

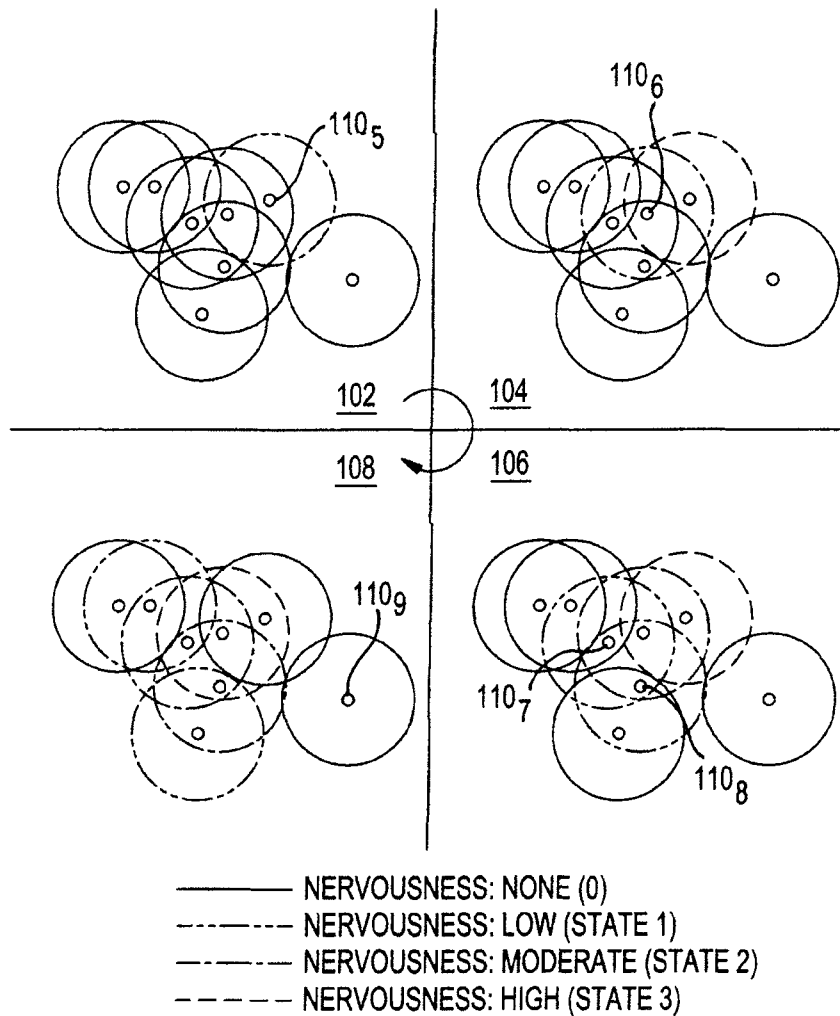


FIG. 1 NETWORK NERVOUSNESS ASSESSMENT

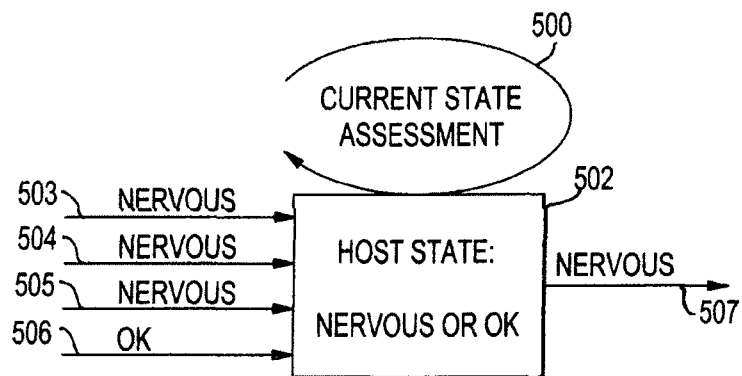


FIG. 5 THEORETICAL CONTEXT DIAGRAM FOR BLOCK ONE

FIG. 2
SYSTEMIGRAM FOR
EMERGENT
NETWORK DEFENSE

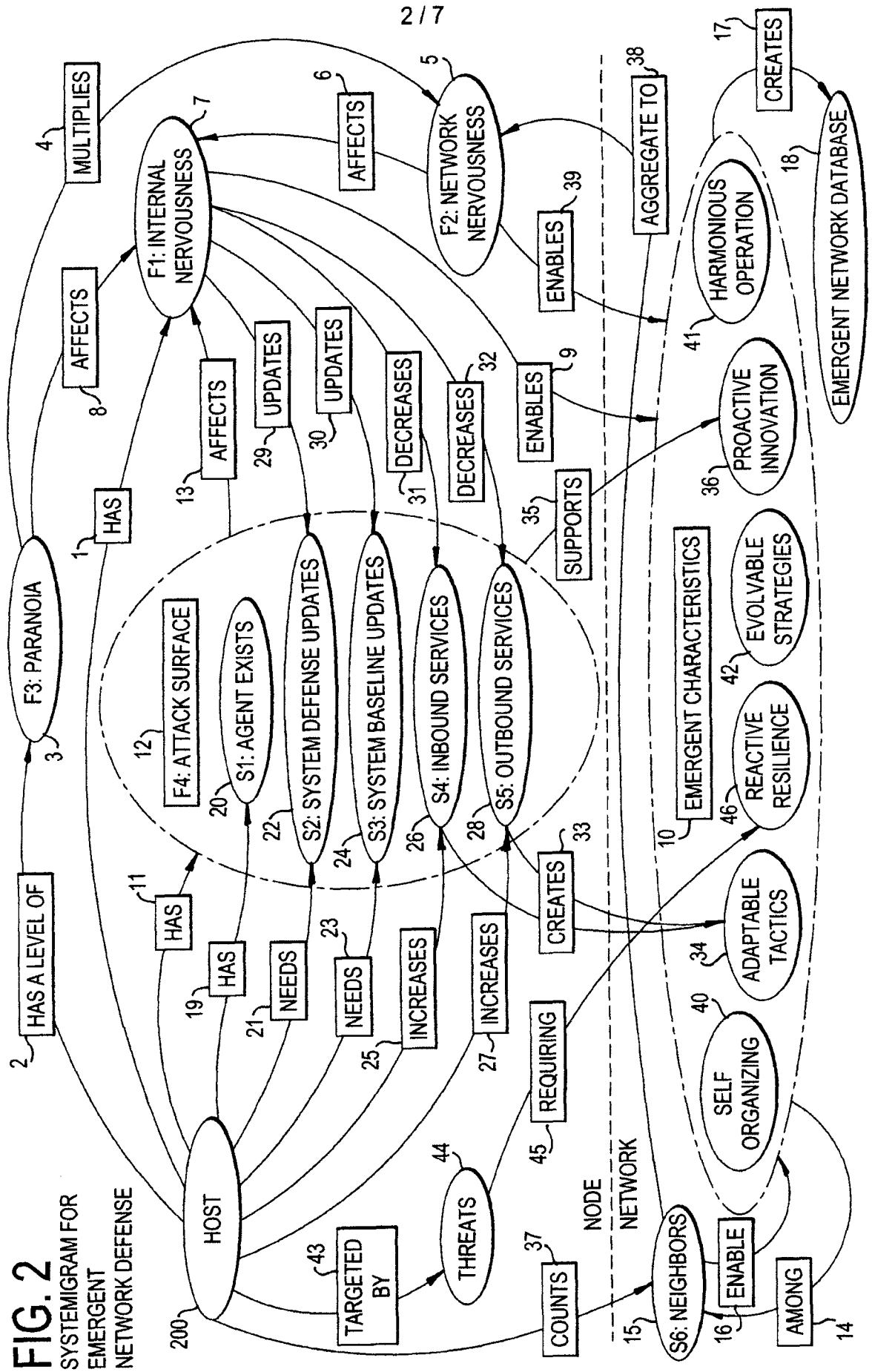
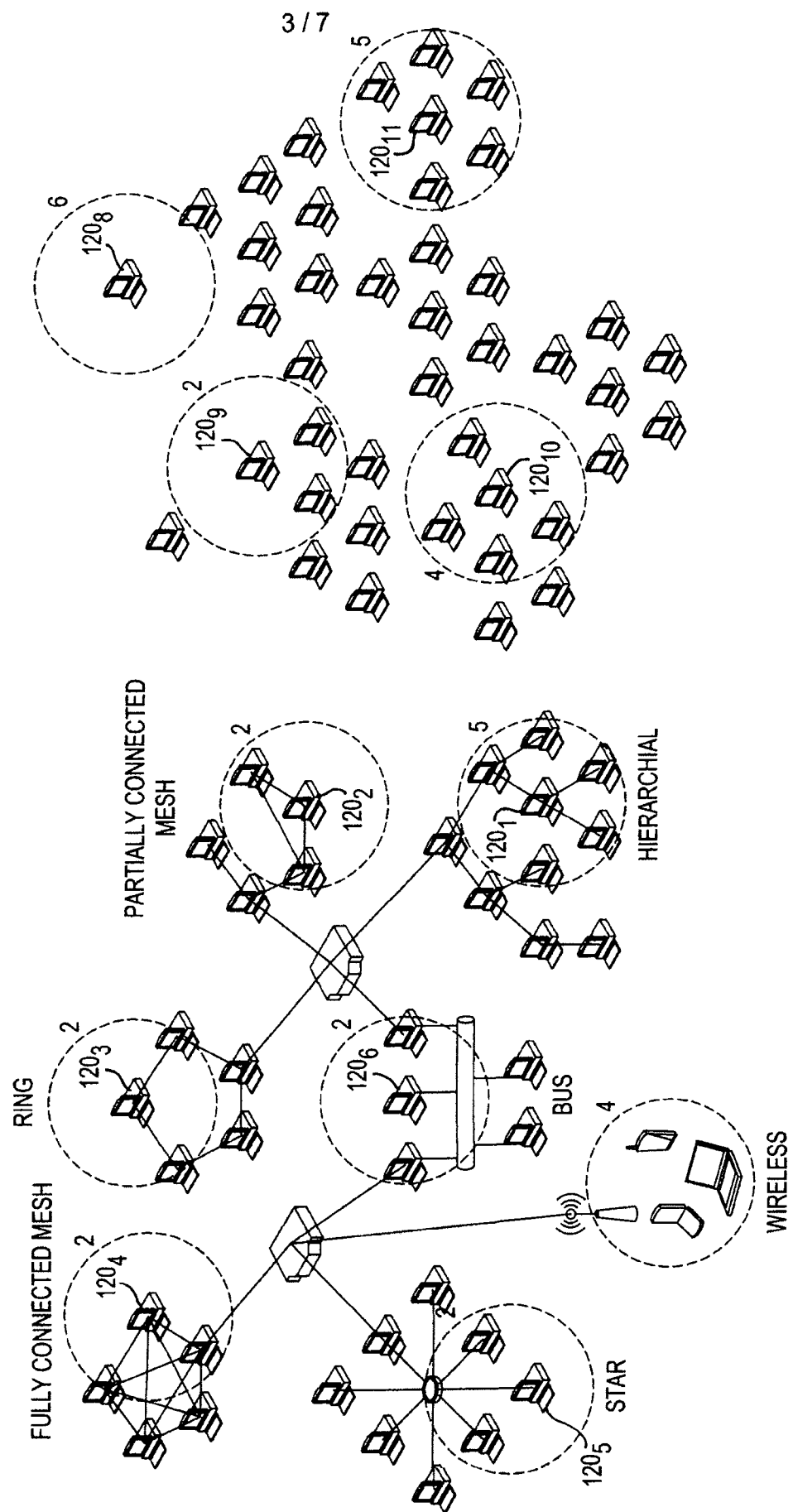


FIG. 3 NEAREST NEIGHBOR ABSTRACTION



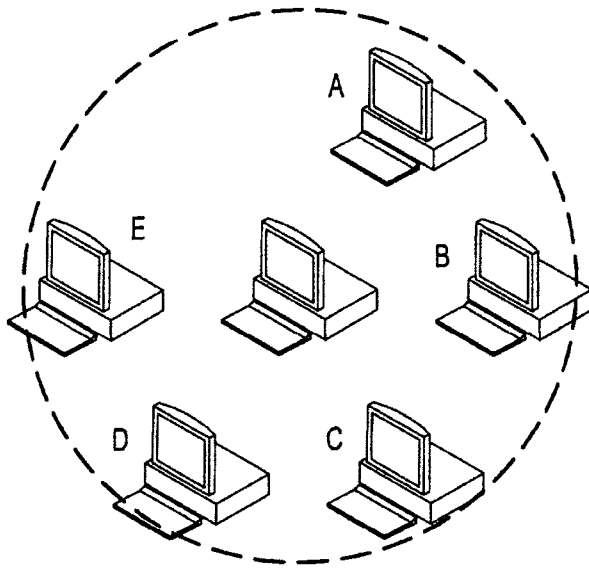


FIG. 4
NERVOUS EXAMPLE

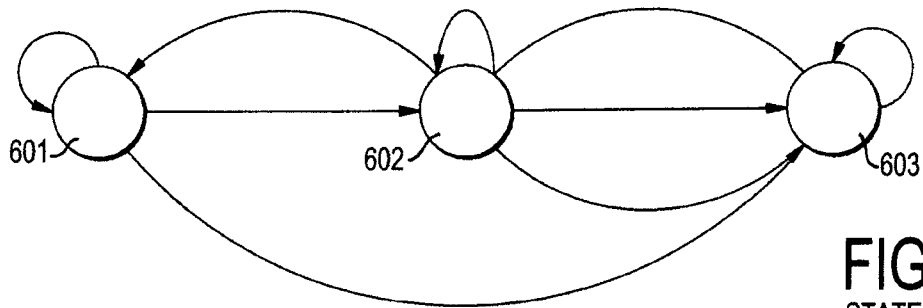


FIG. 6
STATE CHANGE

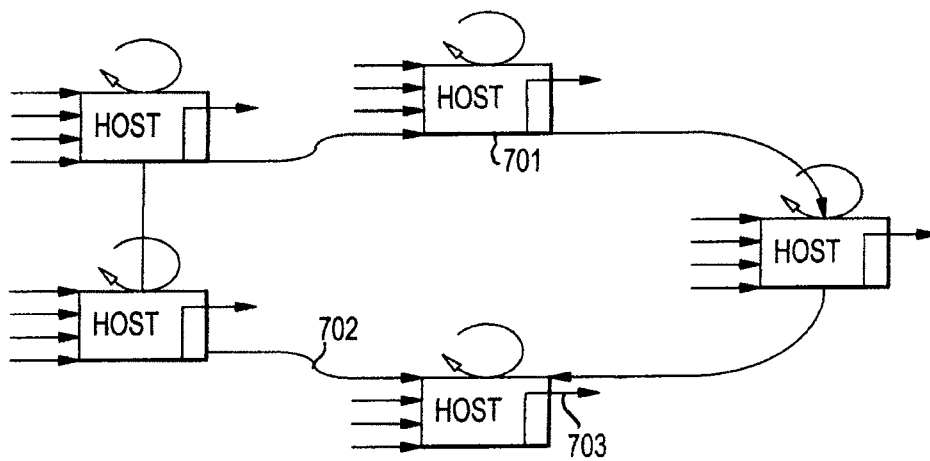
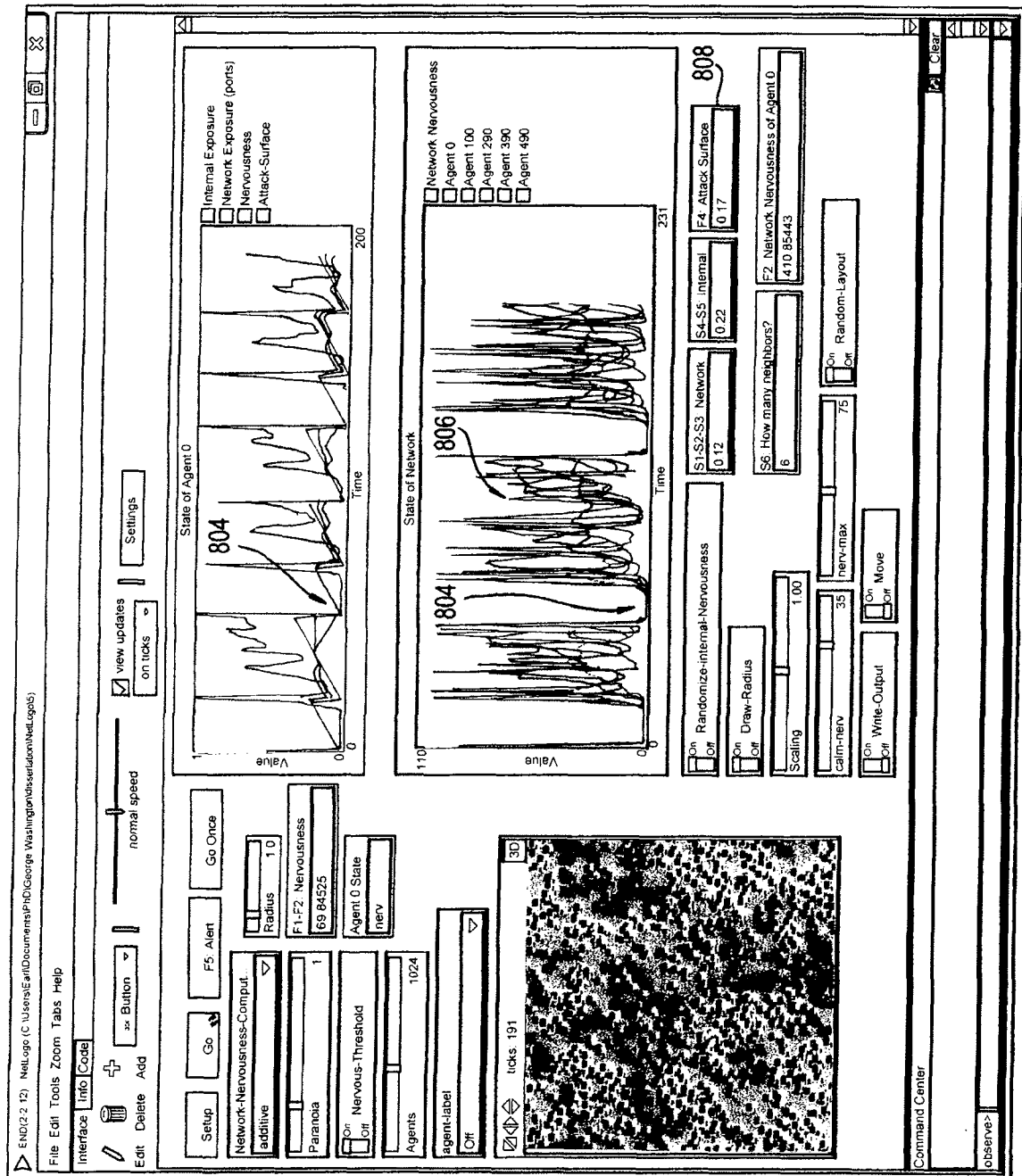


FIG. 7 THEORETICAL CONTEXT DIAGRAM FOR BLOCK TWO



5 / 7

FIG. 8
THREE ALERTS DEMONSTRATE
EMERGENT BEHAVIOR

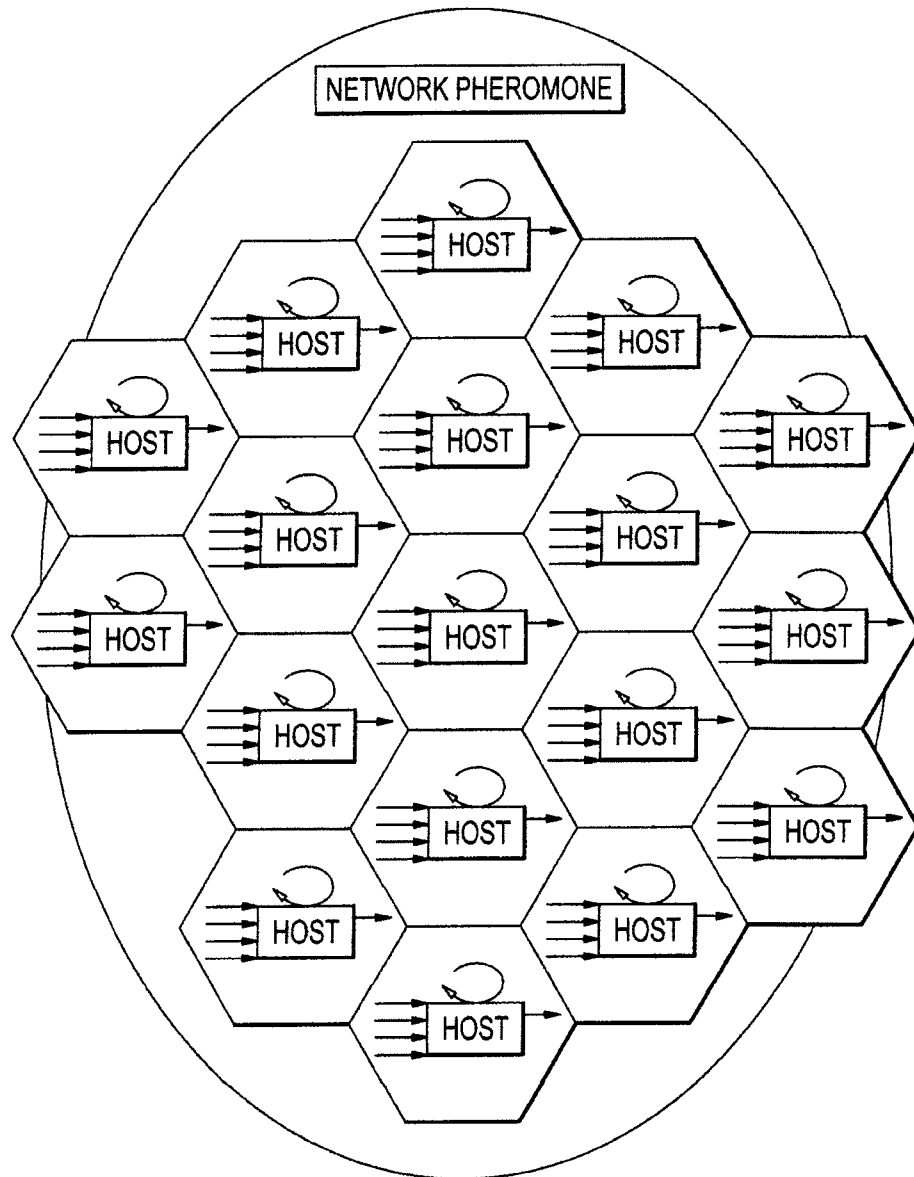


FIG. 9 THEORETICAL CONTEXT DIAGRAM FOR BLOCK THREE

FEEDBACK DATA:	STATE DATA:
F1: LEVEL OF INTERNAL NERVOUSNESS	S1: AGENT EXISTS ON NODE
F2: LEVEL OF NETWORK NERVOUSNESS	S2: SYSTEM DEFENSES (HBSS, AV, IDS) AT LATEST SIGNATURE LEVEL
F3: LEVEL OF PARANOIA	S3: SYSTEM BASELINE (OS, APPLICATIONS) AT LATEST PATCH/CONFIGURATION LEVEL
F4: ATTACK SURFACE	S4: INBOUND SERVICES RESTRICTED (SERVICES RESTRICTED, PORTS BLOCKED)
	S5: OUTBOUND SERVICES RESTRICTED (BLOCKED IP, SUBNETS, URLs)
	S6: NUMBER OF NEIGHBORS

	F1: LEVEL OF INTERNAL NERVOUSNESS	F2: LEVEL OF NETWORK NERVOUSNESS	F3: LEVEL OF PARANOIA	F4: ATTACK SURFACE	S1: AGENT EXISTS ON NODE	S2: SYSTEM DEFENSES AT LATEST SIGNATURE LEVEL	S3: SYSTEM BASELINE AT LATEST PATCH/CONFIGURATION LEVEL	S4: INBOUND SERVICES RESTRICTED	S5: OUTBOUND SERVICES RESTRICTED	S6: NUMBER OF NEIGHBORS
BLOCK ONE: ENDPOINT ATTACK SURFACE CHARACTERISTICS				X	X	X	X	X	X	
BLOCK TWO: ENDPOINT NODES SHARE SECURITY STATES THROUGH "NERVOUS NETWORK"	X	X	X		X					X
BLOCK THREE: NODE SYSTEMS CHANGE THEIR ATTACK SURFACE AND NODE NERVOUS STATE BASED ON INPUTS	X	X	X	X	X	X	X	X	X	X

FIG. 10 REQUIRED DATA ELEMENTS

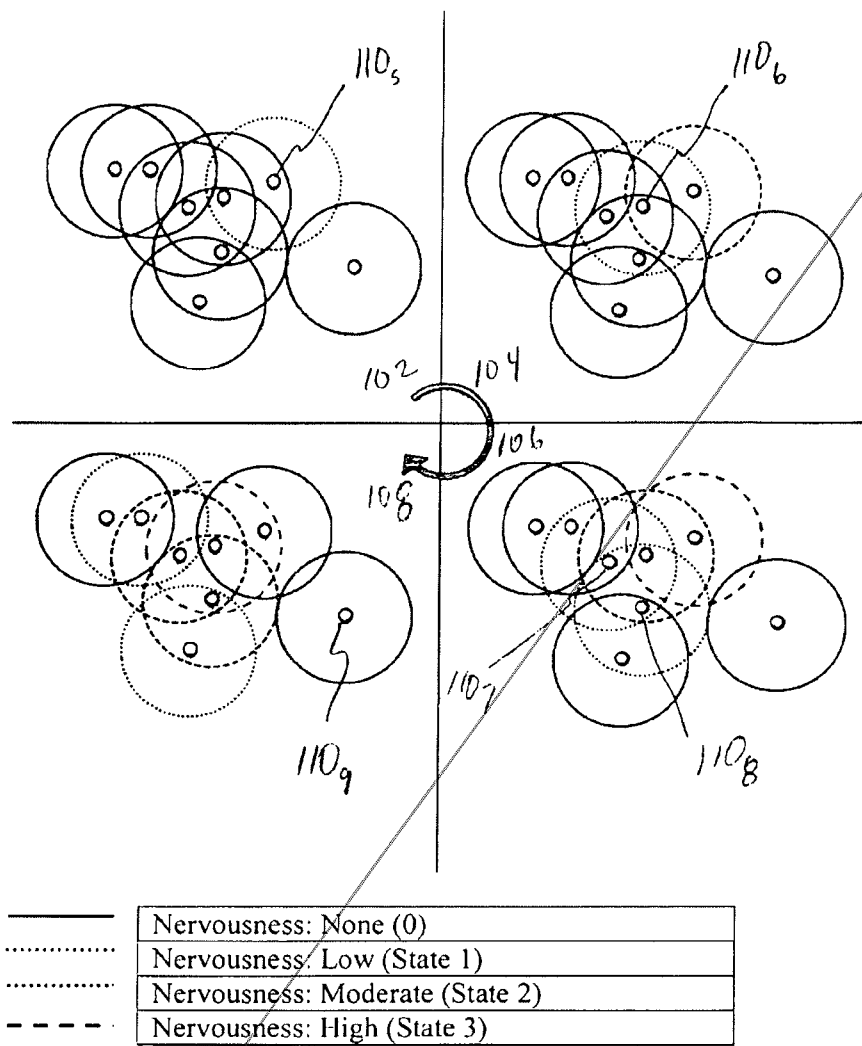


Figure 1: Network Nervousness Assessment

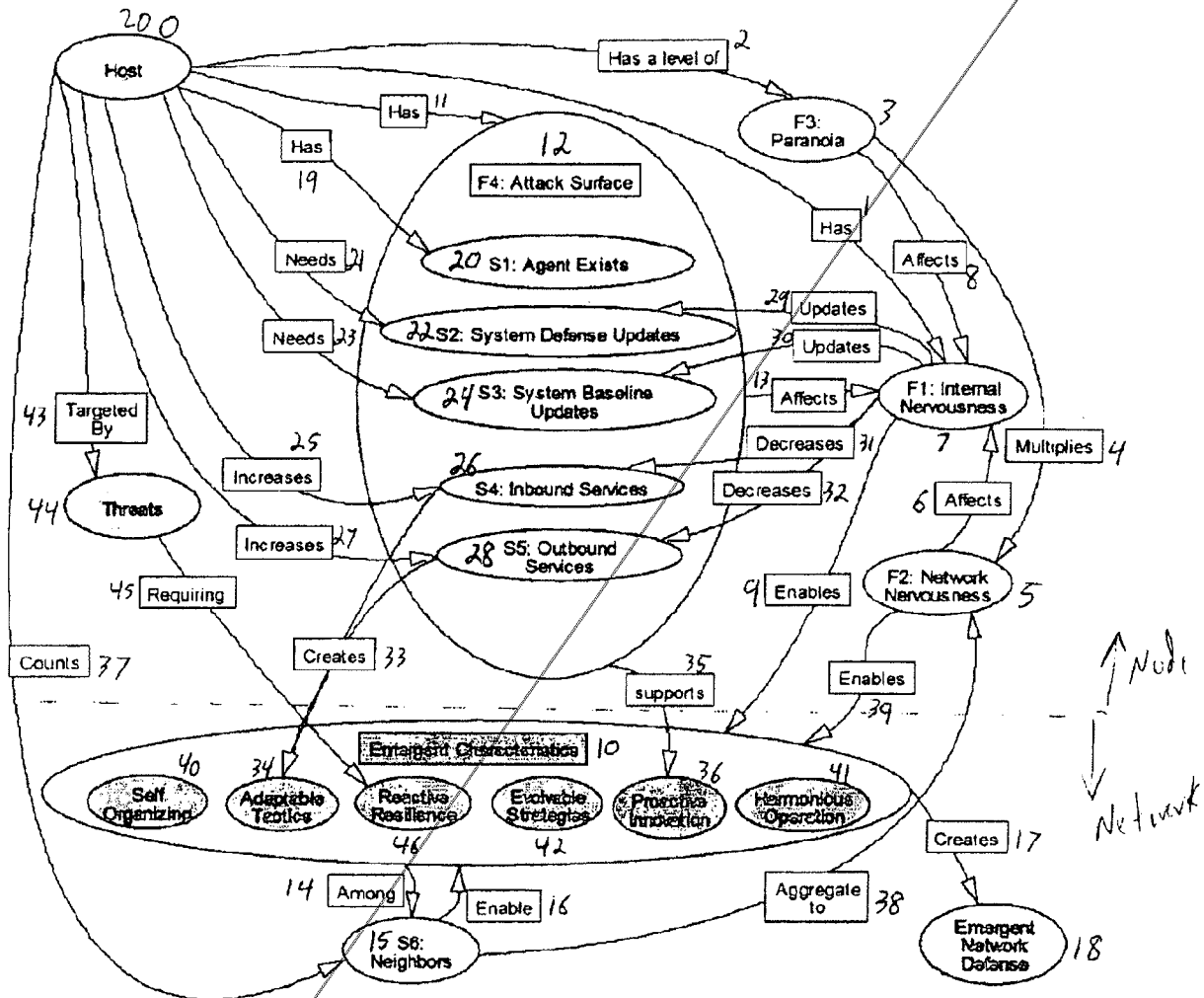


Figure 2: Systemigram for Emergent Network Defense

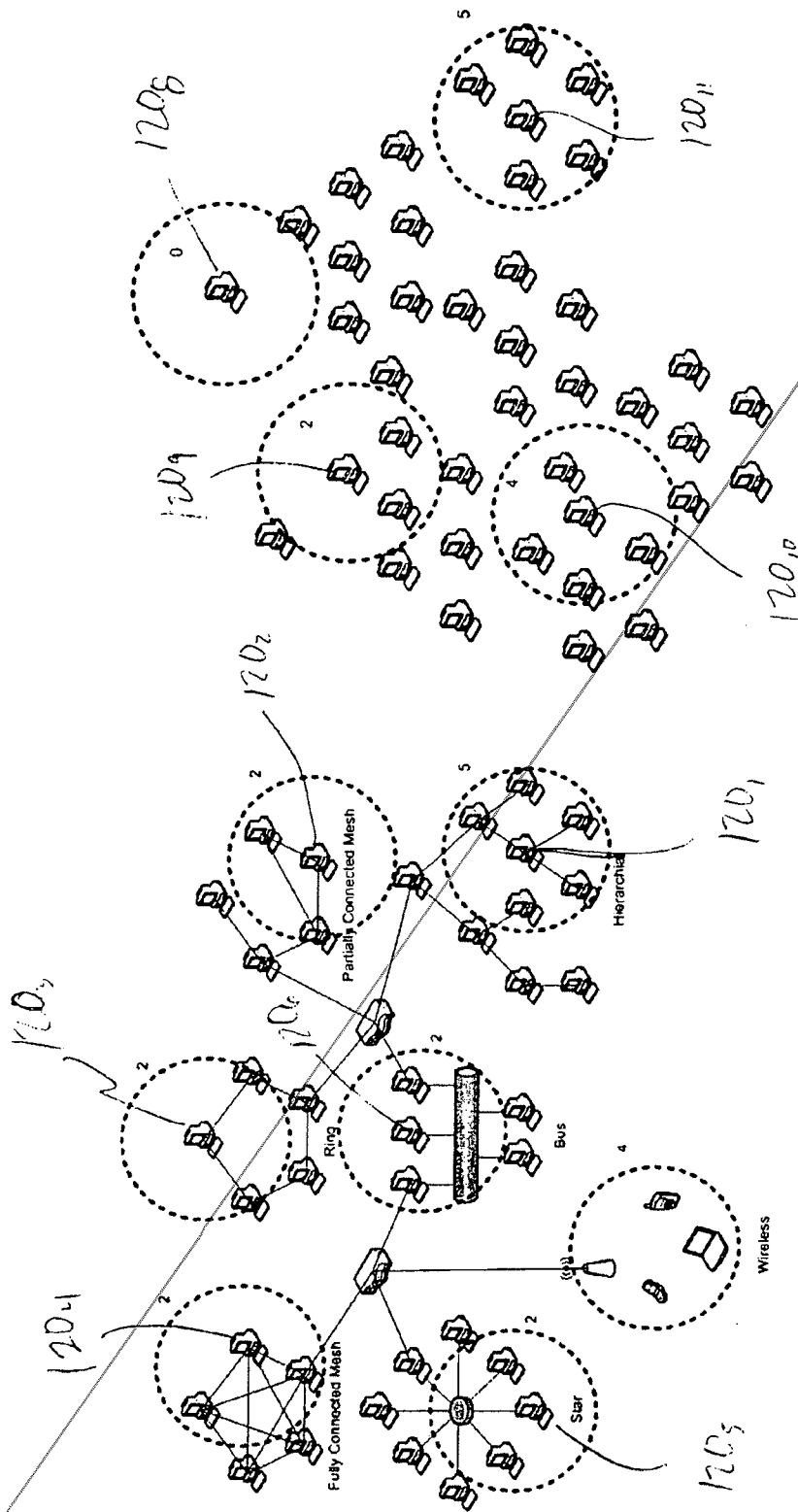


Figure 3: Nearest Neighbor Abstraction

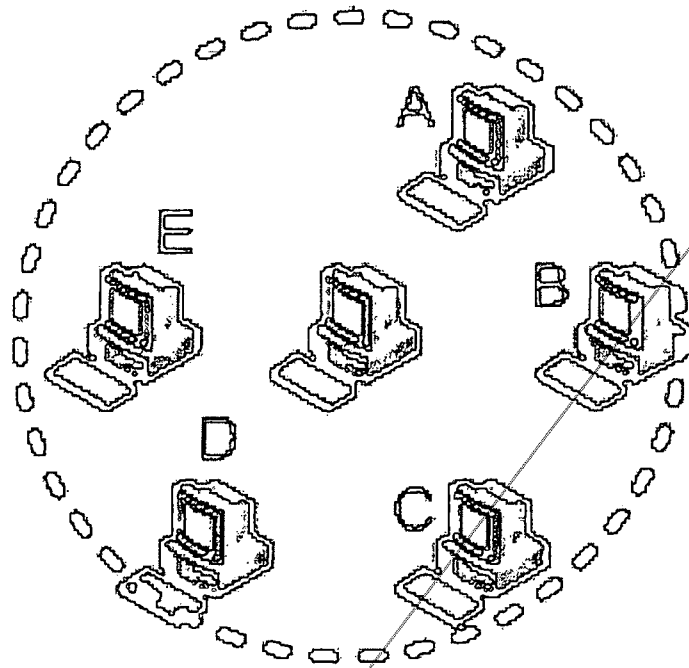


Figure 4: Nervous Example

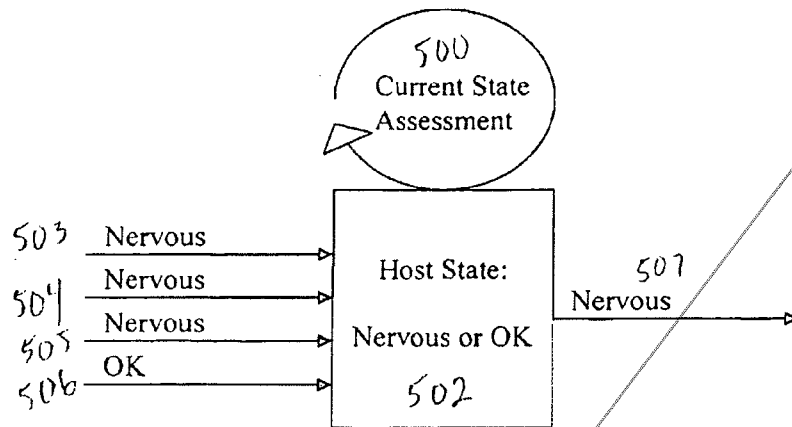


Figure 5: Theoretical Context Diagram for Block One

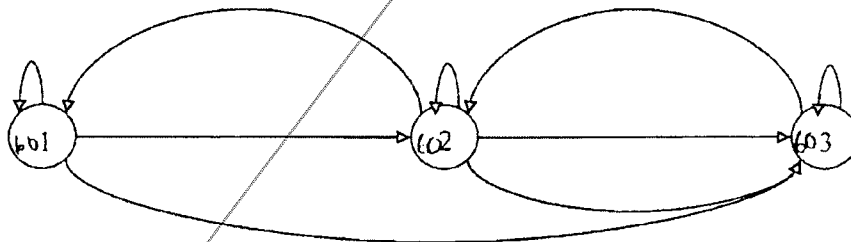
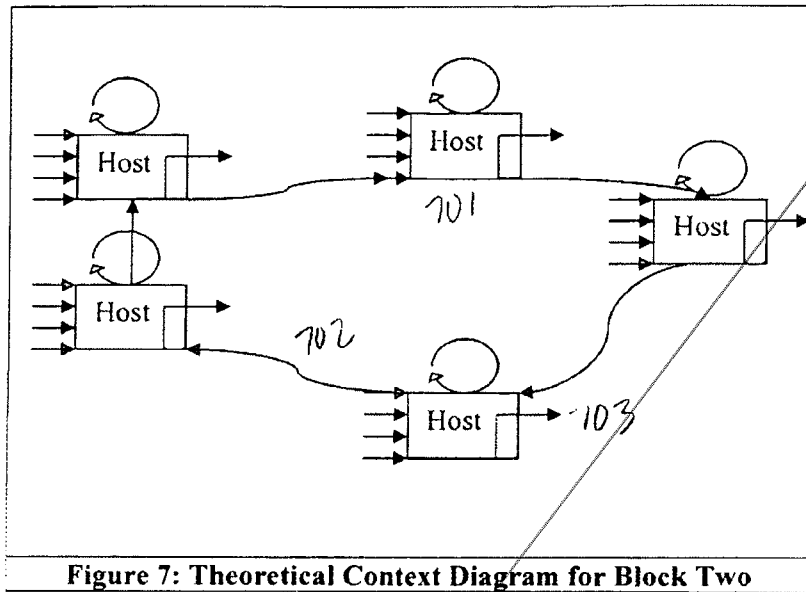


Figure 6: State Change



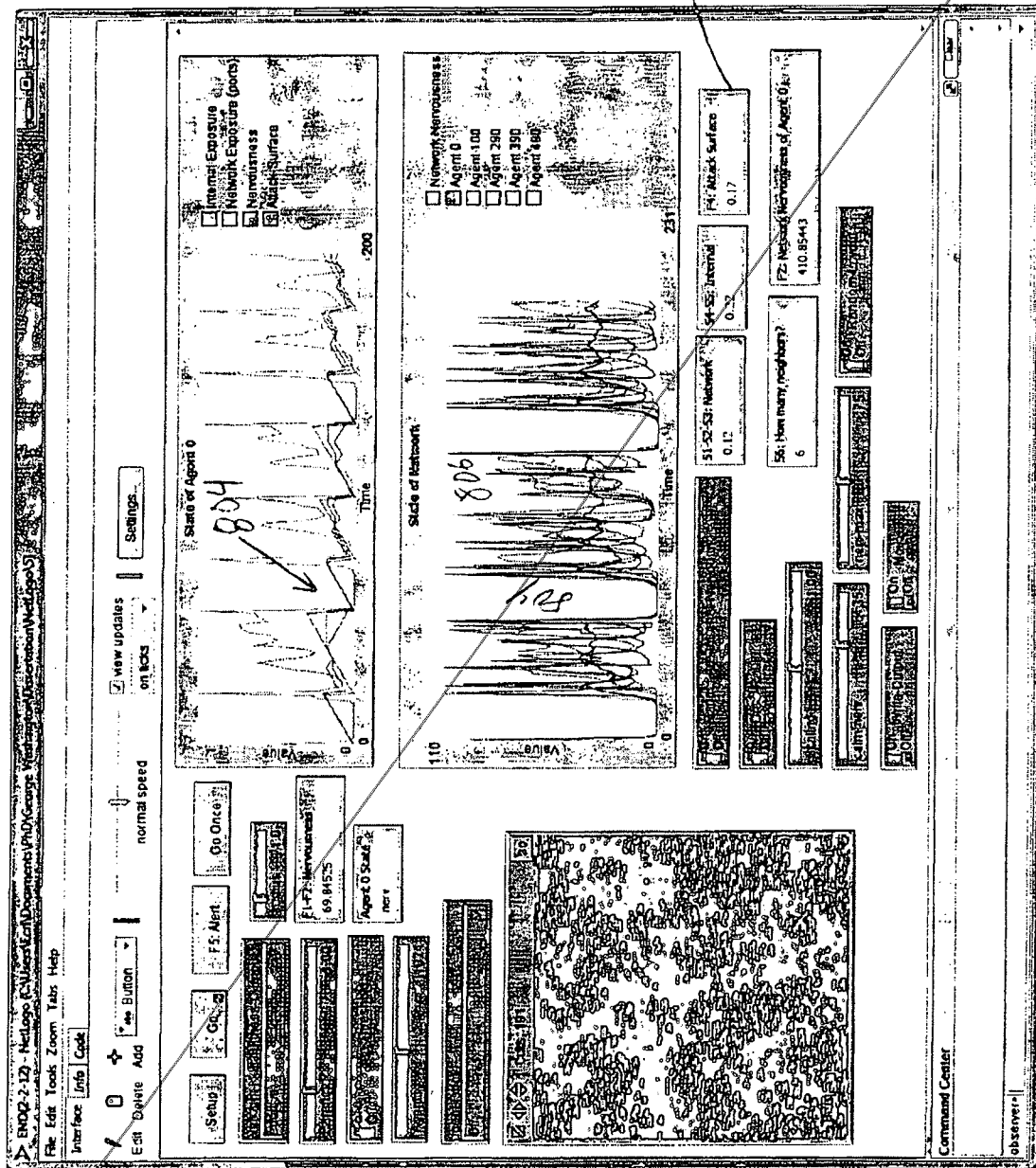


Figure 8: Three Alerts Demonstrate Emergent Behavior

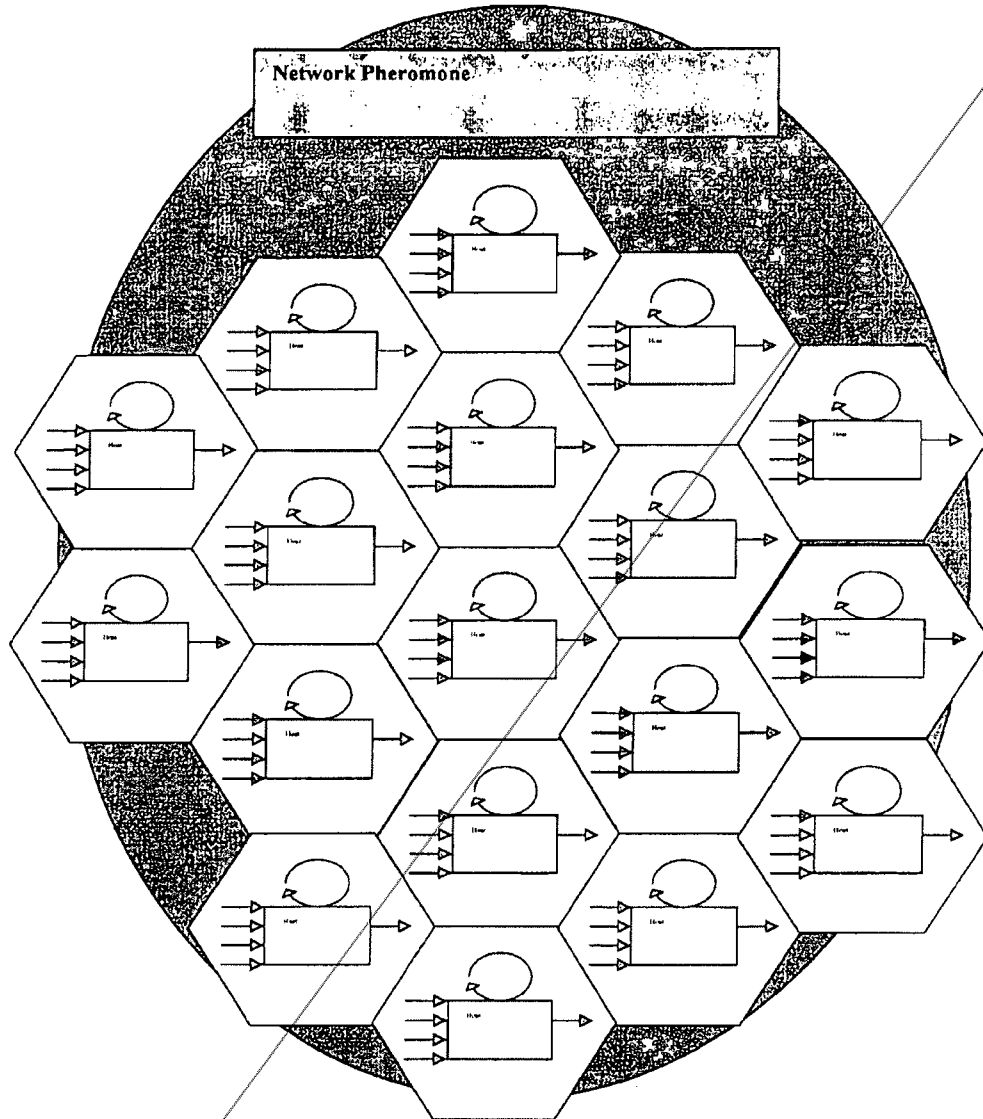


Figure 9: Theoretical Context Diagram for Block Three

Feedback Data:	State Data:
F1: Level of Internal Nervousness F2: Level of Network Nervousness F3: Level of Paranoia F4: Attack Surface	S1: Agent exists on node S2: System Defenses (HBSS, AV, IDS) at latest signature level S3: System Baseline (OS, Applications) at latest patch/configuration level S4: Inbound services restricted (services disabled, ports blocked) S5: Outbound services restricted (blocked IP, subnets, URLs) S6: Number of Neighbors

	F1: Level of Internal Nervousness	F2: Level of Network Nervousness	F3: Level of Paranoia	F4: Attack Surface	S1: Agent exists on node	S2: System Defenses at latest signature level	S3: System Baseline at latest patch/configuration level	S4: Inbound services restricted	S5: Outbound services restricted	S6: Number of Neighbors
Block One: Endpoint attack surface characteristics				X	X	X	X	X	X	
Block Two: Endpoint nodes share security states through "nervous network"	X	X	X		X					X
Block Three: Node systems change their attack surface and node nervous state based on inputs	X	X	X	X	X	X	X	X	X	X

Figure 10: Required Data Elements