Intelligent And Learnable Approaches For Intrusion Detection

Okan CAN,[1*] Murat AYDOS,[2]

[1]Turkish Air Force, Ankara,
[2]Hacettepe University, Computer Engineering Department, Ankara

In current time, using variety of computer systems and network structure in fields of economic, military, educational, social life, otomation systems and business e.g. increases day by day and as a matter of course number of users of computer systems multiplies excessively. As a result, academic studies and commercial products made for identifying, detecting and warding off cyber attacks are hot topics. Even cyber war is a new operational area in addition to land, air and maritime operational areas. Anymore it is more important protecting, processing, hiding and moving the data because of unreasonable progressing of information technologies so importance of cyber security has increased. There are two main approaches for serving a security solution. These approaches are prevention-based (encryption, authentication e.g.) and detection based (intrusion detection systems). Preventing approach is the first line and it sometimes can not be suitable for information systems because of their limited resources (processor, storage, energy e.g.). Wireless Sensor Networks can be an example for these systems having limited resources. Detecting approach is the second line for a security plan and it aims that maintaining deterrence for possible cyber attacks, detecting attacks earlier, detecting infraction occuring in the system, serving continuity for system security rules, gathering evidence about attacks coming true. IDS can be explained as a software or hardware that reporting internal and external attacks by observing the system. As mentioned above, there is not unlimited resources. Main motivation is creating an IDS structure consuming resources a bit for this study. If detecting attacks can be taught to an information system like a human, it knows how it act during an attack and consumes fewer resources. Artificial Neural Networks are used for solving problems that can not be formulated as an algorithm. People make learning by their brains and computers have some processor and storage devices too. With Neural Networks, it is aimed that creating a structure simulating human brains learning ability by these processor and storage devices. Learning is a comprehensive process. A learning system makes learning by adaption to environmental changes. Basically, a neural network provides learning by changing own components (Inputs from other neurons, propagation function, activation function, output function, outputs to other neurons and weights). In [Kaynak] an artificial neural network is trained by a supervised learning metodology and tested by KKD 91 training set on a computer. As test results, detection rate is 91.64%, success is 81.17% and false positive rate is 8.36 %. As a proposal, neuron weights can be got from [Kaynak1] and an artificial neural network can be implemented with these trained neuron weights on a WSN (as mentioned above WSN has limited resources). Because of WSN does not consume resource to train neural network, system uses fewer resources (*1*) (*2*) (*3*).

References

1. O. Can and O. K. Sahingoz, “An intrusion detection system based on neural network,” in *Signal Processing and Communications Applications Conference (SIU), 2015 23th.* IEEE, 2015, pp. 2302–2305.

2. C. Okan and O. K. Sahingoz, “A survey of intrusion detection systems in wireless sensor networks,” in *Modeling, Simulation, and Applied Optimization (ICMSAO), 2015 6th International Conference on*. IEEE, 2015, pp. 1–6.

3. O. Can and O. K. Sahingoz, “The architecture of mobile agent based intrusion detection system (mabdids),” in *Proceedings of the World Congress on Engineering*, vol. 1, 2014, London, pp. 432–437.