Toward Systems with a Will to Live

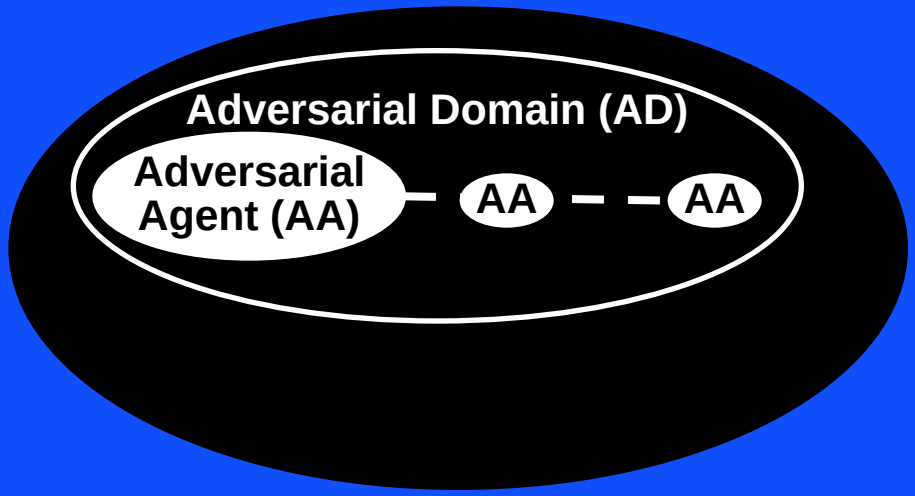
Autonomic Awareness

Enchantment Chapter Presentation
12 January 2010

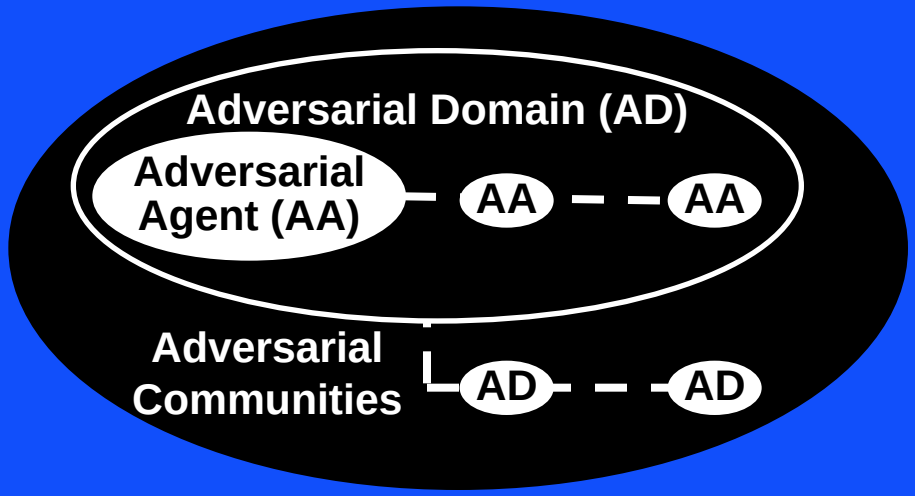
INTRO

asymmetry of static vs dynamic is the problem to solve,
balancing with dynamic vs dynamic

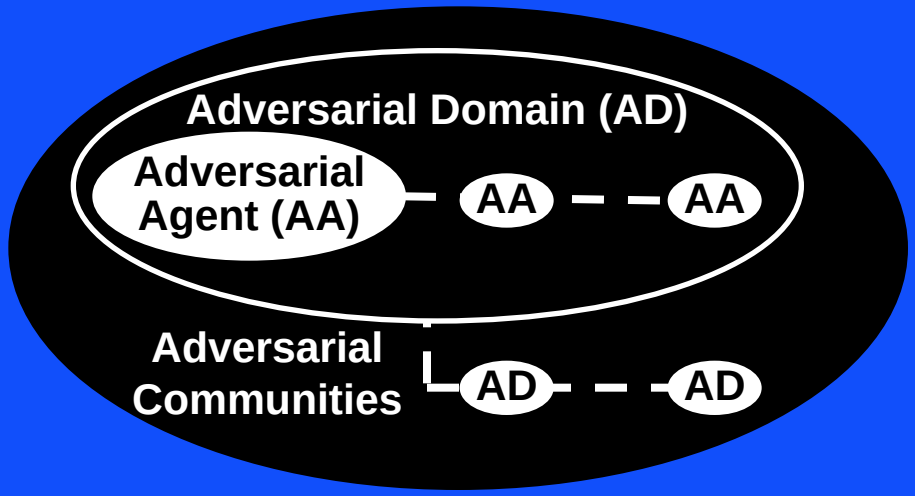
General Current Situation

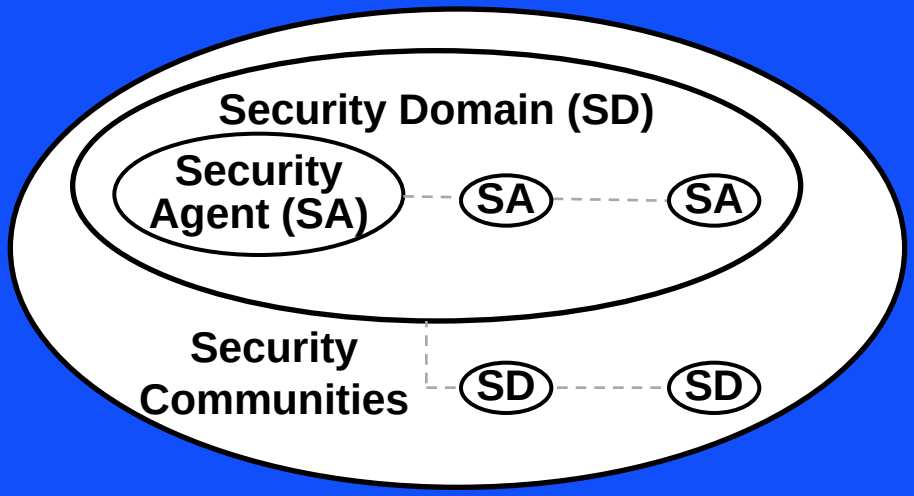


General Current Situation

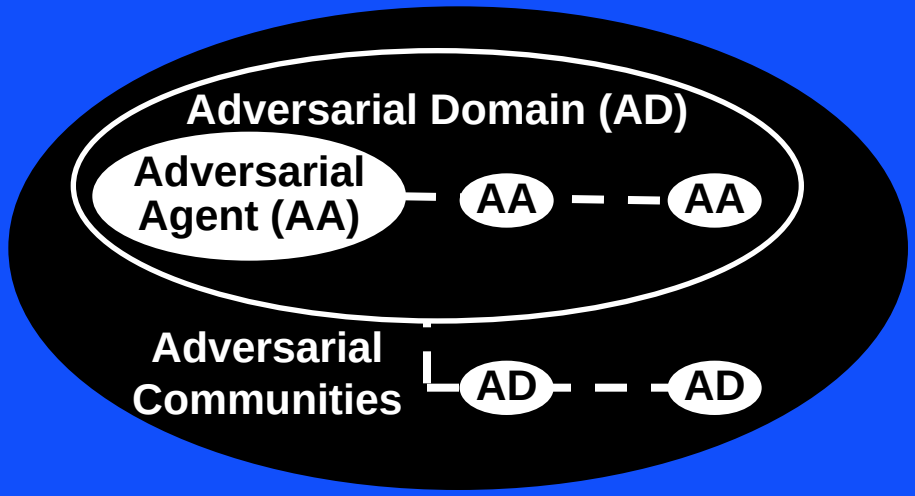


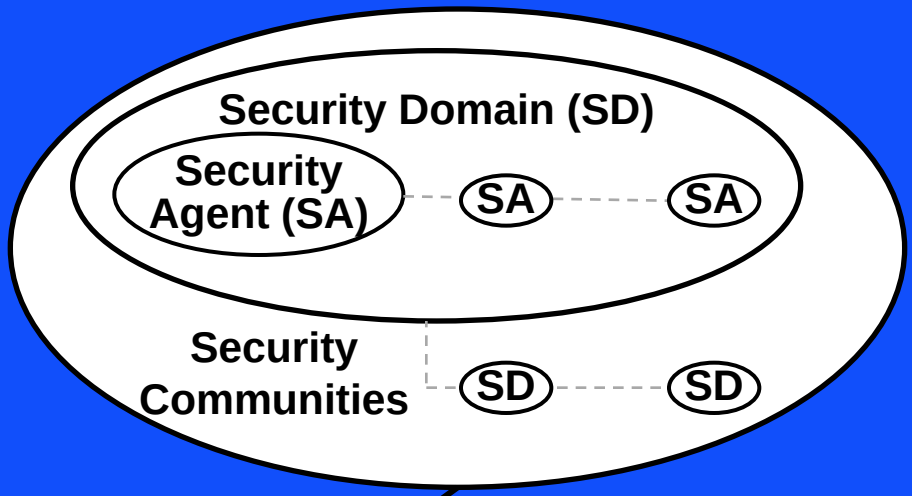
General Current Situation



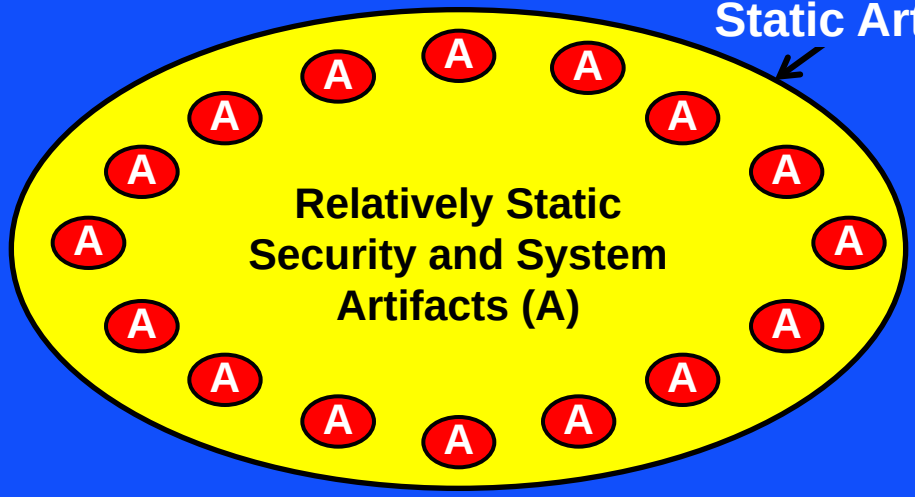


General Current Situation



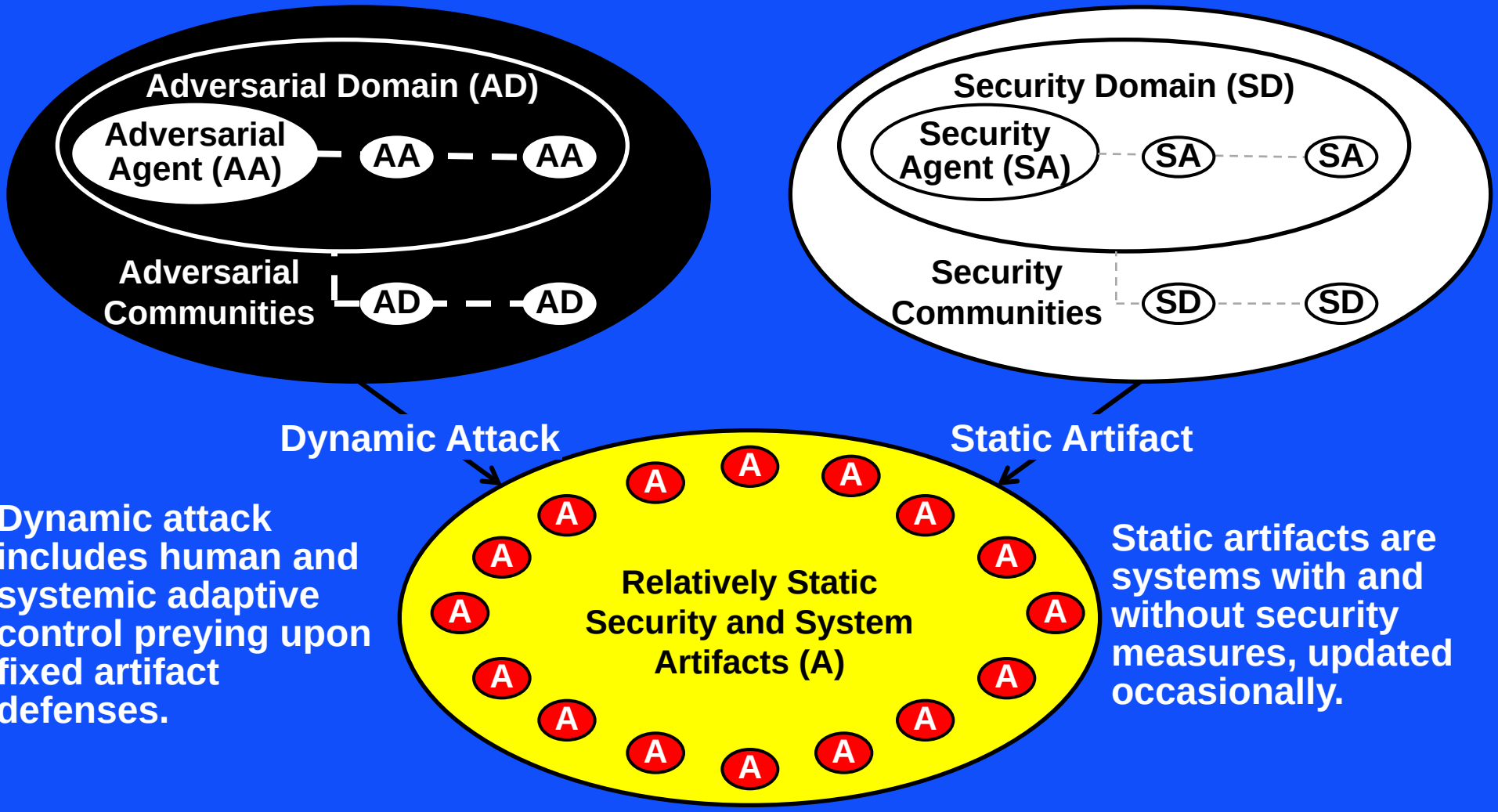


Static Artifact



Static artifacts are systems with and without security measures, updated occasionally.

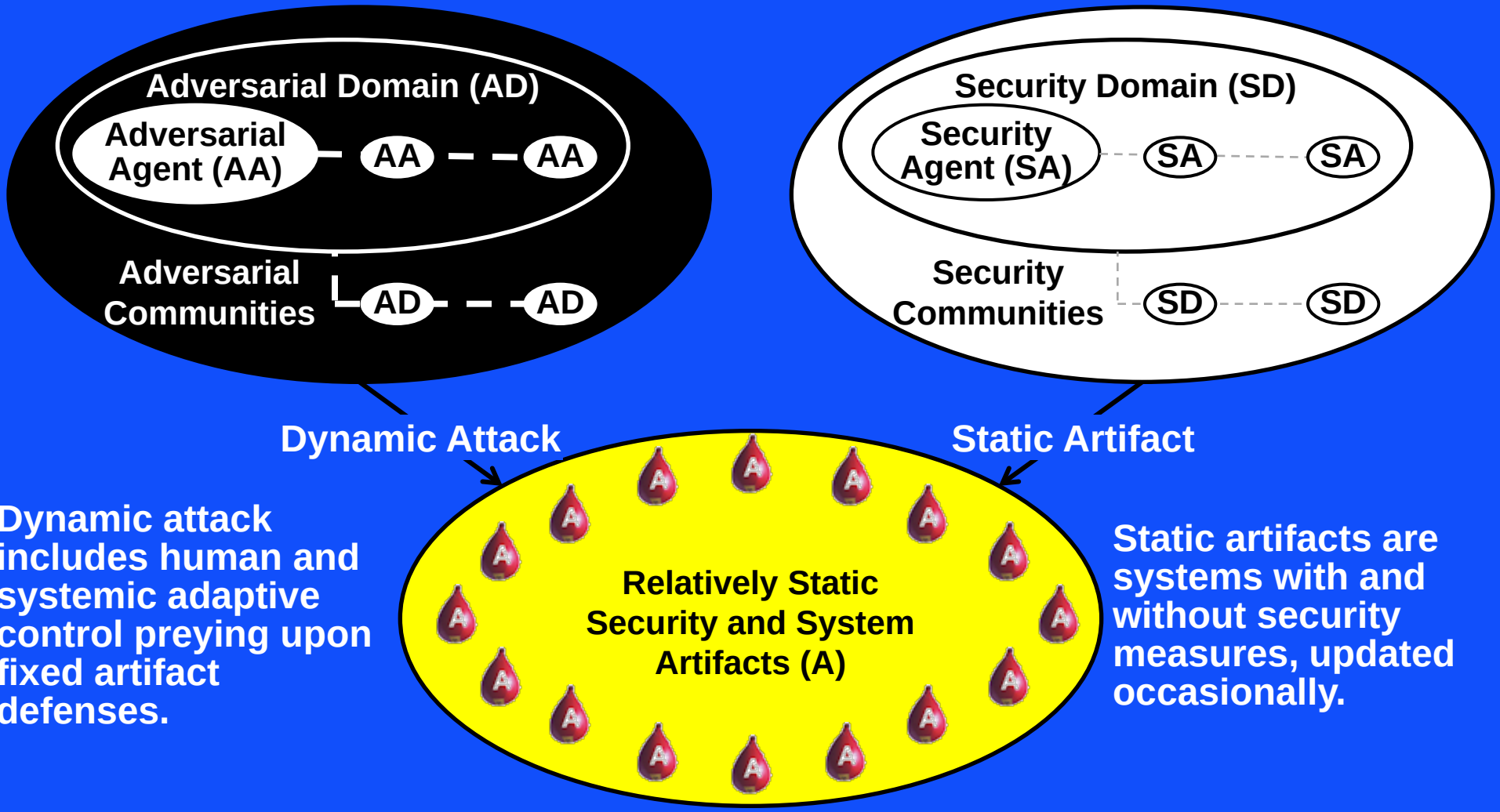
General Current Situation



Dynamic attack includes human and systemic adaptive control preying upon fixed artifact defenses.

Static artifacts are systems with and without security measures, updated occasionally.

General Current Situation



Dynamic attack includes human and systemic adaptive control preying upon fixed artifact defenses.

Static artifacts are systems with and without security measures, updated occasionally.


Static
System
Dynamic
Adversary

Assumption

Assumption

Reality

Asymmetries

Adversary is a natural system, security strategy is an artificial system

Adversary leads with innovation and evolution

Adversary self-organizes as a dynamic system-of-systems

This Talk

Three Dynamic Self organizing System-of-System Security Patterns

Pattern employment example – funded project-in-process

Inspirational Patterns

from natural systems that effectively process noisy sensory input from uncertain and changing environments

Autonomic System Properties

General properties of an autonomic, or self-managing, computing system

Four Objectives

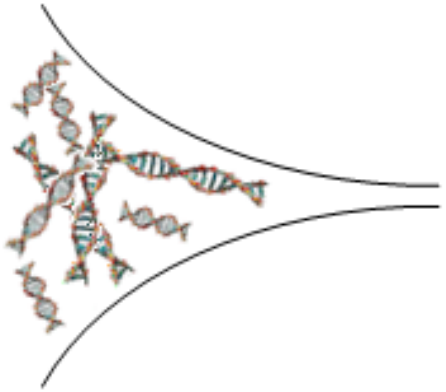
- ***Self-configuration: Readjustment to support a change in circumstances.***
- ***Self-healing: Reactive – recovering when a fault occurs.***
  Proactive – monitoring vital signs to predict and avoid problems.
- ***Self-optimization: Measure performance and employ policies to improve.***
- ***Self-protection: Defend against accidental or malicious external attacks,***
  requires awareness of threats and means to manage them.

Four Attributes

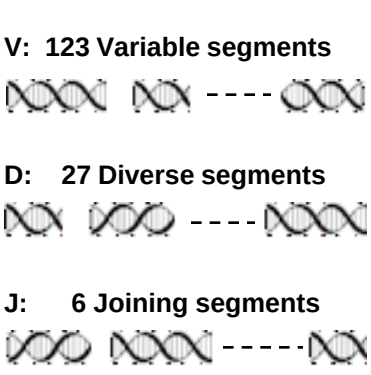
- ***self-aware—aware of its internal state;***
- ***self-situated—aware of current external operating conditions and context;***
- ***self-monitoring—aware of changing circumstances; and***
- ***self-adjusting—able to adapt accordingly.***

J.O. Kephart and D.M. Chess, "The Vision of Autonomic Computing," *Computer, Jan. 2003, pp. 41-52.*
R. Sterritt, "Apoptotic Computing: Programmed Death by Default for Computer-Based Systems," *Computer*, IEEE, Jan. 2011, pp 59-65.

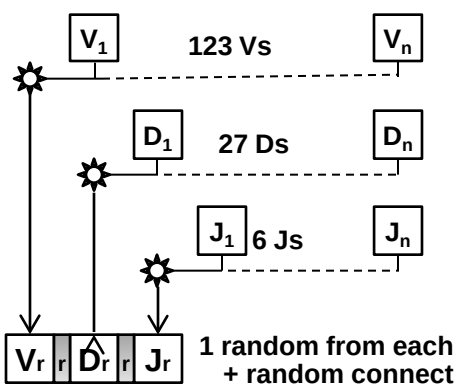
Pattern: Bow Tie Processor (assembler/generator/mediator)



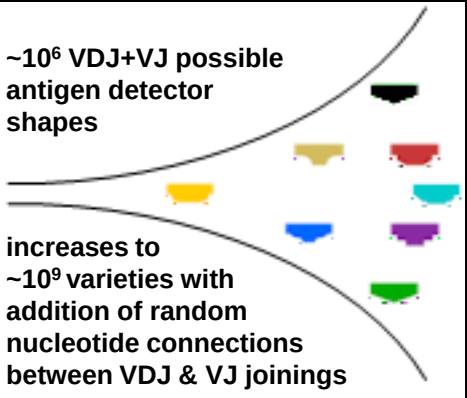
Available high variety genetic DNA input



Evolve three fixed V-D-J gene-segment libraries



Fixed-rule VDJ assembly with random interconnects



Random high variety output with VDJ + VJ assemblies

Millions of random infection detectors generated continuously by fixed rules and modules in the "knot"

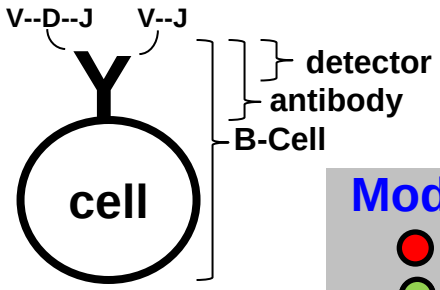
Context: Complex system with many diverse inputs and many diverse outputs, where outputs need to respond to many needs or innovate for many or unknown opportunities, and it is not practical to build unique one-to-one connections between inputs and outputs. Appropriate examples include common financial currencies that mediate between producers and consumers, the adaptable biological immune system that produces proactive infection detectors from a wealth of genetic material, and the Internet protocol stack that connects diverse message sources to diverse message sinks.

Problem: Too many connection possibilities between available inputs and useful outputs to build unique robust, evolving satisfaction processes between each.

Forces: Large knot short-term-flexibility vs small knot short-term-controllability and long-term-evolvability (Csete 2004); robustness to known vs fragility to unknown (Carlson 2002).

Solution: Construct relatively small "knot" of fixed modules from selected inputs, that can be assembled into outputs as needed according to a fixed protocol. A proactive example is the adaptable immune system that constructs large quantities of random detectors (antigen epitopes) for unknown attacks and infections. A reactive example is a manufacturing line that constructs products for customers demanding custom capabilities.

Adaptable Immune System
Bow-Tie Antigen-Detector Generator
(agile architectural concept diagram)



Modules

123 V segments | 27 D segments | 6 J segments | random nucleotides

Integrity Management

- Module pools and mix evolution — genetic evolution — (module evolution)
- Module inventory condition — ??repair mechanisms?? — (module inventory)
- Detector assembly — bone marrow and thymus — (system assembly)
- Infrastructure evolution — genetic evolution — (architecture evolution)

Active

Infrastructure

Passive

long chain / short chain → detector sequence n

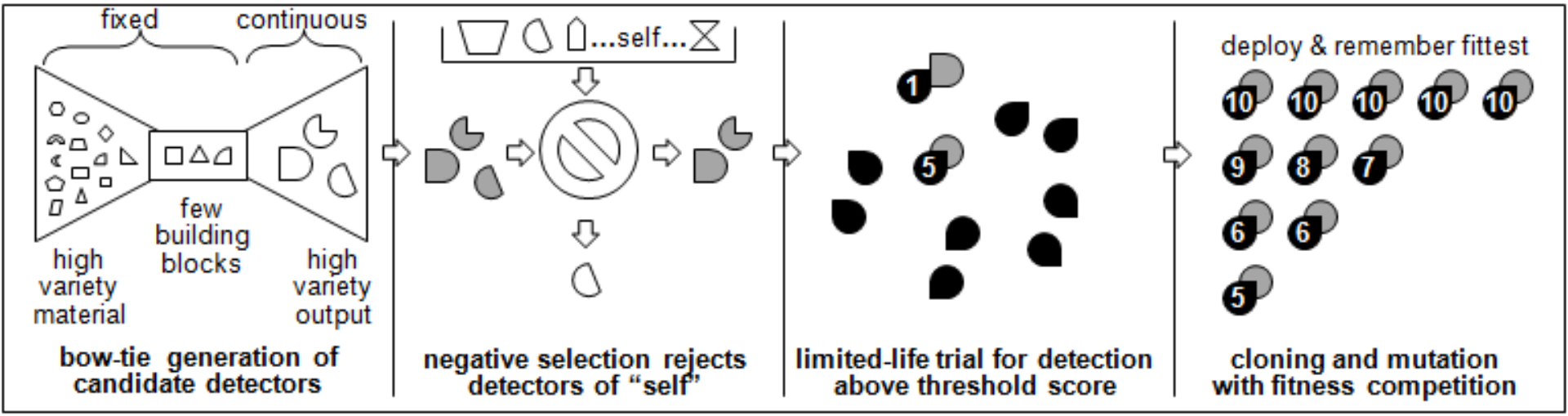
long chain / short chain → detector sequence n+1

long chain / short chain → detector sequence n+2

Assembly Rules

- Use one each V-J
- Use one each V-D-J
- Add random nucleotides
- Combine two assemblies

Pattern: Proactive Search



Speculative generation and mutation of detectors recognizes new attacks like a biological immune system

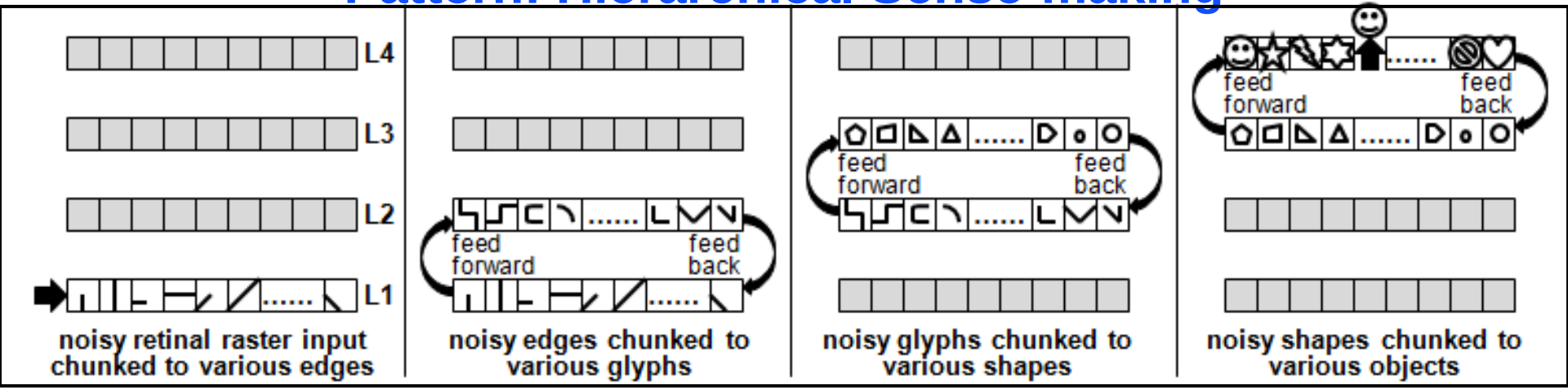
Context: **A complex system or system-of-systems subject to attack and infection, with low tolerance for attack success and no tolerance for catastrophic infection success; with resilient remedial action capability when infection is detected. Appropriate examples include biological organisms, and cyber networks for military tactical operations, national critical infrastructure, and commercial economic competition.**

Problem: **Directed attack and infection types that constantly evolve in new innovative ways to circumvent in-place attack and infection detectors.**

Forces: **False positive tradeoffs with false negatives, system functionality vs functionality impairing detection measures, detectors for anything possible vs added costs of comprehensive detection, comprehensive detection of attack vs cost of false detection of self.**

Solution: **A high fidelity model of biological immune system antibody (detection) processes that generate high quantity and variety of anticipatory speculative detectors in advance of attack and during infection, and evolve a growing memory of successful detectors specific to the nature of the system-of-interest.**

Pattern: Hierarchical Sense-making



Four level feed forward/backward sense-making hierarchy modeled on visual cortex

Context: A decision maker in need of accurate situational awareness in a critical dynamic environment. Examples include a network system administrator in monitoring mode and under attack, a military tactical commander in battle, and the NASA launch control room.

Problem: A very large amount of low-level noisy sensory data overwhelms attempts to examine and conclude what relevance may be present, most especially if time is important or if sensory data is dynamic.

Forces: amount of data to be examined vs time to reach a conclusion, number of ways data can be combined vs number of conclusions data can indicate, static sensory data vs dynamic sensory data, noise tolerated in sensory data vs cost of low noise sensory data.

Solution: Using a bow-tie process, each level looks for a specific finite set of data patterns among the infinite possibilities of its input combinations, aggregating its input data into specific chunks of information. These chunks are fed-forward to the next higher level, that treats them in turn as data further aggregated into higher forms of information chunks. Through feedback, a higher level may bias a lower level to favor certain chunks over others, predicting what is expected now or next according to an emerging pattern at the higher level. Each level is only interested in a small number of an infinite set of data-combination possibilities, but as aggregation proceeds through multiple levels, complex data abstractions and recognitions are enabled.

BIS Architecture

(Biological Immune System)

Antibody Creation & Life Cycle

General antibody life cycle: creation, false-positive testing, deployment efficacy or termination, mutation improvement, and long-term memory.

1. **Candidate antibody semi-randomly created.**
2. **Tolerization period tests immature candidates for false-positive matches.**
3. **Mature & naïve antibodies put into time limited service.**
4. **Activated (B-cell) antibodies need co-stimulation (by T-cells) to ensure "improvement" didn't produce auto-reactive result, non-activated & non-co-stimulated candidates die when time limit ends.**
5. **Highest affinity co-stimulated antibodies are remembered for time-limited long term (eg, many years, decades).**
6. **Co-stimulated antobidies are cloned with structured mutations, looking for improved (higher) affinity scores.**

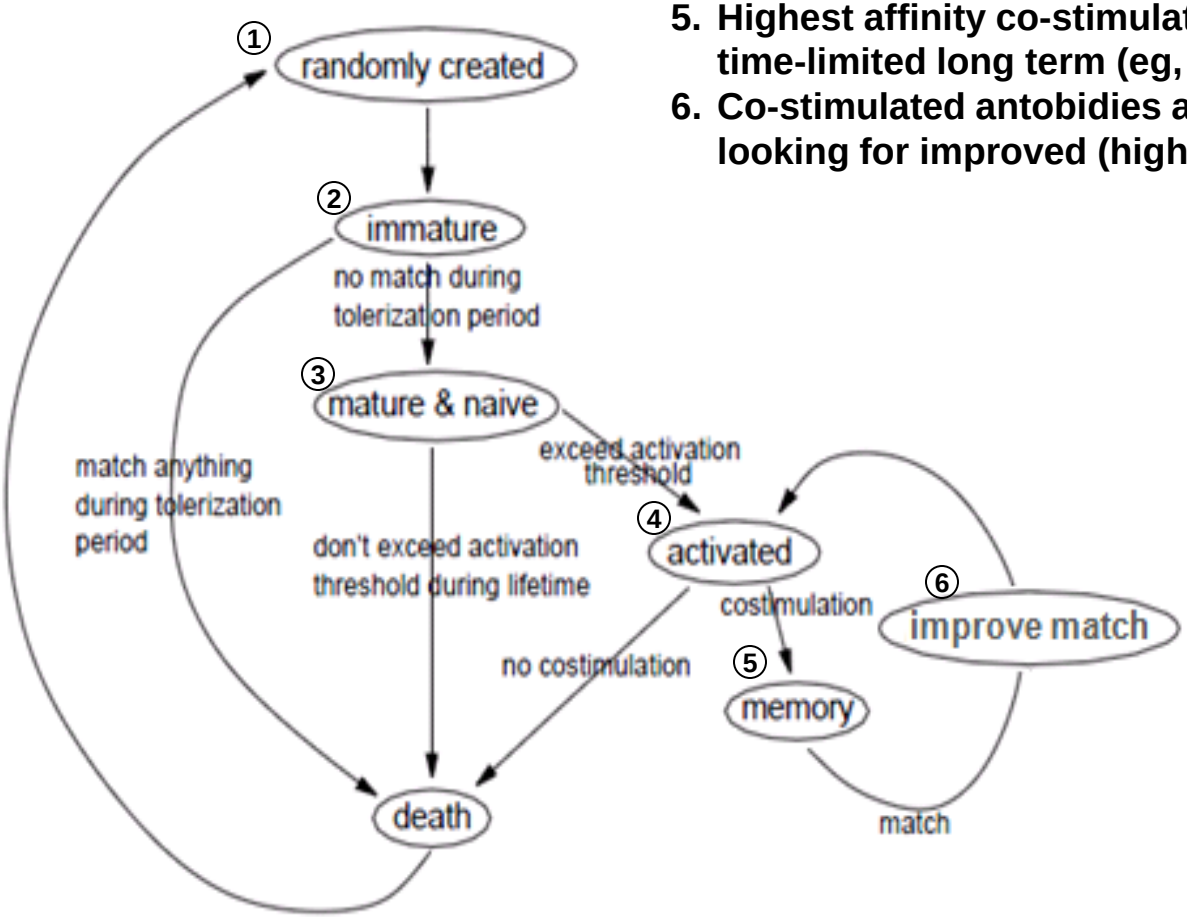


Diagram modified from (Hofmeyr 2000).

SORNS Grounding

Self Organizing Resilient Network – Sensing

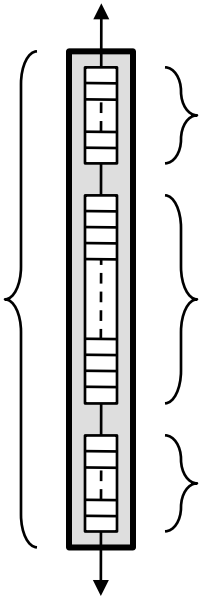
an artificial immune system example under development for a resilient cyber-network sense and sense-making application

Reconfigurable Pattern Processor

Reusable Cells Reconfigurable in a Scalable Architecture

Independent detection cell: content addressable by current input byte

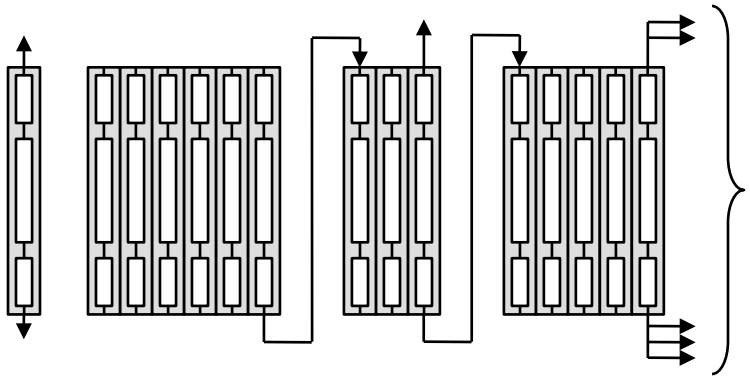
If active, and satisfied with current byte, can activate other designated cells including itself



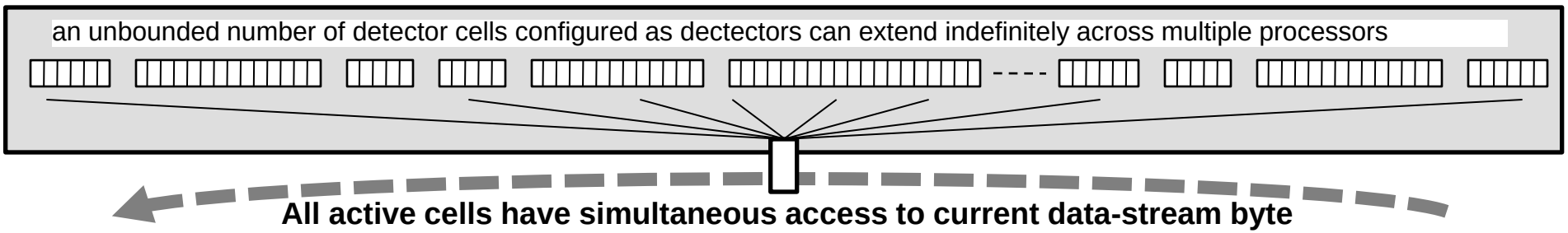
Cell-satisfaction output pointers

Up to 256 possible features can be "satisfied" by all so-designated byte values

Cell-satisfaction activation pointers



Individual detection cells are configured into *detectors* by linking activation pointers.



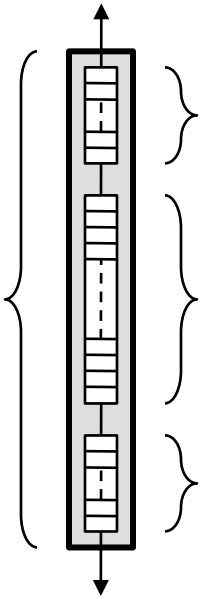
All active cells have simultaneous access to current data-stream byte

Reconfigurable Pattern Processor

Reusable Cells Reconfigurable in a Scalable Architecture

Independent detection cell: content addressable by current input byte

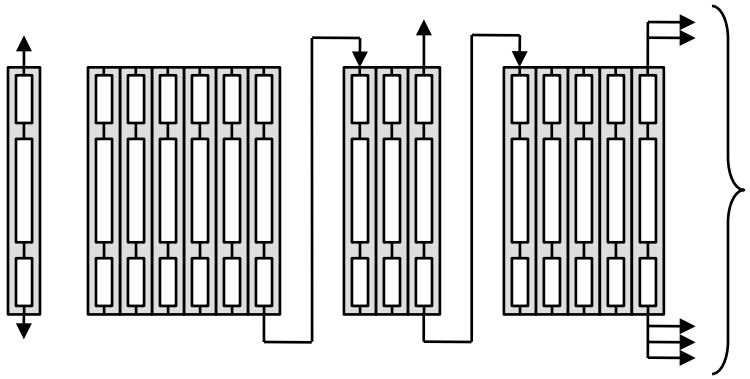
If active, and satisfied with current byte, can activate other designated cells including itself



Cell-satisfaction output pointers

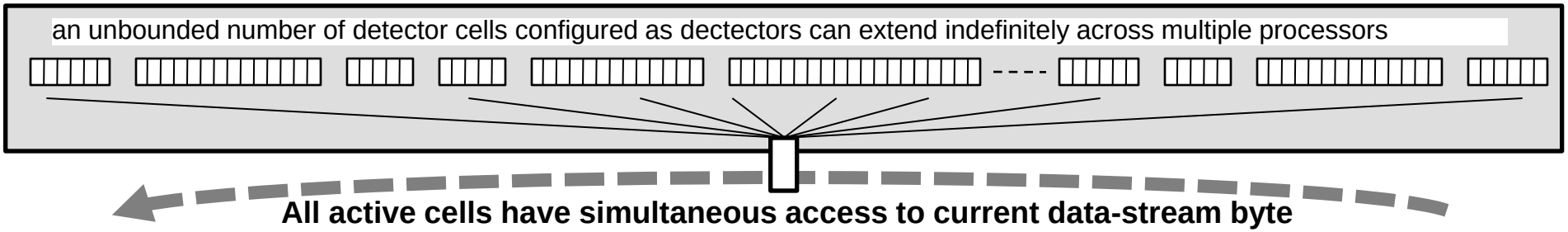
Up to 256 possible features can be "satisfied" by all so-designated byte values

Cell-satisfaction activation pointers



Individual detection cells are configured into *detectors* by linking activation pointers.

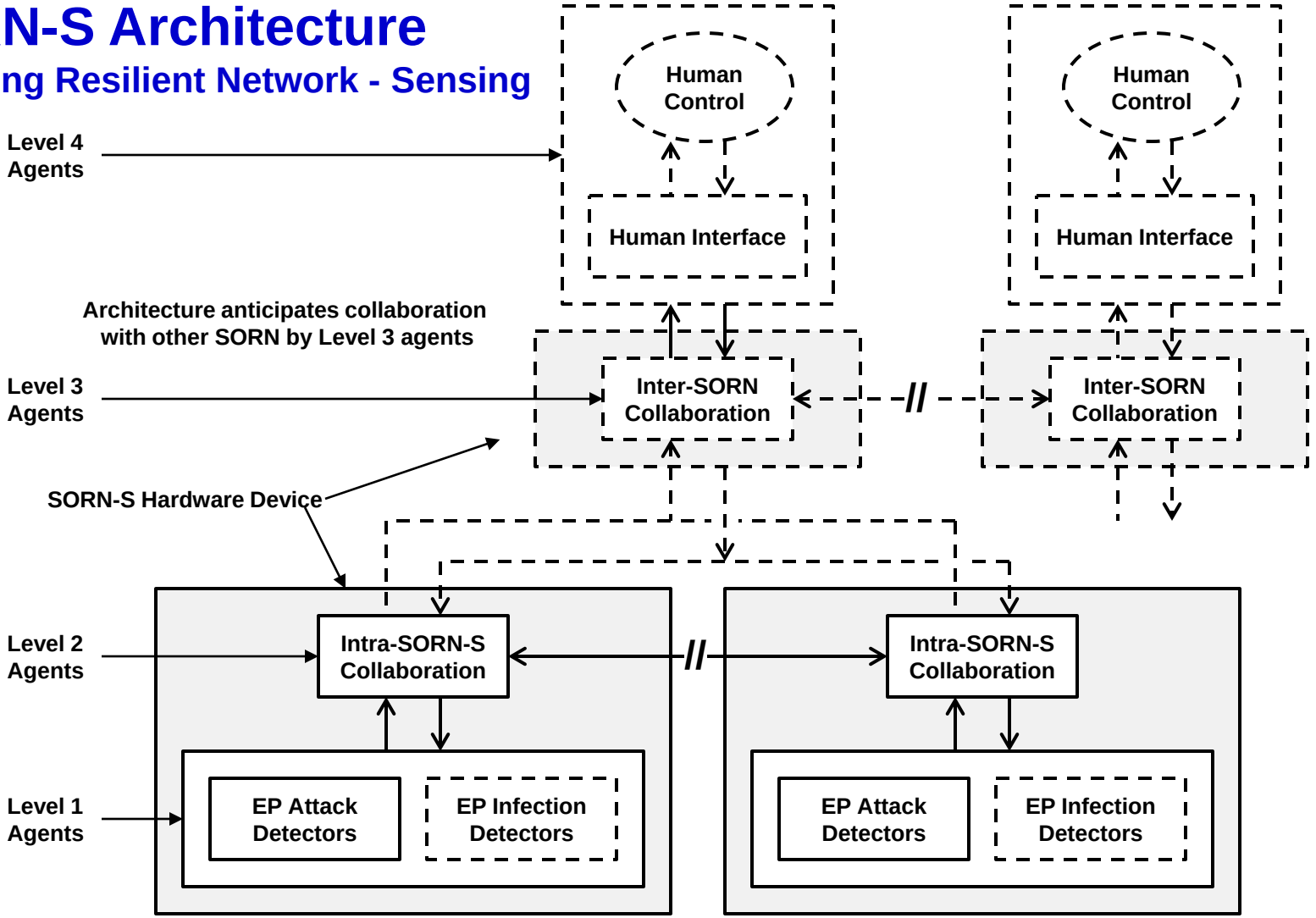
Enables High Fidelity Modeling



All active cells have simultaneous access to current data-stream byte

SORN-S Architecture

Self Organizing Resilient Network - Sensing



Multi-level architecture refines sensory input through learning and sensemaking hierarchy, supports remedial action agents (human/automated) with succinct relevant information.

Notes:

- **For general all-level hierarchical network-agent architecture general concept see (Haack 2009)**
- **For hierarchical feed-forward/backward pattern learning, prediction, and sense-making see (George 2009).**
- **For all-level hierarchical learning of causal patterns spread as time-sequence events see (Hawkins 2010).**

Level 1 & 2 Agent: Detector Creation & Learning Architecture

General L1 detector life cycle: creation, false-positive testing, deployment efficacy or termination, mutation improvement, and long-term memory.

1. **Candidate fuzzy detector semi-randomly created.**
2. **Tolerization period tests immature candidates for false-positive matches.**
3. **Mature & naïve candidates put into time limited service.**
4. **Activated (B-cell) candidates wait for co-stimulation (by T-cells) to ensure "improvement" didn't produce auto-reactive result, non-activated & non-co-stimulated candidates die when time limit ends.**
5. **Highest scoring co-stimulated candidates are remembered for time-limited long term.**
6. **Co-stimulated candidates are cloned with structured mutations, looking for improved (higher) activation scores.**
7. **Level 2 Agent insertion of activated candidates from other end-points, and Level 2 Agent distribution of activated candidates to other end points.**

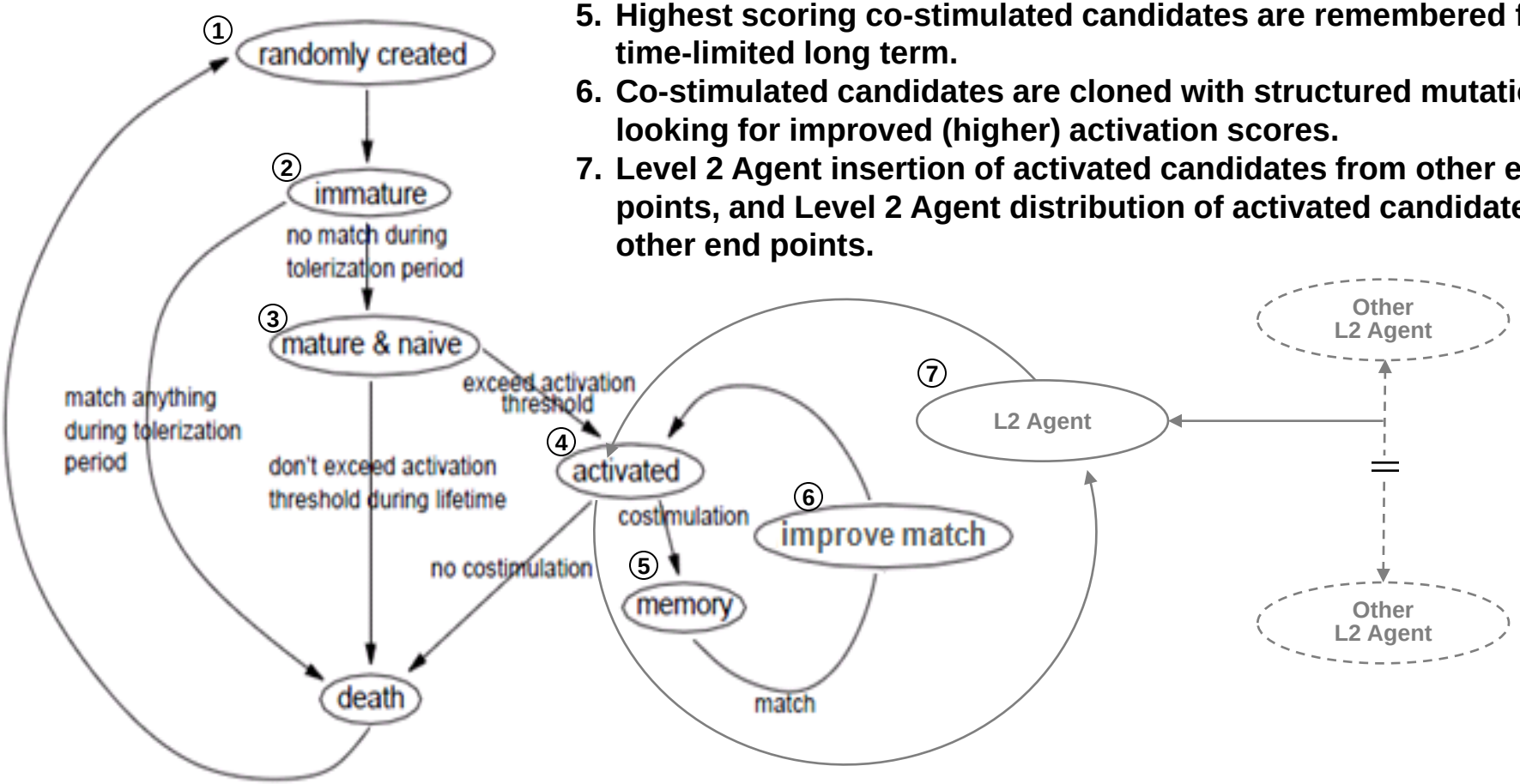


Diagram modified from (Hofmeyr 2000).

Level 1 & 2 Agent: Detector Creation & Learning Architecture

General L1 detector life cycle: creation, false-positive testing, deployment efficacy or termination, mutation improvement, and long-term memory.

1. **Candidate fuzzy detector semi-randomly created.**
2. **Tolerization period tests immature candidates for false-positive matches.**
3. **Mature & naïve candidates put into time limited service.**
4. **Activated (B-cell) candidates wait for co-stimulation (by T-cells) to ensure "improvement" didn't produce auto-reactive result, non-activated & non-co-stimulated candidates die when time limit ends.**
5. **Highest scoring co-stimulated candidates are remembered for time-limited long term.**
6. **Co-stimulated candidates are cloned with structured mutations, looking for improved (higher) activation scores.**
7. **Level 2 Agent insertion of activated candidates from other end-points, and Level 2 Agent distribution of activated candidates to other end points.**

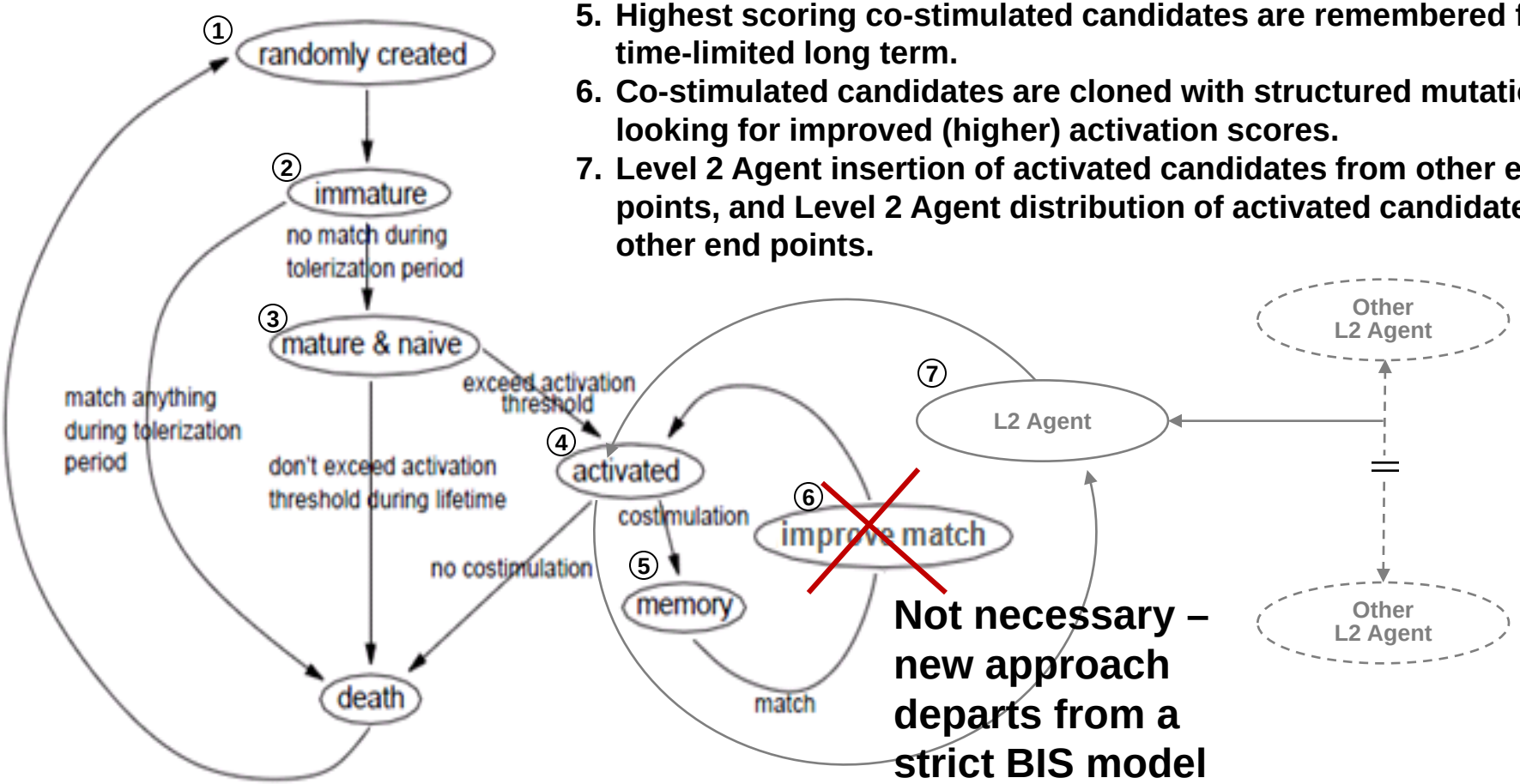


Diagram modified from (Hofmeyr 2000).

Detection Categories (Types)

Spatial Connection	L1 packet headers (feasibility demo for TCP/UDP/ICMP).
Spatial Content	L1 deep packet inspection (feasibility demo for HTTP/SMTP???).
Temporal Connection	L2 multi-packet header detectors (feasibility demo for TCP/UDP/ICMP).
Temporal Content	L2 multi-packet content detectors (feasibility demo for HTTP/SMTP???).

Rather than categorize by attack type (like UTMs do), of which there is a never-ending list as new types emerge, our categories relate to the detection philosophy:

Automated learning of spatial and temporal pattern features within a fixed set of generic pattern structures.

A syn flood attack, e.g. is one instance within the temporal-connection pattern category.

- **Spatial means a collection of features at one instant (packet/log-entry) in time that is detected as a pattern-of-interest.**
- **Temporal means multi-packet/multi-log-entry features that are detected as a pattern.**
- **Correlative (unaddressed here) means multi-flow/multi-log features detected as a pattern.**

Phase 1 Initial Focus

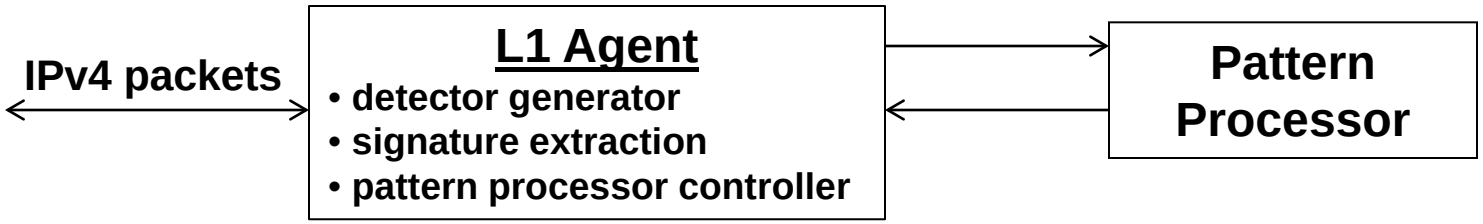
IPv4 packet-header detection

– single packet-header signature patterns (spatial connection category)

Three elements to a pattern signature: address – port – type

- **Address: 4 bytes - Only the non-host address is of interest.**
- **Port: 2 bytes - Only the non-host port is of interest (under question).**
- **Packet types: 3 bits covers 6 types – (TCP, UDP, ICMP) x (incoming, outgoing)**

The L1-Agent preprocessor/controller strips relevant information for packets and feeds the pattern processor

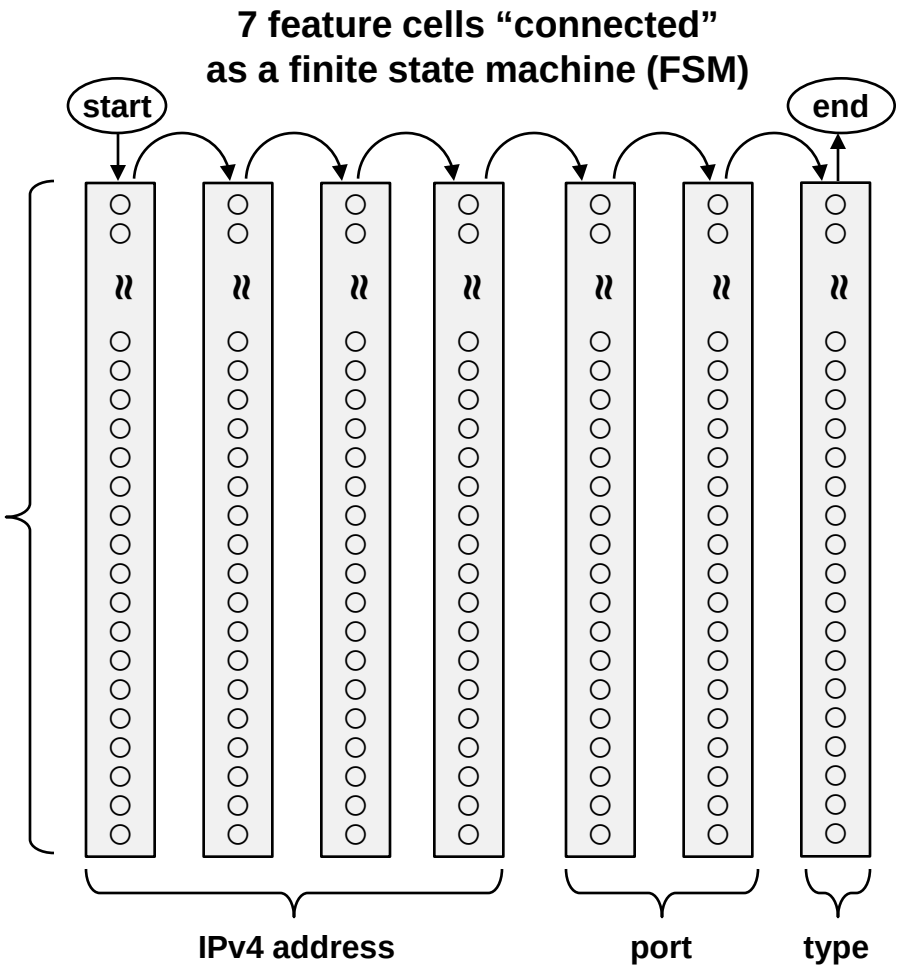


Feature Cells and Finite State Machines
(Illustrative example of pattern processor capability)

256 bit associative memory feature cells (columns).

All active cells are indexed by the input stream's current byte value.

If the index finds a set bit, the next feature cell is activated and looks at the next stream byte, else the process dies.

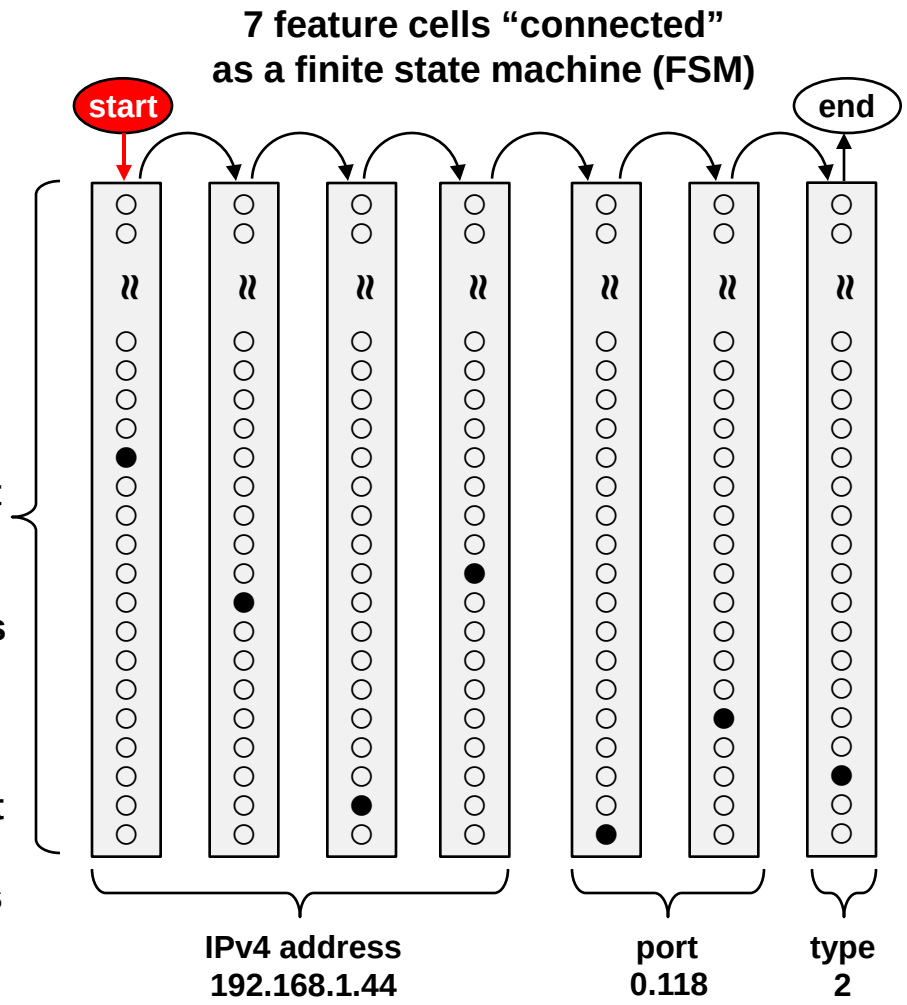


Feature Cells and Finite State Machines
(Illustrative example of pattern processor capability)

256 bit associative memory feature cells (columns).

All active cells are indexed by the input stream's current byte value.

If the index finds a set bit, the next feature cell is activated and looks at the next stream byte, else the process dies.



Loaded with 7 values

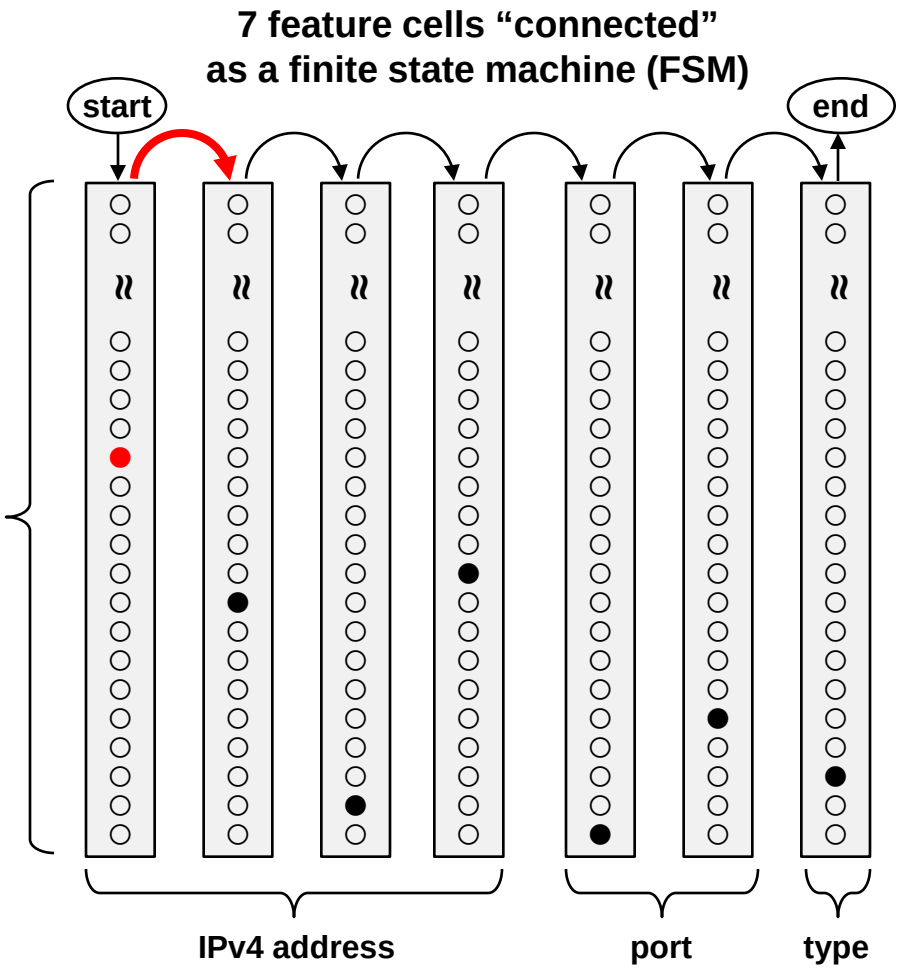
192.168.1.44, 0.118, 2

Feature Cells and Finite State Machines
(Illustrative example of pattern processor capability)

256 bit associative memory feature cells (columns).

All active cells are indexed by the input stream's current byte value.

If the index finds a set bit, the next feature cell is activated and looks at the next stream byte, else the process dies.



Processing Data Stream

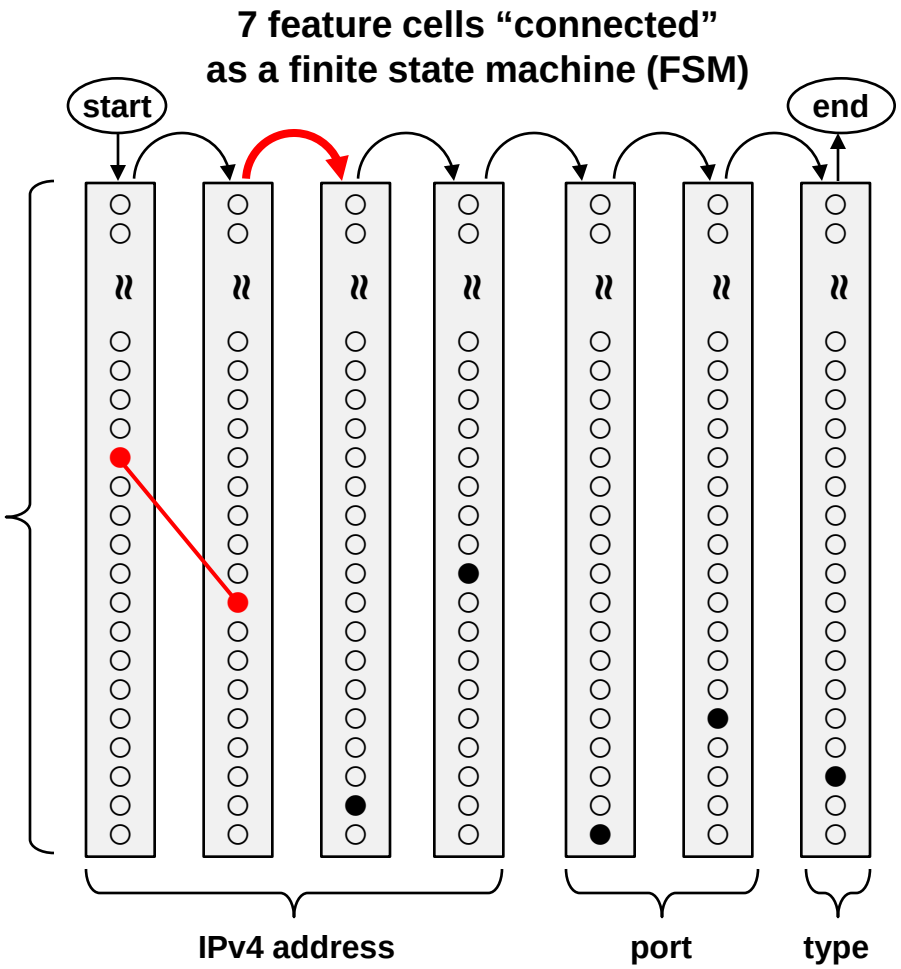
192.168.1.44, 0.118, 2

Feature Cells and Finite State Machines
(Illustrative example of pattern processor capability)

256 bit associative memory feature cells (columns).

All active cells are indexed by the input stream's current byte value.

If the index finds a set bit, the next feature cell is activated and looks at the next stream byte, else the process dies.



Processing Data Stream

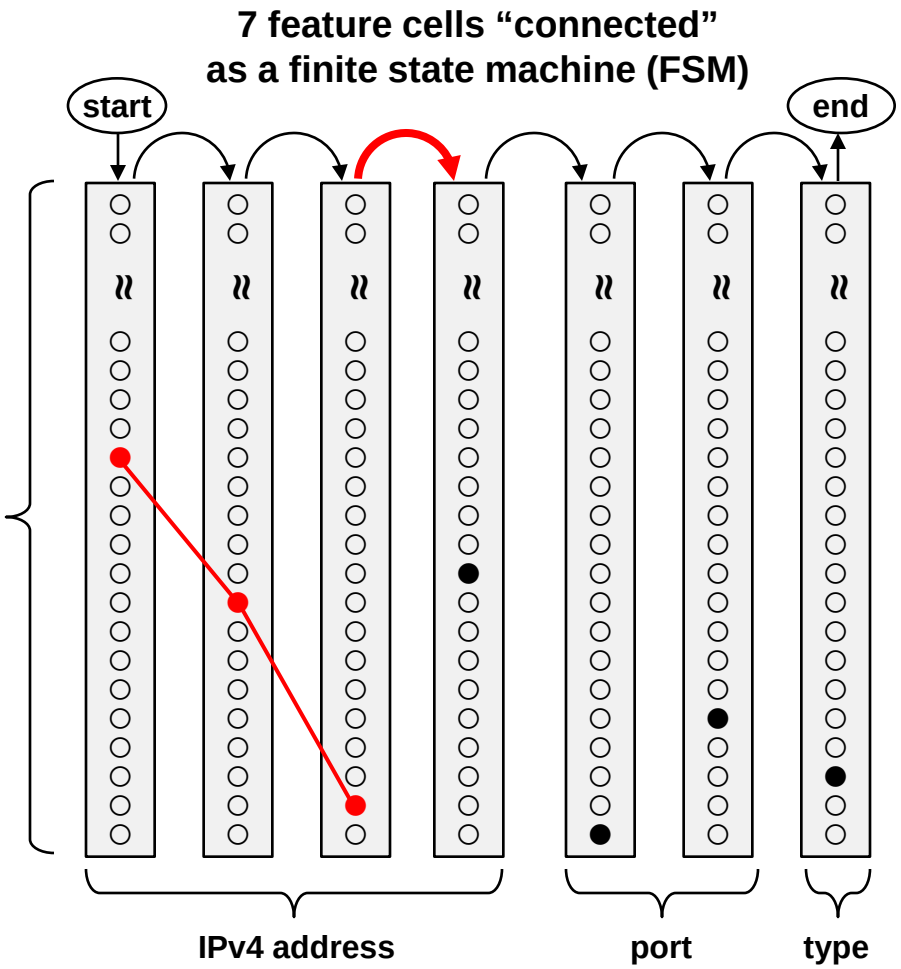
192.168.1.44, 0.118, 2

Feature Cells and Finite State Machines
(Illustrative example of pattern processor capability)

256 bit associative memory feature cells (columns).

All active cells are indexed by the input stream's current byte value.

If the index finds a set bit, the next feature cell is activated and looks at the next stream byte, else the process dies.



Processing Data Stream

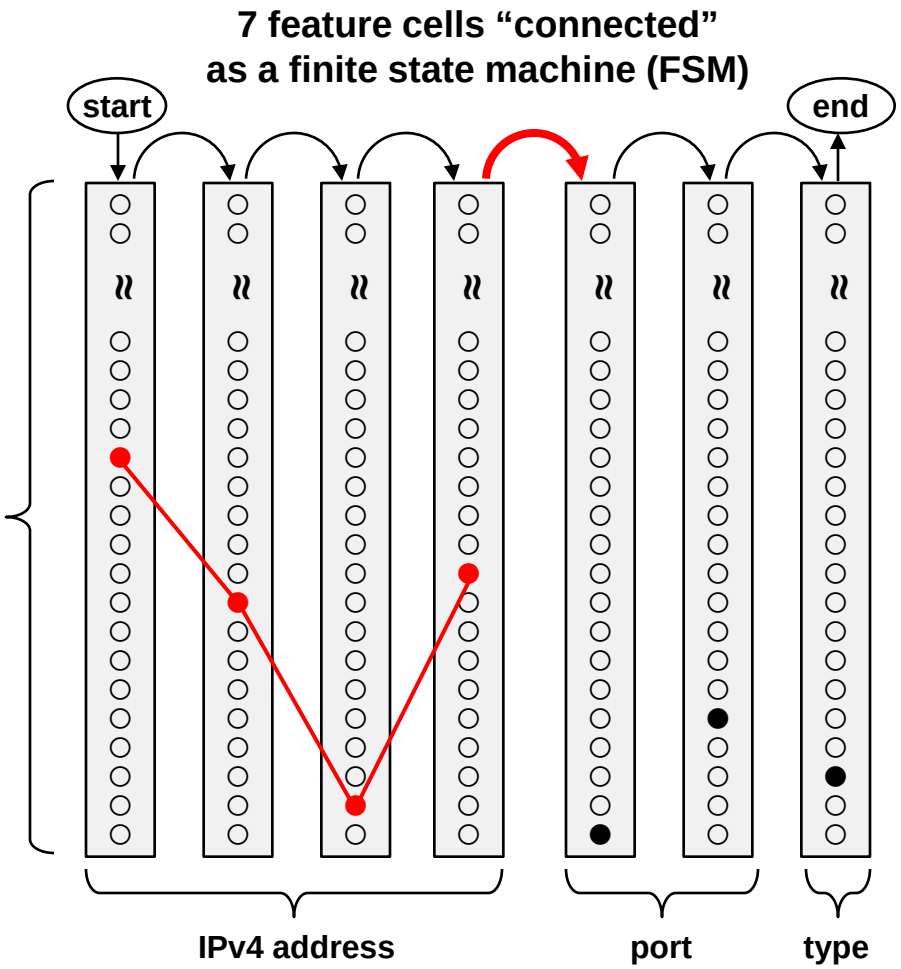
192.168.1.44, 0.118, 2

Feature Cells and Finite State Machines
(Illustrative example of pattern processor capability)

256 bit associative memory feature cells (columns).

All active cells are indexed by the input stream's current byte value.

If the index finds a set bit, the next feature cell is activated and looks at the next stream byte, else the process dies.



Processing Data Stream

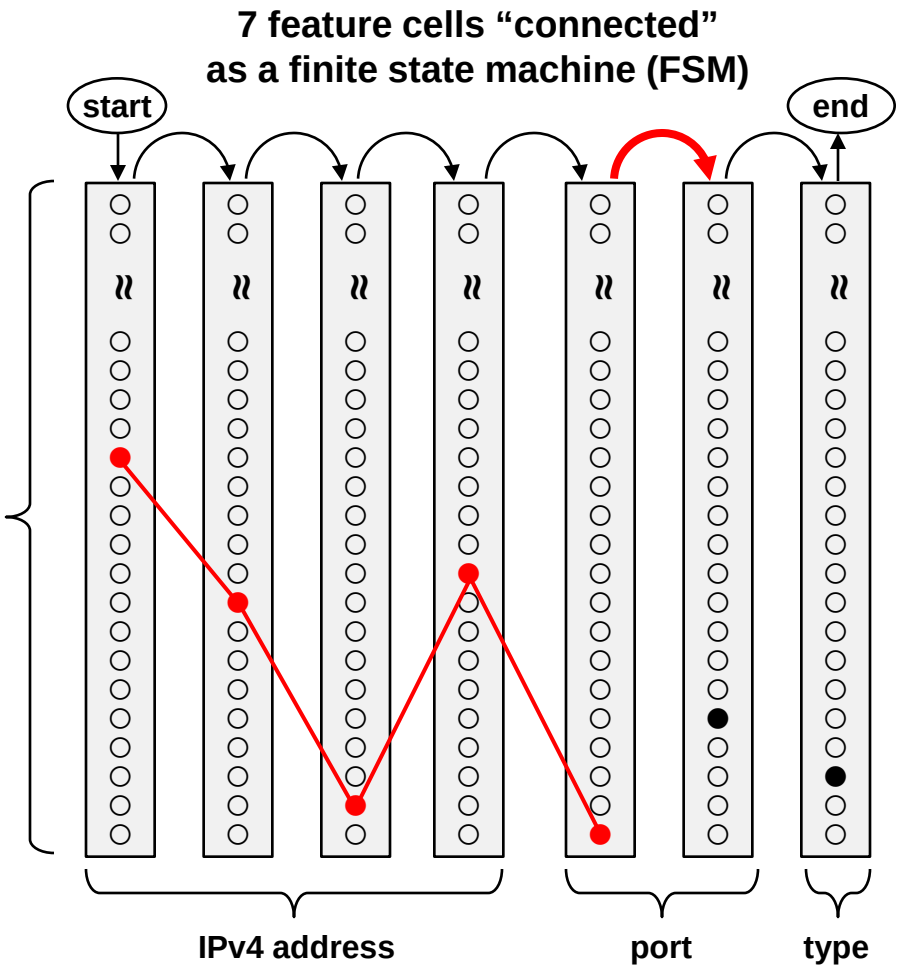
192.168.1.44, 0.118, 2

Feature Cells and Finite State Machines
(Illustrative example of pattern processor capability)

256 bit associative memory feature cells (columns).

All active cells are indexed by the input stream's current byte value.

If the index finds a set bit, the next feature cell is activated and looks at the next stream byte, else the process dies.



Processing Data Stream

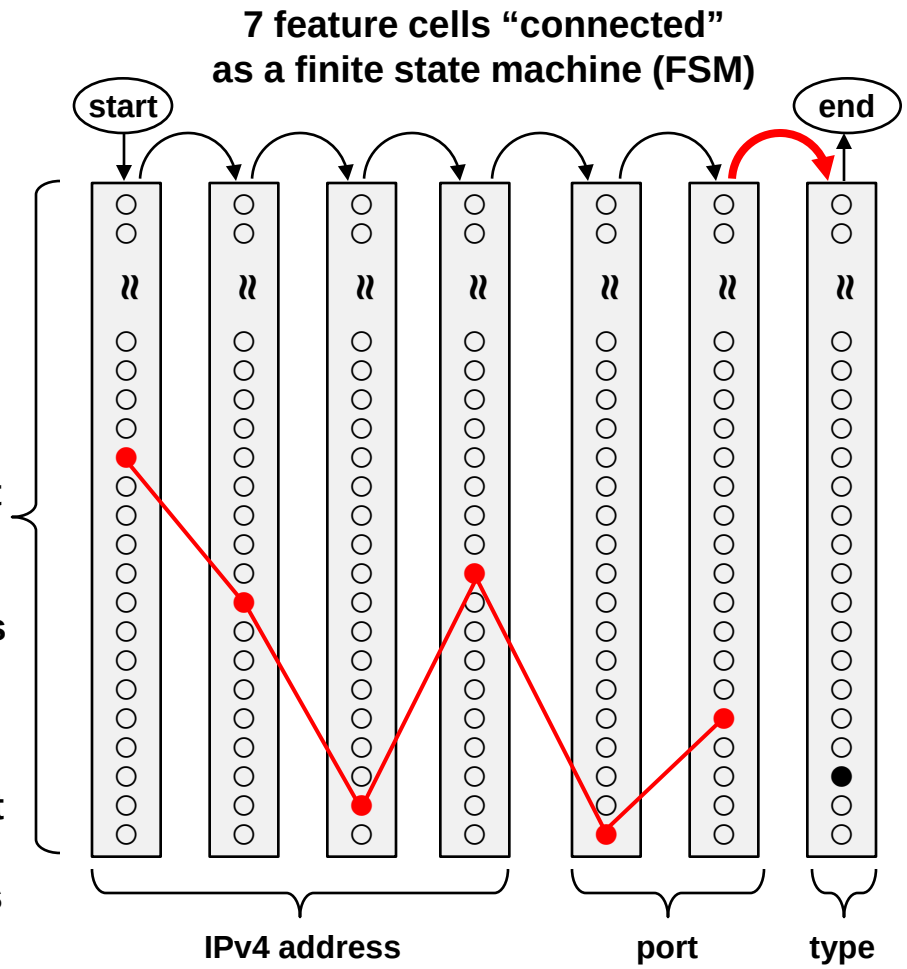
192.168.1.44, 0.118, 2

Feature Cells and Finite State Machines
(Illustrative example of pattern processor capability)

256 bit associative memory feature cells (columns).

All active cells are indexed by the input stream's current byte value.

If the index finds a set bit, the next feature cell is activated and looks at the next stream byte, else the process dies.



Processing Data Stream

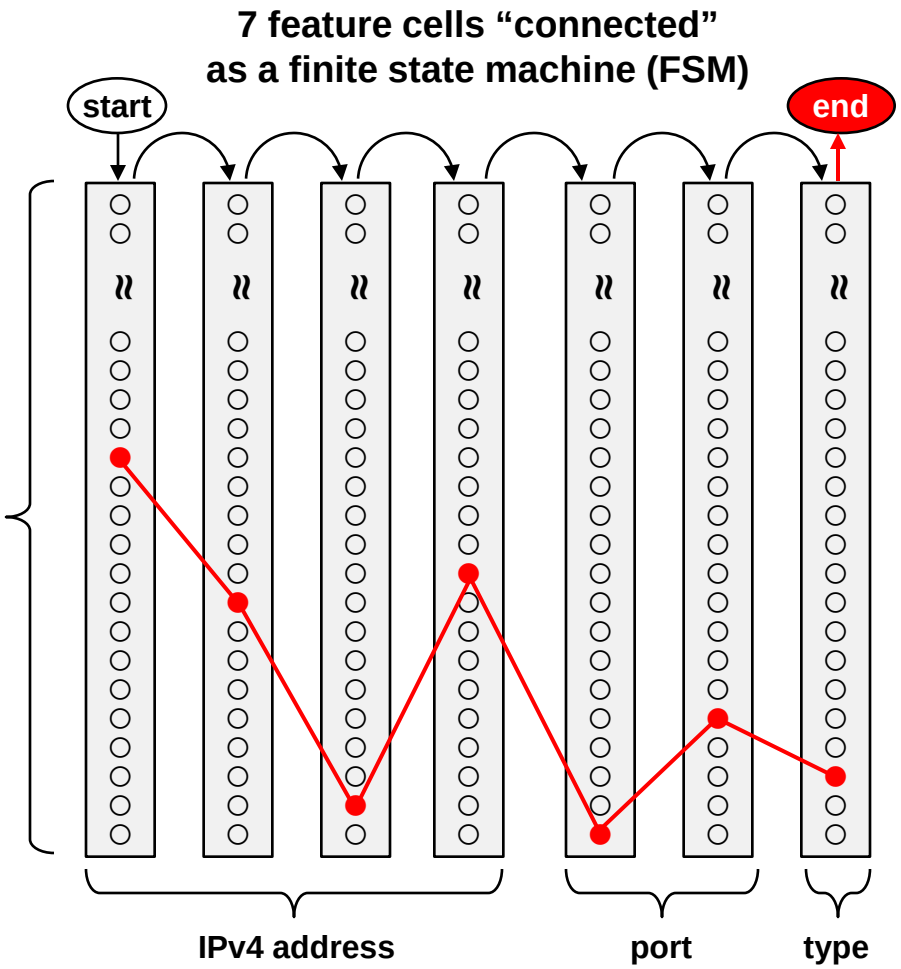
192.168.1.44, 0.118, 2

Feature Cells and Finite State Machines
(Illustrative example of pattern processor capability)

256 bit associative memory feature cells (columns).

All active cells are indexed by the input stream's current byte value.

If the index finds a set bit, the next feature cell is activated and looks at the next stream byte, else the process dies.



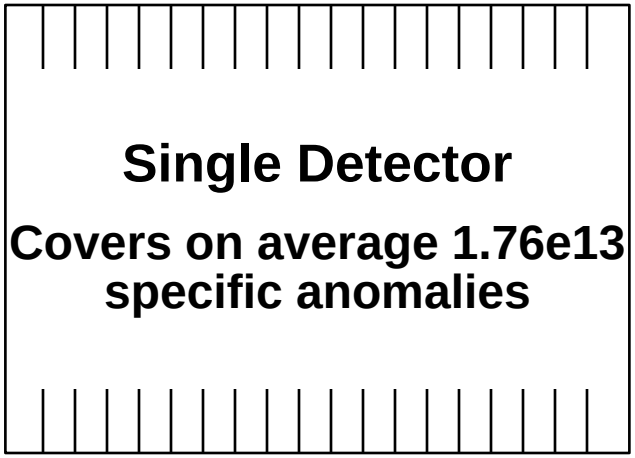
Processing Data Stream

192.168.1.44, 0.118, 2

Detector “Pattern Space” Coverage

Methods Cannot be Shared as Yet…But

2^{51} possible patterns
= 2.25e15



~0.78% average pattern space covered per detector

<u>Current Model Under Test</u>
256 Detectors in Training Pool
1024 Detectors in Service Pool

With lots of pattern-chip capacity still unused

Other Aware-Systems Domains

applications in non-cyber domains
sensors are proliferating – sensemaking needs attention

Automated Disease Surveillance

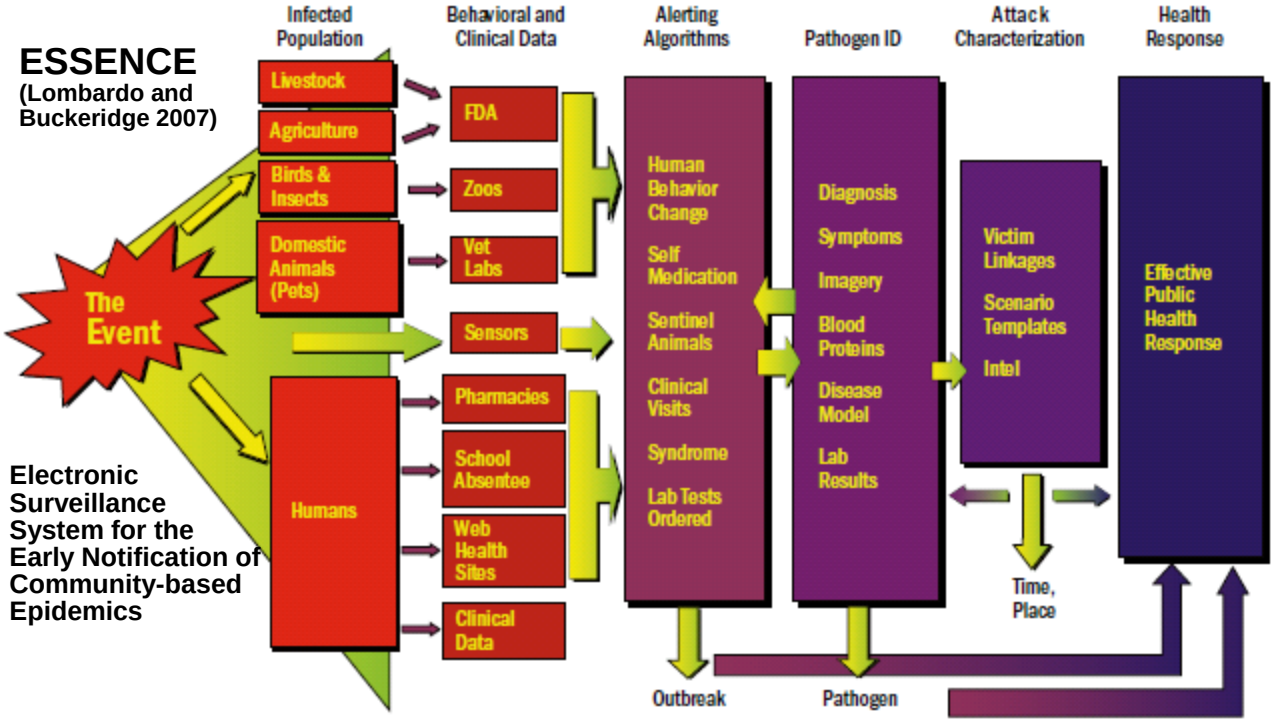
Requirements Challenges

The requirements include a significant reduction in the time for the recognition of a significant health event so that an effective public-health response can be launched to minimize casualties.

The system must be able to recognize emerging health risks for both naturally occurring infectious diseases and those that are intentional. False positives must be kept to a minimum, and periodic evaluation is needed to ensure that the system provides the performance needed.

For an automated disease-surveillance system to achieve timely positive detection of a covert attack of weaponized bacillus anthracis spores, the system must rely on the behaviors of individuals manifesting early symptoms of the disease. The system may also need to rely on other sources of information not used in a clinical setting.

ESSENCE
(Lombardo and Buckeridge 2007)



Electronic Surveillance System for the Early Notification of Community-based Epidemics

Figure 2. Concept of operations used in the development of ESSENCE

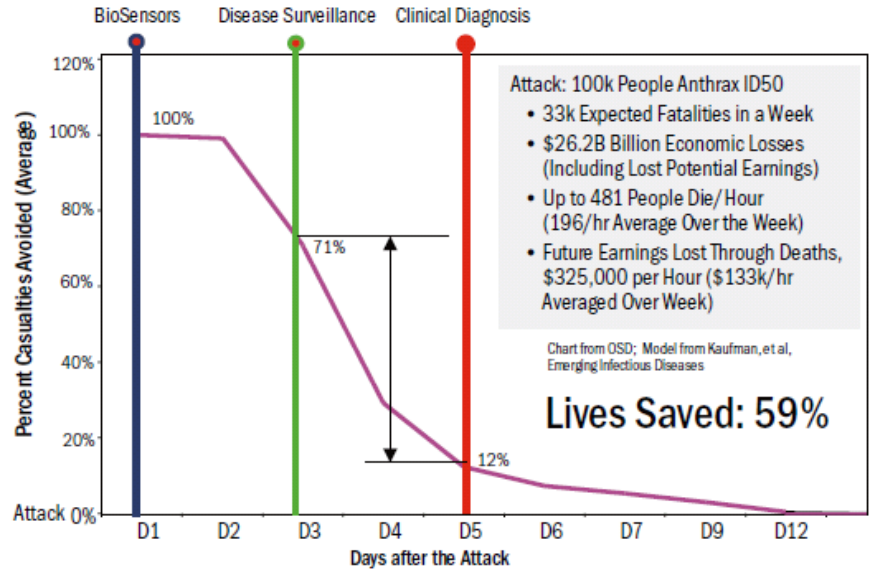


Figure 1. Comparison of the value of sensors, automated disease surveillance, and routine clinical diagnosis in the recognition of a biological attack

Joseph Lombardo, Sheri Lewis, Rich Wojcik, and Wayne Loschen. 2010. Systems Engineering to Support Discovery of Threats to Public Health. INSIGHT 13(4), December.

Smart Roads. Smart Bridges.

7Feb2009, WSJ, http://online.wsj.com/article/SB123447510631779255.html

SMART MOVES Freeway signs give estimated travel times and other information on Interstate Highway 80 in the San Francisco Bay area.

Radio receivers are installed along several freeways in the San Francisco Bay area that read the electronic toll tags in passing cars.

One promising avenue: real-time information about road conditions, traffic jams and other events.

The next generation of technologies promises to get that news -- and even more detailed information -- directly to drivers in their cars.

dove@parsh

Gi-Lu Cable-Stay Bridge in Taiwan has wireless sensors and accelerometers that monitor its structural health.

www.scientificamerican.com/slideshow.cfm?id=smart-bridges-harness-tech&photo_id=EF0F0341-A452-806C-8CDD679765CAA94B

Fractal at national transmission and local distribution levels.

Securing the Smart Grid: Next Generation Power Grid Security

Chapter 2 provides an overview of the threats and impacts of smart metering at the consumer level.

With the benefits come security and privacy issues.

Leaving security to vendors of home-based products has traditionally not been met with much success.

Chapter 4 notes … An important group working on this is the NIST Cyber Security Working Group (CSWG). The primary goal of the CSWG is to develop an overall cyber security strategy for the smart grid. This strategy addresses prevention, detection, response, and recovery.

The CSWG recently created NISTIR 7628 — Guidelines for Smart Grid Cyber Security.

Review: samzenpus, 5Jan2010, http://books.slashdot.org/story/11/01/05/1251224/Securing-the-Smart-Grid?from=headlines

Smart grids are a reality and the future, and they promise greater reliability, affordability, efficiency and, hopefully, a better and environmentally cleaner exploitation of available resources. But all that brings to light new threats to the grids. What does that entail and what can we do to defend them - these are the two main questions that this book offers the answers to.

You'll find out more about the threats to smart grids: natural, individual and organizational threats. A special part of the chapter is dedicated to the hacker threat and its various incarnations and motives. The impacts of these threats on utility companies and others are next, with various believable scenarios that point out the threats, their attack vectors and their impacts. From threats to individuals to those to entire countries - it makes you realize what the danger really is.

Review: Zeljka Zorz, 6Dec2010, www.net-security.org/review.php?id=240

Assessing Fleet Characteristics Useful for Sensing

Michael J. Ravnitzky, Offering Sensor Network Services Using the Postal Delivery Vehicle Fleet, 18th Conference on Postal and Delivery Economics, Center for Research in Regulated Industries, Porvoo, Finland, June 2-5, 2010
http://www.prc.gov/(S(je2vev45qxfhtai2g3npcczd))/prc-docs/newsroom/techpapers/Ravnitzky Postal Sensors Paper 070910-MJR-1_1191.pdf

Fleet Type	Single National Owner	Regular Routes	Time on the Road	Universal Geographic Coverage	Centralized Maintenance	Geographic Flexibility / Selectivity
Taxis			X			
Police Cars			X		X	
City Buses		X	X		X	
School Buses		X			X	
City Fleet					X	
UPS / FedEx	X	Limited	X	X	X	Limited
Postal Trucks	X	X	X	X	X	X

From Slashdot: The US Postal Service may face insolvency by 2011 (it lost $8.5 billion last year). An op-ed piece in the December 17, 2010 New York Times proposed an interesting business idea for the Postal Service: use postal trucks as a giant fleet of mobile sensor platforms.Think Google Streetview on steroids. The trucks could be outfitted with a variety of sensors (security, environmental, RF ...)

Potential Applications for Postal Truck-Borne Mobile Sensors

Michael J. Ravnitzky, Offering Sensor Network Services Using the Postal Delivery Vehicle Fleet, 18th Conference on Postal and Delivery Economics, Center for Research in Regulated Industries, Porvoo, Finland, June 2-5, 2010
http://www.prc.gov/(S(je2vev45qxfhtai2g3npcczd))/prc-docs/newsroom/techpapers/Ravnitzky Postal Sensors Paper 070910-MJR-1_1191.pdf

Application Description	Likely Customer Base
Chemical Agents	DHS, States
Biological Agents	DHS, States
Radiological Materials	DOE, DHS, States
Air Quality	EPA, States, Cities
Environmental Sensing	EPA, States, USDA, Cities
Radio/Television Signal Strength	FCC, Telecoms
Wireless Signal Strength	FCC, Telecoms
Weather/ Meteorological	National Weather Service
Pothole Mapping/Road Assessment	Public Works Departments
Natural Gas Leaks	Gas Utilities
License Plate Scanning	Law Enforcement
Methamphetamine Labs	Law Enforcement
Marijuana Farms/ Drug Depots	Law Enforcement
Illicit Explosives Production	Law Enforcement
Photo Imaging	Google, Law Enforcement, Local Governments
Noise Profiling/ Acoustic Signature	Zoning, Cities, Research
Pest Control	State, County Governments
Biological Surveys	Scientific Community
Nuclear Radiation Leaks	NRC, Utilities
Electric Field Mapping	EPA, Cities, Scientific Community
Magnetic Field Mapping	EPA, Cities, Scientific Community
Other Scientific Investigation	DoD, DOE, Scientific Community,
Meter Reading	Universities

Personal weather station is alien chic

"Weather information from thousands of personal weather stations are being used for weather forecasting by several private and government agencies, including the National Oceanic and Atmospheric Administration (NOAA) and the Dept. of Homeland Security (DHS).

The Citizens Weather Observation Program (CWOP) was created by a few amateur radio operators experimenting with transmitting weather data with packet radios, but it has expanded to include Internet-only weather stations as well. As of September 2007, nearly 5,000 stations worldwide reported weather data regularly to CWOP's FindU database.

In Feb 2007 (http://www.pnl.gov/main/publications/external/technical_reports/PNNL-16422.pdf) DHS listed CWOP as a national asset to the 'BioWatch' Network, stating that data from personal weather stations could be useful in weather forecasts for hazardous releases.

In 2007, the FindU server received 422,262,687 weather reports which is a 29.5% increase over 2006. ***[http://science.slashdot.org/article.pl?sid=08/01/19/1835237]***

No longer do home forecasting gadgets look like hospital equipment thanks to Oregon Scientific's efforts to add an aesthetic dimension to its products. Its latest offering looks more like a retro sci-fi movie prop than something used to guess whether you should bring a sweater to the picnic.

[http://crave.cnet.com/8301-1_105-9842340-1.html]

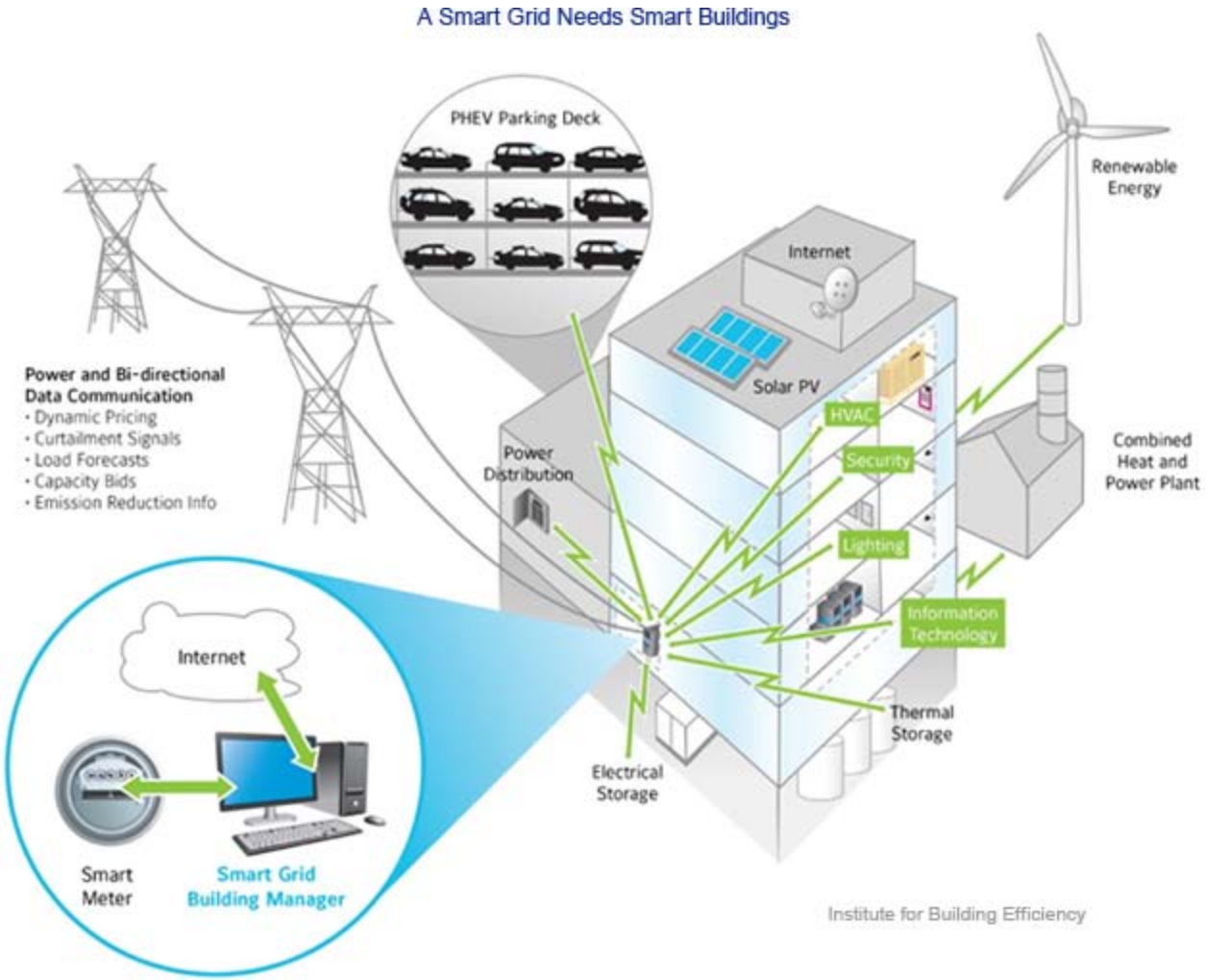
Physical Security & Smart Buildings

Sensors on the property, at the building entry ways, within the building.

IR motion, video, sound, pressure, ….

ID entry ways (key card, fingerprint, iris, facial recognition…)

RFID individual-human tracking within a building




IBM Tivoli

Wrap

SPECIAL FORUM
on NEXT-GENERATION SECURITY at ITNG 2011

International Conference on Information Technology - New Generations (ITNG)
WWW.ITNG.INFO, Las Vegas, Nevada, April 11-13, 2011

Toward Next-Generation Security: Self-Organizing Perspectives, Principles, and Patterns

A new approach to systems security is in order. The innovation of determined adversaries adapts and evolves faster than reactive defense. Looked upon as self-organizing exploitation systems, adversaries are diverse in nature and allegiance, but their strength is rooted in common characteristics: self-organizing, adaptive, evolving, proactive, resilient, and single-minded purpose.

In a word, the adversary is agile. The strength of adversary success stems from common roots. Roots that should be respected and mirrored for parity in new proactive strategy. Critical mass appears to exist, but is working narrowly-focused goals in relative isolation. This forum is a preliminary catalyzing event – one that could inspire a broad based community loosely defined by a shared sense of common goal and principles for next generation security strategy.

Nine papers articulate perspectives, principles and patterns appropriate for a self-organizing system-of-systems security strategy, featuring systemic innovation and evolution enabled by holistic system architecture.

Opportunities…

ITNG April Forum – Catalyzing a Community
there will be an informal diner discussion forum

Contribute a pattern to the growing collection
(and/or Join INCOSE SSE WG)

Write a 2000 word essay for INCOSE Insight July 2011
(Theme: Systems of Systems and Self Organizing Security)

Be a SORN-S Project Reviewer
(Get a work-in-progress project brief, act as soft Red Team)

Be on the Pattern Processor Technology Intro Tour
(Date TBD: pattern processor capability/applications briefing)

References

Armstrong, Robert C. and Jackson R. Mayo. 2009. Leveraging Complexity in Software for Cybersecurity. CIIRW 2009, April 13-15, Oakridge TN. http://portal.acm.org/beta/ft_gateway.cfm?id=1558643&type=pdf&CFID=82493696&CFTOKEN=93605741

Carlson, Jean and John Doyle. 2000. Highly Optimized Tolerance: Robustness and Design in Complex Systems, *Physical Review Letters* 84 (11): 2529–2532, 13 March.

Carlson, Jean and John Doyle. 2002. Complexity and Robustness. PNAS 99: 2538–2545, 19 February.

Csete, Marie and John Doyle. 2010. Bow Ties, Metabolism and Disease, TRENDS in Biotechnology 22(9), September 2004. www.cds.caltech.edu/~doyle/CmplxNets/Trends.pdf.

Dixon, Colin, Anderson, Thomas and Krishnamurthy, Arvind, Phalanx: Withstanding Multimillion-Node Botnets, NSDI'08: Proceedings of the 5th USENIX Symposium on Networked Systems Design and Implementation, April 2008.

Dove, Rick. 2009. Embedding Agile Security in System Architecture. *Insight* 12 (2): 14-17. International Council on Systems Engineering, July. www.parshift.com/Files/PsiDocs/Pap090701Incose-EmbeddingAgileSecurityInSystemArchitecture.pdf

Dove, Rick. 2010. Pattern Qualifications and Examples of Next-Generation Agile System-Security Strategies, IEEE International Carnahan Conference on Security Technology (ICCST), San Jose, CA, USA, 5-8 October.

Dove, Rick. 2010. Self Organizing Resilient Network Sensing Using Patterns from Natural and Adversarial Processes, working paper, www.parshift.com/Files/PsiDocs/PatternsForResilientNetworkSensing&Sensemaking.pdf

Dove, Rick. 2010. Illuminating Next Generation Agile Security Patterns. SERC Security Research Roadmap Workshop, March 31-April 1, Washington, D.C. www.parshift.com/Files/PsiDocs/Pap100331SERC-IlluminatingNextGenAgileSecurityPatterns.pdf

Dove, Rick. 2010. Pattern Qualifications and Examples of Next-Generation Agile System Security Strategies. IEEE International Carnahan Conference on Security Technology (ICCST), San Jose, CA, USA, 5-8 Oct. www.parshift.com/Files/PsiDocs/PatternQualificationsForAgileSecurity.pdf.

Forrest, S., Perelson, A. S., Allen, L., and Cherukuri, R., Self-Nonself Discrimination in a Computer, In Proceedings IEEE Symposium on Research in Security and Privacy, Oakland, CA., May 16–18, 1994.

Forrest, S., Balthrop, J., Glickman, M. and Ackley, D.. K. Park and W. Willins Eds. *The Internet as a Large-Scale Complex System*, Oxford University Press, 2005.

Haack, Jereme N., Glenn A. Fink, Wendy M. Maiden, David McKinnon, and Errin W. Fulp. 2009. Mixed-Initiative Cyber Security: Putting Humans in the Right Loop. www.cs.wfu.edu/~fulp/Papers/mims09f.pdf

Hofmeyr S. and S. Forrest. 2000. "Architecture for an Artificial Immune System." Evolutionary Computation 7(1), Morgan-Kaufmann, San Francisco, CA, pp. 1289-1296. http://cs.unm.edu/~forrest/publications/hofmeyr_forrest.pdf

Mahimkar, A. , Dange, J., Shmatikov, V., Vin, H. and Zhang, Y., dFence: Transparent Network-Based Denial of Service Mitigation, in Proceedings 4th USENIX Symposium on Networked Systems Design and Implementation (NSDI 2007), Cambridge, MA, April, 2007.

Smets, Barth F. and Tamar Barkay. 2005. Horizontal gene transfer: perspectives at a crossroads of scientific disciplines. *Nature Reviews Microbiology* 3, 675-678 (September 2005).

Wilkinson, Sophie, Plants to Bugs: Buzz Off!, Chemical and Engineering News, June 30, 2001.

Woese, Carl. 2000. Interpreting the universal phylogenetic tree. PNAS. 97(15):8392-6. www.ncbi.nlm.nih.gov/pmc/articles/PMC26958/pdf/pq008392.pdf

Zhang, C., Zhang, J., Liu, S., and Liu, Y., Network Intrusion Active Defense Model Based on Artificial Immune System. Fourth International Conference on Natural Computation, Jinan, China, October 18-20, 2008.

Toward Systems with a Will to Live

Autonomic Awareness

Enchantment Chapter Presentation
12 January 2010

dove@parshift.com, attributed copies permitted