Novel Approach for Security in Wireless Sensor Network using Bio-Inspirations

Heena Rathore, Venkataramana Badarla, Sushmita Jha, Anupam Gupta
Indian Institute of Technology, Jodhpur
{heena7sept, ramana, sushmitajha, ag}@iitj.ac.in

***Abstract*—Exploring the symbiotic nature of biological systems can result in valuable knowledge for computer networks. Biologically inspired approaches to security in networks are interesting to evaluate because of the analogies between network security and survival of human body under pathogenic attacks. Wireless Sensor Network (WSN) is a network based on multiple low-cost communication and computing devices connected to sensor nodes which sense physical parameters. While the spread of viruses in wired systems has been studied in-depth, applying trust in WSN is an emerging research area. Security threats can be introduced in WSN through various means, such as a benevolent sensor node turning fraudulent after a certain period of time. The proposed research work uses biological inspirations and machine learning techniques for adding security against such threats. While it uses machine learning techniques to identify the fraudulent nodes, consecutively by deriving inspiration from human immune system it effectively nullify the impact of the fraudulent ones on the network. Proposed work has been implemented in LabVIEW platform and obtained results that demonstrate the accuracy, robustness of the proposed model.**

***Index Terms*—Biologically Inspired, Machine Learning, WSN, Human Immune System, Security.**

I. Introduction

Inspired by intrinsic appealing characteristics of biological systems, many researchers are engaged in producing novel design paradigms to address challenges in current network systems [1]. Bio-inspired systems are those systems where biology plays an important role to solve the problems in other domain. Biological inspired approaches seem promising since they are capable to self adapt, self heal, self organise in varying environmental conditions [2]. One of the incredibly diverse characteristic of biological system is that they are robust.

Over the recent years, there has been a paradigm shift in the development of computer networks; from monolithic, centralised systems to independent, distributed, self organised systems such as Wireless Sensor Networks (WSN). There are various factors which influence sensor network design like scalability, production cost, operating environment, hardware constraints, transmission media, power consumption while sensing, data processing, and communicating [3]. Due to expandability and scalability features of the system, new nodes can enter at various times. However, this also makes them prone to various types of attacks [10]. Due to this, it is imperative for these distributed systems to have the ability to adapt and organise in the changing world. If one looks at the characteristics of biological systems and the challenges faced by distributed network systems, it is pretty evident that one can apply bio-inspired techniques to solve these challenges [9]. While the spread of viruses in wired systems has been studied in-depth, applying trust in wireless sensor network nodes is an emerging area [4], [5], [6], [7], [8].

The objective of this paper is to present the design of a security system for WSN using human immune system as inspiration. Section II explains the trust and reputation model and its implementation. Section III describes the novel approach that can be used in WSN for detection and removal of fraudulent nodes. It also describes the human immune systems and explains the concept of T-cells and B-cells in our system. Section IV describes the antigen and antibody concept used for the removal of the fraudulent node. Section V summarizes the paper and presents scope for future work.

II. Related Work

WSN can be considered as living beings usually born (configured) in a controlled environment, where all its nodes are cells that work selflessly towards a common goal. Sensor nodes acquire data and send them to the gateway in a wireless fashion. Since the sensor nodes are remotely located, it is possible that someone tampers the sensor nodes.

A simple example of malicious behaviour can occur when the node is communicating the data. It is possible that the node can start misbehaving while forwarding data, and can become selfish or can all together exclude the data [14]. Detection of such fraudulent nodes become mandatory in such type of networks.

Trust management systems for WSN could be very useful for detecting such misbehaving nodes and for assisting the decision-making process. The concept of trust has become very relevant in these days as a consequence of the growth of fields such as internet transactions or electronic commerce. The trust models in wireless sensor networks are aimed to provide trust ratings to the sensor nodes based upon its performance and measurements which it sends. Consecutively based upon the trust ratings the nodes can be removed from the system. Higher the trust ratings higher its performance, similarly lower the trust ratings higher are the chances to remove it from the system. In literature there are many trust models developed such as weightings method, artificial neural network method, swarm intelligence method etc [15]. This section describes the three models used to compute the trust ratings.

978-1-4799-3635-9/14/$31.00 ©2014 IEEE

A. Weightings method

In weightings method, initially every node is highly trusted assigning them the weights equal to one. The network is adapted in the architecture between a group of sensor nodes and their forwarding node (FN) as shown in Figure 1. The FN

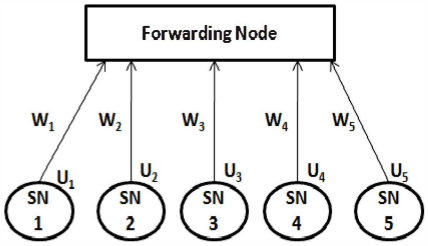

Fig. 1. Topology of weightings method

collects all information provided by sensor nodes and calculates an aggregation result E using the weight W_n assigned to each sensor node as given in the formula [20]:

$$E = \sum_{i=1}^{N} W_n \times U_n \tag{1}$$

Where U_n is data collected from sensor nodes and is application dependent i.e. it could be temperature readings for thermocouple sensor nodes. If weights are equal to one then E equals U so no need to update else weights are updated for each based upon the variation of E with respect to U with the help of following equation where θ is a constant value and r is the ratio of sensor node sending bad data to the total number of nodes under the same FN.

$$W_n = \begin{cases} W_n - \theta \times r_n & \text{if } U_n \neq \text{E} \\ W_n & \text{elsewise} \end{cases} \tag{2}$$

For implementation, topology of 5 sensor node was taken, where initially every node was given weight equal to one and θ was kept as 0.1. Random data was generated between 10 and 20 for each of the sensor node and its deviation from mean value of past history was checked and if its variation is greater than 0.1 then weights were updated from the above equations. Figure 2 shows the result depicting rate of change of weights. Y-axis on the graph represents the weights and and X-axis on the graph represents the time which explains how the trust ratings is decreased with respect to time based on the formula used.

B. Artificial Neural Network

Artificial Neural Network (ANN) approach in WSN calculates trust value based on present values as well as past history of neighbouring nodes. The result so computed is based on three parameters that is the interconnection pattern, learning process and activation function as shown in Figure 3. Based on the actual value received from the selected sensor node and the predicted value from estimation and prediction block, trust ratings are generated. Figure 4 is the result, where y axis is the measurement and x axis is the time in seconds. Dark

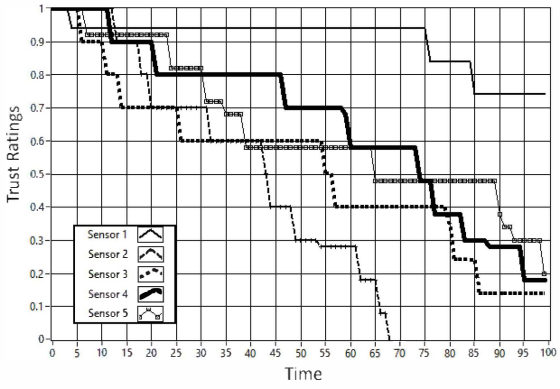

Fig. 2. LabVIEW implementation of weightings method

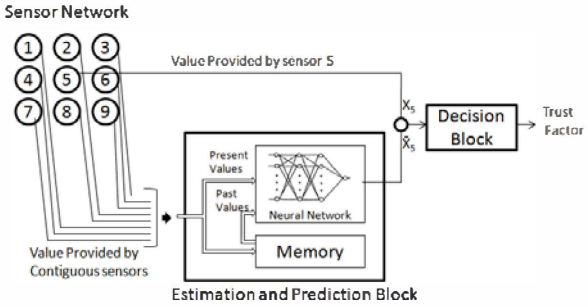

Fig. 3. Artificial Neural Network approach [17]

line shows the predicted value of measurement and light line shows the actual reading. The trust ratings are assigned in such

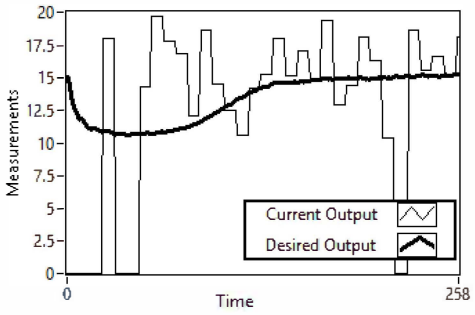

Fig. 4. LabVIEW implementation of ANN

a way that lesser the variation between the predicted value and the actual value higher the trust rating and vice versa.

C. Swarm Intelligence

Swarm Intelligence can be defined as collection of social insects and animals which can be represented by spatial arrangement and synchronized motion of individuals. Collectively they can perform impressively complex tasks such as nest building and food gathering eg. ant colony. In ant colony optimization technique, each of the ant deposit pheromone while traversing for the shortest path [19]. The amount of pheromone deposition is inversely

proportional to distance such that shorter the path larger is the deposition. Finally the ants converge to the shortest path.

Swarm Intelligence in trust model is used to find the most reputable path leading to the most trustworthy node. For implementation, 10 random active nodes was taken in a grid. Shortest path was computed between the source and destination using Dijkstra's algorithm, showing the nodes in between the path as the trustworthy nodes. As seen in Figure 5, first part denotes all the active nodes between the source 1 and destination 10; second part shows the shortest path between the two having 4, 5, 6 and 9 calculated using Dijkstra's Algorithm [18].

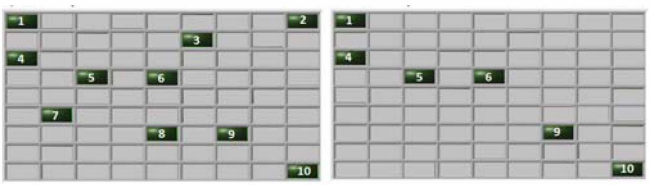

Fig. 5. LabVIEW implementation of swarm intelligence

III. Proposed Work

Machine Learning Based Biologically Inspired Security model for WSNs can be divided into two essential blocks namely machine learning module and immune module. Machine Learning Module has three basic part K means, Support Vector Machine (SVM) and Anomaly Detection Engine and is used for the detection of fraudulent nodes. Followed by Immune Module which is used to remove the fraudulent node from the system just like the defensive mechanism used to remove foreign particles in our body. The flowchart describing the overall model is as shown in Figure 6.

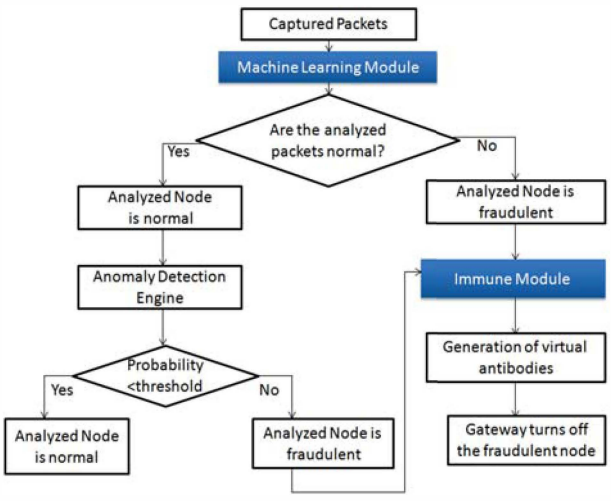

Fig. 6. Flowchart of proposed work

1) Data is acquired for certain time.
2) K-means algorithm is performed for making clusters. Essentially there would be two clusters in it, *faulty* cluster and *normal* cluster.
3) Passed to support vector machine for creation of decision block. The decision block that is created would have faulty region, normal region and critical region(Boundary values).
4) Identify the critical or border line area by anomaly detection algorithm. Anomaly detection engine takes the mean and standard deviation of the benevolent data set identified by SVM. Threshold ϵ is set such that for values $<$ threshold, consider it as anomaly otherwise normal.
5) When anomaly is detected, we activate immune module by initializing a variable set as g(t) to one for that particular sensor node for others it is zero. When g(t) becomes one, then immune module comes into picture.
6) Virtual antibodies are produced for changing the sampling interval of the fraudulent node. Measurements are predicted and sent to gateway on taking account of antigen value.
7) Finally gateway would be turning off the sensor node based upon the virtual antibody values.

A. Machine Learning Module

Machine learning is one of the Intrusion Detection System(IDS) which checks the network traffic and decides whether these are symptoms of an attack or not [16], [25]. Machine learning techniques develop algorithms for making predictions from data, to develop a model for accomplishing a particular task. Tom Mitchell described it as making a machine learn with time. A computer program is said to learn from experience E with respect to some task T and some performance measure P, if P improves in direct proportion with E [21]. Anomaly Detection is a major component of IDS. It detects abnormal activities from a predefined normal profile in order to identify possible attack. It can be supervised (having prior knowledge of the classes), or unsupervised (No knowledge).

1) K-Means: K-means is an unsupervised machine learning method which works on principle of finding a structure out of an unlabelled data set. It groups data to make clusters [22]. It has two major tasks:

- **Cluster assignment**: Assign each observation to the closest centroid.
- **Move centroids**: Take the average of all points pointing to each centroid and then move each of these to the average position.

Repeat the above two steps till convergence.

Algorithm for K-means:
Input:
k(Number of clusters),
Training set($x^{(1)}, x^{(2)}.....x^{(m)}$), where $x^{(i)} \in R^{(n)}$ and denotes observation.
Procedure:
Randomly initialize k cluster centroids $\mu_1, \mu_2.....\mu_K$,

repeat [
for i=1 to m
c^i =*index from 1 to k of cluster centroid closest to* x_i

$$c^i = min_k \parallel x^{(i)} - \mu_k \parallel \tag{3}$$

for k=1 to k
μ_k = *average(mean) of points assigned to cluster k.]*

Figure 7 first part shows the random data and second part shows two clusters generated out of random data.

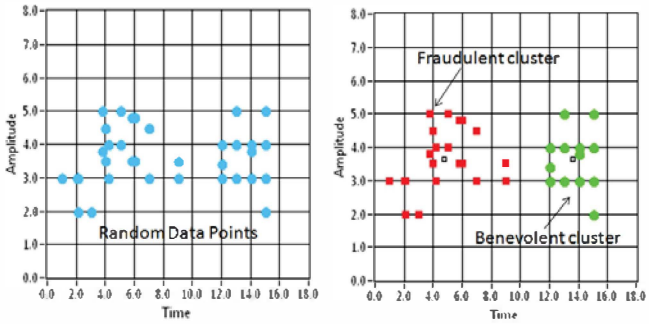

Fig. 7. Learned data from K-Means algorithm

2) Support Vector Machine: Classification of data comes under this category and it is used when we are given labelled data and we need to describe pattern and create decision boundary [23], [24]. Support vector machine(SVM) is a popular tool used to classify the data and create a decision boundary to distinguish between fraudulent and good data. Hence the data which was classified into clusters from k-means algorithm when given to support vector machine creates the decision boundary as shown in Figure 8. Now as new data is received, if it lies in the fraudulent data points region, it is considered as fraudulent, else it is considered as benevolent (good) data.

3) Anomaly Detection Engine: SVM creates the decision boundary however the data which lies on the boundary needs to be further evaluated for better accuracy and precision. Anomaly Detection Engine is used for the boundary values between the two regions as shown in Figure 8 which is the output of SVM. It works in such a way that we calculate mean and standard deviation of the benevolent data points and compute the probability distribution of data points using Equations 4, 5 and 6. Equations 4 and 5 are used to compute the mean/average and standard deviation of the benevolent data points respectively. Equation 6 is used to calculate the probability distribution.

$$\mu_j = \frac{1}{m}\sum_{i=1}^{m} x_j^i \tag{4}$$

$$\sigma_j^2 = \frac{1}{m}\sum_{i=1}^{m}(x_j^i - \mu_j)^2 \tag{5}$$

Given new example x, we compute p(x).

$$p(x) = \Pi_{j=1}^{n} p(x_j, \mu_j, \sigma_j^2) = \Pi_{j=1}^{n} exp\frac{-(x_j - \mu_j)^2}{2\sigma_j^2} \tag{6}$$

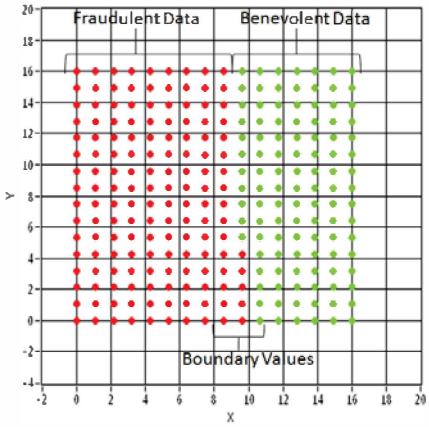

Fig. 8. Support Vector Machine in 2D

The probability distribution function of x and y is as shown in Figure 9.

The combined probability distribution function of x and y is

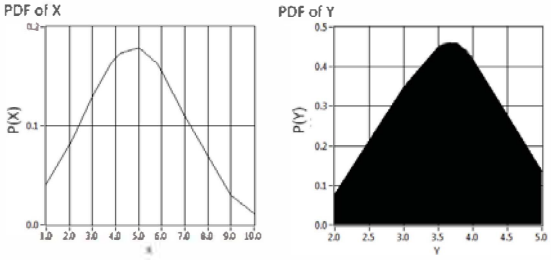

Fig. 9. Probability distribution function

as shown in Figure 10 using Equation 7.

$$p(x) = p(x, \mu_x, \sigma_y^2)p(y, \mu_y, \sigma_y^2) \tag{7}$$

Threshold ϵ is maintained and if the probability of new data

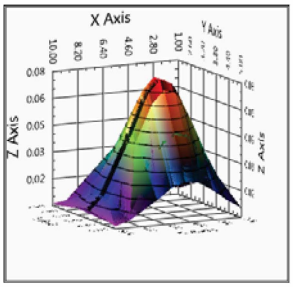

Fig. 10. Combined PDF

point $< \epsilon$, it is considered as anomaly otherwise not.
The outcome of the machine learning module is the set of all malicious data points.

B. Immune Module

Biological immune systems have intelligent capabilities of detecting antigens (foreign bodies in the system) in the body. The adaptive immune system consists of two complementary

systems, namely cellular immune system and humoral immune system. The humoral immune system is aimed at bacterial infections and extracellular viruses, but can also respond to individual foreign proteins. This system contains soluble proteins called antibodies which bind bacteria, viruses, or large molecules identified as foreign and target them for destruction. Antibodies are produced by B-cells. The cellular immune system destroys host cells infected by viruses and also destroys some parasites. The agents at the heart of this system are a class of T-cells. B-cells are like the body's military intelligence system, seeking out their targets and sending defences to lock onto them [12]. Antigens are secreted by the pathogens which causes the adaptive immune system to respond. B-cells produce and secrete antibodies after they encounter antigens. Once they produce specific antibody for the antigen it forms a complex called antigen antibody complex which in turn is engulfed by T-cells. After the B-cells produce antibodies they give rise to plasma cells from which further antibodies are produced for that specific antigen.

Mathematical Model

In 1977, Dibrov's et al. devised a model to study the rate of change of antibodies and antigen. Dibrov Model consists of coupled equations for the antibody quantity *a*, the antigen quantity *g*, and the small B cell population *x* [13]. Since *x* is generally considered as a constant, the rate of change of *x* is zero and the third equation is ignored. Now consider the set of equations describing antigen-antibody interactions:

$$\frac{dg}{dt} = Kg - Qag \tag{8}$$

$$\frac{da}{dt} = AH(t-T)g(t-T) - Rag - Ea \tag{9}$$

where Equations 8 and 9 are the rate of change of antigen and antibody respectively. Also K, Q, A, R, E are rate constants. K is the overall growth rate of antigen.

H(t) in Equation 9 is the Heaviside step function whose value is zero for negative argument and one for positive argument.

$$H(t) = 0, \quad t < 0 \tag{10}$$

$$H(t) = 1, \quad t \geq 0 \tag{11}$$

The product '*ag*' is the complex formed as antibody-antigen complex. As the complex is formed, it results in net loss of the antibody and antigen. The simplest assumption is that of the law of mass action, valid when the densities are below a saturation level, that is that the losses are proportional to the product of the antibody and antigen densities. The rate constants Q and R are necessarily not same. The rate of antibody production at time t is supposed to be proportional to the rate of small B cell stimulation at time *t - T*. That is, there is a delay *T* between stimulation of a small B-cell and the subsequent production of plasma cells from it [26].

When simulations were carried out using the Runge-Kutta(variable) method for solving the differential equations, following results were seen as shown in Figure 11. It shows the graph of rate of change of antigen and antibody as a function

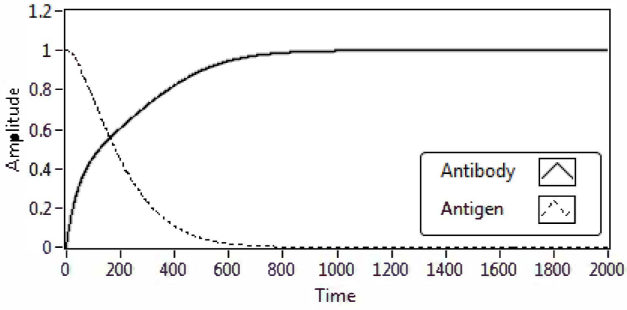

Fig. 11. Rate of change of antigen and antibody

of time, for values of $K = 0.01$, $Q = 1$, $A = 1$, $R = 1$, $E = 1$ with initial conditions $a_0 = 0$ and $g_0 = 1$. This shows that the antigen count linearly increases and when the body comes to know about it, the B-cells start producing antibodies and when the antigen antibody complex is formed, the count of antigen decreases linearly and rate of change of antibody becomes constant.

IV. Experiments and Results

In the Immune Module, Dibrov Model was the basis for virtual antibodies production analogous to antibody production by B-cells in human immune system. It focuses on giving correct readings even if the node has become malicious. This is done to increase the lifetime of malicious node so that even if it gets corrupted, node gives correct readings. This is done by assigning weights to the measurement values and these weights are proportional to the antigen values. Prior to the malicious node detection, weights are assigned as one. After the malicious node is detected, the expected measurement value would be dependent on the previous measurements and the weights would be decreased proportional to the antigen values taken from the differential equation as shown in Figure 12.

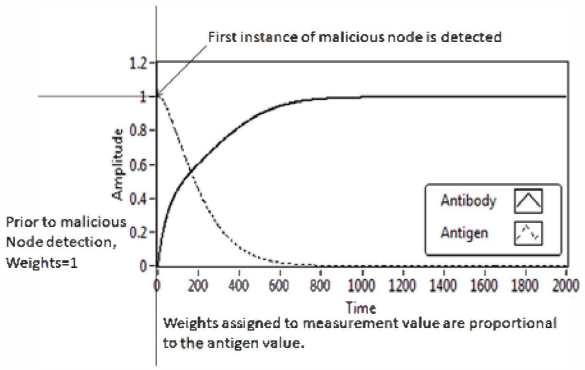

Fig. 12. Relationship between weights and antigens

Also in sensor node the measurements are taken keeping the sampling interval constant. Hence after the node becomes malicious, there is need to turn off the malicious node. However turning off the fraudulent node immediately after

detection is not a feasible solution since it would affect the stability of the system. Hence a better solution would be to either slowly decrease the sampling interval to zero or to increase the sampling interval depending upon the application. For instance increasing the sampling interval means the rate at which the samples are collected is increased so that good measurements would last for longer period. Other probability is that sometimes fraudulent node can become benevolent after sometime. This particular thing is called ON-OFF attack [7]. In that case increasing the sampling interval would be beneficial. Figure 13 shows the raw measurements from the fraudulent sensor node. It shows when there is no security on fraudulent node and no sampling interval change, measurements would be like this. Four different scenarios were considered for

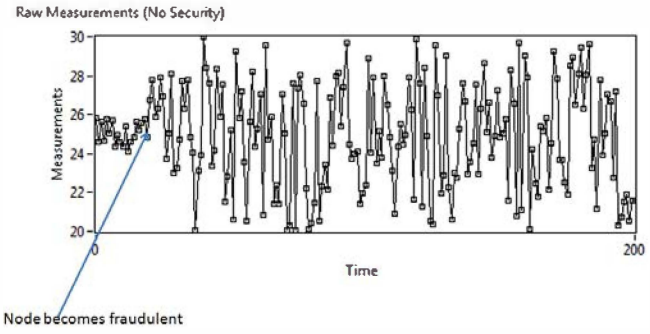

Fig. 13. Measurements on no security

comparison purpose:

- Non Weighted Averaging: Simple averaging is done, not assigning weights to the previous measurements.
- Weighted Averaging: Weight is assigned to the previous measurement readings for the computation of new measurement readings.
- Weighted Averaging and increasing sampling interval
- Weighted Averaging and decrease sampling interval

A. Non Weighted Averaging

In non weighted averaging the measurement readings would be varied according to the noise in the malicious node. The variance from the true measurement is also varied. Lifetime of the malicious node is infinity here, since there is no change in the sampling interval for capturing the future measurements.

B. Weighted Averaging

In weighted averaging case, clearly the measurements would decrease since it is dependent on the weights given to the previous readings as shown in Figure 14. Here weights are made proportional to the antigen value taken from the differential equation. Hence the measurements would be calculated as per the following equation.

$$T_{new} = \frac{\sum_{i=1}^{N} Wi \times T_{prev}}{N} \tag{12}$$

where T_{new} is the new measurement obtained by applying weights, T_{prev} is the previous measurement, N is the history length, W is the weight which is kept proportional to the antigen value i.e. $W_i = k \times g_i$ where K is kept as 1.

C. Weighted Averaging and increasing sampling interval

In weighted averaging + increase in sampling interval, good measurements would persist its state on true measurement for longer duration making the lifetime of malicious node longer. The sampling interval is increased by taking into account the antibodies value from differential equation. The rate at which the sampling interval is increased is

$$s_{afterAttack} = 2^{\left\lfloor \frac{a_i}{\frac{(a_{max} - a_{min})}{k}} \right\rfloor + 1} \times s_{priorToAttack} \tag{13}$$

Here $s_{afterAttack}$ is the sampling interval after the malicious node is detected and $s_{priorTottack}$ is the sampling interval prior to the detection, a is the antibody value where a_{max} and a_{min} is fixed to 1 and 0 respectively. k is the number of steps desired to end influence of malicious node (in this case it is fixed to 10).

D. Weighted Averaging and decrease sampling interval

In the fourth scenario where sampling interval is decreased, variance from true measurements would be high leading to make malicious node lifetime very less. And when sampling interval is changed, sampling interval of other channels would also be affected. The rate at which the sampling interval is decreased is

$$s_{afterAttack} = \frac{s_{priorToAttack}}{2^{\left\lfloor \frac{a_i}{\frac{(a_{max} - a_{min})}{k}} \right\rfloor + 1}} \tag{14}$$

Results comparing various options is as shown in Figure 14.

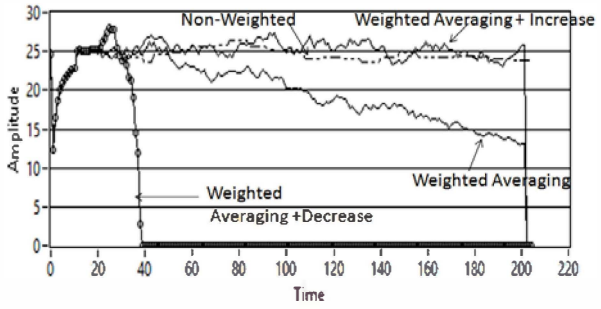

Fig. 14. Measurements on various options

E. Results comparing different options

As seen from Figure 14 following tabular result can be formulated. The comparison is done on three metrics; lifetime of malicious node, variance from true measurement and impact on other channels. Intuitively lifetime of malicious node should be less and is least in case when there is decrease in sampling interval. Variance from true measurement is less in case of weighted averaging and increase in sampling interval. The impact on other channels only happen in the last two cases. As seen from the results it is recommended to use

weighted averaging. We can choose to increase or decrease the sampling interval based upon the application we are using. If we want an application to remove the fraudulent node immediately but still giving correct readings then decrease in sampling interval is better option. And if we want to still monitor the malicious node after the detection as well then we can increase the sampling interval. The qualitative

Metric	Non-weighted Averaging	Weighted Averaging	Weighted Averaging+ Increase sampling interval	Weighted Averaging+ Decrease sampling interval
Malicious Node Lifetime (Response Time)	Infinity	Medium	Medium	Low
Variance from True Measurement	Varied, depends on type of noise	High	Low	High
Impact on other channels in infected node	None	None	High	High

Fig. 15. Results comparing different options

method comparison of the three models vs proposed model is tabulated in the below table: The table explains in terms of

Method	Dependence on neighboring nodes	Complexity	Response Time
Weightings	Yes	Low	Low
Neural Network	Yes	High	Low
Swarm Intelligence	Yes	Low	Medium
Proposed Algorithm	Controllable	Med-High (during Training) Very Low (post training)	Controllable

Fig. 16. Qualitative method comparison

qualitative comparison, proposed algorithm is better making it energy and efficient model. It tells during the training phase it can take time but post training it takes very less time to remove the fraudulent node from the picture since immune model revolves around solving only two differential equations. The response time is also controllable since we can either increase or decrease the sampling interval depending upon the application.

V. Conclusion and Future Scope

This paper described the human immune system, specifically focussing on the adaptive immune system consisting of the T-cells and B-cells. Aim was to derive inspiration from these cells to design a security system for next generation wireless sensor network (WSN). In sensor network where fraudulent nodes can hamper the system it is necessary to remove these nodes without affecting the overall system. Various trust models have been developed for the same. The proposed model is a mixture of machine learning module and immune module. Where machine module is used for the detection of the fraudulent nodes; immune module is used for the removal of those nodes taking into account the antigen and antibody concept. Where antigen values are used for the prediction of new values, antibody values are used to change the sampling interval. The proposed model proved to be a benefactor as against the previous models. Since we have only incorporated the primary response of immune system, future work aims on including the secondary response as well focussed primarily on weighted averaging and decrease in the sampling interval. Secondary response means if the same type of maliciousness occurs in the sensor network, the antibody production increases at faster rate, in the similar way which happens in our body.

Acknowledgements

This work was carried out under the National Instruments PhD Summer Internship Program under the supervision of Dr. Ajay Gupta. Authors would like to thank Mr. Abhay Samant, Mr. Chinmay Misra and Mr. Hardik Asawa for their help with the simulations performed using National Instruments LabVIEW 2012. Authors are also indebted to The Tata Consultancy Services for providing the sponsorship to the project.

References

[1] Meisel, Michael, Vasileios Pappas, and Lixia Zhang, "A taxonomy of biologically inspired research in computer networking.", *Elsevier Computer Networks Journal*, vol. 54, no. 6, pp. 901-916, 2009.

[2] Falko Dressler , Ozgur B. Akan, "A survey on bio-inspired networking", *Elsevier Computer Networks Journal*, vol. 54, no. 6, pp. 881900, 2010.

[3] I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci, "Wireless sensor networks: a survey", *Elsevier Computer Networks Journal*, vol. 38, pp. 393422, 2002.

[4] Guang Yang,"Introduction to TCP/IP Network Attacks", *Secure Systems Lab*, 1997.

[5] Sudhir Agrawal, Sanjeev Jain, Sanjeev Sharma, "A Survey of Routing Attacks and Security Measures in Mobile Ad-Hoc Networks", *Journal of computing*, vol. 3, no. 1, pp. 41-48, 2011.

[6] Yenumula B. Reddy , "Trust-Based Approach in Wireless Sensor networks using an Agent to each Cluster, *International Journal of Security, Privacy and Trust Management*, vol.1, no.1, pp. 19-36, 2012.

[7] Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago , "Trust management systems for wireless sensor networks: Best practices", *Elsevier Computer Communications Journal*, vol. 33, no. 9, pp. 1086-1093, 2010.

[8] Haiguang Chen1, Huafeng Wu, Xi Zhou, Chuanshan Gao, "Agent-based Trust Model in Wireless Sensor Networks", *ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*, no. 8, pp. 119-124, 2007.

[9] Gomez Marmol, Felix, and Gregorio Martnez Perez. "Providing trust in wireless sensor networks using a bio-inspired technique." *Telecommunication systems*, vol. 46, no. 2, pp. 163-180, 2011.

[10] A. Boukerch, L. Xu, K. EL-Khatib, "Trust-based security for wireless ad hoc and sensor networks." *Elsevier Computer Communications Journal*, vol. 30, no. 11, pp. 24132427, 2007.

[11] Julie Greensmith, Amanda Whitbrook and Uwe Aickelin, "Artificial Immune Systems", Book on Handbook of Metaheuristic, 2010.

[12] Heena Rathore, Abhay Samant, "A system for building immunity in social networks", in proc. *Fourth World Congress on Nature and Biologically Inspired Computing (NaBIC)*, no.4, pp. 20-24, 2012.

[13] A. C. Fowler, "Approximate Solution of a Model of Biological Immune Responses Incorporating Delay", *Journal of Mathematical Biology*, vol. 13, pp. 23-45, 1981.

[14] Mohammad Momani and Subhash Challa , "Probabilistic modelling and recursive bayesian estimation of trust in wireless sensor networks", *Book on Bayesian Network*, 2007.

[15] Mohammad Momani , Subhash Challa," Survey of Trust Models in Different Network Domains, *International Journal of Ad Hoc, Sensor and Ubiquitous Computing*, vol. 1, no.3, pp. 1-19, 2010.

[16] Murad A. Rassam, M.A. Maarof and Anazida Zainal, "A Survey of Intrusion Detection Schemes in Wireless Sensor Networks, *American Journal of Applied Sciences*, vol. 9, no. 2, pp. 69-83, 2012.

[17] Daniel-loan Curiac, Constantin Volosencu, Alex Doboli, Octa Vian Dranga, Tomasz Bednarz,"Discovery of Malicious Nodes in Wireless Sensor Networks Using Neural Predictors, *WSEAS Transactions On Computer Research*, vol. 2, no. 1, pp. 38-43, 2007.

[18] John N. Tsitsikli,"Efficient Algorithms for Globally Optimal Trajectories", *IEEE Transactions on Automatic Control*, vol. 40, no. 9, pp. 1528-1538, 1995.

[19] Flix Gmez Mrmol, Gregorio Martnez Prez "Providing trust in wireless sensor networks using a bio-inspired technique, *Telecommunication Systems*, vol. 46, no. 2, pp. 163-180, 2011.

[20] Idris M. Atakli, Hongbing Hu, Yu Chen, Wei Shinn Ku , "Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation, in proc. *Spring simulation Multiconference*, pp. 836-843, 2008.

[21] Mitchell, T., *Book on Machine Learning*, McGraw Hill, pp.2, 1977. Rehan Akbani, Turgay Korkmaz, and G. V. S. Raju ,"A Machine Learning Based Reputation System for Defending Against Malicious Node Behavior", *IEEE Globecom Computer and Communications Network Security Symposium (GC'08 CCNS)*, 2008.

[22] MacKay, David, "Information Theory, Inference and Learning Algorithms", *Chapter 20. An Example Inference Task: Clustering*, Cambridge University Press, pp. 284-292, 2003.

[23] John Felix Charles Joseph, Bu-Sung Lee, Amitabha Das, Boon-Chong Seet,"Cross-Layer Detection of Sinking Behavior in Wireless Ad Hoc Networks Using SVM and FDA", *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 2, pp. 233-245, 2011.

[24] Simon Tong, Daphne Koller, "Support Vector Machine Active Learning with Applications to Text Classication", *Journal of Machine Learning Research*, pp. 45-66, 2001.

[25] Hichem Sedjelmaci and Mohamed Feham, "Novel Hybrid Intrusion Detection System for clustered wireless sensor network", *International Journal of Network Security and Its Applications*, vol.3, no.4, pp. 1-14, 2011.

[26] Heena Rathore, Sushmita Jha, "Bio-Inspired Machine Learning Based Wireless Sensor Network Security", *Fifth world Congress on Nature and Biologically Inspired Computing*, 2013.