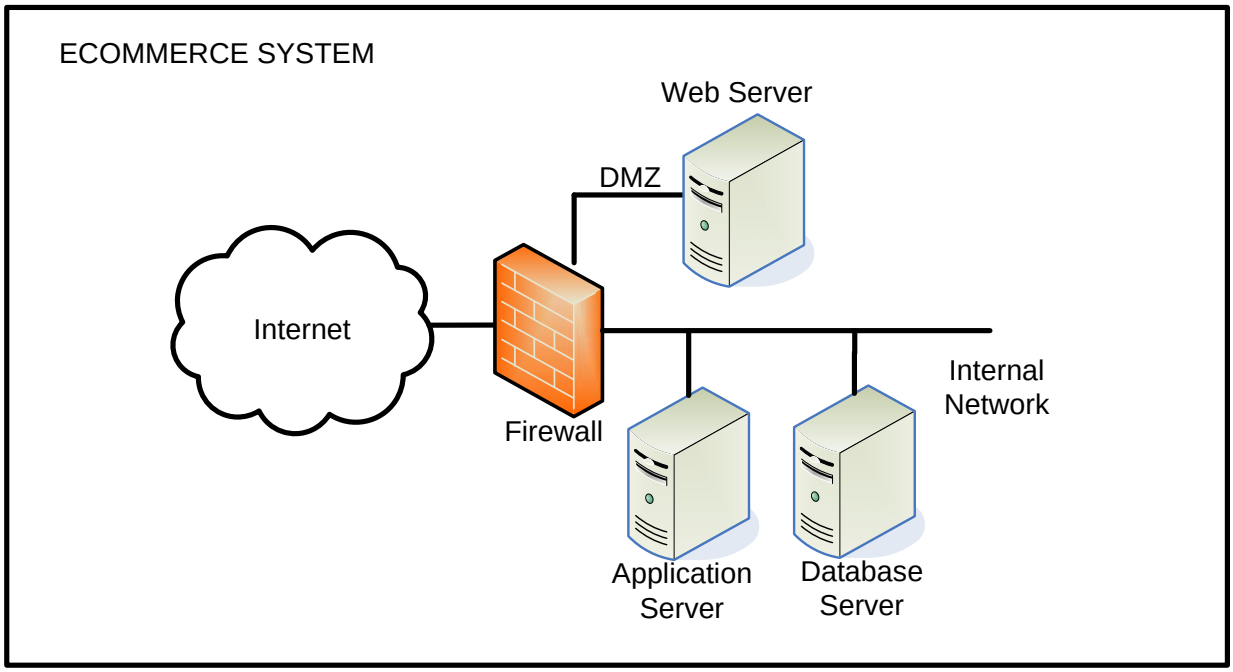
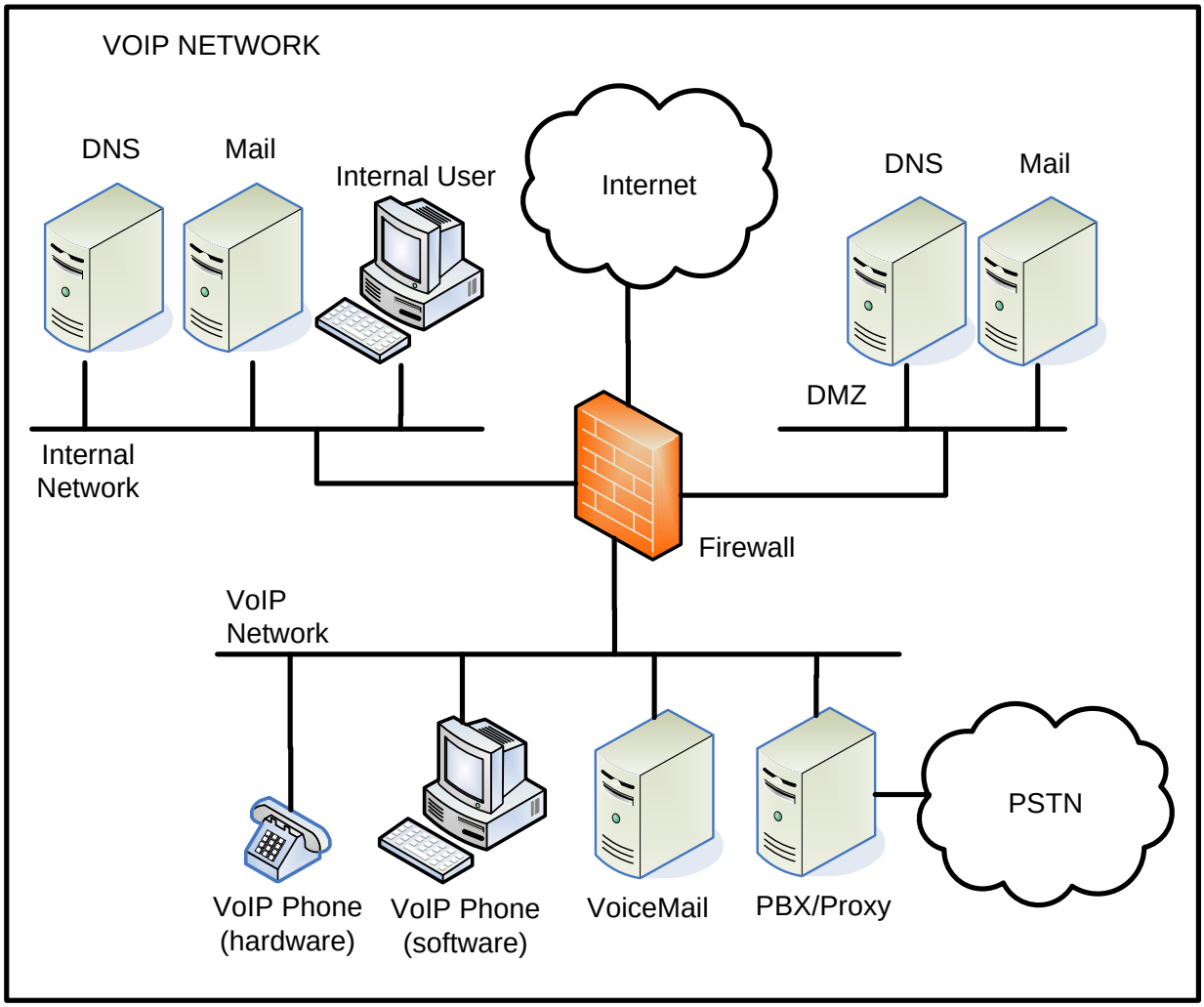
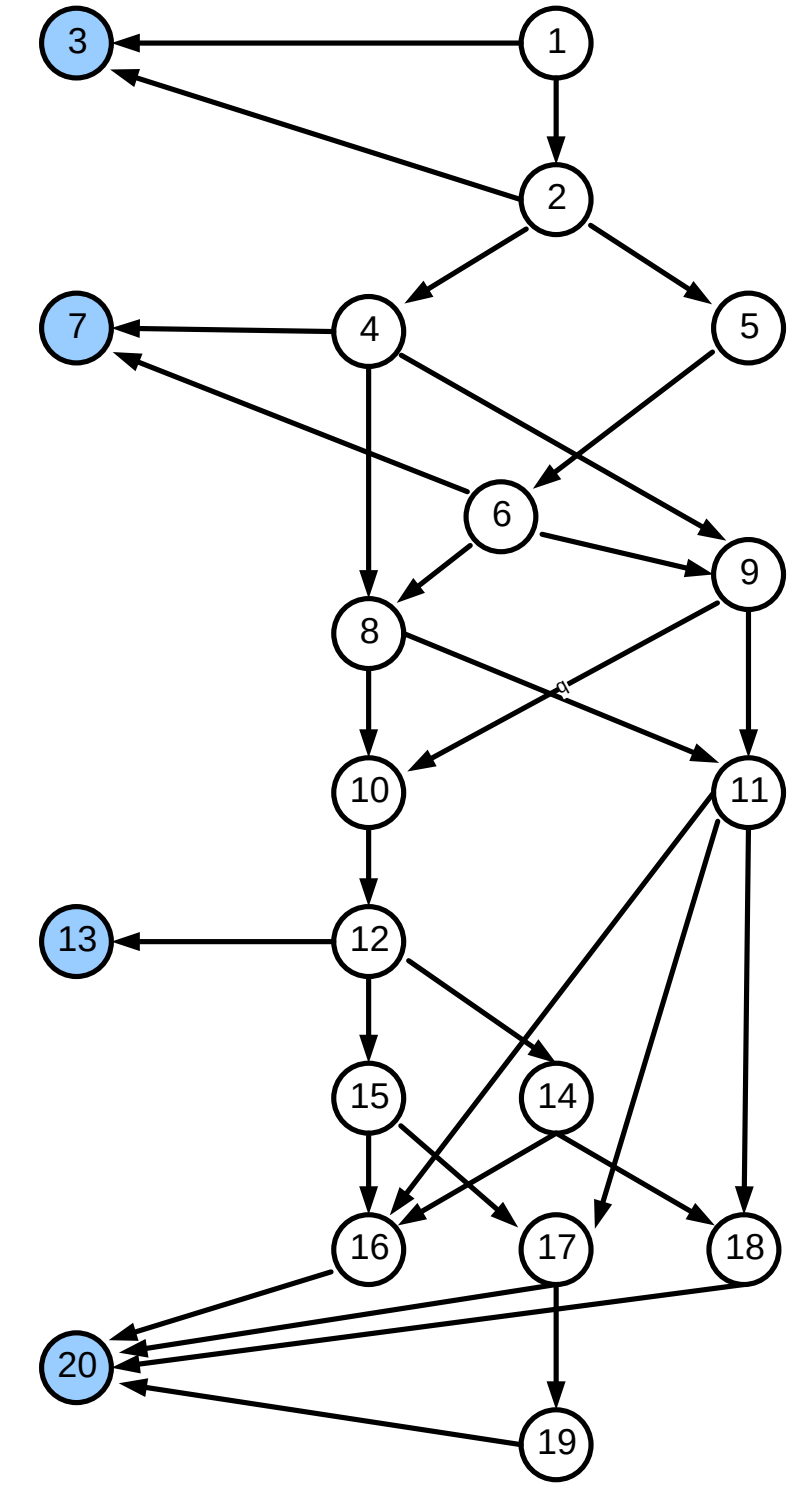
ADDENDUM TO DETERMINING PLACEMENT OF INTRUSION DETECTORS
FOR A DISTRIBUTED APPLICATION THROUGH BAYESIAN NETWORK MODELING

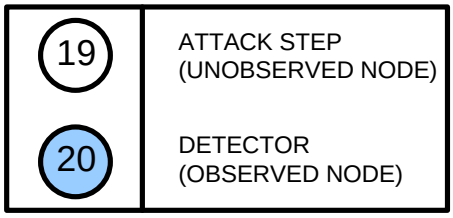
Gaspar Modelo-Howard, Purdue University





DIRECTED ACYCLIC GRAPH REPRESENTATION OF ATTACK SCENARIO
FOR E-COMMERCE DISTRIBUTED SYSTEM





DESCRIPTION OF NODES

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

NODE 2: Attack step - run portscanner on web servers

NODE 3: Detector alert – IPTables

NODE 4: Attack step - exploit ssldump 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 pwds

NODE 12: Attack step - Exploit rpc.statd 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

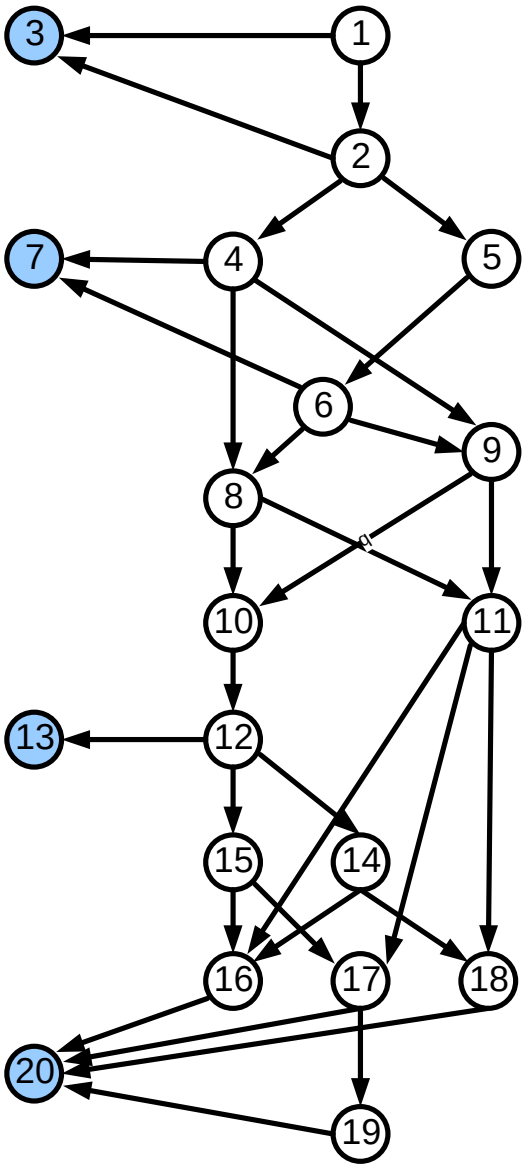
NODE 17: Attack step - Connect to MySQL server with admin account

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)

BAYESIAN NETWORK FOR E-COMMERCE DISTRIBUTED SYSTEM



	X1
F	0.99998
T	0.00002

	X2	
X1	F	T
F	0.7	0.3
T	0.3	0.7

		X3	
X2	X1	F	T
F	F	0.9	0.1
T	F	0.6	0.4
F	T	0.4	0.6
T	T	0.2	0.8

	X4	
X2	F	T
F	0.3	0.7
T	0.1	0.9

	X5	
X2	F	T
F	0.3	0.7
T	0.1	0.9

	X6	
X5	F	T
F	0.9	0.1
T	0.7	0.3

		X7	
X6	X4	F	T
F	F	0.95	0.05
T	F	0.7	0.3
F	T	0.3	0.7
T	T	0.15	0.85

		X8	
X6	X4	F	T
F	F	0.3	0.7
T	F	0.2	0.8
F	T	0.2	0.8
T	T	0.1	0.9

		X9	
X6	X4	F	T
F	F	0.99	0.01
T	F	0.3	0.7
F	T	0.3	0.7
T	T	0.01	0.99

		X10	
X9	X8	F	T
F	F	0.99	0.01
T	F	0.1	0.9
F	T	0.1	0.9
T	T	0.01	0.99

		X11	
X9	X8	F	T
F	F	0.99	0.01
T	F	0.1	0.9
F	T	0.1	0.9
T	T	0.01	0.99

	X12	
X10	F	T
F	0.2	0.8
T	0.1	0.9

	X13	
X12	F	T
F	0.9	0.1
T	0.1	0.9

	X14	
X12	F	T
F	0.2	0.8
T	0.1	0.9

	X15	
X12	F	T
F	0.2	0.8
T	0.1	0.9

			X20	
X19	X18	X17 X16	F	T
F	F	F F	0.99	0.01
T	F	F F	0.4	0.6
F	T	F F	0.35	0.65
T	T	F F	0.3	0.7
F	F	T F	0.35	0.65
T	F	T F	0.3	0.7
F	T	T F	0.3	0.7
T	T	T F	0.15	0.85
F	F	F T	0.35	0.65
T	F	F T	0.3	0.7
F	T	F T	0.3	0.7
T	T	F T	0.15	0.85
F	F	T T	0.3	0.7
T	F	T T	0.15	0.85
F	T	T T	0.15	0.85
T	T	T T	0.01	0.99

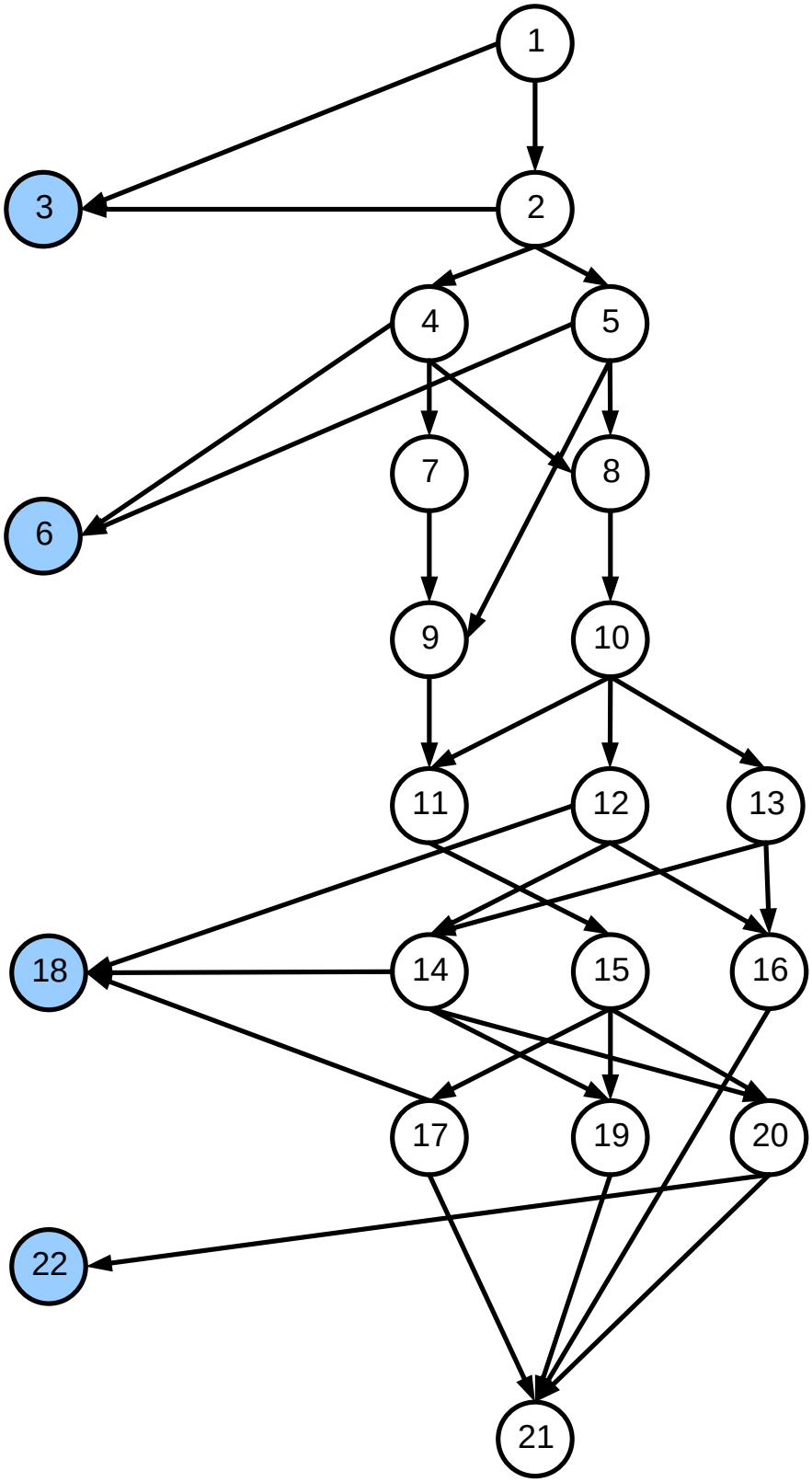
			X16	
X15	X14	X11	F	T
F	F	F	0.9	0.1
T	F	F	0.8	0.2
F	T	F	0.7	0.3
T	T	F	0.3	0.7
F	F	T	0.7	0.3
T	F	T	0.3	0.7
F	T	T	0.3	0.7
T	T	T	0.2	0.8

		X17	
X15	X11	F	T
F	F	0.95	0.05
T	F	0.7	0.3
F	T	0.8	0.2
T	T	0.2	0.8

		X18	
X14	X11	F	T
F	F	0.9	0.1
T	F	0.6	0.4
F	T	0.4	0.6
T	T	0.2	0.8

	X19	
X17	F	T
F	0.9	0.1
T	0.1	0.9

DIRECTED ACYCLIC GRAPH REPRESENTATION OF ATTACK SCENARIO
FOR VOIP NETWORK
(v0.50 – 080208)



DESCRIPTION OF NODES

NODE 1: Attack step - ping or traceroute to DNS server

NODE 2: Attack step - run portscanner on DNS server

NODE 3: Detector alert - IPTables

NODE 4: Attack step – exploit FTP buffer overflow in Mail server

NODE 5: Attack step – brute force administrator password using VNC in DNS server

NODE 6: Detector alert – Snort

NODE 7: Attack step – install sniffer to capture passwords

NODE 8: Attack step – TFTP to external repository to download sniffer

NODE 9: Attack step – TFTP to external repository to download sniffer

NODE 10: Attack step – sniff traffic to DNS server

NODE 11: Attack step - login with sniffed account/password from mail server to voicemail server

NODE 12: Attack step – exploit IIS buffer overflow in voicemail server

NODE 13: Attack step – exploit SQL buffer overflow in VoiceMail server

NODE 14: Attack step - portscan VoIP network

NODE 15: Attack step – local privilege escalation exploit in voicemail server

NODE 16: Attack step – ARP poisoning the communication switch

NODE 17: Attack step – brute force administrator password using VNC in PBX/Proxy server

NODE 18: Detector alert – Snort

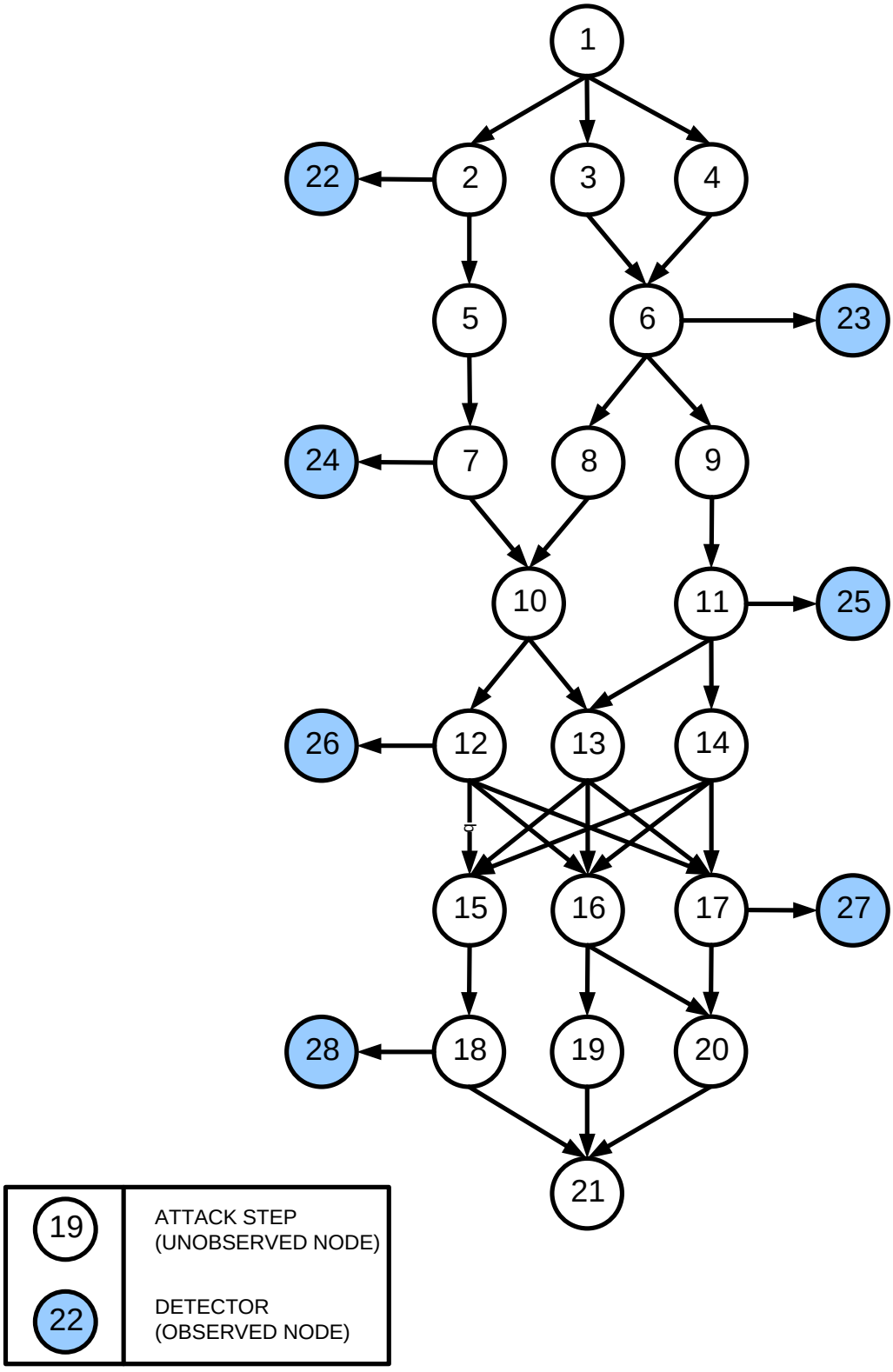
NODE 19: Attack step – exploit IIS buffer overflow in PBX/Proxy server

NODE 20: Attack step – buffer overflow to Win2K of computer with soft phone

NODE 21: Attack step – eavesdrop VoIP communication

NODE 22: Detector alert – antivirus software

DIRECTED ACYCLIC GRAPH REPRESENTATION OF ATTACK SCENARIO
FOR GENERIC NETWORK



Experiment: Impact on Choice and Placement of Single Detector

The objective of this experiment was to determine the impact of selecting the detectors and their corresponding locations, in order to provide a high accuracy when detecting if an attached step has been achieved. We ran experiments on the e-commerce network to determine a single detector that would be most effective to detect when attack step 19 was performed. This is similar to the experiment 3 shown in the paper, but with the difference in the number of detectors selected. An optimal detector is chosen according to the algorithm described in Section 3.2 of the paper. The performance of the optimal detector is presented with a ROC curve and compared against additional pairs selected at random. For our experiment, node 19 is selected as the ultimate goal in the e-commerce system.

To calculate the performance of each detector, we created 50,000 samples from each Bayesian network, corresponding to that many actual attacks. Then we performed Bayesian inference and calculated the conditional probability of the attack step, given the detector being evaluated. We determined the true positive rate and false positive rate by sweeping across threshold values.

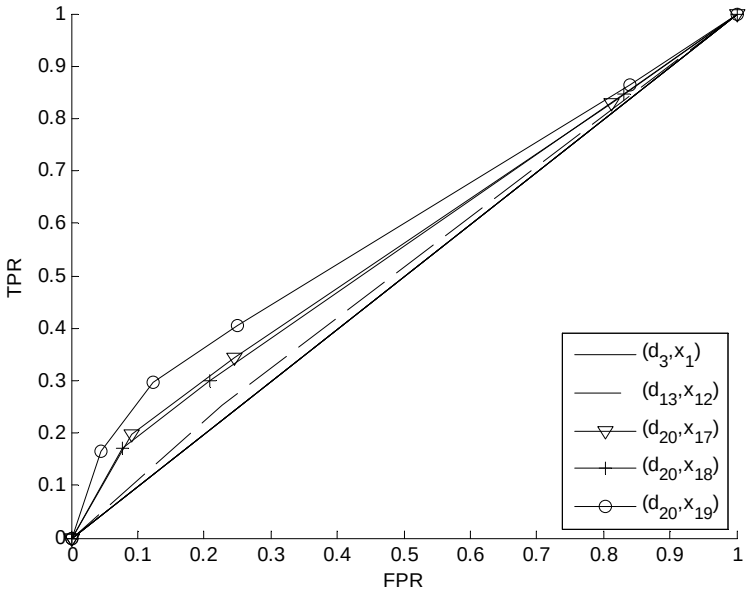


Fig. 1. ROC curves for detection of attack step 19, using a single detector, in the e-commerce network.

Results show that the detector determined from the algorithm performs better than the other randomly selected alternatives. Figure 1 shows the situation in which a single detector (d_{20}) attached to the attack node (x_{19}) performs better than the same detector connected to other attack nodes (x_{17} and x_{18}). It also performs better than other detectors connected to different nodes (d_{13} to x_{12} and d_3 to x_1). This can be explained by the fact that having a detector directly connected to the attack step provides better predictive performance than having the detector connected to any other attack step, since the performance of the detector, in terms of its TP and FP values, is high.