INDIAN INSTITUTE OF TECHNOLOGY GUWAHATI
SHORT ABSTRACT OF THESIS

Name of the Student : RITESH RATTI

Roll Number : 156101013

Programme of Study : Ph.D.

Thesis Title: APPLICATION SPECIFIC NIDS (USING UNSUPERVISED TECHNIQUES)

Name of Thesis Supervisor(s) : Prof. SUKUMAR NANDI / Prof. SANASAM RANBIR SINGH

Thesis Submitted to the Department/ Center : COMPUTER SCIENCE & ENGINEERING

Date of completion of Thesis Viva-Voce Exam : 17-JUNE-2024

Key words for description of Thesis Work :

SHORT ABSTRACT

In recent years, the use of unsupervised learning-based methods for network intrusion detection has attracted much attention. Multiple methods using unsupervised mechanisms have been proposed that utilize the information in various formats like network packets, flow information, etc., and use various methods for attack identification. Most of these methods have the limitations on not considering the time factor inherently but explicitly using the time-dependent features for various time windows and considering equal importance for all previous contexts. Also ignoring the fact that each protocol-specific attack is unique and ignoring the protocol awareness to determine attacks. Moreover, considering a single type of view or set of features (network header or flow) to build a machine learning model and ignoring the importance of different views in attack determination. This thesis presents various unsupervised learning-based methods in this direction. One of the method proposes a network intrusion detection method by using a Time-aware LSTM autoencoder that uses the concept of regeneration error estimation on contextual data and predicts an attack if it is higher than the defined threshold. It considers the time decay inherently based on previous contextual information and leads to better overall metrics in comparison to other units like MLP / LSTM.. This research work further utilized the autoencoder-based method to build a protocol-aware system for attack detection. In this method, a Protocol aware unsupervised network intrusion detection method is proposed that provides a way to incorporate protocol channel importance while deciding attacks. The concept of protocol awareness is introduced by learning the local (protocol-specific) and global representation individually by protocol channels and incorporating the channel importance by utilizing an attention network. We also propose a multiview-based network intrusion detection system that is developed

by using a self-supervised learning-based method. In this method, the network packet level data is utilized to extract multiple possible views with predefined time windows consecutively and construct the autoencoder-based model specific to each view. Once the encoders for each specific view are created, this work proposes the strategy to build the self-supervised learning-based model using majority voting on the classified output from individual encoders. It is demonstrated that the proposed method outperforms the individual view-based mechanism when multiple views are utilized in computation. The last method is the online method for network attack detection by using an on-the-fly mechanism to create clusters and utilize the statistical features of computed clusters and compare the cluster profiles. Later on, the distance between cluster profiles is estimated and an attack is identified if the distance is more than the defined threshold. The proposed model executes in an online mode as it executes the algorithm for each discrete time window data generated through flows.

Ritesh Rathi