Abstract No: SC-06 **Smart Computing**

A reinforcement learning approach to enhance the trust level of MANETs

***Gihani Jinarajadasa[1], Wayomi Jayantha[1], Lakmal Rupasinghe[1] and Iain Murray[2]**

[1]Faculty of Computing, Sri Lanka Institute of Information Technology, Sri Lanka
[2]Curtin University, Australia
**madhushikagihani@gmail.com*

Abstract

A Mobile ad-hoc network (MANET) consists of many freely interconnected and autonomous nodes that is often composed of mobile devices. MANETs are decentralized and self-organized wireless communication systems, which are able to arrange themselves in various ways and have no fixed infrastructure. Since MANETs are mobile, the network topology is changing rapidly and unpredictably. Because of this nature of mobility of the nodes in MANETs, the main problems that occur are unreliable communications and weak security where the data can be compromised or easily misused. Therefore, a trust enhancement approach to a MANET is proposed which is RLTM (Reinforcement Learning Trust Manager), a set of algorithms, considering Ad-hoc On-demand Distance Vector (AODV) protocol as the specific protocol, via Reinforcement Learning (RL) and Deep Learning concepts. The proposed system consists of RL agent, who learns to detect and give predictions on trustworthy nodes, reputed nodes, and malicious nodes and classifies them. The identified parameters from AODV simulation using Network Simulator-3(NS-3) were given to the designed RNN (Recurrent Neural Network) model and results were evaluated.

Keywords: Ad-hoc On-demand Distance Vector (AODV), Mobile-ad-hoc network (MANET), Reinforcement Learning (RL), Recurrent Neural Network (RNN)

Introduction

With the growth of the ubiquitous computing, the concepts of the Internet of Things (IoT) security or Wireless Network security have become an interesting research area through the past two decades. With the improvement of wireless communication technologies Mobile-ad-hoc network (MANETs) play a vital role, but there are some issues due to the direct effect of mobility of the nodes to the network environment such as unreliability of communication and weak physical protection. This may provide an opportunity for an adversary to steal or misuse the data. The reliability of the connectivity depend on the trust of each node. Because of these issues, many studies have been conducted to enhance the trust within MANETs. Jain (2015) defines the trust in Mobile Ad-hoc Networks simply as the adherence of a node to a given specific protocol where it can be an enabler of communication and cooperation. When compared to the infrastructure-based networks, since they have a dynamic topology, error-prone communication media, and energy constraining nodes, MANETs are more liable to malicious attacks and random failures (Li, et al., 2011). In Mobile ad-hoc networks, the corresponding functions such as network management, packet forwarding, and routing are carried by all available nodes without having a set of dedicated nodes for functioning. Therefore, one node can be captured by an adversary which may lead to node misbehaviour or non-cooperated behaviour with the rest of the nodes in the network and aims at damaging other nodes