ICWMC 2022

The Eighth International Conference on Wireless and Mobile Communications

ISBN: 978-1-61208-973-7

May 22nd –26th, 2022

Venice, Italy

ICWMC 2022 Editors

Pascal Lorenz, University of Haute Alsace, France

ICWMC 2022

Forward

The Eighteenth International Conference on Wireless and Mobile Communications (ICWMC 2022) continued a series of events addressing wireless related topics concerning integration of latest technological advances to realize mobile and ubiquitous service environments for advanced applications and services in wireless networks. Mobility and wireless, special services and lessons learnt from a particular deployment complemented the traditional wireless topics.

We welcomed technical papers presenting research and practical results, position papers addressing the pros and cons of specific proposals, such as those being discussed in the standard fora or in industry consortia, survey papers addressing the key problems and solutions on any of topics, short papers on work in progress, workshops and panel proposals.

We take here the opportunity to warmly thank all the members of the ICWMC 2022 technical program committee, as well as all the reviewers. The creation of such a high-quality conference program would not have been possible without their involvement. We also kindly thank all the authors who dedicated much of their time and effort to contribute to ICWMC 2022. We truly believe that, thanks to all these efforts, the final conference program consisted of top-quality contributions. We also thank the members of the ICWMC 2022 organizing committee for their help in handling the logistics of this event.

ICWMC 2022 Chairs

ICWMC 2022 Steering Committee

Dragana Krstic, University of Niš, Serbia
Rajat Kumar Kochhar, Ericsson, Sweden
Magnus Jonsson, Halmstad University, Sweden

ICWMC 2022 Publicity Chairs

Mar Parra, Universitat Politècnica de València (UPV), Spain
Hannah Russell, Universitat Politècnica de València (UPV), Spain

ICWMC 2022
Committee

ICWMC 2022 Steering Committee

Dragana Krstic, University of Niš, Serbia
Rajat Kumar Kochhar, Ericsson, Sweden
Magnus Jonsson, Halmstad University, Sweden

ICWMC 2022 Publicity Chairs

Mar Parra, Universitat Politècnica de València (UPV), Spain
Hannah Russell, Universitat Politècnica de València (UPV), Spain

ICWMC 2022 Technical Program Committee

Mohamed Abid, University of Gabes, Tunisia
Afrand Agah, West Chester University of Pennsylvania, USA
Iness Ahriz, CNAM, France
Khalil Aissaoui, Tunisia Polytechnic School (TPS), Tunisia
Wafa Akkari, University of Manouba, Tunisia
Ali Kadhum M. Al-Quraby, University of Babylon, Iraq
Diego Alberto Godoy, Universidad Gastón Dachary, Argentina
Adel Aldalbahi, King Faisal University, Saudi Arabia
Stefan Alfredsson, Karlstad University, Germany
Rashid Ali, Sejong University, Seoul, Republic of Korea
Adda Ali-Pacha, University of Sciences and Technology of Oran, Algeria
Karine Amis, IMT Atlantique, France
Tran Hai Anh, Hanoi University of Science and Technology (HUST), Vietnam
Antonio Arena, University of Pisa, Italy
Kamran Arshad, Ajman University, UAE
Radu Arsinte, Technical University of Cluj-Napoca, Romania
Nebojša Bačanin-Džakula, Singidunum University, Serbia
Salih Safa Bacanli, University of Central Florida, USA
Nedia Badri, ENSI - University of Manouba, Tunisia
Corey E. Baker, University of Kentucky, USA
Chaity Banerjee, University of Central Florida, USA
Kamel Barkaoui, Cedric | Cnam, France
Paolo Barsocchi, ISTI (Institute of Information Science and Technologies) | Italian National Research Council (C.N.R.), Pisa, Italy
Hadda Ben Elhadj, SM@RTS | Higher Institute of Informatics | Monastir University, Tunisia
Sonia Ben Rejeb, Higher Institute of Computer Science (ISI) - Higher School of Communications of Tunis (SUPCOM), Tunisia
Djamila Bendouda, Ecole Nationale Supérieur de Technologie, Algeria
Driss Benhaddou, University of Houston, USA
Djedjiga Benzid, École de Technologie Supérieure - Université du Québec, Canada
Vincent Beroulle, Grenoble INP, France

Copyright Information

For your reference, this is the text governing the copyright release for material published by IARIA.

The copyright release is a transfer of publication rights, which allows IARIA and its partners to drive the dissemination of the published material. This allows IARIA to give articles increased visibility via distribution, inclusion in libraries, and arrangements for submission to indexes.

I, the undersigned, declare that the article is original, and that I represent the authors of this article in the copyright release matters. If this work has been done as work-for-hire, I have obtained all necessary clearances to execute a copyright release. I hereby irrevocably transfer exclusive copyright for this material to IARIA. I give IARIA permission or reproduce the work in any media format such as, but not limited to, print, digital, or electronic. I give IARIA permission to distribute the materials without restriction to any institutions or individuals. I give IARIA permission to submit the work for inclusion in article repositories as IARIA sees fit.

I, the undersigned, declare that to the best of my knowledge, the article is does not contain libelous or otherwise unlawful contents or invading the right of privacy or infringing on a proprietary right.

Following the copyright release, any circulated version of the article must bear the copyright notice and any header and footer information that IARIA applies to the published article.

IARIA grants royalty-free permission to the authors to disseminate the work, under the above provisions, for any academic, commercial, or industrial use. IARIA grants royalty-free permission to any individuals or institutions to make the article available electronically, online, or in print.

IARIA acknowledges that rights to any algorithm, process, procedure, apparatus, or articles of manufacture remain with the authors and their employers.

I, the undersigned, understand that IARIA will not be liable, in contract, tort (including, without limitation, negligence), pre-contract or other representations (other than fraudulent misrepresentations) or otherwise in connection with the publication of my work.

Exception to the above is made for work-for-hire performed while employed by the government. In that case, copyright to the material remains with the said government. The rightful owners (authors and government entity) grant unlimited and unrestricted permission to IARIA, IARIA's contractors, and IARIA's partners to further distribute the work.

Table of Contents

Performance Analysis of MIMO using Machine Learning in 5G Networks

Christos Bouras
Computer Engineering and Informatics Department
University of Patras
Patras, Greece
e-mail: bouras@upatras.gr

Ioannis Prokopiou
Computer Engineering and Informatics Department
University of Patras
Patras, Greece
e-mail: st1059554@ceid.upatras.gr

Apostolos Gkamas
University Ecclesiastical Academy of Vella
Ioannina, Greece
e-mail: gkamas@aevellas.com

Vasileios Kokkinos
Computer Engineering and Informatics Department
University of Patras
Patras, Greece
e-mail: kokkinos@cti.gr

Abstract— **Massive Multiple-Input Multiple-output (MIMO) is a high-potential radio antenna technology for mobile wireless networks, such as 5th Generation (5G). The use of hybrid analog and digital precoding to minimize the energy consumption as well as the hardware complexity of mixed signal components is an essential strategy. Machine Learning (ML) could be able to boost 5G technologies due to the rising difficulty of configuring cellular networks. More than ever, an ML computational framework focused on successfully processing the expected huge data generated normally by 5G networks with high subscriber cell density, is required. In the Ultra-Dense Networks (UDNs) of 5G and beyond high demanding networks paired with beamforming and massive MIMO technologies, ML struggles to define network traffic aspects distinctively, especially when they are projected to be much more dynamic and complicated. This paper presents a state-of-the-art analysis of the combined and multiple uses of ML along with MIMO technology in 5G Networks.**

Keywords-MIMO; Machine Learning; 5G; Deep Learning; Internet of Things; Big Data.

I. INTRODUCTION

In recent decades, a rise in Internet traffic has been observed, which is projected to continue to grow exponentially in the near future. The reason for this is the widespread use of a wide range of User Equipment (UE), which includes everything from Internet of Vehicles (IoV) and Machine-to-Machine Communication (M2M) to Internet of Things (IoT), and so on. Network traffic management is expected to be a critical problem, especially in the 5th Generation (5G) and beyond cellular Ultra-Dense Networks (UDNs) and Heterogeneous Networks (HetNets), which are the main technologies that will host this traffic, reason being the significant congestion on wireless communication networks due to the amount of traffic generated from big data. The primary problem with the wireless network's ongoing growth is that to achieve the necessary area throughput, it must either increase bandwidth (spectrum) or densify the cells and increasing bandwidth or densifying the cells raises hardware costs and increases latency.

Because of its unique performance and freedom, Massive Multiple-Input Multiple-Output (MIMO) is a critical method for 5th Generation and future mobile wireless networks. Massive MIMO is a type of MIMO that requires connecting a base station with hundreds or even thousands of antennas to be able to boost spectral efficiency and throughput. Massive MIMO makes use of huge antenna arrays at base stations and Access Points (APs). When combined with millimeter-wave (mm-Wave) communications, which employ a bigger spectrum, this architecture enables for enhanced cellular communications with increased spectral density and reduced complexity. Massive MIMO can perceive data from several sensors in real time thanks to its high multiplexing gain and beamforming capabilities, resulting in decreased latency and larger data rates for sensors.

Artificial Intelligence (AI) has emerged as a cutting-edge method with the potential to make major advancements in a variety of telecommunications problems, thanks to the uses of Machine Learning (ML) and furthermore deep Learning, including network management, self-organization, self-healing, and Physical Layer (PHY) improvements (DL). The communication system will be taught how to recognize emergent channel models and how to react to changing channel conditions by utilizing deep learning techniques, all while delivering a cutting-edge tool for maximizing end-to-end efficiency. DL-based approaches are also perfect for operating on Graphics Processing Units (GPUs) to fully use parallel hardware because of the Deep Neural Network (DNN) framework with ways that can help manage big data and fast evolving scenes based on parallel processing architectures. The secure uses of AI can greatly optimize classical ways in most of the areas. To improve its performance, many machine learning methods have been applied to MIMO technology.

In [2], a methodology is presented for producing channel realizations that depict 5G scenarios with transceiver and artifact mobility. In [3], researchers investigate MT localization in Distributed Massive MIMO (DM-MIMO) systems using the Apache Spark big data computing

 ISBN: 978-1-61208-973-7

framework and the RSS fingerprinting approach in conjunction with ML algorithms, with the goal of using it in microcells in metropolitan areas. The work in [1] explains how to utilize deep Long Short-Term Memory (LSTM) learning to produce localized traffic load estimates at the UDN base station, while [4] shows a Partial Learning (PL)-based detection technique and [5] gives a comprehensive review of 5G communications research utilizing DL. In [6], the authors undertake a review of the evolution of DL solutions for 5G communication before providing efficient strategies for DL-based 5G scenarios, whilst in [7], they provide a complete overview of the primary enabling technologies 5G and 6G networks, with a focus on massive MIMO systems. For successful hybrid precoding, [8] proposes a deep-learning-enabled mmWave massive MIMO architecture, in which each precoder selection for getting the best decoder is considered as a DNN mapping link. We will include a study of how MIMO technology can benefit from the modern application of ML in this paper.

We will present how the components of a single 5G network that uses this combination work, what has been researched so far, and how it might be enhanced in the future. The rest of this work is organized as follows: In the following section, we showcase the literature review of the most state-of-the-art combinations of MIMO and ML. In Section III, we evaluate the use of ML and MIMO in 5G networks and Section IV includes our conclusions and future applications.

II. Related Work

A. MIMO

We can think of communicating in a MIMO system as sending a matrix rather than a single vector. As a result, we can deliver a data stream in parallel to numerous recipients. The data to be delivered is encoded by the system, and the stream is sent via transmitters. MIMO is using multiple antennas to send data to a large number of wireless endpoints simultaneously. MIMO is a technique for doubling the capacity of a radio link by taking advantage of multipath propagation by using multiple transmission and receiving antennas. MIMO, being a radio antenna technology, uses many antennas at the transmitter and receiver to offer several signal channels for data transmission, effectively. Each antenna is associated with a distinct signal path, allowing for the usage of several signal paths. Massive MIMO is a new technology that scales up MIMO and provides significant energy economy, spectrum efficiency, resilience, and dependability benefits.

To highlight the importance of massive MIMO, we look at the work that has been done in [9]-[11]. In [10], Massive MIMO as an enabling technology for future generation of networks, is being showcased as a novel technology that scales up MIMO and offers considerable benefits. It enables both the base station and the mobile unit to use low-cost hardware. Expensive and powerful but inefficient equipment is replaced at the base station with many low-cost, low-power components that work together. The term "massive" refers to the utilization of the multiple antenna arrays to support a plethora of terminals at the same time-frequency resource. Comprehensively describing massive MIMO systems from several different perspectives in [11], the authors point out that, by expanding the capacity of Radio Frequency (RF) networks, MIMO provides a more reliable connection and reduces congestion. A base station's spectrum and energy efficiency can be considerably optimized by providing it with hundreds or even thousands antennas.

MIMO can enhance data carrying capacity without requiring more bandwidth due to spatial multiplexing, however, when compared to the classic single antenna antenna-based system, the resource requirements and hardware complexity are higher. Investigating the performance constraints of developing "wireless-powered" communication networks using opportunistic energy harvesting from ambient radio signals or specialized wireless power transfer, the authors conclude at [9] that when developing MIMO systems, compromises must be made in order to make simultaneous information and energy transmission as efficient as possible. When allocating resources in terms of communication to provide optimal solutions for network interference levels for maximum information vs. energy transfer, there are a few nontrivial considerations to keep in mind.

B. Machine and Deep Learning

Machine learning is a subfield of AI that refers to when computers are using data for learning techniques. It's the intersection of computer science and statistics when algorithms are used to carry out a procedure without being specifically written. The learning process for these algorithms falls into two categories based on the variety of data hat are given as an input: supervised or unsupervised. DL algorithms are a mathematically more complex and advanced evolution of machine learning techniques. DL is a subset of machine learning that deals with algorithms that analyze data in a way similar to the human brain.

The work that has been done in [3], [4] and [8] best describes the role of ML and DL in enhancing MIMO. The Partial Learning (PL)-based detection scheme that is proposed in [4] can achieve low Bit Error Rate (BER) with low computational complexity. They use non-linear techniques to have a more efficient BER while relying on linear methods to reduce computing complexity, which can be even more optimized by using neural network for linear detection. Because neural networks ensure that the signals are appropriately recognized at the start, this technique can achieve lower BER than standard techniques. The results of the evaluation of thirteen machine learning methods that is performed comparatively, in conjunction with fingerprint-based MT localization for dispersed Massive MIMO topologies [3], reveals that a subset of the assessed ML systems may accurately anticipate the position of an MT. Finally, the K-Nearest Neighbor (KNN) has been proven to appear the best ML algorithm performance, second being the

 ISBN: 978-1-61208-973-7

Kernel Ridge Regression (KRR) and Random Forest (RF) in all scenarios evaluated.

The deep-learning-enabled mmWave massive MIMO framework proposed in [8] presents a solution to the difficulty that already implemented hybrid precoding schemes have, which is that they are computationally complex and do not fully leverage geographical information. This method achieves successful hybrid precoding by treating each precoder choice as a associating relation in the DNN in order to achieve the best decoder, which is chosen by DNN training for optimization of the mmWave massive MIMO precoding process. The system model is a typical mmWave massive MIMO system with one BS and a modern DNN utilized to create a unique precoding framework. The suggested approach which has DL in it's core is viewed as a operation that is performing the mapping, and a training mechanism to acquire the mmWave-based model's structural statistics. With the data fed dynamically changing in accordance with the channel circumstances, the DNN is trained. The computational complexity of this unsupervised learning training strategy is reduced as well.

C. 5G Networks

After 1G, 2G, 3G, and 4G networks, 5G is a new global standard that is taking over wireless communications. 5G is intended to provide data speeds many times faster than the previous classic networks, latency that is being characterized as "ultra-low", enhanced dependability, massive network capacity, increased availability, larger bandwidth of up to 10 gigabits per second (Gbit/s) ensuring a more consistent user experience for a larger number of people. AI along with the infrastructure of Internet of Things (IoT) enable higher performance and efficiency. In 2019, cellular phone companies began installing 5G networks around the world, which are the projected successors to the 4G networks that connect the majority of today's handsets. In 5G, the service area is separated into cells, which are small geographical areas. All 5G wireless devices are connected to the Internet and to the telephone network via radio waves via a local antenna in the cell. Massive New antennas will be employed by MIMO for the several transmitters and receivers to be able to transfer a larger amount of data at the same time.

Observing [1], [2], [7] and [11], the authors take a close look at the fundamental technologies that will be critical for 5G and beyond networks, with a particular focus on massive MIMO systems. They discuss some of the many and most important challenges in a massive MIMO system, such as pilot contamination, channel estimation, precoding, user scheduling, energy efficiency, and signal identification, as well as some cutting-edge mitigation measures, as seen in [7]. For massive MIMO systems, they discuss contemporary advances, such as terahertz communication, Ultra-Massive MIMO (UM-MIMO), Visible Light Communication (VLC), ML, and DL. They believe that MIMO is the solution to the massive increase in wireless data traffic because to achieve excellent spectrum and energy efficiency with very simple processing, antennas are used in combination at both the transmitter and the receiver ends. In [11], the authors conclude that DL models, such as DNN and Convolutional Neural Networks (CNN), while optimizing channel estimations and feedback for large MIMO, will dramatically improve BER performance and system capacity. Massive MIMO and Non-Orthogonal Multiple Access (NOMA) will give improved performance and lower internal power usage, resulting in overall energy efficiency gains.

[1] describes the way to employ the deep LSTM learning method to produce traffic load based on location estimates at the base station of UDN, emphasizing how important it is for the 5G network operators to perform control on all the resources of the radio in an efficient manner. According to this study, traditional traffic control strategies are "reactive," meaning that if alike traffic circumstances arise, they are prone to congestion again. Predicting congestion incidents seeks to prevent them from happening in the first place. The study in [2] describes a system with a car traffic simulator along a raytracing simulator, in combination, to create channel realizations that reflect 5G scenarios and allow for the use of sophisticated traffic simulator features with mobility of transceivers as well as objects. The research then goes on to offer a dataset that may be used to investigate beam selection approaches for vehicle-to-infrastructure communication utilizing millimeter waves in mmWave MIMO.

III. MACHINE AND DEEP LEARNING ALGORITHMS COMPARISON

ML and DL methods' dynamic nature may be advantageous for analysis of complex tasks while also conserving a substantial amount of processing power. Massive MIMO beamforming, channel estimation, signal detection, load balancing, and spectrum optimization can all benefit from ML and DL technology, according to [7]. During channel estimation, data coming from the channel can be assumed to be big, and a variety of ML methods can be used to predict massive MIMO channels. Massive MIMO will see a significant increase in throughput thanks to ML-based channel prediction. In massive MIMO, ML was utilized in the past for effective beam alignment to track users, and numerous machine learning and DL approaches are also useful for uplink signal detection in massive MIMO. Despite its benefits, massive MIMO has many challenges, including pilot contamination, channel estimation, precoding, user scheduling, hardware impairments, energy efficiency, and signal detection, all of which need understanding and need to be applied in a real-world setting before their promised benefits can be realized.

The work in [8] indicates that using DL to solve the channel feedback problem could be a promising path for addressing concerns like codebook size and feedback overhead. The work in [6] states that improvement can be found if the data set acquisition and selection of the model issues are overcome, while the explainable development of DL methods is progressing, and we will have to establish the standard data sets that individuals in the industry support. The work in [1] discovers opportunities for improvement by taking a large number of traffic parameters and tensor-modeling them in order to create a learning framework that is

 ISBN: 978-1-61208-973-7

even more robust and that can adapt and forecast with even more precision. The two challenges encountered in [3] are the effect of different locations and terrain on accuracy in terms of localization and the quantity of training datasets, as well as the effect of employing other DM-MIMO antenna array shapes and their effect on MT localization. Future work from [2] will entail simulating many sites and scenarios, as well as testing some of them with measurements, because it is crucial to decrease the computing cost in addition to precise modeling. DL in 5G can be examined utilizing a systematic and repeatable technique via experimentation.

All in all, finding effective techniques to decrease the pilot contamination effect is a crucial subject to research. A scheduling method that guarantees more efficiency and fairness that can deliver a higher rate of data while also ensuring fairness among users, to increase overall system performance is also an important topic of research, as is finding effective precoding techniques for massive MIMO. Finding a more effective and low-complexity uplink signal identification method is one of the most important topics of research. Designing a Massive MIMO that is able to work with today's 4G network is a fascinating topic to research (Figure 1). The following two algorithms show especially favorable results. [6] illustrates how DL models, like DNN and CNN for massive MIMO, may dramatically optimize the performance of BER and the capacity of the system while channel estimation and feedback are optimized. [4] proposes a neural network-based intelligent detection method to strike a balance between cheap computing complexity and low BER.

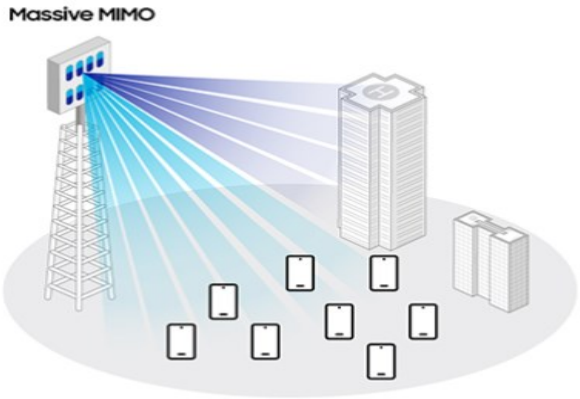

Figure 1. Massive MIMO

IV. Performance Evaluation

In this section, we discuss the performance evaluation of the works done in [1], [6] and [8]. We are observing interesting results in the use of ML and especially DL in combination with MIMO in 5G and beyond networks.

In general, in [6], a DL-based communication framework's performance has been demonstrated for channel estimation, encoding and decoding in massive MIMO, even though no theoretical work has been derived in this work to further verify and improve the framework's performance through understanding. Specifically, three deep learning-based frameworks, NOMA, massive MIMO, and mmWave hybrid precoding, are introduced and their performance evaluated with an emphasis on 5G. These models use extremely large parameters, a high level of memory and have increased time complexity. This suggests that we can create high-performance deep compression techniques and model compression strategies to increase the efficiency of the networks that utilize deep learning, making them simpler as well. As a result, in the future, the deep reinforcement learning-based wireless physical layer should be thoroughly researched in order to optimize critical resource management tasks and be capable of improving precoding performance, BER, SNR, and data rates by enhancing equipment performance, such as CSI, latency, and bandwidth management. Because the original input signals are frequently transformed into binary signals, one-hot vectors, modulated integers, and other styles of data representation for improving network performance in the DL area, it is unclear whether the most modern methods' performance is able to be achieved in DL-based wireless communication frameworks while the representation data is varying. In the field of DL-based wireless physical layer, the principles of learning schemes are still unclear, and a mechanism for picking training instances has not been created, which is one of the challenges that must be investigated further.

The authors in [8] compare the DNN-based scheme's BER performance to that of the SVD-based hybrid precoding scheme, fully digital SVD-based precoding method, fully GMD-based precoding method, and new GMD-based precoding scheme, demonstrating that the techniques with deep-learning at their core are more efficient than the traditional methods. In terms of BER, it is noticed that the deep-learning-based strategy's performance diminishes as batch size increases. In the DNN-based method, the performance of hybrid precoding is improved by using a lower rate of learning to guarantee a smaller validation error. The suggested hybrid precoding strategy surpasses prior strategies by achieving improved hybrid precoding performance thanks to DL's superior mapping and learning capabilities. The Mean Square Error (MSE) performance improves as the number of iterations increases, which is due to the fact that all of these algorithms approach conversion with more iterations. As a result, when compared to existing systems, the proposed DL-based methodology achieves improved performance in terms of hybrid precoding accuracy and conversion.

By comparing the work in [1] to the conventional method, the technique showcased in [1] achieves a lower rate of packet loss than the conventional method. The resource allocation approach that is given clearly leads to increased throughput. This result demonstrates that, even with a huge number of UEs, the proposed strategy outperforms the standard way. The solution that is stated results in a much

 ISBN: 978-1-61208-973-7

lower packet loss rate, because it may make a localized prediction of future crowding and attempt to alleviate or completely eschew it ahead of time. Unlike the traditional methodology, the proposed method may employ DL to generate a localized forecast of future bottleneck, which would then be utilized to adjust the UL/DL settings to reduce congestion. When compared to the old technique, the UDN that utilizes the proposed method can achieve significantly higher throughput and lower rates of packet loss. Furthermore, in comparison to the traditional method, the proposal results in a higher throughput while, in terms of network efficiency, surpasses traditional solutions.

To sum up, from DL-based communication frameworks to DL predictions, the DL is clearly the state-of-the-art technique that seems to have overtaken the way MIMO in 5G and beyond networks work.

V. CONCLUSIONS

All in all, we conclude that the use of ML and DL in combination with MIMO in 5G and beyond networks (Figure 2) has a lot of benefits and better performance in the variety of the aspects that are being showcased. Especially, the most promising state-of-the-art techniques consist of the various uses of DL. It is obvious that such techniques, as well as all the principles of learning schemes, still have some unclear areas that can be further explored. In the future, more analysis needs to be conducted on DL-based wireless physical layer mechanisms, congestion optimization techniques and precoding strategies, expanding the comparison presented in Table I. It is safe to assume that with exploration and exploitation of the aforementioned artificial intelligence combinations, various benefits can be derived in terms of BER, energy consumption, complexity, throughput, congestion and, in general, overall efficiency.

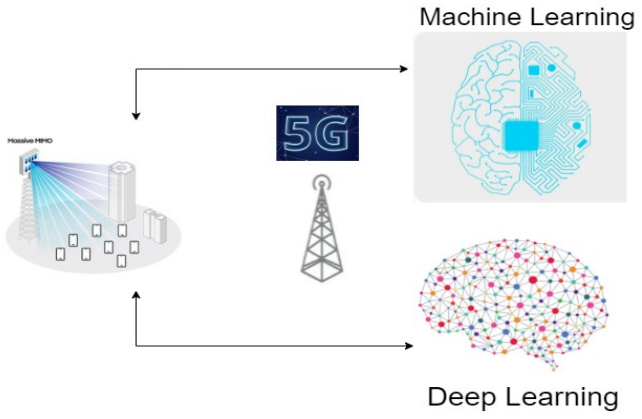

Figure 2. Machine/Deep Learning – 5G - MIMO

TABLE I. COMPARISON OF DL-BASED MECHANISMS, CONGESTION OPTIMIZATION TECHNIQUES AND PRECODING STRATEGIES

Work	***Strategy***	***Results***
[2]	In mmWave MIMO, a dataset is used to examine beam selection algorithms for vehicle-to-infrastructure interaction	Channel realizations that simulate 5G scenarios with transceivers and objects moving about.
[10]	Energy and spectrum efficiency, robustness, and reliability analyses	Massive MIMO description
[7]	Overview of core issues in massive MIMO system	MIMO as the solution to the massive increase in wireless data traffic
[8]	Deep-learning-enabled mmWave massive MIMO framework	Successful hybrid precoding
[6]	Overcoming the dataset acquisition and model selection issues	Better results with the progressing use of DL
[1]	Deep LSTM learning technique for localized traffic load predictions at the UDN base station	Learn and forecast with even greater precision
[4]	Partial Learning (PL)-based detection scheme	Low BER with low computational complexity
[3]	Comparative performance evaluation	KNN was the best ML algorithm performance that could effectively forecast the position of an MT.
[11]	Comprehensively describing massive MIMO systems from several different perspectives	Better BER performance and system capacity while optimizing channel estimates and feedback for massive MIMO and overall energy efficiency gains on NOMA
[5]	Overview of 5G communications research using DL	DNN and CNN can increase BER performance and system capacity while optimizing channel estimates and feedback for massive MIMO
[9]	Investigating the performance constraints of developing "wireless-powered" communication networks using opportunistic energy harvesting from ambient radio signals or specialized wireless power transfer	To maximize the efficiency of simultaneous information and energy transmission, fundamental compromises must be made when developing wireless MIMO systems.

 ISBN: 978-1-61208-973-7

REFERENCES

[1] Y. Zhou, Z. M. Fadlullah, B. Mao, and N. Kato, "A Deep-Learning-Based Radio Resource Assignment Technique for 5G Ultra Dense Networks," in IEEE Network, vol. 32, no. 6, pp. 28-34, November/December 2018J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] A. Klautau, P. Batista, N. González-Prelcic, Y. Wang, and R. W. Heath, "5G MIMO Data for Machine Learning: Application to Beam-Selection Using MACHINE," 2018 Information Theory and Applications Workshop (ITA), 2018, pp. 1-9.

[3] W. Y. Al-Rashdan and A. Tahat, "A Comparative Performance Evaluation of Machine Learning Algorithms for Fingerprinting Based Localization in DM-MIMO Wireless Systems Relying on Big Data Techniques," in IEEE Access, vol. 8, pp. 109522-109534, 2020.

[4] Z. Jia, W. Cheng, and H. Zhang, "A Partial Learning-Based Detection Scheme for Massive MIMO," in IEEE Wireless Communications Letters, vol. 8, no. 4, pp. 1137-1140, Aug. 2019.

[5] A. Ly and Y. -D. Yao, "A Review of Deep Learning in 5G Research: Channel Coding, Massive MIMO, Multiple Access, Resource Allocation, and Network Security," in IEEE Open Journal of the Communications Society, vol. 2, pp. 396-408, 2021.

[6] H. Huang et al., "Deep Learning for Physical-Layer 5G Wireless Techniques: Opportunities, Challenges and Solutions," in IEEE Wireless Communications, vol. 27, no. 1, pp. 214-222, February 2020.

[7] R. Chataut and R. Akl, "Massive MIMO Systems for 5G and Beyond Networks—Overview, Recent Trends, Challenges, and Future Research Direction. Sensors." 20. 2753. 10.3390/s20102753, 2020.

[8] H. Huang, Y. Song, J. Yang, G. Gui, and F. Adachi, "Deep-Learning-Based Millimeter-Wave Massive MIMO for Hybrid Precoding," in IEEE Transactions on Vehicular Technology, vol. 68, no. 3, pp. 3027-3032, March 2019.

[9] R. Zhang and C. K. Ho, "MIMO Broadcasting for Simultaneous Wireless Information and Power Transfer," in IEEE Transactions on Wireless Communications, vol. 12, no. 5, pp. 1989-2001, May 2013.

[10] E. G. Larsson, O. Edfors, F. Tufvesson, and T. L. Marzetta, "Massive MIMO for next generation wireless systems," in IEEE Communications Magazine, vol. 52, no. 2, pp. 186-195, 2014.

[11] L. Lu, G. Y. Li, A. L. Swindlehurst, A. Ashikhmin, and R. Zhang, "An Overview of Massive MIMO: Benefits and Challenges. in IEEE Journal of Selected Topics in Signal Processing", vol. 8, no. 5, pp. 742-758, 2014.

 ISBN: 978-1-61208-973-7

Considerations When Designing Sponge-based Extendable-Output Functions for Lightweight and Mobile Devices

Meaad Tori, David Paul, William Billlingsley
School of Science & Technology
University of New England
Armidale, Australia
email: mtori@myune.edu.au, David.Paul@une.edu.au, wbilling@une.edu.au

***Abstract*—Through the study of existing lightweight cryptographic algorithms, we suggest a number of design guidelines for creating new sponge-based extendable-output functions for use in resource-constrained environments. While several such algorithms exist, some knowledge that can be generalized from studying them in aggregate has not previously been presented. The developed guidelines include consideration of the round function width, the number of rounds, the selection of round constants, the rate, the linear and non-linear layers, and the required security claim. The result of these guidelines is a set of recommendations for the design of sponge-based extendable-output functions that should allow correctly balanced security and performance in environments where compute power, available memory, and battery life may all be limited. These recommendations could be used to help design purpose-built implementations for various wireless or mobile systems.**

Keywords-lightweight cryptography; extendable-output function; security analysis; Internet of Things.

I. INTRODUCTION

The Internet of Things (IoT), sensor networks, Radio Frequency Identifiers (RFID) and smart devices are connecting the world in ways not previously imagined [1]. However, many of these devices are resource-limited, having low computational power, small amounts of memory and limited power supply, often relying on batteries. Because of this limitation, traditional standardized cryptographic algorithms, such as the Advanced Encryption Standard (AES) [2] and Secure Hash Algorithms SHA-2 [3] and SHA-3 [4], which can have high computational and memory requirements, are not appropriate for use in these lightweight devices.

The combination of having these resource-constrained devices interacting directly with the real world and not being able to protect them using traditional algorithms means new approaches are needed to ensure their security and privacy [5]. Lightweight cryptography aims to develop secure cryptographic primitives that better fit the environment of resource-constrained devices [5]. The US National Institute of Standards and Technology (NIST) is currently holding a competition to standardize lightweight cryptographic algorithms because the performance of existing standards is not acceptable [6] but the competition does not cover all cryptographic primitives. In particular, the competition does not include an extendable-output function (XOF), and even a cryptographic hash function is optional.

A cryptographic hash function is an algorithm that maps a message of any length to a fixed-size message digest. It is a one-way function that is difficult and impractical to invert, and is important for many forms of authentication, including digital signatures [7]. An XOF has similar functionality to a cryptographic hash function, but its output can be extended to any desired length, rather than a single fixed size. This can prove very useful in lightweight environments, allowing system designers to choose the length of the output required for their individual circumstances to better balance security and performance [8].

While the inclusion of a cryptographic hash function is optional in the current NIST lightweight cryptography competition, 12 of the 32 second-round candidates included such an algorithm. With the exception of SATURNIN [8], each of these candidates chose to use a sponge construction (or derivative) [9], which allows for XOFs. Of the ten finalists in the NIST competition, the Ascon [10], Photon-Beetle [11], TinyJAMBU [12] and Xoodyak [13] algorithms are the only ones that include hashing, and each of these are based on a sponge construction.

In this paper, we examine three representative candidates from the second round of the NIST lightweight cryptography competition and, combined with general insight from the other candidates and related research, present a new set of design aspects that must be taken into account to design a secure lightweight sponge-based XOF. Our analysis includes two of the finalists (Ascon and Xoodyak) and one algorithm that did not make it to the final round of the NIST competition (Gimli [14]). The inclusion of Gimli in this analysis is because some of the reasons it did not make it to the final round are pertinent to this discussion. This aggregate study leads to general guidelines that could be used to develop custom-built XOFs for lightweight environments, including wireless and mobile systems.

The remainder of this paper is organized as follows. Section II recounts literature-supported background information required to understand the analysis of the existing lightweight sponge-based XOFs presented in

 ISBN: 978-1-61208-973-7

Section III. Section IV then generalizes the outcomes of the analysis to present a number of design guidelines that should be considered when creating such an XOF. Finally, Section V concludes the paper and suggests future directions for this research.

II. BACKGROUND INFORMATION

This section briefly outlines, in Section II-A, the requirements of cryptographic hash functions and, in Section II-B, why it is often useful to have a more general XOF instead of a fixed-sized hash. Section II-C then gives an overview of the general sponge construction, which is required to create sponge-based XOFs. This information will be important when we examine three sponge-based XOFs in Section III.

A. Cryptographic Hash Function

A hash function converts an arbitrarily-sized message into a message digest of some fixed length, say *d*. In order to be a cryptographic hash function, a hash function must also have the following properties [4]:

- Pre-image resistance: Given a particular message digest, it should be difficult to find a message that maps to that value.
- Second pre-image resistance: Given a particular message, it should be difficult to find a different message that has the same message digest.
- Collision resistance: It should be difficult to find any two different messages that have the same message digest.

Generic attacks on hash functions, such as brute force (which repeatedly tries different inputs until the desired message digest is found), depend only on the value of *d*, so *d* must be large enough to ensure that such an attack is computationally inefficient. In general, attacks on hash functions attempt to break (some of) the above properties of cryptographic hash functions without resorting to brute force (i.e., the attack should take fewer than 2^d steps).

B. Applications of Extandable-Output Functions

XOFs generalize hash functions by allowing an arbitrary output digest size. The computational complexity of an XOF is a combination of the computational complexity of a hash and a stream cipher [15]. Thus, the security of XOFs relies on more than just the length of the produced digest, so different security strengths can be selected. This is useful in areas where available key material might vary dramatically from one application to another, with no correlation to the required security strength [4].

For example, the ED448 digital signature standard [7] adopts the XOF SHAKE-256 [4] as its internal hash function. This significantly increases performance compared to using SHA3-512, without reducing the 256 bits of security required by the standard [7].

C. The Sponge Construction

Each of the finalists in the NIST lightweight cryptography competition that support a cryptographic hash function use a sponge construction [16], which can generally

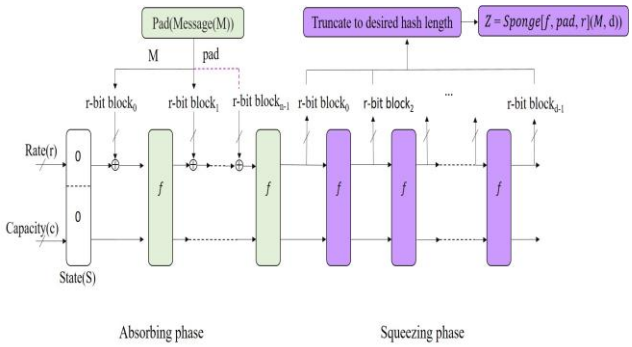

Figure 1. Hashing mode in Sponge Construction.

be extended to an XOF. A sponge function, as illustrated in Figure 1, is built from three components:

- A state memory, *S*, consisting of $r + c$ bits, where *r* is the *rate* of the sponge, and *c* its *capacity*.
- A function f: $\{0,1\}^{r+c} \rightarrow \{0,1\}^{r+c}$ that transforms the state memory. It typically consists of a non-linear, a mixing, and a linear layer.
- A padding function *Pad* that appends bits to any input string to ensure its length is a multiple of *r*.

The state is initialized to zero and then, for each *r*-bit block of the padded input string, the state is updated by replacing the first *r* bits of the state with the first *r* bits of the state bitwise XORed with the *r*-bit input block. The state is then further updated by passing it through the function f, which is often a pseudorandom permutation over all possible state values. This "absorbs" all blocks of the padded input into the sponge construction's state.

The output of the sponge construction is then "squeezed out" by initially outputting the first *r*-bits of the state and then, repeatedly until enough output is generated, replacing the state *S* by $f(S)$ and outputting the first *r* bits of the result (truncating if necessary).

Assuming f is suitably difficult to invert, the following security results can be derived for a sponge construction that creates a message digest of length *d* [17] [18] [36]:

If $d \geq c$ and $c > 2r$ then:

- The construction has pre-image security of 2^{d-r}.
- The construction has second pre-image and collision security of $2^{c/2}$.
- The best pre-image attack would require a complexity of $2^{d-r} + 2^{c/2}$.

Otherwise:

- The construction has second pre-image security of 2^d.
- The construction has collision security of $2^{c/2}$.
- The best pre-image attack would require a complexity of $\{\min 2^d, \{\max 2^{d-r}, 2^{c/2}\}\}$.

The security claims of a sponge construction are typically flattened to rely purely on the capacity *c*, allowing the required security to be defined independently of the length of the output *d* [16]. Further, the sponge construction is often used with duplexing to allow the absorb and squeeze operations to alternate [19].

TABLE I. COMPARSION OF ASCON, GIMLI AND XOODYAK XOFS

Algorithm	Number of Rounds	State Size (bits)	Rate (bits)	Capacity (bits)
Ascon	12	320	64	256
Gimli	24	384	128	256
Xoodyak	12	384	130	254

III. EXISTING SPONGE-BASED XOFS

This section examines Ascon-XOF (in Section III-A), Gimli-XOF (in Section III-B) and Xoodyak-XOF (in Section III-C) in order to understand and generalize design decisions for creating sponge-based XOFs. A comparison of the three algorithms is presented in Table I. Lessons learned from these algorithms will be presented as a set of design considerations in Section IV.

A. Ascon-XOF

Ascon-XOF [10] uses a 12-round permutation based on a sponge construction with a state size of 320 bits, consisting of five 64-bit words. It uses a 64-bit rate and 256-bit capacity. The substitution layer is identical to the Keccak χ mapping [20] and an adaptation of the $\sum$ function of SHA-2 [21] is used to provide diffusion.

Ascon-XOF has received significant third-party analysis (e.g., [22]). A summary is provided in Table II. The pre-image attacks target the low algebraic degree of the reduced round version of Ascon-XOF; the search for pre-images can be speed up for low degree functions. Ascon-XOF has fast diffusion because it applies its linear layer to every five words. It also has a strong word structure with a good choice of round constants, which makes it challenging to apply a cube attack [23] effectively. However, since each output bit depends on only three input bits, of which two are non-linear, consecutive dependent bits can lead to the derivation of linear equations that can be solved to break the system. Even the original Ascon specification [10] admits that the Ascon permutation is not ideal in terms of differential and linear properties [22] [24]. However, it has been shown that Ascon-XOF has a good security margin against collision attacks [22]. Currently, even with the use of all 320 bits of the state in a semi-free-start collision, only four out of Ascon-XOF's twelve rounds can effectively be broken.

B. Gimli-XOF

Gimli-XOF [14] uses a 24 round permutation based on sponge construction with a state size of 384 bits, represented as a 3×4 matrix of 32-bit words. It uses a 128-bit rate and 256-bit capacity. The non-linear layer operates on the column level. The linear layer operates on the row level and applies one of two swap operations, a small swap, or a big swap.

Gimli has a slow diffusion compared to Ascon because its small and big swap operations only apply to the first row, and not in every round. This makes it easier to analyze multiple rounds of Gimli-XOF. Table III demonstrates Gimli's lower diffusion compared to Ascon.

TABLE II. SUMMARY OF ATTACKS ON ASCON-XOF

Attack	Method	Round	Time Complexity	Ref
Pre-image	cube	2	2^{39}	[22]
Pre-image	Algebraic	6	$2^{63.3}$	[22]
SFS collision	Differential	4	Practical	[22]
Collision	Differential	2	Practical-2^{15}	[25]

TABLE III. UPPER BOUND FOR THE ALGEBRAIC DEGREE OF DIFFUSION AFTER DIFFERENT NUMBERS OF ROUNDS FOR ASCON AND GIMLI

Round	1	2	3	4	5	6	7	8	9
Ascon	2	4	8	16	32	64	128	256	298
Gimli	2	4	8	16	29	52	95	163	266

A divide-and-conquer technique, which applies an exhaustive search to a divided message space, allows theoretical pre-image attacks on up to five of the nine rounds of Gimli-XOF [26]. By exploiting Gimli's weak diffusion, equations that represent the bit dependencies in Gimli-XOF's rate can be constructed and solved. This did require fixing the block size to 128 bits, and ignoring the padding rule, but does give a practical attack on a reduced-round version of Gimli-XOF.

The slow diffusion of Gimli's state means that the swap operations only affect 256 of the 384 bits of Gimli's state, and this does not even occur each round. This can be exploited to construct equations that can be practically solved with a SAT solver [27].

C. Xoodyak-XOF

Xoodyak-XOF [13] uses a 12-round permutation based on a sponge construction with a state size of 384 bits, consisting of three planes of 128 bits. It uses a 130-bit rate and 254-bit capacity (reduced by two for internal reasons [13]). It is based on the Xoodoo Permutation [28] and uses a column parity mixer [29]; this provides good diffusion and is suitable for modes that do not need inverses, such as sponge constructions. The non-linear layer uses a shift-invariant mapping based on the parity of three bits and implements bitwise boolean operations. The narrowing of the non-linear layer from five bits to three bits increases Xoodyak's resistance to cube attacks [13].

A deep-learning pre-image attack has been proposed on Xoodyak-Hash [30], though only with a fixed message size of 32 bits and with adjusted squeeze rates, hash lengths, or round numbers. The first model increases the squeezing rate to 384 bits, rather than the original 128 bits, representing the entire state. The second model increases the hash length to 384 bits, rather than the original 256. The third model is identical to Xoodyak-Hash, but they reduce the number of rounds to just one. Xoodyak-Hash is proven to be strong enough to resist these attacks, as they only have any success on at most one round [30], though it has been demonstrated that reducing the capacity of Xoodyak down to 128 bits helps make pre-image attacks over a small number of rounds possible [30].

 ISBN: 978-1-61208-973-7

IV. Design Consideration for Lightweight Sponge-based XOFs

The main goal when designing a lightweight XOF should be to provide the best trade-off between security and performance in both hardware and software. While the sponge construction gives a general framework that can work well in a resource-constrained environment, choices related to a particular implementation can greatly affect the overall result. In this section, we discuss the main choices that need to be made, including recommendations and considerations, when developing a sponge-based XOF.

A. Round Function Width

In general, a wider round function (i.e., one that maps more bits) offers improved security over a narrow one, though typically has performance and cost implications [29]. Wider round functions may require more circuitry or more complex software implementations which may not be appropriate in lightweight environments. Implementing widths that are a multiple of 32 or 64 bits, such as Ascon (320-bit state), Gimli (384-bit state) and Xoodyak (384-bit state), can allow vectorization on some platforms to allow parallel computation on different blocks of the state. In contrast Keccack [15], which SHA-3 is based on, uses permutations that are a multiple of 25 bits, which can severely impact performance on lightweight devices since vectorization cannot be used [14].

B. Number Of Rounds

A round function is typically used multiple times per round, potentially with some different parameters (e.g., round constants). A high number of rounds reduces performance but can improve security [31]. For lightweight algorithms it is best to select the minimum number of rounds for which there are no shortcut attacks that have a higher success probability than generic attacks such as brute force. Linear, differential and truncated differential [32] attacks exploit constructed propagation in n rounds, then attack later rounds of the primitive. If an attack is successful on n rounds, the designer should double the number of rounds to increase security resistance [33].

C. Selection Of Round Constants

Good rounds constants eliminate symmetries in iterative primitives [33]. Round constants should be different for each round, independent of the non-linear layer and defined by a specific rule to avoid slide, rotational, self-similarity, and similar attacks [34].

To see how important round constants are, consider Gimli. Gimli's use of round constants only each four rounds and having them affect just one 32-bit word of the state, led to the construction of a distinguisher for the full Gimli permutation [27]. Instead, some constant rotation should be applied each round to help provide fast diffusion [13].

Round constants also have an implication for performance. For example, Ascon's choice of round constants allows pipelining, while still ensuring that differential attacks are impossible [10].

D. Rate

In general, a low rate is less susceptible to pre-image and differential cryptanalysis attacks [31]. In Ascon-XOF, a rate of 64 bits is used. Increasing the rate would decrease the capacity, reducing robustness of the primitive [10] and increasing the likelihood of rebound attacks [36]. Recent collision attacks on Ascon [22] [25], Gimli [26] [27] and Xoodyak [30] are constrained to at most six round reduced versions of these algorithms, primarily because each uses a small rate.

E. Non-linear Layer

The non-linear layer is essentially an s-box, which is a vectorial Boolean function that performs substitution. It is mainly responsible for creating confusion (measured using Shannon's entropy) in the cryptographic primitive [37]. There is a trade-off between the size of s-boxes and the security they provide; a small differential probability, high algebraic degree and significant non-linearity reduce the number of rounds needed to secure the primitive, but often require larger, less efficient sizes [38]. In resource-constrained devices, designers are left with the choice of using smaller optimal s-boxes (perhaps combined to give a virtual larger s-box) or using a larger sub-optimal s-box that gives moderate performance [38]. In lightweight cryptographic primitives, smaller 4×4 s-boxes are the most commonly used [38].

F. Linear Layer

The design of a linear layer specifies how the non-linear and mixing layers are combined and affects propagation of the function [39]. For lightweight cryptography, a bit-oriented design should be used to improve efficiency. Further, the linear layer should be carefully considered to ease the derivation of algebraic, diffusion and correlation propagation [29]. This is achievable by ensuring weak alignment of the primitive [40], as this reduces susceptibility to truncated differential, saturation and trail clustering efforts related to differential or linear cryptanalysis. Ascon-XOF achieves this using a similar approach to SHA-2, using variant rotation constants for each word without decreasing performance [10]. On the other hand, Xoodyak uses column parity mixers, similar to Keccak [29], which are lightweight and offer weak alignment [39]. Further, using an odd number of rows makes a column parity mixer invertible, which gives immediate full diffusion in the backward direction [29].

G. Security Cliam

For sponge-based XOFs, the security claim is typically flattened to only rely on the capacity *c*, though the length of the digest used must be long enough to make generic attacks implausible (i.e., at least 128-bits). It is recommended to use a 255-bit capacity to give a strength of 128 bits [41].

V. Conclusion And Future Work

This paper examined three sponge-based XOF implementations (Ascon-XOF, Gimli-XOF and Xoodyak-XOF) to inform some design considerations that need to be taken into account when designing a secure lightweight

 ISBN: 978-1-61208-973-7

XOF. While exact considerations depend on the environment in which the XOF will operate, the following general guidelines were presented:

- Wider round functions offer improved security, though often at the expense of performance.
- Many platforms that support vectorization perform best when the round function width is a multiple of 32 or 64 bits.
- The number of rounds used should be minimized to improve performance while giving an adequate level of security; if there is a known attack on n rounds, doubling the number of rounds should give adequate security in many cases.
- Round constants should be different for each round and should eliminate symmetries in the primitive.
- Low absorbing and squeezing rates are preferable; 64 bits seems to be a good rate size.
- The non-linear layer should consist of smaller (e.g., 4 × 4) optimal s-boxes or larger sub-optimal s-boxes to balance performance and security.
- A bit-oriented design should be used for the linear layer and should ensure weak alignment of the primitive. The use of column parity mixers is recommended.
- A capacity of at least 255 bits and a digest length of at least 128 bits should be used to provide a security strength of 128 bits.

These guidelines help ensure the creation of a performant and secure lightweight sponge-based XOF, suitable for use in low-resource environments such as mobile systems. Future work will consider automatic security analysis of XOFs created using these guidelines with the goal of using evolutionary computation to design XOFs that are fit for purpose in a wide range of resource-constrained environments.

REFERENCES

[1] K. McKay, L. Bassham, M. Sönmez Turan, and N. Mouha, "Report on lightweight cryptography," tech. rep., National Institute of Standards and Technology, 2016.

[2] J. Daemen and V. Rijmen, "AES and the wide trail design strategy," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 2332, no. April 2002, pp. 108–109, 2002.

[3] W. Penard and T. van Werkhoven, "On the secure hash algorithm family," *Cryptography in context*, pp. 1–18, 2008.

[4] M. J. Dworkin et al., "SHA-3 standard: Permutation-based hash and extendable-output functions," tech. rep., National Institute of Standards and Technology, 2015.

[5] S. P. Jadhav, "Towards light weight cryptography schemes for resource constraint devices in IoT," *Journal of Mobile Multimedia*, pp. 91–110, 2019.

[6] National Institute of Standards and Technology, "Lightweight Cryptography," tech. rep., National Institute of Standards and Technology, 2022.

[7] National Institute of Standards and Technology, "Digital Signature Standard (DSS)," tech. rep., National Institute of Standards and Technology, 2013.

[8] A. Canteaut et al., "Saturnin: A suite of lightweight symmetric algorithms for post-quantum security," *IACR Transactions on Symmetric Cryptology*, vol. 2020, Special Issue 1, pp. 160–207, 2020.

[9] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Cryptographic sponges," tech. rep., Team Keccak, 2011.

[10] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2," *Submission to the CAESAR Competition*, 2016.

[11] A. Chakraborti, N. Datta, M. Nandi, and K. Yasuda, "Beetle family of lightweight and secure authenticated encryption ciphers," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, vol. 2018, no. 2, pp. 218–241, 2018

[12] H. Wu and T. Huang, "TinyJAMBU: A Family of Lightweight Authenticated Encryption Algorithms," *Submission to Lightweight Cryptography Competition*, March, 2021.

[13] J. Daemen, S. Hoffert, M. Peeters, G. V. Assche, and R. V. Keer, "Xoodyak, a lightweight cryptographic scheme," in *IACR Transactions on Symmetric Cryptology*, vol. S1, pp. 60–87, 2020.

[14] D. J. Bernstein et al., "Gimli: a cross-platform permutation," in *International Conference on Cryptographic Hardware and Embedded Systems*, pp. 299–320, Springer, 2017.

[15] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Keccak sponge function family main document," *Submission to NIST (Round 2)*, vol. 3, no. 30, pp. 320–337, 2009.

[16] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Sponge functions," in *ECRYPT hash workshop*, vol. 9, 2007.

[17] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "On the indifferentiability of the sponge construction," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 181– 197, Springer, 2008.

[18] J. Guo, T. Peyrin, and A. Poschmann, "The PHOTON family of lightweight hash functions," in *Annual Cryptology Conference*, pp. 222– 239, Springer, 2011.

[19] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "Duplexing the sponge: single-pass authenticated encryption and other applications," in *International Workshop on Selected Areas in Cryptography*, pp. 320– 337, Springer, 2011.

[20] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche, "Keccak," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 313–314, Springer, 2013.

[21] National Institute of Standards and Technology, "Secure Hash Standard (SHS) Publication," *tech. rep. March 2012, National Institute of Standards and Technology*, 2012.

[22] C. Dobraunig and F. Mendel, "Preliminary Analysis of Ascon-Xof and Ascon-Hash," *Tech. Rep.* 2019.

[23] I. Dinur and A. Shamir, "Cube attacks on tweakable black box polynomials," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 278–299, Springer, 2009.

[24] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Cryptanalysis of Ascon," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9048, pp. 371–387, 2015.

[25] R. Zong, X. Dong, and X. Wang, "Collision Attacks on Round-Reduced Gimli-Hash/Ascon-Xof/Ascon-Hash," *Cryptology ePrint Archive*, 2019.

[26] F. Liu, T. Isobe, and W. Meier, "Exploiting Weak Diffusion of Gimli: Improved Distinguishers and Preimage Attacks," *IACR Transactions on Symmetric Cryptology*, pp. 185–216, 2021.

[27] A. Flórez Gutiérrez, G. Leurent, M. Naya-Plasencia, L. Perrin, A. Schrottenloher, and F. Sibleyras, "New results on Gimli: full-permutation distinguishers and improved collisions," in *International Conference on the Theory and*

 ISBN: 978-1-61208-973-7

Application of Cryptology and Information Security, pp. 33–63, Springer, 2020

[28] J. Daemen, S. Hoffert, M. Peeters, G. Van Assche, and R. Van Keer, "Xoodoo Cookbook," *Cryptology ePrint Archive*, 2018.

[29] K. Stoffelen and J. Daemen, "Column Parity Mixers," *IACR Transactions on Symmetric Cryptology*, vol. 1, pp. 126–159, 2018.

[30] G. Liu, J. Lu, H. Li, P. Tang, and W. Qiu, "Preimage Attacks Against Lightweight Scheme Xoodyak Based on Deep Learning," in *Future of Information and Communication Conference*, pp. 637–648, Springer, 2021.

[31] L. Song, G. Liao, and J. Guo, "Non-full sbox linearization: applications to collision attacks on round-reduced Keccak," in *Annual International Cryptology Conference*, pp. 428–451, Springer, 2017.

[32] L. R. Kundsen, "Truncate and higher order differentials ," in *International Workshop on Fast Software Encryption*, pp. 196-211, Springer, 1994.

[33] J. Daemen and V. Rijmen, "The design of Rijindal, vol 2.2 Springer, 2002.

[34] C. Beierle, A. Canteaut, G. Leander, and Y. Rotella, "Proving resistance against invariant attacks: How to choose the round constants," in *Annual International Cryptology Conference*, pp.647-678, Springer, 2017.

[35] M. Eichlseder, "Differential Cryptanalysis of Symmetric Primitives," *Ausgezeichnete Informatikdissertationen*, 2019.

[36] A. Bogdanov, M. Knezevic, G. Leander, D. Toz, K. Varici, and I. Verbauwhede, "SPONGENT: the design space of lightweight cryptographic hashing," *IEEE Transactions on Computers*, vol. 62, no. 10, pp. 2041– 2053, 2012.

[37] I. Haitner, T. Holenstein, O. Reingold, S. Vadhan, and H. Wee, "Universal one-way hash functions via inaccessible entropy," in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 616–637, Springer, 2010.

[38] S. Picek, L. Mariot, B. Yang, D. Jakobovic, and N. Mentens, "Design of S-boxes defined with cellular automata rules," *ACM International Conference on Computing Frontiers 2017, CF 2017*, pp. 409–414, 2017.

[39] N. Bordes, J. Daemen, D. Kuijsters, and G. V. Assche, "Thinking Outside the Superbox," in *Annual International Cryptology Conference*, pp. 337–367, Springer, 2021.

[40] G. Bertoni, J. Daemen, M. Peeters, and G. V. Assche , *"On alignment in Keccak,"* ECRYPT II Hash Workshop, pp. 1-18, 2011.

[41] G. Bertoni et al., "Kangaroo twelve: Fast Hashing Based on Keccak-p," in *International Conference on Applied Cryptography and Network Security*, pp. 400-418, Springer, 2018.

 ISBN: 978-1-61208-973-7

Raptor Code for Selecting a Receiver Antenna

Djedjiga Benzid
Department of electrical engineering
École de Technologie supérieure
Montreal, Canada
e-mail: djedjiga.benzid.1@ens.etsmtl.ca

Michel Kadoch
Department of electrical engineering
École de Technologie supérieure
Montreal, Canada
e-mail: michel.kadoch@etsmtl.ca

***Abstract*— Massive Multiple-Input Multiple-Output (m-MIMO) is a promising technique for operating fifth-generation wireless networks (5G). However, this technique suffers from the radio frequency chain's higher cost and processing complexity. One solution to deal with this problem is improving the antenna selection method. Nevertheless, many antenna selection methods require knowledge of channel state information (CSI) to select the best performing antenna subset. Which is impossible due to the driver contamination issue in m-MIMO. Furthermore, the exhaustive search method used in conventional multiple-Input Multiple-Output is inefficient for the m-MIMO system. Consequently, this paper proposes an optimal selection algorithm for determining the best subset of antennas at the receiver when CSI is unavailable. For this purpose, we propose a water-filling algorithm based on the mutual information maximization criterion and Raptor-decoded symbols. Numerical results show that our proposed selection algorithm attains close to optimal values as the exhaustive search method.**

Keywords-antenna selection; CSI; m-MIMO; pilot-contamination; water-filling.

I. INTRODUCTION

Massive Multiple-Input Multiple-Output (m-MIMO) is a promising technique that uses hundreds of antennas at the transmitter and receiver to improve channel performance in Fifth Generation (5G) wireless networks. m-MIMO demonstrates improved link reliability, data rate, and radiated energy efficiency than conventional systems [1]. However, the large number of antennas requires the addition of radio frequency (RF) chain elements at both links, increasing the cost and system complexity of m-MIMO. An antenna selection method is used in MIMO conventional to address this issue. A practical solution where a subset of the available antennas at the transmitter and receiver are chosen on a predefined selection criterion to minimize the system complexity and cost in MIMO [2] [3]. The successive selection method, an exhaustive search method, is the most used in these systems for its optimality to find the most performant subset of antennas. However, this method is inefficient for the massive MIMO system because of the significant number of antennas which introduce complexity in the processing. Therefore, an efficient antenna selection algorithm that performs an affordable computational cost is required in m-MIMO.

Several solutions have been proposed in the literature to fix the antenna selection methods problem in m-MIMO. One of those studies used a maximum sum-rate criterion to find the optimal number of antennas [4]. Another paper proposed the maximisation of capacity/sum-rate as the selection criteria for transmitting antennas in massive MIMO's downlink [5]. This later study performed several measurement campaigns in the 2.6 GHz frequency range and used convex optimisation to select the antenna subset that maximises the downlink's Dirty-Paper Coding (DPC) capacity. The authors of the paper assumed that perfect CSI was available at the transmitter. A third method for selecting an optimal antenna is based on a binary searching algorithm using the maximising energy criterion [6]. The authors aimed to ensure energy efficiency in the m-MIMO system and assumed there was imperfect channel estimation at the transmitter.

An algorithm that selects antennas with the highest channel gain in m-MIMO has also been proposed [7]. The selected antennas are combined with Non-Orthogonal Multiple Access (NOMA) to achieve high spectral efficiency in the 5G communication network. Antenna selection at the receiver side has also been studied [8]. In this paper, upper channel capacity bounds were statistically derived for both the Sub-Array Switching (SAS) and Full-Array Switching (FAS) systems in the large-scale limit. The authors assumed that the CSI was only available on the receiver side.

Several of these solutions are fast and optimal. However, most of the solutions that have been proposed in the literature, including those cited above, assume that the channel is perfectly known when selecting antennas. This is impossible in practice, especially when m-MIMO suffers from pilot contamination.

Motivated by these observations, we previously proposed an antenna selection method that considers pilot contamination issue [10]. For this purpose, we presented a water-filling algorithm combined with Low-Density Parity-Check (LDPC) to find the optimal subset of the antennas that maximised the ergodic capacity [10]. In this method, an LDPC decoder retrieves the received symbols. The recovered

 ISBN: 978-1-61208-973-7

message was then used to estimate the gain H. The estimated channel was employed to select the optimal subset of antennas that satisfied the maximum capacity criterion. For more details about the channel estimation method, we refer the readers to our previous work [9]

This paper aims to enhance the performance of our previously published method [10] The Raptor codes are the most reliable among the erasure code, therefore, we include them instead of LDPC codes [10]. For more details about these codes, we refer the readers to [11] [12] [13] [14]. We, furthermore, add theoretical analysis to demonstrate how the water filling and the Raptor code will judiciously be exploited to select a performant subset of the antennas.

The proposed solution exploits the physical layer features and does not add more chain elements. In addition, the method based on Raptor decoded symbols requires less transmit power and avoids overload in the network since the symbol pilot are not sent. Furthermore, the Lagrangian and the Water filling algorithm do not require an exhaustive search, making them less complex. Consequently, the proposed solution contributes to reducing energy consumption and processing resources.

At the beginning of the process, when the decoded symbols are not yet available, we assume that the estimated channel is equal to one (that is, $\widehat{H} = 1$); moreover, no subset is selected.

This document is organised as follows: Section II presents the system models. Section III presents the simulation results, and Section IV concludes the paper.

II. SYSTEM MODEL

We consider m-MIMO system with a total of N_t transmit antennas and N_r receive antennas, $N_r \geq N_t$. For each transmission period, a set of $L_r < N_r$ receive antennas is chosen for signal reception. Here, we consider the case where $L_r > N_t$ to ensure spatial multiplexing. If $L_r < N_t$, the system will be rank-deficient [15]. The channel gains form the channel matrix $\boldsymbol{H} = [h_{ij}] \in \mathbb{C}^{N_r \times N_t}$, where $h_{ij} \sim \mathcal{CN}(0,1)$ are independent and identically distributed (i.i.d.). Moreover, $\boldsymbol{H}$ is known to the transmitter but not to the receiver. N_t Raptor-encoded symbols are sent through the channel, and the received signal is given by:

$$Y = HX + N \tag{1}$$

$\boldsymbol{X}$ contains the elements x_i,are the transmitted signals from antenna i. $\boldsymbol{Y}$ contains the entries y_j, which represent the received signals of the jth antenna where $j = 1, \ldots, N_r$.
The water-filling algorithm was used to find the optimal subset of the antennas that maximized the ergodic capacity [15]. Moreover, we used Raptor-decoded symbols to estimate the channel [9].

Gaussian noise vector $\boldsymbol{N} \in C^{N_r}$ consists of i.i.d. $CN(0, N0)$ variables so that $E[\boldsymbol{N}\boldsymbol{N}^{\dagger}] = \sigma_n^2 I_{Nr}$.

The receiver uses the belief propagation algorithm to retrieve the transmitted message with a soft decoding process. The likelihood ratio of the channel for each coded bit are expressed as follows [7]:

$$Z_0 = \frac{2\widehat{H}}{\sigma_n^2} Y \tag{2}$$

The details for Raptor encoding and decoding are provided in a previous study [7].

$\widehat{H}$ is the estimated random variable coefficients of H. The channel estimation is calculated using the Minimum Mean Squared Error (MMSE) as previously described [11] [13]. The $\widehat{H}$ channel is given by:

$$\widehat{H} = R_{HH}(R_{HH}XX^T + \sigma_n^2 I)^{-1} X^T Y \tag{3}$$

where R_{HH} is the covariance of H.

To avoid symbol pilot contamination, the Raptor-decoded symbols $\widehat{S}$ are used instead of the pilot symbols X to estimate.

the channel, as previously described [9]. Hence, X is substituted with $\hat{S}$ in (3) as follows:

$$\widehat{H} = R_{HH}(R_{HH}SS^T + \sigma_n^2 I)^{-1} S^T Y \tag{4}$$

However, to perfectly estimate H at the receiver, the average Bit Error Rate (BER) must approach zero, which means that the message must be entirely recovered (i.e., $S = X$); otherwise, the system is in an outage and H cannot be estimated.

Corresponding to this outage probability, there is a minimum received Signal-to-Noise Ratio (SNR), SNR_{min}, given by:

$$P_{out} = p(SNR < SNR_{min}) \tag{5}$$

$$BER = \frac{1}{2} erfc\sqrt{SNR}$$

$$BER_{max} = \frac{1}{2} erfc\sqrt{SNR_{min}}$$

$$BER_{max} \propto \frac{1}{SNR}$$

$$P_{out} = p(BER > BER_{max})$$

When $SNR \geq SNR_{min}$, the outage probability at the receiver reaches zero: $P_{out} \to 0$ and $BER \to 0$ .Under the fading, the channel is varying slowly. The capacity of the channel C can therefore be expressed as the maximum of mutual information using the following equation:

$$C = log_2\, det(I + SNR) \tag{6}$$

 ISBN: 978-1-61208-973-7

Because $= \frac{\hat{H}\hat{H}^T}{\sigma_n^2}$, (6) can be rewritten as:

$$C = log_2\, det\left(I + \frac{\hat{H}\hat{H}^T}{\sigma_n^2}\right) \quad (7)$$

A. Antenna Selection

As discussed in the previous section, no symbols are recovered when $SNR = SNR_{min}$ the system is in an outage. In this case, the estimated channel cannot be processed using our approach .Therefore, our antenna selection method will not be applied since it is based on maximizing the capacity criterion.

However, when the BER at the receiver approaches zero, $\hat{H}$ can be calculated. Antenna selection can then be performed to find the optimal antenna subset.

As in a previous study [15], a diagonal matrix Δ of size $N_r \times N_r$ is defined as follows:
$Tr(\Delta) = \sum_i^{N_r} \Delta_i = L_r \leq N_r$ represents the number of receive antennas selected at the reception. The received signal is re-written, including receive antenna selection, as:

$$Y = \Delta HX + N \quad (8)$$

The ergodic capacity function of selected antennas can be written through the matrix Δ as follows:

$$C = log_2\, det\left(I + \Delta\hat{H}\hat{H}^H\right) \quad (9)$$

The optimization problem is to pick the L_r receive antennas such that the capacity in (9) is maximized. It is equivalent to finding the matrix Δ such that:

$$C(\Delta) = arg \max_{\substack{\Delta_i \in \{0,1\} \\ \sum_i \Delta_i = L_r}} log_2\, det\left(I + \Delta\hat{H}\hat{H}^H\right) \quad (10)$$

The antenna selection problem in the massive antenna system can be expressed as:

$$\underset{\{\Delta\}}{maximize}\; C(\Delta) = log_2\, det\left(I + \Delta\hat{H}\hat{H}^H\right) \quad (11)$$

subject to:

$$0 \leq \Delta \leq 1 \rightarrow (Condition\ 1) \quad (12)$$

$$Trace(\Delta) = L_r \rightarrow (Condition\ 2)$$

However, the term $\hat{H}\hat{H}^H$ introduces a complexity on the order of $o(n^6)$. This complexity can be reduced using the low-rank approximation method. The key point is to use the Single Value Decomposition (SVD) method to achieve an ideal low-level estimator.

According to the signal processing theory, the channel correlation matrix can be decomposed using SVD of low-rank approximation, as previously described [16]:

$$R_{HH} = U \wedge U^H \quad (13)$$

U is a unitary matrix and ∧ is a diagonal matrix with the singular values of R_{HH}. The MMSE equation can therefore be represented by:

$$svd(\hat{H}) = U \wedge U^H (U \wedge U^H SS^T + \sigma_n^2)^{-1} SY \quad (14)$$

If taking $\Sigma = \wedge (U \wedge U^{H_P} + \sigma_n^2)^{-1}$, the eigenvalue of ∧ is $\lambda_1 \geq \lambda_2 \geq \cdots \lambda_n \geq 0$ non-zero.

$$\Sigma = \frac{\lambda_k SY}{\lambda_k SS^T + \sigma_n^2} \quad (15)$$

Only the diagonal value is considered in the low rank, so Σ could be written by:

$$\Delta_P = \begin{cases} \frac{\lambda_k SY}{\lambda_k SS^T + \sigma_n^2} & if\ k = 0;\ 1; \ldots\ldots\ldots P-1; \\ 0 & if\ k = P; P+1; \ldots\ldots\ldots N-1; \end{cases} \quad (16)$$

Then finally, the SVD algorithm can be represented as previously described [8]:

$$\Sigma = \begin{bmatrix} \Delta_P & 0 \\ 0 & 0 \end{bmatrix} \quad (17)$$

$$\Delta_P = \begin{bmatrix} \frac{\lambda_0 S^T Y}{\lambda_0 SS^T + \sigma_n^2} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{\lambda_{P-1} S^T Y}{\lambda_{p-1} SS^T + \sigma_n^2} \end{bmatrix} \quad (18)$$

$$svd(\hat{H}\hat{H}^H) = U\Delta_p^2 U^H = U \begin{bmatrix} {\Delta_P}^2 & 0 \\ 0 & 0 \end{bmatrix} U^H \quad (19)$$

$${\Delta_P}^2 = \begin{bmatrix} \frac{\lambda_0 SYY^H S^T}{\left(\lambda_0 SS^T + \sigma_n^2\right)^2} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{\lambda_{P-1} SYY^H S^T}{\left(\lambda_{P-1} SS^T + \sigma_n^2\right)^2} \end{bmatrix} \quad (20)$$

The simplification term in the denominator can be written as:

$$(SS^T\lambda_0 + \sigma_n^2)^2 = \lambda_0 S^T SSS^T + (\sigma_n^2)^2 \quad (21)$$

Hence,

$${\Delta_P}^2 = \begin{bmatrix} \frac{\lambda_0 SYY^H S^T}{SS^T SS^T + \left(\sigma_n^2\right)^2} & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \frac{\lambda_{P-1} SYY^H S^T}{SS^T SS^T + \left(\sigma_n^2\right)^2} \end{bmatrix} \quad (22)$$

 ISBN: 978-1-61208-973-7

In high Signal-To-Noise Ratio (SNR), the equation (22) can be rewritten as follows:

$$\Delta_P{}^2 = \lambda_k \frac{YY^T}{SS^T} \quad (23)$$

$$\Delta_P{}^2 = \sum_{k=1}^{p} \lambda_k \left(\frac{Y_k}{S_k}\right)^2 \quad (24)$$

And the equation (11) becomes:

$$C(\Delta) = arg \max_{\substack{\Delta_i \\ \sum_i \Delta_i}} log_2\, det\left(I + \Delta(U\Delta_P{}^2 U^H)\right) \quad (25)$$

Because $U\Delta U^H = \Pi$,

$$C(\Delta) = log_2\, det(I + \Delta_P \Pi \Delta_P) \quad (26)$$

The objective function is concave in Π. However, the Π are binary integer variables making the optimization problem hard for Non-deterministic Polynomial-time (NP). In time order to solve this optimization problem, as in a previous study [17], we relax the constraint that each Π must be a binary integer to the weaker constraint that:

$$0 \leq \Pi \leq 1 \quad (27)$$

The original problem thus becomes a convex optimization problem solvable with water-filling. The Lagrangian method is used to optimize the power of the selected received antennas L_r.

Let $f(\Pi) = \log_2 det(I + \Delta_P \Pi \Delta_P)$ and $(\Pi) = tr(\Pi) - L_r$. The Lagrangian equation is given as follows:

$$\mathcal{L}(\Pi, \psi) = \Delta_P \Pi \Delta_P - \psi(tr(\Pi) - L_r) \quad (28)$$

The derived form of equation (25) is given bellow:

$$\frac{\partial \mathcal{L}(\Pi,\psi)}{\partial \Pi} = \frac{\Delta_P \Delta_P}{(I+\Delta_P \Pi \Delta_P)} - \psi = 0 \Rightarrow$$

$$\psi \Delta_P{}^{-2} = (I + \Delta_P \Pi \Delta_P) \Rightarrow$$

$$\psi^{-1} \Delta_P{}^2 - 1 = \Delta_P \Pi \Delta_P{}^H \Rightarrow \Pi = \psi^{-1} - \Delta_P{}^{-2} \quad (29)$$

$$\frac{\partial \mathcal{L}(\Pi, \psi)}{\partial \psi} = -tr(\Sigma_s) + L_r = 0$$

From (27) at optimality, Π is diagonal. Then the following water filling solution can be obtained

$$\Pi = \left(\psi^{-1} - \Delta_P{}^{-2}\right)^+ \quad (30)$$

III. Simulation Results

The performance of our scheme is evaluated. The codeword length chosen for LDPC encoding is 80000 bits, the message length is 980 bits, and the code rate is 0.98. The degree of distribution of the Luby Transform (LT) encoding is the same as that used in [18]and is as follows:

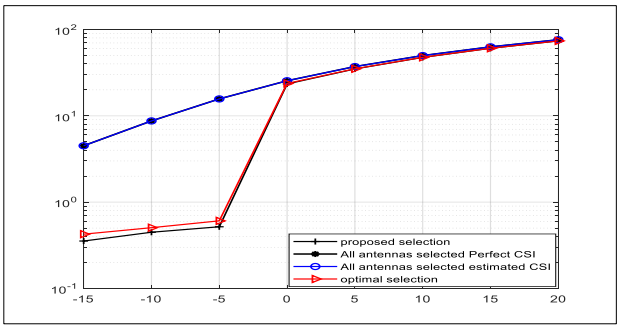

Figure1. Ergodic capacity vs. SNR

$\Omega(x) = 0.008x + 049x^2 + 0.166x^3 + 0.073x^4 + 0.083x^5 + 0.056x^8 + 0.037x^9 + 0.056x^{19} + 0.025x^{65} + 0.003x^{66}$. Furthermore, we use a massive-MIMO system involving 16 antennas at receiver and eight antennas at the transmitter and a subset of the selected antennas Lr=12.

Figure 1 shows the relationship between ergodic capacity and received SNR. The ergodic capacity allows us to select the optimal number of antennas. In this part, the simulation is performed to evaluate four scenarios:

1) Scenario 1: represents our proposed method under perfect CSI and without performing antenna selection method (shown in black with an asterisk)

2) Scenario 2: depicts our proposed method all antennas are selected, and CSI is estimated using the Raptor decoded symbols (blue with circular markers)

3) Scenario 3: describes an exhaustive method (used in conventional MiMo), the number of selected antennas Lr=12. CSI is estimated using the Raptor decoded symbols (red with a triangle pointing to the right)

4) Scenario 4: illustrates our proposed method where Lr=12. CSI estimated using Raptor decoded symbols (black with a plus sign).

Note that the graphs of the first and second scenarios are superposed because they meet the same ergodic capacity values regardless of SNRs' values. This proves our approach's efficiency. However, the ergodic capacity of the two latest scenarios remains low when the SNR is between -15dB and -5dB since the channel cannot be estimated in this interval (see section II-A).

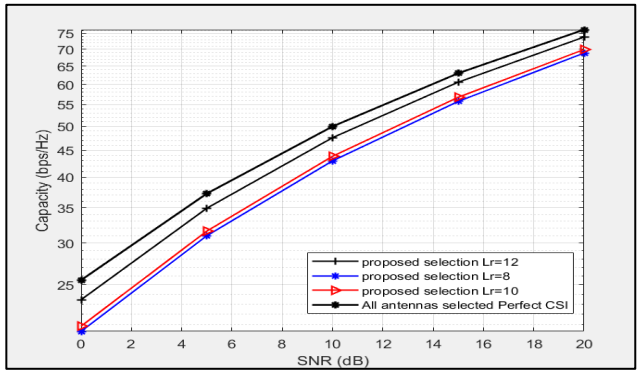

Figure 2. Ergodic capacity vs. SNR for successful decoding

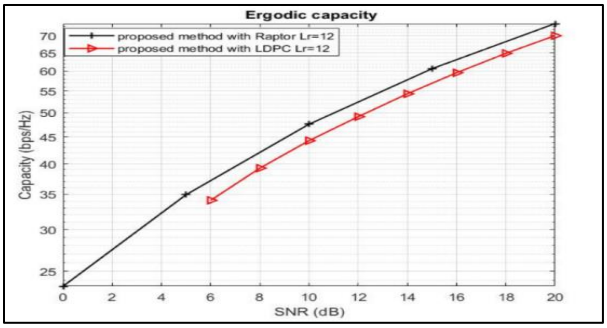

Figure 3. The capacity of Raptor and LDPC code

The ergodic capacity approaches the values of the first two scenarios for an SNR>0. Since the message is completely recovered and the channel is correctly estimated. For the following simulations, we only consider the values when SNR>0.

Figure 2. shows the ergodic capacity vs received SNR per selected antennas Lr, Lr=12, 10 and 8. The results show that Lr=12 achieves the near-to-optimal values.

Figure 3 compares the results of the Raptor-based antenna optimizations and LDPC- based antenna optimizations method proposed in previous work [10]. The channel estimated with Raptor code attains higher optimal capacity than the channel estimated with LDPC code.

IV. CONCLUSION

This paper proposes an antenna selection method performed under imperfect CSI. Our solution combines an antenna selection method based on mutual information maximization and the Raptor decoded information symbols. The Raptor decoded message is used to estimate the channel, and then the water-filling algorithm uses the estimated channel to select the highest-performing subset of antennas. This method requires less transmit power and avoids overload in the network since the symbol pilot are not sent. Which contributes to reducing energy consumption and processing resources Simulation results show that the ergodic capacity reaches near to optimal values using Raptor code than LDPC. Future work can include other methods of antenna selection.

REFERENCES

[1] Y. Zhou, L. Liu, H. Du, L. Tian, X. Wang, and J. Shi, "An overview on intercell interference management in mobile cellular networks: From 2G to 5G," in *2014 IEEE International Conference on Communication Systems*, 2014, pp. 217-221: IEEE.

[2] S. Sanayei and A. Nosratinia, "Antenna selection in MIMO systems," *IEEE Communications magazine*, vol. 42, no. 10, pp. 68-73, 2004.

[3] A. Gorokhov, D. A. Gore, and A. J. Paulraj, "Receive antenna selection for MIMO spatial multiplexing: theory and algorithms," *IEEE Transactions on signal processing*, vol. 51, no. 11, pp. 2796-2807, 2003.

[4] P. D. Selvam and K. S. Vishvaksenan, "Antenna Selection and Power Allocation in Massive MIMO," *Radioengineering*, vol. 28, no. 1, pp. 340-346, 2019.

[5] X. Gao, O. Edfors, J. Liu, and F. Tufvesson, "Antenna selection in measured massive MIMO channels using convex optimization," in *2013 IEEE globecom workshops (GC Wkshps)*, 2013, pp. 129-134: IEEE.

[6] Z. Chang, Z. Wang, X. Guo, Z. Han, and T. Ristaniemi, "Energy-efficient resource allocation for wireless powered massive MIMO system with imperfect CSI," *IEEE Transactions on Green Communications and Networking*, vol. 1, no. 2, pp. 121-130, 2017.

[7] X. Liu and X. Wang, "Efficient antenna selection and user scheduling in 5G massive MIMO-NOMA system," in *2016 IEEE 83rd Vehicular Technology Conference (VTC Spring)*, 2016, pp. 1-5: IEEE.

[8] Y. Gao, H. Vinck, and T. Kaiser, "Massive MIMO antenna selection: Switching architectures, capacity bounds, and optimal antenna selection algorithms," *IEEE Transactions on Signal Processing*, vol. 66, no. 5, pp. 1346-1360, 2017.

[9] D. Benzid and M. Kadoch, "Raptor code to mitigate Pilot contamination in Massive MiMo," *Procedia Computer Science*, vol. 130, pp. 310-317, 2018/01/01/ 2018.

[10] D. Benzid, K. Michel, Z. Chang, J. Lu, and R. Liu, "LDPC for receive antennas selection in massive MiMo," in *2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2020, pp. 322-325: IEEE.

[11] A. Shokrollahi and M. Luby, "Raptor codes," *Foundations and trends® in communications and information theory*, vol. 6, no. 3–4, pp. 213-322, 2011.

[12] T. Stockhammer, A. Shokrollahi, M. Watson, M. Luby, and T. Gasiba, "Application layer forward error correction for mobile multimedia broadcasting," *Handbook of mobile broadcasting: DVB-H, DMB, ISDB-T and media flo*, pp. 239-280, 2008.

[13] W. Ryan and S. Lin, *Channel codes: classical and modern*. Cambridge university press, 2009.

[14] P. G. F. Jorge Castiñeira Moreira, *ESSENTIALS OF ERROR-CONTROL CODING*. John Wiley & Sons Ltd, 2006.

[15] K. T. Phan and C. Tellambura, "A water-filling algorithm for receive antenna selection based on mutual information maximization," in *2007 10th Canadian Workshop on Information Theory (CWIT)*, 2007, pp. 128-131: IEEE.

[16] W. Guo and G. Li, "Study on channel estimation of Long Term Evolution," in *Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on*, 2011, pp. 367-369: IEEE.

[17] X. Gao, O. Edfors, F. Tufvesson, and E. G. Larsson, "Multi-switch for antenna selection in massive MIMO," in *2015 IEEE Global Communications Conference (GLOBECOM)*, 2015, pp. 1-6: IEEE.

[18] D. Benzid and M. Kadoch, "Fountain Codes and Linear Filtering to Mitigate Pilot Contamination Issue in Massive MiMo," *Network and Communication Technologies*, vol. 4, p. 1, 01/10 2019.

 ISBN: 978-1-61208-973-7