SUNY POLYTECHNIC INSTITUTE

X-Infinity Research Group

X-Infinity Research Group

College of Engineering

Annual Report of Research & Scholarly Activities

Faculty Members:	***Research Topics:***
Dr. Bruno Andriamanalimanana[†]	Topics{1-2-3}
Dr. Chen-Fu Chiang[†]	Topics{1-2-3}
Dr. Sam Sengupta[†]	Topics{1-2-3}
Dr. Jorge Novillo[†]	Topics{1-2-3}
Dr. Ali Tekeoğlu[‡]	Topics{1-2-3}
Dr. Korkut Bekiroğlu[§]	Topic{2}
Dr. Michael Reale[†]	Topic{2}
Students:	
Ibraheem Aljamal, *M.Sc.*[†]	Topic{2}
Aaron Gregory, *B.Sc.*[†]	Topic{2}

Departments:

[†]Computer Science

[‡]Network Computer Security

[§]Electrical Engineering Technology

Scope:
Our team consists of researchers with diverse backgrounds including; computer science, mathematical modeling, quantum computing, cryptography, computer vision and cybersecurity. Scope of our interdisciplinary research encompasses three main fields; *(I) Blockchain Research*, *(II) Machine Learning and Artificial Intelligence*, *(III) Post-Quantum Cryptography*. In each of these areas, we are developing and implementing, novel innovative approaches to improve state-of-art. Particularly, scope of Blockchain research so far has been on improving performance of transactions in Distributed Ledger systems, by investigating and exploring efficiently operational architectures. Machine Learning/AI Research started off with developing methods for intrusion/anomaly detection in cloud hyper-visors. Quantum Cryptography research is focusing on review and improvement of post-quantum cryptographic algorithms and methods that would replace the current cryptographic algorithms in presence of super fast quantum computers.

Goals:
Our research goals for three areas can be summarized as follows (I) Identify a normative semi-synchronous delivery architecture model with performance better than IOTA-Tangle. Implementation of the proposed model and deployment in SUNY campuses for purposes such as secure and safe student information archival, secure voting for school related surveys, automation of school processes with smart-contracts on blockchain, (II) To explore and investigate the process of Anomaly Detection, and Intrusion Detection using new Information Theoretic frameworks, (III) To explore and investigate Lattice based cryptography deemed to be quantum resistant.

2018 Accomplishments:
Four papers introducing and outlining a new model architecture were presented at two international conferences both sponsored by IEEE. Student member presented his Master's project[5]. One ML workshop paper submitted to an IEEE conference, pending review.

Topic 1: Blockchain Research

To keep a distributed ledger system at its optimal performance, it is necessary to utilize the resources and avoid latency in its network. To achieve this goal, dynamically and efficiently injecting the unverified transactions to enable synchronicity based on the current system configuration and the traffic of the network is crucial. To reduce latency and provide optimization, we offer [1, 2, 3, 4] a distributed ledger architecture, Tango, that is based on the Iota-Tangle distributed system. We model periodic pulsed injections into the evaluation layer from the entry layer, as shown in Figure 1. To meet this need, we introduced four protocols: Decentralized Semi-synchronous Pulse Diffusion (DSPD) protocol [4], Pulsed Injection of Transactions into the Evaluation Corridor (PITEC) protocol[3], Pulsed Transaction Injection Parameterization (PTIP) protocol and Verification Performance Optimizer (VPO) protocol [1].

The DSPD Protocol lays out the roles of the participants in the network and introduces the diffusion mechanism for the controllers to provide semi-synchronicity to the system. The diffusion speed is dependent on the p2p network performance. The PITEC Protocol simulates the inventory system by estimating the optimal pulse injection size to be released for the verifiers at each periodic cycle in order to keep the system's performance. The PTIP protocol regulates the injection volume based on the performance from previous verification cycle. The VPO takes the capacity of the verifiers pool as a constraint to optimize for various house policies. We observed that under property construction of the system, we can refine the parameters to integers such that dynamic programming to offer us a pseudo-polynomial complexity to solve this NP-hard optimization problem.

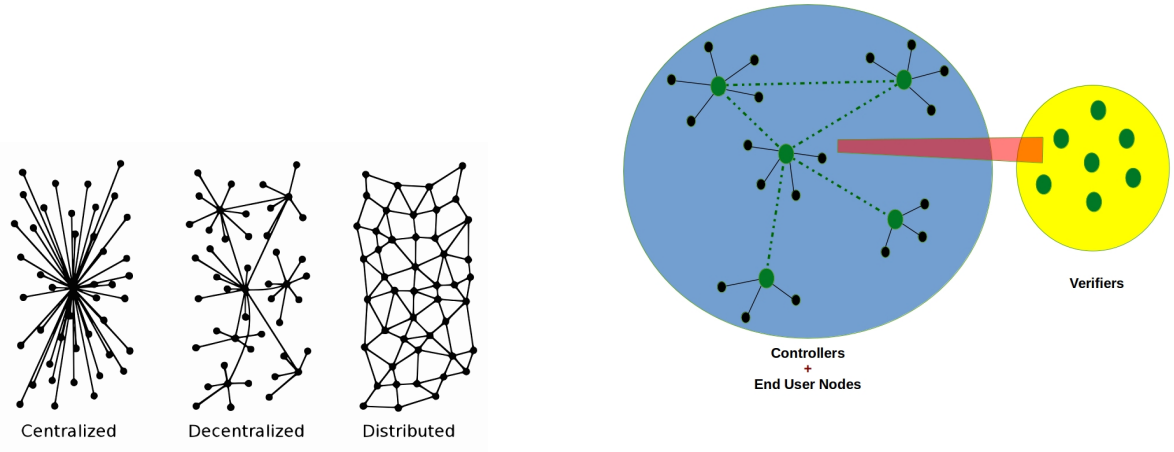

Figure 1: *(*left) Centralized, Decentralized vs Distributed Computing. *(right)* Proposed model of verifiers, controllers and end-user nodes.

Future work:
Further latency reduction, Tango system simulation, optimization

Topic 2: Machine Learning/AI Research

Intrusion Detection systems for Cloud Hypervisors are vital due to the amount of Virtual Machines that would be affected in a possible compromise. A Cloud Hypervisor orchestrates, manages many Virtual Machines, and their central role in cloud computing made them a target for the attackers. Intrusion detection has been mostly relied on signature-based detection of malicious behaviour. However, when a new type of attack occurs it won't have a signature in the Intrusion Detection system's database. In those cases, behaviour based anomaly detection produces better results in detection. In this work, we have started with a data-set provided by University of Victoria's ISOT lab, which includes 2 weeks of logs, including network packet captures; memory dumps; disk, memory, CPU usage statistics; and more. The proposed method of anomaly detection only used vmstat and iostat command output generated on the cloud hypervisor, and developed algorithms to detect anomalies which indicates attacks. For anomaly detection we have evaluated values in the data-set in a sliding time window, where for each window a KL value is calculated and compared to the 3 previous windows, as shown in Figure 2. Our team open-sources the developed and implemented methods for anomaly detection [6] [7].

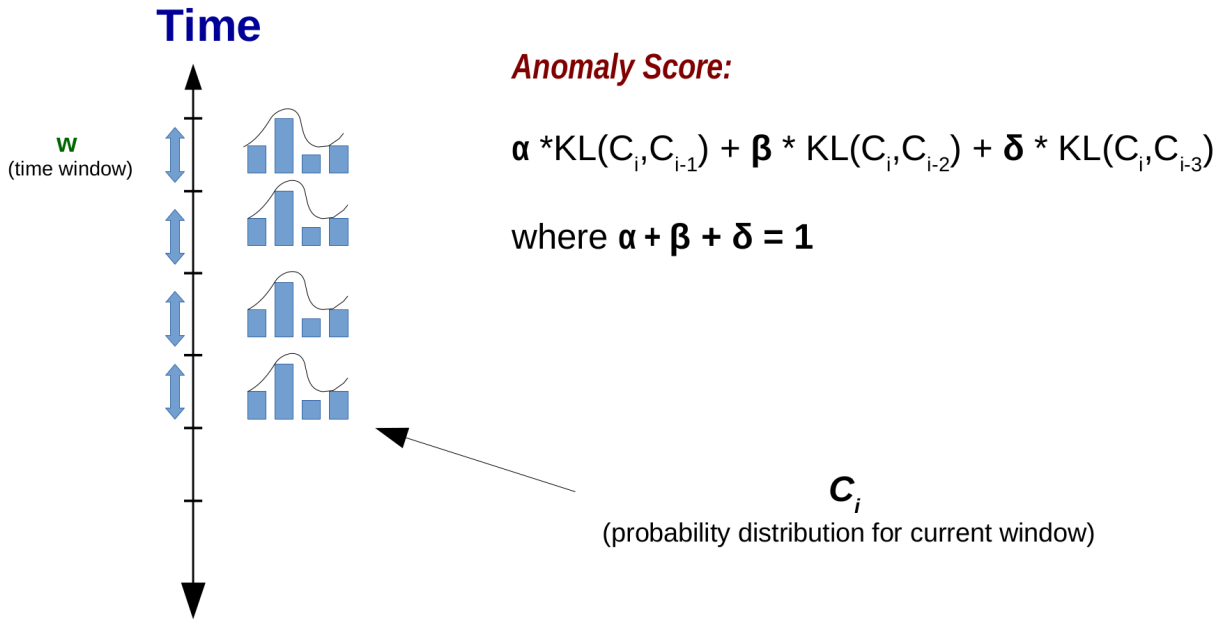

Figure 2: Proposed method of anomaly score calculation

Topic 3: Post-Quantum Cryptography Research

Cybersecurity has become a necessity for today's digital world. Cryptography has played an extremely critical role in cybersecurity for defending the privacy and integrity of the data. However, with recent advances in quantum technologies, it is likely many existing commonly used cryptosystems will be broken by quantum computers. Post-quantum cryptography is cryptography under the assumption that the attacker has a large quantum computer; post-quantum cryptosystems strive to remain secure even in this scenario. It is known that hard instances of NP-complete problems cannot be solved "exactly" and "efficiently" by quantum computers. There are many candidate problems, such as shortest vector problem and closest vector problem in a lattice system, that can be further designed and used for post-quantum cryptography. This relatively young research area has seen some successes in identifying mathematical operations for which quantum algorithms offer little advantage in speed, and then building cryptographic systems around those. The central challenge in post-quantum cryptography is to meet demands for cryptographic usability and flexibility without sacrificing confidence.

We are exploring and investigating Lattice (Figure 3) based cryptography which is deemed to be quantum resistant. Research continues in this area.

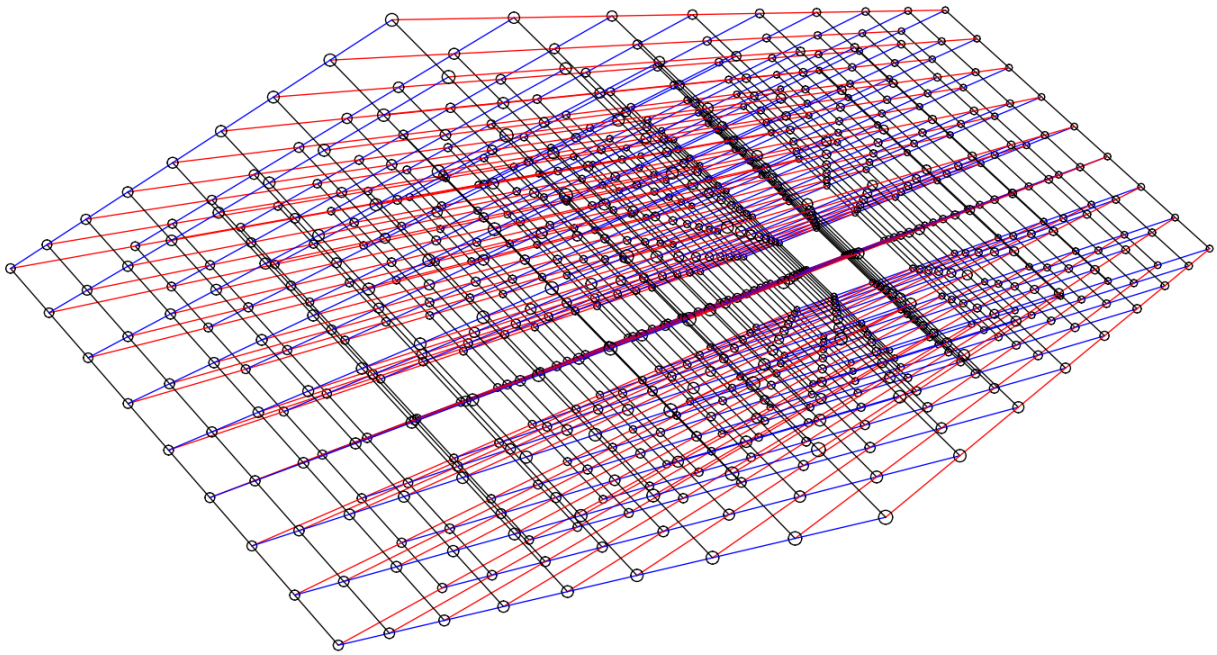

Figure 3: Perspective view of a 9×9×9 subset of a non-orthogonal three-dimensional lattice. Lattice-based cryptography hides a point in a high-dimensional lattice mod q by making small changes to all coordinates. Code-based cryptography hides a point in a very-high-dimensional lattice mod 2 by changing some coordinates.

References

[1] Bruno Andriamanalimanana, Chen-Fu Chiang, Saumendra Sengupta, Jorge Novillo and Ali Tekeoglu, *"Parameterized Pulsed Transaction Injection Computation Model And Performance Optimizer For IOTA-Tango"* 13th Int.Conf.on P2P, Parallel, Grid, Cloud and Internet Computing. Taiwan, October 27-29, 2018

[2] Bruno Andriamanalimanana, Chen-Fu Chiang, Saumendra Sengupta, Jorge Novillo and Ali Tekeoglu, *"Semi-Synchronocity Enabling Protocol and Pulsed Injection Protocol For A Distributed Ledger System"* 13th Int.Conf.on P2P, Parallel, Grid, Cloud and Internet Computing(3PGCIC). Taiwan, October 27-29, 2018

[3] Bruno Andriamanalimanana, Chen-Fu Chiang, Saumendra Sengupta, Jorge Novillo and Ali Tekeoglu, *"A Probabilistic Model of Periodic Pulsed Transaction Injection"*, The 2nd Cyber Security In Networking Conference (CSNet'18), Paris, France, October 24-26, 2018.

[4] Bruno Andriamanalimanana, Chen-Fu Chiang, Saumendra Sengupta, Jorge Novillo and Ali Tekeoglu, *"Tango: The Beginning - A Semi-Synchronous Iota-Tangle Type Distributed Ledger with Periodic Pulsed Entries"*, The 2nd Cyber Security In Networking Conference (CSNet'18), Paris, France, October 24-26, 2018.

[5] Ibraheem Aljamal, Master of Science in Computer Science Final Project, *"Hybrid Intrusion Detection System Using Machine Learning Techniques in Cloud Computing Environments"*, presented December'18.

[6] X-Infinity Research Group Website.
`http://www.cs.sunyit.edu/~chiangc/xinfinity/`

[7] Machine Learning Methods for Anomaly Detection in Cloud Hypervisors
`https://github.com/aliteke/mlintrusiondetection`