Iranian Journal of Wargaming
AJA Command and Staff University
http://www.ijwg.ir/
Online ISSN: 2676-7708
Print ISSN: 2676-5284

Identification of threats in the field of intrusion to integrity in military ad-hoc networks

Sajad Alimohammadi[1]✉ | Vahid Sajadi Asil [2] | Hasan Kochaky[3]

1. Faculty Member of AJA Command and Staff University, Tehran, Iran. E-mail: S.alimohammadi33@casu.ac.ir
2. Faculty Member of AJA Command and Staff University, Tehran, Iran. E-mail: v.d.sajadi@gmail.com
3. Faculty Member of AJA Command and Staff University, Tehran, Iran. E-mail: hasan.gdjb@gmail.com

Article Info

Article type:

Research Article

Article history:

Received

19 July 2024

Received in revised form

27 August 2024

Accepted

7 Septmber 2024

Keywords:

Ad hoc network,

integrity,

intrution

ABSTRACT

Background: In order to establish stable and continuous communication between soldiers on a battlefield with the command system, using a fixed wireless access point is dangerous, because the enemy can disrupt or destroy the entire network by attacking it. . By using ad-hoc networks, it is possible to communicate between military units in remote areas, in harsh weather conditions, and even in areas with harsh environmental conditions. In order to have a permanent connection, the issue of data integrity in this network is essential, and therefore, in order to deal with the enemy, it is necessary to investigate and identify the methods of penetration and integrity attacks in military ad hoc networks with a scientific approach.

Objective: to identify the methods of infiltrating the integrity of the military ad-hoc network.

Methodology: The type of research in this research is applied and the descriptive research method and information analysis approach are mixed. The society studied in this research is the available books, articles, documents and documents as well as opinions obtained in the form of interviews with 8 experts who have sufficient knowledge in the field of electromagnetic cyber networks and are practically working in These are the fields. The statistical population of the research was 130 people with characteristics, familiarity with cyber-electromagnetic networks, familiarity with telecommunication and computer networks, having at least a bachelor's degree and 10 years of service experience, whose opinions were received and analyzed online in the form of a questionnaire.

Findings and Originality: By analyzing the collected information, regarding the ways of infiltrating ad-hoc networks in the field of integrity, 10 indicators for the active classic component, 3 indicators for the passive classic component and 4 indicators for the meter attack component were identified, among them , malicious code injection attack with average (4.74), masquerading attack with average (4.71), packet or message injection attack with average (4.70), for active classic component, traffic analysis attack with average (66. 4) For the inactive classic component and the popular attack with an average of (4.92) for the Mitratech component, according to the opinion of the statistical community, they are the best attacks on the integrity of military ad hoc networks.

Cite this article: alimohammadi, S., Sajadi asel, V. & kochaky, H. (2024). Identification of threats in the field of intrusion to integrity in military ad-hoc networks. *Iranian Journal Of Wargaming*, 6 (13), 155-182.

DOI: 10.22034/ijwg.2024.468605.1088

Publisher: AJA Command and Staff University

Iranian Journal of Wargaming
AJA Command and Staff University
http://www.ijwg.ir/
Online ISSN: 2676-7708
Print ISSN: 2676-5284

شناسایی تهدیدات در حوزه نفوذ به یکپارچگی در شبکه‌های اد_هاک نظامی

سجاد علی‌محمدی[1] ✉ | وحید سجادی اصیل[2] | حسن کوچکی[3]

۱. عضو هیئت علمی داخلی دانشگاه فرماندهی و ستاد آجا، تهران، ایران. ،رایانامه: S.alimohammadi33@casu.ac.ir

۲. عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: v.d.sajadi@gmail.com

۳. عضو هیئت علمی دانشگاه فرماندهی و ستاد آجا، تهران، ایران. رایانامه: hasan.gdjb@gmail.com

اطلاعات مقاله

نوع مقاله:
مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۴/۲۹

تاریخ بازنگری:
۱۴۰۳/۰۶/۰۶

تاریخ پذیرش:
۱۴۰۳/۰۶/۱۷

کلیدواژه‌ها:
شبکه اد هاک، یکپارچگی، نفوذ.

چکیده

زمینه: جهت برقراری ارتباط پایدار و مداوم میان سربازان در یک میدان نبرد با سامانه فرماندهی، استفاده از یک نقطه دسترسی بی‌سیم ثابت خطرناک است، زیرا دشمن می‌تواند با حمله به آن کل شبکه را مختل نماید یا از بین ببرد. . با استفاده از شبکه‌های اد_هاک، امکان برقراری ارتباط بین دستگاه‌های نظامی در مناطق دورافتاده، در شرایط آب و هوایی سخت و حتی در مناطقی با شرایط محیطی سخت فراهم شده است. جهت داشتن یک ارتباط دائم، مسئله یکپارچگی داده‌ها در این شبکه ضروری است و بنابراین، برای مقابله احتمالی با دشمن ضروری است روش‌های نفوذ و حمله به یکپارچگی در شبکه های ادهاک نظامی، با رویکردی علمی مورد بررسی و شناسایی قرار گیرد.

هدف: شناسایی شیوه‌های نفوذ به یکپارچگی شبکه اد_هاک نظامی.

روش پژوهش: نوع تحقیق در این پژوهش از نوع کاربردی است و روش تحقیق توصیفی و رویکرد تجزیه و تحلیل اطلاعات، آمیخته است.

جامعه مورد مطالعه در این تحقیق، کتب، مقالات، اسناد و مدارک موجود و همچنین نظرات اخذ شده در قالب مصاحبه با تعداد ۸ نفر صاحب‌نظرانی است که در حوزه شبکه‌های سایبر الکترومغناطیس، دانش کافی را داشته و به‌صورت عملی در حال فعالیت در این حوزه می‌باشند. جامعه آماری تحقیق ۱۳۰ نفر با مشخصات، آشنایی با شبکه‌های سایبر الکترومغناطیس، آشنایی با شبکه‌های مخابراتی و رایانه‌ای، حداقل دارای مدرک کارشناسی و ۱۰ سال سابقه خدمت باشند بودند که نظرات آنها در قالب پرسشنامه به‌صورت آنلاین دریافت و مورد تجزیه و تحلیل قرار گرفت.

یافته‌ها و نتیجه‌گیری: با تجزیه و تحلیل اطلاعات جمع آوری شده، درخصوص شیوه‌های نفوذ به شبکه‌های اد_هاک در حوزه یکپارچگی، تعداد ۱۰شاخص برای مولفه کلاسیک فعال، ۳ شاخص برای مولفه کلاسیک غیر فعال و ۴شاخص برای مولفه میتر اتک شناسایی گردید که از میان آنها، حمله تزریق کد آلوده با میانگین (۴/۷۴)، حمله بالماسکه کردن با میانگین (۴/۷۱)، حمله تزریق بسته یا پیام با میانگین (۴/۷۰)، برای مولفه کلاسیک فعال، حمله تحلیل ترافیک با میانگین (۴/۶۶) برای مولفه کلاسیک غیر فعال و حمله مردمیانی با میانگین (۴/۹۲) برای مولفه میتراتک، براساس نظر جامعه آماری، بهترین حملات به یکپارچگی شبکه های ادهاک نظامی هستند.

استناد: علی محمدی، سجاد؛ سجادی اصیل، وحید؛ و کوچکی، حسن (۱۴۰۳). شناسایی تهدیدات در حوزه نفوذ به یکپارچگی در شبکه‌های اد_هاک نظامی. *دوفصلنامه علمی بازی جنگ*، ۶ (۱۳)، ۱۵۵-۱۸۲.

DOI: 10.22034/ijwg.2024.468605.1088

ناشر: دانشگاه فرماندهی و ستاد ارتش جمهوری اسلامی ایران

مقدمه

در سال‌های اخیر رویکرد جنگ شبکه محور باعث بروز و استفاده از فناوری‌ها و نوآوری‌های جدید جهت برقراری ارتباطات در میدان نبرد گردیده که یکی از این فناوری‌ها و نوآوری‌ها، تلفیق فضای سایبر با طیف الکترومغناطیس و بهره‌برداری مشترک و هماهنگ از آن‌ها است. شبکه‌های اد_هاک نمونه‌ای ازاین‌گونه شبکه‌ها است که مجموعه‌ای از گره‌های متحرک، یک شبکه موقت را بدون کمک مدیریت متمرکز یا دستگاه‌های پشتیبانی استاندارد تشکیل می‌دهند (Narsimha, 2012). استقرار سریع یکی از ویژگی‌های اصلی شبکه‌های اد_هاک است. این ویژگی باعث می‌شود شبکه‌های اد_هاک برای انواع محیط‌های که ارتباط در آنجا نقش حیاتی دارد مناسب گردد. شبکه اد_هاک به دلیل ماهیت پویا و انعطاف‌پذیر آن، کاربردهای زیادی دارد، مانند عملیات اضطراری، امدادرسانی در بلایا، عملیات نظامی، شبکه وسایل نقلیه، جلسات و غیره (Choudhary, Narayan, Faiz, & Pramanik, 2022).

با نگرش به اینکه در حال حاضر شبکه‌های اد_هاک در سامانه‌های کنترل و فرماندهی بسیاری از کشورهای پیشرفته به شکل گسترده در حال بهره‌برداری است یکی از راه‌های ایجاد تأخیر و از کار انداختن این سامانه‌های درجه اول بررسی راه‌های نفوذ به این شبکه و در مرحله بعد روش‌های مقابله با آن است، به نظر می‌رسد تحقیق در این زمینه لازم بوده و می‌توان با بررسی‌های لازم، راه‌های نفوذ به این شبکه و روش‌های مقابله با آن را روشن ساخت.

در طول دهه گذشته، علاقه زیادی به استفاده از شبکه‌های بی‌سیم در یگان‌های نظامی سراسر دنیا وجود داشته است، زیرا هزینه دستگاه‌های بی‌سیم همراه مانند پی دی ای[1]، رایانه همراه، تلفن‌های همراه و غیره به‌شدت کاهش‌یافته است. آخرین تغییرات در شبکه‌های بی‌سیم به سمت محاسبات فراگیر که هم برای کاربران سیار و هم کاربران ثابت، در هر زمان و هر مکان، قابل‌ارائه هستند پیش می‌رود. استانداردهای متعددی برای شبکه‌های بی‌سیم به‌منظور رفع نیازهای کاربران به بهره‌برداری رسیده است. یکی از رایج‌ترین اشکال شبکه‌های بی‌سیم که امروزه مورداستفاده ارتش‌های دنیا قرار می‌گیرد، شبکه محلی بی‌سیم اد_هاک است (Chlamtac, Jennifer, & LIU, 2004).

جهت برقراری ارتباط پایدار و مداوم میان سربازان در یک میدان نبرد (شامل نیروهایی از یک یکان سازمانی که در یک منطقه بزرگ پراکنده شده‌اند) با سامانه فرماندهی، استفاده از یک نقطه دسترسی بی‌سیم ثابت نه‌تنها امکان‌پذیر نیست، بلکه خطرناک نیز هست، زیرا دشمن می‌تواند با

[1] Personal Digital Assistant (PDA)

حمله به آن کل شبکه را مختل نماید یا از بین ببرد. این مشکل منجر به علاقه روزافزون جامعه تحقیقاتی به شبکه‌های موقت موبایل[1] شده است. با استفاده از شبکه‌های اد_هاک، امکان برقراری ارتباط بین دستگاه‌های نظامی در مناطق دورافتاده، در شرایط آب و هوایی سخت و حتی در مناطقی با شرایط زیرساختی نامناسب، مانند مناطق جنگی وجود دارد. این شبکه‌ها به‌صورت خودکار و بدون نیاز به تنظیمات پیچیده، ارتباط بین دستگاه‌ها را برقرار می‌کنند و به دلیل قابلیت تحمل خطا و قابلیت اصلاح خطا، در فعالیت‌های نظامی مورداستفاده قرار می‌گیرند.

از اواسط دهه ۹۰، پنتاگون تلاش‌های خود را بر روی وعده ایجاد نیروهای سبک‌تر و کشنده‌تر با استفاده از اصول جنگ شبکه محور متمرکز کرده است. با بهره‌گیری از فناوری اطلاعات برای اتصال حسگرها، تیراندازان و تصمیم‌گیرندگان به یکدیگر در یک فضای مشترک، یک نیروی نظامی می‌تواند به کشف سریع و هم‌زمان فعالیت‌ها و تمایلات دشمن دست یابد (Brent A, Major, & USAF, 2007). شبکه اد_هاک چندین مزیت قابل‌توجه برای یک نیروی نظامی ارائه می‌دهد. ازجمله آن‌ها می‌توان به توانایی شبکه اد_هاک برای شکل‌دهی و مدیریت خود اشاره کرد که نیاز به مدیریت فشرده مرکزی پیوندهای شبکه را از بین می‌برد، بنابراین نیاز به کارکنان و تجهیزات پشتیبانی را در مناطق واقع در جلوی منطقه نبرد کاهش می‌دهد. همچنین فنّاوری‌های شبکه اد_هاک به گره‌های سیار اجازه می‌دهند تا داده‌ها را راحت‌تر به اشتراک بگذارند و نسبت به نیروی غیرشبکه‌ای به کسب آگاهی از موقعیت سایر گره‌ها دست یابند. این افزایش آگاهی از موقعیت، سنگ بنای توانمندسازی اصول جنگ شبکه محور در مشارکت و خود همگام‌سازی با شبکه اصلی است (Brent A, Major, & USAF, 2007, p. 13).

شبکه‌های اد_هاک در ارتش امریکا، به‌عنوان یکی از فنّاوری‌های مهم برای ارتباطات نظامی درزمینه‌های مختلف، مانند عملیات نظامی، ارتباطات جاسوسی، کنترل سطح سلامت نفرات، جمع‌آوری اطلاعات محیط عملیات با استفاده از حس‌گرها، برقراری ارتباط با پهپادها درصحنه نبرد و غیره استفاده می‌شوند. با توجه به اینکه ارتش ایالات‌متحده امریکا از این نوع شبکه‌ها در سطح وسیع استفاده می‌نماید (Sharma & Jangra, 2015, p. 1626)، بایستی بررسی در خصوص انواع شیوه‌های نفوذ به این شبکه‌ها و همچنین راه‌کارهایی برای مقابله با آن صورت پذیرد. برای مقابله با این کشورها در نبردهای احتمالی، لازم است بتوان با استفاده از روش‌های امنیتی مناسب، به این‌گونه شبکه‌ها نفوذ کرده و با انجام انواع روش‌های حمله و فریب الکترونیکی و سایبری، بهره‌برداری از آن‌ها را مختل و یا با مشکل همراه کرد. مشکل اصلی در این زمینه نبود اطلاعات امنیتی دقیق و به‌روز برای نفوذ به این شبکه‌ها است. لذا محقق در این تحقیق قصد دارد بامطالعه

[1] Mobile Adhoc Network (MANET)

دقیق و علمی مدارک و مستندات و با بهره‌گیری ازنظر صاحب‌نظران این حوزه، روش‌های نفوذ به شبکه‌های اد_هاک نظامی را از بعد امنیتی یکپارچگی (صحت)[1] بررسی نماید.

مبانی نظری و پیشینه‌های پژوهش

تاریخچه شبکه اد_هاک

"اد_هاک" یک کلمه لاتین به معنای "برای این" یا "برای این منظور" است. اصطلاح "شبکه اد_هاک" به توانایی اعضای یک شبکه برای برقراری ارتباط شبکه بین دستگاه‌ها اشاره دارد (Rennie, 2022 & Nabben).

کل چرخه حیات شبکه‌های اد_هاک را می‌توان به سیستم‌های شبکه‌های اد_هاک نسل اول، دوم و سوم طبقه‌بندی کرد. سیستم‌های شبکه‌های اد_هاک فعلی نسل سوم محسوب می‌شوند. نسل اول به سال ۱۹۷۲ برمی‌گردد. در آن زمان به آن‌ها شبکه‌های رادیویی بسته‌ای[2] می‌گفتند. (Sharma & Jangra, 2015).

نسل دوم شبکه‌های اد_هاک در دهه ۱۹۸۰ پدیدار شد، زمانی که سیستم‌های شبکه اد_هاک به‌عنوان بخشی از برنامه شبکه‌های رادیویی تطبیقی قابل بقاء ارتقا یافتند و پیاده‌سازی شدند. این برنامه با کوچک‌تر کردن، ارزان‌تر کردن و مقاوم‌تر کردن دستگاه‌های بیسیم در برابر حملات الکترونیکی، در بهبود عملکرد دستگاه‌های بیسیم سودمند بود.

در دهه ۱۹۹۰، مفهوم شبکه‌های اد_هاک تجاری با رایانه‌های نوت بوک و سایر تجهیزات ارتباطی قابل دوام مطرح شد. در همان زمان، ایده مجموعه‌ای از گره‌های سیار در چندین اجلاس تحقیقاتی مطرح شد. از اواسط دهه ۱۹۹۰، کارهای زیادی روی استانداردهای موردی انجام‌شده است. در حال حاضر دو نوع شبکه بی‌سیم موبایل وجود دارد. اولین مورد به‌عنوان شبکه‌های زیرساختی با دروازه‌های ثابت و سیمی شناخته می‌شود. کاربردهای معمول این نوع شبکه بی‌سیم "یک هاپ[3]" شامل شبکه‌های محلی بی‌سیم[4] است. نوع دوم شبکه‌های بی‌سیم سیار، شبکه موبایلی با زیرساخت کمتر است که معمولاً به‌عنوان شبکه‌های موقت موبایل[5] شناخته می‌شود. (Sharma & Jangra, 2015)..

[1] Integrity
[2] Packet Radio Network (PRNET)
[3] One-hop
[4] wireless local area networks (WLANs)
[5] Mobile Ad-hoc Networks (MANET)

تفاوت شبکه اد_هاک و شبکه سلولی

شبکه‌های اد_هاک[1] و شبکه‌های موقت تلفن همراه به‌عنوان دو نوع شبکه بی‌سیم که قبل از استفاده نیازی به راه‌اندازی زیرساخت ندارند شناخته می‌شوند، به این معنا که لازم نیست در یک مکان ثابت شوند. در این شبکه‌ها هیچ‌گونه مسیریاب یا نقطه دسترسی در شبکه وجود ندارد و مسیریابی به‌عنوان یک تلاش گروهی در نظر گرفته می‌شود. هر گره به دور زدن داده‌ها روی گره‌های دیگر کمک می‌کند و گره‌ها می‌توانند آزادانه در اطراف حرکت کنند، این شبکه‌ها، شبکه اد_هاک نامیده می‌شوند (Das, Rao, Das, Jain, & Singh, 2022).

شبکه‌های بی‌سیم اد_هاک نیازی به راه‌اندازی یا اجرا توسط افراد ندارند. همه آن‌ها باید ترافیک سایر گره‌ها را نیز ارسال کنند. ساختن شبکه‌های اد_هاک متحرک چالش برانگیزترین بخش است. بین دو گره، ممکن است یک یا چند فرستنده و گیرنده وجود داشته باشد که همگی با یکدیگر متفاوت باشند. درنتیجه توپولوژی شبکه بسیار تغییر می‌کند و بسیار وابسته به خود است (Agrawal, et al., 2023).

برتری شبکه‌های "اد_هاک" این است که نیازی به زمان طولانی‌مدت جهت راه‌اندازی و زیرساخت خاصی ندارند و در مواقع اضطراری مانند بلایای طبیعی یا جنگ می‌توانند به‌سرعت راه‌اندازی شوند. راه‌های زیادی برای ایجاد یک شبکه بی‌سیم کوچک بدون ساختن یک وب‌سایت وجود دارد. مردم می‌توانند شبکه‌های بداهه و آنی را در محل راه‌اندازی کنند تا یک شبکه بی‌سیم ارزان بسازند (Sorribes, Lloret, & Peñalver, 2022).

افراد بسیاری از یک شبکه بی‌سیم موقت برای اتصال چندین دستگاه بی‌سیم به اینترنت از طریق یک دستگاه واسطه موقت، استفاده می‌کنند. این دستگاه واسطه یک رایانه یا لپ‌تاپ با اتصال اینترنت سیمی و یک تراشه یا آنتن بی‌سیم است که می‌تواند به سایر دستگاه‌های دارای قابلیت بی‌سیم متصل شود و اینترنت را با دستگاه‌های دیگر به اشتراک بگذارد. هنگامی‌که زیرساخت شبکه ثابت وجود ندارد، هر گره شبکه بسته‌هایی را به گره‌های دیگر ارسال می‌کند، حتی اگر آن گره مقصد نهایی نباشد (Quanrun, Debiao, Zhichao, Qi, & Kim-Kwang Raymond, 2022).

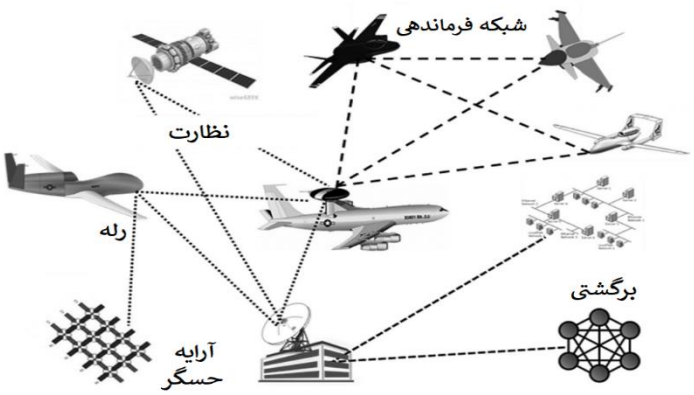
شبکه‌های اد_هاک باید معماری همتا به همتا داشته باشند و توپولوژی شبکه بر اساس تعداد افراد و کاربران موجود در یک مکان تعریف می‌شود. تلفن‌های همراه برد محدودی دارند، بنابراین ممکن است برای رساندن یک بسته به مقصد به کمک تلفن‌های دیگر نیز نیاز داشته باشند. هنگامی‌که دو میزبان تلفن همراه متصل می‌شوند، ممکن است تعداد زیادی پرش بی‌سیم وجود

[1] Wireless ad hoc network

داشته باشد. ساختار شبکه غیرقابل پیش‌بینی، کنترل غیرمتمرکز و اتصالات پرسرعت، اطمینان از قابل‌اعتماد بودن ارتباطات پرسرعت در شبکه‌های بی‌سیم موقت را دشوار می‌سازد، زیرا راه‌های مختلفی برای رسیدن بسته به یک گره وجود دارد (Kaur, et al., 2022).

در عوض، گره‌های شبکه، بسته‌های یکدیگر را از طریق چندین میزبان با استفاده از توپولوژی خود ساخته به مقصد نهایی ارسال می‌کنند. نمونه‌ای از توپولوژی معمولی شبکه‌های اد_هاک متحرک در شکل (۱-۲) نشان داده‌شده است.

شبکه‌های اد_هاک متحرک به تلاش بسیار کمی برای استقرار نیاز دارند و همین ویژگی آن را برای استفاده کوتاه‌مدت مانند کار نجات و اجلاس بسیار جذاب می‌کند. این شبکه‌ها برای خدمات اضطراری مانند بازیابی بلایا که در آن دسترسی سریع به ارتباطات بی‌سیم معمول که وابسته زیرساخت ثابت بوده و یا ارتباطات باسیم، بی‌اثر است یا در دسترس نیست، ضروری هستند. هر



شکل (۱-۲): نمونه توپولوژی معمولی شبکه‌های اد_هاک متحرک در میدان نبرد

گره در شبکه ممکن است به‌عنوان منبع، مقصد یا مسیریاب عمل کند. از آنجایی که هر گره به‌عنوان یک روتر نیز کار می‌کند و بسته‌ها را به گره دیگر ارسال می‌کند، نیاز به زیرساخت‌های دیگر را برطرف می‌کند (Singh, Dutta, & Chakrabarti, 2018).

جایگاه فعالیت‌های سایبر الکترومغناطیس در عملیات‌های نظامی

شبکه‌های موقت در محیط نظامی به‌عنوان یک ابزار ارتباطی حیاتی عمل می‌کنند و انعطاف‌پذیری، سازگاری و کنترل‌پذیری ویژگی‌هایی مانند فرکانس، پهنای باند، سرعت انتقال اطلاعات و زمان پاسخ را فراهم می‌کنند. این شبکه‌ها برای هماهنگی و کنترل عملیات، ارسال

اطلاعات حیاتی (صدا، داده، ویدئو) و اطمینان از تداوم ارتباطات با وجود محیط‌های متفاوتی که ممکن است ایجاد شود، ضروری هستند. آن‌ها در تمام سطوح و در محیط‌های مختلف مانند زمین، هوا و فضا مورد استفاده قرار می‌گیرند. شبکه‌های اد_هاک نیروهای مستقر در میدان، اعم از نیروهای زمینی و هوایی را قادر می‌سازند حتی در سناریوهای بسیار پیچیده جغرافیایی و عملیاتی عمل کنند. آن‌ها ارتباطات چند باندی، پیوند شبکه مبتنی بر ای‌پی، دریافت چند کاناله و مدیریت شبکه تلفن همراه موقت را ارائه می‌دهند و امکاناتی را برای پیکربندی ارتباطات بدون پیچیدگی و ایمن فراهم می‌کنند. این شبکه‌ها نقش مهمی در تضمین ارتباطات مؤثر و ایمن در عملیات نظامی ایفا می‌کنند (Velastegui, Pavon, Jacome, Torres, & Pico, 2022).

فعالیت‌های الکترومغناطیسی فضای سایبری، به اصول مشترک عملیات پایبند است و از بین این اصول، تمرکز قوا، وحدت تلاش، غافلگیری و امنیت بیشترین اهمیت را دارند. فرماندهان و کارکنان قبل از انجام عملیات فضای سایبری و جنگ الکترونیک از رعایت این اصول توسط مقامات مربوطه و چارچوب‌های قانونی مرتبط اطمینان حاصل می‌کنند. هنگام انجام عملیات فضای سایبری، ارتش بر اساس اختیارات فرماندهی عمل می‌کند. به‌عنوان‌مثال، ارتش نیروهایی را برای عملیات تهاجمی فضای سایبری[1] فراهم می‌کند، اما این عملیات را جز به‌عنوان بخشی از نیروی مشترک و طبق تائید فرماندهی نیروی مشترک[2] انجام نمی‌دهد (FM 3-0, OPERATIONS, 2017).

فرماندهان ارتش و کارکنان آن، فعالیت‌های الکترومغناطیسی فضای سایبری را برای برنامه‌ریزی، ادغام و همگام‌سازی عملیات‌های فضای سایبری و جنگ الکترونیک و به‌عنوان تلاشی واحد برای ایجاد قدرت در فضای سایبری و طیف الکترومغناطیسی انجام می‌دهند. اجرای عملیات فضای سایبری و جنگ الکترونیک، ارتش را قادر می‌سازد تا از شبکه‌های نیروی خودی و هم‌پیمان، دفاع نماید و از کارکنان، امکانات و تجهیزات محافظت کند. عملیات مدیریت طیف، فعالیت‌های الکترومغناطیسی فضای سایبری را با اطمینان از دسترسی و عدم تعارض برای استفاده ارتش از طیف الکترومغناطیسی فعال می‌کند. برنامه‌ریزی، ادغام و هماهنگ‌سازی اقدامات مرتبط باهم از مأموریت کلی پشتیبانی می‌کند (Joint Publication 3-85, 2020).

نیروهای ارتش (امریکا)، عملیات فضای سایبری و فعالیت‌های پشتیبانی را به‌عنوان بخشی از عملیات بین ارتش و نیروهای عملیات مشترک انجام می‌دهند. ازآنجایی‌که فضای سایبری یک رسانه جهانی ارتباطی و اشتراک‌گذاری داده است، ذاتاً یک منبع مشترک، بین سازمانی،

[1] Offensive Cyberspace Operations (OCO)
[2] Joint Force Commander (JFC)

چندملیتی و اغلب یک منبع اشتراک‌گذاری است و سازمان‌های اطلاعاتی و سیگنالی در این فضا دارای ارزش‌های قابل‌توجهی هستند (FM 3-0, Operations, 2022).

رادیوهای تاکتیکی مدرن بر پایه شبکه‌های اد_هاک

لینک داده‌های تاکتیکی[1]: لینک داده تاکتیکی، یک شبکه اد_هاک با یک وظیفه خاص است که دارای دو یا چند واحد (گره) مجهز به ارتباطات بی‌سیم با قابلیت یکپارچه‌سازی شبکه برای برقراری تماس مستقیم یا غیرمستقیم است. از ویژگی‌های شبکه لینک داده‌های تاکتیکی، خودسازمان‌دهی و سازگاری است. حتی زمانی که داده در حال تبادل است، مسیر از مبدأ به گره مقصد نیازی به سیستم مدیریت ندارد. عملکرد یک لینک داده تاکتیکی شامل یک گره/واحد منبع است که مایل به برقراری ارتباط با گره دیگری به نام مقصد است که این ارتباط می‌تواند به طور مستقیم یا از طریق گره‌های رله انجام پذیرد. گره‌ها دارای یک رابط انسان- ماشین[2]، یک ماژول پردازنده و یک ماژول انتقال هستند که امکان پخش اطلاعات را فراهم می‌کند (Castro, Sánchez Marín, Agredo Méndez, & Segovia Forero, 2020).

بیشتر پیوندهای داده تاکتیکی، توسط سازمان پیمان آتلانتیک شمالی (ناتو) یا توسط شرکت‌های تجاری خصوصی ایجاد می‌شوند. "این پیشرفت‌ها منبع باز، عمومی یا برای استفاده عمومی نیستند". شبکه سفارشی‌سازی برای کاربر نهایی در دسترس نیست و سازنده اصلی تجهیزات مجاز به انتشار پارامترهای امنیتی شبکه یا سیستم نیست. سناریوی دریای کارائیب با نام پیوند داده‌های تاکتیکی کلمبیا[3] (سی تی دی ال)، یکی از این پروژه‌ها است. با توجه به قابلیت رله گره، گره‌های شبکه اد_هاک و پیوند داده تاکتیکی، باید بتوانند به‌طور هم‌زمان به‌عنوان منبع و رله خدمت کنند که طراحی سی تی دی ال این قابلیت را دارد. با توجه به استفاده از تایمرهای انقضای حافظه پنهان مسیر/جدول، سی تی دی ال از اطلاعات سیستم موقعیت‌یاب جهانی[4] (جی پی اس) در پیام‌های خود برای تعیین موقعیت گره در بین شبکه‌ی ایجاد شده استفاده نموده و همچنین یک ابزار همگام‌سازی هنگام استفاده از سیستم دسترسی چندگانه تقسیم زمان[5] (تی دی ام ای) به‌عنوان یک تکنیک دسترسی به رسانه استفاده می‌کند (Castro, Sánchez Marín, Agredo Méndez, & Segovia Forero, 2020).

---

[1] Tactical Data Link (TDL)
[2] Human Machine Interface (HMI)
[3] Colombian Tactical Data Link (CTDL)
[4] Global Positioning System (GPS)
[5] Time-division multiple access (TDMA)

با توجه به‌اندازه و مقدار گره، سی تی دی ال یک شبکه کوچک در مقایسه با سیستم‌های پیوند داده تاکتیکی استاندارد تولیدشده توسط ناتو است که در آن، شبکه‌ها می‌توانند از دو تا محدوده بین ۱۰۰ تا ۲۰۰ گره یا کاربر (به‌عنوان‌مثال، لینک-22، مطابق با وضعیت پیوندهای داده تاکتیکی دریایی که می‌تواند تا ۱۳۰ ایستگاه را مدیریت کند) را مدیریت نماید. سی تی دی ال دارای ۲۵ گره است که تا ۱۰۰ گره در شبکه قابل‌گسترش است (Castro, Sánchez Marín, Agredo Méndez, & Segovia Forero, 2020).

چالش‌های امنیتی در شبکه‌های موقت بی‌سیم

به‌طورکلی، چندین آسیب‌پذیری را می‌توان در شبکه‌های اد_هاک شناسایی کرد و در سطح بسیار انتزاعی می‌توان آن‌ها را به یکی از مسائل زیر مرتبط کرد:

۱- آسیب‌پذیری کانال: پیام‌ها را می‌توان استراق سمع کرد و پیام‌های جعلی را بدون مشکل دسترسی فیزیکی به اجزای شبکه تزریق یا پخش کرد.

۲- آسیب‌پذیری گره‌ها: ازآنجایی‌که گره‌های شبکه ممکن است در مکان‌های محافظت‌شده فیزیکی قرار نگیرند، می‌توانند به‌راحتی توسط مهاجم کشف (دستگیر) و دست‌کاری شوند. در عمل، یک حریف ممکن است اطلاعات حساس را از آن‌ها بدزدد، رفتار آن‌ها را تغییر دهد یا به سخت‌افزار آسیب فیزیکی وارد کند تا گره‌ها را از کار بیندازد.

۳- عدم وجود زیرساخت: قرار است شبکه‌های اد_هاک مستقل از هر زیرساخت ثابتی کار کنند. این باعث می‌شود راه‌حل‌های امنیتی کلاسیک مبتنی بر مقامات صدور گواهینامه و سرورهای آنلاین غیرقابل اجرا باشند. فرض کلی این است که گره‌هایی که دارای یک کلید مخفی معتبر هستند، قابل‌اعتماد هستند. ما می‌توانیم دو نوع گره غیرهمکار را شناسایی کنیم: گره‌های معیوب یا مخرب و گره‌های خودخواه.

۴- توپولوژی تغییر پویا: اغلب توپولوژی شبکه به‌سرعت تغییر می‌کند؛ بنابراین، پروتکل‌های مسیریابی پیچیده موردنیاز است که امنیت آن‌ها یک چالش اضافی است. درواقع، اطلاعات مسیریابی نادرست می‌تواند توسط گره‌های در معرض خطر یا درنتیجه برخی تغییرات توپولوژی تولید شود. چندین پروتکل مسیریابی برای شبکه‌های اد_هاک معرفی‌شده است و چندین نسخه امن و اصلاحات از این پروتکل‌ها شامل (ARIADNE، SAODV، ARAN، SAR، SRP، SEAD و غیره) پیشنهادشده است (Basagni, Conti, Giordano, & Stojmenovic, 2013).

طبقه‌بندی حملات امنیتی کلاسیک به شبکه‌های اد_هاک

اوساما سبای و محمد البوخاری (۲۰۱۸) در مقاله خود با عنوان "طبقه‌بندی حملات شبکه‌های موقت تلفن همراه" یک طبقه‌بندی حملات را در چهار بعد (۱) وضعیت مهاجم، (۲) شیوه حمله،

(۳) هدف حملات و (۴) لایه‌های شبکه از مدل اتصال سیستم‌های باز را پیشنهاد کرده‌اند. (Sbai & Elboukhari, 2018)

چالش های اصلی که باید توسط سیستم امنیتی شبکه اد_هاک غلبه شود عبارتند از:

• سازگاری داده‌ها: هرگونه تغییر مخرب در روند تبادل اطلاعات حیاتی در شبکه می‌تواند منجر به حوادث غیر قابل جبران گردد، برای جلوگیری از فعالیت‌های مخرب گره‌های احراز هویت شده و غیر احراز هویت شده که باعث ناهماهنگی در داده‌ها می‌شود، باید مکانیزمی طراحی شود. بررسی متقابل اطلاعات دریافتی از گره‌های مختلف برای جلوگیری از چنین فعالیت‌هایی انجام می شود.

• تحرک بالا: این شبکه‌ها بسیار متحرک هستند، بنابراین علیرغم توانایی پردازش و ذخیره‌سازی بالا، به الگوریتم پیچیده‌تری برای امنیت نیاز دارند.

• تحمل خطا: عمل دریافت و پاسخ در در شبکه اد_هاک بسیار سریع است، بنابراین هرگونه اشتباه در پروتکل‌ها یا الگوریتم می تواند به سیستم آسیب جدی وارد کند. بنابراین پروتکل‌ها باید با در نظر گرفتن این موضوع طراحی شوند.

• کنترل تاخیر: اطلاعات به اشتراک گذاشته شده در این شبکه به زمان حساس است. برای دستیابی به محدودیت زمان واقعی، الگوریتم رمزنگاری و سایر الگوریتم‌های مورد استفاده در امنیت باید سریع و کارآمد باشد.

• مدیریت کلید: همه الگوریتم‌های مورد استفاده در امنیت شبکه به کلید وابسته هستند. بنابراین ایجاد، نگهداری و توزیع کلیدها باید به طور ویژه انجام شود.

میتر اتک

شرکت میتر از سازمان‌های دولتی ایالات‌متحده حمایت می‌کند و یک سازمان غیرانتفاعی آمریکایی است. (Copeland, 2021).

در سال ۲۰۱۳ در جهت تجمیع یک ماتریس ساختار یافته از فنونی که توسز مجرمان و هکرهای سایبری مورداستفاده قرار می‌گیرد، برای کار واکنش سریع و به‌موقع به حوادث سایبری ایجاد شد (Enterprise Matrix, 2020).

پایگاه داده میترا تک (تکنیک‌ها، تاکتیک‌ها و دانش مشترک) همان‌گونه که ذکر گردید یک پایگاه در جهت شناسایی روش‌های نفوذ است و مخفف ATT&CK عبارت Adversarial Tactics, Techniques, and Common Knowledge است که:

• A: متخاصم، مانند یک دولت ملی یا سازمان جنایی،

• TT: تاکتیک‌ها و تکنیک‌ها، روش مورد استفاده برای تجزیه‌وتحلیل حملات سایبری؛

• CK: دانش مشترک، مستندسازی تکنیک‌ها و تاکتیک‌ها در قالب یک ماتریس است.

پایگاه داده میتر اتک، یک لیست ساختاریافته از تاکتیک‌ها، تکنیک‌ها و حقایق شناخته‌شده در مورد نفوذگر است که بسته به مرحله و هدف استفاده به گروه‌هایی تقسیم‌شده که در قالب یک ماتریس ارائه‌شده است. طبقه‌بندی روش‌های واقع در پایگاه داده میتر اتک بر اساس وظیفه اجرا شده توسط نفوذگر بر روی حمله کامپیوتری است؛ که لیست آن شامل:

فهرستی از انواع روش‌ها

• دسترسی اولیه؛
• اجرا؛
• ماندگاری؛
• افزایش امتیاز؛
• فرار از دفاع؛
• دسترسی به اعتبار؛
• کشف؛
• حرکت جانبی؛
• مجموعه؛
• استخراج/حذف غیر مجاز داده؛
• دستور و کنترل؛
• تأثیر.

بانک اطلاعات تهدید ازنظر میتر اتک فهرستی از آسیب‌پذیری‌های احتمالی اشیاء در برابر حمله کامپیوتری (شامل اطلاعات بیش از ۲۷ هزار آسیب‌پذیری) و روش‌های پیاده‌سازی این حملات است (Makarova, 2021).

نفوذ در یکپارچگی (صحت)

وقتی در مورد یکپارچگی صحبت می‌کنیم، باید داده‌ها و یکپارچگی خدمات را متمایز کنیم. این حملات سعی می‌کنند داده‌های ارسال‌شده را تغییر دهند. گره‌های مخرب می‌توانند پیام‌های نادرست را تزریق کنند، پیام‌های موجود را تغییر دهند، بسته‌های قدیمی یا کل گره‌ها را تکرار کنند و غیره. هدف از یکپارچگی داده‌ها حفظ یکپارچگی اطلاعاتی است که توسط گره‌ها حس می‌شود.

هدف این حملات مختل کردن خدمات ارائه‌شده توسط شبکه است. بسیاری از حملات انکار سرویس، مسیریابی و فیزیکی در این دسته قرار می‌گیرند و درواقع حفظ عملکرد صحیح

سرویس است. این حملات که در این بخش توضیح داده می‌شود، حملاتی علیه یکپارچگی سرویس هستند.

حملات علیه در دسترس بودن شبکه و یکپارچگی سرویس اغلب به‌عنوان حملات انکار سرویس (DoS) نامیده می‌شود: مهاجم تلاش می‌کند تا سرویس‌های ارائه‌شده توسط شبکه را مختل، وارونه یا نابود کند. حملات DoS می‌توانند هر لایه‌ای از شبکه حسگر را به‌عنوان هدف داشته باشند. درواقع، حملاتی بر روی لایه فیزیکی و همچنین حملاتی به پیوند داده، شبکه و لایه‌های انتقال وجود دارد (Basagni, Conti, Giordano, & Stojmenovic, 2013).

پیشینه‌های پژوهش

جدول (۱): پیشینه تحقیقات انجام‌شده

عنوان پژوهش	اهداف	نتیجه پژوهش	روش‌شناسی	نویسنده و محل اجرای
چالش‌های امنیتی در شبکه‌های اد_هاک	چالش‌های امنیتی در شبکه‌های اد_هاک چیست؟	یک شبکه بی‌سیم، از سیگنال‌های رادیویی برای تبادل داده‌ها بین دو یا چند دستگاه فیزیکی استفاده می‌کند که معمول گره‌های شبکه نامیده می‌شوند. هنگامی‌که گره‌ها به هیچ‌یک از زیرساخت‌های از پیش موجود وابسته نیستند، شبکه‌های بی‌سیم، شبکه‌های اد_هاک بی‌سیم نام می‌گیرند. یک شبکه اد_هاک، اتصالی است که تنها به مدت یک جلسه برقرارمی‌شود و نیاز به ایستگاه پایه ندارد. در عوض، هر دستگاه متصل به شبکه، دیگر دستگاه‌های واقع در یک محدوده خاص را پیدا می‌کند و این دستگاه‌ها یک شبکه بین خود ایجاد می‌کنند. ایجاد امنیت در فرآیند مسیریابی در شبکه‌های اد_هاک یکی از مسائل باز مطرح در طراحی این دسته از شبکه‌ها است. در این مقاله به امنیت و چالش‌های امنیتی در شبکه‌های اد_هاک بپردازد.	روش پژوهش این تحقیق کیفی و با رویکرد مطالعه موردی بود.	متاجی نیمور، سحر، ۱۴۰۰
ارائه روشی به‌منظور تشخیص و مقابله با حملات کرم‌چاله و	ارائه روشی به‌منظور بهبود، شناسایی، تشخیص و مقابله به	در این مقاله به بررسی روش‌های نفوذ در پروتکل در شبکه‌های بیسیم وای فای[1] با پروتکل رمزنگاری دبلیوای‌پی[2] و دبلیوپی‌ای[3]-دبلیوپی‌ای۲ پرداخته که این پروتکل‌ها قسمت عمده‌ای از ارتباطات خانگی و سازمانی را در ارتباطات بیسیم انجام می‌دهند، با ارائه دبلیوپی‌ای۳ کلیه این ایرادات و مشکلات امنیتی رفع شده است؛ اما	در این تحقیق از روش تحقیق علمی تحلیلی استفاده‌شده است.	مولایی فرد، رضا، ۱۴۰۰، دانشگاه آزاد اسلامی

[1] Wireless Fidelity (Wi-Fi)
[2] Wired Equivalent Privacy (WEP)
[3] Wifi Protected Access (WPA)

سیاه‌چاله در شبکه‌های اد_هاک	حملات کرم‌چاله و سیاه‌چاله؟	تجهیزات مجهز به این نوع رمزنگاری در ایران به تعداد کمتری وجود دارند که طبق مطالعات انجام‌شده پروتکل دبلیوای‌پی در بهره‌برداری از آسیب‌پذیری رتبه نخست را دارد و پس‌ازآن پروتکل‌های دبلیوپی‌ای نسخه نخست و دوم در رتبه‌های بعدی هستند.		واحد دزفول، ایران
طبقه‌بندی حملات شبکه‌های موقت تلفن همراه	تکنیک‌های مختلف اجرای حملات اصلی بر روی شبکه‌های اد_هاک متحرک کدامند؟	در این مقاله، حملات مختلف شناخته‌شده علیه شبکه‌های اد_هاک متحرک ارائه‌شده و طبقه‌بندی این حملات را در چهار بعد پیشنهاد داده است: (۱) وضعیت مهاجم، (۲) رفتار حمله، (۳) هدف حملات و (۴) لایه‌های شبکه از مدل مدل اتصال متقابل سامانه‌های باز[1].	در این تحقیق از روش تحقیق علمی تحلیلی استفاده‌شده است.	سبای، اوساما، للبوخاری، محمد، ۲۰۱۸، گروه مهندسی کاربردی، مدرسه عالی فناوری، دانشگاه محمد اول، اوجدا، مراکش

روش‌شناسی پژوهش

نوع تحقیق در این پژوهش از نوع کاربردی بوده و از آنجا که محقق به دنبال شناسایی تهدیدات در حوزه نفوذ بدون هیچ مداخله‌ای است لذا روش تحقیق توصیفی استفاده شده است.

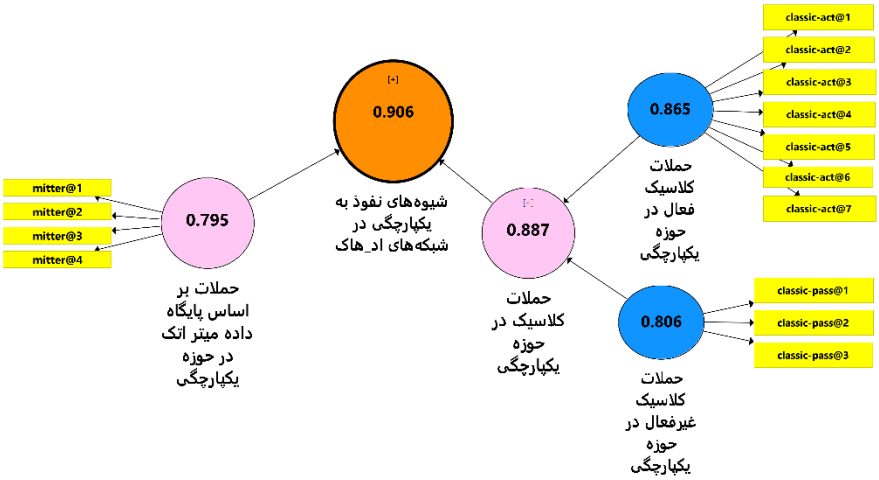
در این تحقیق، به‌منظور پاسخ به سوالات تعیین‌شده تحقیق، محقق پس از جمع آوری اطلاعات از مطالعه منابع علمی و مصاحبه با صاحبی‌نظران، مبادرت به تجزیه‌وتحلیل آنها نموده است. برای احصای مولفه‌ها و شاخص‌های تحقیق، محقق با استفاده از نرم‌افزار اطلس‌تی‌ای (نسخه۸.۴) ، اقدام به تجزیه‌وتحلیل کیفی پیشینه‌های تحقیق، منابع علمی و مصاحبه‌های صورت گرفته به صورت مجزا با عنوان سندهای تفکیک شده نمود و پس از دسته‌بندی داده‌ها و انجام پالایش، تلخیص و نمایش داده‌ها، کدهای باز اختصاص یافته به روایت‌ها احصا گردید.

در گام دوم، پردازش اطلاعات شامل همگرایی داده‌ها (ترکیب)، واگرایی (تعدیل) و تقارن، انجام‌شده است. در نهایت در گام سوم، قضاوت و تصمیم‌گیری با توجه به نوع حملات و داده‌های استخراج شده از دسته‌بندی کدها و پس از پردازش جهت دست‌یابی و رسیدن به هدف مربوطه انجام‌گرفته است.

[1] open systems interconnection (OSI)

پس از احصای شاخص‌های هرکدام از مولفه‌ها، باهدف اندازه‌گیری کمی و دستیابی به بهترین شیوه‌های نفوذ به شبکه‌های اد_هاک نظامی، دیدگاه و نگرش جامعه در پاسخ به سؤالات پرسش‌نامه با استفاده از نرم‌افزار اس‌پی‌اس‌اس تحلیل گردیده است. در نهایت، برای جمع‌بندی نهایی، نتایج به دست آمده از تجزیه و تحلیل کیفی و کمی، درقالب رویکرد آمیخته با یکدیگر تلفیق و نتایج نهایی احصا گردید.

جامعه مورد مطالعه در این تحقیق، کتب، مقالات، اسناد و مدارک موجود و همچنین نظرات اخذ شده در قالب مصاحبه با تعداد ۸ نفر صاحب‌نظرانی خبرگانی است که در حوزه شبکه‌های سایبر الکترومغناطیس، دانش کافی را داشته و به‌صورت عملی در حال فعالیت در این حوزه می‌باشند. جامعه آماری تحقیق، مرحله کمی، ۱۳۰ نفر با مشخصات، آشنایی با شبکه‌های سایبر الکترومغناطیس، آشنایی با شبکه‌های مخابراتی و رایانه‌ای، حداقل دارای مدرک کارشناسی و ۱۰ سال سابقه خدمت باشند بودند که نظرات آنها در قالب پرسشنامه به‌صورت آنلاین دریافت و مورد تجزیه و تحلیل قرار گرفت. روش نمونه‌گیری به صورت تصادفی ساده[1] بوده و جامعه نمونه با فرمول کوکران با سطح خطای ۵ درصد، برابر ۹۷ نفر است. ابزارهای گردآوری اطلاعات به‌صورت میدانی و کتابخانه‌ای بوده و در روش میدانی از ابزار مصاحبه و پرسش‌نامه استفاده گریده است. در این پژوهش از آزمون آلفای کرونباخ جهت بررسی پایایی ابزار سنجش استفاده گردیده است که با استفاده از نرم‌افزار اسمارت پی‌ال‌اس ورژن ۳ محاسبه شده است. نتایج این آزمون را در شکل (۱) و جدول (۳) آورده شده است.



شکل (۱) خروجی نرم‌افزار SMART PLS جهت محاسبه آلفای کرونباخ مؤلفه‌ها

[1] Simple Random Sampling

جدول (۲): مقادیر آلفای کرونباخ و پایایی ترکیبی متغیر تحقیق و مؤلفه‌های آن

متغیر پژوهش	آلفا کرونباخ	پایایی مرکب	مؤلفه‌های پژوهش	آلفا کرونباخ	پایایی مرکب	مؤلفه‌های پژوهش	آلفا کرونباخ	پایایی مرکب
شیوه‌های نفوذ به یکپارچگی در شبکه‌های اد هاک	۰/۹۰۶	۰/۹۲۰	حملات کلاسیک	۰/۸۸۷	۰/۹۰۸	حملات کلاسیک فعال	۰/۸۶۵	۰/۸۹۷
						حملات کلاسیک غیرفعال	۰/۸۰۶	۰/۸۸۵
			حملات بر اساس پایگاه میتر اتک	۰/۷۹۵	۰/۸۶۷			

جدول (۳): مقادیر بارهای عاملی گویه‌ها

شاخص‌ها	مؤلفه تحقیق		
	حملات کلاسیک فعال در حوزه یکپارچگی	حملات کلاسیک غیرفعال در حوزه یکپارچگی	حملات بر اساس پایگاه میتر اتک در حوزه یکپارچگی
حملات تزریق بسته یا پیام	۰/۶۹۵		
حملات علیه مسیریابی	۰/۷۷۱		
حملات ارسال انتخابی	۰/۸۱۶		
حمله بالماسکه کردن	۰/۶۲۱		
حمله تزریق کد آلوده	۰/۷۷۷		
حملات معکوس کردن وضعیت بیت	۰/۷۰۹		
حمله جعل هویت کاربر	۰/۸۱۲		
حملات تحلیل ترافیک		۰/۸۷۰	
حملات استراق سمع		۰/۸۳۱	
حملات مرد میانی غیرفعال		۰/۸۴۴	
تزریق محتوا			۰/۷۷۸
حمله مترجم فرمان و اسکریپت			۰/۷۶۰
حمله مرد میانی			۰.۸۰۰
حملات توسعه بازپخش			۰.۸۱۰

جهت محاسبه پایایی سازه تحقیق از میزان بارعامل شاخص‌ها از طریق محاسبه بار عاملی اقدام می‌گردد. برای محاسبه میزان بار عاملی شاخص‌ها از نرم‌افزار اسمارت پی‌ال‌اس استفاده گردید، بار عاملی مقدار ارتباطی که بین هر یک از شاخص‌های سازه با آن سازه دارد را محاسبه می‌کند، عدد به دست آماده می‌بایست برابر و یا بیشتر از مقدار ۰.۴ شود، این مقدار نشان می‌دهد که واریانس بین سازه‌های تحقیق و شاخص‌های مربوط به آن از واریانس خطای اندازه‌گیری آن سازه بیشتر بوده و در نتیجه پایایی، مدل اندازه‌گیری قابل‌قبول است. همان‌طور که در جدول (۴) آورده شده است کلیه بارهای عاملی شاخص‌های پژوهش بیشتر از ۰/۴ می‌باشد که نشان‌دهنده پایایی قابل‌قبول مدل اندازه‌گیری است.

برای اینکه میزان تغییر رفتار متغیرهای تحقیق بر روی هم را محاسبه کنیم از عامل تورم واریانس[1] استفاده شده است. این عامل شدت میزان هم خطی چندگانه را در تحلیل رگرسیون کمترین مربعات معمولی ارزیابی می‌کند. میزان VIF نشان دهند این است که یک متغیر تا چه اندازه تحت تأثیر دیگر متغیرها رفتارش تغییر می‌کند. عامل تورم واریانس یا VIF از تقسیم عدد یک بر تلورانس حاصل می‌گردد، هرچه میزان ضریب آن از ۲ بزرگ‌تر باشد، میزان هم خطی بین متغیرها نیز بیش‌تر است. برای نتیجه و تفسیر عامل تورم واریانس، هر چه مقدار این ضریب از عدد ۲ بیشتر باشد باعث می‌شود که واریانس ضرایب رگرسیونی افزایش‌یافته و درنتیجه مدل رگرسیون را برای پیش‌بینی نامناسب جلوه می‌دهد. بنابراین هر چه مقدار عمل تورم واریانس برای یک متغیر مستقل بیش‌تر از عدد ۳ باشد نتیجه می‌گیریم که آن متغیر نقش زیادی در مدل، نسبت به بقیه تغییرها ندارد.

جدول (۴): شاخص تورش واریانس VIF بیرونی برای تمامی متغیرهای واردشده

ردیف	حمله	VIF	ردیف	حمله	VIF
۱	حملات تزریق بسته یا پیام	۱/۹۷۰	۸	حملات تحلیل ترافیک	۱/۸۱۶
۲	حملات علیه مسیریابی	۲/۰۹۲	۹	حملات استراق سمع	۱/۱۷۶
۳	حملات ارسال انتخابی	۲/۲۰۲	۱۰	حملات مرد میانی غیرفعال	۱/۶۸۰
۴	حمله بالماسکه کردن	۱/۵۳۴	۱۱	تزریق محتوا	۱/۶۲۲
۵	حمله تزریق کد آلوده	۲/۱۶۰	۱۲	حمله مترجم فرمان و اسکریپت	۱/۴۸۶
۶	حملات معکوس کردن وضعیت بیت	۱/۷۴۷	۱۳	حمله مرد میانی	۱/۶۶۹
۷	حمله جعل هویت کاربر	۲/۱۹۹	۱۴	حملات توسعه بازپخش	۱/۷۷۶

جدول (۵) شاخص تورش واریانس VIF درونی برای تمامی متغیرهای وارد شده

[1] Variance Inflation Factor (VIF)

شیوه‌های نفوذ به یکپارچگی در شبکه‌های اد هاک	
۱/۷۷۲	حملات بر اساس پایگاه داده میتر اتک در حوزه یکپارچگی
۱/۷۷۲	حملات کلاسیک در حوزه یکپارچگی

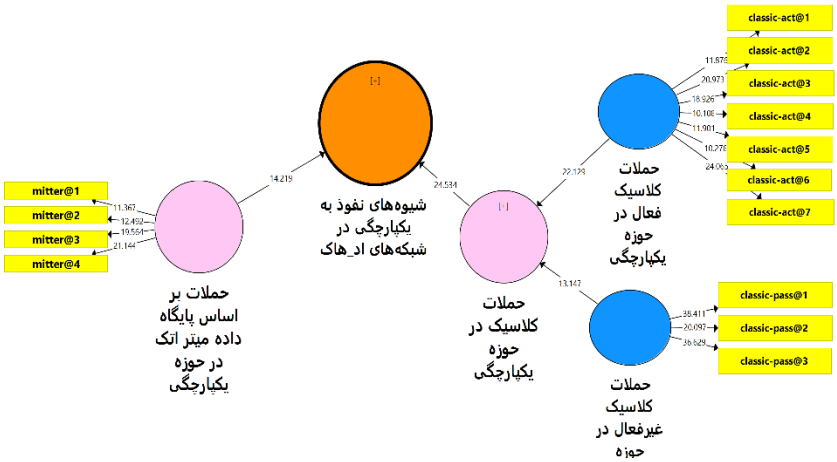
میزان ضرایب به دست آمده از متغیرها و شاخص‌های تحقیق نشان می‌دهد که نقش زیادی در مدل ارائه‌شده دارند و پایایی تحقیق را تائید می‌نماید.

برای سنجش کیفیت و قابل‌قبول بودن ساختار پژوهش، با استفاده از مدل شاخص اندازه‌گیری (شاخص اشتراک) سنجیده شده است، این شاخص توانایی مدل را در پیش‌بینی متغیرهای مشاهده‌پذیر از طریق مقادیر متغیر پنهان متناظرشان می‌سنجد. مقادیر مثبت این ضریب نشانگر آن است که مدل ارائه‌شده کیفیت مناسب و قابل‌قبول را دارد. در جدول زیر می‌توان مقادیر این شاخص که مربوط به هر یک از متغیرها پژوهش است را مشاهده کرد. همان‌طور که مشاهده می‌شود کلیه مقادیر بزرگ‌تر از صفر و مثبت هستند.

جدول (٦): نتایج آزمون کیفیت مدل اندازه‌گیری

متغیر	CV.Com
شیوه‌های نفوذ به یکپارچگی در شبکه‌های اد هاک	۰/۳۶۹
حملات بر اساس پایگاه داده میتر اتک در حوزه یکپارچگی	۰/۳۶۴
حملات کلاسیک در حوزه یکپارچگی	۰/۳۸۳
حملات کلاسیک غیرفعال در حوزه یکپارچگی	۰/۴۱۸
حملات کلاسیک فعال در حوزه محرمانه بودن	۰/۴۰۳

جهت ارزیابی میزان برازش مدل ساختاری ارائه شده بر اساس ضرایب معناداری، مقادیر t-values در نرم‌افزار اسمارت پی‌ال‌اس محاسبه شده است که با اجرای فرمان بوت استراپینگ مقادیر بر روی خطوط مسیرها نشان داده می‌شوند. برای تائید فرضیه پژوهش می‌بایست مقادیر از ۱/۹۶ بیش‌تر باشد، تا صحت رابطه بین سازه‌ها در سطح اطمینان ۹۵ درصد تائید گردد. در شکل (۲) و جدول (۸) می‌توان مقادیر به‌دست‌آمده برای ارزیابی بخش ساختاری مدل نشان داده شده است. که حاکی از معنادار بودن مسیرها، تأیید تمام فرضیه‌های پژوهش و مناسب بودن مدل ساختاری است.



شکل (۲): خروجی نرم‌افزار SMART PLS جهت محاسبه نتایج آزمون مسیر و آماره T

جدول (۷): نتایج آزمون مسیر و آماره T

	ضریب مسیر	میانگین نمونه (M)	انحراف استاندارد (STDEV)	آماره T	مقادیر P
حملات بر اساس پایگاه داده میتر اتک در حوزه یکپارچگی -> شیوه‌های نفوذ یکپارچگی در شبکه‌های اد هاک	۰/۳۵۹	۰/۳۶۲	۰/۰۲۵	۱۴/۲۱۹	۰/۰۰۰
حملات کلاسیک در حوزه یکپارچگی -> شیوه‌های نفوذ به یکپارچگی در شبکه‌های اد هاک	۰/۷۲۹	۰/۷۲۴	۰/۰۳۰	۲۴/۵۳۴	۰/۰۰۰
حملات کلاسیک غیرفعال در حوزه یکپارچگی -> حملات کلاسیک در حوزه یکپارچگی	۰/۳۹۲	۰/۳۹۴	۰/۰۳۰	۱۳/۱۴۷	۰/۰۰۰
حملات کلاسیک فعال در حوزه یکپارچگی -> حملات کلاسیک در حوزه یکپارچگی	۰/۶۹۶	۰/۶۹۳	۰/۰۳۱	۲۲/۱۲۹	۰/۰۰۰

تشریح یافته‌های علمی تحقیق

پژوهش حاضر با هدف شناسایی تهدیدات نفوذ به شبکه اد_هاک نظامی در حوزه یکپارچگی پرداخته که در نهایت با معرفی ۷ حمله کلاسیک فعال، ۳ حمله کلاسیک غیر فعال و ۴ حمله بر اساس پایگاه داده میتر اتک با بیشترین تاثیر بر اساس نتایج بدست آمده از تجزیه‌وتحلیل اسناد و مدارک و استفاده از نظر صاحب نظران به‌دست آمده که می‌توان از اطلاعات آن با تمرکز بر روی این گونه حملات در جهت افزایش کارایی و امنیت شبکه موصوف استفاده نموده. می‌توان از تهدیدات نفوذ به شبکه‌های اد_هاک نظامی در حوزه یکپارچگی به حملات کلاسیک فعال شامل حملات ارسال انتخابی، حمله جعل هویت کاربر، حمله تزریق کد آلوده، حملات علیه مسیریابی، حملات معکوس کردن وضعیت بیت، حملات تزریق بسته یا پیام و حمله بالماسکه کردن اشاره و حملات کلاسیک غیرفعال شامل حملات تحلیل ترافیک، حملات مرد میانی غیرفعال و حملات استراق سمع را نام برد.

می‌توان از تهدیدات نفوذ به شبکه‌های اد_هاک نظامی در حوزه یکپارچگی بر اساس پایگاه داده میتر اتک به حملات توسعه بازپخش، حمله مرد میانی، تزریق محتوا و حمله مترجم فرمان و اسکریپت با بیشترین تأثیر در شبکه اشاره نمود

تجزیه‌وتحلیل داده‌ها

نتایج حاصل از تجزیه و تحلیل اطلاعات جمع آوری شده از مطالعه منابع تحقیق، مصاحبه با صاحب‌نظران، حاکی از این است که درخصوص شیوه‌های نفوذ به شبکه‌های اد_هاک در حوزه یکپارچگی ، تعداد ۱۰شاخص برای مولفه کلاسیک فعال شامل حملات تزریق بسته یا پیام، حملات علیه مسیریابی، حملات فیزیکی فعال، حملات ارسال انتخابی، حملات تزریق/تکثیر/ساخت/تغییر بسته، حملات مرد میانی، حملات تغییر، حمله بالماسکه کردن، حمله تزریق کد آلوده و حمله شکنجه محرومیت از خواب، تعداد ۳ شاخص برای مولفه کلاسیک غیر فعال شامل حملات چندلایه، حملات انکار سرویس و حملات تحلیل ترافیک و تعداد ۴ شاخص برای مولفه میتر اتک شامل حمله تزریق محتوا، حمله مترجم فرمان و اسکریپت، حمله مرد میانی و حملات توسعه بازپخش شناسایی گردید.

تجزیه و تحلیل اطلاعات کمی نظرات جامعه آماری نشان می‌دهد که از میان شاحص‌ها و حملات شناخته شده، حمله تزریق کد آلوده با میانگین (۴/۷۴)، حمله بالماسکه کردن با میانگین (۴/۷۱) و حمله تزریق بسته یا پیام با میانگین (۴/۷۰)، برای مولفه کلاسیک فعال، حمله تحلیل ترافیک با میانگین (۴/۶۶) برای مولفه کلاسیک غیر فعال و حمله مردمیانی با میانگین (۴/۹۲) برای مولفه میتراتک، بهترین حملات به یکپارچگی شبکه های ادهاک نظامی هستند.

بر این اساس می‌توان مدل مفهومی زیر را به عنوان روش‌های نفوذ به مولفه یکپارچگی در شبکه های ادهاک نظامی معرفی کرد.

شکل (۳): مدل مفهومی

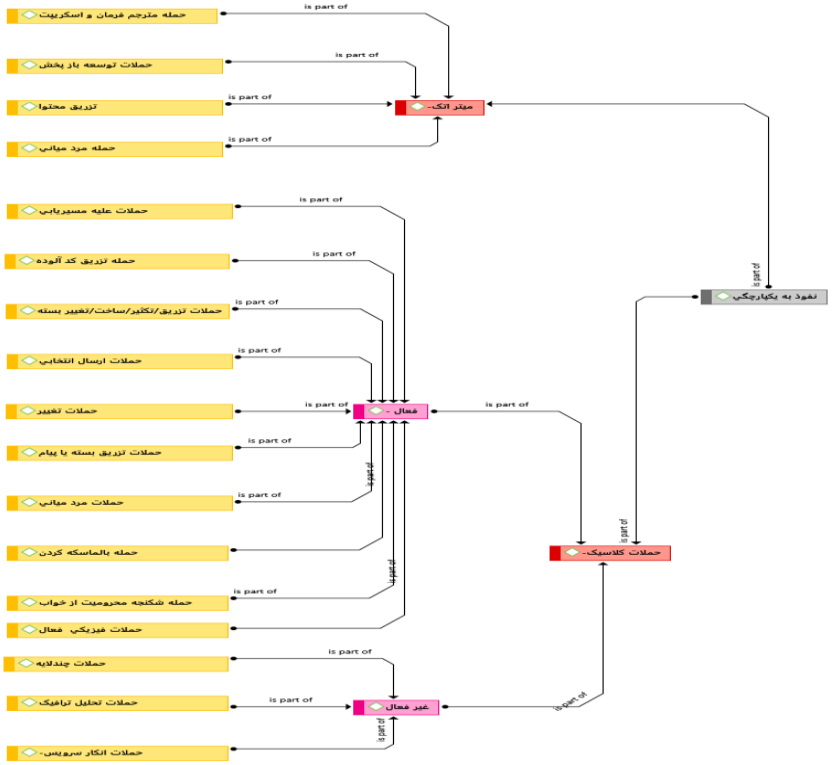
نتیجه‌گیری و پیشنهادها

این تحقیق به‌منظور شناسایی تهدیدات در حوزه نفوذ به شبکه‌های اد_هاک نظامی، انجام‌شده است، در این تحقیق از روش توصیفی با رویکرد آمیخته و ابزارهای اطلس تی ای، اسمارت پی ال اس و اس‌پی‌اس‌اس برای تجزیه‌وتحلیل داده های کیفی و کمی استفاده گردیده است؛ برای دستیابی به نتایج از اسناد و مدارک دسته اول، مصاحبه و پرسشنامه، جهت گردآوری اطلاعات و داده‌های تحقیق، استفاده‌شده است. به همین منظور جهت دسترسی به هدف اصلی پژوهش، منابع تحقیقات گذشته، کتب، اسناد و مدارک موجود و مصاحبه‌های صاحب‌نظران که در راستای اهداف تحقیق بوده با استفاده از نرم‌افزار اطلس تی‌ای مورد تجزیه‌وتحلیل کیفی قرارگرفته و سپس بر اساس نتایج به‌دست‌آمده پرسشنامه تدوین، جهت پاسخگویی برای گروه نمونه ارسال و

پس از جمع‌آوری با نرم‌افزار آماری اس.پی.اس.اس و اسمارت پی‌ال‌اس مورد تجزیه‌وتحلیل قرارگرفته که در جمع‌بندی کلی، نتایج نهایی به شرح زیر استخراج گردیده است.

تهدیدات نفوذ به یکپارچگی در شبکه‌های اد_هاک نظامی در حوزه حملات کلاسیک فعال ۱۰ حمله، در حوزه کلاسیک غیرفعال ۳ حمله و براساس طبقه‌بندی میتر اتک نیز ۴ حمله شناسایی گردیده است. از میان حملات کلاسیک فعال جهت نفوذ به یکپارچگی، حمله تزریق کد آلوده به عنوان بهترین حمله و پس از آن حمله بالماسکه کردن و تزریق بسته یا پیام در رده‌های بعدی قرار می‌گیرند. اگر مهاجم قصد داشته باشد به صورت غیرفعال و به منظور جلوگیری از شناسایی و با هدف به‌دست‌آوردن اطلاعات از شبکه به حوزه یکپارچگی نفوذ کند، برابر نتایج به‌دست آمده بهترین روش تحلیل ترافیک با نرم‌افزارهای معرفی شده در ادبیات تحقیق، حمله انکار سرویس و حملات چند لایه است. با توجه به نتایج در زمینه حملات براساس پایگاه داده میتر اتک، تعداد ۴ حمله برای شبکه اد_هاک بیان شده که مهم‌ترین حملات آن حمله مردمیانی، تزریق محتوا، توسعه بازپخش و مترجم فرمان و اسکریپت هستند.

در شکل (۴) شماتیک شیوه‌های نفوذ به محرمانه بودن نشان داده شده است.



شکل (۴): تهدیدات احصاء شده در حوزه نفوذ به یکپارچگی

پیشنهادها

سازمان‌های فناوری اطلاعات (فاوا) از جمله سازمان فناوری اطلاعات (افتا) نسبت به ایجاد و به‌روزرسانی زیرساخت‌های لازم و نیز سازوکار مورد نیاز برای به‌کارگیری روش‌های نفوذ و حمله به شبکه‌های سایبر الکترومغناطیس، خصوصا شبکه‌های اد_هاک در حوزه یکپارچگی، به روش‌های گوناگون احصا شده در این تحقیق اقدام نماید.

سازمان فناوری اطلاعات (افتا) با همکاری سایر بخش‌های مرتبط از جمله مراکز آپا (آگاهی‌رسانی، پشتیبانی و امداد)، نسبت به محیط‌شناسی (تهدید شناسی) و کشف سامانه‌ها و شبکه‌های اد_هاک هدف، اقدام نماید.

سازمان فناوری اطلاعات با همکاری سایر بخش‌های مرتبط نسبت به تجهیز مراکز سایبری و جنگ الکتر.نیک به توانایی هدایت و کنترل به‌صورت شبکه‌ای، در راستای شناسایی فعالیت شبکه‌های اد_هاک اقدام نماید.

سازمان فناوری اطلاعات با همکاری سایر بخش‌های مرتبط، ازجمله مراکز آپا، فرماندهی یکپارچه هوشمند برای اجرای حملات احصاء شده در تحقیق، رسد و پایش آن طرح‌ریزی نماید و در رزمایش‌های سایبری به‌گونه‌ای طرح‌ریزی نماید تا این اقدام به‌صورت عملی تمرین شود.

پیشنهادهای پژوهشی برای آینده می‌توان به مواردی زیر اشاره نمود،

۱- بررسی چگونگی امکان راه‌اندازی شبکه اد_هاک در راستای برقراری ارتباطی مستمر و مداوم بدون نیاز به زیرساخت؟

۲- بررسی راه‌های اقدام متقابل در برابر هرکدام از حملات پیشنهادی در این تحقیق و شیوه مقابله با آن راه‌کارها؟

۳- ارائه راه‌کار جهت افزایش امنیت در شبکه اد_هاک؟

۴- ارائه یک مدل مسیریابی بهینه برای شبکه اد_هاک؟

۵- برای بررسی تهدیدات در شبکه های اد_هاک، مدل سازی با نرم افزارهای شبیه ساز صورت پذیرد و هر کدام از حمات اشاره شده در این مقاله مورد تجزیه‌وتحلیل قرار گیرد.

۶- ارائه مدل‌سازی مناسب برای نحوه قرارگیری عناصر شبکه و پروتکل های ارسال و دریافت و .. در شبکه اد_هاک؟

منابع

الف- منابع فارسی

- متاجی نیمور، سحر و سهراب پور، حسن،۱۴۰۰،چالش های امنیتی در شبکه هایAd Hoc ، *چهارمین کنفرانس بین المللی مهندسی برق*، کامپیوتر و مکانیک،تهران.
- مولایی فرد، رضا،۱۴۰۰،ارائه روشی به منظور تشخیص و مقابله با حملات کرم چاله و سیاه چاله در شبکه های Ad-Hoc، *فصلنامه نوآوری های فناوری اطلاعات و ارتباطات کاربردی*، دوره:۱، شماره:۲.

ب- منابع انگلیسی

- Aarika, K., Bouhlal, M., AitAbdelouahid, R., Elfilali, S., & Benlahmar, E. (2020). Perception layer security in the internet of things. *International workshop on Artificial Intelligence & Internet of Things (A2IoT)* August 9-12, 2020, Leuven, Belgium, 175, pp. 591–596. doi:10.1016/j.procs.2020.07.085
- Anand, M., Ives, Z., & Lee, I. (2005). Quantifying Eavesdropping Vulnerability in Sensor Networks. Proceedings of the 2nd Workshop on Data Management for Sensor Networks, in conjunction with VLDB, DMSN 2005 (p. 3). Trondheim, Norway,: Data Management for Sensor Networks. doi:10.1145/1080885.1080887
- Barmanroy, D., & Chaki, R. (2014). Different Types of Attacks for WANs. In N. Chaki, & R. Chaki, Intrusion Detection in Wireless Ad-Hoc Networks (pp. 95-110). Taylor & Francis.
- Basagni, S., Conti, M., Giordano, S., & Stojmenovic, I. (2013). MOBILE AD HOC NETWORKING: Cutting Edge Directions (Second ed., Vol. 23). Printed in the United States of America: y John Wiley & Sons, Inc., Hoboken, New Jersey.
- Bhushan, B., & Sahoo, G. (2017, September 08). Recent Advances in Attacks, Technical Challenges, Vulnerabilities and Their Countermeasures in Wireless Sensor Networks. Wireless Personal Communications: An International Journal, 98(2), 2037-2077. doi:10.1007/s11277-017-4962-0
- Bhushan, B., Sharma, S., Kumar, R., & Priyadarshini, I. (2023). 5G and Beyond. Springer Tracts in Electrical and Electronics. doi:https://doi.org/10.1007/978-981-99-3668-7
- Chang, T.-H., Lin, J.-W., Chen, C.-M., & Lai, G.-H. (2018). The Method of Capturing the Encrypted Password Packets of WPA & WPA2, Automatic,

Semi-Automatic or Manual? 2018 IEEE Conference on Dependable and Secure Computing (DSC) (pp. 1-4). Kaohsiung, Taiwan: IEEE. doi:10.1109/DESEC.2018.8625156

- Chaubey, N., & Yadav, D. (2020). A Taxonomy of Sybil Attacks in Vehicular Ad-Hoc Network (VANET). In IoT and Cloud Computing Advancements in Vehicular Ad-Hoc Networks (pp. 174-190). doi:10.4018/978-1-7998-2570-8.ch009
- Douceur, J. (2002, March). The Sybil attack. Revised Papers from the First International Workshop on Peer-to-Peer Systems, 2429, pp. 251-260. London, Springer-Verlag. doi:10.1007/3-540-45748-8_24
- Dubey, A., Meena, D., & Gaur, S. (2014, January). A Survey in Hello Flood Attack in Wireless Sensor Networks. International Journal of Engineering Research & Technology (IJERT), 3(1), 1882-1887. Retrieved from https://www.ijert.org/research/a-survey-in-hello-flood-attack-in-wireless-sensor-networks-IJERTV3IS10747.pdf
- Ghodichor, N., Thaneeghaivl. V, R., Namdeoe, V., & Borkar, G. (2022). Secure Routing Protocol against Internal and External Attack in MANET. Proceedings of The International Conference on Emerging Trends in Artificial Intelligence and Smart Systems, THEETAS 2022. Jabalpur, India: EAI. doi:http://dx.doi.org/10.4108/eai.16-4-2022.2318163
- Ghoreishi, S.-M., Razak, S., Isnin, I., & Chizari, H. (2014). Rushing attack against routing protocols in Mobile Ad-Hoc Networks. International Symposium on Biometrics and Security Technologies (ISBAST), pp. 220-224. doi:10.1109/isbast.2014.7013125
- Goyal , V., & Arora, G. (2017). review Paper on Security Issues in Mobile Adhoc Networks. International Research Journal of Advanced Engineering and Science, 2(1), 203-207.
- Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: Attacks and countermeasures. Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, 2003. (pp. 113-127). Anchorage, AK, USA: IEEE. doi:10.1109/SNPA.2003.1203362
- Khanna, N., & Sachdeva, M. (2019, MAY). A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs. Computer Science Review, 32, 24-44. doi:10.1016/j.cosrev.2019.03.001
- Kinnunen, T., Sahidullah, M., Delgado, H., Todisco, M., Evans, N., Yamagishi, J., & Lee, K. (2017). The ASVspoof 2017 Challenge: Assessing the Limits of Replay Spoofing Attack Detection. The 2nd Automatic

Speaker Verification Spoofing and Countermeasures Challenge (ASVspoof 2017) Database. doi:https://doi.org/10.7488/ds/2105

- Kumar, S., Vasudeva, A., & Sood, M. (2022). Sybil Attack Countermeasures in Vehicular Ad Hoc Networks. International Conference on Communications, Information, Electronic and Energy Systems (CIEES 2022) (pp. 1-6). Veliko Tarnovo, Bulgaria: IEEE. doi:10.1109/CIEES55704.2022.9990799
- Mishra, R., Singh, A., & Kumar, R. (2016). VANET Security: Issues, Challenges and Solutions. International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) (pp. 1050-1055). IEEE. doi:10.1109/iceeot.2016.7754846
- Miter ATT&CK. (2024, 02 02). techniques/T1660/. Retrieved from attack.mitre: https://attack.mitre.org/techniques/T1660/
- Mitre ATT&CK. (2024, 02 02). techniques/T1464/. Retrieved from attack.mitre: https://attack.mitre.org/techniques/T1498/
- Mitre ATT&CK. (2024, 02 02). techniques/T1640/. Retrieved from attack.mitre: https://attack.mitre.org/techniques/T1640/
- Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., & Pantziou, G. (2009). A survey on jamming attacks and countermeasures in WSNs. IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 11, pp. 42-56. doi: 10.1109/SURV.2009.090404
- Noguchi, T., & Hayakawa, M. (2018). Black Hole Attack Prevention Method Using Multiple RREPs in Mobile Ad Hoc Networks. 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). New York, NY, USA: IEEE. doi:10.1109/TrustCom/BigDataSE.2018.00082
- Patel, N., & Tripathi, D. (2018). Trust Value based Algorithm to Identify and Defense Gray-Hole and Black-Hole attack present in MANET using Clustering Method. 4(4).
- Sari, A. (2015). Security Issues in Mobile Wireless Ad Hoc Networks: A Comparative Survey of Methods and Techniques to Provide Security in Wireless Ad Hoc Networks. In M. Dawson, & M. Omar (Eds.), New Threats and Countermeasures in Digital Crime and Cyber Terrorism (1 ed., Vol. 5, pp. 66-94). IGI Global. doi:10.13140/RG.2.1.1826.6725
- Sarika, S., Pravin, A., Vijayakumar, A., & Selvamani, K. (2016). Security Issues In Mobile Ad Hoc Networks. In Chief (Ed.), 2nd International Conference on Intelligent Computing, Communication & Convergence

(ICCC-2016). 92, pp. 329-335. Bhubaneswar, Odisha, India: Elsevier. doi: 10.1016/j.procs.2016.07.363

- Saxena, S., & Deepika, D. (2018). Performance Evaluation of AODV with Self-Cooperative Trust Scheme Using Jellyfish Delay Variance Attack. Proceedings of the Second International Conference on Intelligent Computing and Control Systems (ICICCS 2018) (pp. 1191-1196). Madurai, India: IEEE. doi:10.1109/ICCONS.2018.8662962
- Sbai, O., & Elboukhari, M. (2018). Classification of Mobile Ad Hoc Networks Attacks. Chulalongkorn University provided by UniNet, 618-624.
- Sharma, S., & Jangra, S. (2015). Mobile Ad Hoc Network: Issues, Research Trend And Challenges. International Journal of Advanced Research in Computer Science and Software Engineering, 5(5), 1625-1630. Retrieved from www.ijarcsse.com
- Singh, V., Chandra, R., Raja, L., Sharma, G., & Trivedi, N. (2018). Source Redundancy Management and Host Intrusion Detection in Wireless Sensor Networks. Recent Patents on Computer Science, 12(1). doi:10.2174/2213275912666181207154754
- Sinha, P., Jha, D., Rai, A., & Bhushan, B. (2017). Security vulnerabilities, attacks and countermeasures in wireless sensor networks at various layers of OSI reference model: A survey. 2017 International Conference on Signal Processing and Communication (ICSPC), (pp. 288-293). Coimbatore, India. doi:10.1109/CSPC.2017.8305855
- Sivanesh, S., & Dhulipala, V. (2019). Comparitive Analysis of Blackhole and Rushing Attack in MANET. 2019 TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW) (pp. 495-499). Tiruchirappalli, India: IEEE. doi:10.1109/IMICPW.2019.8933192
- Srinivas, T., & Manivannan, S. (2020, March). Prevention of Hello Flood Attack in IoT using combination of Deep Learning with Improved Rider Optimization Algorithm. Computer Communications 163, 163, 162–175. doi:10.1016/j.comcom.2020.03.031
- Taggu, A., & Marchang, N. (2019). Random-Byzantine Attack Mitigation in Cognitive Radio Networks using a Multi-Hidden Markov Model System. 2019 International Conference on Electrical and Computing Technologies and Applications (ICECTA) (pp. 1-5). Ras Al Khaimah, United Arab Emirates: IEEE. doi:10.1109/ICECTA48151.2019.8959766
- Tamilselvan , L., & Sankaranarayanan, D. (2008, MAY). Prevention of Co-operative Black Hole Attack in MANET. Journal of Networks, 3(5), 13-20.

- Thapar, S., & Sharma, S. (2020). Direct Trust-based Detection Algorithm for Preventing Jellyfish Attack in MANET. 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (pp. 749-753). Coimbatore, India: IEEE. doi:10.1109/ICECA49313.2020.9297601
- Whyte, C., & Mazanec, B. (2023). Understanding cyber warfare: politics, policy and strategy (Second ed., Vol. 5). LONDON AND NEW YORK: Library of Congress Cataloging-in-Publication. doi:https://doi.org/10.4324/9781003246398
- Wood, A., & Stankovic, J. (2002, October). Denial of service in sensor networks. 35(10), 54-62. doi:10.1109/MC.2002.1039518
- Wu, Z., Zhang, Y., Yang, Y., Liang, C., & Liu, R. (2020, September 07). Spoofing and Anti-Spoofing Technologies of Global Navigation Satellite System: A Survey. in IEEE Access, 8, 165444-165496. doi:10.1109/ACCESS.2020.3022294
- Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2021). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. doi:10.1007/s10270-021-00898-7
- Yaroub, H. M., Naif, J. R., & Hasan, S. M. (2022, Aug). Security Challenges And Security Protocols For Wireless Sensor Networks: A Review. International Journal of Advances in Engineering and Management (IJAEM), 4(8), 1696-1706. doi:10.35629/5252-040816961706
- Zhang, Z., Lai, Y., Chen, Y., Wei, J., & Wang, Y. (2023). Detection method to eliminate Sybil attacks in Vehicular Ad-hoc Networks. Ad Hoc Networks, 141. doi:10.1016/j.adhoc.2023.103092