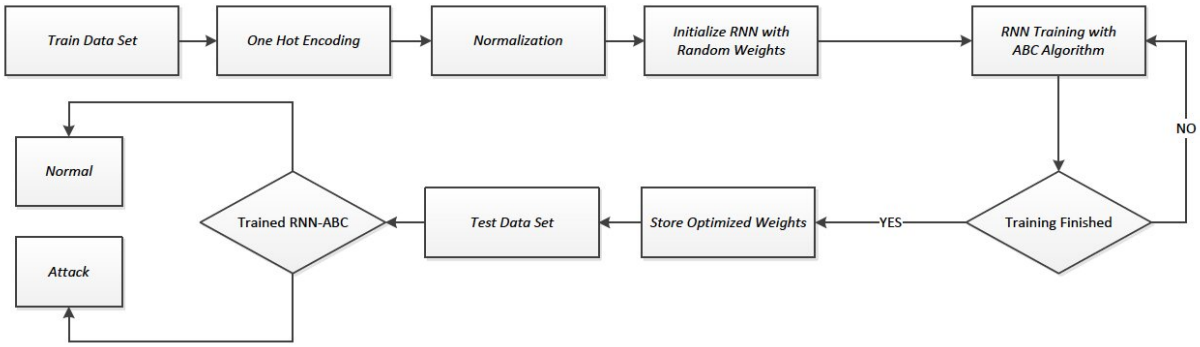
A model to classify cyberattacks using swarm intelligence

November 22 2019, by Ingrid Fadelli



A figure explaining how the RNN-ABC method proposed by the researchers works. Credit: Qureshi et al.

In recent years, new technological advances have led to a growing number of devices, ranging from more conventional computers to other gadgets and smart home appliances, communicating and sharing data with one another. Despite its advantages, this growing interconnection between devices, known as the Internet of Things (IoT), poses serious security threats.

In fact, as more devices share data over the internet, this data becomes exposed to cyberattacks, which are becoming increasingly frequent and sophisticated. Three types of attacks currently seen as the greatest threats

to IoT devices are denial-of-service (DoS), man-in-the-middle and SQL attacks.

Aware of the risks associated with the continuous increase in IoT devices, a team of researchers at Glasgow Caledonian University and COMSATS University in Pakistan have recently developed a new scheme that could help to protect sensitive information shared over the internet. This intrusion detection scheme, outlined in a paper presented at IEEE's 2019 China Emerging Technologies (UCET) conference, is based on an artificial bee colony (ABC) algorithm and a random neural network (RNN).

An ABC algorithm is an swarm intelligence optimization technique widely used in artificial intelligence (AI) research, which simulates the foraging behavior of honey bees to tackle practical and computational problems. A random neural network (RNN), on the other hand, is a class of a machine-learning models inspired by the behavior of biological neural networks in the human brain.

"In this paper, an anomaly-based intrusion detection scheme is proposed that can protect sensitive information and detect novel cyber-attacks," the researchers wrote in their paper. "The artificial bee colony (ABC) algorithm is used to train the random neural network (RNN) based system (RNN-ABC)".

The researchers trained their intrusion detection RNN-ABC scheme on the NSL-KDD Train+ dataset. NSL-KDD is a dataset used to train algorithms to detect cyberattacks, which contains a vast amount of internet traffic record data.

After training their RNN-ABC model on internet traffic data, the researchers carried out a series of tests to evaluate its performance in identifying and classifying cyberattacks. Their findings are highly

promising, as their scheme was able to classify new attacks with a remarkable accuracy of 91.65 percent.

In addition, the team compared the new model with an existing intrusion detection system based on a hybrid multiplayer perceptron (MLP), a type of artificial neural network (ANN) trained using a supervised learning technique known as backpropagation. Remarkably, they found that the RNN-ABC scheme significantly outperformed the MLP technique, as it generalized better across new data.

Interestingly, the researchers observed that their scheme's accuracy in classifying cyberattacks was greater when the colony size of its ABC swarm intelligence component was larger, thus, when more "artificial bees" contributed to the optimization of the model. In the future, their RNN-ABC intrusion detection method could be used to develop more efficient tools to identify cyberattacks on a variety of devices connected to the internet, ultimately enhancing the security of IoT networks.

More information: Ayyaz-Ul-Haq Qureshi et al. Intrusion Detection Using Swarm Intelligence, *2019 UK/China Emerging Technologies (UCET)* (2019). DOI: 10.1109/UCET.2019.8881840