Ripple Down Models, a knowledge acquisition approach to detect network traffic anomaly.

Akara Prayote

In this talk, a traffic anomaly detection technique based on knowledge acquisition is presented. Rather than developing a sufficiently sophisticated model to represent the full range of normal traffic behaviour, the technique gradually adds models of a variety of seen patterns to a knowledge base. Each model covers a specific region in the problem space. Any novel or ad-hoc patterns can be covered easily. The approach uses two knowledge bases, i.e., the first is for capturing network behaviour, the latter for deciding whether enough parameters are anomalous to raise alarm.

Short CV:
Akara Prayote received his PhD in Computer Science and Engineering at the University of New South Wales, Australia, under supervision of Professor Paul Compton. He is now working at King Mongkut’s University of Technology North Bangkok. His research interest covers knowledge acquisition, network intrusion detection, network measurement.