Karafan

Quarterly Scientific Journal of Technical and Vocational University

Autumn 2023, Vol. 20, No. 3, p. 465-484

Journal homepage: https://karafan.tvu.ac.ir/?lang=en

TVU

doi:10.48301/KSSA.2023.409787.2649

Original Research

E-ISSN: 2538-4430
ISSN: 2382-9796

Private Federated Learning for APT Detection in Internet of Drones

Motahareh Dehghan[1], Erfan Khosravian[2*]

[1]Assistant Professor, Department of Industrial and System Engineering, Tarbiat Modares University, Tehran, Iran.

[2]Assistant Professor, Department of Mechanical Engineering, Payam Noor University, Tehran, Iran.

ARTICLE INFO

Received: 08.04.2023
Revised: 08.20.2023
Accepted: 09.11.2023

Keyword:
Internet of Drones
Federated Learning
Privacy
Homomorphic Encryption
Ideal-Real Simulation Paradigm

***Corresponding Author:**
Erfan Khosravian
Email:
erfankhosravain@yahoo.com

ABSTRACT

The Internet of Drones (IoD) is a decentralized network that connects drones to controlled airspace. The connection of drones in these networks is through the Internet of Things. Hence, these networks are vulnerable to all the security and privacy threats that affect IoT networks. In addition, as the application of these networks is highly sensitive in many cases, there are greater potential security threats. The components of these networks work together to identify new and advanced threats. One of the ways to identify new and advanced threats in these networks is distributed machine learning where the data is sent to a central server to learn the general model. This model violates the privacy of network components. It also has a very high level of communication. On the other hand, the central server as the only point of failure may have many problems. In this case, federated learning helps distributed and decentralized networks to share their local model instead of sending their local and secret data. Since the shared models may also disclose some information, we propose a secure and privacy-preserving protocol based on homomorphic encryption. The protocol proposed was for federal learning model and detection of new and advanced threats in the Internet of Drones.

EXTENDED ABSTRACT

Introduction

The Internet of Drones (IoD) is a decentralized network that connects drones to controlled airspace. The connection of drones in these networks is through the Internet of Things. Hence, these networks are vulnerable to all the security and privacy threats that affect IoT networks. In addition, as the application of these networks is highly sensitive in many cases, there are more potential security threats. The components of these networks work together to identify new and advanced threats.

The focus of previous research is on the detection of cyber-attacks in independent drones. The proposed methods are not suitable for distributed architectures such as the Internet of Drones because new threats have a wide variety and have become more complex as exemplified by Advanced Persistent Threats. APTs can be detected when the information on intrusion detection systems, firewalls, antiviruses and other security systems of drones can be obtained. Since drones may not fully trust each other, sharing the information leads to the disclosure of their information. Therefore, privacy violation is one of the problems in this field.

One of the ways to identify new and advanced threats in these networks is distributed machine learning where the data is sent to a central server to learn the general model. This model violates the privacy of network components. It also has a very high level of communication. On the other hand, the central server as the only point of failure may have many problems. In this case, federated learning helps distributed and decentralized networks to share their local model instead of sending their local and secret data. Since the shared models may also disclose some information, we propose a secure and privacy-preserving protocol based on homomorphic encryption. The protocol proposed is for a federal learning model and the detection of new and advanced threats in the Internet of Drones.

Methodology

The proposed protocol is a privacy-preserving federated learning model that can be effectively implemented on an intrusion detection system in the Internet of Drones. Hence, a federated model was first proposed to be used instead of a centralized model. In the proposed model, each sub-network includes several drones that trust each other and at the same time do not fully trust others. Instead of sending their data to a central server to collect data and perform deep learning operations, each of the subnets trains the deep learning model on their side and sends the model parameters to the central server securely. Then, a protocol for securely sending the local parameters of the models, which is the gradient of the deep networks of each sub-network, was designed. The proposed protocol for privacy-preserving federated learning in the Internet of Drones was based on homomorphic encryption. The security of the proposed model was then confirmed, and its complexity was analyzed. Finally, the metrics of the proposed model was evaluate with the centralized model.

Results

In the present paper, the proposed privacy-preserving federated learning protocol based on homomorphic encryption was formally proven to be secure as long as the homomorphic encryption used in this protocol was secure. If the homomorphic encryption is secure against a semi-honest adversary, the proposed protocol is also secure against the self-honest adversary. Moreover, the computational complexity of the proposed protocol was in order of n^2, and its communication complexity was in order of n. For evaluation and comparison of the proposed model with the centralized model, a UAV attack dataset was used. The models were designed and implemented with/ without servers. Then, the dataset was used to evaluate the models. The results are demonstrated in Table 1 as follows:

Table 1. The comparison of models with/ without servers.

	UAV Attack Dataset			
	Accuracy	**Precision**	**Recal**	**F1 Score**
Centralized Deep Learning	0.95	0.947	0.937	0.942
Federated Deep Learning	0.97	0.978	0.968	0.97

Conclusion

In this paper, a private federated learning model that can be effectively implemented in intrusion detection systems in the internet of drones was proposed. In the proposed model, each sub-network included several drones that trusted each other and at the same time did not fully trust each other. Instead of sending its data to a central server to aggregate data and perform deep learning operations, each sub-network trained the deep learning model on its side and sent the model parameters to the central server securely. In this way, while maintaining the privacy of subnets, network traffic was also reduced. The accuracy of attack detection was significantly increased. Moreover, the speed of learning was increased and the traffic overload was reduced. The proposed protocol for private learning of parameters had a computational complexity in the order of n^2 and a communication complexity in the order of n. The evaluation results showed that the model in federated learning model is better than learning with the presence of a central server. Our suggestions for future research are to use the secret sharing scheme, secure multiparty computation, data exchange and storage based on the blockchain to protect the privacy of subnets and prevent the disclosure of their cyber-attack information.

کارافن
فصلنامه علمی دانشگاه فنی و حرفه‌ای
پاییز ۱۴۰۲، دوره ۲۰، شماره ۳، ۴۸۴-۴۶۵
آدرس نشریه: https://karafan.tvu.ac.ir/
doi:10.48301/KSSA.2023.409787.2649

مقاله پژوهشی

شاپای الکترونیکی: ۲۵۳۸-۴۴۳۰
شاپای چاپی: ۲۳۸۲-۹۷۹۶

یادگیری فدرالی حافظ حریم خصوصی برای شناسایی تهدیدات پیشرفتهٔ مانا در سامانهٔ اینترنت پهپادها

مطهره دهقان[۱]، عرفان خسرویان[۲*]

۱- استادیار، دانشکده مهندسی صنایع و سیستم‌ها، دانشگاه تربیت مدرس، تهران، ایران.
۲- استادیار، دانشکده مهندسی مکانیک، دانشگاه پیام نور، تهران، ایران.

اطلاعات مقاله

دریافت مقاله: ۱۴۰۲/۰۵/۱۳
بازنگری مقاله: ۱۴۰۲/۰۵/۲۹
پذیرش مقاله: ۱۴۰۲/۰۶/۲۰

کلید واژگان:
اینترنت پهپادها
یادگیری فدرالی
حریم خصوصی
رمزنگاری هم‌ریخت
پارادایم شبیه‌سازی ایده آل- واقعی

***نویسنده مسئول:** عرفان خسرویان
پست الکترونیکی:
erfankhosravain@yahoo.com

چکیده

اینترنت هواپیماهای بدون سرنشین یا پهپادها، یک شبکهٔ توزیع شده و غیر متمرکز است که دسترسی پهپادها را به حریم هوایی کنترل شده مرتبط می‌کند. اتصال پهپادها در این شبکه‌ها از طریق اینترنت اشیا است. از این رو، این شبکه‌ها در برابر تمام تهدیدات امنیتی و حریم خصوصی که بر شبکه‌های اینترنت اشیا اثر می‌گذارد آسیب پذیر هستند. علاوه بر این، باتوجه به آن که کاربرد این شبکه‌ها در بسیاری از موارد دارای حساسیت بالایی است، تهدیدات امنیتی بالقوه بیشتری را شامل می‌شوند. اجزای این شبکه‌ها با کمک یکدیگر سعی در شناخت تهدیدات پیشرفته و مانا دارند. یکی از روش‌ها برای شناسایی این تهدیدات، یادگیری ماشین توزیع شده می‌باشد. در این روش، داده‌ها برای یک سرور مرکزی ارسال می‌شود و یادگیری در آنجا انجام می‌گیرد. ارسال داده‌ها یا تهدیدات برای سرور مرکزی، حریم خصوصی اجزای شبکه را نقض می‌نماید. در این صورت، یادگیری فدرالی به شبکه‌های توزیع شده و غیر متمرکز کمک می‌کند تا بجای ارسال داده‌های محلی و سری خود، ماشین یادگیرنده را به صورت محلی آموزش دهند و پارامترهای مدل را با یکدیگر به اشتراک گذارند. از آنجا که پارامترهای مدل‌های به اشتراک گذاشته نیز ممکن است حاوی اطلاعاتی از تهدیدات زیرشبکه‌ها باشند، ما در این مقاله یک پروتکل امن و حافظ حریم خصوصی مبتنی بر رمزنگاری هم‌ریخت و برای مدل یادگیری فدرالی جهت تشخیص و شناسایی تهدیدات پیشرفته و مانا در شبکه اینترنت پهپادها پیشنهاد می‌دهیم.

مقدمه

انقلاب صنعتی چهارم[1] به عنوان یکی از خلاقانه‌ترین راه حل‌ها برای سیستم‌های فناوری هوشمند، مانند کارخانهٔ هوشمند، شهر هوشمند، خانهٔ هوشمند و دفتر هوشمند ظاهر شده است. انتظار می‌رود توسعهٔ انقلاب صنعتی چهارم با کاهش هزینه‌های تولید (۴۷٪)، بهبود کیفیت محصول (۴۳٪) و دستیابی به چابکی عملیات (۴۲٪) بیشترین ارزش را به دست آورد [۱]. با اینترنت اشیا، انقلاب صنعتی چهارم می‌تواند به دستاوردهای مهمی در بسیاری از بخش‌ها مانند مراقبت‌های بهداشتی، غذا و کشاورزی دست یابد. به عنوان مثال، انقلاب صنعتی چهارم بخش تولید مواد غذایی را قادر می‌سازد تا بهره‌وری عملیاتی را افزایش دهد، هزینه‌های تولید را کاهش دهد و محصولات پاک، ایمن و با کیفیت را بهبود بخشد.

اینترنت اشیا، یکی از فناوری‌های تاثیرگذار در انقلاب صنعتی چهارم است. در این فناوری، اشیا، انسان‌ها و هر ماهیتی، قابلیت تولید و انتقال داده دارد. یکی از این شبکه‌ها، شبکهٔ اینترنت پهپادها است که اجزای اصلی این شبکه، پهپادها یا هواپیماهای بدون سرنشین برای کاربردهای مختلف، می‌باشند.

غریبی و همکاران [۲]، اینترنت پهپادها[2] را به عنوان یک معماری کنترل شبکه لایه‌ای تعریف کردند که به هماهنگ کردن پهپادها کمک می‌کند [۳]. شبکهٔ اینترنت پهپادها را می‌توان در عملیات جستجو و نجات، نظارت بر ناوگان، بازرسی‌های صنعتی، نظارت بر زیرساخت، سیستم‌های تحویل [۴]، کشاورزی [۵]، [۶]، نقشه‌برداری زنجیرهٔ تأمین، مدیریت بلایا [۷]، [۸]، استفاده نمود. این انتظار وجود دارد که اینترنت پهپادها نقش مهمی در شهرهای هوشمند پیشرفته در آینده نزدیک داشته باشد [۹]. سرویس‌های عمومی پیشرفته اکنون می‌توانند عملیات حیاتی خطر طبیعی و انسانی را با اینترنت پهپادها انجام دهند [۱۰]، [۱۱].

با این حال، ارتباطات بین پهپادها و سایر عناصر شبکه که از طریق کانال‌های بیسیم برقرار می‌شود، هدف بسیاری از حملات سایبری است که محرمانگی[3]، دسترس پذیری[4]، صحت[5] و حریم خصوصی[6] را نقض می‌کنند. این حملات شامل سه دستهٔ اصلی شنود[7]، دستکاری داده[8] و ممانعت از سرویس[9] می‌باشد [۱۲]. یک سامانهٔ مهم و کلیدی برای تشخیص تهدیدات و حملات، سامانه‌های مدیریت رویداد و اطلاعات امنیتی[10] می‌باشد. این سامانه، اطلاعات تهدیدات در سطح یک سازمان را براساس لاگ‌های مختلف سیستم‌ها، شبکه و ... جمع آوری و همبسته‌سازی می‌نماید. همچنین، سامانهٔ تشخیص نفوذ[11] برای تشخیص حملات و نفوذهای رخ داده در یک سازمان می‌باشد. این سامانه، با یادگیری رفتارهای حمله کننده سعی در شناسایی و تشخیص حملات دارند.

از آنجا که در اینترنت پهپادها، زیرشبکه‌ها ممکن است اهداف مختلفی داشته باشند و در محیط جغرافیایی متفاوتی قرار گیرند، تنوع حملات نیز در این زیرشبکه‌ها متفاوت خواهد بود. از این رو، علی‌رغم برخورداری از مزایای برجسته، پیاده‌سازی سامانه‌های تشخیص نفوذ و مدیریت رویداد و اطلاعات امنیتی مبتنی بر یادگیری عمیق در اینترنت اشیای انقلاب صنعتی چهارم با چندین چالش فنی مواجه است. اولاً اینترنت اشیا، یک شبکهٔ غیرمتمرکز با

---

1 Industry 4.0
2 Internet of Drones (IoD)
3 Confidentiality
4 Availability
5 Integrity
6 Privacy
7 Data Interception
8 Data Manipulation
9 Denial of Service (DoS)
10 Security Information and Event Management (SIEM)
11 Intrusion Detection Systems (IDS)

بسیاری از زیرشبکه‌ها[1] است که برای اهداف مختلفی مانند تولید، کشاورزی و تدارکات مستقر شده‌اند. هر زیرشبکه تنها مجموعهٔ کوچکی از دستگاه‌های اینترنت اشیا را کنترل می‌کند و بنابراین داده‌های جمع‌آوری‌شده از هر زیرشبکه معمولاً برای آموزش شبکهٔ یادگیری عمیق برای سیستم تشخیص حملات سایبری کافی نیست. داده‌های ناکافی برای آموزش، دقت مکانیسم یادگیری عمیق را به طور جدی کاهش می‌دهد. در این صورت، زیرشبکه‌ها می‌توانند اطلاعات سامانه‌های تشخیص نفوذ و سامانه‌های مدیریت رویداد و اطلاعات امنیتی خود را به اشتراک گذارند. به اشتراک گذاری داده‌ها بین زیرشبکه‌ها ممکن است باعث نگرانی در مورد حفظ حریم خصوصی و ازدحام شبکه به دلیل تبادل حجم عظیمی از داده‌ها شود. ثانیاً، زیرشبکه‌ها معمولاً توسط دروازه‌های[2] اینترنت اشیا و/یا گره‌های لبه[3] مدیریت می‌شوند که منابع محاسباتی محدودی دارند، و بنابراین اجرای الگوریتم‌های یادگیری عمیق با مجموعهٔ داده‌ای عظیم ممکن است در بلندمدت کارآمد نباشد [۱۳].

یادگیری فدرالی[4]، راه حلی برای رفع چنین چالش‌هایی می‌باشد. در این روش، هریک از زیرشبکه‌ها به طور مستقل و براساس داده‌های محدود محلی خود، مدل محلی را یاد می‌گیرند و پارامترهای مدل خود را با یکدیگر به اشتراک می‌گذارند. از آنجا که مدل اشتراکی نیز منجر به افشای برخی اطلاعات می‌شود، ما در این مقاله، یک مدل یادگیری فدرالی حافظ حریم خصوصی پیشنهاد می‌دهیم که می‌تواند به طور مؤثر بر روی سیستم تشخیص حملات سایبری در شبکه اینترنت پهپادها پیاده‌سازی شود.

در مدل پیشنهادی ما، هریک از زیر شبکه‌ها شامل تعدادی پهپاد است که به یکدیگر اعتماد دارند و در عین حال به پهپادهای سایر زیر شبکه‌ها اعتماد کامل ندارند. هریک از زیر شبکه‌ها به جای ارسال داده‌های خود برای یک سرور مرکزی جهت تجمیع داده‌ها و انجام عملیات یادگیری عمیق، مدل یادگیری عمیق را در سمت خود آموزش می‌دهند و پارامترهای مدل را برای سرور مرکزی ارسال می‌کنند. از آنجا که پارامترهای مدل می‌تواند حاوی اطلاعاتی باشد، ما یک پروتکل حافظ حریم خصوصی برای ارسال پارامترهای مدل به سرور مرکزی پیشنهاد می‌دهیم. بدین ترتیب در ضمن حفظ حریم خصوصی زیرشبکه‌ها، ترافیک شبکه نیز کاهش می‌یابد. ما نه تنها می‌توانیم دقت در شناسایی حملات را به میزان قابل توجهی افزایش دهیم، بلکه سرعت یادگیری را نیز افزایش می‌دهیم. همچنین، ترافیک شبکه را کاهش می‌دهیم و محرمانگی دادگان[5] زیرشبکه‌ها را حفظ می‌کنیم. پروتکل پیشنهادی ما دارای پیچیدگی محاسباتی از مرتبه n^2 و پیچیدگی ارتباطی از مرتبه n می‌باشد. به طور خلاصه دستاوردهای پژوهش حاضر شامل موارد زیر می باشد:

- طراحی یک مدل یادگیری فدرالی برای تشخیص تهدیدات پیشرفته مانا در سامانه اینترنت پهپادها
- طراحی پروتکل حافظ حریم خصوصی و مبتنی بر رمزنگاری هم‌ریخت برای حفظ حریم خصوصی در مدل یادگیری فدرالی

بدین منظور، ما در بخش دوم، پژوهش‌هایی را که در زمینهٔ تشخیص تهدیدات و حملات سایبری پهپادها انجام شده است مرور می کنیم. در بخش سوم، تعاریف و مفاهیم پایه برای ارائه مدل را بیان می‌کنیم. این تعاریف شامل اینترنت پهپادها، یادگیری عمیق مستقیم و غیرمستقیم (فدرالی)، حریم خصوصی و رمزنگاری هم‌ریخت است. در بخش چهارم، مدل پیشنهادی خود را ارائه می‌دهیم. این مدل، تلفیقی از مدل یادگیری فدرالی و رمزنگاری هم‌ریخت برای تبادل امن پیام‌ها است که جزئیات گام‌های انجام شده برای یادگیری فدرالی و مبتنی بر رمزنگاری هم‌ریخت، اثبات، تحلیل پیچیدگی و ارزیابی آن در بخش چهارم بیان می‌شود.

---

[1] Subnets
[2] Gateway
[3] Edge
[4] Federated Learning
[5] Dataset

پژوهش‌های پیشین

نیازمندی‌های امنیتی که در اینترنت پهپادها وجود دارد شامل صحت، محرمانگی، دسترس پذیری، تصدیق اصالت و حریم خصوصی است. ارتباطات بین پهپادها و سایر عناصر شبکه که از طریق کانال‌های بیسیم برقرار می‌شود، هدف بسیاری از حملات سایبری است که این نیازمندی‌های امنیتی را نقض می‌کنند. این حملات شامل سه دستهٔ اصلی شنود، دستکاری داده و ممانعت از سرویس می‌باشد [۱۲]. در [۱۴] برای مقابله با حملاتی که منجر به نقض صحت داده‌ها می‌شود همانند حمله مرد میانی[1] (زیرمجموعهٔ حملهٔ دستکاری داده)، از پروتکل‌های رمزنگاری استفاده شده است. علاوه بر این، نویسندگان آن مقاله پیشنهاد داده‌اند که از روش‌های تشخیص نفوذ بسیار قوی، آنتی ویروس‌های قابل اعتماد، خط مشی‌های سختگیرانه و فایروال‌ها استفاده شود. همچنین، تحلیل کانال جانبی[2] برای تشخیص تروجان‌ها پیشنهاد داده شده است. همچنین، برای جلوگیری از حملات ممانعت از سرویس که منجر به نقض دسترس پذیری پهپادها می‌شود، روش‌های تشخیص نفوذ جهت تمایز قائل شدن بین ارتباطات مخرب و واقعی پیشنهاد داده شده است. همچنین، نویسندگان آن مقاله، حسگرهایی را پیشنهاد داده‌اند که قادر به بررسی وضعیت پرواز پهپادها در زمان واقعی هستند که به خوبی می‌تواند عملکرد نامناسب پهپادها به دلیل رخداد حملاتی مثل ممانعت از سرویس را هشدار دهد. با این حال، نویسندگان مقاله، هیچ‌گونه مکانیزمی که مناسب محدودیت‌های شبکه‌های اینترنت پهپادها است ارائه نداده‌اند. علاوه بر این، در [۱۵] روش مبتنی بر زنجیره بلوکی[3] برای پهپادهایی که سرویس‌های تحویل دهنده محصولات هستند جهت اطمینان از صحت داده‌ها پیشنهاد داده شده است که از قراردادهای هوشمند[4] بین فروشنده و خریدار استفاده می‌کند.

در [۱۶] یک مکانیزم دفاعی با توان مصرفی پایین که برای محدودیت‌های منابع پهپادها کاربردی است پیشنهاد داده شده است. این مکانیزم، جهت مقابله با حملات فیزیکی در شبکه‌های اینترنت پهپادها و دسترس پذیری پهپادها مناسب است. نویسندگان مقاله [۱۷] این موضوع را مطرح کرده‌اند که پهپادهای تجاری، حسگرهای تشخیص مجاورت دارند که تنها اشیای ایستای بسیار بزرگ را تشخیص می‌دهند و قادر به تشخیص اشیای پویا با سرعت بالا را ندارند. بنابراین، جهت حل این مسئله نویسندگان حسگرهایی را پیشنهاد داده‌اند که این ضعف پوشش داده شود و جلو حملاتی را که با استفاده از اشیا با سرعت بالا رخ می‌دهد، بگیرند. حملاتی که در این مقاله مدنظر است منظور حملات فیزیکی می‌باشد.

همچنین برای تصدیق اصالت مؤلفه‌های مختلف ارتباطات پهپادها، در [۱۸] یک طرح تصدیق اصالت بسیار سبک پیشنهاد داده شده است. آن طرح در مقابل حملات شناخته شده تصدیق اصالت مقاوم است. با این حال، در [۱۹] بیان شده است که طرح پیشنهادی در مقاله [۲۰] مقیاس پذیر نیست و تنها در یک منطقهٔ کوچکی از پهپادها قابل استفاده است. همچنین، در مقابل ردیابی آسیب پذیر است. از این رو نویسندگان مقاله [۲۰] طرح جدیدی را پیشنهاد داده‌اند که ضعف‌های طرح قبلی را پوشش داده است.

در زمینهٔ امنیت پهپادها، چندین مقاله مروری ارائه شده است که از جنبه‌های مختلفی به بررسی تهدیدات و اقدامات مقابله‌ای[5] پرداخته‌اند و دسته‌بندی‌های لازم برای آنها ارائه داده‌اند. در [۲۱] مروری بر کاربردهای نظامی پهپادها شده است و حملات و تهدیدات فیزیکی مد نظر قرار گرفته است. در آن مقاله هیچ‌گونه دسته‌بندی از اقدامات مقابله‌ای ارائه نشده است. در [۱۲] تهدیدات امنیتی به سه دسته شنود، دستکاری داده و ممانعت از سرویس تقسیم شده‌اند. در آن

[1] Man in the middle attack
[2] Side channel analysis
[3] Blockchain
[4] Smart Contracts
[5] Countermeasures

مقاله هریک از این دسته تهدیدات را به تهدیدات جزئی‌تر تقسیم نموده و برای هریک از آنها اقدامات مقابله‌ای متناسب را بیان نموده‌اند. در [۲۲] تمرکز بر اقدامات مقابله‌ای امنیتی است. در آن مقاله، اقدامات مقابله‌ای به سه دسته جلوگیری[۱]، تشخیص[۲] و کاهش[۳] تقسیم شده‌اند که آنها برای شش دسته حمله شامل اختلال کانال[۴]، شنود پیام[۵]، پاک نمودن، تزریق[۶] و جعل پیام[۷] و حملات فیزیکی قابل اعمال می‌باشند. در مقاله [۲۳] یک دسته‌بندی توصیفی از انواع تهدیدات امنیتی پهپادها ارائه می‌شود. در آن مقاله انواع معیارهای ارزیابی امنیتی رایج برای تهدیدات امنیتی و اقدامات مقابله‌ای ارائه شده است. همچنین در مقالهٔ مروری مورد نظر، انواع حوزه‌های نوظهور مانند یادگیری ماشین، محاسبات لبه و مه[۸] و زنجیره بلوکی در ارتباطات بین پهپادها مورد بحث قرار گرفته است. در مقاله [۲۳] از یادگیری ماشین برای شناسایی تهدیدات به صورت خودکار یاد شده است. اما اشاره‌ای بر مشارکت شبکهٔ پهپادها در یادگیری ماشین برای شناسایی تهدیدات پیشرفته مانا و تهدیدات جدید نشده است.

در [۲۴] مدل‌های مختلف یادگیری عمیق به کار برده شده است تا از فایل‌های لاگ پرواز پهپادها و داده‌های ارتباطات برای تشخیص جعل ساموجی[۹] در زمان واقعی و به صورت بلادرنگ استفاده نمایند. در آن مقاله، دادگان مورد نیاز برای ارزیابی مدل‌ها ایجاد شده است. روش مورد استفاده در مقالهٔ مورد نظر برای تشخیص حملات جعل ساموجی براساس داده‌های یک پهپاد و مستقل از داده‌های لاگ سایر پهپادها پیشنهاد شده است.

تمرکز پژوهش‌های پیشین بر تشخیص حملات سایبری در پهپادها به صورت کاملا مستقل می‌باشد. به گونه‌ای که از تصدیق اصالت، محافظت‌های فیزیکی، سیستم‌های تشخیص نفوذ، زنجیره بلوکی و سایر روش‌ها برای جلوگیری از حملات سایبری در پهپادها بدون توجه به روابط و شبکه بین آنها استفاده نموده‌اند. روش‌های پیشنهادی برای معماری‌های توزیع شده مانند اینترنت پهپادها مناسب نمی‌باشد. زیرا امروزه تهدیدات، تنوع گسترده‌ای دارند و پیچیده‌تر شده‌اند. به عنوان نمونه تهدیدات پیشرفته مانا[۱۰] به عنوان رایج‌ترین تهدیدات در شرایط کنونی می‌باشد. این تهدیدات زمانی قابل تشخیص هستند که اطلاعات سیستم‌های تشخیص نفوذ، فایروال‌ها، آنتی ویروس‌ها و سایر سامانه‌های امنیتی پهپادها قابل دست‌یابی باشد. از آنجا که ممکن است پهپادها به یکدیگر اعتماد کامل نداشته باشند، به اشتراک‌گذاری اطلاعات مذکور منجر به افشای اطلاعات آنها می‌شود. از این رو نقض حریم خصوصی یکی از مشکلات در این زمینه می‌باشد. ما در این مقاله، یک مدل یادگیری فدرالی حافظ حریم خصوصی برای اشتراک‌گذاری مدل‌های آموزش دیده پهپادها پیشنهاد می‌دهیم.

تعاریف و مفاهیم پایه

اینترنت پهپادها

اینترنت هواپیماهای بدون سرنشین یا پهپادها [۲]، یک معماری کنترل شبکه لایه‌ای است که عمدتاً برای هماهنگ کردن دسترسی وسایل نقلیهٔ هوایی بدون سرنشین به فضای کنترل‌شده و ارائه خدمات ناوبری بین مکان‌های مختلف

[1] Prevention
[2] Detection
[3] Mitigation
[4] Channel Jamming
[5] Interception
[6] Injection
[7] Spoofing
[8] Fog and Edge Computing
[9] GPS Spoofing
[10] Advanced Persistent Threats (APTs)

طراحی شده است. اینترنت پهپادها، خدمات عمومی را برای کاربردهای مختلف هواپیماهای بدون سرنشین مانند تحویل بسته، نظارت بر ترافیک، جستجو، نجات و غیره ارائه می‌دهد.

یادگیری عمیق[1]

یادگیری عمیق [۲۵]، دسته‌ای از الگوریتم‌های یادگیری ماشین است که ساختاری لایه‌ای به نام شبکه‌های عصبی دارد. طرح چنین ساختاری، الهام گرفته از مغز انسان است. هدف یادگیری عمیق، طراحی سیستم‌های کامپیوتری هوشمندی است که بتوانند مشابه انسان دربارهٔ موضوعی خاص، راه حل ارائه کنند و مفاهیم جدید را یاد بگیرند.

در شبکه‌های عمیق، تعداد لایه‌ها بیشتر از دو لایه می‌باشد. در هر گره از این شبکه، ابتدا عملیات جمع انجام می شود. سپس تابع فعالسازی[2] بر روی خروجی عملیات جمع صورت می‌گیرد. این عملیات بر روی تمامی گره‌های شبکه تا لایه آخر انجام می‌شود. سپس، خطای این عملیات محاسبه شود تا براساس آن، میزان نزدیک شدن به هدف اصلی مشخص شود. پس از به دست آوردن خطا، گرادیان محاسبه می‌گردد که برای به روزرسانی وزن یال‌های شبکهٔ عصبی مورد نیاز است. برای محاسبه گرادیان، روش‌های مختلفی وجود دارد که یکی از این روش‌ها، استفاده از نزول گرادیان[3] است.

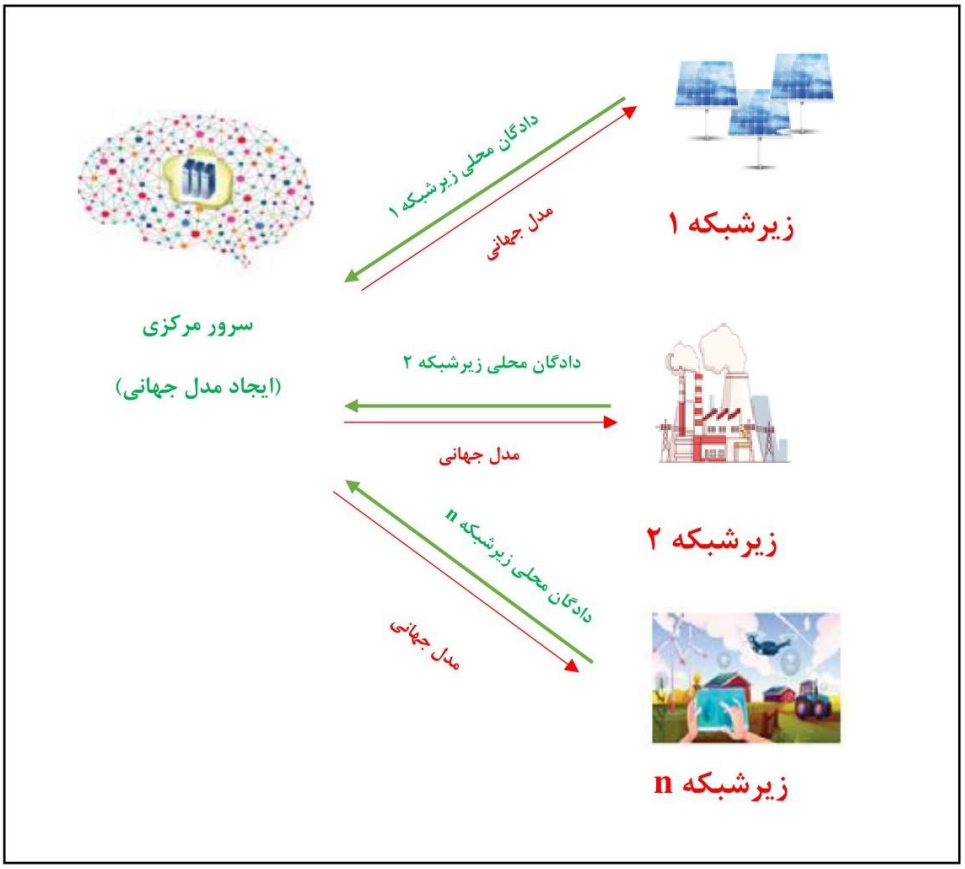
جهت به روزرسانی وزن‌های شبکه، از فرمول (۱) استفاده می‌شود که G مقدار گرادیان محاسبه شده، α نرخ یادگیری[4]، W^{t-1} نیز وزن یال‌ها در زمان t-1 است.

$$W^t = W^{t-1} + \alpha.G \qquad (۱)$$

یادگیری عمیق مشارکتی مستقیم

در یادگیری عمیق مشارکتی مستقیم[5] [۲۵]، یک سرور مرکزی و چندین کاربر وجود دارد. سرور مرکزی از یک مدل جهانی[6] پشتیبانی می‌کند. کاربران دارای دادگان محلی[7] مستقل هستند. در طول فرآیند آموزش[8]، هر کاربر دادگان محلی خود را روی سرور بارگذاری می‌کند. سرور مرکزی داده‌های کاربر را جمع آوری می‌کند و الگوریتم یادگیری عمیق را به صورت مرکزی اجرا می‌کند تا مدل نهایی به دست آید . شکل ۱، روش آموزش یادگیری عمیق مشارکتی مستقیم را نشان می‌دهد که در آن، هریک از زیرشبکه‌ها نقش کاربر را ایفا می‌نمایند.

[1] Deep Learning
[2] Activation Function
[3] Gradient Descent
[4] Learning Rate
[5] Direct Collaborative Deep Learning
[6] Global Model
[7] Local Dataset
[8] Training



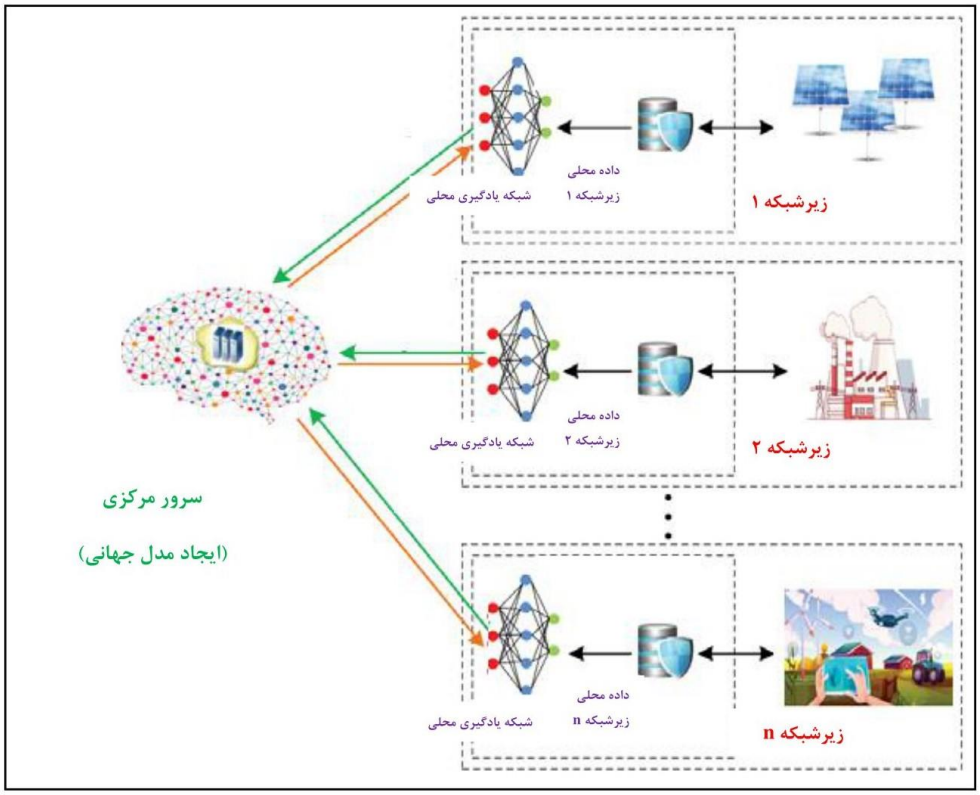
شکل ۱. یادگیری عمیق مشارکتی مستقیم [۲۵]

یادگیری فدرالی (یادگیری عمیق مشارکتی غیر مستقیم)

در یادگیری عمیق مشارکتی غیرمستقیم[1] [۲۵] یا یادگیری فدرالی، یک سرور مرکزی و چندین کاربر وجود دارد. سرور مرکزی از یک مدل جهانی پشتیبانی می‌کند. هر کاربر، یک مجموعه داده محلی دارد و از یک مدل محلی پشتیبانی می‌کند. در طی فرآیند آموزش مدل، کاربر ابتدا مدل جهانی را از سرور مرکزی دانلود می‌کند. سپس با استفاده از دادگان محلی خود، یادگیری عمیق را در سمت خود به صورت محلی انجام می‌دهد و مدل محلی خود را آموزش می‌دهد. نهایتاً پارامتر مدل محلی یا به عبارتی دیگر، گرادیان را برای سرور مرکزی ارسال می‌کند.

سرور مرکزی این اطلاعات را جمع آوری می‌کند تا یک مدل جهانی به روز شده را ایجاد نماید. برای همگرا شدن به مدل بهینه، در فرآیند آموزش چندین تکرار لازم است. نکته حائز توجه این است که در این نوع یادگیری، دادگان در سرور مرکزی بارگذاری نمی‌شوند و از دستگاه کاربر خارج نمی‌شود و صرفاً پارامترهای مدل محلی که همان مقدار گرادیان است، در اختیار سرور قرار می‌گیرد.

[1] Indirect Collaborative Deep Learning



شکل ۲. یادگیری فدرالی (یادگیری عمیق مشارکتی غیرمستقیم) [۲۵]

حریم خصوصی

یکی از مباحث مهم در امنیت اطلاعات، بحث حریم خصوصی[1] است. برای حریم خصوصی در منابع مختلف، تعاریف متفاوتی ارائه شده است که پر استنادترین آن، تعریف وستین است:

حریم خصوصی به معنی حق افراد، گروه‌ها یا مؤسسات برای تعیین این است که چه زمانی، چگونه، تا چه حدی و به چه کسانی اطلاعات مربوط به آنها داده شود [۲۶].

رمزنگاری همریخت

رمزنگاری همریخت[2] [۲۷]، توسط ریوست و همکارانش در سال ۱۹۷۸ ارائه شد. در این طرح رمزنگاری، می‌توان مجموعه‌ای از عملیات را بر روی داده‌های رمز شده، بدون آن که تابع ترجمه رمز را بدانیم، انجام دهیم. وجود طرح‌های رمزنگاری همریخت امن، یک خواستهٔ اساسی برای انجام محاسبات امن چندلایه[3] است. بدین

[1] Privacy
[2] Homomorphic Encryption
[3] Multilayer Secure Computation

صورت که داده‌ها را در اولین سطح رمزنگاری می‌کنیم، سپس محاسبات را در سطح پایین انجام داده و نتیجه را در اولین سطح ترجمه رمز می‌کنیم.

طرح رمزنگاری همریخت دارای ویژگی جمع و ضرب می‌باشد که در فرمول (۲) و (۳) نمایش داده شده‌اند.

$$E(a+b) = E(a) + E(b) \quad (۲)$$

براساس فرمول (۲)، در صورتی که بخواهیم جمع دو مقدار سری a,b را به صورت رمز شده و بدون اطلاع از مقادیر اصلی آنها داشته باشیم، لازم است ابتدا دو مقدار سری را با استفاده از طرح‌های رمزنگاری همریخت، رمز و سپس آنها را جمع نماییم. در این صورت، بدون اطلاع از مقادیر سری، جمع رمزشده آنها را به دست می‌آوریم. از طرف دیگر، ویژگی ضرب مقدار ثابت در رمزنگاری همریخت براساس فرمول (۳) مورد استفاده قرار می‌گیرد.

$$c.E(a) = E(c.a) \quad (۳)$$

پروتکل پیشنهادی مبتنی بر رمزنگاری همریخت

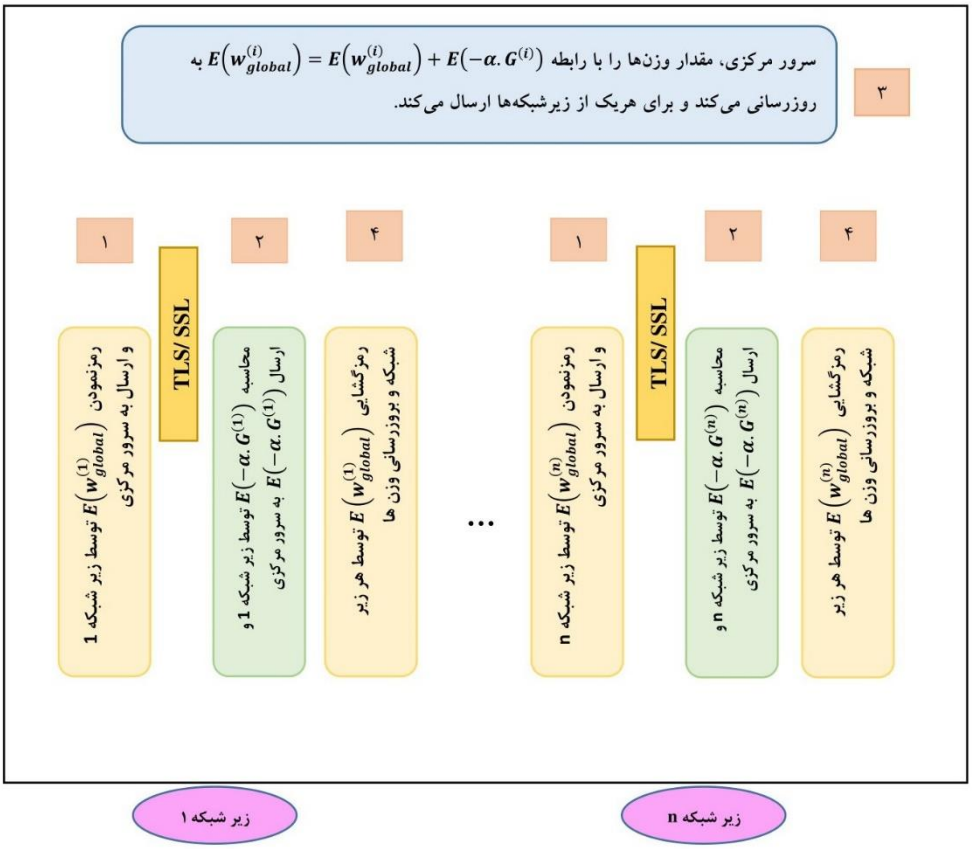
ما در این بخش، یک مدل یادگیری فدرالی حافظ حریم خصوصی پیشنهاد می‌دهیم که می‌تواند به طور مؤثر بر روی سیستم تشخیص حملات سایبری در شبکه اینترنت پهپادها پیاده‌سازی شود. در مدل پیشنهادی ما، هریک از زیر شبکه‌ها شامل تعدادی پهپاد است که به یکدیگر اعتماد دارند و در عین حال به پهپادهای سایر زیر شبکه‌ها اعتماد کامل ندارند. هریک از زیر شبکه‌ها به جای ارسال داده‌های خود برای یک سرور مرکزی جهت تجمیع داده‌ها و انجام عملیات یادگیری عمیق، مدل یادگیری عمیق را در سمت خود آموزش می‌دهند و پارامترهای مدل را برای سرور مرکزی به صورت امن ارسال می‌کنند. بدین منظور، ما پروتکلی برای ارسال امن پارامترهای محلی مدل‌ها که همان گرادیان شبکه‌های عمیق هر زیر شبکه است، طراحی می‌نماییم که در ادامه جزئیات پروتکل مطرح می‌شود.

پروتکل پیشنهادی ما برای یادگیری فدرالی حافظ حریم خصوصی در اینترنت پهپادها، مبتنی بر رمزنگاری همریخت و با استفاده از ویژگی جمع و ضرب این طرح رمزنگاری می‌باشد که در فرمول (۲) و (۳) نمایش داده شده‌اند. این دو ویژگی مطلوب رمزنگاری همریخت، در سمت سرور مرکزی مورد استفاده قرار می‌گیرد که جزئیات آن در ادامه بیان می‌گردد.

- **مرحلهٔ اول پروتکل:** هریک از زیر شبکه‌ها در سمت خود، شبکهٔ عمیقی را ایجاد و براساس دادگان محلی خود، شبکه عمیق محلی را آموزش می‌دهد. سپس، براساس خطا و گرادیان محاسبه شده، وزن‌های شبکهٔ محلی خود را به روزسانی می‌کند. از آنجا که این وزن‌ها حاوی اطلاعاتی دربارهٔ شبکهٔ محلی زیر شبکه است، به جای ارسال وزن‌ها برای سرور مرکزی، مقدار وزن‌های خود $\left(W_{global}^{(i)}\right)$ را با استفاده از رمزنگاری همریخت رمز می‌کند و $E\left(W_{global}^{(i)}\right)$ را برای سرور مرکزی ارسال می‌کند.
- **مرحلهٔ دوم پروتکل:** هر زیرشبکه، گرادیان (G) شبکهٔ محلی خود را در نرخ یادگیری $(-\alpha)$ ضرب می‌کند و $E(-\alpha \cdot G^{(i)})$ را محاسبه و برای سرور مرکزی ارسال می‌نماید.
- **مرحلهٔ سوم پروتکل:** سرور مرکزی، مقدار وزن‌ها را با استفاده از فرمول (۴) بروز رسانی می‌کند و برای هر یک از زیر شبکه‌ها ارسال می‌کند.

$$E\left(W_{global}^{(i)}\right) = E\left(W_{global}^{(i)}\right) + E(-\alpha \,.\, G^{i}) \quad (۴)$$

- **مرحلهٔ چهارم:** هریک از زیر شبکه‌ها مقدار رمز شده وزن‌های بروزرسانی شده را دریافت $E\left(W_{global}^{(i)}\right)$ **پروتکل** می‌کند و آن را با استفاده از کلید خصوصی خود رمزگشایی می‌نماید و مقدار وزن خود را بروزرسانی می‌کند. در شکل ۳، مراحل اجرای پروتکل پیشنهادی، شرح داده شده است.



شکل ۳. مراحل پروتکل پیشنهادی یادگیری فدرالی حافظ حریم خصوصی

اثبات امنیت پروتکل پیشنهادی

ما در این بخش، اثبات می‌کنیم که پروتکل یادگیری فدرالی حافظ حریم خصوصی پیشنهادی ما بر اساس رمزنگاری همریخت امن است، تا زمانی که سیستم رمزنگاری همریخت بکار برده شده در این پروتکل امن باشد. در واقع، اگر سیستم رمزنگاری همریخت در مقابل دشمن نیمه درستکار[1] امن باشد، پروتکل پیشنهادی ما نیز در مقابل دشمن نیمه درستکار امن است.

[1] Semi-honest Adversaries

– **قضیه ۱.** پروتکل پیشنهادی ما در مقابل دشمن نیمه درستکار امن است.

اثبات. ما برای اثبات پروتکل از مدل امنیتی ایده آل- واقعی [۲۸] استفاده می‌کنیم. ما شبیه‌ساز S_1 را توصیف می‌کنیم که با داشتن ورودی و زیرشبکه۱، دید او را در محیط ایده‌آل شبیه‌سازی می‌کند. بدون از دست دادن کلیت مسئله، ما اثبات امنیت را برای حالتی که شبیه‌ساز، زیرشبکه۱ را شبیه‌سازی می‌کند ارائه می‌دهیم ولی برای حالتی که شبیه‌ساز، سایر زیرشبکه‌ها را در محیط ایده‌آل شبیه‌سازی می‌کند نیز مشابه است. دید زیرشبکه ۱ در اجرای واقعی پروتکل که شامل ورودی و پیام‌های دریافتی او در گام‌های پروتکل است. در فرمول شماره (۵) دید زیرشبکه ۱ نمایش داده شده است.

$$(w_{global}^{(1)},\ -\alpha.G^{(1)}, E(w_{global}^{(1)})) \quad (۵)$$

که $w_{global}^{(1)},\ -\alpha.G^{(1)}$ ورودی های Sub_1 و $E(w_{global}^{(1)})$ خروجی آن است. شبیه ساز با داشتن ورودی زیرشبکه۱، پروتکل را شبیه سازی می‌نماید و دید زیرشبکه۱ را در محیط ایده‌آل ایجاد می‌کند. در صورتی که دو دید ایجاد شده در محیط واقعی و ایده‌آل، از هم قابل تمایز نباشند، نشان دهندهٔ امن بودن پروتکل است؛ زیرا شبیه ساز از گام‌های مختلف پروتکل، اطلاعات فراتری به دست نیاورده است. بدین منظور، شبیه‌ساز پروتکل را در حالت ایده‌آل و صرفاً با داشتن ورودی‌های زیرشبکه۱ اجرا می‌کند و به یک خروجی دلخواه و رندوم بجای $E(w_{global}^{(1)})$ دست می‌یابد که آن را h می‌نامیم. شبیه‌ساز به سایر شرکت کننده‌ها و سرور مرکزی در محیط ایده‌آل و شبیه‌سازی دسترسی ندارد. او صرفاً با داشتن ورودی‌های مورد نظر، در محیط ایده‌آل و شبیه‌سازی سعی می‌کند پروتکل پیشنهادی ما را اجرا نماید. در هر مرحله از پروتکل که به داده‌ها دسترسی ندارد مقدار دلخواه و رندوم جایگزین می‌کند. حال اگر دید شبیه‌ساز از محیط واقعی و ایده‌آل از هم قابل تمایز نباشد می‌توانیم امنیت پروتکل خود را اثبات کنیم. بدین منظور، لازم است تا رابطهٔ عدم تمایز بیان شده در فرمول (۶) را اثبات کنیم.

$$\{S_1(x,f(x,y))\}_{x,y\in\{0,1\}^*} \overset{c}{\equiv} \{view_1^{\pi}(x,y)\}_{x,y\in\{0,1\}^*} \quad (۶)$$

که $\{S_1(x,f(x,y))\}_{x,y\in\{0,1\}^*}$ دید شبیه ساز در اجرای واقعی است و $\{view_1^{\pi}(x,y)\}_{x,y\in\{0,1\}^*}$ دید آن در اجرای ایده‌آل است و نباید از هم قابل تمایز باشند. در واقع، می‌توانیم با جایگزینی دید شبیه ساز و زیرشبکه۱، رابطهٔ عدم تمایز شماره (۷) را اثبات نماییم.

$$\left(w_{global}^{(1)},\ -\alpha.G^{(1)}, E(w_{global}^{(1)})\right) \overset{c}{\equiv} \left(w_{global}^{(1)},\ -\alpha.G^{(1)},\ h\right) \quad (۷)$$

عدم تمایز دیدها ما از برهان خلف برای اثبات پروتکل خود استفاده می‌کنیم. فرض کنید که یک تمایزدهندهٔ احتمالاتی زمان چندجمله‌ای[1] D و یک چندجمله‌ای $p(.)$ وجود دارد به‌طوری‌که برای n داده‌شده، طبق رابطهٔ عدم تساوی (۸) داریم:

$$\left|Pr[D(H_1(w_{global}^{(1)}, -\alpha.G^{(1)}, h)) = 1] - Pr[D(H_n(w_{global}^{(1)}, -\alpha.G^{(1)}, h)) = 1]\right| > 1/p(n) \quad (۸)$$

[1] Polynomial Probabilistic Distinguisher

عدم تساوی (۸) نشان دهندهٔ این است که اگر پروتکل را n بار در حالت ایده‌آل اجرا کنیم، احتمال آن که تمایزدهنده بتواند اولین و آخرین اجرا را از هم تمایز دهد بسیار ناچیز است. در واقع، ما یک i داریم که برای n داده‌شده رابطهٔ عدم تساوی (۹) برقرار است:

$$Pr\left[D(H_0(w_{global}^{(1)}, -\alpha.G^{(1)}, h)) = 1\right] - Pr\left[D\left(H_1(w_{global}^{(1)}, -\alpha.G^{(1)}, h)\right) = 1\right] +$$
$$Pr\left[D(H_1(w_{global}^{(1)}, -\alpha.G^{(1)}, h)) = 1\right] - Pr\left[D\left(H_2(w_{global}^{(1)}, -\alpha.G^{(1)}, h)\right) = 1\right] +$$
$$Pr\left[D(H_2(w_{global}^{(1)}, -\alpha.G^{(1)}, h)) = 1\right] - Pr\left[D\left(H_3(w_{global}^{(1)}, -\alpha.G^{(1)}, h)\right) = 1\right] +$$
$$\ldots + Pr\left[D(H_{n-1}(w_{global}^{(1)}, -\alpha.G^{(1)}, h)) = 1\right] - Pr\left[D\left(H_n(w_{global}^{(1)}, -\alpha.G^{(1)}, h)\right) = 1\right] > \frac{1}{p(n)}$$

$$\rightarrow Pr\left[D(H_i(w_{global}^{(1)}, -\alpha.G^{(1)}, h)) = 1\right] - Pr\left[D\left(H_{i+1}(w_{global}^{(1)}, -\alpha.G^{(1)}, h)\right) = 1\right] > \frac{1}{p(n)} \quad (۹)$$

ما از یک تمایزدهنده D برای نقض کردن امنیت پروتکل استفاده می‌کنیم. تنها تفاوت بین H_i و H_{i+1} این است که $i+1$ امین اجرای این گام در H_i بر اساس $(w_{global}^{(1)}, -\alpha.G^{(1)}, E(w_{global}^{(1)}))$ است و $i+1$ امین اجرای این گام در H_{i+1} بر اساس $(H_i(w_{global}^{(1)}, -\alpha.G^{(1)}, h)$ است. اگر تمایزدهنده بتواند تمایز بین این دو مقدار را در دو اجرای متفاوت تشخیص دهد نشان دهندهٔ این است که توانسته است خروجی اصلی پروتکل را از مقدار رندوم و دلخواه تمایز بخشد. این تمایز بخشیدن با امن بودن رمزنگاری همریخت تناقض دارد.

تحلیل پیچیدگی پروتکل پیشنهادی

ما برای بررسی پیچیدگی محاسباتی پروتکل، محاسبات موجود در پروتکل را بر اساس کوچک‌ترین عملیات باینری مانند and، or و xor بیان می‌کنیم. همچنین، برای بررسی پیچیدگی ارتباطی، تعداد بیت‌های انتقالی در هریک از گام‌ها را محاسبه می‌کنیم. جزئیات تحلیل پیچیدگی‌های محاسباتی و ارتباطی در ادامه بیان می‌گردد. برای دست‌یابی به جزئیات بیشتر دربارهٔ نحوهٔ بررسی پیچیدگی پروتکل‌های رمزنگاری به [۲۹; ۳۰] مراجعه شود.

- **مرحلهٔ اول:** هریک از زیر شبکه‌ها مقدار وزن‌های خود را رمز می‌کند و برای زیر شبکه‌ها ارسال می‌کند. عملیات رمزنگاری همریخت از الگوریتم توان رسانی پیمانه‌ای سریع استفاده می‌کند که به تعداد $n^2 \times m^4$ عمل and و $n \times m^2 + n$ عمل or نیاز است که m تعداد بیت کلید و n تعداد بیت ورودی است. از طرفی خروجی عملیات رمزنگاری n بیت است.

$$n^2 \times m^4 + n \times m^2 + n$$

- **مرحلهٔ دوم:** در این مرحله، گرادیان G در هر زیر شبکه در α – ضرب می‌شود و سپس رمز می‌شود و برای سرور مرکزی ارسال می‌شود. در این مرحله نیز یک عملیات ضرب انجام می‌شود که هر عمل ضرب n بیتی، معادل n عمل and می‌باشد. همچنین برای رمزنگاری مقدار α.G– نیز از الگوریتم توان رسانی پیمانه‌ای استفاده می‌شود که همانند مرحلهٔ اول می‌باشد و تعداد عملیات آن بصورت زیر است:

$$n^2 \times m^4 + n \times m^2 + n$$

- **مرحلهٔ سوم:** سرور مرکزی مقدار وزن‌ها را بروز رسانی می‌کند و برای هر یک از زیر شبکه‌ها ارسال می‌کند. برای به روزرسانی وزن‌ها، سرور مرکزی یک عمل جمع انجام می‌دهد که n عملیات or است. همچنین، n بیت انتقال می‌یابد.
- **مرحلهٔ چهارم:** هریک از زیر شبکه‌ها مقدار رمز شده وزن‌های به روزرسانی شده را دریافت می‌کند و آن را رمزگشایی می‌کند و مقدار وزن شبکه خود را به روزرسانی می‌کند. برای رمزگشایی نیز همانند رمزنگاری، عملیات توان رسانی پیمانه‌ای نیاز است و تعداد عملیات آن به صورت زیر است:

$$n^2 \times m^4 + n \times m^2 + n$$

بنابراین تعداد محاسبات در این پروتکل برابر است با:

$$3 \times (n^2 \times m^4 + n \times m^2 + n) + n + n \approx n^2$$

از آنجا که طول بیت کلید را می‌توان ثابت در نظر گرفت و تعداد بیت ورودی قابل تغییر و رشد است، می‌توان از m چشم پوشی کرد.

همچنین، پیچیدگی ارتباطی پروتکل پیشنهادی ما از مرتبه n است.

ارزیابی

جعل ساموجی و اختلال، دو مورد از حملات رایج در شبکه‌های اینترنت پهپادها است که به ترتیب زیرمجموعهٔ حملات دستکاری داده و ممانعت از سرویس می‌باشند. با این حال، انجام این آزمایش‌ها برای تحقیق در بسیاری از زمینه‌ها می‌تواند کاری دشوار باشد. زیرا تشخیص این حملات و جمع آوری گزارش‌ها ثبت وقایع[1] از آنها کاری هزینه‌بر و دشوار می‌باشد. از این رو در [۳۱]، با شبیه‌سازی این حملات در فضای اینترنت پهپادها، دادگانی[2] ایجاد شده است که در دسترس عموم قرار دارد. ما برای ارزیابی مدل پیشنهادی خود از دادگان پیشنهادی در [۳۱] استفاده کرده‌ایم. بدین منظور، ما ابتدا رکوردهای دادگان را بین زیرشبکه‌ها به صورت رندوم و دلخواه توزیع نمودیم. سپس، مدل را به دو صورت با/ بدون سرور مرکزی اجرا نموده و مورد مقایسه قرار داده‌ایم. ما از شبکه‌های پرسپترون چندلایه[3] [۳۲] با پارامترهای مختلف در هریک از زیرشبکه‌ها استفاده کردیم. علاوه بر این، مدل پیشنهادی خود را با مدل ارائه شده در [۲۴] که برای تشخیص حملات جعل ساموجی و مبتنی بر یادگیری عمیق است مقایسه نمودیم. تفاوت مدل ارائه شده در [۲۴] و مدل پیشنهادی ما این است که اولاً، مقالهٔ مورد نظر صرفاً داده‌های جمع‌آوری شده در یک پهپاد را بدون در نظر گرفتن داده‌های سایر پهپادها، برای یادگیری استفاده می‌کند. ثانیاً، تشخیص حمله جعل ساموجی مدنظر مقاله بوده است. نتایج ارزیابی سه مدل در جدول ۱ نمایش داده شده است. مدل اول، مدل پیشنهادی در مقاله [۲۴] است. مدل دوم، یادگیری عمیق به صورت متمرکز و با ارسال داده‌های محلی برای سرور مرکزی است. مدل سوم، یادگیری عمیق فدرالی و با ارسال مدل‌های محلی برای سرور مرکزی است.

[1] Log files
[2] Dataset
[3] Multi-layer Perceptron (MLP)

جدول ۱. مقایسهٔ دو مدل با/ بدون سرور مرکزی

امتیاز F1[1]	بازخوانی[2]	صحت[3]	دقت[4]	نوع حمله	دادگان مورد استفاده	
۰.۹۴۹	۰.۹۴۹۳	۰.۹۵۰۳	۰.۹۴۹۸	جعل ساموجی	دادگان ایجاد شده توسط نویسندگان مقاله	مدل یادگیری عمیق در [۲۴]
۰.۹۴۲	۰.۹۳۷	۰.۹۴۷	۰.۹۵	جعل ساموجی و اختلال	دادگان پیشنهادی در [۳۱]	یادگیری عمیق متمرکز
۰.۹۷	۰.۹۶۸	۰.۹۷۸	۰.۹۷	جعل ساموجی و اختلال	دادگان پیشنهادی در [۳۱]	یادگیری عمیق فدرالی پیشنهادی ما

همان‌گونه که در جدول بالا قابل مشاهده است نتایج ارزیابی مدل در حالت یادگیری فدرالی بهتر از یادگیری با حضور سرور مرکزی است. علاوه بر این در مدل فدرالی، سرور مرکزی از دادگان هریک از زیرشبکه‌ها مطلع نمی‌شود که دستاورد مورد نظر ما است.

ما در این ارزیابی صرفاً سه مدل را مقایسه کردیم و نتایج ارزیابی و تحلیل پیچیدگی مدل پیشنهادی مبتنی بر رمزنگاری همریخت را در بخش قبلی با جزئیات کامل بیان نمودیم. نهایتاً ارزیابی‌ها نشان می‌دهد که پیچیدگی مدل پیشنهادی ما مناسب است، دقت بالایی در تشخیص دارد و مهم‌تر از همه آن که دادگان زیرشبکه‌ها افشا نمی‌شود.

نتیجه‌گیری

شبکه‌های اینترنت پهپادها، کاربردهای بسیار زیادی در زمینه‌های مختلف دارند. با این حال، این شبکه‌ها می‌توانند هدف بسیاری از تهدیدات مخرب امنیتی و حریم خصوصی باشد. یکی از راه‌ها برای مقابله با نفوذ، طراحی و پیاده‌سازی سیستم‌های تشخیص نفوذ مبتنی بر یادگیری عمیق می‌باشد.

علی‌رغم برخورداری از مزایای برجستهٔ این سیستم‌ها، با چندین چالش فنی مواجه هستند. اولاً اینترنت پهپادها یک شبکهٔ غیرمتمرکز با تعداد بسیار زیادی از زیرشبکه‌ها است که برای اهداف مختلفی مانند تولید، کشاورزی و تدارکات مستقر شده‌اند. هر زیرشبکه تنها مجموعهٔ کوچکی از دستگاه‌های اینترنت اشیا را کنترل می‌کند و بنابراین داده‌های جمع‌آوری‌شده از هر زیر مجموعه معمولاً برای آموزش شبکهٔ یادگیری عمیق برای سیستم تشخیص حملات سایبری کافی نیست. داده‌های ناکافی برای آموزش، دقت مکانیسم یادگیری عمیق را به طور جدی کاهش می‌دهد. به اشتراک‌گذاری داده‌ها بین زیرشبکه‌ها ممکن است باعث نگرانی در مورد حفظ حریم خصوصی و ازدحام شبکه به دلیل تبادل حجم عظیمی از داده‌ها از طریق اینترنت شود. دوم، زیرشبکه‌ها معمولاً توسط دروازه‌های اینترنت اشیا و/یا گره‌های لبه مدیریت می‌شوند که توسط منابع محاسباتی محدود می‌شوند، و بنابراین اجرای الگوریتم‌های یادگیری عمیق با دادگان عظیم و انبوه ممکن است در بلندمدت کارآمد نباشد.

در این مقاله، ما یک مدل یادگیری فدرالی و امن را پیشنهاد کرده‌ایم که می‌تواند به طور مؤثر بر روی سیستم تشخیص حملات سایبری در شبکه اینترنت پهپادها پیاده‌سازی شود. در مدل پیشنهادی ما، هریک از زیر شبکه‌ها شامل تعدادی پهپاد است که به یکدیگر اعتماد دارند و در عین حال به پهپادهای سایر زیر شبکه‌ها اعتماد کامل ندارند. هریک از زیر شبکه‌ها به جای ارسال داده‌های خود برای یک سرور مرکزی جهت تجمیع داده‌ها و انجام عملیات یادگیری عمیق،

[1] F1-Score
[2] Recall
[3] Precision
[4] Accuracy

مدل یادگیری عمیق را در سمت خود آموزش می‌دهد و پارامترهای مدل را برای سرور مرکزی به صورت امن ارسال می‌کند. بدین ترتیب در ضمن حفظ حریم خصوصی زیرشبکه‌ها، ترافیک شبکه نیز کاهش می‌یابد. ما نه تنها توانسته‌ایم دقت در شناسایی حملات را به میزان قابل توجهی افزایش دهیم، بلکه سرعت یادگیری را نیز افزایش داده‌ایم. همچنین، ترافیک شبکه را کاهش داده و از حریم خصوصی داده‌ها برای زیرشبکه‌ها محافظت نمودیم. پروتکل پیشنهادی ما دارای پیچیدگی محاسباتی از مرتبه n^2 و پیچیدگی ارتباطی از مرتبه n است. نتایج ارزیابی نشان می‌دهد که مدل در حالت یادگیری فدرالی بهتر از یادگیری با حضور سرور مرکزی است. علاوه بر این در مدل فدرالی، سرور مرکزی از دادگان هریک از زیرشبکه‌ها مطلع نمی‌شود که دستاورد مورد نظر ما است. پیشنهاد ما برای پژوهش‌های آتی، استفاده از طرح شراکت سر[1]، محاسبات چند طرفه امن[2]، تبادل و ذخیره سازی داده‌ها مبتنی بر زنجیره بلوکی[3] جهت حفظ حریم خصوصی زیرشبکه‌ها و جلوگیری از افشا اطلاعات حملات سایبری آنها است.

References

[1] Lasi, H., Fettke, P., Kemper, H-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, *6*(4), 239-242. https://doi.org/10.1007/s12599-014-0334-4

[2] Gharibi, M., Boutaba, R., & Waslander, S. L. (2016). Internet of Drones. *Institute of Electrical and Electronics Engineers Access*, *4*, 1148-1162. https://doi.org/10.1109/ACCESS.2016.2537208

[3] Choudhary, G., Sharma, V., Gupta, T., Kim, J., & You, I. (2018, Auguest 29- September 1). *Internet of drones (iod): Threats, vulnerability, and security perspectives.* The 3rd International Symposium on Mobile Internet Security, Cebu, Philippines. https://doi.org/10.48550/arXiv.1808.00203

[4] Bernama. (2019, June 18). *Food delivery via drones in Cyberjaya by end of the month*. New Straits Times. https://www.nst.com.my/lifestyle/bots/2019/06/497157/food-delivery-drones-cyberjaya-end-month

[5] Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Karimipour, H., Srivastava, G., & Aledhari, M. (2021). Enabling Drones in the Internet of Things With Decentralized Blockchain-Based Security. *Institute of Electrical and Electronics Engineers Internet of Things Journal*, *8*(8), 6406-6415. https://doi.org/10.1109/JIOT.2020.3015382

[6] Boursianis, A. D., Papadopoulou, M. S., Diamantoulakis, P., Liopa-Tsakalidi, A., Barouchas, P., Salahas, G., Karagiannidis, G., Wan, S., & Goudos, S. K. (2022). Internet of Things (IoT) and Agricultural Unmanned Aerial Vehicles (UAVs) in smart farming: A comprehensive review. *Internet of Things*, *18*(24), 100187. https://doi.org/10.1016/j.iot.2020.100187

[7] Magistretti, S., & Dell'Era, C. (2019). Unveiling opportunities afforded by emerging technologies: evidences from the drone industry. *Technology Analysis & Strategic Management*, *31*(5), 606-623. https://doi.org/10.1080/09537325.2018.1538497

[8] Paddeu, D., Calvert, T., Clark, B., & Parkhurst, G. (2019). *New technology and automation in freight transport and handling systems*. Government. https://uwe-repository.worktribe.com/output/851875/new-technology-and-automation-in-freight-transport-and-handling-systems

[1] Secret Sharing Scheme
[2] Secure Multi-party Computation
[3] Blockchain

[9] Vattapparamban, E., İ, G., Yurekli, A. İ., Akkaya, K., & Uluağaç, S. (2016, September 5-9). *Drones for smart cities: Issues in cybersecurity, privacy, and public safety*. 2016 International Wireless Communications and Mobile Computing Conference, Paphos, Cyprus. https://doi.org/10.1109/IWCMC.2016.7577060

[10] Półka, M., Ptak, S., & Kuziora, Ł. (2017). The Use of UAV's for Search and Rescue Operations. *Procedia Engineering*, *192*, 748-752. https://doi.org/10.1016/j.proeng.2017.06.129

[11] Kharchenko, V., & Torianyk, V. (2018, May 24-27). *Cybersecurity of the Internet of Drones: Vulnerabilities analysis and IMECA based assessment.* 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, Kyiv, UKraine https://doi.org/10.1109/DESSERT.2018.8409160

[12] Riahi Manesh, M., & Kaabouch, N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Computers & Security*, *85*, 386-401. https://doi.org/10.1016/j.cose.2019.05.003

[13] Kovar, D. (2015, March 18). *Cybersecurity and non-military UAVs (AKA drones)*. URSA. https://ursainc.com/2015/03/18/cybersecurity-and-non-military-uavs-aka-drones/

[14] Altawy, R., & Youssef, A. M. (2016). Security, privacy, and safety aspects of civilian drones: A survey. *Association for Computing Machinery Transactions on Cyber-Physical Systems*, *1*(2), 1-25. https://doi.org/10.1145/3001836

[15] Singh, M., Aujla, G. S., Bali, R. S., Vashisht, S., Singh, A., & Jindal, A. (2020, September 25). *Blockchain-enabled secure communication for drone delivery: A case study in COVID-like scenarios.* The 26th Annual International Conference on Mobile Computing and Networking, London, England, United Kingdom. https://doi.org/10.1145/3414045.3415937

[16] Garg, N., & Roy, N. (2020, March 3). *Acoustic Sensing for Detecting Projectile Attacks on Small Drones.* Proceedings of the 21st International Workshop on Mobile Computing Systems and Applications, Austin, TX, USA. https://doi.org/10.1145/3376897.3379167

[17] Garg, N., & Roy, N. (2020, March 3). *Enabling Self-defense in Small Drones.* Proceedings of the 21st International Workshop on Mobile Computing Systems and Applications, Austin, TX, USA. https://doi.org/10.1145/3376897.3377866

[18] Srinivas, J., Das, A. K., Kumar, N., & Rodrigues, J. J. P. C. (2019). TCALAS: Temporal Credential-Based Anonymous Lightweight Authentication Scheme for Internet of Drones Environment. *IEEE Transactions on Vehicular Technology*, *68*(7), 6903-6916. https://doi.org/10.1109/TVT.2019.2911672

[19] Ali, Z., Chaudhry, S. A., Ramzan, M. S., & Al-Turjman, F. (2020). Securing Smart City Surveillance: A Lightweight Authentication Mechanism for Unmanned Vehicles. *Internet of Drones. Institute of Electrical and Electronics Engineers Access*, *8*, 43711-43724. https://doi.org/10.1109/ACCESS.2020.2977817

[20] Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT press. https://mitpress.mit.edu/9780262035613/deep-learning/

[21] Yaacoub, J-P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, *11*, 100218. https://doi.org/10.1016/j.iot.2020.100218

[22] Pandey, G. K., Gurjar, D. S., Nguyen, H. H., & Yadav, S. (2022). Security Threats and Mitigation Techniques in UAV Communications: A Comprehensive Survey. *Institute of Electrical and Electronics Engineers Access*, *10*, 112858-112897. https://doi.org/10.1109/ACCESS.2022.3215975

[23] Kong, P. Y. (2021). A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles. *Institute of Electrical and Electronics Engineers Access*, *9*(1), 148244-148263. https://doi.org/10.1109/ACCESS.2021.3124996

[24] Agyapong, R. A., Nabil, M., Nuhu, A. R., Rasul, M. I., & Homaifar, A. (2021, December 5-7). *Efficient Detection of GPS Spoofing Attacks on Unmanned Aerial Vehicles Using Deep Learning* 2021 IEEE Symposium Series on Computational Intelligence, Orlando, Florida, USA. https://doi.org/10.1109/SSCI50451.2021.9659972

[25] Zhang, D., Chen, X., Wang, D., & Shi, J. (2018, June 18-21). *A Survey on Collaborative Deep Learning and Privacy-Preserving.* 2018 IEEE Third International Conference on Data Science in Cyberspace, Guangzhou, China https://doi.org/10.1109/DSC.2018.00104

[26] Westin, A. F. (1968). Privacy And Freedom. *Washington and Lee Law Review 25*(1), 166-170. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20/

[27] Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A Survey on Homomorphic Encryption Schemes: Theory and Implementation. *Association for Computing Machinery Computing Surveys*, *51*(4), 1-35. https://doi.org/10.1145/3214303

[28] Lindell, Y., & Pinkas, B. (2009). A Proof of Security of Yao's Protocol for Two-Party Computation. *Journal of Cryptology*, *22*(2), 161-188. https://doi.org/10.1007/s00145-008-9036-8

[29] Dehghan, M., & Sadeghiyan, B. (2019). Privacy-preserving collision detection of moving objects. *Transactions on Emerging Telecommunications Technologies*, *30*(3), e3484. https://doi.org/10.1002/ett.3484

[30] Dehghan, M., Sadeghiyan, B., & Khosravian, E. (2021). Private Trajectory Intersection Testing: Is Garbled Circuit Better than Custom Protocols? *International Journal of Engineering*, *34*(4), 863-872. https://doi.org/10.5829/ije.2021.34.04a.12

[31] Whelan, J., Sangarapillai, T., Minawi, O., Almehmadi, A., & El-Khatib, K. (2020). *UAV attack dataset* [Data set]. IEEE DataPort. https://ieee-dataport.org/open-access/uav-attack-dataset

[32] Popescu, M-C., Balas, V. E., Perescu-Popescu, L., & Mastorakis, N. (2009). Multilayer perceptron and neural networks. *World Scientific and Engineering Academy and Society Transactions on Circuits and Systems*, *8*(7), 579-588. https://www.researchgate.net/publication/228340819_Multilayer_perceptron_and_neural_networks