Swarm Intelligence and IDS

Sohn Jong-Soo

Intelligent Information System lab.
Department of Computer Science
Korea University

Contents

- Introduction to swarm intelligence
  - Concepts
  - Principal
  - Ant colony optimization
  - Particle swarm optimization
- Related papers
  - Collective intelligence and priority routing in networks
  - A swarm intelligence based intrusion detection technique
  - ANTIDS : Self organized ant-based clustering model for intrusion detection system
- Conclusion

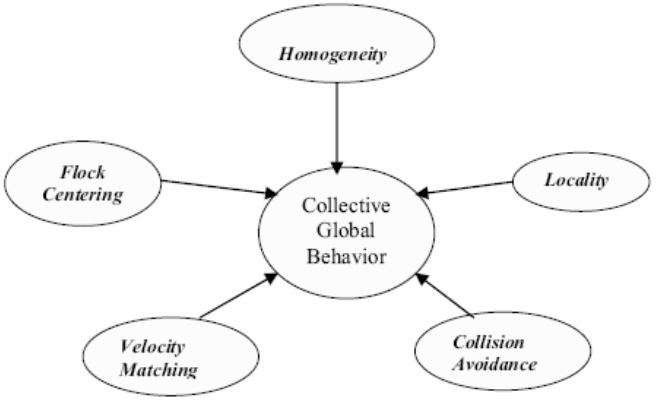
Introduction to swarm intelligence

Swarm intelligence

- Relatively new interdisciplinary field of research
- Draw inspiration from the collective intelligence emerging from the behavior of a group of social insects
  - Likes bees, ants, wasps etc.
  - Cooperatively perform many complex tasks necessary for their survival
  - Problems
    - finding and storing foods
    - selecting and picking up materials
    - Problems are solved by insect colonies without any kind of supervisor or controller

Introduction to swarm intelligence

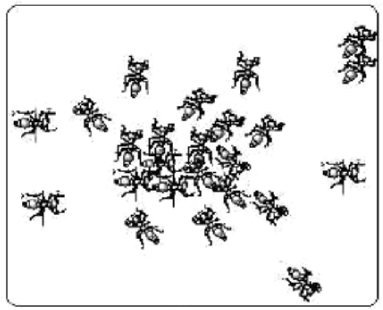
- Collective and social behavior of living creatures motivated researchers
- Beny and Wang, 1989
  - Context of cellular robotics
- Collective behavior (Couzin et al., 2002)
  - Homogeneity
    - Every bird in flock has the same behavioral model
  - Locality
    - Nearest flock-mates only influence the motion of each bird
  - Collision Avoidance
  - Velocity Matching
  - Flock Centering

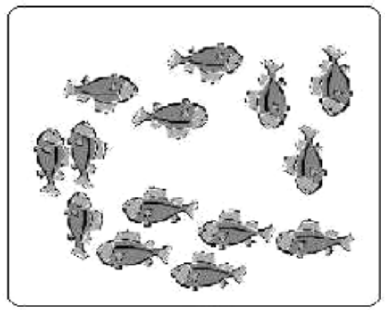


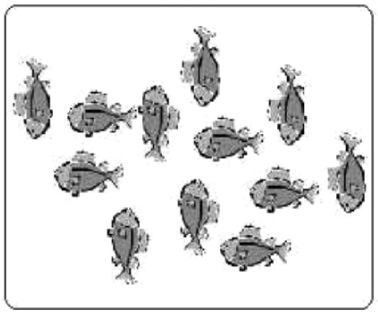
Introduction to swarm intelligence

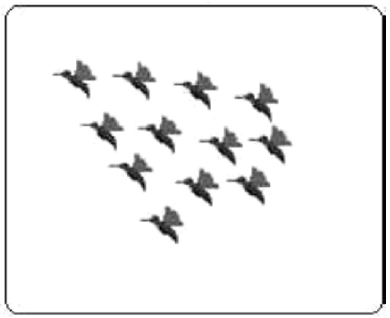
- Collective dynamical behaviors (Couzin, 2002)
  - Swarm
  - Torus
  - Dynamic parallel group
  - Highly parallel group

  - Swarm can be viewed as a group of agents cooperating to achieve some purposeful behavior and achieve some goal


(a) Swarm


(b) Torus





Basic principle of collective intelligence

Fact : X_k

- $X_k = a + n_k$
  - a : correct fact (knowledge)
  - n_k : noise

$$x_{\mathrm{CI}} = \sum_{k=1}^{K} x_k = Ka + \sum_{k=1}^{K} n_k$$

Using many facts

$$x_{\mathrm{CI}}[i] = \sum_{k=1}^{K} \begin{cases} x_k[i_k] & i_k = i \\ 0 & i_k \neq i \end{cases} = K_i a[i] + \sqrt{K_i} n$$

- $X_k[i_k] = a[i_k] + n_k$
  - i-th knowledge of user K

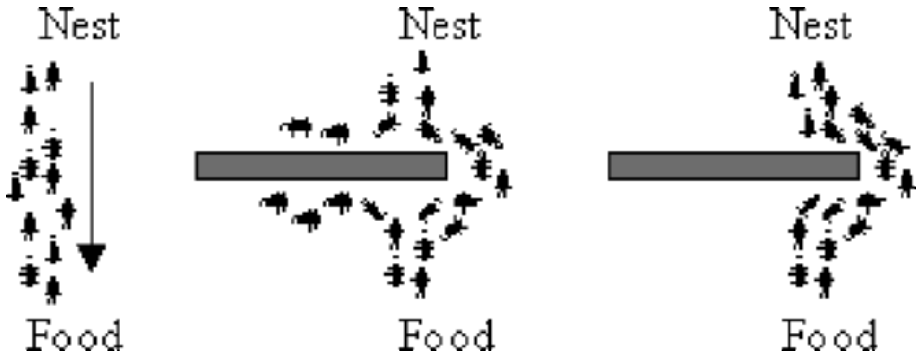
Introduction to swarm intelligence

- **Ant Colony Optimization (ACO)**
  - Dorigo et al., 1996
  - Focuses on discrete optimization problems
  - Applied successfully to a large number of NP hard discrete optimization problems
    - Traveling salesman
    - Scheduling, vehicle
    - Routing in telecommunication networks
- **Particle Swarm Optimization (PSO)**
  - Kennedy and Everhart, 1995
  - One of the very popular swarm intelligence Algo.
  - Global optimization over continuous search spaces

The ant colony systems (ACO)

Ants behavior

- Ants move in a straight line
- An obstacle is inserted between the nest and the food
- To avoid the obstacle
  - Each ant chooses to turn left or right at random
- Pheromone accumulates faster in the shorter path around the obstacle
  - Shorter path : more pheromone
  - Longer path : less pheromone



The ant colony systems (ACO)

Finding the optimal tour in the TSP

- Set of n cities
- R(Cx, Cy) be a measure of cost for traversal from city Cx to Cy
- The total cost of traversing n cities indexed by i1. ... in

$$Cost(i_1, i_2, ..., i_n) = \sum_{j=1}^{n-1} r(Ci_j, Ci_{j+1}) + r(Ci_n, Ci_1)$$

- The probability that ant k in city *i visits city j is given* by:

$$p_{ij}^k(t) = \begin{cases} \frac{[\tau_{ij}(t)]^\alpha [\eta_{ij}]^\beta}{\sum_{h \in allowed_k(t)} [\tau_{ih}(t)]^\alpha [\eta_{ih}]^\beta} & if\ h \in allowed_k(t) \\ 0 & otherwise \end{cases}$$

- Pheromone is updated on all the ages as,

$$\tau(i,j) = (1-\rho).\tau(i,j) + \sum_{k=1}^{m} \Delta\tau_k(i,j)$$

The ant colony systems (ACO)

Algorithm for ant colony system

Algorithm 1: Procedure ACO

1: Initialize pheromone trails;
2: **repeat** {at this stage each loop is called an iteration}
3: Each ant is positioned on a starting node
4: **repeat** {at this level each loop is called a step}
5: Each ant applies a *state transition rule like rule (2)* to incrementally build a solution and a *local pheromone-updating rule like rule (4);*
6: **until** all ants have built a complete solution
7: global pheromone-updating rule like rule (5) is applied.
8: **until** terminating condition is reached

The particle swarm optimization (PSO)

- **Kennedy et al., 2001**
  - Only use primitive mathematical operators
    - Do not use gradient information
- **PSO**
  - Population of conceptual "Particles" is initialized with
    - random positions X_i
    - velocities V_i
    - function f
  - N-dimensional search space
    - $X_i = (x_{i1}, x_{i2} \ldots x_{in})$, $V_i = (v_{i1}, v_{i2}, \ldots v_{in})$
  - The basic update equations for the d-th dimension of the i-th particle in PSO may be given as

$$V_{id}(t+1) = \omega.V_{id}(t) + C_1.\varphi_1.(P_{lid} - X_{id}(t)) + C_2.\varphi_2.(P_{gd} - X_{id}(t))$$
$$X_{id}(t+1) = X_{id}(t) + V_{id}(t+1)$$

Ø1 and Ø2 : random positive numbers

The particle swarm optimization (PSO)

PSO Algorithm

Algorithm 2: The PSO Algorithm

Input: Randomly initialized position and velocity of the particles: $\mathbf{X}_i(0)$ and $\mathbf{V}_i(0)$

Output: Position of the approximate global optima $\mathbf{X}^*$

```
1: while terminating condition is not reached do
2:     for i = 1 to numberofparticles do
3:         Evaluate the fitness: =f(X_i(t));
4:         Update P(t)andg(t);
5:         Adapt velocity of the particle using Equation 3;
6:         Update the position of the particle;
7:     end for
8: end while
```

Related paper

- Collective intelligence and priority routing in networks
  - Tony White, 2002
- A swarm intelligence based intrusion detection technique
  - Zhou Lianying, 2006
- ANTIDS : Self organized ant-based clustering model for intrusion detection system
  - Vitorino, 2007

Collective Intelligence and Priority Routing in Networks

- To solve complex routing problems
  - Incorporating prioritized information flow
  - By biologically-inspired agents
- The collection of agents (swarm system)
  - Deals only with local knowledge and exhibit a form of distributed control with agent communication
- Swarm routing
  - Communication network
    - Weighted graph where the vertices correspond to switching nodes and edges represent the physical links
  - Connection creation monitoring agent
    - When a connection request is made
    - CCMA are decide when a path has emerged
  - Point to point, Point to multi point, Cycle

Collective Intelligence and Priority Routing in Networks

Evaluation

- 18% more traffic
  - Sending CCMA
  - Communications Between CCMA
- Much more quickly
  - Typically 30% lower discovering time
  - Nice adaptability about new situation
  - Quickly re-routing for traffic jam

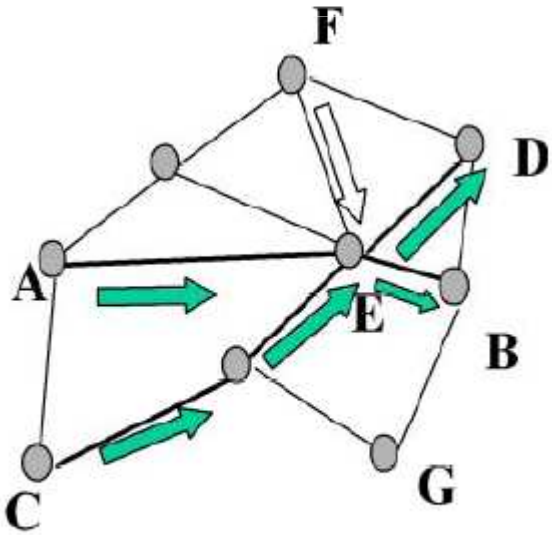


Fig. 3. Priority Routing

A swarm intelligence based intrusion detection technique

- Inspirations as following
  1. In order to decentralize burden, the entity intrusion detection system should be separated into numbers of intrusion units that are independent, flexible and self-adaptive
  2. In order to improve real-time characteristic of detection, each detection unit should be lightweight—adopting simple algorithms and processing less data
  3. The most important thing is that a detection unit can't work alone, it should not only make the best of information but also leave information to others, which means IDS should also gather "swarm intelligence".

ANTIDS : Self organized ant-based clustering model for intrusion detection system

- IDS
  - ANTIDS vs SVM vs DT vs Linear genetic programming
- Distributed and collaborative clustering
  - The swarm intelligence Algo. fully uses agents
    - Stochastically move around the classification “habitat”
      - Following pheromone concentrations
      - Ant’s food : intrusion data
- Picking and dropping data objects
  - Behavior of ants
    - Dropping and picking up objects
  - Use of combinations of different response thresholds

ANTIDS : Self organized ant-based clustering model for intrusion detection system

Pheromone weight function

$$W(\sigma) = \left(1 + \frac{\sigma}{1 + \delta\sigma}\right)^{\beta}$$

- Pheromone density : σ(r)
- 1/δ : sensory capacity

Transition probabilities

$$P_{ik} = \frac{W(\sigma_i)w(\Delta_i)}{\sum_{j \in k} W(\sigma_j)w(\Delta_j)}$$

- Δθ : the change in direction at each time step
- w(Δθ) : weighting factor

ANTIDS : Self organized ant-based clustering model for intrusion detection system

- Picking and dropping data objects
  - Behavoir of ants associated to different tasks
    - As dropping and picking up objects
    - Use of combinations of different response thresholds
  - Two major factor
    - The number of objects in his neighborhood
    - And their similarity
  - Every indivisual has a response of the task-associated stimulti s, exceeds their thresholds
    - In this papar, proposes
      - Intensity of a stimulus associated with a particular task

ANTIDS : Self organized ant-based clustering model for intrusion detection system

Picking and dropping data objects

- Number of object in one neighborhood

$$T_\theta(s) = \frac{s^n}{s^n + \theta^n}$$

- Response threshold

$$\chi = \frac{n^2}{n^2 + 5^2}$$

- Dropping object

$$\delta = \left(\frac{k_1}{k_1 + d}\right)^2$$

- Pickking up

$$\varepsilon = \left(\frac{d}{k_2 + d}\right)^2$$

- Test function

$$P_p = (1-\chi).\varepsilon \qquad P_d = \chi.\delta$$

ANTIDS : Self organized ant-based clustering model for intrusion detection system

Attribute deduction, experiment setup and results

- Attack types
  - DoS
  - R2L : Unauthorized access from a remote machine
  - U2R : Unauthorized access to local super user
  - Probing
- Conventional methods
  - DT (ID3), SVM, and LGP
- Labeled feature
  - A, B, C, D … AA, AB, … AO
    - 41 feature are labeled
  - And class label : AP
- Reduced the 12 variable data set
  - C E, F, L, W, X, Y, AB, AE, AF, AG and AI

ANTIDS : Self organized ant-based clustering model for intrusion detection system

Experiments

Attack type	Classification accuracy on test data set (%)				
	ANTIDS-*a*	ANTIDS-*b*	DT	SVM	LGP
Normal	70.52	99.64	99.64	99.64	**99.73**
Probe	71.73	98.29	99.86	98.57	**99.89**
DOS	83.39	**99.97**	96.83	99.92	99.95
U2R	0.00	64.00	**68.00**	40.00	64.00
R2L	10.47	**99.47**	84.19	33.92	**99.47**

Table 1. Performance comparison using full data set

Attack type	Classification accuracy on test data set (%)				
	ANTIDS-*a*	ANTIDS-*b*	DT	SVM	LGP
Normal	69.40	99.73	**100.00**	99.75	99.97
Probe	60.07	99.86	97.71	98.20	**99.93**
DOS	84.31	**99.97**	85.34	98.89	99.96
U2R	47.62	68.00	64.00	59.00	**68.26**
R2L	87.63	99.47	95.56	56.00	**99.98**

Table 2. Performance comparison using reduced data set

Conclusion

- Swarm intelligence
  - Weak point
    - Hard to understanding computing model
      - Biological terms + statistical knowledge + linear algebra + various clustering algorithm + etc
    - Hard to establish computing model for problem solving
    - Unexplored field
  - Strong point
    - Unexplored field
    - Distributed computing environment
      - Useful for agent
      - Routing
      - Knowledge processing, datamining
    - computing cost is very cheap!

Thank you