School of Mathematical and Statistical Sciences
Arizona State University

M E M O R A N D U M

DATE: 06/02/2023

TO: Faculty and Students

FROM: Professor(s) Chair/Co-Chairs of Defense for the PhD Committee Members

Nicolas Lanchier
Axel La Salle
Petar Jevtic

in Applied Mathematics

Dragan Boscovic
Rodrigo Platte
Sebastien Motsch

DEFENSE ANNOUNCEMENT

Candidate: Axel La Salle

Defense Date: 06-23-2023

Defense Time: 9:00 AM

Virtual Meeting Link: https://asu.zoom.us/j/86033016854 Live Attendance: WXLR 206

Title: On Stochastic Modeling Applications to Cybersecurity: Loss, Attack, and Detection

Please share this information with colleagues and other students, especially those studying in similar fields. Faculty and students are encouraged to attend. The defending candidate will give a 40-minute talk, after which the committee members will ask questions. There may be time for questions from those in attendance. However, guests are invited to attend as observers and will be excused when the committee begins its deliberations or if the committee wishes to question the candidate privately.

ABSTRACT
-See next page-

PO Box 871804 Tempe, AZ 85287-1804
(480) 965-3951 Fax: (480) 965-8119
http://math.asu.edu

ABSTRACT

The main objective of this work is to study novel stochastic modeling applications to cybersecurity aspects across three dimensions: Loss, attack, and detection. First, motivated by recent spatial stochastic models with cyber insurance applications, the first and second moments of the size of a typical cluster of bond percolation on finite graphs are studied. More precisely, having a finite graph where edges are independently open with the same probability p and a vertex z chosen uniformly at random, the goal is to find the first and second moments of the number of vertices in the cluster of open edges containing x. We derive exact expressions for the first and second moments of the size distribution of a bond percolation cluster on essential building blocks of hybrid graphs: the ring, the path, the random star, and regular graphs. We also give upper bounds for the moments when the graph is the random rooted tree with a given offspring distribution and a given finite radius using a coupling argument to compare the percolation model with branching processes. Although not realistic for network purposes, exact and approximations for these quantities are computed for the five Platonic solids. Second, the histo,y of the Petri Net modeling framework for performance analysis is well established; extensions provide enough flexibility to examine the behavior of a permissioned blockchain platform in the context of an ongoing cyberattack via simulation. The relationship between system performance and cyberattack configuration is analyzed. The simulations vary the blockchain's parameters and network structure revealing the factors that contribute positively or negatively to a sybil attack through the performance impact of the system. Lastly, denoising diffusion probabilistic models (DDPM) ability for synthetic tabular data augmentation isstudied. DDPMs surpass generative adversarial networks in improving computer vision classification tasks and image generation, for

example, stable diffusion. Extremely recent research and open-source implementations point to a strong quality of synthetic tabular data generation for classification and regression tasks. Unfortunately, the present state for literature concerning tabular data augmentation with DDPM for classification is lacking. Further, cyber datasets commonly have highly un-balancecl distributions complicating training. We investigate synthetic tabular data augmentation with cyber datasets and present performance improvements of well-known metrics in machine learning classification tasks.