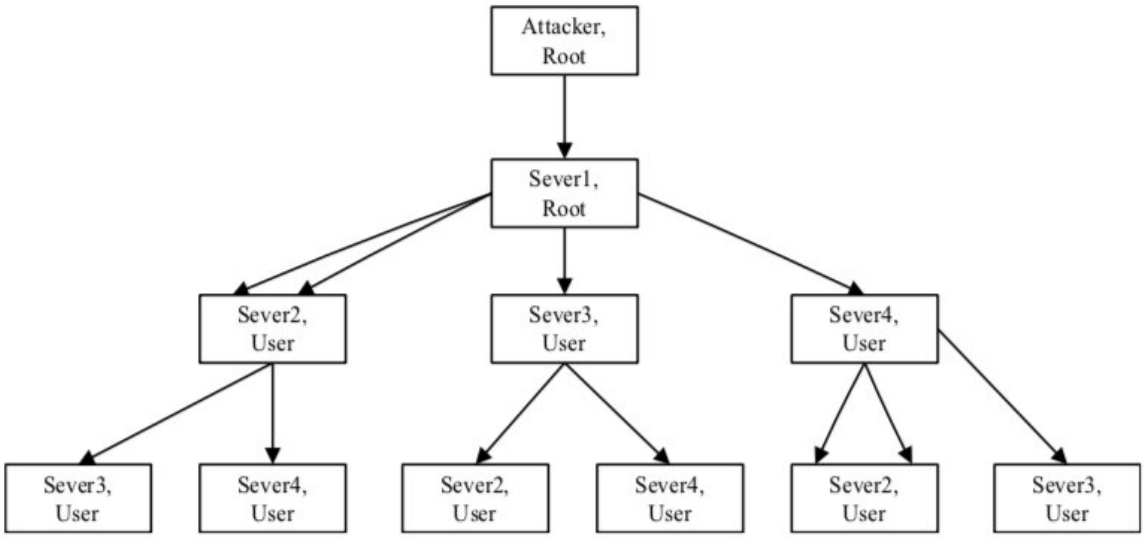
Defense against wireless attacks using a deep neural network and game theory

May 29 2019, by Ingrid Fadelli



State attack and defense map generated by the researchers' technique. Credit: Wang & Zhang.

A growing number of devices are now connected to the internet and are capable of collecting, sending and receiving data. This interconnection between devices, referred to as the Internet of Things (IoT), poses serious security threats, as cyberattackers can now target computers and smartphones, but also a vast array of other devices, such as tablets, smart

watches, smart home systems, transportation systems and so on.

For the time being, examples of large-scale IoT implementations (e.g. connected infrastructure, cities, etc.) are somewhat limited, yet they could soon become widespread, posing significant risks for businesses and public services that heavily rely on the internet in their daily operations. To mitigate these risks, researchers have been trying to develop security measures to protect devices connected to the internet from wireless network attacks.

To this end, two researchers at Baoji University of Arts and Sciences, in China, have recently developed a new method to defend devices in an IOT environment from wireless network attacks. Their approach, presented in a paper published in Springer's *International Journal of Wireless Information Networks*, combines a deep neural network with a model based on game theory, a branch of mathematics that proposes strategies for dealing with situations that entail competition between different parties.

"Firstly, according to the topology information of the network, the reachability relationship and the vulnerability information of the network, the method generates the state attack and defense map of the network," the researchers explained in their paper. "Based on the state attack and defense map, based on the non-cooperative non-zero-sum game model, an optimal attack and defense decision algorithm is proposed."

Essentially, their method generates a state attack and defense map based on network reachability and vulnerability information, which identifies all possible attack and defense paths. It then calculates the probability of success of each of these "attack paths," a hazard index and the utility value of different attack a defense strategies applicable when the network reaches particular security states. In addition, the interaction

between attack and defense is abstracted into a non-cooperative, non-zero and hybrid game model; a game theory framework applicable to problems related offense and defense.

This optimal attack and defense model also integrates prevention and control measures of vulnerable points. The method's fuzzy system then quantifies an information security risk factor index and feeds it to a radial basis function (RBF) neural network. To optimize and train the parameters of the RBF neural network, the researchers used a particle swarm optimization algorithm. Ultimately, all these steps allow their method to attain an optimized defense model.

In the future, the technique developed by this team of researchers could help to protect IoT devices against wireless network attacks. In a series of simulations evaluating its effectiveness, the defense algorithm performed remarkably well, with an average error below 2 percent.

"Simulation results show that the wireless network attack defense algorithm using a deep neural network combined with game model can solve the defects of subjective randomness and fuzzy conclusion of traditional wireless network attack defense methods," the researchers wrote in their paper. "The average error is less than 2 percent, and it is more traditional than machine learning algorithm that have higher fitting accuracy, greater learning ability, and faster convergence."

More information: Xifeng Wang et al. Wireless Network Attack Defense Algorithm Using Deep Neural Network in Internet of Things Environment, *International Journal of Wireless Information Networks* (2019). DOI: 10.1007/s10776-019-00430-1