \frac{dI_a}{dt} &= \beta (1 - I_a - E_a) I_a - \mu I_a - \varepsilon_a I_a - \alpha I_a, \\ \frac{dE_a}{dt} &= \alpha (1 - I_a - E_a) + \alpha I_a - \sigma E_a + \mu - \mu E_a. \end{aligned} \quad (3.3)$$

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

$$\Psi = \{ (S_t, I_t, I_a, E_a) \in R^4 : S_t > 0,$$

$$I_t \geq 0, I_a \geq 0, E_a \geq 0, S_t + I_t \leq 1, I_a + E_a \leq 1 \}$$

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_0) 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_0 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 $R_0 > 1$ باشد، هر گره آلوده به طور متوسط بیش از یک گره مستعد را آلوده می‌کند و از این رو آلودگی همچنان ادامه دارد، در حالی که اگر $R_0 \leq 1$ باشد، هر کدام گره آلوده، به طور متوسط کمتر از یک گره مستعد را آلوده می‌کند و از این رو آلودگی از بین می‌رود [۲۱]. به عبارت دیگر، عدد تکثیر R_0 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 $R_0 > 1$ لذا عدد تکثیر R_0 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_0 نمایش می‌دهند.

در واقع زمانی که هر گره آلوده به طور متوسط کمتر از یک گره مستعد را آلوده کند یعنی $R_0 \leq 1$ باشد، سرانجام آلودگی از بین خواهد رفت و اگر $R_0 > 1$ 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 $\frac{dI_a}{dt} > 0$ و $\frac{dI_t}{dt} > 0$ شرایط اساسی برای ایجاد یک اپیدمی هستند، عدد تکثیر پایه برای جمعیت هدف (R_{ot}) و برای جمعیت حمله‌کننده (R_{oa}) به شرح زیر است

$$R_{ot} = \frac{\beta}{y} \quad \text{و} \quad R_{oa} = \frac{\beta}{(\mu + \varepsilon_a + \alpha)}$$

با ادغام هر دو رابطه خواهیم داشت

$$R_0 = \sqrt{\frac{\beta^2}{(\mu + \varepsilon_a + \alpha)y}} \quad (4.3)$$

مدل اپیدمی عمومی برای شبکه بی‌سیم می‌تواند این چنین باشد:

فرض کنید $x = (x_1, x_2, \dots, x_n)^T$ که در آن x_i تعداد گره‌ها در بخش i -ام باشد و فرض می‌شود بخش‌ها مرتب شده‌اند به طوری که 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

$$X_s = \{x \geq 0 \mid x_i = 0; i = 1, 2, \dots, m\}.$$

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

$$\dot{x}_i = f_i(x) = F_i(x) - V_i(x) \quad (5.3)$$

که در آن $V_i = V_i^- - V_i^+$ ، $i = 1, 2, \dots, m$ و فرض می‌شود V_i و F_i در ملزومات (۱) تا (۴) صدق کند:

$$(1) \text{ اگر } x \geq 0, \text{ آن‌گاه } V_i^+, V_i^-, F_i \geq 0 \text{ برای } i = 1, 2, \dots, m.$$

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

$$(2) \text{ اگر } x_i = 0, \text{ آن‌گاه } V_i^-(x) = 0. \text{ به ویژه اگر } x \in X_s, \text{ آن‌گاه } V_i^- = 0 \text{ برای } i = 1, 2, \dots, m.$$

چون از n بخش، m تایی، آن‌ها آلوده هستند. با توجه به این که بروز آلودگی برای بخش‌های غیر آلوده صفر است، لذا

$$(3) \text{ اگر } i > m, F_i(x) = 0.$$

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 $x \in X_s$ ، آن گاه $V_i^+(x) = 0$ و $F_i(x) = 0$ برای $i = 1, 2, \dots, m$ طبق شرط (۲).

لذا مدل انتقال آلودگی با توجه به رابطه (۵.۳)، بر اساس شرایط (۱) و (۲) به صورت زیر

خواهد بود

$$f_i(x) = F_i(x) + V_i^+(x) - V_i^-(x) \xrightarrow{V_i^-(x)=0} f_i(x) = F_i(x) + V_i^+(x) \geq 0$$

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

شبکه‌ای را نزدیک به نقطه تعادل در نظر بگیرید. آن گاه 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 $1 \leq i$ و $j \leq m$. حال که ماتریس‌های F و V به دست آمدند، FV^{-1} را

ماتریس نسل بعدی نامیدند و به صورت $R_0 = FV^{-1}$ تعریف کردند.

دستگاه (۳.۳) را به صورت زیر می‌نویسیم

$$\begin{bmatrix} \dot{I}_t \\ \dot{I}_a \\ \dot{E}_a \end{bmatrix} = \begin{bmatrix} \beta S_t I_a \\ \beta I_a \\ 0 \end{bmatrix} - \begin{bmatrix} +yI_t \\ +\beta I_a + \beta E_a I_a + \mu I_a + \varepsilon_a I_a + \alpha I_a \\ -\alpha(1 - I_a - E_a) - \alpha I_a + \sigma E_a - \mu + \mu E_a \end{bmatrix}$$

در این صورت داریم

$$F = \left[\frac{\partial f_i}{\partial x_j}(\bar{x}) \right] = \begin{bmatrix} 0 & \beta & 0 \\ 0 & \beta & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

$$V = \left[\frac{\partial V_i}{\partial x_j}(\bar{x}) \right] = \begin{bmatrix} 0 & y & 0 \\ \mu + \varepsilon_a + \alpha & 0 & 0 \\ 0 & 0 & \alpha + \sigma + \mu \end{bmatrix}$$

$$V^{-1} = \frac{1}{y(-\beta + \mu + \varepsilon_a + \alpha)(\alpha + \sigma + \mu)} \begin{bmatrix} \circ & \circ & \circ \\ y(\mu + \varepsilon_a + \alpha)(\alpha + \sigma + \mu) & y(\alpha + \sigma + \mu) & \circ \\ \circ & \circ & y(\mu + \varepsilon_a + \alpha) \end{bmatrix}$$

بنابراین

در نتیجه داریم

$$FV_t^{-1} = \begin{bmatrix} \circ & \beta & \circ \\ \circ & \beta & \circ \\ \circ & \circ & \circ \end{bmatrix} \begin{bmatrix} \circ & \frac{1}{\mu + \varepsilon_a + \alpha} & \circ \\ \frac{1}{y} & \circ & \circ \\ \circ & \circ & \frac{1}{\alpha + \sigma + \mu} \end{bmatrix} = \begin{bmatrix} \beta/y & \circ & \circ \\ \beta/y & \circ & \circ \\ \circ & \circ & \circ \end{bmatrix}$$

از طرف دیگر می‌دانیم

$$\begin{cases} \dot{s}_t = -\beta s_t I_a + \varepsilon_t (\lambda - s_t - I_t) \\ \dot{I}_a = \beta I_a - \beta I_a^Y - \beta E_a I_a - \mu I_a - \varepsilon_a I_a - \alpha I_a \\ \dot{I}_t = \beta s_t I_a - y I_t \\ \dot{E}_a = \alpha (\lambda - I_a - E_a) + \alpha I_a - \sigma E_a + \mu - \mu E_a \end{cases}$$

در نتیجه

$$\begin{bmatrix} \dot{I}_a \\ \dot{I}_t \\ \dot{E}_a \end{bmatrix} = \begin{bmatrix} \beta I_a \\ \beta s_t I_a \\ \circ \end{bmatrix} - \begin{bmatrix} +\beta I_a^Y + \beta E_a I_a + \mu I_a + \varepsilon_a I_a + \alpha I_a \\ +y I_t \\ -\alpha (\lambda - I_a - E_a) - \alpha I_a + \sigma E_a - \mu + \mu E_a \end{bmatrix}$$

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

بنابراین

$$\begin{aligned} \left[\frac{\partial V_i}{\partial x_j} \right] &= \begin{bmatrix} \mu + \varepsilon_a + \alpha & \circ & \circ \\ \circ & y & \circ \\ \circ & \circ & \alpha + \sigma + \mu \end{bmatrix} \\ \Rightarrow V^{-1} &= \begin{bmatrix} \frac{1}{\mu + \varepsilon_a + \alpha} & \circ & \circ \\ \circ & \frac{1}{y} & \circ \\ \circ & \circ & \frac{1}{\alpha + \sigma + \mu} \end{bmatrix} \\ \Rightarrow V^{-1} &= \frac{1}{y(\varepsilon_a + \alpha + \mu)(\mu + \sigma + \alpha)} \begin{bmatrix} y(\alpha + \sigma + \mu) & \circ & \circ \\ \circ & (\mu + \varepsilon_a + \alpha)(\mu + \alpha + \sigma) & \circ \\ \circ & \circ & y(\mu + \varepsilon_a + \alpha) \end{bmatrix} \end{aligned}$$

در این صورت داریم

$$FV_a^{-1} = \begin{bmatrix} \beta & 0 & 0 \\ \beta & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ \mu + \varepsilon_a + \alpha & 0 & 0 \\ y & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \alpha + \sigma + \mu \end{bmatrix} = \begin{bmatrix} \frac{\beta}{\mu + \varepsilon_a + \alpha} & 0 & 0 \\ \frac{\beta}{\mu + \varepsilon_a + \alpha} & 0 & 0 \\ \frac{\beta}{\mu + \varepsilon_a + \alpha} & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

و این همان مقادیر مورد نظر است

$$R_{oa} = \frac{\beta}{\mu + \varepsilon_a + \alpha},$$

$$R_{ot} = \frac{\beta}{y}.$$

۲.۲.۳ وجود پایداری موضعی نقاط تعادل

قضیه ۱.۲.۳. دستگاه (۳.۳) یک نقطه تعادل عاری از آلودگی $E_o(1, 0, 0, 0)$ و همچنین یک

نقطه تعادل اندمیک $E^*(S_t^*, I_t^*, I_a^*, E_a^*)$ را قبول می کند، که تنها وقتی که $\beta > (\mu + \varepsilon_a + \alpha)$ باشد، موجود است.

برهان. برای محاسبه نقاط تعادل، داریم

$$\frac{dS_t}{dt} = 0; \quad \frac{dI_t}{dt} = 0; \quad \frac{dI_a}{dt} = 0; \quad \frac{dE_a}{dt} = 0.$$

یعنی

$$-\beta S_t I_a + \varepsilon_t (1 - S_t - I_t) = 0,$$

$$\beta S_t I_a - y I_t = 0,$$

$$\beta (1 - I_a - E_a) I_a - \mu I_a - \varepsilon_a I_a - \alpha I_a = 0, \quad (۶.۳)$$

$$\alpha (1 - I_a - E_a) + \alpha I_a - \sigma E_a + \mu - \mu E_a = 0.$$

^{۱۱}نقطه تعادل عاری از آلودگی $E_o = 0$ و $I_a = 0$, $I_t = 0$.

پس از حل معادلات فوق، نقاط تعادل $E_0(1, 0, 0, 0)$ 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

$$aI_a^{*2} + bI_a^* + c = 0 \quad (۷.۳)$$

که در آن

$$a = \beta, \quad b = -\frac{[(\beta - \mu - \varepsilon_a - \alpha)(\alpha + \sigma + \mu) - \beta(\alpha + \mu)]}{(\alpha + \sigma + \mu)}, \quad c = 0.$$

فرض کنید تابع ممین (۷.۳) به صورت $\Delta = b^2 - 4ac$ باشد. اگر $b \geq 0$ ، آن گاه (۷.۳) هیچ

جواب مثبتی ندارد. همچنین اگر $\Delta < 0$ آن گاه (۷.۳) هیچ جواب حقیقی ندارد. اما اگر $b < 0$ و

$\Delta > 0$ ، آن گاه (۷.۳) دارای دو جواب مثبت است. توجه داشته باشید که اگر $\beta > (\mu + \varepsilon_a + \alpha)$

یا معادلاً $R_{0a} > 1$ باشد، آن گاه $b < 0$ برقرار است.

بنابراین داریم

$$\begin{aligned} S_t^* &= \frac{\varepsilon_t}{\left[\frac{(\beta - \mu - \varepsilon_a - \alpha)(\alpha + \sigma + \mu) - \beta(\alpha + \mu) \pm \Delta}{2(\alpha + \sigma + \mu)} + \left(1 + \frac{\beta}{y}\right) \varepsilon_t \right]} \\ I_t^* &= \frac{\varepsilon_t}{y \left[1 + \frac{2\varepsilon_t(1 + \beta/y)(\alpha + \sigma + \mu)}{(\beta - \mu - \varepsilon_a - \alpha)(\alpha + \sigma + \mu) - \beta(\alpha + \mu) \pm \Delta} \right]} \\ I_a^* &= \frac{(\beta - \mu - \varepsilon_a - \alpha)(\alpha + \sigma + \mu) - \beta(\alpha + \mu) \pm \Delta}{2\beta(\alpha + \sigma + \mu)} \\ E_a^* &= \frac{(\alpha + \mu)}{(\alpha + \sigma + \mu)}. \end{aligned} \quad (۸.۳)$$

□

۳.۲.۳ پایداری موضعی نقطه تعادل عاری از آلودگی

قضیه ۳.۲.۳. اگر $R_{oa} \leq 1$ باشد، نقطه تعادل عاری از آلودگی $E_0(1, 0, 0, 0)$ سیستم (۳.۳) به طور موضعی و مجاناً پایدار در Ψ است و در صورتی که $R_{oa} > 1$ باشد، ناپایدار است.

برهان. در نقطه تعادل عاری از آلودگی $E_0(1, 0, 0, 0)$ از سیستم (۶.۳)، ماتریس ژاکوبین آن به

شکل زیر است

$$J_{IFE} = \begin{pmatrix} -\varepsilon_t & -\varepsilon_t & -\beta & 0 \\ 0 & -y & \beta & 0 \\ 0 & 0 & \beta - (\mu + \varepsilon_a + \alpha) & 0 \\ 0 & 0 & 0 & -(\alpha + \sigma + \mu) \end{pmatrix} \quad (9.3)$$

معادله مشخصه ماتریس ژاکوبی فوق به شکل زیر محاسبه می گردد

$$(\lambda + \varepsilon_t)(\lambda + y)(\lambda - \beta + \mu + \varepsilon_a + \alpha)(\lambda + \alpha + \sigma + \mu) \quad (10.3)$$

از این رو مقادیر ویژه رابطه (۹.۳)، برابر است با

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

از این چهار مقادیر ویژه λ_1, λ_2 و λ_4 منفی و مقدار ویژه بعدی؛ یعنی λ_3 نیز هرگاه شرط

$\beta < (\mu + \varepsilon_t + \alpha)$ برقرار باشد، منفی می شود که معادل است با $R_{oa} \leq 1$. بنابراین، نقطه تعادل

عاری از آلودگی E_0 به صورت موضعی مجاناً در Ψ پایدار است. این نقطه تعادل می تواند ناپایدار

باشد، یعنی $R_{oa} > 1$ اگر λ_3 مثبت باشد. به عبارت دیگر، اگر $\beta > (\mu + \varepsilon_a + \alpha)$ برقرار باشد،

نقطه تعادل E_0 ناپایدار می شود و نقطه تعادل اندمیک یکتا E^* در درون Ψ ظاهر می شود و این نقطه

به طور موضعی مجاناً پایدار است. از این رو اثبات می شود که E_0 به طور موضعی مجاناً پایدار

□

است اگر $R_{oa} \leq 1$ و ناپایدار است اگر $R_{oa} > 1$.

۴.۲.۳ پایداری موضعی نقطه تعادل اندمیک

قضیه ۳.۲.۳. اگر $R_{oa} > 1$ ، آن گاه یک نقطه تعادل اندمیک یکتایی مانند $E^*(S_t^*, I_t^*, I_a^*, E_a^*)$

وجود دارد که به طور موضعی مجاناً 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

$$J_{EE} = \begin{pmatrix} -(\beta I_a^* + \varepsilon_t) & -\varepsilon_t & -\beta S_t^* & \circ & \circ & \circ \\ \beta I_a^* & -y & \beta S_t^* & \circ & \circ & \circ \\ \circ & \circ & -\beta(\gamma I_a^* E_a^*) + \beta - (\mu + \varepsilon_a + \alpha) & \circ & \circ & \circ \\ \circ & \circ & \circ & \circ & \circ & -(\alpha + \sigma + \mu) \end{pmatrix} \quad (۱۱.۳)$$

به واسطه مقادیر ویژه از رابطه (۱۱.۳)، $\lambda_4 = -(\alpha + \sigma + \mu) < 0$ منفی است که با شرط $R_{oa} > 1$

معادل است. دیگر مقدار ویژه $\lambda_3 = -\beta(\gamma I_a^* + E_a^*) + \beta - (\mu + \varepsilon_a + \alpha)$ است. بعد از انجام

محاسبات داریم $\lambda_3 < 0$ اگر $\beta > (\mu + \varepsilon_a + \alpha)$ یا به طور معادل $R_{oa} > 1$.

دو مقدار ویژه دیگر، ریشه‌های معادله مشخصه زیر هستند

$$\lambda^2 + [y - (\beta I_a^* + \varepsilon_t)]\lambda + [\beta I_a^*(y + \varepsilon_t) + \varepsilon_t y] = 0. \quad (۱۲.۳)$$

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 $R_{oa} > 1$. \square

۳.۳ شبیه‌سازی عددی و بحث درباره آن‌ها

نتیجه جالب مدل ما این است که موفقیت یا شکست حمله توزیع شده به منابع هدفمند، فقط بستگی

به R_{oa} دارد. بنابراین، در هر دو مثال ذکر شده در زیر، مدل ما بر اساس $R_{oa} < 1$ یا $R_{oa} > 1$

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 این جا نقطه اولیه به صورت زیر در نظر گرفته شده است

$$S_t = 0.97, I_t = 0.02, R_t = 0.01, S_a = 0.55, I_a = 0.2, E_a = 0.25$$

با مقادیر پارامتر

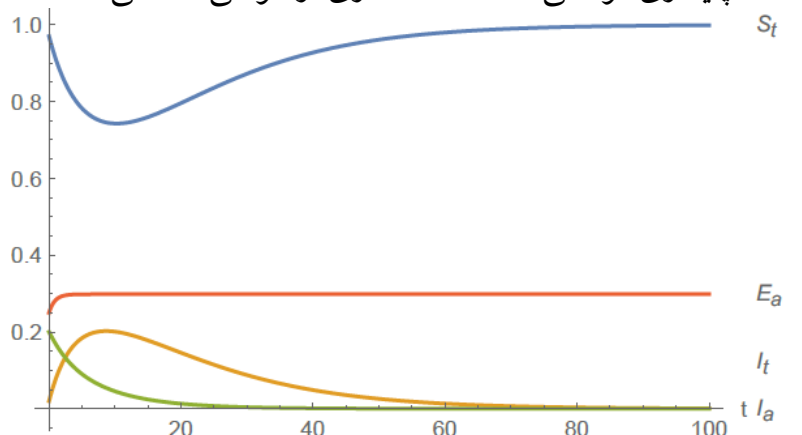
$$\beta = 0/35, \varepsilon_t = 0/2, y = 0/07, \mu = 0/12, \varepsilon_a = 0/02, \sigma = 0/8, \alpha = 0/22.$$

مقدار R_{oa} برابر است با $0/97$ و $R_{oa} < 1$. که این یعنی نقطه تعادل E_0 پایدار می شود. با استفاده از نرم افزار 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
0	0/97	0/02	0/2	0/25
5/38	0/7756	0/1881	0/0853	0/2981
10/47	0/7426	0/1995	0/0427	0/2982
15/52	0/7627	0/1747	0/0227	0/2982
20/18	0/7973	0/1446	0/0129	0/2982
25/12	0/8367	0/1138	0/0072	0/2982
30/25	0/8740	0/0864	0/0039	0/2982
35/45	0/9054	0/0640	0/0021	0/2982
40/27	0/9287	0/0478	0/00125	0/2982
45/03	0/9467	0/0355	0/00072	0/2982
55/4	0/9724	0/1819	0/000221	0/2982
60/36	0/98011	0/01309	0/000125	0/2982
65/41	0/9857	0/00933	0/0000705	0/2982
70/58	0/9899	0/006577	0/00003905	0/2982
75/7	0/9929	0/004639	0/00002174	0/2982
80/21	0/9947	0/003406	0/0000129	0/2982
85/74	0/9964	0/00232	$6/89 \times 10^{-6}$	0/2982
90/09	0/9973	0/001723	$4/19 \times 10^{-6}$	0/2982
95/02	0/9981	0/001225	$2/38 \times 10^{-6}$	0/2982
100	0/9986	0/0008673	$1/34 \times 10^{-6}$	0/2982

شکل ۲.۳: پایداری موضعی نقطه تعادل عاری از آلودگی هنگامی که $R_{oa} < 1$.



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 این جا نقطه اولیه به صورت زیر در نظر گرفته شده است

$$S_t = 0.97, I_t = 0.02, R_t = 0.01, S_a = 0.55, I_a = 0.2, E_a = 0.25$$

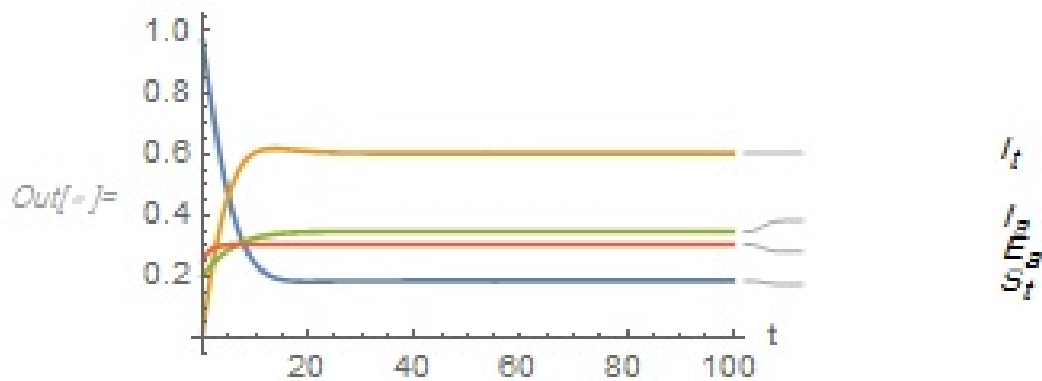
$$\beta = 0.65, \varepsilon_t = 0.2, y = 0.07, \mu = 0.12, \varepsilon_a = 0.005, \sigma = 0.5, \alpha = 0.1.$$

مقدار R_{oa} برابر است با ۲/۸۹ و $R_{oa} > 1$. در شکل ۳.۳، مؤلفه I_a و I_t در مقادیر غیر صفر پایدار شده‌اند. این‌جا پایداری نقطه تعادل اندمیک نشان داده می‌شوند.

جدول ۲.۳: توزیع جمعیت از کلاس های مختلف گره ها بر حسب زمان برای سناریوی یک حمله موفق ($R_{oa} > 1$).

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 هنگامی که $R_{oa} > 1$.



۴.۳ نتیجه گیری

در این فصل، یک مدل اپیدمی برای حمله DDoS از طریق دستگاه های IoT در منابع هدفمند توسعه داده شده است و همه دینامیک های 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 حالی که 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_0 به صورت موضعی پایدار است هنگامی که $R_{0a} < 1$.

(۲) نقطه تعادل اندمیک E^* به صورت موضعی پایدار است وقتی $R_{0a} > 1$.

علاوه بر این، 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]:

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

چند جمله‌ای‌های $\sum_{i=0}^N a_i t^i$ 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

^۱Mei Peng

N : کل جمعیت رایانه‌های موجود در شبکه،

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

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

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

β_1 : نرخ تماس رایانه‌های آسیب پذیر با رایانه‌های آلوده،

β_2 : نرخ تماس رایانه‌های آسیب پذیر با رایانه‌های در معرض خطر،

μ : نرخ حذف یک رایانه از شبکه،

r : نرخ بازیابی رایانه‌های آلوده که درمان می‌شوند.

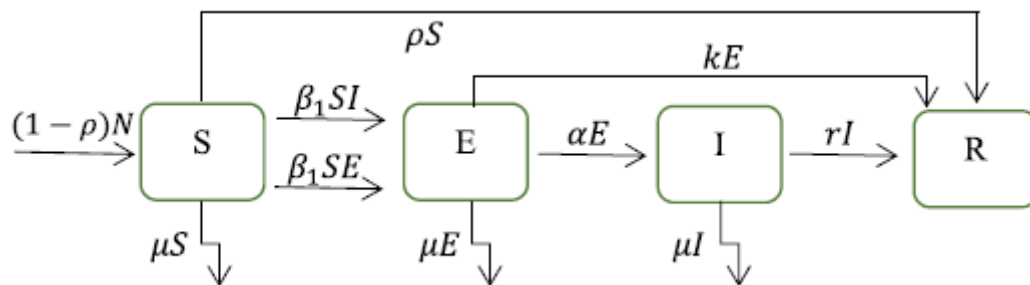
سیستم معادلات حاکم برای مدل به صورت زیر ارائه شده است

$$\begin{cases} S'(t) = (1-p)N - \beta_1 S(t)I(t) - \beta_2 S(t)E(t) - pS(t) - \mu S(t), \\ E'(t) = \beta_1 S(t)I(t) + \beta_2 S(t)E(t) - kE(t) - \alpha E(t) - \mu E(t), \\ I'(t) = \alpha E(t) - rI(t) - \mu I(t), \\ R'(t) = pS(t) + kE(t) + rI(t). \end{cases} \quad (1.4)$$

در اینجا

$$S(t) + E(t) + I(t) + R(t) = N(t). \quad (2.4)$$

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



فرض کنید

$$X_1(t) = A - \beta_1 S(t)I(t) - \beta_2 S(t)E(t) - aS(t),$$

$$X_2(t) = \beta_1 S(t)I(t) + \beta_2 S(t)E(t) - bE(t),$$

$$X_3(t) = \alpha E(t) + cI(t),$$

$$A = (1-p)N, \quad a = p + \mu, \quad b = k + \alpha + \mu, \quad c = r + \mu.$$

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

$$\begin{cases} S'(t) = X_1(t), \\ E'(t) = X_2(t), \\ I'(t) = X_3(t). \end{cases} \quad (3.4)$$

شرایط اولیه به صورت زیر هستند

$$S_0 = S(0) = 50, \quad E_0 = E(0) = 40, \quad I_0 = I(0) = 20.$$

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 تابع 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

$$S(t) \approx \frac{\sum_{i=0}^N a_i t^i}{1 + \sum_{j=0}^M b_j t^j}, \quad E(t) \approx \frac{\sum_{i=0}^N c_i t^i}{1 + \sum_{j=0}^M d_j t^j}, \quad I(t) \approx \frac{\sum_{i=0}^N e_i t^i}{1 + \sum_{j=0}^M f_j t^j}. \quad (4.4)$$

با توجه به شرایط اولیه $S(t_0) = S_0$ ، $E(t_0) = E_0$ ، $I(t_0) = I_0$ ، اگر $t_0 = 0$ ، آن‌گاه داریم

$$a_0 = S_0, \quad c_0 = E_0, \quad e_0 = I_0. \quad (5.4)$$

که پیش‌تر مقادیر $I_0 = 20$, $E_0 = 40$, $S_0 = 50$ و با استفاده از نرم‌افزار کدنویسی در متمتیکا مقادیر $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2, e_1, e_2, f_1, f_2$ برای تقریب پده مرتبه $(2, 2)$ 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 $P_{2,2}$ برای هر یک از روابط (۴.۴) به صورت زیر به دست می‌آید

$$S_{2,2}(t) \approx \frac{a_0 + a_1 t + a_2 t^2}{1 + b_1 t + b_2 t^2} = \frac{50 - 1076t - 0.516816t^2}{1 - 1/3333t + 0.3333t^2},$$

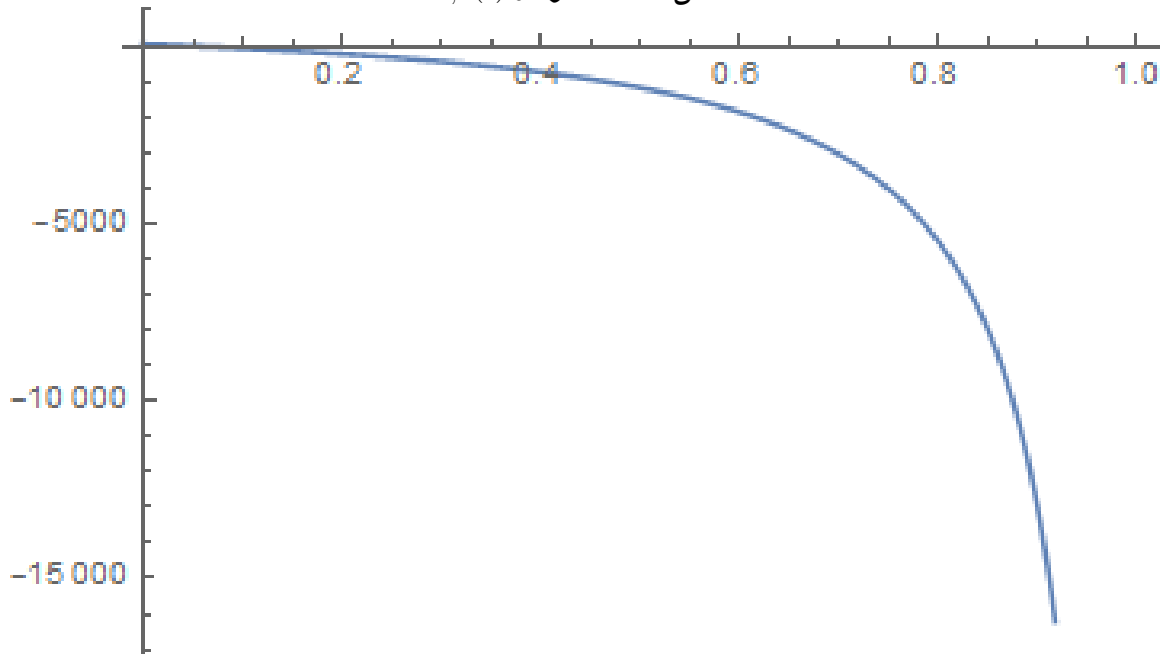
$$E_{2,2}(t) \approx \frac{c_0 + c_1 t + c_2 t^2}{1 + d_1 t + d_2 t^2} = \frac{40 + 1062/4t + 0.415764t^2}{1 - 1/3333t + 0.3333t^2},$$

$$I_{2,2}(t) \approx \frac{e_0 + e_1 t + e_2 t^2}{1 + f_1 t + f_2 t^2} = \frac{20 + 12/8t - 0.040184t^2}{1 - 0.731139t + 0.121693t^2}.$$

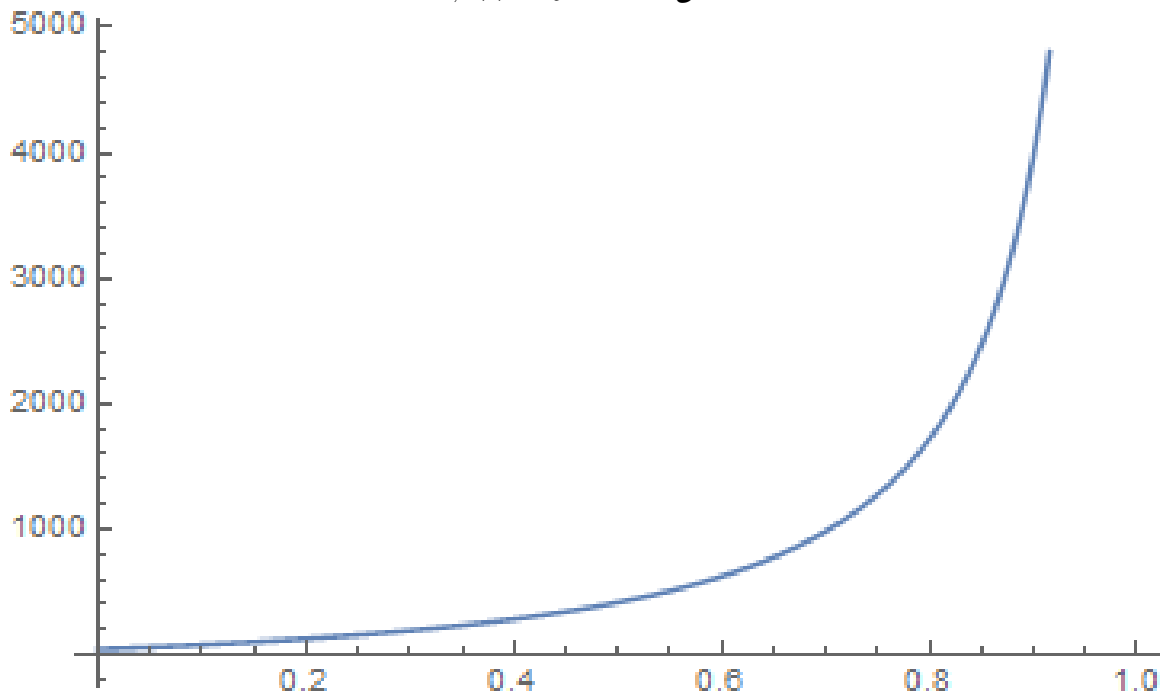
تقریب‌های $S_{2,2}(t)$, $E_{2,2}(t)$ و $I_{2,2}(t)$ بسط مک‌لورن تابع $f(t)$ هستند.

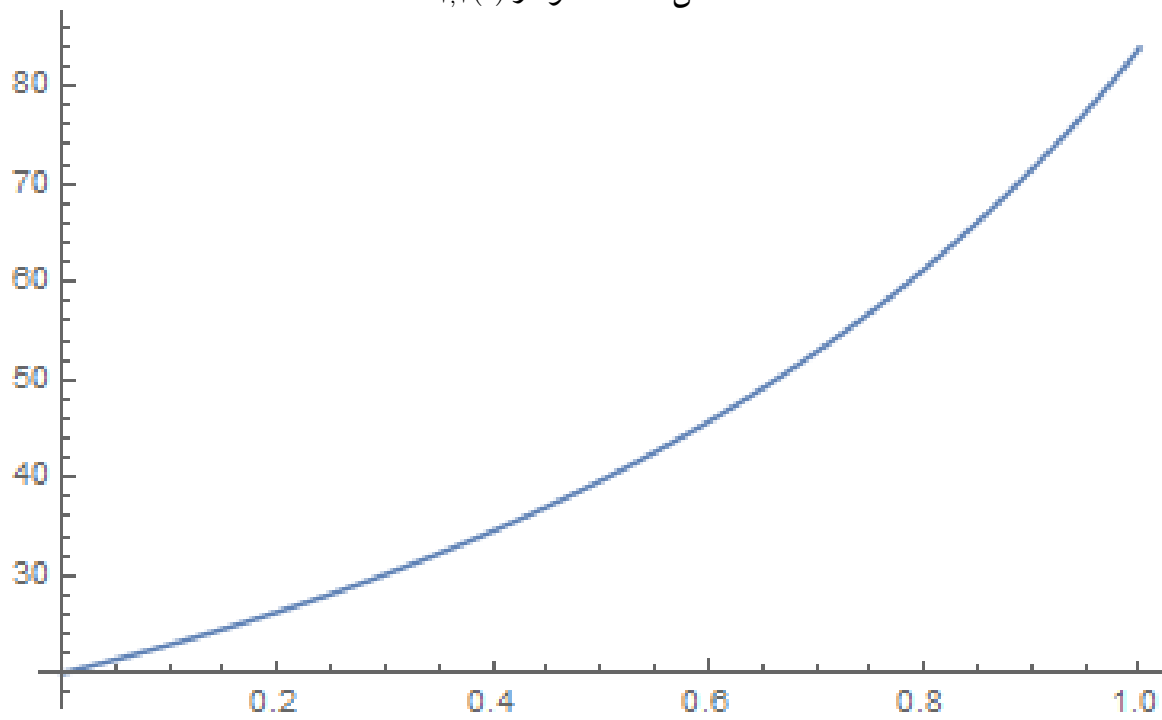
نمودارهای $S_{2,2}(t)$ و $E_{2,2}(t)$ و $I_{2,2}(t)$ برای بازه $[0, 1]$ به ترتیب در شکل‌های ۲.۴، ۳.۴ و ۴.۴ به دست می‌آوریم.

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

۲ - 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 - 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:

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

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 λ_1, λ_2 و λ_4 منفی و برای مقادیر ویژه λ_3 دو حالت داریم که اگر $\lambda_3 = \beta - \alpha - \mu - \varepsilon_a < 0$ ، در نتیجه $\beta < \alpha + \mu + \varepsilon_a$ که در نهایت $R_{oa} \leq 1$. بنابراین نقطه تعادل عاری از آلودگی E_0 در ψ مجاناً پایدار است و اگر $\lambda_3 = \beta - \alpha - \mu - \varepsilon_a > 0$ ، آن‌گاه در E^* تعادل اندمیک E_0 پایدار می‌شود و نقطه تعادل E_0 ناپایدار می‌شود و نقطه تعادل اندمیک E^* در E_0 ظاهر می‌شود و این نقطه به طور موضعی مجاناً پایدار می‌شود. از این رو می‌توان گفت E_0 به طور موضعی مجاناً پایدار است اگر $R_{oa} \leq 1$ و ناپایدار است اگر $R_{oa} > 1$.

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

$$J|_{E^*} = \begin{pmatrix} -\beta I_a^* - \varepsilon_t & -\varepsilon_t & -\beta S_t^* & 0 \\ \beta I_a^* & -y & \beta S_t^* & 0 \\ 0 & 0 & \beta(1 - \nu I_a^* - E_a^*) - \mu - \alpha & -\beta I_a^* \\ 0 & 0 & 0 & -\alpha - \sigma - \mu \end{pmatrix}$$

معادله مشخصه:

$$(-\beta I_a^* - \varepsilon_t - \lambda)(-y - \lambda)((\beta(1 - \nu I_a^* - E_a^*) - \mu - \alpha) - \lambda)(-\alpha - \sigma - \mu - \lambda) = 0.$$

$$\lambda_1 = \frac{1}{\nu} \left(-y - \varepsilon_t - \beta I_a^* - \sqrt{(y + \varepsilon_t + \beta I_a^*)^2 - 4(y\varepsilon_t + y\beta I_a^* + \beta\varepsilon_t I_a^*)} \right),$$

$$\lambda_2 = \frac{1}{\nu} \left(-y - \varepsilon_t - \beta I_a^* + \sqrt{(y + \varepsilon_t + \beta I_a^*)^2 - 4(y\varepsilon_t + y\beta I_a^* + \beta\varepsilon_t I_a^*)} \right),$$

$$\lambda_3 = -\alpha - \mu + \beta - \varepsilon_a - \beta E_a^* - \nu \beta I_a^*,$$

$$\lambda_4 = -\alpha - \mu - \sigma.$$

چهار مقدار ویژه $\lambda_1, \lambda_2, \lambda_3$ و λ_4 منفی هستند. با توجه به توضیحات ۳.۳، نقطه تعادل اندمیک E^* به طور موضعی مجاناً پایدار است اگر $R_{oa} > 1$.

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 فرسای، 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 method 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.*, 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 global stability problems*, SIAM Journal, **27** (4), (1996) 1070-1083.
- [27] Li, Y. and Muldowney, J. S., *On Bendixson's criterion*, Journal of Differential Equations, **106**, (1994) 27-39.

- [28] Martín 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 Classification 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 d'une fonction par des fractions rationnelles*, 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-borne 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, **8th**, 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 Threat 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, ٤th 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

Infected	آلوده
Zombie	ارتش زامبی
Trojan horse	اسب تروجان
Algorithm	الگوریتم
Internet of thing	اینترنت اشیا
Malicious object	بدافزار مخرب
Maclaurin expansion	بسط مک لورن
Locally asymptotically stable	به طور موضعی پایدار مجانبی
Uniformly persistent	به طور یکنواخت پایدار
Bandixon	بندیکسون
Stable	پایداری
Stability of dynamical systems	پایداری سیستم‌های دینامیکی
Asymptotic Stability	پایداری مجانبی
Local Stability	پایداری موضعی
Patch	پچ-وصله
User Datagram Protocol (UDP)	پروتکل ارتباطی کاربر
Intial approximation	تقریب اولیه

Pade approximation	تقریب پده
Endemic equilibrium point	نقطه تعادل اندمیک
Approxiation solution	جواب تقریبی
Exact solution	جواب دقیق
Characteristic polynomial	چندجمله‌ای مشخصه
Taylor polynomial	چندجمله‌ای تیلور
Distributed denial of service attack	حمله انکار سرویس توزیع شده
Targeted attack	حمله هدفمند
Error	خطا
Autonomous	خودگردان
System of differential equations	دستگاه معادلات دیفرانسیل
Approximate method	روش‌های تقریبی
Rung-Kutta method	روش رانگ-کوتا
Numerical method	روش عددی
Saddle	زینی
Linear system	سیستم‌های خطی
Nonlinear system	سیستم‌های غیرخطی
Wireless network	شبکه‌های بی‌سیم
Intial conditions	شرایط اولیه
Stationary conditions	شرایط پایداری
Basic reproduction number	عدد تکثیر پایه
Infectious node	گره آلوده

External node	گره خارجی
Susceptible node	گره مستعد (آسیب‌پذیر)
Node targeted	گره هدفمند
Radio Frequency Identification (RFID)	فناوری شناسایی مبتنی بر فرکانس رادیویی
Rolle's theorem	قضیه رُل
Weiershtrass theorem	قضیه ویراشتراس
Jacobian matrix	ماتریس ژاکوبی
Characteristic equation	معادله مشخصه
Rout hurwitz criterion	معیار روت-هرویتس
Eigen value	مقدار ویژه
Mirai botnet	میرای بات نت
Unstable	ناپایدار
Equilibrium point	نقطه تعادل
Infected free equilibrium point	نقطه تعادل عاری از آلودگی
Virus	ویروس
Convergence	همگرایی

واژه‌نامه انگلیسی به فارسی

Approximate method	روش‌های تقریبی
Approximation solution	جواب تقریبی
Asymptotic Stability	پایداری مجانبی
Autonomous	خودگردان
Basic reproduction number	عدد تکثیر پایه
Bandixon	بندیکسون
Characteristic equation	معادله مشخصه
Characteristic polynomial	چندجمله‌ای مشخصه
Convergence	همگرایی
Distributed denial of service attack	حمله انکار سرویس توزیع شده
Endemic equilibrium point	نقطه تعادل اندمیک
Equilibrium point	نقطه تعادل
Error	خطا
Exact solution	جواب دقیق
External node	گره خارجی
Infected	آلوده
Infected free equilibrium point	نقطه تعادل عاری از آلودگی

Infectious node	گره آلوده
Internet of thing	اینترنت اشیا
Intial approximation	تقریب اولیه
Intial conditions	شرایط اولیه
Jacobian matrix	ماتریس ژاکوبی
Linear system	سیستم‌های خطی
Locally asymptotically stable	به طور موضعی پایدار مجانبی
Local Stability	پایداری موضعی
Maclaurin expansion	بسط مک لورن
Malicious object	بدافزار مخرب
Mirai botnet	میرای بات نت
Nonlinear system	سیستم‌های غیرخطی
Numerical method	روش عددی
Pade approximation	تقریب پده
Patch	پیچ-وصله
Radio Frequency Identification (RFID)	فناوری شناسایی مبتنی بر فرکانس رادیویی
Rolle's theorem	قضیه رُل
Rout hurwitz criterion	معیار روت-هرویتس
Rung-Kutta method	روش رانگ-کوتا
Saddle	زینی
Stability of dynamical systems	پایداری سیستم‌های دینامیکی
Stable	پایداری

Stationary conditions	شرایط پایداری
Susceptible node	گره مستعد (آسیب‌پذیر)
System of differential equations	دستگاه معادلات دیفرانسیل
Taylor polynomial	چندجمله‌ای تیلور
Targeted attack	حمله هدفمند
Targeted node	گره هدفمند
User Datagram Protocol (UDP)	پروتکل ارتباطی کاربر
Uniformly persistent	به طور یکنواخت پایدار
Unstable	ناپایدار
Virus	ویروس
Weiershtrass theorem	قضیه وایراشتراس
Wireless network	شبکه‌های بی‌سیم
Zombie	ارتش زامبی

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: 68

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