Sample Bayesian Network for a Real Multi-Stage Attack

```
DIRECTED ACYCLIC GRAPH REPRESENTATION OF ATTACK SCENARIO
(v0.81 – 070925)

DESCRIPTION OF NODES

NODE 1: Attack step - ping or tracert to web servers

NODE 2: Attack step - run portscanner on web servers

NODE 3: Detector alert – IPTables

NODE 4: Attack step - exploit tdump vuln. on web server

NODE 5: Attack step - access web server admin site

NODE 6: Attack step - Brute force admin pwd

NODE 7: Detector alert – Snort

NODE 8: Attack step - Copy hacker tool to web server by using tftp

NODE 9: Attack step - Install vuln scanner on web server

NODE 10: Attack step - Run portscanner on internal network

NODE 11: Attack step - Install sniffer to capture pwd's

NODE 12: Attack step - Exploit rpc.idlid service on app controller

NODE 13: Detector alert – Libsafe

NODE 14: Attack step - Exploit remote vuln. on MySQL server

NODE 15: Attack step - Brute force root pwd on app controller

NODE 16: Attack step - Run SQLplus to execute queries on tables

NODE 17: Attack step - Connect to MySQL server with admin account

NODE 18: Attack step - Read customer data table

NODE 19: Attack step - Copy customer credit card list

NODE 20: Detector alert - Database IDS (Application Security DbProtect)
```
Difference between the marginal probability of a node in the Bayesian Network above (without any detector information) and conditional probability of the node with the detector alert

The difference is shown as a function of the distance between the detector and the node.