مجله‌ی علمی- تحقیقی علوم اجتماعی پوهنتون کابل
https://jns.edu.af
Print ISSN: 3078-6657 E-ISSN:3078-6665

تشخیص حملات DDoS در زراعت هوشمند مبتنی بر یادگیری عمیق

پوهنیار الله‌محمد هځاند
دیپارتمنت انجنیری مخابرات، پوهنځی تکنالوژی معلوماتی و مخابراتی، پوهنتون کابل، کابل، افغانستان
ایمیل: amhassand@gmail.com

چکیده

تکنولوژی نقش مهمی در زراعت ایفا می‌کند و با استفاده از اینترنت اشیاء، زراعت به سمت هوشمندسازی پیش می‌رود. ا ستفاده از این تکنولوژی برای هو شمند سازی زراعت در جهان رو به افزایش ا ست؛ زیرا در زراعت هو شمند اطلاعات قابل‌اطمینان در مورد مزارع به دست می‌آید که منجر به افزایش محصولات و صرفه‌جویی در مصرف آب و منابع می‌شود. با این حال، زراعت هوشـمند چالش‌هایی نیز دارد، از جمله هزینه‌های بالا، وابسـتگی به تکنولوژی، و مشـکلات امنیت شبکه. امنیت شبکه و اطلاعات در اینترنت اشیاء زراعت هوشمند یکی از چالش‌های اساسی است. به‌ویژه، حملات منع سرویس توزیع شده (DDoS) از جمله تهدیدهای شایع هستند که شبکه اینترنت ا شیاء زراعت هو شمند را با خطر مواجه می‌کنند. به‌طورکلی، حمله منع سرویس در اینترنت اشیاء شامل قطع موقت، دائمی، یا تعلیق خدمات یک میزبان متصل به شبکه است که در نتیجه، شبکه زراعت هوشمند از دسترس خارج شده و خسارات قابل‌توجهی به مزارع و کشاورزان وارد می‌شود. در این مقاله، با استفاده از برنامه RapidMiner، یک روش پیشنهادی ترکیبی مبتنی بر یادگیری عمیق برای بهبود دقت طبقه‌بندی و ت شخیص حملات در شبکه اینترنت ا شیاء زراعت هو شمند ارائه شده ا ست. این روش پی شنهادی از الگوریتم‌های یادگیری عمیق بهره می‌گیرد. نتایج نشان می‌دهد که روش پیشنهادی عملکرد بهتری دارد و با دقت ۹۹,۸۲٪ و خطای ۰,۱۸٪ همراه است.

واژه‌های کلیدی: انترنت اشیاء؛ زراعت هوشمند؛ یادگیری عمیق؛ حملات منع سرویس، امنیت شبکه؛ افغانستان

Detection of DDoS Attacks in Smart Agriculture Based on Deep Learning

Allah Mohammad Hassand
Department of Telecommunication Engineering, Faculty of Information & Communication Technology, Kabul University, Kabul, Afghanistan
Email: amhassand@gmail.com

Abstract

Technology plays a crucial role in agriculture, and with the Internet of Things (IoT), it has evolved into smart agriculture. The use of this technology for smart farming is increasing worldwide as it provides reliable information about farms, leading to enhanced productivity and the conservation of water and other resources. However, smart farming also faces challenges such as high costs, dependence on technology, and network security, with network and information security in IoT agriculture being among the most critical concerns. One common issue is Distributed Denial of Service (DDoS) attacks, which pose a significant threat to IoT agriculture networks. A DDoS attack in IoT generally refers to the temporary or permanent disruption or suspension of services to a host connected to the IoT agriculture network. This makes the intelligent farming network inaccessible, causing substantial damage to farms and fields. This paper presents a proposed combined method based on deep learning using the RapidMiner program for more accurate classification and detection of attacks in IoT agriculture networks. The proposed method integrates deep learning, Decision Tree, and K-nearest neighbors (KNN) algorithms. The results show that the proposed method performs exceptionally well, achieving an accuracy of 99.82% and an error rate of 0.18%.

Keywords: Agriculture, Smart agriculture, Smart farming, Technology

ارجاع: هځاند، ا. م. (۱۴۰۳). تشخیص حملات DDoS در زراعت هوشمند مبتنی بر یادگیری عمیق. *ژورنال علوم طبیعی- پوهنتون کابل ۷* (شماره فوق‌العاده کنفرانس بین‌المللی انقلاب سبز برای خودکفایی افغانستان). ۷۵-۸۹.
https://jns.edu.af/jns/article/view/91

مقدمه

در سال‌های اخیر استفاده از تکنالوژی معلوماتی در زراعت گسترش یافته است و امروزه شاهد آن هستیم که تکنالوژی‌های مختلف از جمله انترنت اشیاء، هوش مصنوعی و یادگیری عمیق در صنعت زراعت استفاده می‌شود. تحول دیجیتالی زراعت می‌تواند مزایای مختلفی ازجمله بهبود کیفیت محصولات، افزایش کمیت محصولات زراعتی، بهینه‌سازی فرایند آبیاری، بهینه‌سازی فرایندهای کاشت و برداشت محصولات و از طرف دیگر کاهش هزینه‌های زراعتی را به همراه بیاورد. علاوه بر این تقاضا برای غذا در حال افزایش است. بر اساس گزارش غذا و زراعت سازمان ملل متحد، تخمین می‌شود که تقاضا برای غذا تا سال ۲۰۵۰ در مقایسه با سطح تولید فعلی، ۷۰% افزایش خواهد یافت تا بتواند نیازمندی‌های جمعیت ۱۰ میلیارد نفری جهان را برآورده سازد. علاوه بر مزایای زیاد زراعت هوشمند، برخی نواقص هم دارند مانند، هزینه پیاده‌سازی، حریم خصوصی، امنیت اطلاعات و حملات سایبری، پذیرش تکنالوژی، وابستگی به تکنالوژی و دیگر موارد (Vatambeti et al., 2023). زراعت هوشمند یا انترنت اشیای زراعت و یا زراعت 4.0، شامل تکنالوژی‌های پیشرفته مانند، انترنت اشیاء، یادگیری عمیق، هوش مصنوعی و سایر تکنالوژی‌های است که در مزارع زراعتی برای بهبود کیفیت محصولات زراعتی، اطلاعات دقیق از مزارع، تصمیم‌گیری به‌موقع، استفاده بهینه از منابع، کنترول آبیاری و کود دهی، از بین بردن گیاهان هرزه و افزایش محصولات زراعتی استفاده می‌شود. ازآنجایی‌که استقرار هزاران دستگاه مبتنی بر انترنت اشیاء در یک ساحه باز، تهدیدات زیادی در زراعت هوشمند به وجود می‌آورد. بنابراین محققان تکنالوژی و امنیت سایبری مصروف این موضوع هستند تا از امنیت سیستم زراعت هوشمند مطمئن شوند، زیرا یک دشمن می‌تواند حملات سایبری زیادی را آغاز انجام دهد، مانند حملات منع سرویس توزیع‌شده برای خارج کردن کنترول استفاده‌کننده‌ها به شبکه زراعت هوشمند و سپس تزریق اطلاعات نادرست به شبکه (Ferrag et al., 2021).

به‌دلیل سهولت‌های زیادی که زراعت هوشمند برای دهاقین ارائه می‌دهد، مانند نظارت بهتر بر پارامترهای محیطی مربوط به خاک، محصولات زراعتی، تشخیص امراض گیاهان، تشخیص گیاهان هرز و غیره، زیاد استفاده می‌شود؛ اما به‌هم‌پیوستگی سنسورها و دستگاه‌های شبکه متنوع امکان حملات متعددی مانند حملات منع سرویس توزیع‌شده را فراهم می‌کند. به‌دلیل اینکه این دستگاه‌ها ضعیف و در مقابل حملات انترنتی آسیب‌پذیر هستند. اختلال در چنین شبکه‌های زراعت هوشمند

منجربه عواقب ناگوار در زراعت می‌شود. بناً نظارت و طبقه‌بندی دیتای شبکه برای خنثی کردن حملات موضوع مهمی است (Vatambeti et al., 2023).

زراعت در افغانستان در مرحله 2.0 یا در حالت زراعت میکانیزه قرار دارد که پاسخ‌گوی نیازهای غذایی نفوس فعلی افغانستان نیست و این سبب می‌شود که هرسال به هزارها تن گندم، برنج و دیگر حبوبات از کشورهای دیگر به افغانستان وارد شود.

هدف تحقیق

هدف از این تشخیص حملات منع سرویس توزیع‌شده در زراعت هوشمند با استفاده از یک روش طبقه‌بندی ترکیبی (متشکل از یادگیری عمیق، نزدیک‌ترین همسایه و درخت تصمیم) است.

سؤال تحقیق

چگونه می‌توان با حملات منع سرویس توزیع‌شده در زراعت هوشمند مقابله کرد؟

بیان مسئله

امنیت شبکه و اطلاعات در زراعت هوشمند یکی از مهم‌ترین چالش‌ها است. به‌طور خاص، حملات منع سرویس توزیع‌شده به شبکه اینترنت اشیاء زراعت هوشمند تهدیدی جدی محسوب می‌شوند. حملات منع سرویس توزیع‌شده عبارتند از قطع موقت، دائمی یا تعلیق خدمات یک میزبان متصل به شبکه اینترنت اشیاء زراعت هوشمند که در نتیجه، شبکه زراعت هوشمند از دسترس خارج می‌شود و خسارات جدی به مزارع و دهاقین وارد می‌شود. در این تحقیق از الگوریتم طبقه‌بندی ترکیبی برای تشخیص حملات منع سرویس توزیع شده و ترافیک عادی در زراعت هوشمند استفاده می شود.

روش تحقیق

این تحقیق با استفاده از پروگرام رپیدماینر و مجموعه دیتای NSL-KDD انجام‌شده است. یک روش پیشنهادی ترکیبی مبتنی بر یادگیری عمیق برای ایجاد طبقه‌بندی دقیق‌تر و تشخیص حملات در شبکه انترنت اشیای زراعت هوشمند ارائه گردیده است.

یافته‌ها

امنیت در انترنت اشیاء یک مسئله مهم و حیاتی می‌باشد که علاقه‌مندان این تکنالوژی تحقیقات زیادی را در این زمینه انجام داده و باگذشت زمان روش‌ها، الگوریتم‌ها و سیستم‌های بهتر برای تشخیص و مقابله با حملات روی زراعت هوشمند ارائه گردیده است. در این مقاله بعضی تحقیقات مهم که در سال‌های آخر انجام شده است، مرور گردیده که از هوش مصنوعی، یادگیری عمیق، یادگیری ماشینی،

الگوریتم‌های RNN[1]، LSTM[2]، CNN[3]، DT3[4]، DDN[5] و سایر الگوریتم‌ها استفاده گردیده است. در تحقیقات انجام شده از مجموعه دیتای CICDDoS2019، TON_IoT، NSL-KDD و معیارهای دقت، صحت، معیار F_1 و سایر معیارها برای ارزیابی مدل‌های پیشنهادی استفاده شده است. در مورد زراعت هوشمند در افغانستان تحقیقاتی انجام نشده است. خلاصه‌ای برخی از تحقیقات مرور شده در جدول ۱ درج گردیده است.

جدول ۱. تحقیقات انجام شده در زمینهٔ تشخیص و مقابله با حملات در زراعت 4.0

مقاله مرجع	نتیجه
(Munir et al., 2019)	اطلاعات به‌دست‌آمده توسط سنسورها در مورد پارامترهای حرارت، رطوبت، نور به دهاقین کمک می‌کند تا در فصل جاری کدام گیاه کشت شود.
(Yang et al., 2020)	معرفی هفت تکنالوژی مهم و یازده کاربرد کلیدی آن‌ها در زراعت هوشمند. بر اساس تکنالوژی‌های فوق، شش راه‌حل امنیتی در زراعت هوشمند ارائه گردیده است.
(Farooq et al., 2019)	معرفی مؤلفه‌های اصلی زراعت هوشمند مبتنی بر انترنت اشیاء و مسائل امنیتی آن. ارائه فهرستی از برنامه‌های کاربردی مبتنی بر تیلفون‌های هوشمند و مبتنی بر سنسورها برای مدیریت مزرعه. مقررات و سیاست‌های ایجاد شده توسط کشورها برای استانداردسازی زراعت مبتنی بر انترنت اشیاء ارائه شده است.
(Vatambeti et al., 2023)	ارائه یک مدل امنیتی IDSNet که از PDO برای پیش‌بینی حملات احتمالی در زراعت 4.0 استفاده می‌شود. در این مقاله از مجموعه دیتای CICDDoS2019 و TON_IoT استفاده شده است. نتایج تحقیق دقت ۹۸,۳۲٪ این سیستم را نشان می‌دهد.
(Ferrag et al., 2021)	ارائه یک سیستم تشخیص نفوذ مبتنی بر یادگیری عمیق برای حملات DDoS بر اساس سه مدل، یعنی شبکه‌های عصبی کانولوشنل، شبکه‌های عصبی عمیق و شبکه‌های عصبی بازگشتی. در این مقاله از مجموعه دیتای CICDDoS2019 و TON_IoT استفاده شده است. نتایج تحقیق دقت ۹۹,۹۲٪ این سیستم را نشان می‌دهد.
Kethineni & Gera,) (2023	معرفی یک مدل یادگیری عمیق پیشرفته مبتنی بر رمزگذاری حریم خصوصی (SCAE) و تشخیص حملات زراعت هوشمند. پارامترهای مانند دقت، صحت و معیار F1 به ترتیب ۹۹,۷، ۹۹,۹٪ و ۹۹,۸٪ است. روش پیشنهادی با استفاده از انواع روش‌های یادگیری ماشین مانند شبکه عصبی عمیق (DNN)، شبکه عصبی کانولوشنال (CNN)، شبکه عصبی بازگشتی (RNN) و LSTM مقایسه شده است.

[1] Recurrent Neural Network (RNN)
[2] Long Short-Term Memory (LSTM)
[3] Convolutional Neural Networks
[4] Decision Trees (DT3)
[5] Deep Neural Network (DNN)

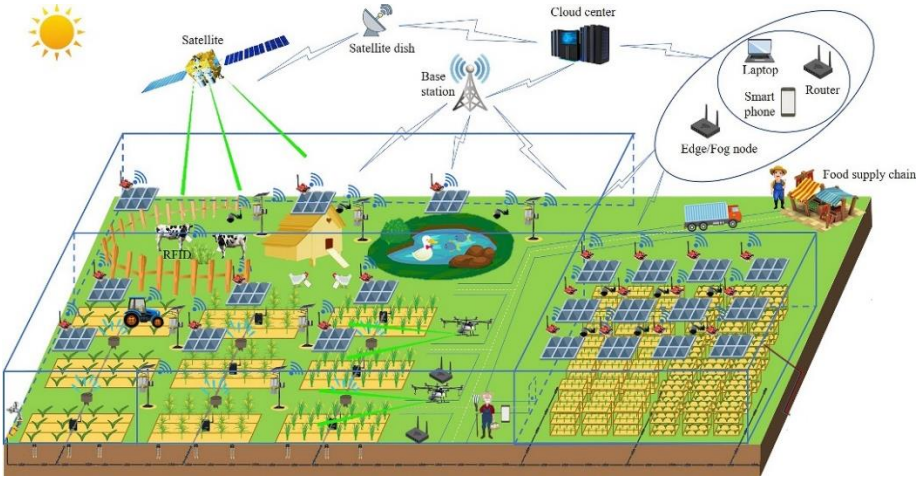
(Fathy & Ali, 2023)	ارائه یک روش رمزنگاری در اکوسیستم انترنت اشیاء برای زراعت هوشمند تا نیازهای دستگاه‌های انترنت اشیاء با محدودیت منابع را برآورده سازد. ایجاد یک کانال امن و استفاده از پروتوکول MQTT به‌عنوان پیام‌رسان در سیستم آبیاری زراعتی. کانال امن از تصمیمات آبیاری اتخاذ شده توسط نهاد در مورد زمان آبیاری و مقدار آن از هرگونه تغییر محافظت می‌کند. عملکرد این سیستم در مقایسه با استاندارد رمزگذاری پیشرفته (AES) از نظر مصرف انرژی، زمان اجرا و استفاده از حافظه موردنیاز بهبودیافته است.
Aldhyani &) (Alkahtani, 2023	ارائه یک سیستم ترکیبی CNN-LSTM برای تشخیص حملات منع سرویس توزیع شده در زراعت 4.0 که از مجموعه دیتای CICDDoS2019 استفاده شده است. نتایج تحقیق دقت ۱۰۰٪ این سیستم را نشان می‌دهد. در طراحی این سیستم از یادگیری عمیق استفاده شده است.

انترنت اشیاء

تکنالوژی‌های پیشرفته ارتباطات امروزی نشان می‌دهند که در دنیای کسب‌وکار، آن‌هایی که به دیتای بیشتر و اطلاعات بهتری دسترسی دارند آینده را کنترل خواهند کرد. اطلاعات به‌روز و مفید آنگاه که در زمان و مکان مناسب در اختیار طراحان قرار گیرد، منجربه تولید محصولات و ارائه خدماتی می‌شود که زندگی بشر را با همه‌ی پیچیدگی‌ها و مصائب جهان امروز، هر روز بیش‌ازپیش آسان‌تر می‌کند. تکنالوژی انترنت اشیاء نیز با همین فلسفه توسعه‌یافته است. اولین و اساسی‌ترین تعریف این تکنالوژی در سال ۱۳۹۹ ارائه گردید. به مجموعه‌ای از تجهیزات دریافت اطلاعات، مانند سنسورها، وسیله شناسایی از طریق فرکانس رادیویی[6]، سیستم تعیین موقعیت جغرافیایی[7] و دیگر تجهیزات که برای تشکیل یک شبکه عظیم باهم ترکیب‌شده‌اند، انترنت اشیاء می‌گوییم. هدف از ارائه این شبکه، سهولت مدیریت و شناسایی این وسایل است. به عبارت دقیق‌تر، انترنت اشیاء ارتباط با هر دستگاه در هر مکان و هر زمان را به‌صورت هوشمندانه پدید می‌آورد (Dahane et al., 2022). این تکنالوژی نوظهور تأثیر شگرفی بر زندگی انسان گذاشته، زیرا با کمک آن بسیاری از موارد غیرممکن ارتباطی بین اشیاء امکان‌پذیر خواهد بود. امروزه دستگاه‌های هوشمند مجهز به تکنالوژی انترنت اشیاء دیتای بزرگ، ارزشمند و بسیار دقیق در زراعت هوشمند و سایر کسب‌وکار تولید می‌کنند. از طرفی، گسترش دامنه کاربرد و هوشمند سازی زراعت، کارخانه‌ها، سیستم آبیاری، شفاخانه‌ها، خانه‌های مسکونی و غیره می‌تواند اطلاعات بسیار ارزشمندی را در اختیار طراحان قرار دهد (شکل ۱). امّا هوشمند کردن بیشتر دستگاه‌ها با کمک انترنت اشیاء به معنی ریسک بیشتر است؛ زیرا اگر با گسترش این تکنالوژی هر شیء

[6] Radio Frequency Identification (RFID)
[7] Global Positioning System (GPS)

نوعی سیستم‌عامل و حافظه داشته باشد، این پوتانشیل را دارد که توسط اشخاص غیرمجاز هک شده و درنتیجه اطلاعات به خارج دستگاه منتقل و به اشتراک گذاشته شود. به‌این‌ترتیب فرصت استراق سمع یا نفوذ در ارتباطات افزایش می‌یابد. شکل ذیل یک مزرعه هوشمند زراعتی را نشان می‌دهد.



شکل ۱. مزرعه هوشمند مبتنی بر انترنت اشیاء (Yang et al., 2020)

امنیت در انترنت اشیاء

امروزه تکنالوژی انترنت اشیاء یک نیاز مهم برای استانداردسازی و معماری‌های نوین سیستم‌های هوشمند است که توضیح می‌دهد، این تکنالوژی چگونه پیاده‌سازی شده و دستگاه‌های مبتنی بر انترنت اشیاء چگونه با یک روش امن باهم ارتباط برقرار کنند. با توجه به دستگاه‌هایی که در این تکنالوژی نوظهور استفاده می‌شود که معمولاً قابل‌حمل و کوچک هستند، محدودیت‌هایی همچون حافظه، بطری، پروسس و عدم توانایی نصب دیواره‌های دفاعی[۸] در سطوح پیشرفته، راه را برای هکرها و سارقان اطلاعات باز نموده است. ازجمله چالش‌های امنیتی در سیستم‌های هوشمند مبتنی بر انترنت اشیاء می‌توان به تهدیدات مسیریابی، ارسال بسته‌های مخرب، تهدید تروجان[۹]، حمله منع سرویس[۱۰]، تزریق کدهای مخرب، مجوز دسترسی به اطلاعات و آسیب‌پذیری نرم‌افزاری، امنیت و حریم خصوصی اشاره کرد. به عبارت دیگر، امنیت در انترنت اشیاء یکی از مهم‌ترین دغدغه‌های کاربران و تولیدکنندگان نرم‌افزاری و سخت‌افزاری وسایل موردنیاز هست، به‌طوری‌که می‌توان گفت اصلی‌ترین چالش پیشرو برای گسترش زراعت هوشمند، فارم‌های هوشمند و شهرهای هوشمند محسوب می‌گردد. ترس از

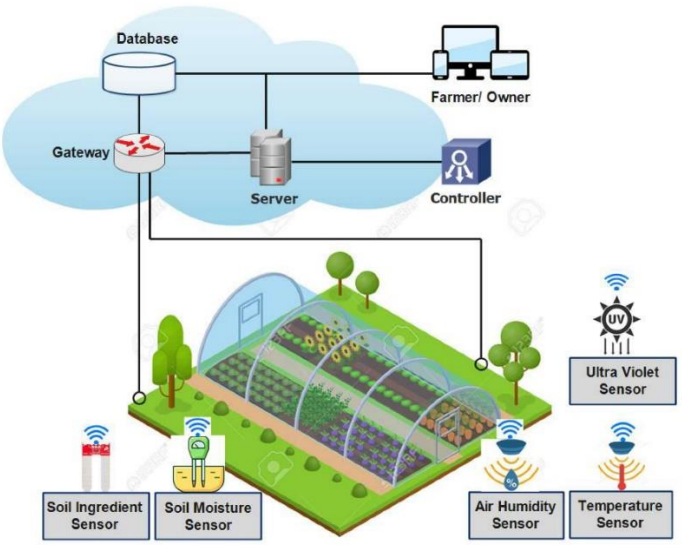
---

[۸] Firewall

[۹] Trojan

[۱۰] Denial of Service (DoS)

حملات احتمالی، سرقت اطلاعات و از بین رفتن حریم خصوصی توسط هرگونه شخص و یا سازمانی می‌تواند خسارات جبران‌ناپذیری را برای زراعت، دهاقین و سایر کسب‌وکار ایجاد نماید. یکی از مهم‌ترین حملات، حمله منع سرویس و حمله منع سرویس توزیع‌شده می‌باشد که این حملات، تلاش برای خارج کردن ماشین و منابع شبکه از دسترس کاربران مجاز است. اگرچه منظور از حمله منع سرویس و انگیزه انجام آن ممکن بسته به کاربرد انترنت اشیاء متفاوت باشد، اما به‌طورکلی شامل تلاش برای قطع موقت، دائمی یا تعلیق خدمات یک میزبان متصل به شبکه انترنت اشیاء است. شکل ۲ نظارت بر مزارع با استفاده از انترنت اشیاء را نشان می‌دهد (Quy et al., 2022).



شکل ۲. نظارت بر مزارع با استفاده از انترنت اشیاء (Quy et al., 2022)

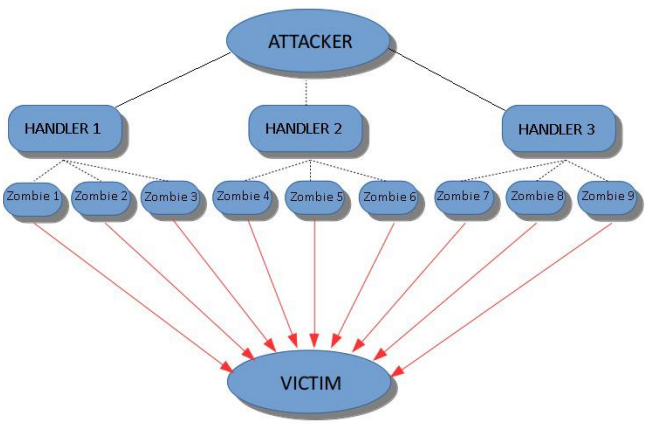
حملات منع سرویس توزیع‌شده روی زراعت هوشمند

مسائل امنیت اطلاعات، حملات انترنتی و بخصوص حملات منع سرویس توزیع‌شده در زراعت 4.0 را نمی‌توان نادیده گرفت (Yang et al., 2020). حملات منع سرویس ازجمله حملات معروف روی این شبکه‌ها هستند که ابتدا در سال ۱۹۹۹ معرفی شدند (Jara et al., 2009)؛ امّا بااین‌حال این نوع حملات هنوز هم دارای ساختاری پیچیده از لحاظ کشف رمز و در عین حال ساده برای اجرا هستند. اگرچه چندین سال است که حملات اختصاصی منع سرویس توزیع‌شده استفاده می‌شوند؛ سیستم‌هایی که این نوع حمله بر روی آن‌ها اجرا می‌شود، عواقب مخربی را متحمل می‌شوند. حمله بات نت[11] یکی

[11] Botnet

از انواع حملات منع سرویس توزیع‌شده است. در سال‌های اخیر، تهدید حمله منع سرویس توزیع‌شده به‌اندازه‌ای جدی تلقی شده که تعداد این نوع حملات در سه ماه آخر سال ۲۰۱۵، در مقایسه با سه ماه آخر سال ۲۰۱٤ به‌اندازه ٦٦ درصد افزایش یافت. یکی از تهدیدات حمله منع سرویس توزیع‌شده به نام حمله بوتر[12] است که یک ترافیک ۲٤۰ گیگا بیت در ۳۰۰ ثانیه در شبکه تولید می‌کند که منجربه قطع موقت یا دائمی سرویس می‌شود (Karagiannis et al., 2015).

در حملات منع سرویس توزیع‌شده، مهاجمان با در اختیار داشتن سیستم انترنت اشیاء، حجم گسترده‌ای از تقاضاها را به سمت سرورهای مقصد روانه می‌کنند که درنهایت با اشغال تمامی ترافیک مربوط به سرورهای موردنظر، موجب از کار افتادن سرویس‌دهی آن‌ها می‌شوند. این‌گونه حملات جزو رایج‌ترین حملاتی است که تاکنون بر روی انترنت اشیاء اجراشده است (Tamanna et al., 2017). شکل ۳ معماری حمله منع سرویس توزیع‌شده را نشان می‌دهد.



شکل ۳. معماری حمله منع سرویس توزیع‌شده

شناسایی حملات منع سرویس توزیع‌شده مبتنی بر یادگیری عمیق

یادگیری عمیق یکی از بزرگترین پیشرفت‌ها درزمینهٔ هوش مصنوعی، پردازش تصویر و شناسایی الگو است. شبکه‌های عمیق، پیشرفت قابل‌توجه‌ای در دقت طبقه‌بندی و پیش‌بینی‌ها در این وظایف پیچیده به دست آورده‌اند که با تقلید از توانایی مغز انسان برای یادگیری غریزی از تجارب مختلف، الهام گرفته‌شده است. همانند توانایی مغز انسان در پردازش اطلاعات خام ناشی از ورودی‌های نورونی[13] و یادگیری ویژگی‌های سطح بالای خودمان، یادگیری عمیق می‌تواند اطلاعات خام را با شبکه‌های عصبی

[12] Booter
[13] Neuron

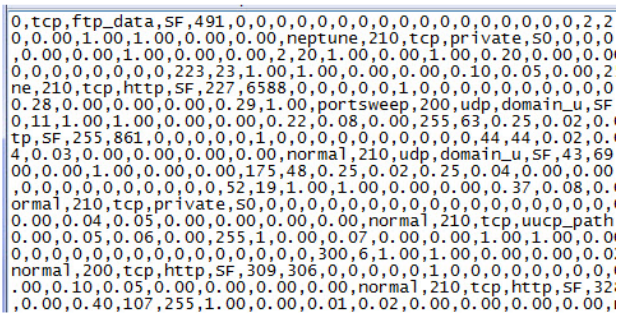
عمیق تغذیه کند که طبقه‌بندی مواردی که در آن آموزش‌دیده است را یاد می‌گیرد (Bengio et al., 2006; Deng, 2014). اخیراً، تحقیقات گسترده‌ای در مورد امنیت سایبری انترنت اشیاء با استفاده از رویکرد یادگیری عمیق در حال شکل گرفتن است. یادگیری عمیق یکی از جدیدترین روش‌ها برای پایداری و تعمیم الگوریتم‌های آموزش شبکه‌های مصنوعی می‌باشد و این روش توانسته مقیاس‌پذیری بسیار خوبی را درزمینهٔ اطلاعات بزرگ به دست آورد که ورودی را به خروجی تبدیل کرده یا به عبارتی، طبقه‌بندی را انجام دهد (Diro & Chilamkurti, 2018).

الگوریتم پیشنهادی

الگوریتم پیشنهادی، یک روش طبقه‌بندی ترکیبی[14] (متشکل از یادگیری عمیق، نزدیک‌ترین همسایه[15] و درخت تصمیم[16]) است که بر اساس روش دیتا ماینینگ[17] جهت تشخیص دقیق‌تر حملات منع سرویس توزیع‌شده در انترنت اشیاء تشکیل شده است. در این روش فرض می‌شود که ترافیک شبکه شامل حمله و ترافیک عادی است. تعداد حملات در شبکه به‌طور معمول بخش بسیار کوچکی از ترافیک در کل شبکه را تشکیل می‌دهد. به‌کارگیری روش‌های دیتا ماینینگ هوشمند برای تشخیص حملات در چنین شبکه‌هایی با حجم بالای ترافیک رو به افزایش است. اکثر سیستم‌های تشخیص حملات از یک الگوریتم طبقه‌بندی و ترافیک شبکه که به‌عنوان رفتار طبیعی یا غیرعادی است استفاده می‌کنند. یک الگوریتم به‌تنهایی در بیشتر اوقات برای تشخیص نفوذ در شبکه مؤثر نبوده، لذا برای حل این مشکل ترکیبی از چندین الگوریتم کارا می‌تواند ویژگی‌های برجسته دیتا را از مجموعه دیتا در شبکه به دست آورد و با میزان دقیق‌تر حملات را شناسایی کند. برای ارزیابی عملکرد و مقایسه روش پیشنهادی با سایر الگوریتم‌ها همچون یادگیری عمیق، نزدیک‌ترین همسایه و درخت تصمیم بر اساس میزان تشخیص و دقت شناسایی حملات منع سرویس توزیع‌شده در انترنت اشیاء، از مجموعه دیتای NSL-KDD[18] استفاده‌شده است.

---

[14] Ensemble Classification
[15] K-Nearest Neighbor
[16] Decision Tree
[17] Data Mining
[18] Network Services Library-Knowledge Discovery and Data Mining (NSL-KDD)



شکل ٤. نمونه‌ای از مجموعه دیتای NSL-KDD

معیارهای ارزیابی الگوریتم پیشنهادی ترکیبی

چون هدف اصلی این تحقیق شناسایی و مقابله با حملات منع سرویس توزیع‌شده در انترنت اشیاء در زراعت هوشمند است و مجموعه دیتای مورد استفاده متشکل از ترافیک عادی و حملات است. لذا تفکیک و طبقه‌بندی دقیق ترافیک عادی و حملات توسط این مدل، یک معیار مناسب برای ارزیابی روش پیشنهادی است. همچنین در این مقاله، از چندین معیار دیگر جهت ارزیابی و مقایسه روش پیشنهادی با سایر الگوریتم‌ها استفاده‌شده است که مهم‌ترین معیارهای روش پیشنهادی جهت تشخیص حملات منع سرویس توزیع‌شده عبارت‌اند از دقت و صحت شناسایی حملات توسط مدل است. نمایش ریاضی این معیارها توسط یک کانفویژن متریکس[۱۹] در شکل ۵ نشان داده‌شده است (GeeksforGeeks, 2022). کانفویژن متریکس اغلب برای توصیف عملکرد یک مدل طبقه‌بندی یا طبقه‌بندی کننده بر روی مجموعه‌ای از دیتای آزمایشی مورد استفاده قرار می‌گیرد.

مقادیر تخمین شده	مقادیر واقعی: مثبت	مقادیر واقعی: منفی
مثبت	True Positive	False Positive
منفی	False Negative	True Negative

[۱۹] Confusion Matrix

شکل ۵. کانفویژن متریکس

طبقه‌بندی دیتا با استفاده از الگوریتم‌های طبقه‌بندی، هدف دستیابی به بالاترین دقت و صحت ممکن در طبقه‌بندی و تشخیص طبقه‌ها است. در برخی از مسائل، تشخیص صحیح نمونه‌های مربوط به یکی از طبقه‌ها برای ما اهمیت بیشتری دارد. به‌عنوان مثال، در تحقیق حاضر، هدف شناسایی حملات منع سرویس توزیع‌شده در انترنت اشیاء است. کانفویژن متریکس، نتایج حاصل از طبقه‌بندی را بر اساس اطلاعات واقعی موجود، نمایش می‌دهد. حال بر اساس این مقادیر می‌توان معیارهای مختلف ارزیابی طبقه‌بندی و اندازه‌گیری دقت را تعریف کرد. در ذیل معیارهای ارزیابی مدل پیشنهادی معرفی شده‌اند.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

$$Precision = \frac{TP}{TP + FP}$$

$$DR^{20} = \frac{TP}{TP + FN}$$

$$FAR^{21} = \frac{FP}{TN + FP}$$

$$F_{1_{Measure}} = \frac{2TP}{2TP + FP + FN}$$

$$Recall = \frac{TP}{TP + FN}$$

۱. پارامتر TP[22] بیانگر تعداد نمونه‌هایی است که درست تشخیص داده‌شده است؛ یعنی دیتاهای نورمال هستند که توسط الگوریتم نیز نورمال تشخیص داده‌شده است.

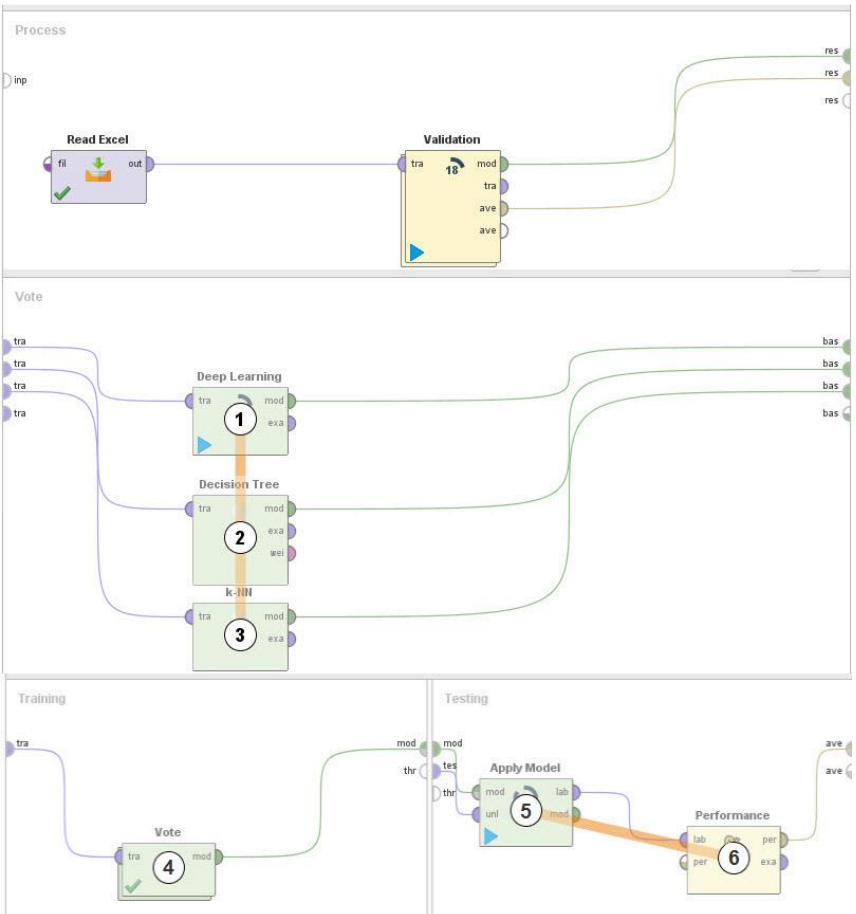
۲. پارامتر TN[23] دیتای حملات بوده و الگوریتم نیز آن‌ها را به‌درستی حملات تشخیص داده است.

۳. پارامتر FP[24] بیانگر تعداد نمونه‌هایی است که به‌اشتباه، درست تشخیص داده‌شده است؛ یعنی دیتای حملات بوده، امّا الگوریتم آن‌ها را به‌اشتباه دیتای نورمال تشخیص داده است.

---

[20] Detection Rate (DR)
[21] False Alarm Rate (FAR)
[22] True Positive (TP)
[23] True Negative (TN)
[24] False Positive (FP)

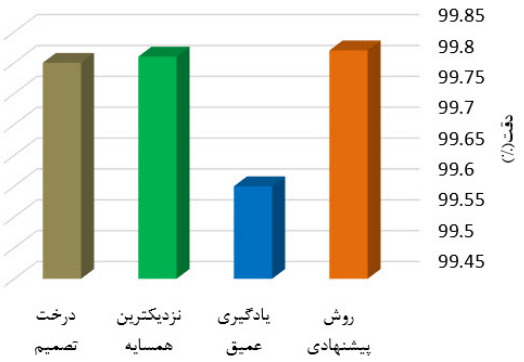
۴.پارامتر FN[۲۵] بیانگر تعداد نمونه‌هایی است که به‌درستی، اشتباه تشخیص داده‌شده است؛ یعنی دیتای نورمال بوده و الگوریتم آن‌ها را به‌اشتباه حملات تشخیص داده است. شکل ٦ شبیه‌سازی روش پیشنهادی ترکیبی را در پروگرام رپیدماینر نشان می‌دهد.



شکل ٦. شبیه‌سازی روش پیشنهادی ترکیبی

میزان دقت روش پیشنهادی ۹۹,۸۲% است که میزان بهبود دقت آن در مقایسه با الگوریتم‌های یادگیری عمیق، نزدیک‌ترین همسایه و الگوریتم درخت تصمیم به ترتیب برابر با ۰,۲۲%، ۰,۰۱ و ۰,۰۲ می‌باشد.

[25] False Negative (FN)



شکل ۷. مقایسه دقت روش پیشنهادی با سایر الگوریتم‌ها

نتیجه‌گیری

انترنت اشیاء یک شبکه عظیم از انواع اشیاء هوشمند است که می‌تواند برای کاربردهای مختلف در زراعت هوشمند از آن استفاده شود. هوشمند بودن، این تکنالوژی را بیشتر در معرض حملات قرار داده است. از طرف دیگر محدودیت‌هایی همچون حافظه، بطری، پردازش و عدم توانایی نصب دیواره‌های دفاعی در سطوح پیشرفته، مقابله با حملات را در این تکنالوژی با مشکل روبرو ساخته است. رویکردهای متفاوتی برای حل آن در شبکه انترنت اشیاء ارائه‌شده است. تمرکز روش پیشنهادی بر روی یک الگوریتم ترکیبی جدید است که سه الگوریتم یادگیری عمیق، درخت تصمیم و الگوریتم نزدیک‌ترین همسایه در قالب بوستینگ[۲۶] باهم ترکیب شد. الگوریتم‌های درخت تصمیم و نزدیک‌ترین همسایه به‌عنوان یادگیرنده‌های ضعیف در ترکیب با الگوریتم یادگیری عمیق توانست یک سیستم یادگیرنده قوی ایجاد کند و حملات را دقیق‌تر تشخیص دهد. این ناشی از آن می‌شود که الگوریتم نزدیک‌ترین همسایه با محاسبه کوچک‌ترین فاصله بین نمونه‌ها و الگوریتم درخت تصمیم با الهام از تئوری اطلاعات، بهره اطلاعات را از نمونه‌ها به دست می‌آورد که در ایجاد طبقه‌بندی و تشخیص دقیق‌تر حملات منع سرویس توزیع‌شده در زراعت 4.0 کمک می‌کند. همچنان برای تشخیص جهش‌های کوچک حملات تأثیرگذار است.

بررسی مطالعات نشان داد که روش پیشنهادی ترکیبی نسبت به الگوریتم‌های مستقل از عملکرد مطلوب‌تری برخوردار است. روش پیشنهادی دارای بیشترین دقت ۹۹,۸۲ ٪ و کمترین خطا ۰,۱۸ ٪

---

[۲۶] Boosting

است. این امر باعث اعتماد دهاقین بالای زراعت هوشمند می‌شوند تا برای افزایش بهره‌وری و استفاده بهینه از منابع، از زراعت هوشمند استفاده کند.

منابع

Aldhyani, T. H., & Alkahtani, H. (2023). Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model. Mathematics, 11(1), 233 .

Bengio, Y., Lamblin, P., Popovici, D., & Larochelle, H. (2006). Greedy layer-wise training of deep networks. Advances in neural information processing systems, 19 .

Dahane, A., Benameur, R., & Kechar, B. (2022). An IoT low-cost smart farming for enhancing irrigation efficiency of smallholders farmers. Wireless Personal Communications . ۳۲۱۰-۳۱۷۳,(٤)۱۲۷,

Deng, L. (2014). A tutorial survey of architectures, algorithms, and applications for deep learning. APSIPA transactions on Signal and Information Processing, 3, e2 .

Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82, 761-768 .

Farooq, M. S., Riaz, S., Abid, A., Abid, K., & Naeem, M. A. (2019). A Survey on the Role of IoT in Agriculture for the Implementation of Smart Farming. Ieee Access, 7, 156237-156271 .

Fathy, C., & Ali, H. M. (2023). A secure IoT-based irrigation system for precision agriculture using the expeditious cipher. Sensors, 23(4), 2091 .

Ferrag, M. A., Shu, L., Djallel, H., & Choo, K.-K. R. (2021). Deep learning-based intrusion detection for distributed denial of service attack in agriculture 4.0. Electronics, 10(11), 1257 .

GeeksforGeeks. (2022). https://www.geeksforgeeks.org/visualize-confusion-matrix-using-caret-package-in-r/

Jara, A. J., Zamora, M .A., & Skarmeta, A. F. (2009). HWSN6: Hospital wireless sensor networks based on 6LoWPAN technology: Mobility and fault tolerance management. 2009 International conference on computational science and engineering ,

Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F., & Alonso-Zarate, J. (2015). A survey on application layer protocols for the internet of things. Transaction on IoT and Cloud computing, 3(1), 11-17 .

Kethineni, K., & Gera, P. (2023). Iot-Based Privacy-Preserving Anomaly Detection Model for Smart Agriculture. Systems, 11(6), 304 .

Munir, M. S., Bajwa, I. S., & Cheema, S. M. (2019). An intelligent and secure smart watering system using fuzzy logic and blockchain. Computers & Electrical Engineering, 77, 109-119 .

Quy, V. K., Hau, N. V., Anh ,D. V., Quy, N. M., Ban, N. T., Lanza, S., Randazzo, G., & Muzirafuti, A. (2022). IoT-Enabled Smart Agriculture: Architecture, Applications, and Challenges. Applied Sciences, 12(7), 3396 .

Tamanna, T., Fatema, T., & Saha, R. (2017). SDN, A research on SDN assets and tools to defense DDoS attack in cloud computing environment. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) ,

Vatambeti, R., Venkatesh, D., Mamidisetti, G., Damera, V. K., Manohar, M., & Yadav, N. S. (2023). Prediction of DDoS attacks in agriculture 4.0 with the help of prairie dog optimization algorithm with IDSNet. Scientific Reports, 13(1), 15371 .

Yang, X., Shu, L., Chen, J., Ferrag, M. A., Wu, J., Nurellari, E., & Huang, K. (2020). A Survey on Smart Agriculture: Development Modes, Technologies, and Security and Privacy Challenges. IEEE/CAA Journal of Automatica Sinica, 8, 273-302 .