MULTIMEDIA COMMUNICATIONS TECHNICAL COMMITTEE
IEEE COMMUNICATIONS SOCIETY
http://mmc.committees.comsoc.org/

MMTC Communications – Review

IEEE COMMUNICATIONS SOCIETY

Vol. 15, No. 2, June 2024

TABLE OF CONTENTS

Message from the Review Board Directors

Welcome to the June 2024 issue of the IEEE ComSoc MMTC Communications – Review.

This issue comprises three reviews that cover multiple facets of multimedia communication research including privacy protection over metaverse, machine learning based network abnormal traffic detection, mobile video streaming enhancement. These reviews are briefly introduced below.

The first paper, published in IEEE Journal on Selected Areas in Communications and edited by Dr. Ye Liu, provides a comprehensive approach to understanding and mitigating the risks associated with linking virtual and real identities in the metaverse, offering theoretical models and practical solutions to enhance user privacy and security in this emerging digital realm.

The second paper, edited by Dr. Shengjie Xu, was published in IEEE Wireless Communications. This paper presents a framework for anomalous traffic detection leveraging deep reinforcement learning.

The third paper, edited by Dr. Qichao Xu, was published in IEEE Transactions on Wireless Communications. The paper presents a framework that considers different factors in the design of caching and computing strategies, aiming to maximize the overall user satisfaction.

All the authors, reviewers, editors, and others who contribute to the release of this issue deserve appreciation with thanks.

IEEE ComSoc MMTC Communications – Review Directors

Yao Liu
Rutgers University, USA
Email: yao.liu@rutgers.edu

Wenming Cao
Shenzhen University, China
Email: wmcao@szu.edu.cn

Dongfeng (Phoenix) Fang
California Polytechnic State University, USA
Email: dofang@calpoly.edu

Ye Liu
Macau University of Science and Technology, Macau, China
Email: liuye@must.edu.mo

Privacy Protection Framework for Metaverse

A short review for "VRIL: A Tuple Frequency-Based Identity Privacy Protection Framework for Metaverse"

Edited by Ye Liu

Z. Yang, X. Cao, H. Wang, D. Wu, R. Wang, and B. Yang, " VRIL: A Tuple Frequency-Based Identity Privacy Protection Framework for Metaverse," in IEEE Journal on Selected Areas in Communications, vol. 42, no. 4, pp. 933-947, April 2024.

The concept of the metaverse [1] refers to a shared, open, human-centric digital realm that transcends reality. Enabled by advanced technologies like artificial intelligence, blockchain, 5G/6G, extended reality, and bionics, the metaverse allows users to experience immersive interactions within this virtual environment. It is an advanced and interactive virtual reality system where users' sensory perceptions are isolated from the real world and simulated in a controlled environment. This simulation is achieved through multi-sensory display and tracking technologies, allowing real-time interactions between users through their avatars [2].

A key element in the metaverse is the virtual identity, which can either mirror a user's real-world identity or exist as a separate, decentralized identity, particularly in Web3 applications. The debate over whether virtual identities should be seamlessly linked with real identities is ongoing. Proponents of decentralization argue for user control and privacy, opposing the oversight of technology giants and governments. In contrast, supporters of centralization stress the importance of trust and security, advocating for the linkage of virtual identities to real legal identities. A middle ground suggests allowing law enforcement to link virtual and real identities when necessary.

This discussion, however, often overlooks the privacy risks associated with linking virtual and real identities (VRIL). The metaverse expands communication beyond time and space constraints, but also increases the risk of privacy breaches. As metaverse applications grow, the dangers of VRIL become more apparent. For example, in platforms like Roblox, attackers can trace users from their avatars and infer their real-world identities, posing significant risks as users are often unaware of the external environment during immersive experiences. This exposure can lead to illegal violations and cybercrimes, as depicted in the film "Ready Player One," where the protagonist's real identity revelation leads to dire consequences.

Furthermore, VRIL can negatively impact the user experience within the virtual world. Attackers can carry real-world grievances into the metaverse, committing virtual assaults or defrauding users by exploiting their virtual identities. As the user base of the metaverse grows, the risks associated with VRIL will likely increase, potentially hindering the development of metaverse applications.

To mitigate VRIL risks, users should adopt protective measures such as using pseudonyms and avoiding the disclosure of real-world information in virtual environments. However, these de-identification methods are not foolproof. Even without sophisticated hacking tools, attackers can link a user's virtual and real identities by observing overlapping attribute information (e.g., gender, age, occupation) from both realms. This intersection of attribute data makes it easier for attackers to make these connections, even with minimal technical expertise.

This paper introduces a VRIL attack model that links virtual identities with real ones using observable attribute values. Current studies on VRIL attacks are limited, focusing mainly on fields like medical and demographic re-identification. Re-identification involves matching anonymized user data with identified records to reveal the user's identity.

The contributions of this paper are: (i) VRIL Risk Analysis Method: The paper constructs a VRIL attack model and proposes a new quantitative VRIL risk analysis method. It provides theoretical insights into VRIL attacks, describing the relationship between tuple frequency distribution and VRIL risk mathematically. (ii) Theoretical Framework: A theoretical framework for tuple frequency distribution is developed, along with models for population distribution, RH distribution, and approximate binomial distribution of tuple frequency with incomplete statistical information. These models support VRIL risk prediction and are tested using random data, showing high accuracy for the RH distribution and strong practicability for the approximate binomial distribution. (iii) Attribute Correlation Analysis: The paper identifies the influence of attribute correlation and value correlation on tuple frequency distribution. It proposes a method for quantitatively analyzing these correlations to distinguish characteristics of biased and unbiased samples. An improved method incorporating prior correlation knowledge is suggested to better predict VRIL risks in biased samples. (iv) Random Dataset Generation: A method for generating random datasets is proposed, and the TupPre model's performance is verified in both random and real-world datasets. The TupPre model, using the approximate binomial distribution, demonstrates excellent accuracy (mean AUC 0.86~0.98) on unbiased datasets and real-world datasets with certain biases. Introducing prior knowledge significantly improves prediction accuracy on biased samples, validating the practical value of the TupPre model in VRIL risk prediction.

Overall, the paper provides a comprehensive approach to understanding and mitigating the risks associated with linking virtual and real identities in the metaverse, offering theoretical models and practical solutions to enhance user privacy and security in this emerging digital realm.

References:

[1] Y. Wang et al., "A Survey on Metaverse: Fundamentals, Security, and Privacy," in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 319-352, Firstquarter 2023,

[2] H. Duan, et al. "Metaverse for social good: A university campus prototype." Proceedings of the 29th ACM international conference on multimedia. 2021.

[3] C. Zhang, M. Zhao, W. Zhang, Q. Fan, J. Ni and L. Zhu, "Privacy-Preserving Identity-Based Data Rights Governance for Blockchain-Empowered Human-Centric Metaverse Communications," in IEEE Journal on Selected Areas in Communications, vol. 42, no. 4, pp. 963-977, April 2024.

Ye Liu, received the M.S. and Ph.D. degrees in electronic science and engineering from Southeast University, Nanjing, China, in 2013 and 2018, respectively. He was a Visiting Scholar with Montana State University, Bozeman, MT, USA from October 2014 to October 2015. He was a visiting Ph.D. Student from February 2017 to January 2018 with the Networked Embedded Systems Group, RISE Swedish Institute of Computer Science, Kista, Sweden. He is currently an Associate Professor with Nanjing Agricultural University, Nanjing, China. He has authored or co-authored papers in several prestigious journals and conferences, such as the IEEE WCM, IEEE IEM, IEEE ComMag, IEEE Network, IEEE IoTJ, IEEE TII, ACM TECS, INFOCOM, IPSN, ICNP, and EWSN. His current research interests include wireless sensor networks, energy harvesting systems, and smart agriculture. Dr. Liu was awarded the 1st place of the EWSN Dependability Competition in 2019.

Network Abnormal Traffic Detection Framework Based on Deep Reinforcement Learning

A short review for "Network Abnormal Traffic Detection Framework Based on Deep Reinforcement Learning"

Edited by Shengjie Xu

S. Dong et al, "Network Abnormal Traffic Detection Framework Based on Deep Reinforcement Learning," in IEEE Wireless Communications, vol. 31, no. 3, pp. 185-193, June 2024.

The dynamic, high-dimensional, and voluminous nature of traffic in high-speed wireless networks exacerbates the difficulty of detecting real-time threats and identifying unknown attacks [1-4]. This paper introduces a novel framework for abnormal traffic detection utilizing deep reinforcement learning, comprising four primary stages: data collection, dataset pre-processing, feature selection, and model detection. Experimental evaluations demonstrate that this framework significantly enhances the performance of abnormal traffic detection.

The contributions of this article can be summarized as follows: 1. Framework for Abnormal Traffic Detection: the authors propose a deep reinforcement learning-based framework for abnormal traffic detection, which encompasses four main stages: data collection, dataset pre-processing, feature selection, and model detection. 2. Feature Selection using Henry Gas Solubility Optimization (HGSO) Algorithm: the HGSO algorithm is employed for feature selection, effectively removing attribute-related and redundant features, selecting the optimal feature subset, and reducing the learning model's time overhead. 3. Enhancements in A3CAD: to avoid the model falling into local optimization, an exploration term is added to the gradient update of the actor-network in A3CAD. Additionally, the logarithm of the number of steps per iteration is introduced in the critic network's gradient update to accelerate the algorithm's convergence. 4. Deep Maxout Neural Network (DMNN) in A3CAD: the neural network in A3CAD utilizes a Deep Maxout Neural Network, which combines the maxout activation function with dropout, resulting in improved approximation capabilities.

The authors outline the comprehensive framework and methodologies employed in their proposed approach for detecting abnormal traffic, emphasizing the significance of each stage in optimizing detection performance and addressing the complexities inherent in traffic analysis.

The selection of datasets is crucial in contemporary abnormal traffic detection techniques, as the data quality significantly influences the detection capabilities of deep reinforcement learning models. Given the diverse nature of abnormal traffic, no single dataset can encapsulate all classes of abnormal traffic, leading to the absence of a universally acknowledged dataset in this field.

Traffic data collected from real network environments often contains numerous missing values, noise, redundant values, attribute correlations, and potential outliers due to manual labeling errors. These issues can hinder the performance of machine learning models. The dataset pre-processing stage addresses these problems by employing operations such as data cleaning and data transformation to produce standardized and continuous traffic data, thereby enhancing the detection performance of machine learning models. Consequently, dataset pre-processing is pivotal in the abnormal traffic detection process.

The massive and high-dimensional nature of network traffic imposes stringent requirements on abnormal traffic detection models. The sheer volume of network traffic can lead to overfitting in machine learning models, reducing their learning efficacy. High-dimensional data, characterized by its sparsity, can significantly escalate the memory and computational costs of data analysis. Feature selection serves as a vital data pre-processing strategy to mitigate the impact of noisy, misleading, or inconsistent features on model performance. It improves learning performance, reduces memory storage, and facilitates the development of better generalized models, making it a widely adopted technique in preparing data for data mining and machine learning applications.

In this stage, the authors enhance the Asynchronous Advantage Actor-Critic (A3C) algorithm by proposing the A3CAD model, which leverages CPU multi-threading capabilities to execute multiple Actor-Critic (AC) agents in parallel and asynchronously. These multiple AC agents learn from various target traffic features, integrate the acquired experience data, and update the global network accordingly.

The proposed model offers several key advantages in real-world environments: 1. Self-Adaptive Capability in Diverse Environments: The model exhibits adaptability across different platforms and protocols without requiring redeployment, ensuring seamless integration and functionality in varied settings. 2. Handling Massive Traffic Data: As network traffic volume increases, the ability to perform real-time analysis and issue alerts becomes critical. Our model is designed to manage large-scale traffic data efficiently. 3. Detecting Unknown Attacks: The model's self-learning capability enables it to adapt to complex and evolving attack patterns, reducing the need for repeated model retraining.

While the proposed framework achieves favorable results, it encounters challenges in detecting certain types of abnormal traffic, specifically R2L (Remote to Local) and U2R (User to Root) attacks. These attack types are typically underrepresented in real network environments compared to simulated datasets. Addressing this discrepancy is crucial for improving detection rates for these low-frequency attacks. The future research will focus on the following areas: 1. Multi-Agent Deep Reinforcement Learning (DRL): Despite their infrequent use in abnormal traffic detection, multi-agent DRL approaches have demonstrated significant potential. The authors plan to investigate multi-agent DRL further to enhance the detection of low-frequency abnormal attacks through adversarial learning among agents. 2. Enhanced Learning Capabilities in A3CAD: Currently, the A3CAD model relies on datasets to provide the state of the next moment rather than generating it through interaction with the environment, leading to limited learning capabilities. The future work will involve integrating artificial intelligence environments with the DRL model to improve the accuracy and robustness of abnormal traffic detection.

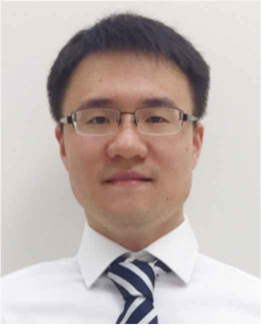
References:

[1] X. Hu et al., "Dynamic Beam Hopping Method Based on Multi-Objective Deep Reinforcement Learning for Next Generation Satellite Broadband Systems", IEEE Trans. Broadcast., vol. 66, no. 3, pp. 630-46, Sept. 2020.

[2] Y. Cao, S.-Y. Lien and Y.-C. Liang, "Deep Reinforcement Learning for Multi-User Access Control in Non-Terrestrial Networks", IEEE Trans. Commun., vol. 69, no. 3, pp. 1605-19, Mar. 2021.

[3] Cheng et al., "Federated Transfer Learning with Client Selection for Intrusion Detection in Mobile Edge Computing", IEEE Commun. Lett., vol. 26, no. 3, pp. 552-56, Mar. 2022.

[4] N. C. Luong et al., "Applications of Deep Reinforcement Learning in Communications and Networking: A Survey", IEEE Commun. Surveys & Tutorials, vol. 21, no. 4, pp. 3133-74, 2019.



Shengjie Xu [SM'14-M'19] received a Ph.D. degree in Computer Engineering from the University of Nebraska-Lincoln and an M.S. degree in Telecommunications from the University of Pittsburgh. Before that, he held a B.E. degree in Computer Science and Information Security. He is an assistant professor in the Department of Cyber, Intelligence, and Information Operations at the University of Arizona. His research interests are cybersecurity, trustworthy AI and robust machine learning, secure edge computing, and critical infrastructure protection. He serves as a Technical Editor for IEEE Wireless Communications. He is the recipient of the IET Journals Premium Award for Best Paper. He holds multiple professional certifications in cybersecurity and computer networking.

Enhancing Mobile Video Streaming: QoE-Aware Edge Caching and Computing

A short review for "QoE-Aware Collaborative Edge Caching and Computing for Adaptive Video Streaming"

Edited by Qichao Xu

W. Liu, H. Zhang, H. Ding, Z. Yu and D. Yuan, "QoE-Aware Collaborative Edge Caching and Computing for Adaptive Video Streaming," IEEE Transactions on Wireless Communications, vol. 23, June 2024.

The digital era has witnessed an exponential growth in the consumption of video content, with mobile devices becoming the primary screen for many users. This surge has put unprecedented pressure on wireless networks to deliver high-quality streaming experiences[1]. The paper addresses these challenges by proposing an innovative framework that integrates edge caching and mobile edge computing (MEC) to enhance the Quality of Experience (QoE) for adaptive video streaming. Video streaming has evolved from a passive viewing experience to an interactive one, where users expect high-definition content with minimal latency and buffering. The advent of Dynamic Adaptive Streaming over HTTP (DASH) has been a game-changer, allowing video streams to adapt in real-time to the user's network conditions[2], [3]. However, the variability in network bandwidth and the diverse range of user devices necessitate a more sophisticated approach to ensure QoE of users[4].

The paper highlights the challenges posed by the increased data volume in DASH, which can lead to network congestion and a degradation of the QoE. The authors emphasize the importance of addressing these challenges by leveraging the potential of edge caching and MEC. Edge caching reduces latency by storing content closer to the user, while MEC offloads computational tasks to the edge, enabling real-time processing and reducing the load on user devices[5].

QoE-centric approach is proposed that goes beyond traditional network performance metrics. They argue that a user's perception of video quality is influenced by factors such as rebuffering events, startup latency, and bitrate fluctuations. The paper presents a framework that considers these factors in the design of caching and computing strategies, aiming to maximize the overall user satisfaction.

An optimization framework is introduced that addresses the complex interplay between caching, computing, and bitrate adaptation. The authors formulate this as an Integer Nonlinear Programming (INLP) problem, which is known to be NP-hard. The complexity arises from the need to coordinate caching and computing decisions across multiple edge nodes while considering the variability in user requests and content popularity.

The authors tackle the caching placement problem by leveraging long-term user request statistics. They reformulate the caching problem as a Multiple-Choice Knapsack Problem (MCKP) and solve it using the Lagrange dual method. This approach allows for the efficient allocation of caching resources, ensuring that popular content is readily available at the edge.

For the joint computing and bitrate adaptation problem, the authors propose a transformation into a Markov Decision Process (MDP). They employ the Deep Deterministic Policy Gradient (DDPG) algorithm, a policy-based reinforcement learning method, to dynamically adjust the bitrate and compute resources. This approach enables the system to adapt to the changing network conditions and user preferences in real-time.

The paper presents extensive simulation results that demonstrate the effectiveness of the proposed framework. The authors compare their approach with existing schemes and show significant improvements in key performance metrics such as video quality, rebuffering rate, and user satisfaction. The results validate the superiority of the proposed QoE-aware collaborative edge caching and computing framework in enhancing the adaptive video streaming experience.

In conclusion, the paper investigated a collaborative caching and computing scheme to improve the QoE for MEC-assisted adaptive video streaming system. The proposed framework, which integrates edge caching and MEC in a QoE-aware manner, offers a promising solution to the challenges of network congestion and degraded user experience. The paper addressed the pressing need to enhance the Quality of Experience (QoE) in mobile edge computing (MEC)-assisted adaptive video streaming. Their work elegantly tackles the complexity of network congestion and variable user demands through a meticulously designed collaborative edge caching and computing scheme. Specifically, the paper introduces an optimization framework that prioritizes QoE, a significant departure from traditional network-centric approaches. By framing the caching and computing strategy as an Integer Nonlinear Programming problem, the authors have highlighted the computational challenges inherent in optimizing adaptive streaming, setting the stage for advanced solution techniques. The proposed solution adeptly navigates the computational complexity by decomposing the problem into caching placement and joint computing and bitrate adaptation, demonstrating a novel approach to tackling NP-hard problems in the field. Caching Placement Strategy: Leveraging user request statistics to inform caching decisions represents a data-driven optimization strategy that is both practical and efficient, aligning with the trend towards analytics in network management. The transformation of the bitrate adaptation problem into a Markov Decision Process and its solution using the DDPG algorithm showcases the potential of reinforcement learning in dynamic network environments.

References:

[1] T. Zhao, Q. Liu, and C. W. Chen, “QoE in Video Transmission: A User Experience-Driven Strategy,” IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 285–302, 2017.

[2] J. Kua, G. Armitage, and P. Branch, “A Survey of Rate Adaptation Techniques for Dynamic Adaptive Streaming Over HTTP,” *IEEE Communications Surveys & Tutorials*, vol. 19, no. 3, pp. 1842–1866, 2017.

[3] A. Bentaleb, B. Taani, A. C. Begen, C. Timmerer, and R. Zimmermann, “A Survey on Bitrate Adaptation Schemes for Streaming Media Over HTTP,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 562–585, 2019.

[4] J. Tian, H. Zhang, D. Wu, and D. Yuan, “Interference-Aware Cross-Layer Design for Distributed Video Transmission in Wireless Networks,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 26, no. 5, pp. 978–991, May 2016.

[5] G. S. Paschos, G. Iosifidis, M. Tao, D. Towsley, and G. Caire, “The Role of Caching in Future Communication Systems and Networks,” *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 6, pp. 1111–1125, Jun. 2018.

Qichao Xu received Ph.D. degree from the school of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China, in 2019. He is currently an associate professor with Shanghai university, Shanghai. He has published more than 90 papers in some respected journals, such as IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, and IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY. His research interests are in trust and security, the general area of wireless network architecture, internet of things, vehicular networks, and resource allocation. He was receipt of the best paper awards from several international conferences including IEEE IWCMC2022, IEEE MSN2020, EAI MONAMI2020, IEEE Comsoc GCCTC2018, IEEE CyberSciTech 2017, and WiCon2016.

MMTC Communications – Review Editorial Board

Multimedia Communications Technical Committee Officers

MMTC examines systems, applications, services and techniques in which two or more media are used in the same session. These media include, but are not restricted to, voice, video, image, music, data, and executable code. The scope of the committee includes conversational, presentational, and transactional applications and the underlying networking systems to support them.