پژوهشکده علوم کامپیوتر

پروپوزال همکاری پژوهشی تک پروژه غیر مقیم

تامین امنیت بواسطه گمنامی، کشف و مقابله با حملات در شبکه ها و سیستمهای سایبری فیزیکی

Security Provisioning through Creating Anonymity, Detecting and Confronting Attackers in Cyber Physical Systems and Networks

نام و نام خانوادگی متقاضی:	نشانی: تهران، خیابان کارگر شمالی، تقاطع خیابان جلال آل احمد، دانشکده فنی دانشگاه تهران، دانشکده برق و کامپیوتر	نشانی پست الکترونیکی:
دکتر محمد صیادحقیقی		sayad@ut.ac.ir
شمارهٔ تلفن ثابت: ۸۸۶۸۴۵۷۵	شمارهٔ تلفن همراه: ۰۹۱۲۲۰۲۷۲۵۱	

چکیده

شبکه های سایبری فیزیکی و یا بصورت کلی تر شبکه های رایانه ای همواره در معرض حملات مختلف بوده اند. برای مقابله با حمله کنندگان روشهای مختلفی ارایه شده اند که ایجاد ساز و کار اعتماد، گمنام سازی برای کاهش دانش مهاجم و در نهایت مقابله از طریق جبرانسازی اثر حمله و جداسازی مهاجم از جمله آنها بوده اند. در این پروژه سعی میشود که این راهبرد های دفاعی در امنیت ترکیب شوند بدان معنی که دانش مهاجم بواسطه ارایه روشهای گمنام سازی داده و ترافیک کمینه گردد و در صورت بروز حمله، کشف و اثر آن جبرانسازی شده و تا حد امکان با شناسایی منبع حمله و ایزوله کردن آن به شکل مجازی (مثلا با کاهش شدید میزان اعتماد)، مهاجم از شبکه بیرون انداخته شود. برای انجام این امر از تکنیکهای گمنام سازی و مسیریابی امن و همچنین روشهای کشف و جبرانسازی نفوذ و همچنین روشهای تحلیل شواهد برای یافتن منبع اصلی حمله استفاده خواهد شد.

واژگان کلیدی:

امنیت سایبری، گمنامی، حریم خصوصی، سیستمهای سایبری فیزیکی، جداسازی نود، مسیریابی امن

Abstract:

Cyber Physical Systems, and more generally computer networks, have always been vulnerable to various attacks. To counter attackers, various methods have been proposed, including establishing trust mechanisms, anonymization to reduce attackers' knowledge, and ultimately, combating through attack effect compensation and isolation of attacker from the network. This project aims to integrate these defensive strategies in security, meaning that attackers' knowledge is minimized through data and traffic anonymization, and in the event of an attack, it is detected and its effects are mitigated, and the attack source is identified and virtually isolated from the network to the extent possible (for example, by significantly reducing trust levels). To accomplish this, techniques such as anonymization, intrusion detection and compensation, and evidence combining theories are used to protect the network/system and to identify the primary source of the attack.

Keywords: Cyber Security, Anonymity, Privacy, Cyber Physical Systems, Node Isolation, Secure Routing

مقدمه

پارادایم جدیدی در صنعت در حالت به وجود آمدن است که در میان اهل فن گاهی از آن با عنوان Industry 4.0 نام برده میشود. تفاوت این تحول با مدلهای قدیمی تر، هوشمند شدن و قابلیت ارتباط گیری خودکار اجزاء درگیر در سامانه های صنعتی است. این مفاهیم در عمل نزدیک به ویژگیهایی است که در اینترنت اشیا (IoT) و سیستمهای سایبری-فیزیکی (CPS) یافت می شود. اما این تکنولوژی ها علاوه بر مزایای خود، چالش های امنیتی بی سابقه ای را به همراه آورده اند. در میان کاربردهای سیستم‌های متصل به هم، سیستمهای حمل و نقل هوشمند[1] (ITS) مثالهای خوبی هستند که در سالهای اخیر بطور ویژه ای مورد توجه قرار گرفته اند. وسایل نقلیه هوشمند نه تنها از طریق شبکه های اقتضایی خودرویی (VANET) با همدیگر ارتباط دارند، بلکه در داخل خود نیز اجزاء آنها از ارتباطات شبکه ای بهره می برند [1].

روشهای تامین امنیت کلاسیک اغلب فقط در یک جنبه موفق هستند و در یک سیستم پیچیده مانند آنچه در پارادایم نوین دیده میشود کارایی خود را از دست میدهند. به همین جهت لازم است که برای مقابله با حملات و تهدیدات شبکه ها و سیستمهای جدید از روشهای پیچیده تر تامین امنیت و بخصوص روشهای ترکیبی استفاده گردد. گمنام سازی داده و ترافیک از گذشته برای حفظ حریم خصوصی استفاده میشده است . اما اکنون میتواند در مدل جدید به کاهش سطح حمله نیز کمک کند. با توجه به اینکه هیچگاه نمیتوان از بروز حملات احتمالی جلوگیری کرد، یک رویکرد صحیح تامین امنیت باید شامل کشف و جبرانسازی اثر حمله در صورت وقوع آن باشد [3] ,[2]. همانگونه که مهاجمین جدید از تکنیکهای متعددی برای شناسایی سیستم/شبکه هدف استفاده میکنند، یک رویکرد دفاعی خوب باید پس از وقوع حمله با بررسی شواهد بجای مانده منبع تهدید را شناسایی و با مکانیزمهایی آنرا بصورت مجازی از شبکه بیرون کند تا حادثه مشابهی در آینده برای دیگر اعضای سالم شبکه رخ ندهد. مدیریت اعتماد به عنوان یکی از مکانیزمهای مکمل، میتواند در کاهش اعتبار مهاجمین و حذف تدریجی و حذف آنها از شبکه در صورت نشان دادن رفتار های سوء، موثر عمل کند [4].

در این پروژه سعی میشود که راهبرد های دفاعی در امنیت ترکیب شوند بدان معنی که دانش مهاجم بواسطه ارایه روشهای گمنام سازی داده و ترافیک کمینه گردد و در صورت بروز حمله، کشف و اثر آن جبرانسازی شده و تا حد امکان با شناسایی منبع حمله و ایزوله کردن آن به شکل مجازی (مثلا با کاهش شدید میزان اعتماد)، مهاجم از شبکه بیرون انداخته شود. برای انجام این امر از تکنیکهای گمنام سازی و مسیریابی امن و همچنین روشهای کشف و جبرانسازی نفوذ و همچنین روشهای تحلیل شواهد برای یافتن منبع اصلی حمله استفاده خواهد شد. با توجه به تجربه قبلی مجری در زمینه امنیت شبکه، سامانه های سایبری-فیزیکی، و نیز اعتماد (که خود موضوع پروژه دیگری در INSF بوده است) و همچنین شبکه محققان همکار بین المللی وی که نتیجه تحقیقات مشترک آنها در این حوزه در بیش از ۳۵ نشریه معتبر Q1 به چاپ رسیده است، مسیر اجرای این پروژه در صورت تامین اعتبار هموار بنظر می رسد.

[1] Intelligent Transportation Systems

پیشینه پژوهش

با توجه به چند وجهی بودن راه حل دفاعی، کارهای پیشین نیز به چند گروه مختلف تقسیم میشوند. نخست پژوهشهای پیشین در حوزه گمنامی و سپس کشف نفوذ و منبع حمله ارایه میشود.

روشهای مخفی و گمنام سازی داده و ترافیک

روش‌های ایجاد گمنامی به دو دسته تقسیم می‌شوند: روش‌های با تاخیر زیاد (مبتنی بر پیام) و روش‌های با تاخیر کم (مبتنی بر جریان). روش‌های گمنامی با تاخیر زیاد سعی دارند تا اطلاعات زمانی مربوط به ارتباط‌های شبکه را که می‌توانند برای تحلیل ترافیک شبکه مورد استفاده قرار بگیرند، پنهان نمایند. اگرچه این روش‌ها بیشترین مزیت‌های امنیتی ممکن را برای گمنام‌سازی فراهم می‌کنند، اغلب با توجه به این که لازمه این روش‌ها به تاخیر انداختن ترافیک شبکه است، در نتیجه در واقعیت غیرقابل استفاده هستند و بیشتر جنبه تئوری دارند. میکس منفرد[۲] [5] را می‌توان نخستین عضو از این دسته دانست. ساختار میکس به عنوان پایه‌ای برای بیشتر سیستم‌های ارتباطی گمنام شناخته می‌شود. یک موجودیت میکس را می‌توان سروری در نظر گرفت که دارای یک جفت کلید نامتقارن عمومی و خصوصی می‌باشد. این موجودیت کلید عمومی خود را از طریق زیرساخت کلید عمومی در دسترس بقیه موجودیت‌ها قرار می‌دهد. کاربرانی که تمایل دارند تا پیام‌های خود را به صورت گمنام ارسال کنند ابتدا پیام خود را با استفاده از کلید عمومی موجودیت میکس و از طریق روش‌های رمزنگاری نامتقارن رمز کرده و سپس پیام رمز شده را برای موجودیت میکس ارسال می‌کنند.اگرچه میکس منفرد ویژگی‌های گمنامی خوبی در برابر دشمن فراهم می‌کند، در عین حال با توجه به نوع ساختار استفاده شده برای فلاش کردن در برابر حملات فعال[۳] متنوعی آسیب‌پذیر است. علاوه بر این، موجودیت میکس فرستنده و گیرنده پیام را می‌شناسد. به همین منظور، برای جلوگیری از اینکه یک موجودیت میکس به تنهایی قادر به مرتبط کردن پیام‌ها به یکدیگر باشد، Chaum اولین پروتکل توزیع شده را برای ارتباط‌های گمنام ارائه کرد [5]. یک شبکه‌ی میکس[۴] شبکه‌ای با ساختار ذخیره-و-پیشرو[۵] است که در آن یک سری از میکس‌های منفرد قرار دارند که در آن هر میکس وظیفه پردازش آن دسته از بسته‌هایی را بر عهده دارد که از میکس‌های قبلی دریافت شده و به میکس‌های بعدی فرستاده خواهند شد.

برخلاف روش‌های با تاخیر بالا که سعی دارند تا اطلاعات زمانی ترافیک‌ها را پنهان کنند، طیف گسترده‌ای از روش‌های با تاخیر کم برای پردازش و انتقال پیام‌ها به صورت تقریبا زمان-حقیقی (real-time) ارائه شده است. این روش‌ها اگرچه امنیت پایین‌تری را نسبت به روش‌های با تاخیر بالا فراهم می‌کنند، ولی کارآیی بهتری را برای ترافیک‌های تعاملی ایجاد می‌کنند. بطور کلی نسبت معکوسی که بین کارآیی و امنیت وجود دارد.

پروکسی تک گامی[۶] ساده‌ترین روش برای به دست آوردن سطح ضعیفی از گمنامی است که تمامی ترافیک موجود بین فرستنده و گیرنده را از طریق یک سرور میانی تحت عنوان پروکسی سرور (مانند سرور VPN[۷]) ارسال کنیم. از جمله نمونه‌هایی از این روش که در عمل پیاده‌سازی شده‌اند می‌توان به anonymizer.com، BTGuard و Ipredator

[2] Single Mix
[3] Active attacks
[4] Mix network
[5] Store-and-forward
[6] Single hop proxy
[7] Virtual Private Network

اشاره کرد. از دیدگاه مقصد پیام فرستنده سرور VPN است و همچنین موجودیت خرابکاری که لینک ارتباطی فرستنده اصلی را شگره می‌کند نمی‌تواند مقصد اصلی پیام را شناسایی کند زیرا فقط مقصد میانی پیام که همان سرور VPN است، برای شگره کننده قابل مشاهده است. اگرچه پروکسی تک گامه یک روش سریع و ساده به حساب می‌آید، ولی با این حال سرور پروکسی مبدا و مقصد پیام را می‌شناسد.

ساختار دیگر، مسیریابی پیازی [6] است که بسیاری از سیستم‌های گمنامی کم‌تأخیر برپایه‌ی این ساختار ایجاد شده‌اند. هدف از مسیریابی پیازی ایجاد یک مدار مجازی دو طرفه[8] و زمان حقیقی[9] برپایه رمزنگاری لایه‌ای بین دو طرف ارتباط است تا بدین ترتیب آسیب‌پذیری‌های موجود در شبکه را محدود به آنالیز ترافیک نماید. برخلاف شبکه‌های میکس که با گروه کردن و برهم زدن ترتیب پیام‌ها قصد از بین بردن ویژگی‌های زمانی ارتباط‌ها را داشتند، در مسیریابی پیازی هدف اصلی ایجاد ارتباط‌هایی با کارآیی مناسب و تاخیر کم است تا بتوان از آن در برنامه‌های تعاملی مانند HTTP استفاده کرد. درنتیجه مسیریابی پیازی نسبت به حملات همبستگی آماری[10] آسیب‌پذیر می‌باشد درحالی که شبکه‌های میکس در برابر این حملات مقاوم بودند.

ساختار Crowds [7] نسبت به سایر ساختارها متفاوت‌تر است، زیرا گمنامی را از طریق ترکیب کردن در میان یک جمعیت[11] به دست می‌آورد. این ساختار از یک مجموعه‌ای از موجودیت‌ها تحت عنوان گره های Jondo تشکیل شده است که مسئولیت پروکسی کردن ترافیک ارسالی از فرستنده را به سمت گیرنده برعهده دارند. هنگامی که یک گره Jondo پیامی را دریافت می‌کند، با یک احتمال تصادفی تحت عنوان p_f که قبلا تعیین شده است تصمیم می‌گیرد که پیام را به یک Jondo دیگر ارسال کند یا اینکه با احتمال $1 - p_f$ پیام را به سمت مقصد اصلی ارسال می‌کند. این مقدار p_f نشان-دهنده درجه‌ی گمنامی[12] یا سطح اطمینانی برای یک Jondo مشخص است که می‌تواند در رابطه با اینکه گره قبلی فرستنده اصلی بوده است یا نه، تصمیم بگیرد. Crowds تنها قادر به تامین گمنامی فرستنده[13] است و از آن‌جایی که Jondo ها می‌توانند پیام را مشاهده کنند، لذا آدرس گیرنده را می‌توانند شناسایی کنند، در نتیجه گمنامی گیرنده[14] برآورده نمی‌شود. این ساختار گمنامی فرستنده و پیوندناپذیری فرستنده و گیرنده[15] را فراهم می‌کند.

پروتکل حریم‌خصوصی Peer-to-peer[16] یا P^5 [8]، گمنامی فرستنده، گمنامی گیرنده و گمنامی ارتباط را فراهم می‌کند. این ساختار برپایه‌ی کانال‌های همه‌پخشی ایجاد شده است که در آن فرستنده پیام خود را به جای ارسال مستقیم به گیرنده، به تمامی اعضای کانالی که گیرنده خود را با آن معرفی کرده است، ارسال می‌کند. در این ساختار اگر کاربران پیامی برای ارسال نداشته باشند، پیام‌های تصادفی ارسال می‌کنند تا بدین‌ترتیب ترافیک پوششی ایجاد کنند. این سیستم براساس ساختار درختی ایجاد می‌شود که در آن هر کاربر با توجه به کلید عمومی خود جایگاهش را در درخت می‌شناسد و می‌تواند با توجه به کلید عمومی خود، به کانال مرتبط با این کلید عمومی که در هر سطح از درخت قرار دارد، بپیوندد. هر چه

[8] Bidirectional virtual circuit

[9] Real-time

[10] Statistical correlation attacks

[11] Blending into a crowd

[12] Degree of anonymity

[13] Sender anonymity

[14] Receiver anonymity

[15] Sender/Receiver unlinkability

[16] Peer-to-peer Personal Privacy Protocol

کاربران به کانال‌های سطوح بالایی درخت بپیوندند، تعداد اعضای بیشتری در این کانال‌ها حضور خواهند داشت، لذا گمنامی کاربران در بین مجموعه‌ی بزرگ‌تری حاصل خواهد شد در عین حالی که تعداد پیام‌های همه‌پخشی و درنتیجه‌ی آن سربار شبکه بیشتر خواهد شد.

پروژه‌ی اینترنت نامرئی[17] یا I2P [9]، در واقع با توجه به ایده‌ی سرویس مخفی در تور ایجاد شده است. در این سیستم هر کاربر برای خود یک یا چند تونل ورودی و خروجی مجزا ایجاد می‌کند تا بدین‌ترتیب تمامی ارتباطات از طریق این تونل‌ها انجام شود. فرستنده برای ارسال پیام به گیرنده، می‌بایست شناسه‌ی مربوط به تونل ورودی گیرنده را بداند و بدین ترتیب پیام خود را از طریق تونل خروجی خود به تونل ورودی گیرنده ارسال کند. ایجاد تونل‌ها در این ساختار مشابه به ایجاد مدار مجازی در ساختار تور است، با این تفاوت که این تونل‌ها با توجه به یک ارتباط ایجاد نمی‌شوند. پیام‌های ارسالی برای رسیدن به تونل ورودی گیرنده با توجه به شناسه‌ی تونل از مسیریابی خاصی که توسط این سیستم ارائه شده است استفاده می‌کنند که به آن Garlic گفته می‌شود. در این ساختار نیز گمنامی فرستنده و گیرنده حفظ می‌شود، ولی انعطاف‌پذیری آن کم است، همچنین اگرچه بین تونل‌ها از مسیریابی استفاده می‌شود ولی این مسیریابی براساس ساختار متمرکزی ایجاد شده است و یک شبکه‌ی توزیع شده نمی‌باشد.

لی بلاند و همکارانش Aqua [10] را ارائه کردند که هدف از آن ارائه‌ی یک سیستم گمنامی با تاخیر کم[18] و پهنای باند زیاد[19] است، که توانایی مقاومت در برابر حملات تحلیل ترافیک را داشته باشد. این سیستم به‌گونه‌ای طراحی شده است تا با استفاده از بستر ارتباطی تور و هنچنین با استفاده از سرورهای میکس[20] در برابر این‌گونه از حملات مقاومت کند. در واقع Aqua هر کاربر را دقیقا به یک میکس متصل می‌کند که این میکس‌ها تحت عنوان میکس لبه‌ای[21] شناخته می‌شوند. در این حالت اگر تعداد k کاربر به میکس یکسانی متصل شوند می‌توان ادعا کرد که گمنامی k-درجه‌ای[22] به دست می‌آید. در این روش فرض می‌شود که کاربران درستکار به میکس‌های آلوده نشده توسط مهاجم متصل می‌شوند و همچنین مهاجم میکس‌های لبه‌ای را تنها در یک طرف ارتباط می‌تواند کنترل کند. از آن‌جایی که برآورده شدن این فرض‌ها کمی دشوار به‌نظر می‌رسد، چرا که کاربر نمی‌تواند به این موضوع پی ببرد که میکسی که به آن متصل است سالم یا آلوده می‌باشد و همچنین مهاجم قدرتمند توانایی تسلط بر هر دو طرف ارتباط را داراست، درنتیجه می‌توان گمنامی مربوط به سیستم Aqua را نیز مانند تور ارزیابی کرد.

ون دل هوف و همکارانش Vuvuzela [11] را ارائه کردند که یک ساختار گمنامی مقیاس‌پذیر برای ارسال و دریافت پیام است. در این ساختار از مفهوم حریم‌خصوصی تفاضلی برای تضمین گمنامی کاربران استفاده شده است، به‌گونه‌ای که مهاجم نتواند بین حالتی که یک فرستنده پیامی را برای گیرنده‌ای خاص ارسال می‌کند و حالتی که همان فرستنده هیچ پیامی را ارسال نمی‌کند و یا اینکه پیام نویز گونه‌ای را ارسال می‌کند، تفاوت محسوسی را احساس کند.

کوان و همکارانش Atom [12] را ارائه کردند که در آن میکس‌ها در گروه‌های مختلفی قرار می‌گیرند که هر گروه

[17] Invisible Internet Project
[18] Low-latency
[19] High-bandwidth
[20] Mix
[21] Edge Mix
[22] K-Anonymity

کلیدعمومی مخصوص خود را دارد. این ساختار بر پایه‌ی شبکه‌ی میکس ساخته شده است که تنها گمنامی فرستنده را تامین می‌کند و در آن از آمیختگی قابل وارسی[۲۳] استفاده شده است. در این سیستم فرستنده پیام خود را با کلید عمومی یکی از گروه‌ها رمز کرده و آن را از طریق سرور ورودی که تنها نقش ارسال کردن پیام فرستنده را به سرورهای میکس موجود در گروه انتخابی فرستنده برعهده دارد.

پیتروسکا و همکارانش Loopix [13] را که یک سیستم گمنامی کم‌تأخیر است برای تامین گمنامی از دید سوم‌شخص ارائه کردند. این ساختار که برپایه‌ی میکس ایجاد شده است از سه جزء اصلی سرورهای میکس، تأمین کننده[۲۴]ها و کاربران تشکیل شده است. هر کاربر خود را به یک تأمین کننده که دارای ویژگی‌های بهتری برای فرستنده است (مثلا از لحاظ مکانی)، متصل می‌کند.

آنگل و همکارانش Pung [14] را که یک ساختار گمنامی با فرض عدم وجود هیچ‌گونه سرور مورداعتماد و درستکار است، ارائه کردند. در این ساختار کاربران برای ارسال و دریافت پیام نیاز دارند تا همدیگر را بشناسند و خارج از شبکه‌ی Pung بر سر کلید مشترکی به توافق برسند. این کلید به عنوان کلید اصلی[۲۵] برای تولید کلیدهای فرعی و همچنین برچسب‌های موردنیاز برای ارتباط دو کاربر یا گروهی از کاربران مورداستفاده قرار می‌گیرد.

تیاگی و همکارانش در [15] ساختار گمنامی را تحت عنوان Stadium ارائه کردند که سیستمی مشابه به Vuvuzela می‌باشد، با این تفاوت که در این ساختار از تولید نویز به صورت توزیع شده[۲۶] و ساختاری موازی و قابل وارسی[۲۷] برای شبکه‌ی میکس استفاده شده است. در این سیستم به جای اینکه تمامی سرورهای میکس به صورت مستقل نویز ایجاد کرده و آن را برای میکس‌های بعدی ارسال کنند، ایجاد نویز در یک مرحله قبل از ورود به شبکه‌ی میکس و توسط سرورهای میکس لایه‌ی ورودی به شبکه انجام می‌شود.

لازار و همکارانش Karaoke [16] را که ساختار گمنامی مشابهی با Vuvuzela و Stadium دارد ارائه کردند. در این ساختار ایجاد نویز به شیوه‌ی متفاوت‌تری نسبت به ساختارهای قبلی انجام می‌شود. در این ساختار هر کدام از سرورهای میکس ابتدا پیام‌های فرستنده‌ها را در اسلات‌های زمانی جمع کرده و در پایان اسلات‌ها نویزهای خود را ایجاد می‌کنند و در مرحله‌ی بعدی هر کدام ترتیب پیام‌ها و نویزهای ایجاد شده توسط خود را بهم ریخته و به سایر سرورهای میکس ارسال می‌کنند.

روشهای کشف حلمه و منبع آن

روشهای تشخیص حمله و یا نفوذ متعدد هستند. این روشها به دو دسته کلی مبتنی بر امضا و یا تشخیص رفتار نامتعارف تقسیم میشوند. در کنار کشف حمله، مکانیزمهای مدیریت اعتماد نیز در شبکه ها و سیستمها بکار میروند که مقدار اعتماد را بر اساس شواهد متخاصم بودن فرد یا گره تنظیم میکنند و در نهایت، میتواند به مکانیزمی برای ایزوله کردن یک گره از شبکه تبدیل شوند.

در روش [17] مقدار اعتماد برای هر پیغام به شکل جداگانه حساب می‌شود. پس از آن شواهد مختلف به روش بیز با

[23] Verifiable Shuffle
[24] Provider
[25] Master key
[26] Distributed noise generation
[27] Verifiable Parallel Mixnet

یکدیگر ترکیب می‌شوند و احتمال درست بودن حادثه محاسبه می‌شود. اعتبار یا اعتماد محاسبه شده به پیغام تابع وضعیت امنیتی گره و گزارش ارسال شده و پارامترهای پویای محیطی مثل زمان و مکان است. در این روش، تابعی به نام security statusتعریف شده که عملا خروجی بخش احرازهویتی است که می‌تواند در سیستم تعریف شود. خروجی صفر به معنای گره‌ای است که گواهی آن ابطال شده و خروجی یک گره درستکار را نشان می‌دهد. پارامتر دیگری که در محاسبه اعتماد برای هر پیام در نظرگرفته می‌شود، اعتماد پایه گره در گزارش‌دهی مشخصی است.

در مقاله [18] مدل اعتمادی با نام RMCV بخصوص برای شبکه خودرویی ارائه شده است. در این مدل پس از اعمال الگوریتم خوشه‌بندی سلسله مراتبی، پیام‌های مربوط به یک حادثه از یکدیگر جدا می‌شوند. در ادامه پیام‌های توصیف‌کننده یک حادثه که با هم تضاد اطلاعاتی دارند در دسته‌های مربوطه قرار میگیرند. سپس بر اساس شباهت محتویات اعضای خوشه ، تضاد محتویات بین خوشه‌های مختلف مربوط به یک حادثه و شباهت مسیرهای ارسالی پیغام‌ها، مقدار اعتماد برای هر خوشه محاسبه می‌شود.

روش [19] برای همه پیام‌های دریافتی مقدار اعتمادی را حساب می‌کند و در نهایت پیام با بیشینه مقدار اعتماد را انتخاب می‌کند. اگر این مقدار اعتماد از حد آستانه تعریف شده در سیستم بیشتر بود این پیام مورد پذیرش سیستم قرار می‌گیرد و طبق آن تصمیم‌گیری صورت می‌گیرد و در غیر این صورت پیام رد می‌شود.

روش [20] برای هر وسیله گره در جریان یک واقعه خودرویی یک نقش تعریف می‌کند. در کل سه نقش در سیستم وجود دارد: گزارش دهنده پیام ، مشاهده کنندگان پیام و گره‌های شرکت‌کننده. هر گره طبق مقدار شهرت ثبت شده در پیام مقدار اعتماد خود به پیام را حساب می‌کند. اگر گره از جنس گره گزارشگر باشد، شهرت پیام (اعتماد به پیام) نسبت فرکانس دریافتی حسگرها به پایه فرکانس مربوط به حادثه است. برای گره مشاهده‌کننده، میزان شهرت ثبت شده در پیام‌های دریافت شده توسط گزارشگرها و توسط سایر گره‌های مشاهده‌کننده با هم به شکل وزن‌دار ترکیب شده و مقدار نهایی اعتماد محاسبه می‌شود.

دسته ای دیگر از روشهای مرتبط با اعتماد سعی دارند که مبتنی بر گره عمل نمایند. برای مثال در مقاله [21] برای محاسبه شهرت گره از تجربیات مستقیم، نظرات سایر گره‌ها و در صورت دسترسی از نظر و امتیازدهی واحد مرکزی استفاده می‌شود. در این روش از نظرهای گره‌های همسایه در محاسبه شهرت به شکل وزن‌دار استفاده می‌شود و پس از آگاهی از درستی یا نادرستی پیغام گزارش شده وزن پیشنهاد دهندگان در محاسبه شهرت گره‌ی هدف به‌روز می‌شود. در این مقاله بر حسب امتیاز به دست آمده برای گره و برای تصمیم‌گیری مبنی بر رد کردن یا پذیرش گزارش سه سطح اعتماد تعریف شده است. علاوه بر این، بر حسب نوع پیغام سه سطح شدت نیز تعریف شده است .

مقاله [22] از رایانش در لبه شبکه برای ساخت سیستم اعتبارسنجی استفاده کرده است. در این مقاله تعدادی عوامل محلی با قابلیت پردازش بالا در نظر گرفته شده است و خودروها به طور مستقیم با آن‌ها ارتباط برقرار می‌کنند و می‌توانند میزان شهرت یک گره را از آن سوال کنند. عامل محلی نظرات را با اعمال وزنی بر اساس میزان آشنایی، شباهت، نزدیکی زمانی با یکدیگر ترکیب می‌کند. وزن نظر هر گره بر اساس جمع اعتماد و عدم اعتماد به عنوان تعیین‌کننده میزان اشنایی نظردهنده به گره هدف، نرخ شباهت کسینوسی برای اطلاعات حرکتی دو گره به عنوان میزان شباهت و تازگی نظر محاسبه می‌شود. نظرات با منطق انگاشتی با یکدیگر ترکیب می‌شوند.

پژوهش [23] روشی به نام RITA را ارائه کرده است که هدف اصلی اش تشخیص حمله on-off بوده است. به این قصد به جای به‌روزرسانی مقادیر شهرت گره‌ها در هر تبادل اطلاعاتی مستقیم، به‌روزرسانی بیشتر انجام می‌شود تا هر گونه تغییر

جزیی در رفتار شناسایی شود. اعتماد به گره شامل دو بخش اعتماد مستقیم و اعتماد غیرمستقیم است که هر چقدر تعداد تبادلات (مستقیم) دو گره بیشتر شود، وزن اعتماد مستقیم در مقدار نهایی اعتماد بیشتر خواهد شد. در RITA برای مقابله با حمله on-off میزان اختلاف بین اعتماد مستقیم در دو بازه زمانی متوالی در نظر گرفته می‌شود. هم چنین این روش پارامترهایی را برای مقابله با حمله بدگویی و جعل پیام در نظر گرفته است.

مقاله [21] روشی با نام TRIPارائه داده است. در این روش با اخذ نظر گره های همسایه، یک مقدار عددی برای شهرت و اعتماد به گره ها محاسبه می شود و از این مقدار به عنوان وزن اطلاعات دریافتی بهره گرفته می شود. سپس با آگاهی یافتن از درستی یا نادرستی پیام گزارش شده مقدار شهرت و اعتماد گره صاحب پیام به روزرسانی می شود.

مقاله [24] برای هر گره یک میزان اعتبار اولیه در نظر گرفته و هر گره تنها با داشتن اعتبار کافی قادر به ارسال پیام در شبکه خواهد بود. هم چنین گره ها با ارسال پیام صحیح یک میزان اعتبار پاداش می گیرند. در این مدل اگر گره ای پیام جعلی یا خلاف واقع ارسال نماید، پاداش ارسال پیام صحیح را از دست داده و فقط مقداری اعتبار مصرف می کند و در واقع تنبیه می شود. در مطالعه [25] رویکردی برای مقابله با گره هایی که پیام دیگران را دریافت کرده و دستکاری شده آن پیام را به دیگران ارسال می نماید، اتخاذ نموده است. در این مطالعه برای جلوگیری از انتخاب گره مخرب به عنوان بازارسال کننده پیام ها، ابتدا برای گره های مجاور، امتیاز هایی جمع آوری شده و وسیله نقلیه ا ی با بالاترین امتیاز به عنوان وسیله نقلیه رله برای انتشار پیام ها انتخاب می شود.

دلایل انجام طرح

دلایل ضرورت اجرای این طرح بصورت فهرست وار در ذیل آمده است:

۱ - از سیستمهای پیچیده و بخصوص شبکه ها و سیستمهای سایبری فیزیکی در کشور در زیرساختهای حیاتی استفاده میشود. با هوشمند شدن سیستمها و شبکه ها، اصطلاحا سطوح حمله گسترش می یابد و امکان صدمه پذیری بوجود آمده و مخاطره افزایش می یابد.

۲- روشهای تامین امنیت کلاسیک در سیستمها و شبکه های جدید اثر محدودی دارند و باید از طیف وسیع تری از روشهای تامین امنیت برای افزایش کارایی بهره برد.

اهداف و محصولات طرح

طرح از نوع پژوهشی بوده و منجر به مقالات علمی و یا ثبت اختراع خواهد شد.. امکانسنجی اولیه (Feasibility Study) تحقیق، انجام شده و در چند جنبه پایه ای پیشرفت خوبی داشته است.

برنامه و نحوه اجرای طرح

در مرحله ۱، روشهای پایه و کلاسیک تامین امنیت مانند گمنام سازی بررسی میشود و سعی میگردد تا در این سطح، ترکیب آنها با یکدیگر امکانسجی گردد.

در مرحله ۲، یک مکانیزم تامین امنیت از راه گمنام سازی، کشف و جبرانسازی مهاجم و حمله بخصوص در شبکه ها و یا سیستمهای مسایبری فیزیکی طراحی و تحلیل خواهد شد. برای این کار سعی بر استفاده از روشهای ترکیبی خواهد بود.

در مرحله ۳، الگوریتمها و مکانیزمهای طراحی شده در فاز های پیشین شبیه سازی خواهد شد و مورد ارزیابی قرار خواهد

گرفت. مقالات نیز در این مرحله ارسال خواهند شد.

برنامه زمانی

مدت انجام این طرح، مطابق روال معمول پژوهشکده خواهد بود و در کمتر از ۱ سال به اتمام خواهد رسید.

شماره مرحله / فعالیت	نام مرحله/ فعالیت	درصد وزنی به کل پروژه	مدت زمان اجرا (ماه)	نمودار زمان‌بندی(ماه)											
				۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲
۱	بررسی روشهای پیشین تامین امنیت و امکانسنجی ترکیب آنها	٪۳۰	۲												
۲	طراحی یک مکانیزم امن سازی از راه گمنام سازی، کشف و یا جبرانسازی حمله	٪۵۰	۷												
۳	ارزیابی مدلها و انتشار یافته های علمی	٪۲۰	۳												

همکاران طرح

همکار علمی طرح، دکتر فائزه فریور عضو هیئت علمی دانشگاه آزاد، واحد علوم و تحقیقات تهران است. سایر همکاران خارجی مانند دکتر علیرضا جلفایی و دکتر مامون العزب نیز ممکن است در جریان تحقیق کمک نمایند.

ابزار مورد نیاز

کیفیت انجام پروژه و میزان واقعی بودن بستر تست و ارزیابی روشهای توسعه داده شده، به مقدار بودجه تصویب شده برای پروژه بستگی دارد. بطور ایده آل این پروژه نیاز به بستر لازم برای پیاده‌سازی عملی دارد. اما برای شبیه‌سازی و در مقیاس کوچک، با توجه به اینکه بسیاری از نرم افزارها قابل حصول بصورت آزمایشی و یا رایگان هستند، می توان در بخش پژوهشی و تولید مقاله از آنها استفاده نمود.

بودجه تقریبی

میزان کار لازم برای این طرح در بخش پژوهشی حدود ۱۸ نفر ماه است که هزینه ای در حدود ۵۶۰/۰۰۰/۰۰۰ ریال برای

آن پیش‌بینی شده است. اما هر گونه حمایت پژوهشگاه دانش های بنیادی کمک شایانی خواهد بود. هزینه ها به نسبت درصد وزنی در فازها توزیع می‌شوند.

مراجع

[1] B. Mokhtar and M. Azab, "Survey on Security Issues in Vehicular Ad Hoc Networks," *Alexandria Engineering Journal*, vol. 54, no. 4. pp. 1115–1126, 2015.

[2] F. Neves, R. Souza, J. Sousa, M. Bonfim, and V. Garcia, "Data privacy in the Internet of Things based on anonymization: A review," *J. Comput. Secur.*, 2023.

[3] M. S. Haghighi and Z. Aziminejad, "Highly Anonymous Mobility-Tolerant Location-Based Onion Routing for VANETs," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 2582–2590, 2020.

[4] M. Ebrahimi, M. H. Tadayon, M. S. Haghighi, and A. Jolfaei, "A Quantitative Comparative Study of Data-oriented Trust Management Schemes in Internet of Things," *ACM Trans. Manag. Inf. Syst.*, 2022.

[5] D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Commun. ACM*, 1981.

[6] D. M. Goldschlag, M. G. Reed, and P. F. Syverson, "Hiding routing information," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1996.

[7] M. K. M. Reiter and A. D. A. Rubin, "Crowds: Anonymity for web transactions," *ACM Trans. Inf. Syst. …*, 1998.

[8] R. Sherwood, B. Bhattacharjee, and A. Srinivasan, "P5: A protocol for scalable anonymous communication," in *Proceedings - IEEE Symposium on Security and Privacy*, 2002.

[9] I2P, "The Invisible Internet Project," *I2P.org*, 2015.

[10] S. Le Blond, D. Choffnes, W. Zhou, P. Druschel, H. Ballani, and P. Francis, "Towards efficient traffic-analysis resistant anonymity networks," in *SIGCOMM 2013 - Proceedings of the ACM SIGCOMM 2013 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, 2013.

[11] J. Van Den Hooff, D. Lazar, M. Zaharia, and N. Zeldovich, "Vuvuzela: Scalable private messaging resistant to traffic analysis," in *SOSP 2015 - Proceedings of the 25th ACM Symposium on Operating Systems Principles*, 2015.

[12] A. Kwon, H. Corrigan-Gibbs, S. Devadas, and B. Ford, "Atom: Horizontally Scaling Strong Anonymity," in *SOSP 2017 - Proceedings of the 26th ACM Symposium on Operating Systems Principles*, 2017.

[13] A. M. Piotrowska, J. Hayes, T. Elahi, S. Meiser, and G. Danezis, "The Loopix anonymity system," in *Proceedings of the 26th USENIX Security Symposium*, 2017.

[14] S. Angel and S. Setty, "Unobservable communication over fully untrusted infrastructure," in *Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2016*, 2016.

[15] N. Tyagi, Y. Gilad, D. Leung, M. Zaharia, and N. Zeldovich, "Stadium: A Distributed Metadata-Private Messaging System," in *SOSP 2017 - Proceedings of the 26th ACM Symposium on Operating Systems Principles*, 2017.

[16] D. Lazar, Y. Gilad, and N. Zeldovich, "Karaoke: Distributed private messaging immune to passive traffic analysis," in *Proceedings of the 13th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2018*, 2007.

[17] M. Raya, P. Papadimitratos, V. D. Gligor, and J.-P. Hubaux, "On data-centric trust

establishment in ephemeral ad hoc networks," in *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, 2008, pp. 1238–1246.
[18] S. Gurung, D. Lin, A. Squicciarini, and E. Bertino, "Information-oriented trustworthiness evaluation in vehicular ad-hoc networks," in *International conference on network and system security*, 2013, pp. 94–108.
[19] R. A. Shaikh and A. S. Alzahrani, "Intrusion-aware trust model for vehicular ad hoc networks," *Secur. Commun. networks*, vol. 7, no. 11, pp. 1652–1669, 2014.
[20] Q. Ding, X. Li, M. Jiang, and X. Zhou, "Reputation-based trust model in vehicular ad hoc networks," in *2010 International Conference on Wireless Communications & Signal Processing (WCSP)*, 2010, pp. 1–6.
[21] F. G. Mármol and G. M. Pérez, "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks," *J. Netw. Comput. Appl.*, vol. 35, no. 3, pp. 934–941, 2012.
[22] X. Huang, R. Yu, J. Kang, and Y. Zhang, "Distributed reputation management for secure and efficient vehicular edge computing and networks," *IEEE Access*, vol. 5, pp. 25408–25420, 2017.
[23] C. A. Kerrache, C. T. Calafate, N. Lagraa, J. Cano, and P. Manzoni, "RITA: RIsk-aware Trust-based Architecture for collaborative multi-hop vehicular communications," *Secur. Commun. Networks*, vol. 9, no. 17, pp. 4428–4442, 2016.
[24] N. Haddadou, A. Rachedi, and Y. Ghamri-Doudane, "Trust and exclusion in Vehicular Ad Hoc Networks: An economic incentive model based approach," in *2013 Computing, Communications and IT Applications Conference, ComComAp 2013*, 2013.
[25] S. Dahmane, C. A. Kerrache, N. Lagraa, and P. Lorenz, "WeiSTARS: A weighted trust-aware relay selection scheme for VANET," in *IEEE International Conference on Communications*, 2017.

نام و نام خانوادگی متقاضی: دکتر محمد صیادحقیقی– دانشیار دانشگاه تهران تـــــاریخ: ۱۴۰۲/۱۱/۱۵