# On Emulating Real-World Distributed Intelligence Using Mobile Agent Based Localized Idiotypic Networks

Shashi Shekhar Jha, Kunal Shrivastava, and Shivashankar B. Nair

Department of Computer Science and Engineering
Indian Institute of Technology Guwahati, Assam, India
{j.shashi,k.kunal,sbnair}@iitg.ernet.in

**Abstract.** Researchers have used Idiotypic Networks in a myriad of applications ranging from function optimization to pattern recognition, learning and even robotics and control. Most of the reported works that have used the Idiotypic network have been simulations wherein not all entities perform in a true distributed, parallel and asynchronous manner. The concentration of an antibody within the network is always assumed to be single valued, which is easily available as a global parameter in such simulated systems. This paper describes a novel architecture and dynamics to *emulate* an Idiotypic network wherein antibodies within a real physical network interact at antigen-affected nodes, sense their respective global populations stigmergically and form *Localized Idiotypic Networks* that eventually control their respective global populations across the network. *Typhon*, a mobile agent platform, running at the various nodes forming the physical network, was used for the emulation. While the mobile agents acted as antibody carriers and ensured their mobility, the nodes forming the physical network formed the antigenic sites. Results, portrayed herein, show the selective rise in global populations of the set of antibodies that are more effective in neutralizing a range of antigens across the network.

**Keywords:** Idiotypic networks, Emulation, Distributed Intelligence, Mobile agents, Typhon.

## 1 Introduction

The Idiotypic network model [1] which is inherently autonomous and has the ability of self-tuning, is a model which postulates that the antibodies interact with one-another even in the absence of an antigen. These interactions among the antibodies modulate the responses of the immune system as a whole. The formal mathematical model proposed by Farmer *et al.* [2] describes the concentration of an antibody to be affected by the amount of stimulations and suppressions it receives from other antibodies and antigens respectively together with the rate at which new ones are added and old ones removed. The Idiotypic network is a dynamic network which is regulated by the virtue of the concentrations of

R. Prasath and T. Kathirvalavakumar (Eds.): MIKE 2013, LNAI 8284, pp. 487–498, 2013.

the various antibodies within the body. The concentration of an antibody refers metaphorically to its population in the system. In most AIS literature [3–6], these concentrations are always presumed to be single valued parameters. Further most of the implementations available for the Idiotypic network model are in the form of simulations [7] thus providing less room for its practical viability. To exploit the characteristics of the Idiotypic network model in real distributed systems, an architecture for the seamless interactions and operations of the concerned antibodies is crucial.

This paper presents a novel emulation architecture for realizing an Idiotypic network model over a real system of networked nodes which perform in a distributed and asynchronous manner. The novelty of our approach is that the intelligence is scattered in the environment (network of nodes) in the form of mobile agents [8] that act as antibodies, which selectively mitigate the problems arising at different nodes along with a competition among themselves to evolve the optimal solution. The succeeding sections provide a background on the related work, details of the proposed model for emulating an Idiotypic network over real systems followed by experimental results, discussions and conclusions.

## 2 Mobile Agents and Artificial Immune System

Mobile agents are autonomous chunks of software programs that can migrate within a network, carry payload, clone whenever required and terminate themselves if required [9]. These agents provide for a possible solution to emulate various population-based computational models in real systems. Using a mobile agent-based paradigm, Dasgupta *et al.* [10] describe a system for intrusion/anomaly detection and subsequent responses in networked computers. In his approach, the immunity-based agents roam around the nodes and routers monitoring the situation of the network. Inspired by the Clonal-Selection theory [11], the mobile immune agents used herein interact freely and dynamically with the environment and also with one another. Castro *et al.* [12], have proposed an artificial immune network model, for data clustering and filtering redundant data. They have used a Euclidean shape-space model in which the network units correspond to the antibodies. The input patterns were treated as the antigens to be recognized and clustered. This network model was successfully applied to several clustering problems, including non-linearly separable tasks. Godfrey *et al.* [13] describe an architecture of a multi-robot system that uses the AIS concepts and mobile agents to service robots. Based on pain, nodes that control the robot are triggered to indicate an antigenic attack. Mobile agents moving in a round-robin manner within the network carry the programs (antibodies) to decrease the pain levels of the robot.

## 3 Motivation for Idiotypic Network Emulation

Most of the systems that have used the Idiotypic network implement Farmer's [2] equation to deliver their models. These works are mostly simulations of the

Idiotypic network where the parameters involved are in some form accessible to all the entities in the network. The functioning of real systems, however remains grossly different and no real efforts seem to have been attempted to *emulate* Idiotypic networks on real networks. The biological Idiotypic network comprises several antibodies that stimulate or suppress one another and are generated based on their affinities with the concerned antigen. A stimulation causes the concerned antibody to increase its concentration i.e. its population increases since it has proved to be more effective in curtailing the antigenic attack. The opposite happens in case of a suppression whereby its concentration reduces. Successive suppressions may eventually lead to the removal of such antibodies. Thus, there need not actually be real physical link between all the individual members of the different antibody populations. At any moment of time during antigenic attacks, a distributed system could contain a repertoire of antibodies whose population sizes differ. If a specific antibody population seems more efficient in containing the antigenic attack its population (concentration) increases since the other less effective antibody populations stimulate it to grow. The more effective population may also suppress the growth of the other less effective ones.

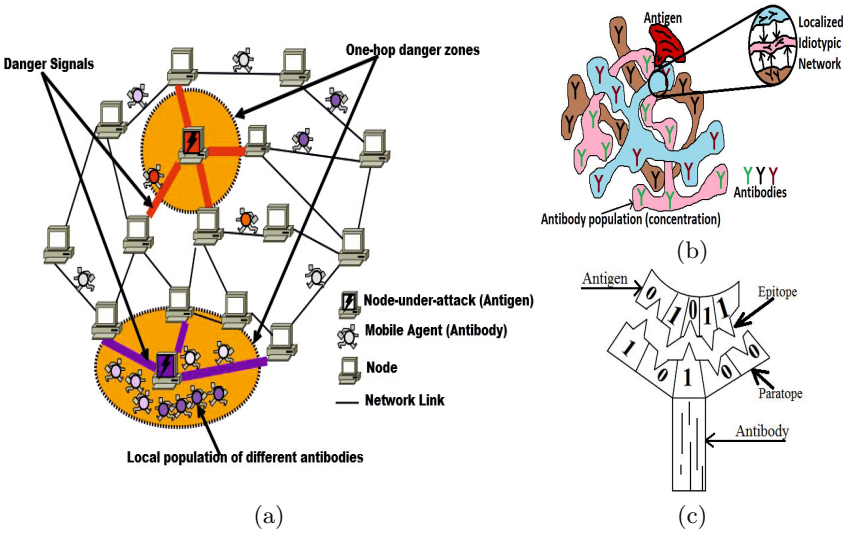



**Fig. 1.** (a) The proposed emulated Idiotypic model based architecture (b) An approximate visualization of the spatial distribution of antibody concentration and the localized Idiotypic network (c) Antigen and antibody in the proposed architecture

In the work reported herein, we have viewed the Idiotypic network as a network of populations (concentrations) of different antibodies. Each population communicates with the other using stimulations and suppressions, which cause dynamic changes in their respective populations thus contributing to a dynamic network. An approximate visualization of this network is shown in Figure 1(b).

As can be seen the populations of the different antibodies constitute a meta-level network but actual Idiotypic networks are formed at different spatial locations due to interactions of their sub-populations. What possibly is difficult to comprehend is the manner in which the idiotopes of all the antibodies of one population communicate and stimulate or suppress the others. Though in Figure 1(b) it seems that all the antibodies of one population stimulate all the others in another population via their idiotopes, this is not the way we envisage things in the work reported herein. We postulate that such stimulations happen only locally at the sites where an antigenic attack occurs. During an antigenic attack, the heterogeneous set of antibodies or sub-populations available in the locality of the attack, which are able cope up with the attack, compete with one another. The ones that are effective in containing the attack suppress those that are not, forming a *Localized Idiotypic Network* (LIN) in the locality of the attack. The sub-population of antibodies in this locality that performs better generate signals of suppression to reduce the number of the other sub-populations while the latter stimulate the former to increase the number of the more effective antibodies. The resultant effect is an increase in the number of the more effective antibodies in the locality of attack, thus containing the local antigen population quickly. Since antigens may attack in large numbers at different areas of a body, such small idiotypic interactions at these places add up to automatically increase the count of the more effective antibodies in the whole body. More effective antibodies are those solutions which have proved to be more effective against the problems or antigens. They also cause the numbers (populations) of other less effective ones to decrease, accordingly. All this happens in a stigmergic [14] and decentralized manner without all the antibodies of one kind interacting with all those of the others.

In the next section we describe the manner in which we portray a set of mobile agents acting as antibodies that move around within a real network of computers (nodes), finding and priming on antigenic attacks at the nodes and eventually increasing or decreasing their populations (concentrations) stigmergically, finally serving to *emulate* the Idiotypic network as described above.

## 4 The Emulated Idiotypic Network Model

The emulated Idiotypic network consists of a physical network comprising $n$ nodes (computers) as shown in Figure 1(a). This set of networked nodes acts as the body of the system, *parts* (nodes) of which need to be *defended* or *serviced* by providing the best set of antibodies. A set of mobile agents move through this network of nodes and comprise (carry) the antibodies. Each node hosts a mobile agent platform to facilitate all mobile agent related functions including migration, cloning, antigen-antibody affinity measurements and generation of stimulations and suppressions. Antigenic attacks are initiated by presenting an antigen at the concerned nodes. Antigenic attacks can be viewed as a service required at a node while the antibodies that nullify these attacks could be seen as the relevant service providers. A node is thus the basic entity or the part

**Table 1.** Immune network metaphors in the Emulated Idiotypic network

| **Biological Immune network** | **Entities within the Emulated Idiotypic Network** |
|---|---|
| Antigen | Service required at a node |
| Antibody | Mobile agent carrying services |
| Organs or parts of the body being defended | Nodes comprising the physical network |
| Antibody circulation | Mobile agent migration |
| Concentrations of various antibodies | Populations of the various mobile agents in the network |
| Stimulations/Suppressions | Increase/decrease in the sub-populations of concerned mobile agents within the node under attack |
| Increase/decrease in antibody count | Cloning of the stimulated mobile agents/ Termination of the suppressed ones, within the node-under-attack |
| Idiotypic Network formed by changes in stimulations and suppressions of antibodies in fluid (plasma) form | Dynamic changes in populations of each type of antibody due to stimulations and suppressions (received from others at nodes attacked by antigens), within the network |

(organ) being defended or serviced within the system. Table 1 lists some of the mapping between the entities of the emulated Idiotypic network and their biological counterparts.

### 4.1 Antigen-Antibody Interactions at the Node-under-Attack

For the sake of explanation, we consider a random binary ($m$-bit) sequence to form an antigen which is presented at a node (node-under-attack or antigenic site). The binary sequence here is the representation of a problem at the node. The corresponding best antibody could be an $m$-bit complemented sequence capable of neutralizing the antigen. An antigen and its corresponding best antibody together with the epitopes and paratopes are shown in the Figure 1(c). In the proposed model, every mobile agent that acts as an antibody carries with it one neutralizing $m$-bit sequence. An affinity function ($\psi(A_g, A_i)$) defines the degree of interaction between the epitopes of an antigen ($A_g$) and the paratopes of the antibody ($A_i$).

$$\psi(A_g, A_i) = \frac{1}{(Epitopes\ of\ Ag)\ XNOR\ (Paratopes\ of\ A_i)} \tag{1}$$

The inverse of the XNOR distance between the bits corresponding to the epitopes and paratopes of an antigen and an antibody respectively describes the affinity of interaction between them. Hence, the best antibody would be the one, which has the complemented version of the antigenic epitope as its paratope.

### 4.2 Emulating Danger Signals at the Node-under-Attack

When a node is presented with an antigen (an $m$-bit string), it immediately radiates danger signals to its immediate neighbours which in turn diffuse the same onto their neighbours at a lesser intensity than that received. As shown in

Figure 1(a), these danger signals thus penetrate the immediate neighbourhood of the node-under-attack similar to the pheromone diffusion model proposed by Godfrey *et al.* [15]. In order to manage the diffusion within this sub-network each danger signal contains five parameters which include the identifier of the node-under-attack and the previous node, the epitopes of the antigen, a Diffused Signal Strength (DSS) whose intensity decreases as it diffuses to other nodes away from the node-under-attack and the life-time of the signal which also decreases similarly. The propagation of the danger signal continues till its strength dies down to zero at nodes in the neighbourhood of the node-under-attack, thus forming a danger zone around it as shown in Figure 1(a).

### 4.3 Antibody Migration and Generation

The mobile agents that represent the antibodies flowing in the network continuously migrate based on a combination of conscientious and danger signal oriented strategies, similar to that described in [15, 16]. The conscientious strategy ensures that the agents avoid recently visited nodes. However, when an agent detects a danger signal at a node, it ascertains whether it is a *candidate antibody* that can cater to the attack. This is done by calculating the affinity $\psi$ between the neutralizing sequence carried by the mobile agent (antibody) and the epitope of the antigen within the danger signal. If this $\psi$ is greater than $\chi$, the affinity threshold (a non-zero positive constant), then the mobile agent assumes itself to be a candidate antibody and proceeds to tracking the increasing signal strength gradient towards the node-under-attack. This gradient aids the mobile agent to reach the node-under-attack via the shortest path [15]. This mechanism of attracting the relevant antibodies could lead to many candidate antibodies reaching the node-under-attack, some of which may be redundant. This redundancy is used to stigmergically sense the population of the candidate antibodies in the network. The numbers of each of the distinct candidate antibodies attracted to the node-under-attack is proportional to their respective global populations in the network.

If $\psi$ is less than $\chi$ the mobile agents ignore the danger signals and continue to migrate to other nodes using the conscientious approach. It may be noted that only one out of the many antibodies that eventually reach the node-under-attack is chosen to neutralize the antigen. In addition, if the same type of antigen affects several nodes across the network simultaneously, it could be neutralized by different antibodies. It may also happen that the danger signals have died down due to the inherent lifetimes and no candidate antibodies have reached the node-under-attack. Under such a condition, the node itself starts generating antibodies proactively. In the present case, it generates random $m$-bit patterns and ascertains its $\psi$ value. If the same is greater than $\chi$ then it uses this pattern (antibody) to neutralize the antigen. This new antibody is then encapsulated within a mobile agent and released into the network. This feature accounts for antibody generation within the network.

### 4.4 Stigmergy Based Antibody Population (Concentration) Control

In order to emulate Jerne's Idiotypic network [1], we have used a variant of Farmer's computational model [2] at each node-under-attack. The Farmer's equation in a general form can be written as:

Change in Concentration of an antibody = Antigenic Stimulation ($AgSt$) + Stimulations received from other antibodies ($St$) - Suppressions from the selected antibodies ($Su$) - Deletions due to disuse or lapse of Lifetime ($Lt$).

Whenever an antigenic attack occurs at a node (node-under-attack), the danger signal diffusions attract one or more antibodies, of the same or different types, to arrive at this node. Let $\zeta$ = {Type-1, Type-2,. . . . . .,Type-k} be the set of such distinct *candidate antibodies* that have arrived at the node-under-attack. Since multiple numbers of each of these types of antibodies could arrive at this node, each type of candidate antibody will have a population of its own within the node-under-attack. As can be seen in Figure 1(a) the node-under-attack at the bottom has three distinct types of candidate antibodies (shown in different shades) for the concerned antigen whose *local population* sizes are 2, 3 and 4 respectively. This is different from the *global population* sizes of the respective candidate antibodies which are not known to any single entity in the Idiotypic network emulation. Using the size of these local populations, the node-under-attack chooses that type of candidate antibody which has the highest local population as the best one for the neutralization of the antigen. We assume herein that in a distributed system, since more number of antibodies of this type have arrived at this node, the global population of this selected candidate antibody is high. Hence, it can be inferred that this type of antibody was possibly more effective in neutralizing attacks by this type of antigen at other nodes across the network. The node-under-attack thus senses the population size and decides the best candidate antibody by an indirect stigmergic manner. After the antigenic neutralization, the stimulations and suppressions received are used to increase or decrease the local population sizes of all the candidate antibodies at the node-under-attack based on an *activation factor* $\tau$ carried by each antibody within the network, details of which have been discussed later. These stimulations and suppressions create the *Localized Idiotypic Network* (LIN) among the local populations of the candidate antibodies at the node-under-attack some of which are shown and explained later in Figure 4. The LINs in turn alter the local population sizes increasing those that are stimulated and decreasing ones that are suppressed. These changes in the local populations (concentrations) at the node-under-attack contribute to the global ones and ensure that the more effective antibodies dominate the entire set of antibodies that flow in the network. It may be noted that in the emulated Idiotypic network, those mobile agents that carry such more effective antibodies, grow in number.

The equations that govern the dynamics of the formation of the LINs and the consequent changes in the local populations of candidate antibodies within the node-under-attack are given below. For all antibodies belonging to the local population, $a_i \in A_i$, the value of $\tau$ is given by -

$$\tau_{new}^{a_i} = \begin{cases} \tau_{old}^{a_i} + AgSt + St, \text{For selected candidate antibody population (Stimulation)} \\ \tau_{old}^{a_i} - Su, \text{For other candidate antibody populations (Suppression)} \end{cases} \tag{2}$$

where,

$$AgSt = \eta\psi(a_g, a_i) \tag{3}$$

$$St = \lambda_1 \frac{\sum_{x \in A_{Selected}} \tau^{a_x}}{\sum_{y \in A_{NotSelected}} \tau^{a_y}} \tag{4}$$

$$Su = \lambda_2\{\phi(A_{Selected}) - \phi(A_i)\} \tag{5}$$

$\tau \in [\tau_{min}, \tau_{max}]$
$\eta$ = Antigen stimulation factor (non-zero positive value)
$a_i$ = The $i^{th}$ candidate antibody
$a_g$ = Antigen at the node-under-attack
$A_i$ = The antibodies forming the local population of the $i^{th}$ candidate antibody that have arrived at the node-under-attack, $i \in \zeta$
$A_{Selected}$ = The local population of the selected type of candidate antibody used to neutralize the antigen
$A_{NotSelected}$ = The local population of those non-selected candidate antibodies
$\phi(A_i)$ = The population of set of antibodies $A_i$
$\lambda_1$ and $\lambda_2$ constitute the stimulation and suppression factors respectively which are positive non-zero values.

The ageing due to the Lifetime of the antibodies as mentioned in the Farmer's equation is handled separately. The change in population of the antibodies thus takes place by cloning or termination of antibodies (mobile agents) based on the following condition. For each candidate antibody $a_i$:

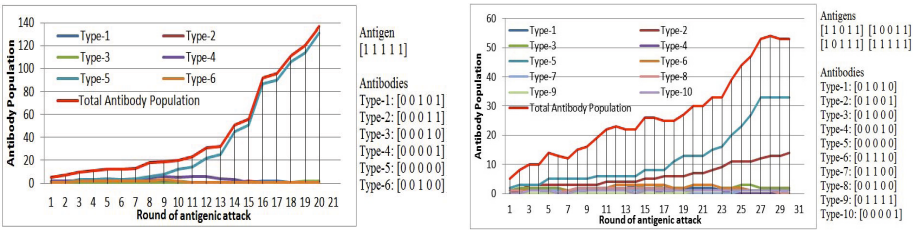
***If*** $\{\tau^{a_i} \geq \tau_{max}\}$ ***then*** *clone* $a_i$, $\tau^{a_i} = 0$, $\tau_{clone}^{a_i} = 0$
***Else If*** $\{\tau^{a_i} \leq \tau_{min}\}$ ***then*** *terminate* $a_i$

Since ageing is an integral part of an Idiotypic network, we have implemented this by conferring a fixed hop-count ($H$) to every mobile agent (antibody) in the network, which is reduced by unity at every hop. Once this hop-count becomes zero, the agents are terminated and hence removed from the system. In future, we intend to use concepts similar to that proposed in [17] to stigmergically control the agent population.

## 5 Experimentation and Results

The proposed model was emulated using *Typhon*, a mobile agent framework [18] on a 50-node network. Since we can instantiate multiple *Typhon* nodes on a single PC, the entire network was emulated using six PCs connected to each other via TCP/IP connections.

Initially since there were no antibodies in the network, the system used the method described in Section 4.3 to generate antibodies at various nodes-under-attack. At each of these nodes the concerned antibody was inserted as a payload




(a) (b)

**Fig. 2.** Antibody population in the system (a) when the same antigen was presented at five different nodes (b) when four different types of antigens were presented at five different nodes

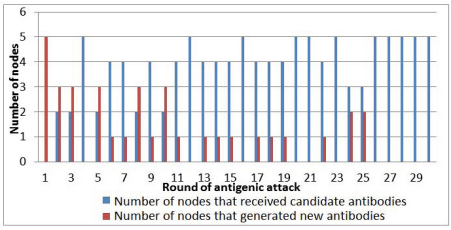



**Fig. 3.** Immunity of the system when four different types of antigens were presented at five different nodes

on to a mobile agent and empowered with $H = 100$, hop-lifetime which is an empirical estimate. Hence, each mobile agent carried a 5-bit string (a single antibody) as its payload. A 5-bit string was presented at a node to generate a node-under-attack. It must be noted that the antigens are the representations of problems occurring at a node and the antibodies are the corresponding solutions.

Each experiment performed consisted of multiple rounds of antigenic attacks. In each round, the system was made to be attacked by the same or different antigens at various nodes. The antibodies generated in each round were retained for use in the next. Experiments were performed by presenting antigens at various nodes, either simultaneously or consecutively. Results which highlight the effectiveness of the proposed architecture in a true distributed setting are presented.

Figures 2(a) and (b) show the variations of population (concentration) of each type of antibody along with the overall total population of antibodies in the system over several rounds. The antibodies generated and the antigen(s) presented are also shown within these graphs. When only one type of antigen was presented to five different nodes simultaneously for 20 rounds (20 attacks per node), six distinct antibodies (Type-1, Type-2, . . . . . .,Type-6) were generated across the network. It can be clearly seen that the population of the Type-5 antibody dominated the network while those of the others decreased drastically due to repeated suppressions at the various node-under-attack. Figure 2(b) shows a similar graph but the nature of antigen attack is different. Here, four different antigens were randomly presented at five different nodes for 30 rounds (30 antigenic attacks

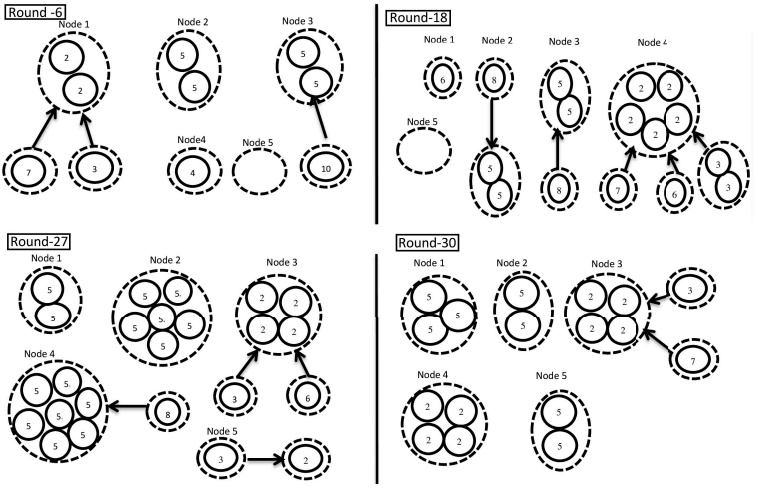



**Fig. 4.** Snapshots of the LINs formed during the rounds shown in Figure 2(b)

per node). It can be seen here that the Type-5 and Type-2 dominate the populations of antibodies. This possibly shows that these two types were capable of neutralizing all the four different antigens. This may also be verified from the bit sequences of the antigens and antibodies shown in the Figures 2(a) and (b). The ups and downs in the total antibody population in both the graphs shown in Figures 2(a) and (b) clearly indicate the regeneration and death of antibodies respectively.

Figure 3 depicts the manner in which the immunity of the network increases when four different antigens were made to attack five different nodes for 30 rounds as mentioned, in Figure 2(b). In the first round, since no antibodies populated the network, all 5 nodes-under-attack needed to generate antibodies locally as mentioned in Section 4.3. As the rounds increased, more antigenic attacks caused the generation of more effective antibodies that catered to some of the other nodes-under-attack. Eventually, beyond the $25^{th}$ round all nodes seemed to be catered to by the circulating antibodies and no new ones needed to be generated. For subsequent rounds possibly the populations of only two types of antibodies viz. Type-2 and Type-5 (see Figure 2(b) ) were sufficient to neutralize attacks by the four distinct antigens. Figure 4 shows a few snapshots of the LINs formed during some of the rounds when four different antigens were presented at five different nodes in the network, as discussed earlier. Each circle with a solid boundary corresponds to a single antibody. The dotted boundary around the antibodies represent the local population of that type of antibody at the node-under-attack during the specified round. The number or the identifier within the antibody (solid circles) indicates the type number of the antibody. The empty dotted circles indicate that no antibody reached the node-under-attack. The arrow-heads indicate the direction of stimulations while their tails form the suppressions. It can be clearly seen that as the rounds progress the populations of antibodies of Type-2 and Type-5 grow and dominate the global

population in the entire network. At the $30^{th}$ round these two antibodies are the ones that have the highest sub populations at all the nodes-under-attack (viz. nodes 1 through 5) and are thus responsible for neutralizing the antigens at all the nodes.

## 6 Conclusions

In this paper, we discuss the manner in which the emulation of a real open-world model of an Idiotypic network on a physical network of computers, can be conceived. Results have shown how stigmergy based local interactions (stimulations and suppressions) at antigen-affected nodes can help generate Localized Idiotypic Networks of sub-populations of candidate antibodies, which in turn govern and control their respective global populations across the network thus validating the assumption made in Section 4.4. The emulation results also show how the populations of the more effective antibodies grow while the others die out and are thus removed from the network. The Idiotypic network can also generate new antibodies if required. The network also seems to be able to converge onto the more generic antibodies that are able to neutralize a set of varied antigens. Hence, given various solutions to solve similar problems arising in an distributed environment, the proposed architecture can evolve the optimal solution and purge the others.

We envisage that this emulation model, with customized modifications and improvements, will aid the realization of a plethora of real-world applications and aid AIS researchers to gain more insights into the actual distributed and parallel working of the Idiotypic network. We are currently working towards incorporating new features such as Clonal selection to evolve memory cells in lieu of the random method of generating antibodies, making some nodes act as lymph nodes and also vaccinating the network with antibodies which are known *a priori*, to eventually realize a networked *Artificial Being*.

**Acknowledgements.** The authors wish to thank the Department of Science and Technology, Government of India, for the funding provided under the FIST scheme to set up the Robotics Lab. (www.iitg.ernet.in/cse/robotics) at the Dept. of Computer Science and Engg., Indian Institute of Technology Guwahati, where the entire reported work was carried out and TCS for the financial support provided to one of the co-authors during the course of this research.

## References

1. Jerne, N.K.: Towards the network theory of the immune system. Ann. Immunol.(Inst. Pasteur) 125, 373–389 (1974)
2. Farmer, J.D., Packard, N.H., Perelson, A.S.: The immune system, adaptation, and machine learning. Physica D: Nonlinear Phenomena 22(1), 187–204 (1986)
3. Watanabe, Y., Ishiguro, A., Uchikawa, Y.: Decentralized Behavior Arbitration Mechanism for Autonomous Mobile Robot Using Immune Network. In: Dasgupta, D. (ed.) Artificial Immune Systems and Their Applications, pp. 187–209. Springer, Heidelberg (1999)

4. Shimooka, T., Shimizu, K.: Idiotypic Network Model for Feature Extraction in Pattern Recognition – Effect of Diffusion of Antibody. In: Palade, V., Howlett, R.J., Jain, L. (eds.) KES 2003. LNCS, vol. 2774, pp. 511–518. Springer, Heidelberg (2003)
5. Hart, E., Ross, P.: Studies on the Implications of Shape-Space Models for Idiotypic Networks. In: Nicosia, G., Cutello, V., Bentley, P.J., Timmis, J. (eds.) ICARIS 2004. LNCS, vol. 3239, pp. 413–426. Springer, Heidelberg (2004)
6. Whitbrook, A.M., Aickelin, U., Garibaldi, J.M.: Two-timescale learning using idiotypic behaviour mediation for a navigating mobile robot. Applied Soft Computing 10(3), 876–887 (2010)
7. Greensmith, J., Whitbrook, A., Aickelin, U.: Artificial immune systems. In: Handbook of Metaheuristics, pp. 421–448. Springer (2010)
8. White, J.E.: Mobile agents. In: Software agents, pp. 437–472. MIT press (1997)
9. Outtagarts, A.: Mobile Agent-based Applications: a Survey. International Journal of Computer Science and Network Security 9, 331–339 (2009)
10. Dasgupta, D.: Immunity-based intrusion detection system: a general framework. In: Proc. of the 22nd NISSC, vol. 1, pp. 147–160 (1999)
11. De Castro, L.N., Von Zuben, F.J.: Learning and optimization using the clonal selection principle. IEEE Transactions on Evolutionary Computation 6(3), 239–251 (2002)
12. De Castro, L.N., Timmis, J.: Artificial immune systems: a novel approach to pattern recognition (2002)
13. Godfrey, W.W., Nair, S.B.: An Immune System Based Multi-robot Mobile Agent Network. In: Bentley, P.J., Lee, D., Jung, S. (eds.) ICARIS 2008. LNCS, vol. 5132, pp. 424–433. Springer, Heidelberg (2008)
14. Dorigo, M., Bonabeau, E., Theraulaz, G.: Ant algorithms and stigmergy. Future Generation Computer Systems 16(8), 851–871 (2000)
15. Godfrey, W.W., Nair, S.B.: A Pheromone Based Mobile Agent Migration Strategy for Servicing Networked Robots. In: Suzuki, J., Nakano, T. (eds.) BIONETICS 2010. LNICST, vol. 87, pp. 533–541. Springer, Heidelberg (2012)
16. Godfrey, W.W., Nair, S.B.: A bio–inspired technique for servicing networked robots. International Journal of Rapid Manufacturing 2(4), 258–279 (2011)
17. Godfrey, W.W., Nair, S.B.: A Mobile Agent Cloning Controller for Servicing Networked Robots. In: International Conference on Future Information Technology IPCSIT, vol. 13, pp. 81–85. IACSIT Press (2011)
18. Matani, J., Nair, S.B.: *Typhon* - A Mobile Agents Framework for Real World Emulation in Prolog. In: Sombattheera, C., Agarwal, A., Udgata, S.K., Lavangnananda, K. (eds.) MIWAI 2011. LNCS, vol. 7080, pp. 261–273. Springer, Heidelberg (2011)