NPS CRUSER Technical Continuum

11-12 April 2017

Title: ? Name: Dr. Josef Schaff

Org /NPS Dept: NAVAIR e-mail: josef.schaff@navy.mil

- [x] Littoral Mesh Networking & Remote Sensing
- [ ] Innovative Undersea Warfare (USW)
- [ ] Autonomous USV Missions
- [x] Other Robotics or Autonomy topic

Preferred Date/Time: TUE 11APR [ ] AM [x] PM WED 12APR [ ] AM [ ] PM

Presentation Title:

Leveraging Complexity Science and Emergence for a Self-organizing Battlespace

Abstract: *

The network-centric battlespace is constructed from thousands of decentralized nodes that need to share a world model known as a common operational picture (COP). The nodes represent each element of the battlespace, and consist of the functional element with aspects of communication and simple autonomy. Each node is mapped to a mobile vehicle or static intelligent communication device, and in some cases, can consist of several intelligent sensors at a single location.

To effectively manage the battlespace, each node should have some awareness of the topology of the force laydown, as well as the relative position of some of its neighbors. This knowledge would facilitate rapid self-organizing strategies for dynamic routing of priority data between nodes in one section of the battlespace, with a more distant section. The chosen topology can affect network failures as well as the success of network attacks, and this information should be transferred within a sparse data element, similar to the stigmergic information used by ant colonies (pheromone marker) and beehives (bee “dance”).

Recent work has shown that spatially distributed large ad-hoc networks lose edge-node communication due to scaling issues for the large numbers of networked nodes needed for a battlespace. This can compromise availability within the network. To further complicate matters, a Congressional Research Report from 2007 showed that the resulting scaling limitations were caused by a combinatorial explosion, due to the massive number of route calculations needed for large scale ad-hoc networks.

To remedy this problem in network-centric clouds and swarms, it was postulated that ad-hoc nodes may be able to self-organize using shared topology data for a COP, by leveraging aspects of complexity science within topology, in particular, deterministic chaos. Fractals topologies are frequently the result of deterministic chaos. Historical works by Leyland et al. (1994) have shown the relationship of complexity and fractals, and the behavior of high volume network traffic packets to self-organize into fractal structures. The book titled "Complexity Theory and Network Centric Warfare" by Moffat (2003), and produced by DoD’s Command and Control Research Program, described complex systems and their relationship to fractals and decentralized Net-Centric Warfare. From these historical works, it appears that fractals are an intrinsic factor in massive volumes of data as well as decentralized communications, and therefore may increase availability for large distributed networks.

This research investigated an adaptive fractal algorithm (NPPR) for emergent self-organizing topologies, that may improve the availability and resiliency for large ad-hoc networks required for cyber offense and defense. The results of this study showed stigmergic behavior, where two variables were able to dynamically convey the collective topology to all network nodes. By using a linear equation similar to the point-slope line equation, the calculation requirement for each node to compute the relative positions of 10,000 other nodes in under 100 milliseconds, was met by even the slowest computational nodes. The resulting topologies exhibited swarm-like self-organizing behaviors that clustered around targets and rendezvous points.

Please see http://CRUSER.nps.edu for additional details on concepts

Please note: *abstracts should be 300-500 words*

Due by 1 March to techcon@nps.edu

2017-04-11

Leveraging Complexity Science and Emergence for a Self-organizing Battlespace [video]

Schaff, Josef

Naval Postgraduate School, Monterey, California

Leveraging Complexity Science and Emergence for a Self-organizing Battlespace

Dr. Josef Schaff, NAVAIR 4.5

What is complexity science?

- Complexity science is informally known as ***order creation science.*** Novel coherent properties can result from self-organizing System of Systems (SoS). Collective actions of many entities in a system produces *emergence*.
- **There are various methods to create complex SoS and emergence, for example:**
  - New approaches in computational (experimental) mathematics for multi-agent systems.
  - Deterministic chaos (fractals).
  - Pecora & Carroll's research on information embedded below chaotic noise threshold, similar chaotic circuit can "decrypt" signal from noise.
- **Application Focus**: Cognitive robotics incorporates the behaviors of intelligent agents within the shared world model.
- Multi-agent systems create challenges for desired behaviors within a planned environment due in part to the problem of translating and using symbolic reasoning for world abstractions.

Why should we use it & how?

- Why?
  - Current systems engineering is limited in its approach to SoS in any consistent way to predict novel / **emergent** behaviors that would give the U.S. an edge on our adversaries.
  - Large-scale multi-agent SoS typically show emergent behaviors.
  - Collective actions of many entities in a system produces emergence.
  - Complexity can provide a solution to translating the world into actions, by bounding the behaviors of distributed agents to produce new (emergent) and desired collective behaviors.
- How?
  - System elements need to be more adaptable, loosely coupled, and create a dynamically interoperable environment.
  - Complexity science is better modeled by using a localized, connectionist ontology of heterogeneous agents than by using equilibrium models from thermodynamics.
- Novel coherent properties can result from these self-organizing systems

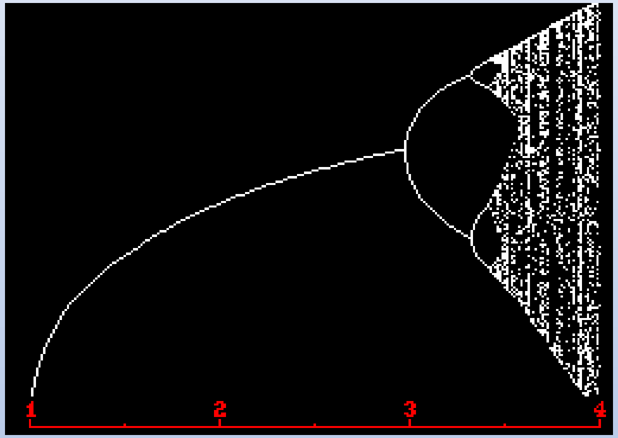
Emergent Behavior: what is it?

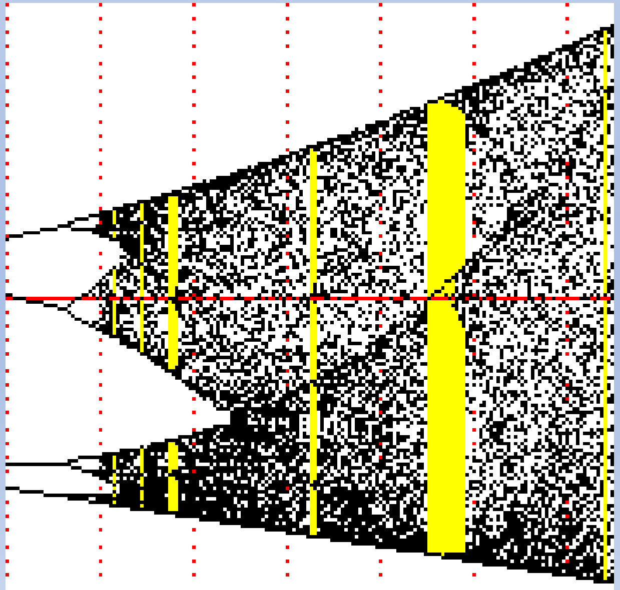
- Emergence can produce 'creative' system behaviors.
- Artificial Life - uses emergence generating algorithms:
  - genetic algorithms, neural nets, cellular automata.
    - E.g. "The Sims" uses genetic algorithms for automata.
- Emergent behaviors result ***not*** from stochastic (e.g. thermodynamics) models, but instead from multi-agent interactions (e.g. RoboCup).
- Emergent SoS ***cannot*** be designed by functional decomposition.
- Nonlinear systems: Can they have predictable behavior?
  - Predictability 'collapses' as sequence progresses (complexity increases).
  - Chaos can result from even small changes.
  - Known initial and intermediate conditions can have unpredictable results = Emergent behavior.

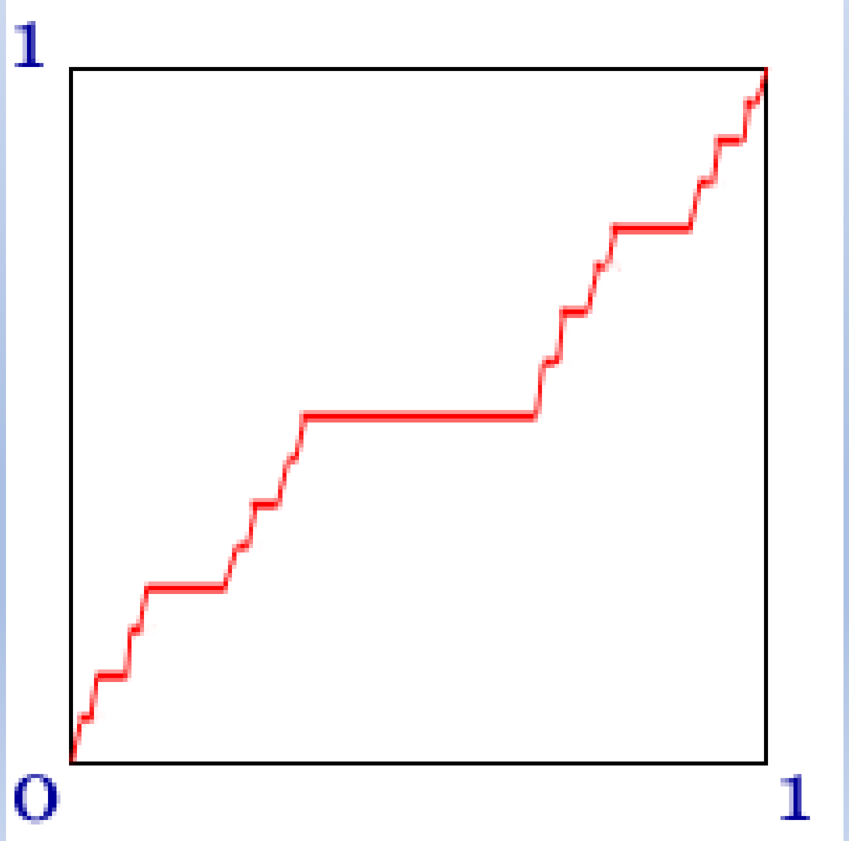
What is a Complex System ?

- Consists of many components associated by structure or just abstract relationship.
- May be scalable and self-similar at more than one level.
- Not described by simple rule or from the fundamental level. Predictable parts can form unpredictable system behavior.
  - E.g.Mandelbrot (fractal’s inventor): “transmission line noise” appeared random, was predictable “Cantor Dust”.
  - Bifurcation - “Feigenbaum diagram” at phase transitions (solid/liquid/gas), etc. represents nonlinear dropoff.
  - Devil’s staircase – at phase transition = chaos.

Diagrams: Feigenbaum and Devil's Staircase







Complexity in Other Realms

- Most body functions exhibit complex behavior - fractal pattern of heartbeat, ionic channels, etc.
  - when ECG pattern becomes *less* complex, then indicates potential heart problem !!
- Chaotic (complex) chemical reactions:
  - Belousov-Zhabotinskii reaction (color change)
- Can even build an electronic circuit with complex behavior - can be driven to chaotic
- ***Can we control chaos?***

Self-Organizing Complex Systems: Chaos under control

- Artificial biological systems:
  - Neural networks, Genetic algorithms, Boolean nets (Kauffman), Cellular Automata (Wolfram).
- Real biological systems:
  - Civilizations, economies, evolution (Kauffman), biological organisms, cognitive thought process.
- Experimental mathematics:
  - ***Not*** formal methods, and no available proofs.
  - May depend upon deterministic chaos.

Control of chaos – *an example*

- ***Problem: Spatially distributed large dynamic networks:***
- Lose edge node communications.
- <u>*Congressional Research Report (2007):*</u>
  - Showed scaling limitations for large numbers of networked nodes needed for battlespace.
  - Combinatorial explosion from massive numbers of route calculations.
- To increase <u>*availability and resiliency*</u> in network-centric clouds and swarms, ad-hoc nodes must rapidly self-organize using shared topology data.
- Topology can affect network **failures** and **success** of cyber offense and defense.
- ***Perhaps we can leverage complexity science for a solution:***
  - Moffat's 2003 paper titled "Complexity Theory and Network Centric Warfare" referenced complex systems and their relationship to fractals and decentralized NCW.
  - High volume network traffic packets self-organize to fractal (Leyland et al., 1994), therefore fractal may increase availability for large networks.
  - Use a fractal that can adapt to needed topology.

Adaptive fractal experimental math discovery: an outgrowth of the linear chaos game

Like the simple point-slope equation for line:

- Deterministic chaos equation is **X(n) = M*X(n-1) + Z.**

X(n-1) = *current point,* **X(n)** = *next point.*

Z: "vertices" = a set of initial points that constrain all node points, can represent network hubs. ***Z** is **randomly** selected* out of this set.

M: scale parameter = controls where the *next point is generated* from the *current point*. $0<|M|<1$.

Both variables **M** and **Z** share interdependencies that affect the overall network topologies, including thresholds for clustering and the mappings to certain cluster elements.

Running NPPR algorithm and using the results

<u>Running it:</u>

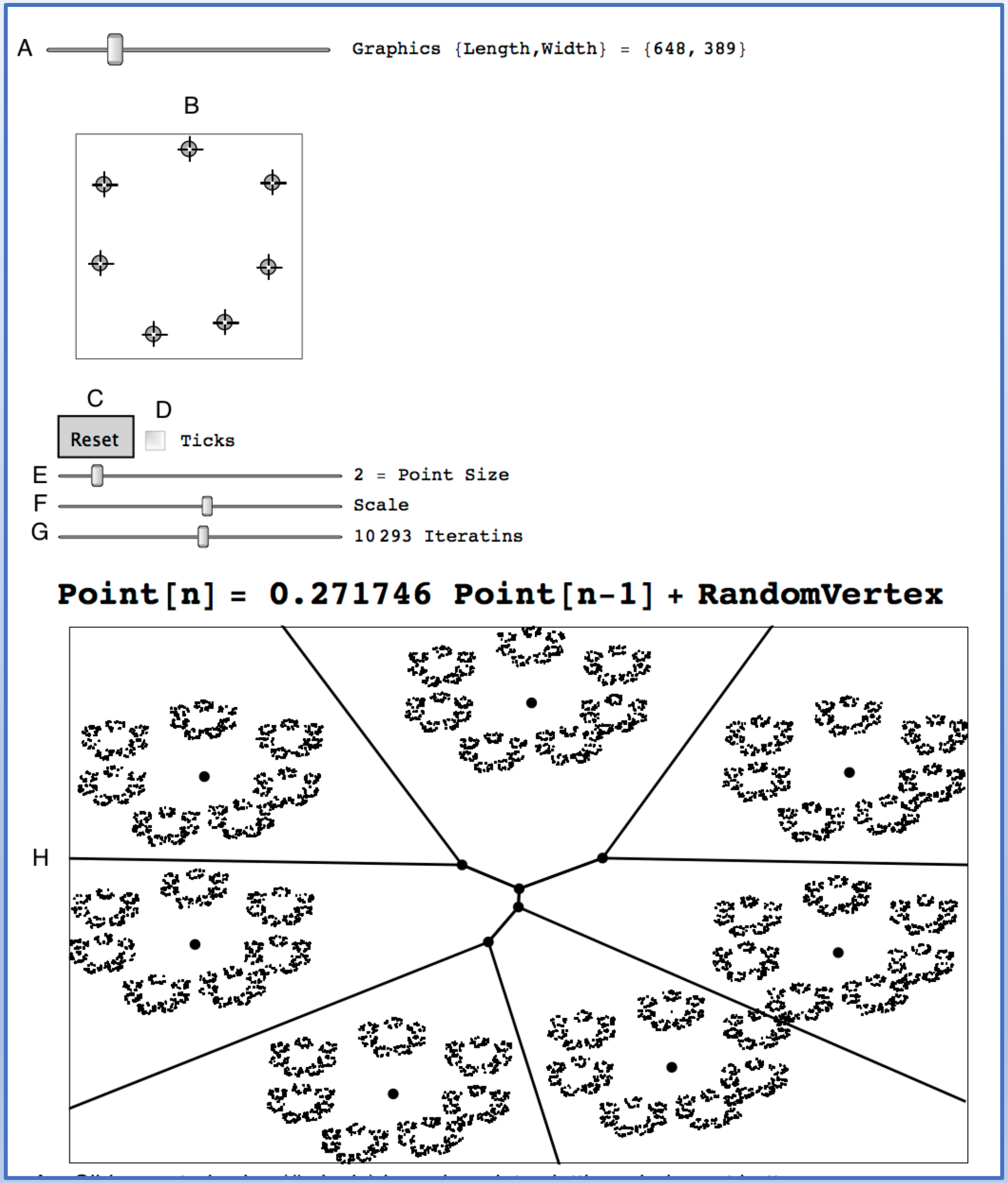
- Node and hub considerations:
  - Points plotted show distribution of network nodes; ***<u>vertices = hubs</u>***.
  - Hubs may be virtual, i.e. location for calculation purposes only, and can add, move, delete.
  - Nodes know relative layout of clusters, coalesce around hubs for communications clusters.

<u>Results:</u>

- Combinatorial explosion and cyber impact avoided by use of NPPR.
  - Usually is an issue in large ad-hoc networks (Adams & Heard, 2014).
- NPPR topology is *information-dense:* a little info can reconfigure network.
  - Hub changes broadcasted as lat-lon position.
  - Scale parameter changes from chaos to order.
- Produces repeatable macroscopic results, even with unique node positions
  - Can apply to large-scale swarm control, adaptive cyber warfare.
  - Shared *stigmergic* knowledge by all nodes – i.e. each knows position of “neighborhoods”

Screen layout of NPPR "tool":

A = Slider controls size (# pixels) in node-points plotting window, at bottom.
B = Hubs topology map, used to drag-and-drop a hub relative to others, or create hubs.
C = Resets diagram to a default 3-vertex, 0.5 scale for equilateral Sierpinski gasket.
D = Checkbox that toggles display of horizontal and vertical axes.
E = Slider for number of pixels selected to represent each node plotted.
F = Scale slider for the NPPR parameter (floating point multiplier).
G = Slider for the total number of points (nodes) to plot.
H = Lines indicate Voronoi partitions, for cluster observation guidance.
I = Nodes plotted using formula at top of window. Center points correspond to hubs.



Some of the references

- Stigmergy:
  - Lemmens and Tuyls (2010) suggested stigmergy for routing protocols issues. Masoumi and Meybodi (2011) showed relationship of shared information to stigmergy.
- Network Topology:
  - Kleinberg, et al. (2004) showed topology affects network failures as well as attack successes.
- Fractal Traffic Self-organizing:
  - Paxson and Floyd (1995).