BIOGRAPHICAL SKETCH

Niraj Rajbhandari was born in Kathmandu, Nepal. He completed his high school from National School of Sciences. After that, he received his Bachelor of Science in Computer Science and Information Technology from Tribhuvan University, Nepal in December 2011. For 3+ years he worked as a web application developer in Nepal. In August 2016, he started his Masters in Computer Science at Tennessee Tech University. He has also been working as a Graduate Teaching Assistant at TTU.

EDUCATION

B.S., Computer Science and Information Technology
Tribhuvan University, Nepal

College of Engineering

TENNESSEE TECH

The Department of

Computer Science

Announces the Thesis Defense

Of

Niraj Rajbhandari

In Partial Fulfillment of the Requirements

For the degree of

Master's of Science in Computer Science

4th April, 2018 at 4 pm

Held at

Bruner Hall, Room 206

University Drive

Tennessee Technological University

Cookeville, TN, 38505

FIELD OF STUDY

Computer Science

THESIS TOPIC

Graph Sampling to Detect Anomalies
In Large Graphs and Dynamic Graph Streams

EXAMINING COMMITTEE

Dr. William Eberle (Chairperson)

Dr. Doug Talbert (Committee member)

Dr. Sheikh Ghafoor (Committee member)

ABSTRACT

Network data is ubiquitous in a variety of domains such as mobile computing, telecommunications, and social networks. In order to analyze these networks of data for valuable structural information, it is sometimes useful to represent the data as graphs or graph streams. However, these underlying network graph streams are massive in size, which can be challenging to mine in terms of both memory and computational complexity. In order to address these challenges, we propose an approach that samples a large and dynamic graph stream and then uses the sampled graph to detect the anomalous structures with minimal loss in accuracy and precision over analyzing the graph stream in its entirety. In our experiments, we use datasets from different domains to evaluate the performance of our proposed system. We also compare the performance of our system against others where the entire original graph is processed. Finally, we demonstrate the effectiveness of applying this approach to detect potential suspicious activities.