دانشکده مهندسی کامپیوتر و فناوری اطلاعات

**پیشنهاد موضوع پایان نامه (Proposal)**

# ارائه یک سیستم تشخیص حملات DDoS مبتنی بر بازه بندی زمانی با استفاده از تکنیک‌های یادگیری ماشین

# A time-interval based DDoS detection system using machine learning techniques

**دانشجو**

علی شامخی (98214038)

کارشناسی ارشد مهندسی کامپیوتر – شبکه‌های کامپیوتری

**استاد راهنما**

دکتر پیروز شمسی نژاد

**استاد مشاور**

دکتر .....

# بیان مساله

## مقدمه

امروزه با توجه به گستردگی شبکه‌های کامپیوتری و همچنین پیشرفته‌تر شدن آن‌ها، مخاطرات آن نیز به مراتب بیشتر شده‌است. در عصری که تمام اشیا در اطراف ما امکان اتصال به شبکه را پیدا کرده‌اند، وجود امنیت در شبکه‌های کامپیوتری یک رکن اساسی به شمار می‌آید؛ چرا که اکنون این شبکه‌ها به جزئی جداناپذیر از زندگی انسان‌ها تبدیل شده‌اند که هرکس به صورت مستقیم یا غیرمستقیم به آن‌ها وابسته است و عدم وجود امنیت در آن‌ها ممکن است باعث بروز خساراتی جبران ناپذیر گردد. از یک طرف شبکه‌های کامپیوتری به سرعت در حال رشد هستند و از طرف دیگر موانعی همچون انواع تهدیدات، حملات و فعالیت‌های خصمانه در برابر شبکه‌های کامپیوتری قرار دارند. در این میان یکی از قدیمی ترین نوع حملات شبکه که در عین حال هنوز هم بسیار متداول است، حمله محروم سازی از سرویس یا (DoS[1]) می‌باشد.

در حملات DoS مهاجم اقداماتی را در جهت از کار انداختن سرویس انجام می‌دهد و باعث بروز اختلال در سرویس می‌شود. معمولا این اقدامات شامل ارسال درخواست‌های هرز و متعدد است که هدف آن ها اشغال کردن منابع سرویس‌دهنده است. همچنین زمانی که این اقدامات از دستگاه‌های مختلفی به صورت همزمان نیز انجام شوند، از این حمله با عنوان محروم سازی از سرویس توزیع شده (DDoS[2]) یاد می‌شود. از دلایل متداول بودن این نوع حملات می‌توان به مواردی از جمله عدم نیاز به دانش فنی بالا، نامتقارن بودن حمله از لحاظ بکارگیری منابع و عدم سهولت در تشخیص و جلوگیری این حملات اشاره نمود. از لحاظ فنی، هویت شخص مهاجم در اکثر حملات ناشناس خواهد ماند چرا که در سناریو حمله، آدرس فرستنده جعلی است و همین مورد باعث سخت‌تر شدن تشخیص منشا حمله می‌شود. امروزه از سیستم‌های تشخیص نفوذ تحت شبکه (NIDS[3]) برای تشخیص حملات شبکه استفاده می‌گردد که با رویکردهای متفاوتی می‌توانند حملات را تشخیص دهند. این سیستم ها قابلیت تشخیص سوءاستفاده[4] و ناهجاری[5] را دارند که در در هرکدام با استفاده از تکنیک‌های مختلفی از وقوع آن ها مطلع می‌شوند. به طور مثال برای تشخیص سوءاستفاده از راهکارهایی همچون تطبیق امضا، ماشین حالت و یا قوانین وضع شده توسط خبرگان استفاده می‌کنند[1]. اما حملات DDoS نوعی ناهنجاری محسوب می‌گردند؛ چراکه رفتار آن‌ها در ظاهر کاملا شبیه رفتار دیگر کاربران شبکه است اما با استفاده از تکنیک‌های مختلفی قابل تشخیص خواهند بود. از تکنیک‌های کشف ناهنجاری می‌توان

[1] Denial of Service
[2] Distributed Denial of Service
[3] Network-Based Intrusion Detection System
[4] Misuse
[5] Anomaly

به تکنیک‌های آماری، ماشین حالت محدود[1] و تکنیک‌های یادگیری ماشین اشاره کرد[1]. تشخیص حملات در تمامی این تکنیک ها با آنالیزهای مختلفی که بر روی جریان داده[2] در شبکه انجام می‌شود، اتفاق می‌افتد. امروزه تشخیص حملات با استفاده از تکنیک‌های یادگیری ماشین بیشتر از روش‌های دیگر مورد توجه توسعه دهندگان و تولیدکنندگان قرارگرفته است؛ چراکه دقت تشخیص در این روش به مراتب از روش‌های دیگر بیشتر است و اکثرا قابلیت تشخیص حملاتی را که تا به حال دیده نشده‌اند نیز دارند. همانطور که گفته شد، با استفاد از آنالیز فراداده[3]های مربوط به جریان داده که می‌توان آن‌ها را با روش‌های مختلفی از شبکه استخراج کرد، می‌توان مدل‌های متعددی را با استفاده از یادگیری ماشین بوجود آورد و با استفاده از آن ها حملات مختلف را تشخیص داد. تعدد ویژگی[4]های موجود برای هر جریان از یک طرف به ساخت مدلی دقیق تر کمک می‌کند و از طرفی دیگر انتخاب ویژگی‌های موثر خود یک چالش در طراحی یک مدل جدید به حساب می‌آید. ارائه یک سیستم جهت تشخیص حملات DDoS دارای چالش‌های گوناگونی در ابعاد مختلف است. به طور مثال جهت تشخیص اینگونه حملات در حوزه اینترنت اشیاء[5] با توجه به محدودیت‌های پردازشی دستگاه‌ها با چالش استفاده بهینه از منابع روبه‌رو هستیم و بایستی از حداقل منابع و به صورت بهینه استفاده نمود. همچنین تشخیص حملات DDoS در شبکه‌هایی که حجم بسیار زیادی از داده را با سرعت بسیار بالا منتقل می‌کنند با چالش تشخیص بلادرنگ[6] روبه‌رو است. اما در این میان دقت تشخیص درست حملات DDoS، خصوصا برای حملات جدیدی که تا به حال دیده نشده‌اند[7]، یک چالش اصلی و مهم به حساب می‌آید. هدف ما در این تحقیق ارائه یک سیستم مناسب جهت تشخیص دقیق‌تر حملات DDoS در شبکه‌های کامپیوتری است.

## سوال پژوهشی پایان نامه

با توجه به اهمیت بالای چالش دقت تشخیص درست حملات DDoS در شبکه‌های کامپیوتری، سوال پژوهشی بدین صورت مطرح می‌گردد.

- چگونه می‌توان میزان دقت در تشخیص حملات DDoS را بالا ببریم؟

[1] Finite-state Machine
[2] Traffic Flow
[3] Metadata
[4] Feature
[5] Internet of Things (IoT)
[6] Real-Time
[7] Zero-Day Attacks

# اهداف و نتایج مورد انتظار

هدف تحقیق ما ارائه یک سیستم تشخیص حملات DDoS با دقت بالا خواهد. اما چه راهکارهایی برای تشخیص دقیق‌تر حمله وجود دارد؟

با بررسی‌های صورت گرفته بر روی راهکارهای موجود در این حوزه، اینگونه مشاهده می‌شود که راهکارهای مبتنی بر ابزار یادگیری ماشین توانسته است به دقت مناسبی در تشخیص حملات دست پیدا کند. با توجه به اینکه داده مورد استفاده ما برای طراحی یک سیستم تشخیص حمله DDoS همان داده‌های مربوط به جریان داده‌های شبکه است، دقت سیستم ارائه شده، با بسنده کردن به داده‌های موجود، با سیستم‌های دیگر تفاوت چندانی نخواهد داشت. اما ما در این تحقیق سعی بر آن داریم که میان دنیای واقعی و سیستم ارائه شده یک ارتباط منطقی ایجاد کنیم. لذا با درنظر گرفتن پارامتر زمان به عنوان یک رکن اساسی در تشخیص حملات DDoS اقدام به بازه بندی داده ها و همچنین با ایجاد ویژگی‌های جدید از ویژگی‌های موجود به افزایش دقت در تشخیص حملات کمک خواهیم نمود. به طور مثال فرض شود در یک شرکت، میزان استفاده از منابع شبکه و حجم ترافیکی در ساعات مختلف متفاوت است. حال با دسته بندی خودکار ساعات پرمصرف و ساعات کم مصرف، حساسیت سیستم تشخیص حمله نیز متفاوت خواهد بود. مثلا در صورتی که در ساعات تعطیلی یک شرکت میزان استفاده از منابع شبکه بالا باشد، این یک مورد مشکوک به حساب خواهد آمد که بایستی در حساسیت سیستم تشخیص تاثیرگذار باشد. از طرفی دیگر با استخراج ویژگی‌های جدید از روی ویژگی‌هایی همچون آدرس مبدا، پورت مبدا، آدرس مقصد و پورت مقصد می‌توان به دقت بالاتری در تشخیص حملات DDoS دست پیدا نمود.

# پیشینه و اهمیت پژوهش

در حوزه سیستم‌های تشخیص حمله تحقیقات گسترده‌ای از دیرباز تا به حال انجام شده است که هرکدام به بهبود و افزایش دقت تشخیص کمک کرده‌اند. در سال‌های اخیر نیز با بهره‌وری از تکنیک‌های یادگیری ماشین و یادگیری عمیق سیستم‌های مختلفی ارائه شده است که هرکدام دارای نکات حائز اهمیتی هستند.

Marcos V.O. de Assis و همکارانش[2] با ایده جلوگیری از بروز حمله در شبکه مبدا، سیستمی را ارائه کرده‌اند که با بکارگیری آن در شبکه‌های مبدا، می‌توان از وقوع حملات DDoS جلوگیری نمود. این سیستم با در نظر گرفتن ترافیک‌های خروجی از شبکه و با بکارگیری از الگوریتم شبکه عصبی پیچشی (CNN[1])،

[1] Convolutional Neural Network

ناهنجاری ها را در شبکه مبدا تشخیص داده و از ورود آن ها به شبکه‌های بالاتر جلوگیری می‌نماید. اگرچه این طرح سربار کمتری برای جلوگیری از حمله در شبکه مقصد دارد اما الزام استفاده از آن برای تمام شبکه ها اجباری خواهد بود.

M. Salahuddin و همکارانش [3] با استفاده از یک رمزگذار خودکار[1] یک سیستم تشخیص ناهنجاری بر اساس ویژگی‌های مبتنی بر زمان ارائه کرده‌اند که با استفاده از الگوریتم Sliding Time Window و تعیین یک آستانه حساسیت می‌تواند حملات DDoS را تشخیص دهد. این تشخیص با مقایسه رفتار جدید با رفتار عادی شبکه اتفاق می‌افتد.

Marcos V.O. Assis و همکارانش[4] با ادعا بر اینکه آنالیز هر یک از جریان‌های داده به صورت مجزا و مجرد باعث افزایش دقت و سرعت در تشخیص حملات DDoS می‌گردد و بر همین اساس نیز با استفاده از الگوریتم GRU که یک الگوریتم مبتنی بر یادگیری عمیق است سیستمی جهت تشخیص و جلوگیری از حملات DDoS ارائه کرده‌اند.

NOVAES و همکارانش[5] در شبکه‌های مبتنی بر نرم‌افزار (SDN[2]) سیستمی را ارائه کرده‌اند که متشکل از سه بخش توصیفگر ترافیک شبکه[3]، تشخیص و جلوگیری است. در بخش توصیفگر، با استفاده از الگوریتم شبکه عصبی بازگشتی (LSTM[4])، رفتار عادی شبکه را توصیف میکنند و در بخش تشخیص با استفاده از منطق فازی هرگونه مغایرت با رفتار عادی شبکه را آشکار می‌کنند. در بخش جلوگیری نیز با استفاده از مجموعه قوانین از قبل تعریف شده اقدام به جلوگیری از حمله می‌نمایند.

Laisen Nie و همکارانش[6] که در حوزه IoT فعالیت داشته‌اند با رائه یک سیستم تشخیص حمله مبتنی بر الگوریتم یادگیری تقویتی عمیق (DRL[5])، رفتار عادی شبکه را مدل کرده و با تعیین یک آستانه حساسیت، اقدام به جلوگیری از حملات DDoS می‌کنند. با توجه به ماهیت محیط IoT که دارای محدودیت استفاده از منابع است، این سیستم به عنوان یک سیستم سبک از لحاظ استفاده از منابع پردازشی به شمار می‌آید.

آن ها همچنین در مقاله‌ای دیگر[7] در حوزه IoT با استفاده از الگوریتم شبکه‌های مولد متخاصم (GAN[6]) سیستمی را ارائه کرده‌اند که شامل سه بخش است. در بخش اول ویژگی‌های جریان داده استخراج می‌گردد. در بخش دوم با استفاده از یک معماری یادگیری عمیق مبتنی بر GAN اقدام به تشخیص یک حمله خاص

[1] Autoencoder
[2] Software Defined Network
[3] Network Traffic Characterization
[4] Long Short-Term Memory
[5] Deep Reinforcement Learning
[6] Generative Adversarial Network

می‌کنند. در بخش سوم نیز با ترکیب تمام مدل‌های بوجود آمده که هرکدام مناسب یک نوع حمله هستند یک سیستم جامع تشخیص حمله شکل گرفته خواهد شد. در این روش، دقت تشخیص سیستم برای حملاتی که برای آن ها آموزش دیده است بسیار بالا خواهد بود اما برای حملات جدید ممکن است عملکرد مشابهی نداشته باشد.

Camila Pontes و همکارانش[8] با ارائه یک الگوریتم جدید با نام EFC[1] که مبتنی بر مدل Inverse Potts است، با رویکرد دسته‌بندی تک حالته ترافیک شبکه که صرفا متشکل از ترافیک عادی شبکه است سیستمی را جهت تشخیص حملات DDoS ارائه کرده‌اند. در این سیستم تا زمانی که ویژگی جریان‌های صحیح و عادی را می‌آموزد می‌تواند بین ترافیک عادی و ترافیک حمله تمایز قائل شود. در این نوع از سیستم ها مزیت تشخیص حملات جدید یک امتیاز محسوب می‌شود؛ کما اینکه در نتایج تحقیقاتشان نیز در حالتی که مجموعه داده‌های یادگیری و آزمون با هم متفات است، دقت تشخیص حملات بیشتر است؛ اما با این رویکرد ممکن است نرخ تشخیص ناصحیح[2] نیز افزایش می‌یابد.

در تحقیقات انجام شده توسط Abdullah Emir Cil و همکارانش[9] در راستای افزایش دقت در تشخیص حملات، خصوصا زمانی که داده‌های آموزش مدل ما بسیار محدود است، استفاده از شبکه‌های عصبی عمیق (DNN[3]) پیشنهاد شده است. چراکه عمل استخراج ویژگی و دسته‌بندی در ساختار این الگوریتم وجود دارد و مدل در طول آموزش به صورت مداوم در حال بهبود خود است.

همچنین Hassan Alamri و همکارانش[10] با استفاده از مکانیزم کنترل پهنای باند مبتنی بر دو پارامتر زمان و حجم انتقالی داده، رفتار شبکه را به سه دسته ترافیک سبک، ترافیک متوسط و ترافیک سنگین دسته بندی کردند و با قرار گرفتن حالت شبکه در هر یک از این دسته ها، آستانه حساسیت تشخیص تغییر می‌یابد. در نهایت با استفاده از الگوریتم تقویت گرادیان (XGBoost) سیستمی جهت تشخیص حملات در شبکه‌های SDN ارائه کرده‌اند. با توجه به اینکه ایده تفکیک حالت‌های شبکه جهت تشخیص حملات بسیار می‌تواند در دقت تشخیص صحیح حملات تاثیرگذار باشد، تعیین تعداد دسته‌های حالت یک شبکه به صورت هوشمند و متغیر ممکن است منجر به افزایش دقت تشخیص شود.

در حوزه طراحی یک سیستم تشخیص حمله، استفاده از یک مجموعه جریان داده‌های شبکه که بتوان برای آموزش و آزمایش از آن استفاده نمود یک امر بسیار حائز اهمیت است. این مجموعه داده باید شامل جریان‌های

[1] Energy-based Flow Classifier
[2] False-Positive
[3] Deep Neural Network

عادی و جریان‌های حمله از انواع مختلف باشد. همچنین علاوه بر تنوع وقوع حملات، بایستی از اعتبار بالایی نیز برخوردار باشد.

در این راستا مجموعه داده انتخابی در این پژوهش، مجموعه داده CICDDoS-2019 خواهد بود که توسط Sharafaldin و همکارانش[11] در سال 2019 تولید شده است. این مجموعه داده یکی از بروزترین مجموعه‌های موجود تا این لحظه به شمار می‌رود که به صورت اختصاصی انواع حملات DDoS را، از جمله حملات DNS، LDAP، MSSQL، NetBIOS، NTP، SNMP، SSDP، UDP، Syn، TFTP و UDPLag شامل می‌شود. لازم به ذکر است که تحقیقات اخیر ذکر شده در این سند نیز با استفاده از همین مجموعه داده اقدام به طراحی و آزمایش سیستم‌های ارائه شده نموده‌اند.

# روش انجام پایان نامه

مراحل انجام پایان نامه به شرح زیر خواهد بود:

1. بررسی و آنالیز تحقیقات انجام شده بر روی مجموعه داده انتخابی
2. پیش پردازش مجموعه و استخراج ویژگی‌های پیشنهادی
3. کاهش بعد مجموعه
4. ارائه یک سیستم تشخیص مبتنی بر یک مدل توسط الگوریتم‌های یادگیری ماشین
5. آموزش و آزمایش مدل ایجاد شده

# منابع


.1 Mishra, P., et al., *A Detailed Investigation and Analysis of Using Machine Learning Techniques for Intrusion Detection.* IEEE Communications Surveys & Tutorials, 2019. **21**(1): p. 686-728.

.2 de Assis, M.V.O., et al., *Near real-time security system applied to SDN environments in IoT networks using convolutional neural network.* Computers & Electrical Engineering, 2020. **86**: p. 106738.

.3 Salahuddin, M.A., et al., *Chronos: DDoS Attack Detection using Time-based Autoencoder.* IEEE Transactions on Network and Service Management, 2021: p. 1-1.

.4 Assis, M.V.O., et al., *A GRU deep learning system against attacks in software defined networks.* Journal of Network and Computer Applications, 2021. **177**: p. 102942.

.5 Novaes, M.P., et al., *Long Short-Term Memory and Fuzzy Logic for Anomaly Detection and Mitigation in Software-Defined Network Environment.* IEEE Access, 2020. **8**: p. 83765-83781.

.6 Nie, L., et al., *Intrusion Detection in Green Internet of Things: A Deep Deterministic Policy Gradient-Based Algorithm.* IEEE Transactions on Green Communications and Networking, 2021. **5**(2): p. 778-788.

.7 Nie, L., et al., *Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach.* IEEE Transactions on Computational Social Systems, 2021: p. 1-12.

.8 Pontes, C.F.T., et al., *A New Method for Flow-Based Network Intrusion Detection Using the Inverse Potts Model.* IEEE Transactions on Network and Service Management, 2021. **18**(2): p. 1125-1136.

.9 Cil, A.E., K. Yildiz, and A. Buldu, *Detection of DDoS attacks with feed forward based deep neural network model.* Expert Systems with Applications, 2021. **169**: p. 114520.

.10 Alamri, H.A. and V. Thayananthan, *Bandwidth Control Mechanism and Extreme Gradient Boosting Algorithm for Protecting Software-Defined Networks Against DDoS Attacks.* IEEE Access, 2020. **8**: p. 194269-194288.

.11 Sharafaldin, I., et al. *Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy*. in *2019 International Carnahan Conference on Security Technology (ICCST)*. 2019.