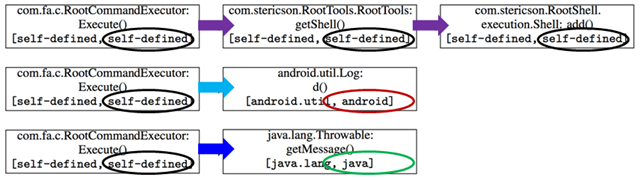
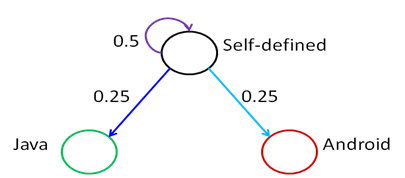
**MAMADROID: Detecting Android Malware by Building Markov Chains of Behavioral Models**

Android smartphones have become profitable targets for cybercriminals, allowing them to bypass two factor authentication or steal sensitive information such as credit cards details or login credentials.

In this example they have use Markov chains to detect the malware and to represent systems based on sequences of events as nodes and edges, representing states and transitions between a state and another one, after Sequence Extraction process to elaborate the probability of passing from one state to another.

The set of these probabilities will form our feature set (as a vector). In package mode there are 340 states and, as a consequence, 115,600 possible transitions; in family mode there are only 11 states and, therefore, 121 possible transitions.

Below we enhance the crucial information needed for the Markov Chain for our example: the arrows indicate the transition between nodes, while the nodes (using family abstraction) are the circles highlighting the family of the call. Then you can find the Markov Chain of the example, using the same colours.

Taking the previous example, the circles indicate the different family nodes, while the arrows indicate the transitions used for the Markov ChainsMarkov Chain generated from the example