Abstract—Protecting computer networks from accidental and malicious harm is a critical issue. Researchers have sought a variety of solutions ranging from the purely statistical approach to approaches inspired from a variety of fields such as economics and biology. In this paper, we focus on the issue of intruder detection and propose two complementary approaches, one economics-based, the other biology-inspired. We discuss the effectiveness of these two approaches put together as compared to each one alone based on Matlab simulations.

I. INTRODUCTION

A. Motivation

The deployment of sensor networks in remote and frequently hostile environments combined with the inherent limitations of the sensors, makes them particularly vulnerable to attacks from adversaries. By nature of the data manipulated in monitoring networks, individual nodes’ data rarely carries any critical or private information, thus, the most damaging type of attacks is Denial of Service (DoS) attacks where parts of the network are crashed or overloaded with a flood of requests forcing them to deplete their power and making them non available for their primary function of monitoring their environment. In this paper we introduce a set of metrics by which intruders are identified and discuss actions taken to make the network immune to their actions. Our approach is characterized by the fact that intruders’ identification is based, not on some extrinsic profiling, but on the intrinsic behavior that is either harmful or not beneficial to the network.

The first generation of sensor networks has been developed with the main concern of having the different nodes in the network communicate with each other efficiently. A prevalent assumption in the protocols and algorithms developed is that of good faith and trust. As wireless sensor networks are becoming widely used in mission critical systems and environments, their security is becoming an ever-growing concern [1]. Their deployment in remote and frequently hostile environments combined with the device constraints, makes them particularly vulnerable to DoS attacks from adversaries. They are especially vulnerable to these kinds of attacks because of their lack of a fixed infrastructure and their limited power, memory, and computation resources.

B. Related Work

Typically, the security protection of networks consists of a collection of complementary tools and methods. The first line of protection consists of fire-walls, which are “fences” built around the system directing all communication towards a small number of guarded gates. If an intruder succeeds in crossing the fence, a fire-wall is of no further help, thus the need for intruder detection. Many of the traditional approaches to intrusion detection consist of a two-step approach: In the first step, a profile is created to characterize intruder behavior. In the second phase, while the network is operating, the observed behavior is compared with what has been catalogued and flagged if it matches catalogued abnormal behavior [2], [3], [4] or if it deviates from catalogued normal behavior [5], [6]. Overall, the literature in sensor network intrusion detection can be divided according to what they protect. The resources typically targeted and protected include: data packets that can be maliciously dropped or changed [4], communication paths that can be intercepted and broken [3], communication signals that can be interfered with [7], normal behavior that can be diverted by intrusion nodes [5], and data routing paths [8]. These approaches tend to be demanding in terms of storage and computation, the patterns that they catalog tend to be generic and not very effective in the very specialized, application specific context of sensor networks [2]. The issue of performance has been partially addressed by distributing the work among nodes and optimizing the code required to identify intruders [9], [10], [11], [12]. Approaches based on the cataloguing of patterns associated with intruders suffer from a fundamental flaw: They only know about patterns of past intruders. To use the words of Sun Tzu in the Oldest military treatise in the world, “If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.” When dealing with malicious intrusions, the network is constantly at risk with new enemies (that may use a different pattern from the ones in the catalog). As a result many of the existing approaches have a high level of false positives and false negatives. On the other hand, using a wider net and looking for all unusual and rare behavior may catch more intruders but would also result in a large number of false alarms.

In this research, we experiment with two complementary paradigms related to the intruder detection problem, an economics-based paradigm, and a nature-inspired paradigm. In the economics-based paradigm, we do not rely on any
extrinsic features of the intruders or their observed behavior; instead we focus on the net effect of that behavior and on its compatibility with the mission of the overall network. A node whose objectives are in conflict with those of the network is considered harmful to the network, irrespective of its intentions. This approach and its experimental results are discussed in section II. The second paradigm is nature-inspired. Nature gives us a large variety of robust multi-cellular systems with very effective immune systems. These immune system are increasingly used as a source of inspiration for computer-based networks security. In section III, we discuss the main characteristics of natural immune systems and how these characteristics are materialized for a sensor network. We combine the two approaches in section IV and conclude in section V.

II. ECONOMICS-BASED MODEL

In [13], Mark Burgess argues that with all their appeal, the nature-inspired concepts of self-immune, self-healing, and “self-anything” systems are not necessarily the best suited model for software-based systems. One of Burgess’ argument is that a strong premise to the natural processes is that of redundancy of life. Biology plays the numbers game by generating a very large number of variations and affording to eliminate some for the benefit of other more robust versions. By contrast, information systems (nodes in a network) are not an expandable good whose instances can be sacrificed for the good of the community (species). Another argument made by Burgess is that biological systems have no purpose or mission (other than surviving as long as possible). By contrast, security threats to security in computer-based systems is a threat to the integrity of the function of the system. For these and other reasons, Burgess argues that an economics-based model may be a more effective model.

The approach proposed here can be thought of as an economics-based approach. It is based on the idea that nodes are characterized as harmful or harmless not based on whether they are internal to the network or external (intruder), nor based on patterns of behavior, but instead, based on whether they are economically beneficial to the functioning of the network or not. For this, we first define two concepts: the function of the network, and the benefits that a node brings to the network. We then use these concepts to characterize intruders.

A. Economics Model

1) Network’s Objective: Typically, sensor networks are used for long-lived monitoring applications. In these applications, the network repeatedly executes the same query with a predefined frequency. An example of such a query would be

\[
\text{Query } Q: \text{ Select Max(pollution Level), position From all nodes every 20mn forever}
\]

In this query, the nodes are supposedly sensing the concentration of some component considered to be a pollutant. The goal is to identify the point of highest concentration as well as the level of concentration. It is very often the case that a network’s mission is restricted to a single query. Without loss of generality, we will assume this to be the case. The query, or the accurate computation of the query constitutes the function of the network.

2) Node Contribution: Staying with the example of pollution detection, intuitively it is clear that not all nodes have the same impact on the accuracy of the query. In particular, nodes that have the lowest level of concentration will have little impact on the result of the query. We use the notion of transinformation introduced by Claude Shannon in his Information Theory [14]. The transinformation value of two random variables \( X \) and \( Y \) is the amount of information that can be gained about \( Y \) from the examination of \( X \) (or vice versa, the concept is symmetric). We use the transinformation value formula to define Usefulness, a time-variable correlation between a query \( Q \) and the node \( N_i \) based on recent history of data collected from \( N_i \) up to the current time \( t \):

\[
U(Q, N_i, t) = \sum_{[t-\delta t, t]} p(q, m_i) \log \frac{p(q, m_i)}{p(q)p(m_i)}.
\]

Because the relevance of a node to the query will vary over time, we focus on recent history over a selected time interval of length \( \delta t \). Because natural phenomena are continuous over time and space, we assume that the relevance of a node at present time is highly correlated with its relevance over the recent history.

We take the position that nodes should be characterized by their effect on the network rather than by some extrinsic classification of their intentions. Therefore, our characterization should identify as innocent any node that is positively contributing to the operation of the network, even if, in fact, it is an intruder. And, our characterization should flag as intruder any node whose operation is a burden on the network, even if the node is in fact legitimate. For this, we define the concept of convergence between a node’s operation and the network’s main function, viz accurate computation of the query. We quantify the level of convergence of a node \( N_i \) with the goals of the network by the extent to which the activity (as measured by power consumption) within that node was used to contribute to the accuracy of the monitoring (i.e. the computation of query \( Q \)). The contribution of a node \( N_i \) to the monitoring task is measured by the power used in communication modulated by the usefulness of the information communicated. We define the following parameters: The Activity of a node \( N_i \) at time interval starting from \( t \) and having duration \( \delta \) is denoted \( A(N_i, t, \delta) \) and defined as:

\[
A(N_i, t, \delta) = R(N_i, t + \delta) - R(N_i, t)
\]

where \( R(N_i, t) \) is the residual power of node \( N_i \) at time \( t \). In other words, the activity of a node is measured by the
power it consumed during time interval of interest. In order to distinguish between nodes whose activity is supporting the main function of the network and nodes whose activity is not, we define the concept of contribution. The contribution of a node $N_i$ to query $Q$ at time interval starting from $t$ and having duration $\delta$ is denoted $T(N_i, Q, t, \delta)$ and defined as the weighed sum of $C(N_i, Q, t_k)$ for those times when the node is queried: where $C(N_i, Q, t_k)$ is the amount of power used by node $N_i$ in participation to computing query $Q$ at time $t_k$. In summary, $T(N_i, Q, t, \delta)$ is defined by:

$$T(N_i, Q, t, \delta) = \sum_{t_k=t}^{t+k\cdot\delta} C(N_i, Q, t_k).$$  \hspace{1cm} (3)

The highest contribution is obtained when a node is often interrogated and it is useful when interrogated. On the other hand, if a node is never interrogated, or if it is often interrogated while it has a low usability, it has a low contribution. Nodes that happen to have a low usability are bound to have a low contribution. Also, nodes that are never interrogated have a null contribution. Nodes that have a low productivity but use very little power are harmless nodes. Nodes that present a risk to the network are those that have a low contribution but use a high amount of power.

The last concept introduced, convergence assesses this risk by comparing the power used to the contribution. In other words, the convergence of a node $N_i$ relative to a query $Q$ during time interval that starts at $t$ and lasts for $\delta$ units is denoted by $G(N_i, Q, t, \delta)$ and defined as:

$$G(N_i, Q, t, \delta) = \frac{T(N_i, Q, t, \delta)}{A(N_i, t, \delta)}$$  \hspace{1cm} (4)

The convergence measures the ratio between the contribution the node made to the query and the total power consumed. The higher the usefulness of a node, the higher will be its convergence, unless it consumed power in other tasks than computing the query. On the other hand, the lower the power used by a node the higher is its convergence. This ensures that nodes that are useless but harmless are not suspect. The essence of this approach is that any node whose activity by far exceeds its contribution to the main function of the network can be counterproductive and safely considered as intrusive, whether it is or not. This does not distinguish between the cases where the source of this activity is an external node that infiltrated the network or an internal node that was high-jacked by an intruder, and does not distinguish between accidental and malicious intrusions. All have the same potential effects, they need to be identified and managed so as to limit, control and cease the damage that they are causing the network. In other words, with this approach we no longer have a problem of false negatives or positives. Furthermore, our approach is unique in the sense that it takes its “order” from the activity on the ground rather than from some arbitrary attributes that have no necessary bearing on the function of the network.

B. Simulation and Results

We tested the proposed approach using Matlab simulation. The sensor network is simulated using a grid (we used a 10 by 10 in the small data set, and a 100 by 100 in the rest of the experiments) representing the region being monitored by the network. The phenomenon being monitored by the network is simulated by a single attribute whose values are a function of the coordinate of the point $(x, y)$ and represented by a function $f(x, y)$ of the form

$$f(x, y) = h \cdot e^{-(x-a)^2-(y-b)^2}/w$$  \hspace{1cm} (5)

This function is used to capture the case where the phenomenon is centered around a single point, $(a, b)$ in this case, with a peak in value at that point and exponential decline as we get farther from the center $(a, b)$. There are three parameters in this equation, namely:

- $h$, the range of the phenomenon, or the height of the peaks in the data. In the experiments, we set $h$ to 100 and do not vary it.
- $w$, the radius of the phenomenon. The smaller is $w$, the narrower is the peak, and the steeper is the decline. With a large $w$, the data changes more slowly.
- $(a, b)$, the point at which the phenomenon peaks. In contrast with $h$ and $w$ which are fixed for each instance of the simulation, the center of the peak moves with time. In other words, $a$ and $b$ are in fact functions of time $t$.

We have used three patterns of movement, a straight line, a zigzag, and a spiral.

Over the 100 by 100 grid, we generate 200 sensor nodes placed at random locations on the grid. Similarly, 20 nodes are used for the 10 by 10 grid. All the nodes are initialized with a residual power of 128 power units. Each query costs one unit. We use the query max.

The network uses selective querying to interrogate only some of the nodes at each iteration. As the nodes are being interrogated, the cluster head collects information about the nodes tracking their residual power and their usefulness. For illustrative purposes, we show here a smaller grid (10 by 10) with 10 nodes in Figure 1.

The first objective of the simulation is to test and refine the metrics that we have proposed for measuring the extent to which the behavior of a node is in line with the main function of the network, i.e. answering the query. The convergence factor is a function of three parameters:

- The total power consumption of a node,
- The useful power consumption of a node, which is in turn, a function of
  - The usefulness of a node (its correlation to the query)
  - The frequency with which it has been interrogated.

For the simulation, we wanted to eliminate one of the parameters and assess the effectiveness of the metric based on the remaining two. Therefore, instead of practicing selective querying, we interrogated all the nodes at every iteration. We ran the simulations with the 200 nodes as well as with a smaller set of 10 nodes. In each case, we have inserted an
intruder node. We have simulated an intruder by a node who uses power in tasks other than answering the query, typically by communicating with other nodes to deplete their power. We have simulated this by decreasing the power of these intruder nodes by 25 at each period. We monitored the convergence metrics for all the nodes. The results are shown in Figures 2 and 3 for 10 and 200 nodes respectively.

In another experiment, we have inserted multiple intruder nodes chosen at random. The results are shown in Figure 4. In the three figures, we see that there is a clear distinction between legitimate nodes (shown in blue) whose convergence value eventually picks up, and intruder nodes (shown in red) whose convergence values hit a very low ceiling and remain there for the remainder of the simulation. Intruder nodes’ convergence values are always low and always much lower than that of legitimate nodes. Therefore, we are able to accurately detect intruders, provided we can wait for at least 30 iterations. On the first iterations, some percentage of the nodes shows also low convergence. These are nodes that are in regions away from the center of the event \((a, b)\), thus the fact that their convergence is low should come as no surprise. They are using up power, but not contributing to the query, and their shutting off for a random interval of time may be beneficial to the network.

To conclude, this economics-based approach has a high level of accuracy, if we give it enough time. The time delay may be too costly though because an undetected intruder may cause havoc in the network before it is shut down. The bio-inspired model will provide us with a fast approach by which potential intruders are flagged. Once flagged, we can interrogate them extensively and reach a conclusion about their status in much less than 30 iterations.

### III. Biology Inspired Model

The use of biological metaphors and models to describe computer security problems and solutions has a long standing...
history [15] back from the phrase “computer virus” coined by Cohen [7]. The arguments made by Burgess [13] about the differences between biology and computing are by no means a rebuttal of any use of biology-inspired models. These models remain an invaluable resource alone or in combination with economics-based or other types of models. In fact, one of the characteristics of living immune systems is the fact that they are multi-layered. Nature relies on many layers of protection so that should one fail, the others can still provide protection.

A. Living organisms Security Model

Natural immune systems have many characteristics that impart them their robustness including the fact that they are multi-layered. The main layer is based on cells and molecules used to detect foreign proteins (antigens). Immune system detectors consist of T cells, B cells, and antibodies. Detection of antigens takes place by binding between the detector and the antigen based on physical or chemical properties of the binding regions. Each detector is able to identify a limited number of structurally related antigens. Detectors are generated in a partially random fashion. Detectors that match “self” proteins are eliminated. By contrast, those that detect non-self proteins have their lives and probability of “reproduction and mutation” modified accordingly, i.e. increased. Many references explain this in detail, e.g. see [16] and discuss the difference between the innate immune system that all individuals are born with and the adaptive immune system reflecting an adaptive behavior based on the history of antigens the individual has been exposed to. Detectors that are not eliminated because they do not match “self” will only bind with proteins that not “self”. Early understanding and modeling of natural immune systems reduced the problem to a binary classification of proteins as self, harmless, and non-self, harmful. This classification has been refined since allowing for harmful self proteins (e.g. rheumatism, cancer) and harmless non-self (symbiotic organism). This refinement is captured by the danger theory introduced by Matzinger who points out that immunity is more complex than distinguishing between self and non self [17], [18].

At some level, all processes, whether innate or adaptive, whether based on self/non-self or based on the danger theory, require a model of detectors, antigens and a model of the process of binding between detectors and antigens. The skeletal algorithm consists of the following steps:

1) Generate detectors using some partial random process.
2) Filter out useless detectors (those that bind with known harmless/self organisms).
3) Compare the detectors with the environing proteins/molecules, perform further tests and modify lifetime and probability distribution of detectors to be generated in the future accordingly.

B. Modeling Antigens and Detectors in Sensor Networks

In nature, detectors and antigens are defined and described by their chemical characteristics and their physical structures. We need an adequate description of nodes in a sensor network that would allow us among other things to distinguish between harmless nodes and potentially harmful nodes. The description must be restricted to those features that are accessible to the rest of the nodes. For example, we cannot include the make or any physical features as these are not available for other nodes. The only information that is available to other nodes is the contents of communication sent and received by a node. At issue then is the specific parameters about the communication that can be used as a signature for “normal” behavior or suspicious behavior. To illustrate this, we show a sample data collected from 54 sensors deployed in the Intel Berkeley Research Lab and available from their website [19]. The nodes are deployed in the lab as shown in Figure 5. We have extracted the data reported by two nodes in the following table:

<table>
<thead>
<tr>
<th>Time</th>
<th>Node</th>
<th>Temp</th>
<th>Humidity</th>
<th>Power</th>
<th>Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:01:19</td>
<td>1</td>
<td>19.2436</td>
<td>38.9742</td>
<td>45.08</td>
<td>2.68742</td>
</tr>
<tr>
<td>00:02:49</td>
<td>1</td>
<td>19.224</td>
<td>38.9401</td>
<td>45.08</td>
<td>2.68742</td>
</tr>
<tr>
<td>00:03:21</td>
<td>1</td>
<td>19.2142</td>
<td>38.9401</td>
<td>45.08</td>
<td>2.68742</td>
</tr>
<tr>
<td>00:04:24</td>
<td>1</td>
<td>19.1848</td>
<td>38.9401</td>
<td>45.08</td>
<td>2.68742</td>
</tr>
<tr>
<td>00:05:20</td>
<td>1</td>
<td>19.1946</td>
<td>38.9401</td>
<td>45.08</td>
<td>2.68742</td>
</tr>
<tr>
<td>00:06:19</td>
<td>1</td>
<td>19.175</td>
<td>38.9061</td>
<td>45.08</td>
<td>2.68742</td>
</tr>
<tr>
<td>00:06:49</td>
<td>1</td>
<td>19.1848</td>
<td>38.9401</td>
<td>45.08</td>
<td>2.68742</td>
</tr>
<tr>
<td>00:07:50</td>
<td>1</td>
<td>19.1848</td>
<td>38.9401</td>
<td>45.08</td>
<td>2.68742</td>
</tr>
<tr>
<td>00:08:20</td>
<td>1</td>
<td>19.175</td>
<td>38.9401</td>
<td>45.08</td>
<td>2.68742</td>
</tr>
<tr>
<td>00:00:21</td>
<td>2</td>
<td>19.616</td>
<td>39.7557</td>
<td>128.8</td>
<td>2.67532</td>
</tr>
<tr>
<td>00:01:18</td>
<td>2</td>
<td>19.616</td>
<td>39.7217</td>
<td>128.8</td>
<td>2.67532</td>
</tr>
<tr>
<td>00:03:23</td>
<td>2</td>
<td>19.5572</td>
<td>39.7896</td>
<td>128.8</td>
<td>2.66332</td>
</tr>
<tr>
<td>00:03:48</td>
<td>2</td>
<td>19.5572</td>
<td>39.6878</td>
<td>128.8</td>
<td>2.66332</td>
</tr>
<tr>
<td>00:06:49</td>
<td>2</td>
<td>19.5768</td>
<td>39.7217</td>
<td>128.8</td>
<td>2.66332</td>
</tr>
<tr>
<td>00:07:18</td>
<td>2</td>
<td>19.5768</td>
<td>39.6878</td>
<td>128.8</td>
<td>2.67532</td>
</tr>
<tr>
<td>00:07:49</td>
<td>2</td>
<td>19.567</td>
<td>39.7217</td>
<td>128.8</td>
<td>2.66332</td>
</tr>
<tr>
<td>00:10:20</td>
<td>2</td>
<td>19.5278</td>
<td>39.7217</td>
<td>128.8</td>
<td>2.66332</td>
</tr>
<tr>
<td>00:12:51</td>
<td>2</td>
<td>19.5376</td>
<td>39.8235</td>
<td>128.8</td>
<td>2.66332</td>
</tr>
</tbody>
</table>

Sample data from nodes 1 and 2 (MIT Lab).

Each row in this table represents the data reported by a sensor node at one iteration of the query. The first block includes...
data reported by node 1 whereas the second block is data reported by node 2. The data in a row consists of a time stamp, along with humidity, temperature, light and voltage values which are measured/queried every 31 seconds. Maybe the most glaring characteristic of the above data is how boring it is as a reflection of the high level of redundancy that exists in data collected by sensor networks. In a nutshell, it is this redundancy or lack thereof that can be used a signature for normal or abnormal signatures. In the above case, we can make the following observations:

- The ranges of the different parameters being sensed can be an important signature of normalcy. With the very limited sample, rounding the values, we can observe that humidity ranges in [19,20]; temperature ranges in [38,40], light ranges in [45, 130], and the voltage ranges in [2.5, 2.7]. Assuming that the nodes on which these observations are based are innocent nodes, we can conclude that values within the above ranges are “normal”. On the other hand, a node sensing values that are far from this range may be suspicious or compromised.

- Typically sensor networks are used to sense natural phenomena. These phenomena tend to be time continuous. The rate of change (or lack of change) is often a characteristic signature of these phenomena. For example, in the data for nodes 1 and 2, changes in humidity between one iteration and the next do not exceed 0.04. Changes in temperature are slightly higher, in the order of .5. The voltage in the other hand seems to be constant with infrequent fluctuations. Again, assuming that the two nodes shown here are normal nodes and that the data shown is typical, the first derivatives of these phenomena can be a valuable abstraction of each of the parameters being sensed.

- Natural phenomena are not only time-continuous but also space continuous. Given two nodes located close to each other, their values tend to be very similar. In the case of nodes 1 and 2, the two nodes are close to each other. They are both in the center of Figure 5. Their coordinates in meters are given in [19] are (21.5, 23) for node 1 and (24.5, 20) for node 2. Using the relative distances between nodes, we can compute the spatial derivatives of the different parameters. Based on the observation that nodes 1 and 2 are relatively closely to each other and that their values reported for humidity and temperature for example are very similar, we can observe that temperature and humidity are continuous. Notice that the same cannot be said about light. Node 2 (which is possibly very close to a window) has a much higher value than node 1. Also, by nature, light can be easily obstructed with moving obstacles and therefore is not necessarily time nor space continuous.

The above discussion pointing to three possible components of the signature of intruders and intruder detectors is but an illustration of the way in which node behavior can be captured and abstracted to identify general patterns that can be deemed innocuous or suspicious. In other words, while examining network behavior that is considered normal, the following properties can be extracted:

1) **Range of values for each of the parameters:** This is useful especially if the data being communicated has a very narrow range (e.g. [0,1]) or has a well defined restricted range (e.g. no negative values).

2) **First order time derivative for each of the parameters:** Most natural phenomena are time continuous. We may not know what value a sensor node is supposed to return, but we do know that the value that they return cannot change in some random fashion from one iteration to the next. If the first-order time derivative is constant or has a very narrow range, knowing the acceptable range will be an effective signature.

3) **First order space derivative for each of the parameters:** Most natural phenomena are also space continuous. We may not know what value a sensor node is supposed to return, but we do know that the value that they return be too dissonant with that of their closest neighbors. If the first-order space derivative is constant or has a very narrow range, knowing the acceptable range will be an effective signature.

4) **Range of values for derivatives:** Whether the rate of change is slow or fast, it may be constrained within a given range. In particular, change may be unidirectional. For example, for untethered sensor nodes, their residual power can only be decreasing. A sensor reporting an increase in its residual power is either suspicious or faulty.

5) **Pattern of change:** There is a variety of patterns of change that can also be easily captured and recognized. For example, light is not globally continuous because it can be suddenly obstructed; but in between an obstruction comes in view of a sensor and the time it leaves, the measurement is continuous. Similarly, from the time an obstruction disappears and the next one appears, the measurement is also continuous time- and space- continuous.

Once normal behavior has been captured using a combination of the above, a rotating randomly subset of the nodes is designated as detectors. The detectors will monitor the communication sent and received by their neighbors and match them against the signatures identified as normal. If a node does not match the normal signature, it is flagged as potentially suspicious; additional measures are taken to either confirm its potential harm to the network or clear its status. The further examination of the suspect nodes is discussed in the next section.

**IV. COMBINING THE TWO APPROACHES**

The danger theory introduced by Matzinger in [17], [18] is based on the idea that not every “self” organism is innocuous and not every non-self organism is harmful. There are diseases where the attackers are part of self and there are a number of non-self organisms that it is necessary to tolerate (e.g. food
in stomach) in order to survive. The theory further states that the distinction between self and non self is only a necessary first step towards immunity. One an organism has been flagged, further examination is needed to confirm its status or clear it. The further distinction is provided by the economic model discussed in section II. As we had noted, whereas the economic-based model is accurate, it is rather slow in identifying intruders. A reason for the slowness is that the detection takes place in networks that use selective querying to save power by interrogating only a small percentage of the nodes. With this, a node that is not interrogated directly may go undetected for a long time. If we rely on the bio-model approach to flag abnormally behaving nodes, the selective querying will include these nodes at every iteration and reach a conclusion quickly. We are currently using the Berkeley data to confirm this hypothesis. Results and analysis will be included in the final version of this paper.

V. SUMMARY, CONCLUSION

In this paper we have reported on our research in combining two complementary approaches to intruder detection in sensor networks. We have proposed an economics-based approach that identifies nodes as intruders if their power consumption is not justified by their overall contribution to the mission of the network. This approach is an outgrowth of research performed on query optimization through selective querying whereby nodes are selected based on their mutual information (correlation) to the query being executed. This approach is economics-based in the sense that nodes are considered harmful and put to sleep for some time interval if and only if they their contribution is not high enough to justify their power consumption. With this approach, nodes that happen to be in un-interesting areas may be flagged as harmful even if they are innocent. Shutting them down would still benefit the network. The shortcoming of this economic approach is the delay taken before a node is recognized as harmful and shut down. As a result, it may do quite a bit of harm before it is shut down.

The bio-inspired approach on the other hand, uses the detectors-antigen paradigm to identify patterns of normal behavior and detect deviations from the norm. The patterns of behavior are abstractions of the set of communication messages from and to a node. We take advantage of the inherent time and space redundancy as well as the physical constraints imposed by the phenomena being measured to capture the signature of normal behavior. Deviations from this behavior are not sufficient to condemn a node as an intruder. Instead, as is prescribed by the danger theory, those nodes are put to closer examination by the economic-model which then decides whether to shut it down or not.

The combination of the approaches gives us the best of two words. The bio-inspired approach requires only a few iterations to flag a node. Once a node is flagged, the economics-based approach can examine it more closely by interrogating it continuously and thus is able to reach a definite conclusion in another 10 or so iterations. More thorough experimental analysis will be included in the final version of this paper.

REFERENCES