A Trust based Advanced Machine Learning Approach for Mobile Ad-hoc Network Security

G. M. Jinarajadasa[1], S. R. Liyanage[2]

[1]*Department of Computer Systems Engineering, Sri Lanka Institute of Information Technology , Malabe, Sri Lanka*
[2]*Department of Software Engineering, University of Kelaniya, Kelaniya , Sri Lanka*

Mobile Ad-hoc Networks (MANETs) are one of the types of Wireless Ad-hoc Networks which consist of autonomous mobile nodes connected wirelessly. These are self-configured, less-infrastructure networks which are having highly dynamic topologies due to the frequent link changes in the network including the addition of new nodes, removal of existing nodes and etc. Because of this dynamic nature, various issues regarding the reliability of the communication and other security threats such as malicious attacks occur in MANETs. Since 'Trust' is the major factor which reliability and the security rely on, enhancing the trust in a MANET ensures that the security of the network environment is achieved. Over the recent past decade, a plenty of researches have been done in the related area including approaches of Machine Learning, Swarm Intelligence, Mobile Agents and Probabilistic Models. When comparing the different properties of each approach such as memory, computational power, flexibility to topology changes, the accuracy of results and cost, applying machine learning techniques has been efficient and accurate in providing results. Among Machine learning approaches reinforcement learning gains a more suitability for applied in mobile ad hoc networks since it gives more accurate results due to the ability to capturing the dynamic behaviour easily as well as no need for historical data to give predictions where it can give predictions on newly joined network nodes also. And when selecting the best algorithm because of the physical distribution of MANET information, an algorithm which has the ability to be distributed among the nodes has to be chosen. Instead of considering direct and indirect trust separately, it is recommended to apply a hybrid trust approach which aggregates the trust values. Hence, considering all this information the future research work is planned to be launch in the area of machine learning; specifically, in the area of reinforcement learning according to the analyzed results of early work. Therefore, this research work is proposing to develop a trust computational model, which uses an advanced machine learning mechanism to predict the trust value of each network node.

Keywords: Mobile Ad-hoc Networks, Malicious Attacks, Nodes, Trust

[a] Corresponding author.
E-mail address: *madhushikagihani@gmail.com*