Network Security Concerns in 5G MIMO Beamforming

Mohamed A. Ismail

November 16, 2023

Network Security Concerns in 5G MIMO Beamforming

Mohamed A. Ismail
Hazem Hassan Co.
Riyadh, Saudi Arabia
mido.world@outlook.com

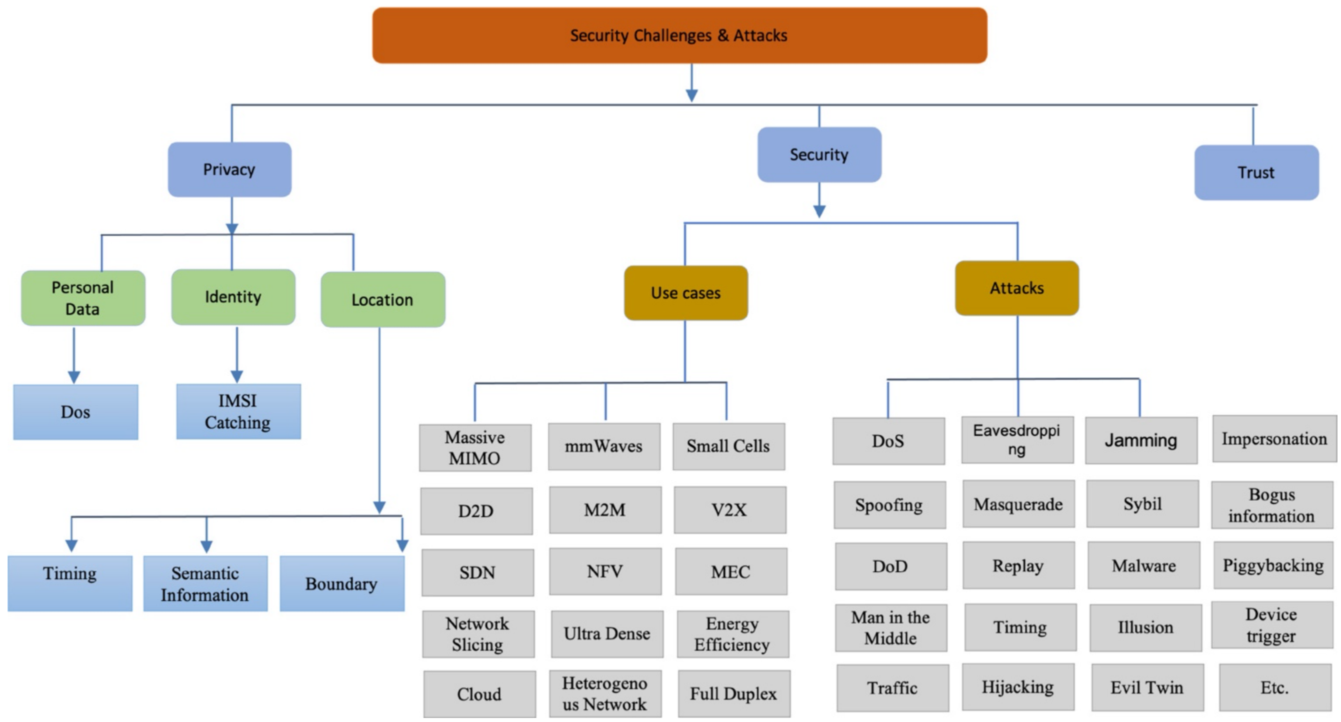
Abstract

MIMO technology is a key technology of 5G, which is widely used in next-generation scenarios such as heterogeneous networks, millimeter-wave networks, and automotive networks. How to build a large-scale MIMO system security situation assessment model for 5G has become the main topic of current concern. The broader reach of network infrastructure and transport layer cryptographic gains on 5G security tend to receive a large proportion of focus in threat modeling and mitigation, but the underlying physical layer backbone has seen significant changes with massive MIMO, beamforming, and mmWave spectrum use at the edge. Examples of the attacks against MIMO are those related to the decentralization of the RAN towards fog computing IoT technologies, the continued blurring of WLAN with Frequency Range 2 (FR2) small cells, and the perceived vulnerability to physical attacks that these spatially isolated networks exhibit further demonstrate the necessity of modeling preexisting threat profiles to be inclusive and emphatic of emerging physical layer attacks. We look at one threat for FR1 (pilot contamination) and one for FR2 (mmWave attacks), both utilizing the physical properties of beamforming and demonstrating the new concerns in the highly heterogeneous network architecture in use by 5GNR. In this paper, we focus on the security concerns related to the Massive MIMO.

Index Terms: Massive MIMO, security, 5G, RAN, privacy, trust.

1. Key security challenges in 5G

The Key security challenges in 5G include more security is required to guarantee the safety of the critical network infrastructure and the privacy of the user in a highly connected environment where everything is connected to the internet and exposed to different attacks. For instance, a security breach in one of the smart grid systems can lead to an electrical system damage and thus to the smart city depending on it. The consequence of the security breach can easily spread over the connected network to harm other systems and other services. In addition, user's privacy can be attacked while transmitting user's sensitive data over the 5G network. Therefore, there is an urgent need for security solutions to protect the 5G network while providing high data rate and low latency. Security challenges and issues can be classified according to which 5G use case is involved. Figure 1 illustrates these challenges and their taxonomy.



In this paper, we focus on the Massive MIMO security. Although its advantages, it can be under several attacks and vulnerabilities, which releases some of the security concerns. Examples of attacks targeting the massive MIMO include jamming, eavesdropping, and pilot spoofing. Jamming attacks are one of the prime security issues threatening the massive MIMO systems. By using multiple antennas with high degrees of freedom, these systems can discard the suspicious signals from malicious users. In [1] the authors suggested reducing the jamming attacks impact by using joint channel estimation and decoding to estimate the channel state instead of using the uplink pilots waveforms. In [2] the authors proposed an energy efficiency method by optimizing the power consumption by increasing the number of antennas at the base stations. However, using more antennas cannot decrease the power consumption anymore at some saturation points. Beamforming has been used to provide more secure MIMO networks and fight against passive eavesdropping attacks. Massive MIMO is one of the promising technologies for the 5G network and beyond. However, it is considered as the most disruptive use case as it uses a large number of antennas to serve a massive number of users simultaneously, which opens the physical layer to many security attacks. These attacks can be either active or passive. Active attacks aim at disrupting, corrupting, or transmitting signals over a legal transmission. They include jamming and contamination attacks. Passive attacks aim at eavesdropping and spying the legal transmissions. Jamming attackers send junk signals to the users or base stations to disrupt the legal transmission. Contamination, also known as pilot spoofing, attackers contaminate the pilots by pretending to be a legal user. Machine learning has been used to protect massive MIMO systems by detecting active attacks [3]. However, massive MIMO involves a large amount of data coming from a high number of antennas and users, which results in a high amount of data overhead and requires a massive amount of data to train the machine learning algorithm. Each base station needs a training dataset per antenna, which requires extra data processing, storage, complexity, and more time by the intrusion detection systems. Moreover, with this large number of users in mobility, machine learning algorithms will not be able to train dynamic environment with changing parameters over time.

The mmWaves communication is another challenge. In [4] the authors proposed to combine the mmWaves with beamforming MIMO to offer more secure communication.

2. 5G MIMO Beamforming Security Concerns

A key component of 5G, massive MIMO, also prompts new security threats to address. Pilot contamination attack on massive MIMO [5], session hijacking by redirection in beamforming towards the attacker, is of primary interest to mitigate. During negotiation when the client sends pilot signals to the base station, those signals can be repeated by the attacker to contaminate the uplink channel training in the attacker's favor. This particular vulnerability relates to the use of Time Duplex Division (TDD) and the need for user pilot signals to estimate the channel for downlink. While the channel, once negotiated, is considerably hardened by the properties of beamforming against eavesdropping, these properties are negated if the eavesdropper's pilot signal power was sufficient to overwhelm the real client's, resulting in the base station beamforming towards the eavesdropper. Humayan *et al.* [5] provides an overview of work done in simulating and mitigating such an attack on Table V of their paper. Some of the promising solutions include matching filter precoding on weak and strongly correlated channels to the attack, hiding the pilot signal within an enlarged set, and employing a sliding length secrecy key based on information leakage estimates. Of note about all three proposals is an active analysis of the pilot contamination attack in the creation of the unique mitigation.

Another of the key components of 5G, millimeter-wave frequency use with small cell base stations, has a similar but distinct threat profile from massive MIMO outside at the micro-wave level. Compared to micro- and macro- cells, small cell sites (pico- and femto- cell) work under different propagation laws and are particularly susceptible to blockage [6]. The short range combined with that susceptibility to blockage results in low visibility of signal on weakly correlated channels and outside of the propagation path [5], making the overlap of the user and eavesdropper particularly important to the level of secrecy in mmWave transmissions. Some proposals found in Humayan *et al.* (on Table VI) [5] vary based on the simulation constraints placed the eavesdropper, single antenna versus multi-antenna being the primary differential. A particularly interesting solution is utilizing antenna subset modulation per symbol in transmission for the desired user, resulting in eavesdroppers receiving statistical noise.

Conclusion

While there is a continuity in 5G of the security concerns of 4G and prior generation architecture, 5GNR has special considerations that must be made. With widespread rates of adoption of 5GNR worldwide in the years preceding 2023 and continued growth in that sector, 5G is no longer just an emerging technology and its attack vectors have now become a facet of the overall attack surface of telecommunication infrastructure in use in production networks. Proposed security solutions can see live testing, analysis, iteration, and implementation while network adoption still outpaces user equipment support and use [6]. For future, we plan to extend the current work with the interested studies introduced in [7-81].

References

[1] Sodagari S, Clancy TC. Efficient jamming attacks on mimo channels. Paper presented at: 2012 IEEE International Conference on Communications (ICC); 2012;852-856; IEEE.

[2] Wang F, Zhong C, Gursoy MC, Velipasalar S. Defense strategies against adversarial jamming attacks via deep reinforcement learning. Paper presented at: 2020 54th Annual Conference on Information Sciences and Systems (CISS); 2020; 1-6; IEEE.

[3] Fourati H, Maaloul R, Chaari L. A survey of 5G network systems: challenges and machine learning approaches. Int J Mach Learn Cybern. 2020; 12: 1-47.

[4] Gong S, Xing C, Fei Z, Ma S. Millimeter-wave secrecy beamforming designs for two-way amplify-and-forward mimo relaying networks. IEEE Trans Veh Technol. 2016; 66(3): 2059-2071.

[5] Wu, Y., Khisti, A., Xiao, C., Caire, G., Wong, K.-K., & Gao, X. (2018). A Survey of Physical Layer Security Techniques for 5G Wireless Networks and Challenges Ahead. IEEE Journal on Selected Areas in Communications, 36(4), 679–695. https://doi.org/10.1109/JSAC.2018.2825560

[6] Humayun, Mamoona, Bushra Hamid, NZ Jhanjhi, G. Suseendran, and M N Talib. “5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey.” Journal of physics. Conference series 1979, no. 1 (2021): 12037–.

[7] A. A. Khalil, M. A. Rahman and H. A. Kholidy, "FAKEY: Fake Hashed Key Attack on Payment Channel Networks," 2023 IEEE Conference on Communications and Network Security (CNS), Orlando, FL, USA, 2023, pp. 1-9, doi: 10.1109/CNS59707.2023.10288911.

[8] Hisham A. Kholidy, Fabrizio Baiardi, A. Azab, "A Data-Driven Semi-Global Alignment Technique for Masquerade Detection in Stand-Alone and Cloud Computing Systems", is Submitted in ", granted on January 2019, US 20170019419 A1.

[9] Hisham A. Kholidy, “Accelerating Stream Cipher Operations using Single and Grid Systems”, US Patent and Trademark Office (USPTO), April 2012, US 20120089829 A1.

[10] Hisham Kholidy, “Multi-Layer Attack Graph Analysis in the 5G Edge Network Using a Dynamic Hexagonal Fuzzy Method”, Sensors 2022, 22, 9. https://doi.org/10.3390/s22010009. (IF: 3.576).

[11] Hisham Kholidy, “Detecting impersonation attacks in cloud computing environments using a centric user profiling approach”, Future Generation Computer Systems, Volume 117, issue 17, Pages 299-320, ISSN 0167-739X, https://doi.org/10.1016/j.future.2020.12.009, (IF: 7.307). April 2021, https://www.sciencedirect.com/science/article/pii/S0167739X20330715

[12] Hisham Kholidy, “Autonomous Mitigation of Cyber Risks in Cyber-Physical Systems”, Future Generation Computer Systems, Volume 115, February 2021, Pages 171-187, ISSN 0167-739X, (IF: 7.307) DOI: https://doi.org/10.1016/j.future.2020.09.002 https://www.sciencedirect.com/science/article/pii/S0167739X19320680

[13] Hisham A. Kholidy, “An Intelligent Swarm based Prediction Approach for Predicting Cloud Computing User Resource Needs”, the Computer Communications Journal, Feb 2020 (IF: 5.047). https://authors.elsevier.com/tracking/article/details.do?aid=6085&jid=COMCOM&surname=Kholidy

[14] Hisham A. Kholidy, “Correlation Based Sequence Alignment Models for Detecting Masquerades in Cloud Computing”, IET Information Security Journal, DOI: 10.1049/iet-ifs.2019.0409, Sept. 2019 (IF: 1.51) https://digital- library.theiet.org/content/journals/10.1049/iet-ifs.2019.0409

[15] I. Elgarhy, M. M. Badr, M. Mahmoud, M. M. Fouda, M. Alsabaan and Hisham A. Kholidy, "Clustering and Ensemble Based Approach For Securing Electricity Theft Detectors Against Evasion Attacks", in IEEE Access, January 2023, doi: 10.1109/ACCESS.2023.3318111. (IF: 3.55).

[16] Mustafa, F.M., Hisham A. Kholidy, Sayed, A.F. et al. “Backward pumped distributed Raman amplifier: enhanced gain”, Optical Quantum Electron 55, 772 (2023). https://doi.org/10.1007/s11082-023-05066-3 (IF: 3.0).

[17] Alahmadi TJ, Rahman AU, Alkahtani HK, Hisham A. Kholidy “Enhancing Object Detection for VIPs Using YOLOv4_Resnet101 and Text-to-Speech Conversion Model”, Multimodal Technologies and Interaction. 2023; 7(8):77. https://doi.org/10.3390/mti7080077 (IF: 3.17).

[18] Alkhowaiter, M.; Hisham A. Kholidy.; Alyami, M.A.; Alghamdi, A.; Zou, C, “Adversarial-Aware Deep Learning System Based on a Secondary Classical Machine Learning Verification Approach”. Sensors 2023, 23, 6287. https://doi.org/10.3390/s23146287 (IF: 3.9).

[19] Badr, Mahmoud M., Mohamed I. Ibrahem, Hisham A. Kholidy, Mostafa M. Fouda, and Muhammad Ismail. 2023. "Review of the Data-Driven Methods for Electricity Fraud Detection in Smart Metering Systems" Energies 16, no. 6: 2852. 2023 (IF: 3.25). https://doi.org/10.3390/en16062852

[20] A Jakaria, M. Rahman, M. Asif, A. Khalil, Hisham Kholidy, M. Anderson, S. Drager, "Trajectory Synthesis for a UAV Swarm Based on Resilient Data Collection Objectives," in IEEE Transactions on Network and Service Management, 2022, doi: 10.1109/TNSM.2022.3216804. (IF: 4.75). https://ieeexplore.ieee.org/document/9928375?source=authoralert

[21] Mustafa, F.M., Hisham Kholidy., Sayed, A.F. et al., “Enhanced dispersion reduction using apodized uniform fiber Bragg grating for optical MTDM transmission systems”. Optical and Quantum Electronics 55, 55 (December 2022). https://doi.org/10.1007/s11082-022-04339-7 . (IF: 2.79).

[22] Hisham A. Kholidy, Abdelkarim Erradi, “VHDRA: A Vertical and Horizontal Dataset Reduction Approach for Cyber-Physical Power-Aware Intrusion Detection Systems”, SECURITY AND COMMUNICATION NETWORKS Journal (IF: 1.968), March 7, 2019. vol. 2019, 15 pages. https://doi.org/10.1155/2019/6816943.

[23] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, "A risk mitigation approach for autonomous cloud intrusion response system", in Journal of Computing, Springer, DOI: 10.1007/s00607-016-0495-8, June 2016. (IF: 2.42).
[24] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, "DDSGA: A Data-Driven Semi- Global Alignment Approach for Detecting Masquerade Attacks", in IEEE Transactions on Dependable and Secure Computing, DOI 10.1109/TDSC.2014.2327966, May 2014. (ISI Impact factor: 6.791).
[25] Hisham A. Kholidy, Hala Hassan, Amany Sarhan, Abdelkarim Erradi, Sherif Abdelwahed, "QoS Optimization for Cloud Service Composition Based on Economic Model", Book Chapter on the Internet of Things. User-Centric IoT, 2015, Volume 150 ISBN : 978- 3-319-19655-8
[26] Atta-ur Rahman, Maqsood Mahmud, Tahir Iqbal, Hisham Kholidy, Linah Saraireh, et al "Network anomaly detection in 5G networks", The Mathematical Modelling of Engineering Problems journal, April 2022, Volume 9, Issue 2, Pages 397-404. DOI 10.18280/mmep.090213
[27] Hisham A Kholidy., et al. "A Survey Study For the 5G Emerging Technologies", Acta Scientific Computer Sciences 5.4 (2023): 63-70, DOI: 10.13140/RG.2.2.22308.04485.
[28] Hisham A. Kholidy, Fabrizio Baiardi, Salim Hariri, Esraa M. ElHariri, Ahmed M. Youssouf, and Sahar A. Shehata, "A Hierarchical Cloud Intrusion Detection System: Design and Evaluation", in International Journal on Cloud Computing: Services and Architecture (IJCCSA), November 2012. DOI 10.5121/ijccsa.2012.2601
[29] Hisham A. Kholidy, Alghathbar Khaled s., "Adapting and accelerating the Stream Cipher Algorithm RC4 using Ultra Gridsec and HIMAN and use it to secure HIMAN Data", Journal of Information Assurance and Security (JIAS), vol. 4 (2009)/ issue 4,pp 274,tot.pag 283, 2009. http://www.mirlabs.org/jias/vol4-issue6.html
[30] Hisham A. Kholidy, "A Smart Network Slicing Provisioning Framework for 5Gbased IoT Networks", The 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2023). San Antonio, Texas, USA. October, 2023.
[31] Hisham A. Kholidy, "Towards A Scalable Symmetric Key Cryptographic Scheme: Performance Evaluation and Security Analysis", IEEE International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, May 1-3, 2019. https://ieeexplore.ieee.org/document/8769482.
[32] Hisham A. Kholidy, "A Study for Access Control Flow Analysis With a Proposed Job Analyzer Component based on Stack Inspection Methodology", the 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 1442-1447, Cairo, Egypt, vol. IEEE Catalog Number: CFP10394-CDR, 2010.
[33] Hisham A. Kholidy, "HIMAN-GP: A Grid Engine Portal for controlling access to HIMAN Grid Middleware with performance evaluation using processes algebra", The 2nd International Conference on Computer Technology and Development ICCTD, pp 163-168, Cairo, 2010.
[34] R. Bohn, A. Battou, B. Choi, R. Chaparadza, S. Song, T. Zhang, T. Choi, Hisham A. Kholidy, M. Park, S. Go, "NIST Multi-Domain Knowledge Planes for Service Federation for 5G & Beyond Public Working Group: Applications to Federated Autonomic/Autonomous Networking", in the IEEE Future Networks World Forum (FNWF), 13–15 November 2023 // Baltimore, MD, USA.
[35] I. Elgarhy, A. El-toukhy, M. Badr, M. Mahmoud, M. Fouda, M. Alsabaan, Hisham A. Kholidy, "Secured Cluster-Based Electricity Theft Detectors Against Blackbox Evasion Attacks", in the IEEE 21st Consumer Communications & Networking Conference (CCNC), 6-9 January 2024.
[36] M. C. Zouzou, E. Benkhelifa, Hisham A. Kholidy and D. W. Dyke, "Multi-Context-aware Trust Management framework in Social Internet of Things (MCTM-SIoT)," 2023 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS), Valencia, Spain, 19-22 June 2023, pp. 99-104, doi: 10.1109/ICCNS58795.2023.10193510.
[37] Hisham A. Kholidy, Andrew Karam, James Sidoran, et al. "Toward Zero Trust Security in 5G Open Architecture Network Slices", IEEE Military Conference (MILCOM), CA, USA, November 29, 2022. https://edas.info/web/milcom2022/program.html
[38] Hisham A. Kholidy, Andrew Karam, Jeffrey H. Reed, Yusuf Elazzazi, "An Experimental 5G Testbed for Secure Network Slicing Evaluation", the 2022 IEEE Future Networks World Forum (FNWF), Montreal, Canada, October 2022. https://fnwf.ieee.org/wp-content/uploads/sites/339/2022/10/AcceptedPaperScheduleV0.1.pdf
[39] Hisham A. Kholidy, Riaad Kamaludeen "An Innovative Hashgraph-based Federated Learning Approach for Multi Domain 5G Network Protection", the 2022 IEEE Future Networks World Forum (FNWF), Montreal, Canada, October 2022. https://fnwf.ieee.org/wp-content/uploads/sites/339/2022/10/AcceptedPaperScheduleV0.1.pdf
[40] Hisham A. Kholidy, Salim Hariri, "Toward an Experimental Federated 6G Testbed: A Federated leaning Approach", the 19th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA 2022), Abu Dhabi, UAE December 5th - December 7th, 2022
[41] Hisham Kholidy, Andrew Karam, James L. Sidoran, Mohammad A. Rahman, "5G Core Security in Edge Networks: A Vulnerability Assessment Approach", the 26th IEEE Symposium on Computers and Communications (The 26th IEEE ISCC), Athens, Greece, September 5-8, 2021. https://ieeexplore.ieee.org/document/9631531
[42] N. I. Haque, M. Ashiqur Rahman, D. Chen, Hisham Kholidy, "BIoTA: Control-Aware Attack Analytics for Building Internet of Things," 2021 18th Annual IEEE International Conference on Sensing, Communication, and Networking (IEEE SECON), 2021, pp. 1-9, doi: 10.1109/SECON52354.2021.9491621.
[43] Samar SH. Haytamy, Hisham A. Kholidy, Fatma A. Omara, "Integrated Cloud Services Dataset", Springer, Lecture Note in Computer Science, ISBN 978-3-319-94471-5, https://doi.org/10.1007/978-3-319-94472-2. 14th World Congress on Services, 18-30. Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA.

[44] Hisham A. Kholidy, Ali Tekeoglu, Stefano Lannucci, Shamik Sengupta, Qian Chen, Sherif Abdelwahed, John Hamilton, “Attacks Detection in SCADA Systems Using an Improved Non- Nested Generalized Exemplars Algorithm", the 12th IEEE International Conference on Computer Engineering and Systems (ICCES 2017), published in February 2018.
[45] Stefano Iannucci, Hisham A. Kholidy Amrita Dhakar Ghimire, Rui Jia, Sherif Abdelwahed, Ioana Banicescu, “A Comparison of Graph-Based Synthetic Data Generators for Benchmarking Next-Generation Intrusion Detection Systems”, IEEE Cluster, Sept 5 2017, Hawaii, USA.
[46] Qian Chen, Hisham A. Kholidy, Sherif Abdelwahed, John Hamilton, "Towards Realizing a Distributed Event and Intrusion Detection System", the International Conference on Future Network Systems and Security (FNSS 2017), Gainesville, Florida, USA, 31 August 2017.
[47] Hisham A. Kholidy, Abdelkarim Erradi, “A Cost-Aware Model for Risk Mitigation in Cloud Computing Systems”, 12th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Marrakech, Morocco, November, 2015.
[48] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, “Attack Prediction Models for Cloud Intrusion Detection Systems”, in the International Conference on Artificial Intelligence, Modelling and Simulation (AIMS2014), Madrid, Spain, November 2014.
[49] Hisham A. Kholidy, Ahmed M. Yousouf, Abdelkarim Erradi, Hisham A. Ali, Sherif Abdelwahed, "A Finite Context Intrusion Prediction Model for Cloud Systems with a Probabilistic Suffix Tree", in the 8th European Modelling Symposium on Mathematical Modelling and Computer Simulation, Pisa, Italy, October 2014.
[50] Hisham A. Kholidy, A. Erradi, S. Abdelwahed, “Online Risk Assessment and Prediction Models For Autonomic Cloud Intrusion Prevention Systems”, in the “11th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), Doha, Qatar, November 2014.
[51] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Abdulrahman Azab, “A Finite State Hidden Markov Model for Predicting Multistage Attacks in Cloud Systems", in the 12th IEEE International Conference on Dependable, Autonomic and Secure Computing (DASC), Dalian, China, August 2014.
[52] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, “A Hierarchical, Autonomous, and Forecasting Cloud IDS”, the 5th Int. Conference on Modeling, Identification and Control (ICMIC2013), Cairo, Aug31-Sept 1-2, 2013.
[53] Hisham A. Kholidy, Abdelkarim Erradi, Sherif Abdelwahed, Fabrizio Baiardi, “HA- CIDS: A Hierarchical and Autonomous IDS for Cloud Environments”, Fifth International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN) Madrid, Spain, June 2013.
[54] Hisham A. Kholidy, Fabrizio Baiardi, "CIDD: A Cloud Intrusion Detection Dataset for Cloud Computing and Masquerade Attacks", the 9th International Conference on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012.
[55] Hisham A. Kholidy, Fabrizio Baiardi, "CIDS: A framework for Intrusion Detection in Cloud Systems", The 9th International Conf. on Information Technology: New Generations (ITNG), Las Vegas, Nevada, USA, 2012.
[56] Hisham A. Kholidy, Chatterjee N., "Towards Developing an Arabic Word Alignment Annotation Tool with Some Arabic Alignment Guidelines", the 2010 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp 778-783, Cairo, Egypt, vol. IEEE Catalog Number: CFP10394-CDR, 2010.
[57] Hisham A. Kholidy, Khaled S. Algathber, "A New Accelerated RC4 Scheme using "Ultra Gridsec" and "HIMAN", 5th Int. Conference on Information Assurance and Security, Aug 2009, China.
[58] Hisham A Kholidy, A. Azab, S. Deif, "Enhanced ULTRA GRIDSEC: Enhancing High- Performance Symmetric Key Cryptography Schema Using Pure Peer-to-Peer Computational Grid Middleware (HIMAN)", IEEE-ICPCA (the 3rd Int. Conf. on Pervasive Computing and Applications, 06-08 Oct 2008.
[59] A. Azab, Hisham A Kholidy, "An Adaptive Decentralized Scheduling Mechanism for Peer-to-Peer Desktop Grids", International Conference on Computer Engineering & Systems Nov 2008.
[60] Mostafa-Sami M., Safia H D., Hisham A Kholidy, "ULTRAGRIDSEC: Peer-to-Peer Computational Grid Middleware Security Using High-Performance Symmetric Key Cryptography" in IEEE-ITNG (5th Int. Conf. On Information Technology-New Generations), LasVegas, Nevada, USA, 7-9 April 2008.
[61] Mohammed Arshad, Patel Tirth, Hisham Kholidy, “Deception Technology: A Method to Reduce the Attack Exposure Time of a SCADA System”, https://dspace.sunyconnect.suny.edu/handle/1951/70148,
[62] Akshay Bhoite, Diwash Basnet, Hisham Kholidy, “Risk Evaluation for Campus Area Network”, https://dspace.sunyconnect.suny.edu/handle/1951/70162
[63] Malkoc, M., & Kholidy, H. A. (2023). 5G Network Slicing: Analysis of Multiple Machine Learning Classifiers. ArXiv. /abs/2310.01747.
[64] Fathy M. Mustafa, Hisham A. Kholidy, Ahmed F. Sayed et al. Distributed Backward Pumped Raman Amplifier Gain Enhancement: New Approaches, 06 April 2023, available at Research Square [https://doi.org/10.21203/rs.3.rs-2770728/v1]
[65] Grippo, T., & Kholidy, H. A. (2022). Detecting Forged Kerberos Tickets in an Active Directory Environment. arXiv. https://doi.org/10.48550/arXiv.2301.00044
[66] Zielinski, D., & Kholidy, H. A. (2022). An Analysis of Honeypots and their Impact as a Cyber Deception Tactic. arXiv. https://doi.org/10.48550/arXiv.2301.00045
[67] Kholidy, H. A., & Abuzamak, M. (2022). 5G Network Management, Orchestration, and Architecture: A Practical Study of the MonB5G project. arXiv. https://doi.org/10.48550/arXiv.2212.13747
[68] Abuzamak, M., & Kholidy, H. (2022). UAV Based 5G Network: A Practical Survey Study. arXiv. https://doi.org/10.48550/arXiv.2212.13329

[69] Kholidy, H. A., Rahman, M. A., Karam, A., & Akhtar, Z. (2022). Secure Spectrum and Resource Sharing for 5G Networks using a Blockchain-based Decentralized Trusted Computing Platform. arXiv. https://doi.org/10.48550/arXiv.2201.00484
[70] Kholidy, H. A. (2021). State Compression and Quantitative Assessment Model for Assessing Security Risks in the Oil and Gas Transmission Systems. arXiv. https://doi.org/10.48550/arXiv.2112.14137
[71] Kholidy, H. A. (2021). A Triangular Fuzzy based Multicriteria Decision Making Approach for Assessing Security Risks in 5G Networks. arXiv. https://doi.org/10.48550/arXiv.2112.13072
[72] Haque, N. I., Rahman, M. A., Chen, D., & Kholidy, H. (2021). BIoTA Control-Aware Attack Analytics for Building Internet of Things. arXiv. https://doi.org/10.48550/arXiv.2107.14136
[73] Kholidy, H. A. (2020). Cloud-SCADA Penetrate: Practical Implementation for Hacking Cloud Computing and Critical SCADA Systems. Department of Computer and Network Security, College of Engineering, SUNY Polytechnic Institute. http://hdl.handle.net/20.500.12648/1605
[74] Hisham A. Kholidy, Abdelkader Berrouachedi, Elhadj Benkhelifa and Rakia Jaziri, "Enhancing Security in 5G Networks: A Hybrid Machine Learning Approach for Attack Classification", the 10th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), December 4-7, Cairo, Egypt.
[75] Soufiane Hamadache, Elhadj Benkhelifa, Hisham kholidy,Pradeeban Kathiravelu, Brij B Gupta, "Leveraging SDN for Real World Windfarm Process Automation Architectures", The 10th International Conference on Software Defined Systems (SDS-2023) San Antonio, Texas , USA. October 23-25.
[76] Adda Boulem, Abdelkader Berrouachedi, Marwane Ayaida, Hisham Kholidy and Elhadj Benkhelifa, "A New Hybrid Cipher based on Prime Numbers Generation Complexity: Application in Securing 5G Networks", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.
[77] Meriem Chiraz zouzou, mohamed shahawy, Elhadj Benkhelifa and Hisham Kholidy, “SIoTSim: Simulator for Social Internet of Things”, The 10th International Conference on Internet of Things: Systems, Management and Security (IOTSMS 2023). San Antonio, Texas, USA. October, 2023.
[78] Hisham A. Kholidy, Keven Disen, Andrew Karam, Elhadj Benkhelifa, Mohammad A. Rahman, Atta-Ur Rahman, Ibrahim Almazyad, Ahmed F. Sayed and Rakia Jaziri, "Secure the 5G and Beyond Networks with Zero Trust and Access Control Systems for Cloud Native Architectures", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.
[79] Ibrahim Almazyad, Sicong Shao, Salim Hariri and Hisham Kholidy, “Anomaly Behavior Analysis of Smart Water Treatment Facility Service: Design, Analysis and Evaluation”, the 10th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA), December 4-7, Cairo, Egypt.
[80] Abdulbast A Abushgra, Hisham A Kholidy, Abdelkader Berrouachedi and Rakia Jaziri, "Innovative Routing Solutions: Centralized Hypercube Routing Among Multiple Clusters in 5G Networks", the IEEE Federated Architectures & Testbeds Workshop on 5G and Beyond (FATW5G 2023), December 6-7, Smart Village Giza, Egypt.
[81] Adda Boulem, Cyril De Runz, Hisham Kholidy, Abdelmalek Bengheni, Djahida Taib, Marwane Ayaida, “A New Classification of Target Coverage Models in WSNs, Survey and Algorithms and Future Directions”, The 7th International Conference on Information and Computer Technologies (ICICT 2024), March 15-17, Honolulu, Hawaii.