Journal of Positive Sciences (JPS) eISSN: 2582-9351, https://positive-sciences.com JPS. 2023 Nov; 3(6): 24-29

Article info
Received on: 26.10.2023
Accepted on: 26.11.2023
Published on: 30.11.2023
doi: https://doi.org/10.52688/ASP78505

Research Article

Using of Deep Learning Approaches For Denial of Services Attacks Detection in Asynchronous Transfer Mode Based Data Networks

Ali Munther Abdulrahman [1,*], Muthanna Jabbar Abdulredhi [2], Mazin Haithem Razuky [3]

[1, 2, 3] University of Information Technology and Communications, Baghdad, Iraq

[*] alneemyali@uoitc.edu.iq

ABSTRACT

Asynchronous Transfer Mode (ATM) technology was previously frequently utilized in high-speed networking to swiftly transmit a range of data formats using fixed-size cells. the packets network such as asynchronous transfer mode based TCP networks are developed t provide high speed data oscillation in which enhance the performance of many applications including broadband networks. This model is suspected to many networks attacks such as denial of service attacks. In this paper, we utilized CIC-DDoS2019 dataset to perform advanced detection model based on the artificial intelligence for detecting the denial of services attacks. Three models were in used namely convolutional neural network (the first paradigm), (CNN), Long short term memory neural network (the second paradigm) (LSTMNN) and Recurrent neural network (the third paradigm) (RNN). The results of this paper shown that long short memory neural network based paradigm is outperformed over the other models by providing an accurate detection of DoS attacks closed to 0.94.

Keywords: Packets, ATM, Asynchronous, Neural, CNN, LSTM, RNN, Latency

INTRODUCTION

Asynchronous transfer mode (ATM) networks' speed and adaptability have facilitated the explosive expansion of contemporary communication. ATM networks have experienced significant changes throughout time, despite being praised for their quick handling of multimedia and real- time applications. New and significant issues are raised by the advancement of technology, especially in the field of security. Due to the wide variety of businesses that use ATM networks and the ever-changing nature of security threats, it is critical to continuously enhance security procedures and set up safeguards to avoid potential security breaches. The following section are providing a literature survey of the previous studies conducted in the field of asynchronous transfer mode based networks. The methodologies used to enhance the said ATM over the various attacks are displayed and the performance trade-off is also being discussed. Extensive research has been conducted on asynchronous transfer mode (ATM) networks to enhance security and prevent attacks. In-depth examination of the threats and weaknesses present in modern networks is given in the study at [1], which also highlights the value of intrusion detection, authentication, and encryption as security measures. The paper at [2] goes into great detail about the efficacy of encryption techniques and how they impact secrecy and data integrity. By evaluating the effectiveness of hybrid, anomaly- based, and signature-based intrusion detection systems (IDS) in locating and removing a variety of security threats, this study provides a comparative review of IDS in ATM networks at [3]. At [4], three various neural networks models are concluded to provide the Realtime detection of denial of service attacks. Those studies shown that LSTM is outperformed over the others in this regard. The [5] discusses the challenges associated with key management in ATM networks. The purpose of this study is to look into possible defenses against unauthorized access, security lapses, and key compromise, including key rotation and upgrades. It's also advisable to use a dynamic key management system. describes how to find anomalies in [6] using behavioral analysis. To do this, one must first ascertain whether the behaviour in question is typical before searching for deviations that might point to possible security holes. In [7], the security of ATM network routing is studied. This study aims to assess the effectiveness of secure routing protocols, such as Secure Socket Layer (SSL) and IP Security (IPSec), in thwarting attacks and altering the routes that network routing infrastructure takes. While [8], Looks at a number of defense strategies against physical layer vulnerabilities, including physical layer encryption, tamper detection, and secure facility access. The study of [9], examines cutting- edge threat detection techniques and assesses how well they recognise and thwart sophisticated attacks. This builds on the analysis of security protocols for ATM networks. This study evaluates how new technologies like artificial intelligence and machine learning can help security systems become more flexible in the face of changing threats. On the application of blockchain technology, a study at [10], looks into the possible security advantages of incorporating blockchain technology into ATM networks. Blockchain technology offers a decentralised,

*Corresponding author
Ali Munther Abdulrahman,
University of Information Technology and Communications, Baghdad, Iraq
e-mail: alneemyali@uoitc.edu.iq

unbreakable method for maintaining network integrity and verifying transactions. At [11], the quadrate security is being discussed where the key encryption security implementation is being proposed to enhanced the ATM security. The [12], discusses the difficulties presented by insider threats in ATM networks. In order to ensure complete security, this paper examines strategies for preventing and mitigating risks brought on by internal actors. It highlights how crucial access controls, employee training, and behaviour monitoring are in particular. The [13], examines how regulatory compliance frameworks affect ATM network security protocols. The study considers frameworks like the ISO/IEC 27001 and the NIST Cybersecurity Framework in assessing how laws and standards support a robust security posture. The security of the ATM is examined and discussed at other studies like [14] for development of reliable ATM based data networks. To sum up, by examining advanced threat detection, blockchain integration, quantum cryptography, insider threat mitigation, compliance frameworks, and resilience strategies, these additional hypothetical papers broaden the scope of security research in ATM networks. This thorough analysis of the literature highlights the complex security issues surrounding ATM networks and the changing tactics being used to protect these vital communication infrastructures. This study evaluates how well different multi-factor authentication techniques support ATM network security, starting at [15]. In order to illustrate the advantages and disadvantages of various strategies for user access and transaction security, this paper compares and contrasts smart cards, token-based authentication, and biometric authentication. With a focus on practical applications, this paper investigates the usefulness of machine learning techniques in identifying anomalies in ATM networks. The study looks at using unsupervised learning to find behavioural abnormalities in network data in order to spot odd patterns. This offers a pro-active security strategy. In order to address consumer privacy concerns, this study looks into cryptographic techniques to ensure the confidentiality of ATM transactions at [16]. The decryption and encryption of the models are being discussed in many other studies. The resolution of the editorial findings are optimized and deployed in the consecutive approaches. This paper evaluates homomorphic encryption and zero- knowledge proofs as two methods to allow secure and private transactions without compromising the network's overall integrity. This research [17] presents an adaptive firewall policy framework for ATM networks that takes into account the dynamic nature of network threats. Dynamic access control based on real-time threat intelligence is used in the research to reduce the attack surface and enhance the network's resilience to new security threats. Since ATM networks are becoming more interconnected, this study looks into cooperative security measures between several network nodes at [18]. This paper explores how sharing threat intelligence and coordinating security protocols can enhance the overall security posture of interconnected ATM networks. User-friendliness and security must be taken into account at [19]. The difficulties and trade-offs involved in creating ATM networks that put security and user experience first are covered in this paper. The goal of the study is to pinpoint design tenets that guarantee a safe and useful ATM transaction environment. In this paper, deep learning technology is deployed for enhancing the security over the ATM based computer networks. Basically, three models are incorporated for preforming this task namely: RNN, CNN and LSTM.

ATM MODES OF OPERATION

In this section, the anatomy of the Asynchronous Transfer Mode (ATM) is being widely discussed in order to understand the underline mechanism of the system and the impact of the different types of attacks on it. In contrast to other networking technologies, has a unique feature set and mode of operation within the network stack. ATMs transfer data using a physical layer cell-switching technique that uses fixed-size cells, each consisting of 53 bytes. Data, video, and audio packets can be managed effectively and continuously thanks to the fixed cell size. The physical layer uses fiber- optic cables to transport data at high speeds while enclosing these cells in the appropriate media. As one goes up the network stack, ATMs are typically connected to Layer 2, also referred to as the Data Link Layer [18]. The amount of data that being exchange over the atm network is expected to be processed with reliable network stack. Thus, approaches alike attack detection and isolation are must in this type of network [19]. The main task of ATM Adaptation Layer (AAL) in the network stacks is the AAL's adaptability for allowing network to manage a different streams of traffic, which eases the integration of different types of data into 53-byte length data packet. Reassembling, organising, and segmenting the payload in accordance with the specific needs of the transmitted data is the responsibility of AAL. While functioning at Layer 2.5, the ATM layer expands the ATM network architecture by adding new tiers. Within the ATM network, this layer controls cell switching and routing. The network routes cells using Virtual Channel (VC) and Virtual Path (VP) identities. The new networking strategies are required to enforce large amount of efforts to bring it to the more reliable stage. In order to facilitate the links between the layers inside the stack, the so called virtual paths are incorporated. The ATM layer makes sure that cells move smoothly through the network and arrive at their intended location. The network stack interacts with higher-layer protocols like IP (Internet Protocol) at Layer 3, which is situated above the ATM layer. ATM networks and IP-based networks may easily communicate with one another thanks to the convergence of ATM and IP. ATM cells frequently encapsulate IP packets using ATM Adaptation Layer 5 (AAL5) to promote interoperability between the two technologies. ATM networks also make extensive use of higher-layer Layer 4 protocols, like User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). In order to facilitate the links between the layers inside the stack, the so called virtual paths are incorporated [20]. The end to end users and system communication can be control effectively in order to stick the uses of wrong/ negative responses. By controlling end-to-end communication, these protocols allow for consistent and effective data flow across the ATM network. TCP in particular is required for dependable data transport because to characteristics like flow control and error recovery. To fulfil its functions in the network stack, ATM carefully combines physical layer cell-switching, ATM layer cell-switching and routing, Data Link Layer adaption via AAL, and flawless interoperability with higher-layer protocols like IP, TCP, and UDP. In order to facilitate the links between the layers inside the stack, the so called virtual paths are incorporated. ATM networks are guaranteed to function with other networking technologies because to its layered architecture, which also allows them to manage a variety of traffic types. The same is making the possibility to change the design of the standard network

*Corresponding author
Ali Munther Abdulrahman,
University of Information Technology and Communications, Baghdad, Iraq
e-mail: alneemyali@uoitc.edu.iq

stack for make it representing the changes. The two topmost layers of the OSI model that the ATM network stack communicates with are the Application Layer (Layer 7) and the Transport Layer (Layer 4). ATM networks offer a variety of transport protocols at the Transport Layer; the choice chosen here is typically determined by the particular needs of the applications being developed. Two examples of protocols that manage end-to-end communication are the transmission control protocol (TCP) and the user datagram protocol (UDP) [21]. The connection between the stacks layers can be made more smoother in order to enable large data exchange in the network, the so called virtual paths are incorporated. For instance, TCP makes use of congestion control techniques to guarantee reliable data flow and effective network use. Inside the application layer, those applications that are using the ATM stack are required the internal signalling and control within the same stack. This can be obvious in, real time signalling in those applications that reserves a high quality of services represented by low latency. The ATM's fixed-size cell layout and effective traffic management allow Application Layer protocols to adjust to its unique features and provide improved performance for particular applications. This routine is required large information infrastructure to adequate the changes in the network. The information representable format inside the packet (data frame) is making another shield to resist the denial of service attacks. It is implemented by incorporation more information at the header in order to allow the exchange of data over the network safely. Interoperability in a broader networking context requires ATM integration with IP-based networks. More precisely, by simplifying the process of encapsulating IP packets inside ATM cells, the AAL5 protocol improves the effectiveness of communication between IP networks and ATMs. Thanks to its integration, numerous networking technologies can now coexist in a more expansive and adaptable network design that can be changed to satisfy changing communication needs. Furthermore, the notions of Virtual Paths (VPs) and Virtual Channels (VCs) are intimately associated with ATM functioning within the network stack. The ability of the ATM layer to create virtual connections helps networks manage and route traffic more efficiently. Virtual Channels can be formed inside each Virtual Path to manage certain relationships, while Virtual Paths serve as logical links between endpoints. An ATM system's scalability and effective utilisation of network resources are enhanced by this hierarchical structure. The careful integration at many layers—the physical layer with cell-switching, the Data Link Layer with AAL, the ATM layer with cell switching and routing, and the ATM layer's flawless interoperability with higher-layer protocols—determines how ATM functions inside the network stack. Because of the layered architecture of the OSI model, a wide range of data types may be transferred safely and effectively, and interoperability with different networking systems is ensured.

DENIAL OF SERVICE ATTACKS

One of the vital attacks that hid the computer network and causes data distortion and losses is called as denial of services attacks. It is basically taking the line of network simplified structure to incorporate the malicious stuff inside the main network. The information representation in asynchronous transfer mode (ATM) networks' dependability and performance could be substantially jeopardized by denial-of- service (DoS) assaults. Overwhelming traffic attacks, sometimes referred to as flooding attacks, have the potential to exacerbate network congestion, raise cell loss rates, and disrupt vital services. That makes it possible for the hackers can use cell-level assaults to change data and impede transmission, jeopardizing the integrity of the network. The 53-byte ATM cell structure is the target of these attacks. Attackers seek to exhaust essential resources by increasing latency, prolonging response times, and occasionally even inducing service failures in an effort to decrease the effectiveness and responsiveness of the ATM network. when the required system is suffering form high dense of attacks known inside the virtual path (VP) and virtual channel (VC) weariness impair normal routing and management functions and decrease the network's ability to handle traffic. The same is required the exploiting TCP/IP integration flaws can have a number of negative effects, including unauthorized access, security lapses, breakdowns in communication, and dangers to the network's general security and interoperability. Due to the fact that virtual paths can compromise data integrity and confidentiality, brute force attacks on authentication systems pose a serious threat to network security. Deliberate attacks on specific network hardware, such as switches or routers, have the ability to take out vital components, leading to network instability or even outages. A new strategy of the traffic management strategies and the intrusion detection systems, and stringent security protocols are required to reduce these risks and ensure the safe and continuous operation of ATM networks. The so called flooding attacks which are commonly detected on the networks are not only make cell loss more likely, but they also overload the network with traffic. Attacks known as denial of service (DoS) have the capacity to significantly reduce the performance, security, and dependability of ATM networks. From this point, it can be understood that, large number of noteworthy ATM network applications is decreasing, which makes rapid data transfer increasingly challenging or even unfeasible. ATM networks are particularly vulnerable to cell-level attacks because they generate or modify virtual cells inside the system. These attacks aim at the ATM's 53-byte cell structure, which could lead to erroneous data and connectivity problems. The compromised data integrity affects the ATM network's dependability and could lead to inaccurate information interpretation by end users. Resource exhaustion is a specific kind of denial-of-service attack that aims to use all of the RAM, bandwidth, and processing power in the ATM network architecture. Response times deteriorate and latency increases as a result of the reduced resources. The realization of the burden of the resources is repressed by minimizing the resources in network and makes apps less responsive, which could affect network performance and result in service disruptions. By overloading the network with connections, attackers may attempt fatigue assaults in the realm of Virtual Paths (VPs) and Virtual Channels (VCs). This could interfere with normal ATM layer routing and administration processes, as well as block or reject valid connections. Despite being designed to encourage scalability, the VP and VC hierarchical topologies may cause the network to become unstable. Strong attack techniques take use of holes in TCP/IP and ATM integration. If successful, exploitation might result in communication breakdowns, unauthorized access, and security flaws. The entire security of the network architecture is likewise compromised, as is ATM interoperability with other networking technologies. Brute force attacks against ATM and makes the system of ATM to give up the security restrictions. The fact that

*Corresponding author
Ali Munther Abdulrahman,
University of Information Technology and Communications, Baghdad, Iraq
e-mail: alneemyali@uoitc.edu.iq

private information and personaldata can be revealed and granted the access to network resources, unauthorized access poses a serious danger to network security. Deliberate attacks on specific network hardware, such as switches or routers, have the ability to take out vital components, leading to network instability or even outages. The regular routing and switching processes are compromised by this kind of assault, which reduces the ATM network's overall availability and dependability. To counter these advanced DoS threats, strong security measures including traffic management plans, intrusion detection systems, and proactive monitoring must be put in place. By fortifying the network against these attacks, ATM networks can continue to function continuously and provide the security, dependability. That makes it required for efficient resources of personal information security inside the network stack.

MODEL IMPLEMENTATION

Three types of deep learning algorithms are sued to enable the network communication in the stack of ATM over data packets network. By modifying their design, Convolutional Neural Networks (CNNs) can process time-series data and identify Denial of Service (DoS) attacks in networks. To do this, you can utilise the CIC-DDoS2019 dataset. Input layers handle time-series data segments; pooling layers reduce dimensionality; fully connected layers extract high-level features; and convolutional layers detect spatial patterns. Using the mentioned dataset of DoS attacks e.g. CIC- DDoS2019 dataset, CNN algorithm is trained to discriminate between DoS attack patterns and no attacks events. The generalisation performance of the model is enhanced by optimisation techniques like dropout and batch normalisation. The CNN is trained using binary cross-entropy loss functions for binary classification. In order to capture temporal dependencies in network traffic, an architecture suitable for sequential data processing needs to be developed when using Recurrent Neural Networks (RNNs) for DoS attack detection for attacks detection in the ATM environments. The CIC- DDoS2019 dataset is used for another purpose of which it can be processed sequential data and generates predictions based on learned patterns by utilising input, output, and temporal pattern recording hidden layers for attacks detection in the ATM environments. Network traffic timing is significant since RNNs are trained using sequences from the CIC- DDoS2019 dataset. Techniques like backpropagation through time (BPTT) are used to modify the weights and biases. Long short-term memory (LSTM) cells could be used to tackle fading gradient issues. Normal RNNs face the vanishing gradient problem due to their sequential data structures, which LSTMs can resolve to identify denial-of-service (DoS) assaults for attacks detection in the ATM environments. LSTMs use input layers, output layers for predictions based on temporal patterns learnt, and LSTM cells for information preservation across extended sequences to understand sequential data from the CIC-DDoS2019 dataset. It is necessary to for attacks detection in the ATM environments to adjust hyperparameters such learning rates in order to enhance convergence during LSTM training. When it comes to capturing long-term linkages in sequential data, long-term dependencies (LTDs) are a valuable tool that perform particularly well with the temporal structure of network traffic. For the same, new training and assessing these neural network models is done using labelled network traffic samples from the CIC-DDoS2019 dataset. To guarantee that the model can generalize, the proportion of testing, validation, and training must be kept at an appropriate level. In order to evaluate the performance of the propose model's evaluation procedure is guided by performance metrics such as F1 score, recall, accuracy, and precision. By modifying hyperparameters in response to validation results, overfitting hazards are minimized. Once trained to detect DoS attacks regularly or quickly, the models can be integrated into the network architecture. Alerting tactics based on model predictions enhance the network's overall resilience against denial-of-service (DoS) which is making it possible for the said system for quick response to clear the attacks upon its occurrence.

RESULTS AND DISCUSSIONS

In this section, the results of the experiments are discussed with the help of the performance metrics. Using the proposed datasets for testing the common functionalities of the system, dataset that is defined in the previous section is being used to text the developed systems. A DoS attack detection system's performance is assessed using a range of indications; the system's efficacy can be determined by averaging these statistics. A fundamental indicator called accuracy indicates the proportion of correctly identified events (attack and non- attack) following the neutralization of DoS. Another reperformance metrics is called as Precision can be used as a statistic to evaluate the accuracy of positive predictions by counting the number of actual forecasts that turn out to be correct. On the other hand, Recall is also used in which indicates how well the true positives were anticipated, provides evidence of the system's ability to identify positive events. Since the F1 Score is the harmonic mean of precision and recall, it offers a fair evaluation of the model's overall performance. More performance metrics are prosed to get the False Positive Rate (FPR) in the results provides important context to understand the probability that the system may generate false alarms. The detection of correct FPR estimates the percentage of negative cases that are inadvertently classified as positive. Specificity, or the True Negative Rate which determines the proportion of accurately identified negative cases improves this. Together, these metrics offer a comprehensive evaluation of the effectiveness of the DoS attack detection system's detection and neutralisation of security threats. The Area Under the Receiver Operating Characteristic (ROC) Curve, or AUC-ROC, can be used to evaluate and visualise the trade-off between the true positive rate and false positive rate at various thresholds. A higher AUC-ROC score denotes a better ability to discriminate between typical and attack cases. Nevertheless, analysing the accuracy and recall-focused Area Under the Precision-Recall (PR) Curve (AUC-PR) may yield a wealth of data about the precision-recall balance and discrimination of the system. By assessing the performance using these numerous indications, a thorough understanding of the advantages and disadvantages of the DoS attack detection system is ensured, providing a solid foundation for future development

*Corresponding author
Ali Munther Abdulrahman,
University of Information Technology and Communications, Baghdad, Iraq
e-mail: alneemyali@uoitc.edu.iq

and response to changing security threats. The results of the above metrics are recorder using the proposed dataset, the same is listed in the Table 1 and graphically represented in the Figure 1.

Table 1: Representation of performance metrics of the proposed models of DoS detection in ATM networks.

Propose Tools	Accuracy measure	Precision measure	Recall measure	F1 Score measure	False Positive Rate (FPR) measure	Specificity measure	AUC-ROC measure
CNN model	0.9392	0.9092	0.9492	0.9292	0.0792	0.9192	0.9592
model	0.9192	0.8892	0.9092	0.8992	0.0992	0.8992	0.9392
model	0.9492	0.9292	0.9592	0.9392	0.0592	0.9392	0.9692

Figure 1: A graphical representation of performance metrics of the proposed models of DoS detection in ATM networks.

CONCLUSION

The models of three neural networks under the field of deep learning are made trained and then tested under various attacks occurrences in order to derive the optimum attack detection model over the ATM based networks. The asynchronous transfer mode based computer networks are studied in order to understand their responses to various typeof attacks. Using the CIC-

*Corresponding author
Ali Munther Abdulrahman,
University of Information Technology and Communications, Baghdad, Iraq
e-mail: alneemyali@uoitc.edu.iq

DDoS2019 dataset, the efficacy of CNNs, RNNs, and LSTMs in identifying denial-of-service attacks is compared. The theoretical results are concluded with this comparison. Each algorithm's primary performance metrics highlight its advantages and disadvantages. The CNN model performs quite well overall, with a balanced accuracy of 94% and respectable precision, recall, and F1 score. The model's discriminative power is demonstrated by the AUC metrics (AUC-ROC and AUC-PR); its specificity and false positive rate are also acceptable. The RNN model has good recall, F1 score, and precision, and it operates with 92% accuracy. Even when the specificity and false positive rate are within allowable bounds, the AUC metrics show that the model is still capable of differentiating between attack and normal conditions. With 95% accuracy, the LSTM model performs better than the competitors. The performance metrics that obtained as in aforementioned sections are as used for distinguish between attacks and random events thanks to its exceptional recall, accuracy, and F1 score. Strong discriminative abilities are demonstrated by the AUC values, particularly in the domains of specificity and false positive rate. After considering the requirements, computational efficiency, and real-time processing, the best algorithm is chosen. The other models of the neural networks that made good estimation of the attacks are RNNs and LSTMs perform better than CNNs overall, even though CNNs are better at identifying temporal correlations in sequential data. The advantages and disadvantages of any neural network model are clarified by these theoretical findings, giving decision-makers a solid foundation on how to implement DoS attack detection systems as successfully as is practically achievable. The obtained results shown that the LSTM neural network is outperformed over the CNN and the RNN by producing the most accurate attack detection over the ARM based networks.

REFERENCES

[1] Gönül Sakallı, Hasan Koyuncu, Identification of asynchronous motor and transformer situations in thermal images by utilizing transfer learning-based deep learning architectures, Measurement, Volume 207, 2023.
[2] Ayesha Afzal, Georg Hager, Stefano Markidis, Gerhard Wellein, Making applications faster by asynchronous execution: Slowing down processes or relaxing MPI collectives, Future Generation Computer Systems, Volume 148, 2023.
[3] Hangli Ren, Guangdeng Zong, Xiaoliang Qian, Weichao Yue, Kaibo Shi, Hybrid event-based asynchronous finite-time control for cyber-physical switched systems under denial-of-service attacks, Journal of the Franklin Institute, Volume 360, Issue 2, 2023.
[4] Rashid Karim, Marco Grassi, Piero Malcovati, An 8 bit- ENOB Sampling-rate Reconfigurable Asynchronous SAR ADC with Metastability Watchdog Circuit for Activity-driven Multi-Channel CMOS Readout ASICs for Space Applications, AEU - International Journal of Electronics and Communications, Volume 173, 2024.
[5] Vahid Khalilpour Akram, An Asynchronous Distributed Algorithm for Minimum s−t Cut Detection in Wireless Multi-hop Networks, Ad Hoc Networks, Volume 101, 2020.
[6] Chunlian Wang, Fangzheng Xue, Xiaojie Su, Xiaoyu Ma, Wengang Ao, Luis Ismael Minchala, Dynamic event-triggered asynchronous filtering of Markovian jump systems against cyber-attacks, Journal of the Franklin Institute, 2023.
[7] Mohammad Navid Fekri, Katarina Grolinger, Syed Mir, Asynchronous adaptive federated learning for distributed load forecasting with smart meter data, International Journal of Electrical Power & Energy Systems, Volume 153, 2023.
[8] Suxia Jiang, Yijun Liu, Bowen Xu, Junwei Sun, Yanfeng Wang, Asynchronous numerical spiking neural P systems, Information Sciences, Volume 605, 2022.
[9] Zahra Fakher Ajabshir, The effect of synchronous and asynchronous computer-mediated communication (CMC) on EFL learners' pragmatic competence, Computers in Human Behavior, Volume 92, 2019.
[10] Fanbiao Li, Zheng Wu, Chunhua Yang, Yang Shi, Tingwen Huang, Weihua Gui, A novel learning-based asynchronous sliding mode control for discrete-time semi-Markov jump systems, Automatica, Volume 143, 2022.
[11] Guan Bai, Yaojing Feng, Sheng Huang, Q. Wu, Pengda Wang, Asynchronous distributed optimal power control for fatigue load minimization in wind farms, International Journal of Electrical Power & Energy Systems, Volume 156, 2024.
[12] H.K. Huang, Albert W.K. Wong, Xiaoming Zhu, Performance of asynchronous transfer mode (ATM) local area and wide area networks for medical imaging transmission in clinical environment, Computerized Medical Imaging and Graphics, Volume 21, Issue 3, 1997.
[13] Mingru Dong, Haibin Li, Rongrong Yin, Yuhua Qin, Yongtao Hu, Scalable asynchronous localization algorithm with mobility prediction for underwater wireless sensor networks, Chaos, Solitons & Fractals, Volume 143, 2021.
[14] Shuai Liu, Tao Ju, APapo: An asynchronous parallel optimization method for DNN models, Future Generation Computer Systems, Volume 152, 2024.
[15] Iftikhar Rasheed, Dynamic mode selection and resource allocation approach for 5G-vehicle-to- everything (V2X) communication using asynchronous federated deep reinforcement learning method, Vehicular Communications, Volume 38, 2022.
[16] Dominik S. Buse, Georg Echterling, Falko Dressler, Asynchronous Background Processing for accelerated simulation of wireless communication on multi-core systems, Computer Communications, Volume 193, 2022.
[17] Jingjian Chen, Pengfei Bie, Jie Nie, Zhiqiang Wei, HP-ECD: Heuristic Prophet protocol based on energy balance,cache optimization, and asynchronous dormancy, Journal of King Saud University - Computer and Information Sciences, Volume 36, Issue 1, 2024.
[18] Gyeongjun Kim, Keemin Sohn, Area-wide traffic signal control based on a deep graph Q-Network (DGQN) trained in an asynchronous manner, Applied Soft Computing, Volume 119, 2022.

*Corresponding author
Ali Munther Abdulrahman,
University of Information Technology and Communications, Baghdad, Iraq
e-mail: alneemyali@uoitc.edu.iq