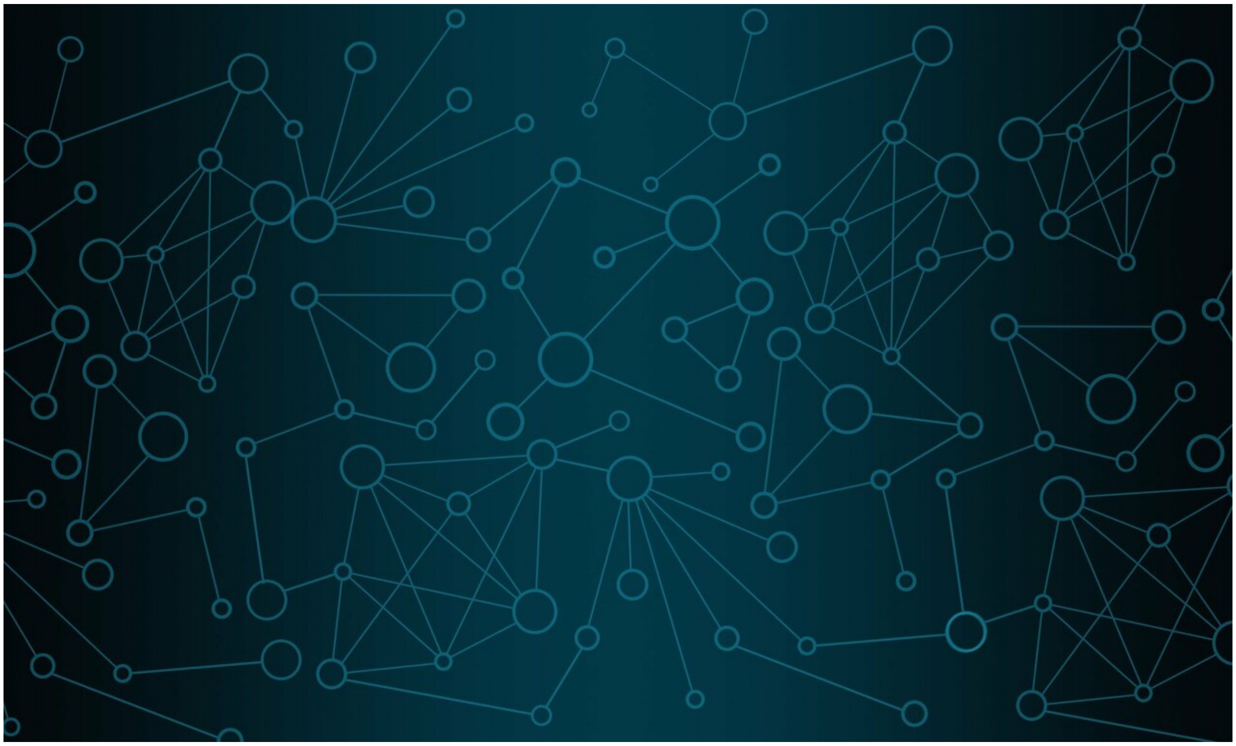
Tech Xplore

Saving the IoT from botnets

April 3 2020, by David Bradley



Credit: CC0 Public Domain

The advent of the Internet of Thing, essentially smart devices with connectivity to the internet has wrought many benefits, but with it comes the problem of how to cope with third party users with malicious or criminal intent.

Ivan Letteri, Giuseppe Della Penna, and Giovanni De Gasperis of the

Department of Information Engineering at the University of L'Aquila, Italy, writing in the International Journal of High Performance Computing and Networking have looked at an aspect of IoT insecurity, attacks on smart devices by so-called botnets. A botnet is a network of computers or other devices that have been repurposed by a third party, often surreptitiously and almost always with improper use the ultimate aim. The improper use might be for personal gain, financial or otherwise, sabotage or other destructive or disruptive purposes.

Botnets are propagated through malware and might be operated by malicious individuals, hacker groups, corporate entities, criminal gangs, organized crime cartels, or indeed rogue states. One particularly insidious purpose to which they are put is to apply a directed attack on a target's computers so that they are overwhelmed. Such a distributed denial of service attack, leads, as the name would suggest to disruption of the normal computing activities of the target. This might be simply for the purposes of sabotage, perhaps to interfere with the day to day operations of an individual, company or even a government. But, often the dDOS is carried out so that while the system is overwhelmed, its security might be breached at another exposed entry point.

With IoT and other networked smart devices being recruited by botnet operators for nefarious purposed, the team has focused on how such dDOS attacks might be detected and halted by the system using deep learning techniques. Obviously, it is difficult to distinguish between normal activity and activity from distributed sources that are designed to overwhelm a system. To the system, it simply sees lots of requests and knowing which are from genuine users and which malicious cannot easily be discerned. The team points out that with the rise of software-defined networking (SDN), which is increasingly replacing conventional networking in IoT, the problem is becoming more acute.

The team's deep learning approach has been tested on two state-of-theart frameworks, i.e., Keras and TensorFlow, and found to have 97 percent accuracy in detecting botnet attacks on the systems.

More information: Ivan Letteri et al. Security in the internet of things: botnet detection in software-defined networks by deep learning techniques, *International Journal of High Performance Computing and Networking* (2020). DOI: 10.1504/IJHPCN.2019.106095

Provided by Inderscience

Citation: Saving the IoT from botnets (2020, April 3) retrieved 9 April 2024 from https://techxplore.com/news/2020-04-iot-botnets.html