Anomaly based IDS for Ad-Hoc Networks

Anush MANGLANI, Tadrush DESAI

Institute of Technology, Nirma University

15bce009@nirmauni.ac.in
15bce028@nirmauni.ac.in

NIRMA UNIVERSITY
INSTITUTE OF TECHNOLOGY
NAAC ACCREDITED 'A' GRADE

Abstract

Ad hoc networks are used in heterogeneous environments like tactical military applications, where no centrally coordinated infrastructure is available. The network is required to perform self-configuration, dynamic topology management and ensure self-sustainability of the network. Security is hence of paramount importance. Anomaly based Intrusion Detection System (IDS) is a distributed activity, carried out by all nodes of the network in a cooperative manner along with other network related activities like routing etc. Machine Learning and its advances have found promising place in anomaly detection. This paper describes journey of defining the most suitable routing protocol for implementing IDS for tactical applications, along with the selection of the related suitable data-set. The paper also reviews the latest machine learning techniques, their implementation capabilities and limitations.

Introduction

Ad hoc networks are the self organizing and self maintaining wireless networks where, nodes communicate with each other in an infrastructure-less environment. The nodes with 802.11 radios are mobile and cooperate with each other for communicating the data and control packets in a coordinated and distributed fashion. In the absence of external support for managing the network, vulnerabilities are introduced in the network. In this distributed and cooperative environment, nodes are themselves responsible for ensuring secured communication and detecting internal as well as external intrusions or penetrations.

Literature Survey

Anomaly based IDS is able to filter out any malicious packet that may be existing in the network.Anomaly is detected using either the statistical analysis or using machine learning approaches. This mechanism plays an important role in the functioning of an IDS. The major setback of using statistical IDS is that, it is not able prevent or detect different types of malicious activities, because information regarding the activities need to be fed to the IDS before-hand. This isnt the case with machine learning based IDS, as they can be trained to recognize patterns that define the malicious activities instead of checking every packet for malicious behaviour.

- Clustering Based
- Classification Based
- Deep Learning Based
- Knowledge Based
- Statistical Based

Scope and Methodology

The nodes in the ad hoc network are capable of managing all network related tasks in a coordinated and distributed strategy. As the central infrastructure is not available to ad hoc networks, vulnerabilities are introduced in the network. Hence, the network and the nodes are to be equipped to handle these attacks. This section proposes the scope of the work and the methodology adopted for identifying the simulation parameters, dataset to be used and the implementation results to be considered.

Concerned Application

The success of mobile ad-hoc networks can be attributed to the fact that they are very well adapted for use in multiple scenarios where an underlying network infrastructure is not readily available or it is not feasible to set up one. An example of such a scenario which relies heavily on the versatility of ad hoc networks is Military or Army combat operations. For the execution of such operations, the army often gets deployed at remote geographical locations where the Global Positioning Systems (GPS) may be unreliable. In such circumstances, the capacity of the ad hoc nodes to quickly set up a channel for communication without any need for primary infrastructure grants the army unit a premeditated advantage over the enemy.

AODV Routing Protocol

The study shows that for tactical implementation Ad-hoc On-demand Distance Vector (AODV) protocol is the best suitable under heterogeneous circumstances. Hence, this poster primarily focuses on AODV routing protocol. By creating the routes on-demand rather than keeping the list of every route, AODV reduces the number of times the broadcast packets have to be sent. AODV uses bi-directional links for packet routing. The working of this protocol can be majorly classified into two categories, which are as follows:

- Route Discovery

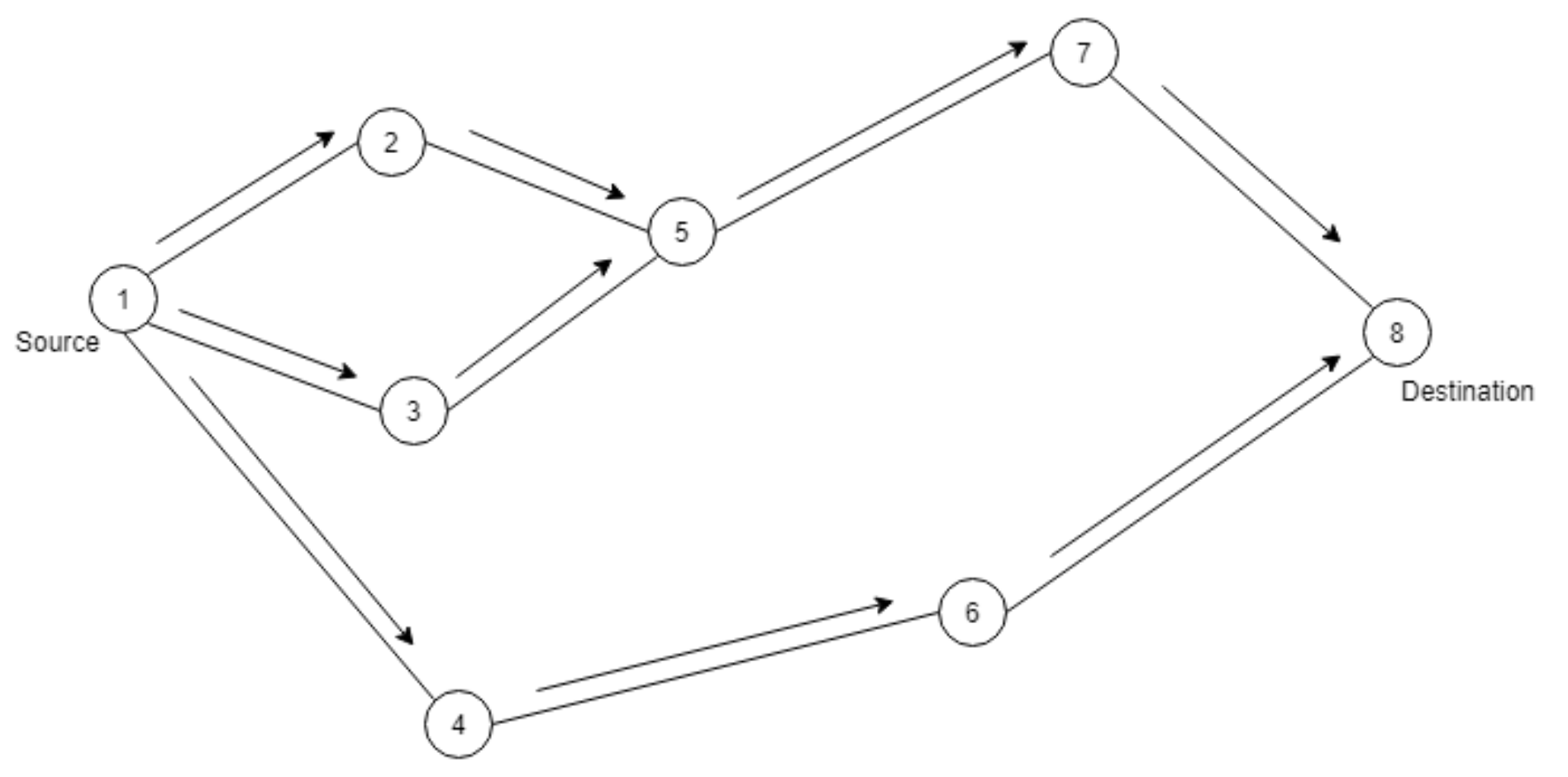

Figure 1: Propagation of Route Request (RReq) Packets

- Route Maintenance

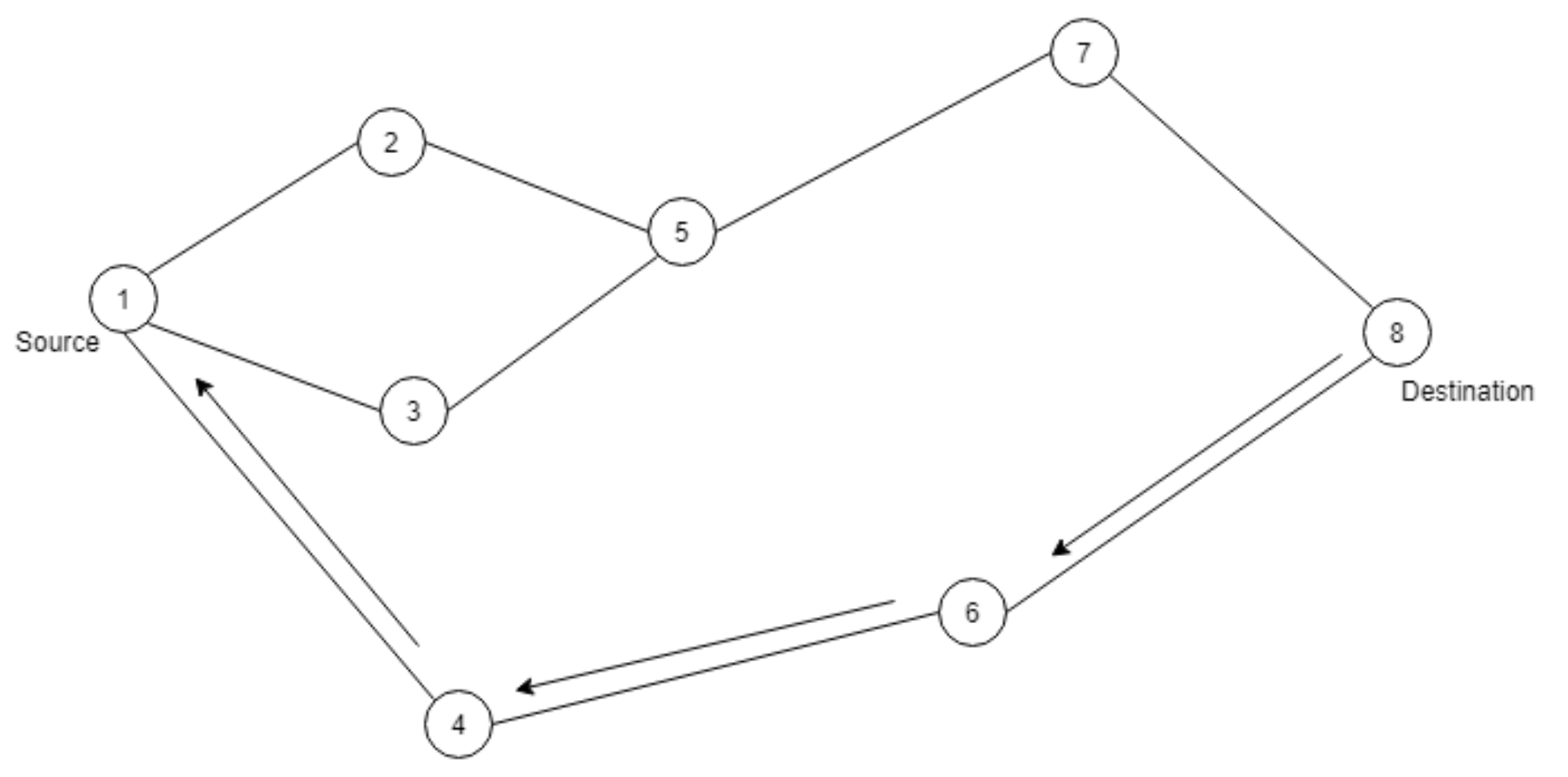

Figure 2: Path taken by Route Reply (RRep) Packets

Proposed Approach

For the development of an intrusion detection system that is accurate and works almost in real time, the approach that seems to be most suitable is the use of LSTM RNN. This is because LSTM RNN has the capability of learning long range dependencies and use that information before making any decisions in the current iteration. Therefore, we can make the model learn about the previously malicious activities and use that information in the future. This will help in reducing the number of route requests sent by the nodes in order to find a path from source to destination in the network, thereby increasing the efficiency of the network.

Frameworks

Today, we have a myriad of frameworks at our disposal that allows us to develop tools that can offer a better level of abstraction along with simplification of difficult programming challenges. Each framework is built in a different manner for different purposes. The fromaworks that we have use are as follows:

- TensorFlow
- Keras

Technology

LSTMs are explicitly designed to avoid the long-term dependencies. They find their use in a large variety of applications. Its their inherent nature to remember information across long periods of time. Similar to normal RNNs, LSTMs also have a chain like structure however, it is a bit different enabling LSTMs to retain information from across longer periods of time as shown in Fig. 3

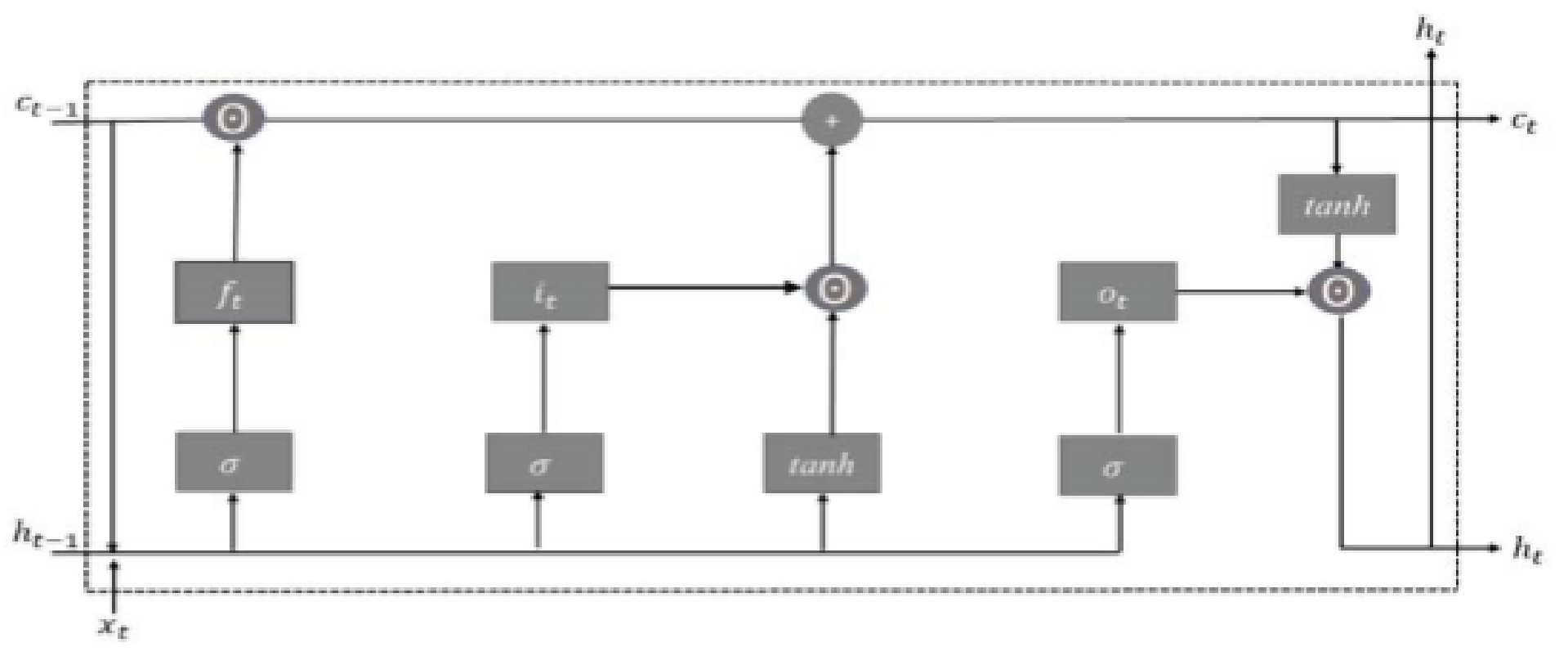

Figure 3: A single LSTM Unit

LSTMs have a cell state which is akin to a conveyor belt subjected to no or only a few moderations. They also have the capability of adding or removing information through carefully regulated structures called Gates. LSTMs have three of these gates, for controlling the information flow along the cell state.

$$f_t = \sigma(W_f.[h_{t-1}, x_t] + b_f) \tag{1}$$

$$i_t = \sigma(W_i.[h_{t-1}, x_t] + b_i) \tag{2}$$

$$\widetilde{C_t} = \tanh(W_C.[h_{t-1}, x_t] + b_C) \tag{3}$$

$$C_t = f_t * C_{t-1} + i_t * \widetilde{C_t} \tag{4}$$

$$o_t = \sigma(W_o.[h_{t-1}, x_t] + b_o) \tag{5}$$

$$h_t = o_t * \tanh(C_t) \tag{6}$$

Architecture

The below shown image Fig. 4 depicts the overall architecture of the proposed approach.

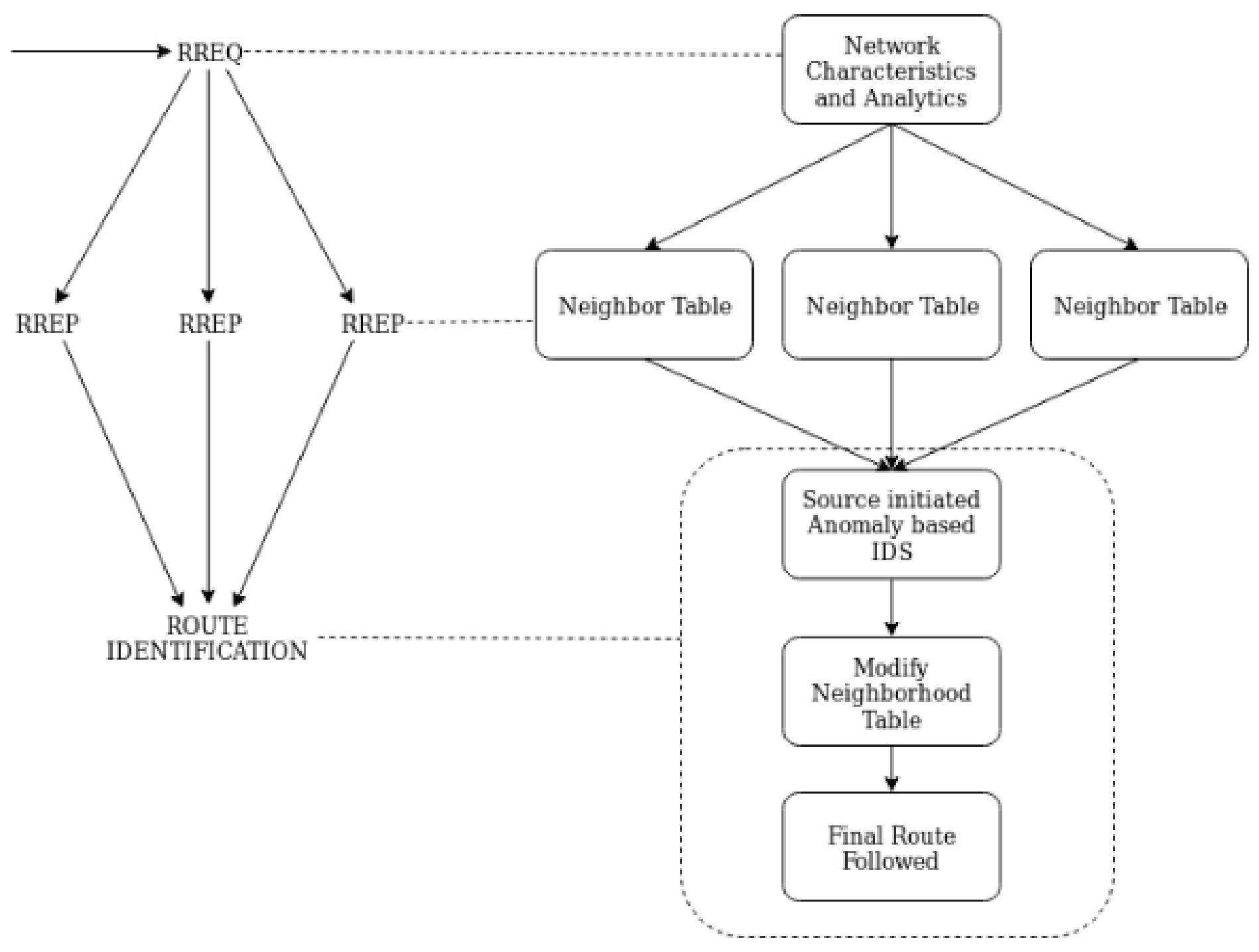
RREQ
Network Characteristics and Analytics
RREP
RREP
RREP
Neighbor Table
Neighbor Table
Neighbor Table
Source initiated Anomaly based IDS
ROUTE IDENTIFICATION
Modify Neighborhood Table
Final Route Followed

Figure 4: The Architecture of our IDS

1 Results

The accuracy for Binary and Multi-class classification are as follows:

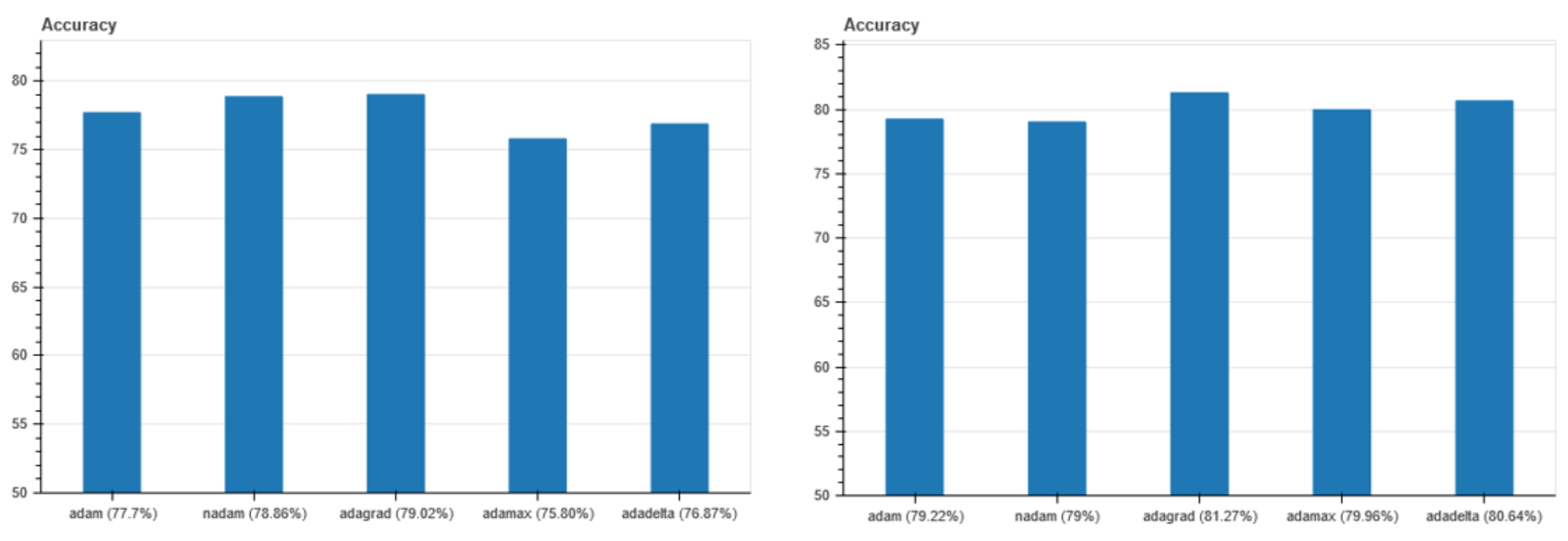

Figure 5: Accuracy of Binary and Multi-class Classification

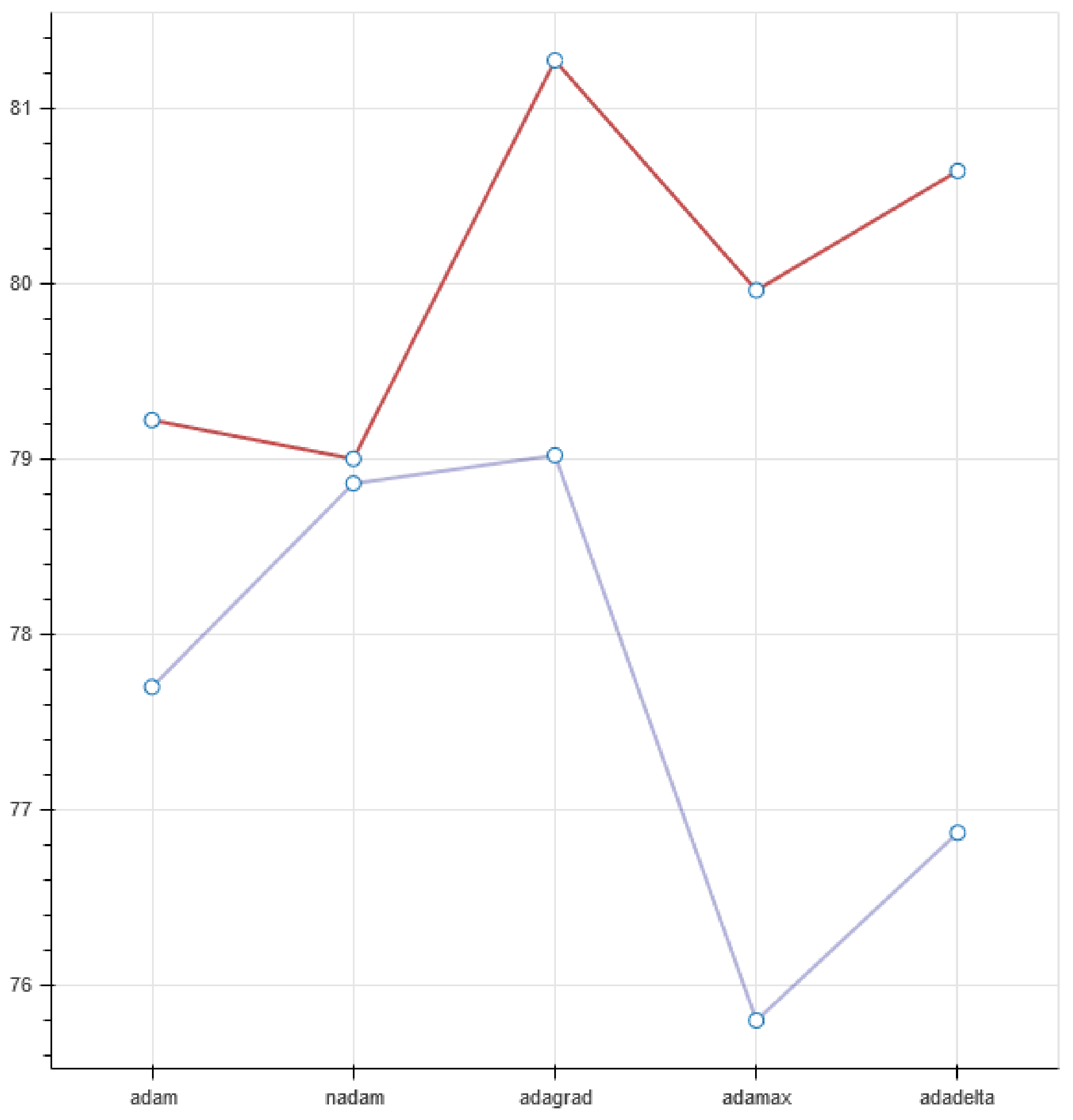

Figure 6: Accuracy comparison

Conclusions

An anomaly based intrusion detection system used in tactical ad hoc netwok has to detect anomalies efficiently and without compromising upon the QoS standards. Therefore, wisdom is needed to select suitable underlying technique among various options like machine learning, deep learning, or statistical analysis. A thorough comparison between all the currently available intrusion detection systems and their algorithms are presented. Research shows that AODV has been used as the routing protocol for tactical military applications. NSL-KDD dataset and CICIDS dataset are suitable for ensuring proper implementation and verification with required pre-processing of these datasets. Lack of pre-processing of the dataset might lead to imprecise results when implementing using any statistical, machine learning or deep learning techniques. Several papers have also shown development of customized data-sets for implementing the IDS framework. used.