IDEAS: Intrusion Detection based on Emotional Ants for Sensors

Soumya Banerjee[1], Crina Grosan[2] and Ajith Abraham[3]
[1]*Dept. of Computer Applications, Institute of Management Studies, India*
[2]*Department of Computer Science, Babeş-Bolyai University, Cluj-Napoca, 3400, Romania*
[3]*School of Computer Science and Engineering, Chung-Ang University, Korea*
soumyabanerjee@imsddun.com, cgrosan@cs.ubbcluj.ro, ajith.abraham@ieee.org

Abstract

Due to the wide deployment of sensor networks recently security in sensor networks has become a hot research topic. Popular ways to secure a sensor network are by including cryptographic techniques or by safeguarding sensitive information from unauthorized access/manipulation and by implementing efficient intrusion detection mechanisms. This paper proposes a novel ant colony based intrusion detection mechanism which could also keep track of the intruder trials. The IDEAS technique could work in conjunction with the conventional machine learning based intrusion detection techniques to secure the sensor networks. The algorithm is presented and illustrated by simulating a sensor network.

1. Introduction

Sensor networks present a feasible and economic solution to some of our most challenging problems like defense applications, traffic monitoring, pollution/weather monitoring, wildlife tracking and so on. Many applications, in particular military applications are dependent on the secure and reliable operation of the sensor network. The survivability of the network is threatened by resource limitations and security attacks. With the increasing adoption of wireless sensor devices and networks, it becomes essential to design efficient IDS. Such networks are particularly vulnerable as they operate in an open medium.

The traditional prevention techniques such as user authentication, data encryption, avoiding programming errors and firewalls are used as the first line of defense for sensor networks. If a password is weak and is compromised, user authentication cannot prevent unauthorized use, firewalls are vulnerable to errors in configuration and ambiguous or undefined security policies. They are generally unable to protect against malicious mobile code and insider attacks. Programming errors cannot be avoided as the complexity of the system and application software is changing rapidly leaving behind some exploitable weaknesses. Intrusion detection is therefore required as an additional wall for protecting systems [1]. We will approach the intrusion detection as a distributed coordination problem in the face of uncertain, incomplete information with soft time and resource constraints. We will assume that agents embedded in each sensor in the network act as cooperative peers who not only monitor their hosts and the sensor network traffic for possible attack signatures but also monitor their peers in case they have been compromised by malevolent attackers. The goal of these agents is to form the 'first line of defense' against attacks. This role entails identifying early signs of attack and recognizing situations that are likely to predate an actual attack, e.g., systematic scanning activity. Virtual human technology is being applied to marketing [3] and entertainment [5] too. Emotion models are a critical component of this technology, providing virtual humans that are better facsimiles of humans as well as providing a more engaging experience. Some recent work related to intrusion detection for sensor networks could be located in [7], [10], [13]. This paper proposes an emotional ant based approach to identify possible pre-attack activities and subsequently correspond with a centralized intrusion detection mechanism. Security monitoring in the sensor network is achieved by the foraging behavior of natural ant colonies. Ants may be positioned at relevant locations in the interconnected sensor networks and for some of the related vocabularies to be described in this section please refer [1] [2]. An important advantage of the proposed approach is that the intruder traversed trails could be easily available.

2. Ant Colony Approach

Data mining approaches for intrusion detection were first implemented in mining audit data for automated models for intrusion detection. Several data mining algorithms are applied to audit data to compute models that accurately capture the actual behavior of intrusions as well as normal activities [4]. Audit data analysis and mining combine the

association rules and classification algorithm to discover attacks in audit data. Other approaches include fuzzy rule based classifiers [2], Genetic Programming techniques [1], Support Vector Machines, Decision Trees [6]. A hierarchical distributed IDS architecture is analyzed in [12]. In [13] a self-organized ant colony based clustering technique is introduced (ANTIDS) to detect intrusions. Different adaptive and self organized techniques have been already envisaged in designing the IDS. The present work contemplates some of the related works in a different form, where the ant agent would create a framework that allows user to define the characteristics of a given interaction due to intrusion. The ant system given in [8] and [9] and the proposed approach for IDS are presented as follows.

2.1 Ant Colonies System

The basic algorithm is described as follows:

Initialize pheromone values (τ)
while termination condition not met do
for $j = 1$ to k do
$S^j \leftarrow$ ***construct solution (τ)***
endfor
Apply online delayed pheromone update ***(τ,s^1,……s^k)***
end while

The *initialize pheromone values* step basically initialize all the pheromone values to the same positive constant value and adheres to the following conditions:

- Whether or not the node has already been visited by any ant, a memory (called as tabu list) is maintained. It expands within a particular traversal and is then emptied between visits.
- The inverse of the distance $\eta_{ij} = 1/d_{ij}$ is called visibility. Visibility is based on strictly local information and represents the hemistich desirability of choosing node j when ant is in node i. Visibility is used to direct the searching capabilities of ants, although a constructive method based on its sole use could produce very low quality solution.
- The amount of virtual pheromone trail τ_{ij} (t) on the edge and this trail is updated online.

The a*pply online delayed pheromone update (τ, s^1,….,s^k)* is used to store the track and edge details in the Tabu list with the following pheromone update rule:

$$\tau_j \leftarrow (1-\rho).\tau_j + \sum_{j=1}^{k} \Delta s^j \tau_j \qquad (1)$$

where

$$\Delta S^j \tau_j = \begin{cases} f(s^j) \text{ if } s^j \text{ contributes to } \tau j, \\ 0 \text{ otherwise} \end{cases} \qquad (2)$$

$\Delta S^j \tau_j$ is the combination of a solution s_j to the update for pheromone value τ_j (k is the number of solution used for updating the pheromones), ρ is the evaporation rate and f is a function which usually maps the quality of a solution to its inverse.

2.2. Emotional Ants System

The basic idea is to identify the affected path of intrusion in the sensor network by investigating the pheromone concentration. The work also emphasizes the emotional aspects of agents, where they can communicate the characteristics of particular path among them through pheromone update. Therefore, in a sensor network if the ants (we call it here them as emotional ants) are placed, they could keep track the changes in the network path, following certain knowledge base of rules depicting the probable possibilities of attack. Once the particular path among nodes is detected by the spy emotional ant, it can communicate the characteristics of path through pheromone balancing to the other ants; and thereafter the network administrator could be alerted. The entire model has been inspired by several contemporary works. In pure cognitive form, the approach finally incorporates two basic parts:

- emotion and its utility in decision making.
- transformation of the ant agent into an emotional ant.

First, we would like to discuss the emotion model of generic agents. The structure of any emotion model is primarily based on certain thematic reactions exhibited by the agents with the real world. They encompass affinity, satisfaction dejection and approach etc.

Emotional Agent Definition

Here the agents have to be conceived and created (characteristics should be defined e.g. name class, etc). An agent can be of the type of an object, where its function is related to the environment or of the type no object, where its functions are related to the actions to that agent must carry out.

We define the emotional ants as adaptive ants with variable conflict tendencies that can adjust their schema with phenomena communication.

Basis of Rules

Rules for possible attacks scenarios as suggested by the network administrator are cumulated. Again certain primitives could be proposed to formulate these rules of sensor networks.

Emotion Templates

These templates stand for individuals and to represent different emotion states, i.e. if the parameters match with existing agents. For a clear picture of the emotion exchange model some mathematical concepts are formulated in the forth coming section.

Emotional Model of Ants

The present work closely adopts the strategy followed by the ant colony system [8][9]. Here in the ant colony system only the ant that generated the best tour since the

beginning of the trail is allowed to globally update the pheromone concentration on the branches.

2.2. IDEAS Description

The ants therefore are encouraged to search for paths in the vicinity of the best traversing so far.

So, the updating rules are:

$\tau_{ij}(t) \leftarrow (1\text{-}p).\ \tau_{ij}(t) + p.\Delta\ \tau_{ij}(t)$ (3)

where (i,j) are the edges belonging to the most successful traversing across sensor nodes, since the beginning is a parameter governing phenomena decay.

When an ant visits an edge, the application of the local update rule makes the edge pheromone level diminish. This has the effect of making the visited edge less and less attractive as they are visited by ants, indirectly favoring the exploration of not yet visited edge. As a consequence, ants tend not to converge to a common path. So, we extrapolate certain local updates of the pheromone trails of ant agents across sensor networks. The basis of this is to update the network nodes in terms of affinity towards intrusion at any particular point of time.

It is performed, while performing a trip across the sensor network, ant K is in a node I and selects node $j \in J_i^k$, The pheromone concentration of (i,j) is updated by the formula

$\tau_{ij}(t) \leftarrow (1\text{-}p).\ \tau_{ij}(t) + \rho.\tau_o$ (4)

τ_o is the same as the initial value of pheromone trails and it was set as $\tau_o = (\eta.\ L_{nn})^{-1}$ (after some experiments/ trial and error approach) where n is the number of nodes and L_{nn} is the length of the trip made by the ant.

We prepared set of ant agents as templates with basic emotion exchange ability. This exchange is accomplished through pheromone level balancing. To formulate an emotion model, the following proposition is suggested:

Let $A(I,s,t)$ be the tendency of an intruder object that I assigns to the sensor object S at time t, $I1$(intruder 1)$\_C(I,s,t)$ the potential to generate the state of affinity(choice) to a particular path.

G(varg_1, varg_n) is a combination of global intensity variables which directly /indirectly affects the intrusion activity. So $I\_C\ (I,s,t)$ the intensity of attack, $T\_c(I,t)$ a threshold value and $f\_c(.)$ is a function specific thinking of intruder. The rule to generate a state of thinking or the choice of an intruder would look like:

if $I\_C(I,s,t) > I\_C(I,t)$

then set I_1(intruder 1)$\_C(I,s,t) = I\_C\ (I,s,t) - T\_c(I,t)$

else

Set $I\_C(I,s,t) = 0$

2.2 IDEAS Algorithm

The basic algorithm is outlined as follows:

/*Initialization*/

for every edge (i,j) of sensor network graph **do**

$\tau_{ij}(0) = \tau_0$

for $k = 1$ to m **do**

place ant k on a randomly chosen node.

Endfor

Let S^+ be the shortest trip found from beginning of traversing of all nodded in a sensor session and L^+ is its length.

/* Main Body Loop*/

for $t = 1$ **to** t_{max} **do**

for $k = 1$ to m **do**

Build traversing T^K by applying $(n\text{-}1)$ times the following steps:

if exists at least one node $j \in$ emotion _template _tabu _List (ETT List)

then

Choose the next node (possible to be attacked) j, $j \in J_i^k$ among the n nodes in the ETT list as follows:

$$j = \begin{cases} \arg\max_{u \in J_i^k} ([\tau_{iu}(t)][\eta_{iu}]^{\beta}) & if\ q < q0 \end{cases}$$

where $j \in J_i^k$ is chosen according to the probability of attack:

$$\rho_{ij}^k(t) = \frac{[\tau_{ij}(t)][\eta_{iu}]^{\beta}}{\sum_{i \in J_i^k} [\tau_{ij}(t)][\eta_{iu}]^{\beta}}$$

where i is the current node.

else

Chose the closest node where the possibilities of attack is high

end if

After each transition ant k applies the local update rule (Learning)

$\tau_{ij}(t) \leftarrow (1\text{-}p).\ \tau_{ij}(t) + \rho.\tau_o$

end for

for every edge (i,j) a$\in S^+$ **do**

Update pheromone trail by applying rules,

Apply Online Delayed Phenomone Update$(\tau, s^1, \ldots\ldots, s^k)$

if $I\_C(I,s,t) > I\_C(I,t)$

then set I_1(intruder 1)$\_C(I,s,t) = I\_C\ (I,s,t) - T\_C(I,t)$

else

Set $I\_C(I,s,t) = 0$

Call Intialize Pheromone Value (τ)

if $(\tau) > (\tau, s^1 \ldots\ldots s^k)$

then *Validate Path (*τij*)*

$S \leftarrow$ *G*enerate Initial Trace()

InitializeTabu lists ($TL_1 \ldots\ldots TL_n$)

$K \leftarrow 0$

While termination condition not met **do**

Allowed Pheromone Trace $(s,k) \leftarrow \{z \in N(s)$

No tabu condition is violated or at least one aspiration condition is satisfied.

$s \leftarrow$ (s,Allowed Pheromone Trace Set (S,k))

Update Tabu List and Detection Condition( )

$K \leftarrow K+1$

end while

Update the pheromone to every ant agents via Agent Template (I,S,t)

Compute the changes of pheromone in every node

Exchange the (I,S,t) with $I\_C(I,s,t)$ through

Validate Path()

Detect Intruder( )

Check for Next Session( )

End

The algorithm is based on multi agent system completely driven by parallel search. At a given iteration each ant moves from the current node of sensor network to adjacent node with the maximum number of violations. The probabilistic nature of algorithm also can be programmed according to the historical knowledge of the sensor network**.** We have introduced the concept of tabu list, where for every session the list would like to store the pheromone trace or path that is prone to attack. Here tabu $_{ij}$ (t) indicates the tabu list of ant (i j). The list consists in nodes in the sensor network that already has been visited nodes until the time t and the ant is forbidden to choose such node repeatedly. This is set to φ (not shown in the experiment), when the ant agent visit all nodes and completes its trip across the network. So ant agent in this work adopts the setting of parameter φ (i,l), where l is the degree of influence from the colony l. The absolute value of φ (i,l) indicates the degree of pheromone effect. The effect becomes stronger as the value increases and weakens if the value decreases. The actual validity of this rule will be examined by matching the historical data set comprised of connections marked as intruded or normal.

3. Experiment results

The basic idea is to identify the affected path of intrusion in a sensor network by investigating the particular path or pheromone concentration. So behavior of the path of ant agents is being formulated through a knowledge base of rules, although the rules may also depict the possibilities of attack. If a network connection, where all the micro sensors are deployed, with source IP address 1.0.0.1 – 255.0.0.0, destination IP address 2.**.?.?, source port number 75, destination port 80, duration time 30 seconds ends with the state 11 (the connection terminated by the originators) uses protocol type 2 (TCP) and the originator sends 43.2 MB/Sec data the responder sends 36.5 MB /sec data then this is a suspicious behavior and can be identified as probable intrusion.

The practical validation of the rule can be done by the ant algorithm. The ant should prepare the tree depending on the following parameters within the sensor network.

We begin by defining the following sets:

V = set of all nodes in the network

s = transmission step number

NR^S = new nodes reached in transmission step s

$NR^{0:S}$ = all nodes reached till transmission step s

$NNR^{0:S}$ = nodes not reached till transmission step s

$\Delta = V \setminus NR^{0:s}$

A node, i, is newly reached in step s if $i \in$ NRs but $i \in NR^{0:s\_1.}$

Tree building by an ant is an iterative process which starts with a transmission from the source to a destination node and continues until all the intended destination nodes are reached. At a given time instant t, the decision rule governing which edge an ant chooses to travel on at step s of the tree building process is pseudo random proportional, Starting with $s = 0$ and the initialization NR^0 = [source], this decision rule is executed until all the intended destination nodes are reached, i:e:, $NNR^{0:S} = \Phi$. Based on the obtained probable intrusion, *Intialize Pheromone Values (τ)* ants could detect the trace and produce the above choice range of intruders after traversing the nodes. We also define emotional ants as adaptive agents with variable conflict tendencies that could also adjust their agent schema and behavior during the traversing of sensor nodes. The pheromone update i.e. PH_{abs} and PH_{sum} is analyzed and shown in the Table 2.

Table 1. Status of ant agents positioned in sensor network

Action	Value Range	Pilot Range	Ant Agent Assigned	Theme of action
Source IP address	1.0.0.1 – 255.0.0.0	1. ** .** .?	ANT Agent A	A subnet with IP addresses 1.0.0.1 to 255.0.0.0.
Destination IP address	2.0.0.1 – 255.0.0.0 (Different sensor net cascaded)	2.**.?.?	ANT Agent B	A subnet with IP addresses 2.0.0.1 – 255.0.0.0
Source Port number	0- 80	75	Fused Ant Agent A+ B	Source Port number of the connection
Destination Port Number	0-80	80	Fused Ant Agent A+ B	Destination port number to indicate that this http service
Duration	0- 180	30	Ant Agent C	Duration of the connection in 30 seconds
State	1-20	11	Ant Agent C	The connection is terminated by the Network Administrator for internal use
Protocol	1-9	3	Fused Ant Agent B+ C	TCP
Number of bytes sent by admin.	1.44 MB/Sec	43.2 MB/Sec	Tabu List TL_1	The Admin. Sends 43.2 MB/Sec
Number of bytes sent by Recipient	1.44 MB/Sec	36.5 MB /sec	Tabu List TL_n	The receiver receives 36.5 MB/sec

As envisaged, because of the different pheromone balance on different track on a sensor network, experiment has produced encouraging results. The simulation clearly indicates different categories of intrusion where pheromone value seems to be positive and coordination mechanism looks effective.

Practically the calculation of synthetic pheromone for all nodes have been calculated and expressed as the following syntax (see Table 3):

```
for j=0 to j < g.size() do
  if i!=j
  then if j=0
        prob[j]=(g.get_edge(i,j).get_pheromone()+
        g.get_edge(i,j).get_weight())/sum_pheromone;
        else
         prob[j]=prob[j-1] +
         ((g.get_edge(i,j).get_pheromone() +
         g.get_edge(i,j).get_weiht())/sum_pheromone)
  else
       prob[j]=0.0;
```

The regulation of final tendency of ants to detect the intrusion is high according to the coordination mechanism adopted in the behavioral template.

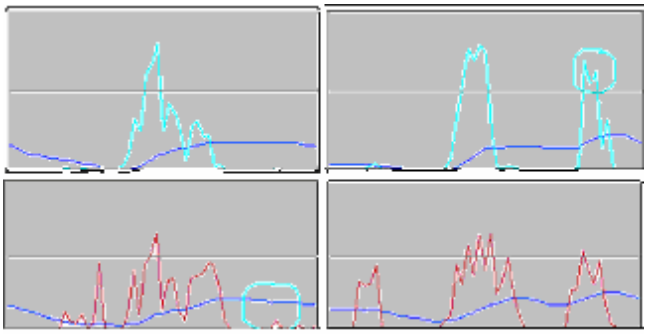

Figure 2. Simulation exhibiting transmits and receives signals

Figure 2 illustrates trials on simple sensor simulation model exhibiting simple transmit and receive signals, where in the sent mode the marked regions (circled) indicates distortion

of communication in the existing model and similarly on the received mode demonstrates certain possibilities of intrusion.

Table 2. Behavioral ant agents investigating the affinity/choice of intrusion.

Schema	Pheromone Value	Tendency		Decision on intrusion or attack
		Conflict	Action	
Agent A	Positive	Present	>0.5	Attack is likely to be **high** on this trace of pheromone
Agent B	Optimum	< 0	<0.5	Attack is likely to be **deadly** on this trace
Fusion of several ants	2.3	0.575	>4.5	Several nodes have the possibilities of severe attack.

5. Conclusions

The proposed model of emotional ants presented the collaborative distributed intelligence as a distributed coordination problem in the face of uncertainty, incomplete information with soft time and resource constraints. An important feature of the IDEAS framework is the ability to perceive behavioral patterns, deliberate and act based on self organizational principle initiated with probability values. Future research will be targeted to coordinate with the conventional IDS approaches (example, SCIDS) [2] to aid the detection process.

References

[1] Abraham A., Evolutionary Computation in Intelligent Web Management, Evolutionary Computing in Data Mining, Ashish Ghosh and Lakhmi Jain (Eds.), Studies in Fuzziness and Soft Computing, Springer Verlag Germany, Chapter 8, pp. 189-210, 2004.

[2] Abraham A., Jain R., Sanyal S. and Han S.Y, SCIDS: A Soft Computing Intrusion Detection System, 6th International Workshop on Distributed Computing (IWDC 2004), A. Sen et al. (Eds.) Springer Verlag, Germany, Lecture Notes in Computer Science, Vol. 3326, pp. 252-257, 2004.

[3] Andre, E., Rist, T., Mulken, S. V., and Klesen, M. The automated design of believable dialogues for animated presentation teams, In Cassell, J., Sullivan, J., Prevost, S., and Churchill, E., editors, Embodied Conversational Agents, pages 220-255, Cambridge, MA: MIT Press, 2000

[4] Barbara D., Couto J., Jajodia S. and Wu N., ADAM: A Testbed for Exploring the Use of Data Mining in Intrusion Detection**.** SIGMOD Record, 30(4), pp. 15-24, 2001

[5] Cavazza, M., Charles, F., and Mead, S. J. Interacting with virtual characters in interactive storytelling, In Proceedings of First International Joint Conference on Autonomous Agents and Multi-agent Systems (AAMAS-02), 318-325, 2002.

[6] Chebrolu S., Abraham A. and Thomas J., Feature Deduction and Ensemble Design of Intrusion Detection Systems, Computers and Security, Elsevier Science, 2005 (in press). http://dx.doi.org/10.1016/j.cose.2004.09.008

[7] Deng, J., Han, R. and Mishra, S. INSENS: INtrusion-tolerant routing in wireless SEnsor NetworkS Technical Report CU-CS-939-02, Department of Computer Science, University of Colorado, November 2002.

[8] Dorigo.M. and L.M. Gambardella, Ant Colony System: A cooperative Learning Approach to the Travelling Salesman Problem, IEEE Transactions. Evolutionary Computation.1 :53-66, 1997.

[9] Dorigo.M. and L.M. Gambardella, Ant colonies for the Traveling Salesman Problem", Biosystem 43 :73-81, 1997.

[10] Doumit, S. and Agrawal, D.P. "Self-organized criticality & stochastic learning based intrusion detection system for wireless sensor networks", *MILCOM 2003 - IEEE Military Communications Conference,* vol. 22, no. 1, pp. 609-614, 2003

[11] Karlof, C. and Wagner, D. Secure Routing in Sensor Networks: Attacks and Countermeasures. Ad Hoc Networks, vol 1, issues 2--3 (Special Issue on Sensor Network Applications and Protocols), pp. 293-315, Elsevier, 2003

[12] Mell, P., Marks, D.G. and McLarnon, M. A denial-of-service resistant intrusion detection architecture. Computer Networks 34(4): 641-658 2000.

[13] Ramos, V. and Abraham, A. ANTIDS: self-organized ant-based clustering model for intrusion detection system. 4th IEEE International Workshop on Soft Computing as Transdisciplinary Science and Technology, Muroran, Japan, Springer Verlag, Germany, pp. 977-986, 2005. 2005.