Artificial Immune Systems Application in Power Grid and Security Architecture

Akash K Singh
IBM Corporation
Sacramento, USA
E,mail: akashs@us.ibm.com

***Abstract*— Artificial immune system (AIS) research is to address the security problem caused by the immunodeficiency. This study is focused on the biological immune system that provides the biological immunity to fight with the diseases and other virus. Research in system protection is important as biological immune system is not good at because of problems like immunodeficiency, hypersensitivity and autoimmunity. Analysis of immune protection principle helps in the development of intelligent system that is highly efficient and robust. Computation Intelligence aspects of the system design based on the properties of the Immune systems helps in the development of algorithms and technique that are biologically inspired and function better. Application of AIS in Power System and Security is being studied.**

Keywords - Auto Immune pathology, artificial immune system, negative selection algorithm, immunodeficiency, Intelligent System

I. INTRODUCTION

Forecasting is a major operation task of many industrial projects like power engineering, Energy Systems. There are many artificial intelligence based models that are available to forecast the payload and simulate the future process and execution of plant. Especially in Smart Grid Infrastructure it is highly required to have optimal forecast to reduce the waste and conserve the energy and reduce the wastage of energy or electricity in power grids. This kind of framework aids in ensuring the appropriate amount of energy delivered to the customer and specific devices for power production. Implementation of this kind of decision support model improves the power distribution, network performance and device failure in advance. Demand and Supply is based on many factors like time & frequency of delivery, payload and environmental conditions. So it is very important to develop a relationship and forecast map in terms of above mentioned factors that could trigger the changes in the power delivery. Classical methods like Mutual Information, Expectation Maximization and Bayesian Algorithms helps in predicting the future payload, disturbance and node failure.

Artificial Intelligence technique are primarily in use for forecasting the load, power distribution pattern is based on many factors and AI based model do help in optimizing the electrical energy payload graph.

Non Linear variables and associate functions are calibrated and analyzed based on Artificial Intelligence techniques. Technique primarily looks for temperature and weather variables, payload growth and changes are attributed to the weighting factors to calculate the functional relationship between payload and nonlinear variables.

The more recent approaches for load forecasting are based on Artificial Intelligent (AI), Machine Learning and Neural Networks technique. Realizing that the electrical energy load pattern is heavily dependent on the non-linear variables such as temperature, environment factors and weather, therefore the main task in the AI technique is to find a functional relationship between the nonlinear variables associated with electrical components and the system load [3]. The future load is predicted by inserting the predicted array of variable information into the predetermined functional relationship matrix. One of the AI techniques that are commonly used for performing load forecasting task is the Artificial Neural Network (ANN) along with Fuzzy Maps. ANN is a computational tool inspired by the network of neurons in biological nervous system; neurons are the unit for information. It is a network consisting of arrays of artificial neurons linked together with different weights of connection and dendrites with synapse and axons. The states of the neurons as well as the weights of connections among them are dependent upon the activation state and the threshold that can be supported by the neuron and evolves according to certain learning rules like supervised learning or unsupervised learning [3]. In other word, neural networks are dynamic intelligent modeling tools that are in use to find the relationship between input and output or to find patterns in large database or gives the decision model for real time events and changes in the dynamics of the system. ANN has been applied in statistical model development, adaptive control system, pattern recognition in data mining, and uncertainty in decision based system and support models and its application in Medical, Engineering and Robotics,

etc[4]. Autoimmune system is able to learn to perform a pattern recognition task by automatically changing the values of its weights and optimized results by adjusting the parameters and its values to reach the optimal level of performance and robustness. In the past few decades, different types of learning algorithms for the ANN have been developed by many researchers and more to come. For instance, Hebbian learning and competitive learning and Self Organizing Map (SOM) were developed for unsupervised learning, while Least Mean Squares (LMS) and Back Propagation (BP) of error algorithms were developed for supervised learning [5]. Artificial Immune System (AIS) has emerged in the 1990s as a new branch in Artificial Intelligence and since then AIS has been used in various applications such as intelligence system, pattern recognition, fault detection, social network and consumer behavior and user characteristics on internet, computer security and optimization [6]. The basic fundamental principle of the AIS is inspired from the vertebrae immune system. The natural immune system is a very interesting subject from the computational standpoint as it is parallel, distributed, diverse, self-organizing with ability for recognition, self learning and memory management capabilities and decision making [7].

A. Science of Immune Systems

Based on pathological details, immune diseases are listed below. This research is focus on finding the cause of this disease and proposing a solution in systems that can be developed based on AIS and don't have below disease models.

(1) Immunodeficiency: is a condition in which immune system is not able to fight against infectious disease. Primary immunodeficiency disorders are hereditary, autosomal recessive or X-linked. There are immunodeficiency syndromes that are grouped for example lymphocytes or granulocytes.

(2) Hypersensitivity: is a immune response that damages tissues. Type I hypersensitivity is an anaphylactic reaction associated with allergy. Type II hypersensitivity is a binding of antibodies with antigens on subjects cells and marking them for destruction. Type III hypersensitivity is because of immune complexes (IgM antibodies, IgG, aggregation of antigens, and complement protein). Type IV hypersensitivity are in autoimmune and infectious diseases.

(3) Autoimmunity: It's a Long-term inflammation, physical and chemical factors can activate T and B cells that respond to self-antigens to produce immune response towards self- tissues. During this course antibody killing self cells and hypersensitive lymphocytes will appear in symptoms. Immunodeficiency, Hypersensitivity and Autoimmunity are three immune diseases, immunodeficiency has no killing effect on biological system, while autoimmunity and hypersensitivity will exert killing effect on biological system, and is called immune injury or allergic reaction to the tissues. According to the difference in immune mechanism, immune injury can be classified into various types of immune allergic reactions, such as

- Type 1 immune allergic reaction is also called anaphylaxis. Since it takes place with high speed

- Type 2 immune allergic reaction is a kind of immediate hypersensitivity.

- Type 3 immune allergic reaction is also called cell toxin antibody reaction. It is related with the combination of antibody with antigen on the surface of target cells. The antigens can be the cell membrane and outer antigens or semi- antigens on the surface of the cells. This type of allergic reaction will lead to cell injury with different mechanisms.

- Type 4 immune allergic reaction is also called immune complex mediated hypersensitivity. Immune complex is generated with the combination of antigen with antibody, these immune complex will immediately cleared off by phagocyte cells. Yet, if the immune complex deposits on the blood vessel and leads to sever vessel inflammation, immune diseases will arise. The antigens will lead to immune complex mediated hypersensitivity vary in type and property.

- Type 5 immune allergic reaction is also called lagging hypersensitivity; it is related with allergy causing T cells.

- In Type 6 immune allergic reaction, phagocyte cells are usually the basic effecting immune cells. In cell mediated cell toxin reactions, allergy causing T cells have killing effect and will exert killing effect on the target cells.

B. Influence of Immune Pathology on AIS

Artificial immune system introduces the superior properties of biological immune system into the study of intelligent system, but the disease-causing mechanism of immune pathology has been transmitted into artificial immune system too. With the development of attacking techniques, the security

problems from immune pathology have been more and more sever. Taking artificial immune security system as an example, we analyze the security problems and system flaws connected with immune pathology in artificial immune system. The security problems from immune pathology can be classified as the following: (1) Security threats from immunodeficiency This kind of threats can be found in the following cases: if the attack properties in detector string are innately incomplete or mistaken under attack, the detectors generated by negative selection algorithm will suffer defense deficiency and will fail to identify certain attacks and insecure operations. Then the security system will probably develop "immune tolerance" to certain attacks, and security "vacuum phenomenon" will arise. (2) Security threats from hypersensitivity These security problems are similar with type I immune allergic reaction in immune system, if the threshold value of negative selection algorithm is inappropriate , many detectors with self antibody and killing effect will be released into security system. These improper detectors will produce abnormally frequent attack responses and the system resources will be harmfully taken up to react to these false attacks. A typical attack method of hypersensitivity is DoS (denial of service) attack. Because of the complexity in user behavior and operation, if the detector analyzes valid user activity with different operating mode or network packets with different protocols, the detectors will probably produce frequent intrusion responses. If the suspicious valid activities exceed certain amount, the security system will deny the access of these operations and even destroy software and hardware devices. (3)Security threats from autoimmunity This kind of security problems are complex, there are many different reasons for these problems and the symptom of these security problems vary greatly. The essential part in security system is the negative selection algorithm, and the self-matching unit in the algorithm is also essential in detector selecting. If self properties are incomplete in the self library, many detectors with self antibody will be released for duplicating. These abnormal detectors have mistaken matching mechanisms with normal activities and valid operation. They will accept attack or invalid operation, while identify valid operating as dangerous ones. Just like self- destroying in biological immune system, the security system will deny normal operation and even take killing actions on system software and hardware [17-20]. To solve the above security problems and system flaws, we can introduce other artificial intelligent methods into AIS, such as evolutionary algorithms. With the intelligent optimizing method in evolutionary algorithms, we can improve the selection of detectors and avoid the problem of immunodeficiency and autoimmunity. In the meantime, biological treatment of immune pathology can also be an approach to avoid similar security problems and system flaws in artificial immune system. For example, medicine interfering is an effective method in immune treatment; similarly, in artificial immune system, we can also adjust the system operating and parameter selecting to improve the efficiency and preciseness of the system.

II. ADAPTIVE IMMUNE LEARNING MODEL

A. Tri-tier Immune Model of Artificial Immune System

The adaptive immune tier is the second tier of the tri-tier immune model for the artificial immune system, and the first tier is the innate immune tier and the third tier is the parallel immune tier [25-27]. The innate immune tier is comprised of two modules. The first module is used to detect the selfs and the non-selfs in the system that the artificial immune system protects. The second module is used to recognize the features of known non-selfs and classify the types of the known worms. The adaptive immune tier is comprised of two modules. The first one is used to learn features and types of the unknown worms with the knowledge about all the known worms. The second is used to eliminate the non-selfs that were detected.

B. Model for Learning Unknown Worms

The model for learning unknown worms is comprised of the feature space of known worms, the algorithm for reading the features of non-selfs, the algorithm for searching the most similar non-self, the unknown worm that is being recognized, and the result set of learning. Model for learning unknown worms Algorithm for reading features of non-selfs Algorithm for searching the most similar non-self Unknown worm that is being recognized. For the unknown worm, dimension features among its features are measured, and the known features are represented but the other features are unknown.

In the process for learning the unknown worm, the non-self is classified into the type of the most similar known worm to the unknown one, according to the feature vector of the unknown worm. The types of known worms are known and the amount of the known worms is limited. However, the unknown worm cannot be classified into any type of known worms, and a new type must be created for the unknown one at that time. With creation of new type repeated, the types of unknown worms may be unlimited but numerable. The dimension coordinate of the feature space for the worms is represented with, small balls are used to denote the non-selfs, and the big circles represent the type of the worms.

III. ROBUSTNESS DEFINITION OF ARTIFICIAL IMMUNE SYSTEM

Up to now, the uniform definition on robustness of the artificial immune system has not been given. In order to analyze the robustness of the artificial immune system based on the normal model, it is necessary to define the robustness of the artificial immune system as such. In general, when a system has a parameter uncertainty with a definite scope or is dynamic without modeling to a certain extent, if the system still maintains some properties unchanged and keeps definite dynamic traits, then the system have the ability, which is called as robustness.

Definition 1 After the immune system is infected by foreign pathogen, the system can recuperate its health with its immune mechanism to keep it work in a normal pattern. Such trait of the system is called as robustness of the as non-selfs, the artificial immune system on the normal model can keep the self percent to 100%, the non-self percent to 0, some functions unchanged, and assure a definite dynamic immunity, by detecting selfs and non-selfs, recognizing the non-selfs and eliminating the non-selfs. Such ability of the system is called as robustness of the artificial immune system. Immune computation of the artificial immune system has robustness, and such robustness is maintained through maximizing the self percent and minimizing the non-self percent. Because normal artificial immune system has only selfs and no non-selfs, the goal of immune computation is to detect recognize and eliminate the non-selfs, and repair the selfs infected by the non-selfs.

Definition 3 In the artificial immune system, the set of robustness criterions is the condition set for maximizing the self percent of the system and minimizing the non-self percent of the system. According to the above definitions, the theorem of robustness criterion for the artificial immune system is proposed to analyze the robustness of the system.

Theorem 1 In mathematics, the criterion that the artificial immune system has robustness is the condition that the self percent for the system increases to 100% and the non-self percent decreases to 0.

[Proof] According to the statistic trait, when the artificial immune systems at different time points have same compositions of selfs and non-selfs, their self percents, their non-self percents and some functions for the systems are all same. Therefore, though some disturbance are caused by the non-selfs on the self percent, the non-self percent and some functional parameters, at the time point the self percent, the non-self percent and some functions of the artificial immune system S are same as the normal artificial immune system. At the time, the system maintains a definite trait of dynamic immunity, such as the dynamic traits of anti-virus, fault diagnosis and fall-over. According to definition 1, during the process of immune computation from the initial time to the time point, the artificial immune system has robustness. Thus, the problem for analyzing robustness of the artificial immune system can be extended into the problem for designing and maintaining robustness of the artificial immune system. The maximization of the selfs and the minimization of the non- selfs in the artificial immune system can be kept with the immune algorithms to make the artificial immune system robust.

A. Memory Cell Identification

The adaptive and evolutionary property of Genetic algorithms has been used to evolve the highly fit sister detectors activated when an anomaly has been encountered. The genetic operators – selection, cloning, crossover and mutation - have been used for this purpose. When an anomaly is encountered, the sister detectors activated as a result is called the set of "Activated Detectors", which are candidates for memory cells. Then, the genetic operator of selection is applied to determine which of these detectors should be cloned. The cloning threshold is set by the following formula:

Cloning Threshold = Sum of fitness of all the detectors / Total number of detectors

Those activated detectors having a fitness value greater than or equal to the cloning threshold undergo the cloning. The number of clones to be generated for the candidate detectors is determined by the following formula:

Number of Clones = Int{Fitness of detector*10 /Total Fitness}

Once the process of cloning is complete, the clones and the remaining activated detectors together form the set of "Winner Detectors". Subjecting these Winner Detectors to the genetic operators of Mutation and Crossover facilitates the evolution of these detectors. After a substantial number of generations, the detector with fitness value greater than all the Winner Detectors is treated as a "Memory Cell".

IV. METHODOLOGY

In this research, an intelligent decision support system is proposed. The architecture of the proposed decision support system comprises four components in this system: two databases and two subsystems for planning. The historical database record previous data and other related statistics and the reserved database record the particular events that are reserved. The planning subsystem is the intelligent mechanism. In the research, AIS is adopted. Once the instructions are received, the planning subsystem will get data from the historical database and reserved databases then perform AIS heuristic algorithm to plan the events and evaluate the quality of the outcomes. When the given "stop" criterion is satisfied, this subsystem will output the planned output and corresponding evaluation data to the decision support subsystem. The decision support subsystem provides a adjustment tool for the user. It will provide information such as the number of constraint violations to assist the users to modify the parameters of decision support system. Besides, through this subsystem, users can save a dataset that they accept at the historical event database or the changes that particular event exhibit at the reserved event database. The core technology of this system is AIS, which is inspired by theoretical immunology, as well as observed immune functions, principles and mechanisms in order to solve problems in [2, 9]. The AIS makes use of designing a shape- space to represent the application domain, then defining an affinity measuring mechanism to evaluate the interactions among these elements, and then using the immune algorithms to find the approximation of its optimum solution. There are many immune algorithms in AIS, each of which is suitable for certain domains. In this research, we choose the CLONALG and aiNet, which were proposed by de Castro, and they are suitable to perform tasks such as machine learning, pattern recognition, and optimization.

The algorithm works as follows [4]:

1. Generate a set of N candidate solutions randomly;
2. Select n highest affinity solutions according to affinity measures function;
3. Clone these n selected solutions, the number of copies is proportional to their affinities;
4. Mutate these n selected solutions with a rate inversely proportional to their affinities;
5. Re-select m highest affinity mutated solutions to compose the new repertoire;
6. Replace some low affinity solutions by new ones;
7. Determine the similarity between each pair of solutions;
8. Eliminate all solutions whose affinity is less than a pre- specified threshold;
9. Save the best solution which has highest affinity so far;
10. Repeat step 2 to 9 until a given stopping criterion is met.

A normal model is built with the space-time properties of each component in the system to identify the normal state of the artificial immune system uniquely. With the normal model, the artificial immune system has many advantages in detecting the selfs and the non-selfs, eliminating the unknown non-selfs, and repairing the damaged system.

A. Normal Model of System with Space-Time Properties

In the four-dimension space that Einstein used to describe his relativity theory, the state of everything is identified by the space-time coordinates uniquely [9]. Inspired by the mapping relation, every component (B-cell, T-cell, or antibody etc.) in biological immune system is assumed to have unique spacetime properties, which are sure useful for uniquely identifying the normal state of the biological immune system. The space property is the DNA pattern of the component and the time property is the time state of the component. The capacity of bacterial DNA (CpG-DNA) for inducing APCs to differentiate into professional APCs is an interesting discovery [10]. The DNA pattern and the time state are useful for identifying the normal state of the immune system. Inspired by the biological immune system, the file-based object system, which the artificial immune system protects, consists of some files and directories, and the space property (the absolute pathname) and time property (the last revision time) uniquely identify each component in the system. Suppose a component of the object system S, which the artificial immune system protects, is represented as ci, the space property of the component ci is its absolute pathname pi, and the time property of the component ci is its last revision time ti, thus the space property is a space coordinate and the time property is a time coordinate. With the mapping relation from the physical space of the real world to the cyberspace on computers, the combined vector of the space coordinate and the time coordinate for each component is unique, and the vector of space-time properties is used to represent the state of the component. If and only if the states of all components of the system S are normal, the state of the system is normal [11].

Theorem 1 Suppose the time property is correct in the cyberspace, all files of the object system S are normal,

the function N(.) represents the normal function (if the parameter is normal, then the function s(.) represents the state of the object that the parameter denotes and the return of the function is 1; if the parameter is abnormal, then the return of the function is 0), then the set for the vectors of space-time properties for all the files {(pi, ti)|N(s(ci))=1, i=1, 2, …, n} uniquely identifies the normal state s(S) (N(s(S))=1) of the system S [12]. With the normal model of the object system S, all the selfs become known and the process for detecting the selfs is much easier than that for detecting the non-selfs.

B. Unknown non-self Detection of AIS with Normal Model

For human beings, detection of an unknown object is not easy and sometimes causes cognitive errors, but if the selfs are known, discrimination of the unknown object from the selfs becomes easier. Due to known complexity of the non-selfs, the feature set of the non-selfs is unlimited in theory and is not enough for the criterions for detecting unknown non-selfs. However, many non-self detecting techniques such as virus detecting, abnormity detecting and fault detecting are based on matching the features of the non-selfs, and the probability for detecting the non-self is quite limited. In fact, any unknown non-selfs such as viruses and faults may cause fatal lost in the application system, so that many problems such as anti-virus security, fault diagnosis and robust control, push the non-self detecting techniques to improve thoughts & methods. The core problem is how to identify the normal object system uniquely in cyberspace, and in the real world the space-time coordinates uniquely identify the object that may be a system. For designers and users, many computer systems are more knowable and easier to control than the non-selfs, so that the selfs for the computer system should be used to the utmost. In nature, designers should know whether the system is normal or abnormal, and the advantage of the normal model is to identify the normal state of the object system with the spacetime properties of the selfs. With the file-based object system protected by the AIS, the algorithm for building the normal model is designed.

Step 1. Backup the system and initialize the set of selfs.
Step 2. Read from the root of the system to find files.
Step 3. If there is at least an unread file or directory in the current directory, then read the pathname and last revision time of the current file or directory; otherwise go to step 6.
Step 4. Add the space-time properties of the file or directory into the set of selfs.
Step 5. For sub-directory, build the normal model of the sub-system at the sub-directory recursively.
Step 6. If all the files and directories of the system are processed, then end the algorithm; otherwise go to step 3.

The time complexity of the algorithm for building the normal model is O(n+m). Here, n represents the sum of files in the normal system, and m represents the sum of directories in the normal system. With the normal model, the algorithm for detecting the selfs and the non-selfs is designed as such.

Step 1. Read from the root of the system to find files.
Step 2. If there is at least an unread file or directory in the current directory, then read the pathname and last revision time of the current file or directory; otherwise go to step 6.
Step 3. Query in the self database with the space-time properties of the file or directory.
Step 4. If a record is matched, then the file or directory is a
self; otherwise the file or directory is a non-self, and the nonself is recognized by the algorithms for recognizing the nonselfs.
Step 5. For sub-directory, detect each component of the sub- system at the sub-directory recursively.
Step 6. If all the files and directories of the system are processed, then end the algorithm; otherwise go to step 2. The time complexity of the algorithm for building the normal model is O((k+l)(m+n)). Here, k represents the sum of files in the current system, and l represents the sum of directories in the current system.

Theorem 2 On the condition that the time property is correct in the cyberspace, detecting the selfs and the non-selfs with the normal model of the object system, the probability for detecting the selfs is 1 and the probability for detecting the non-selfs is also 1 [12]. The time property depends on the timing mechanism of the operation systems, and should be the same with the time meaning in the real world. For an anti-worm system, the probability for detecting the non-selfs, the artificial immune system is normal before the worms attack the system, so that the normal model is very useful for detecting all the non-selfs. Afterwards, some worms infect the artificial immune system and damage the storage of the normal model afterwards. The normal model is not good enough to detect all the non-selfs and the artificial immune system begins to repair itself. After repairing, the artificial immune system starts to detect all the non-selfs with the normal model and eliminate all the non-self in the end. According to the comparison between the two approaches for detecting

the non-selfs, the normal model is very necessary and important for detecting the non-selfs, even though the normal model is not enough for detecting all the non-selfs when the artificial immune system itself is damaged.

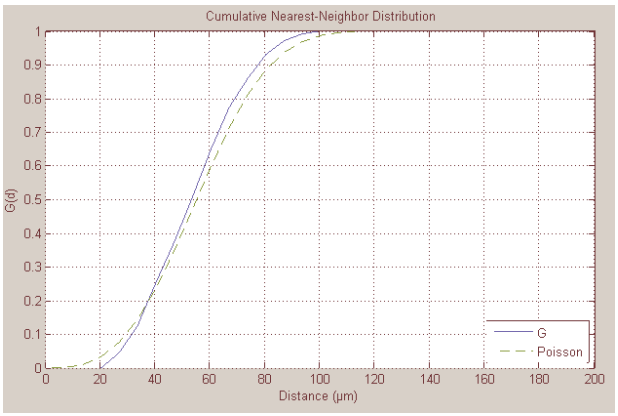

Fig 1. G Function (Cumulative Nearest Neighbor Distribution)

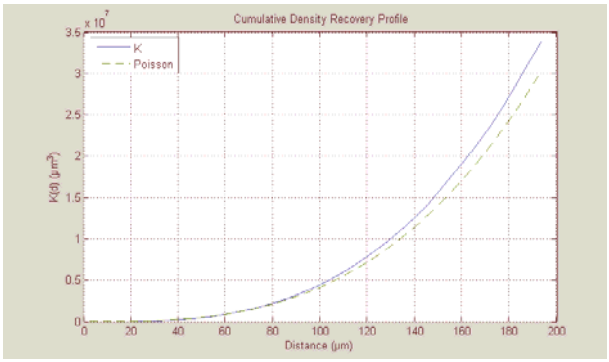

Fig 2. K Function (Cumulative Density)

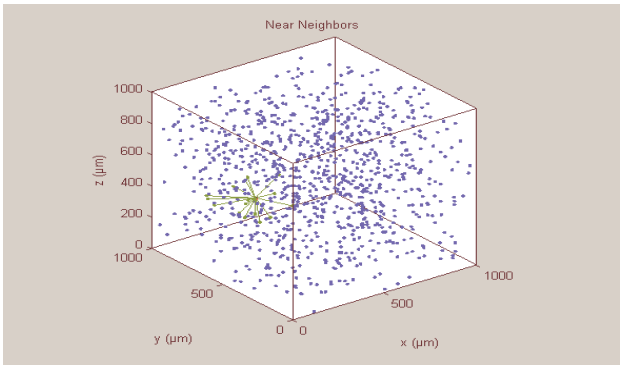

Fig 3. Near Neighbors

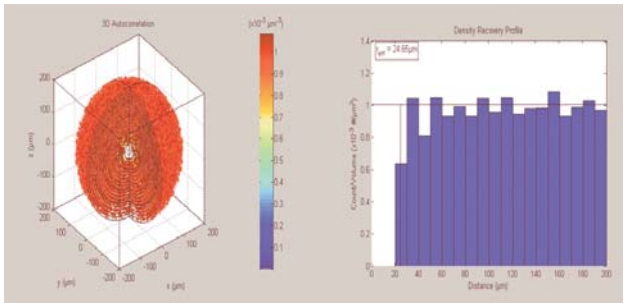

Fig 4. Three Dimension Autocorrelation and Histogram

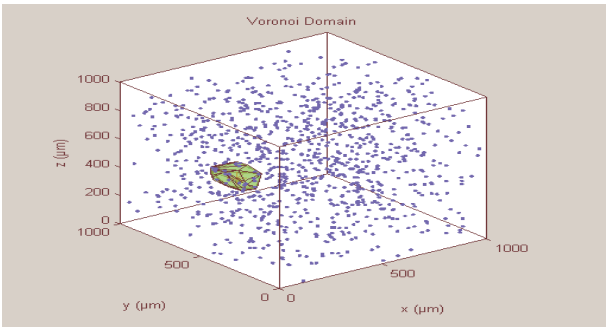

Fig 5. Voronio Domain

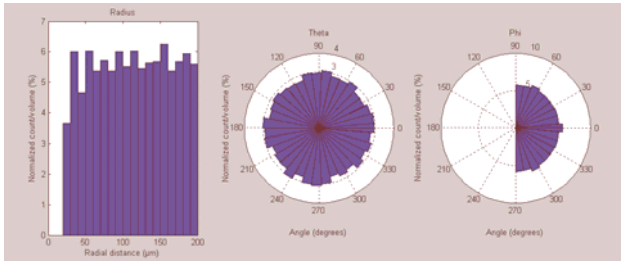

Fig 6. Autocorrelation Histogram

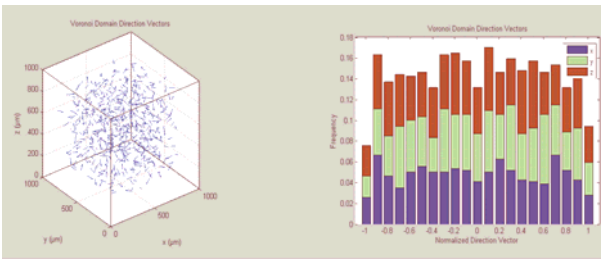

Fig 7. Voronio Domain Director Vector and Histogram

AUTHOR AND AFFILIATIONS

Dr Akash Singh is working with IBM Corporation as an IT Architect and has been designing Mission Critical System and Service Solutions. He has published

papers in IEEE and other International Conferences and Journals.

He joined IBM in July 2003 as a IT Architect which conducts research and design of High Performance Smart Grid Services and Systems and design mission critical architecture for High Performance Computing Platform and Computational Intelligence and High Speed Communication systems. He is a Senior Member of IEEE (Institute for Electrical and Electronics Engineers), the AAAI (Association for the Advancement of Artificial Intelligence) and the AACR (American Association for Cancer Research). He is the recipient of numerous awards from W orld Congress in Computer Science, Computer Engineering and Applied Computing 2010, 2011, and IP Multimedia System 2008 and Billing and Roaming 2008. He is active research in the field of Artificial Intelligence and advancement in Medical Systems. He is in Industry for 18 Years where he performed various role to provide the Leadership in Information Technology and Cutting edge Technology.

REFERENCES

[1] Dynamics and Control of Large Electric Power Systems. Ilic, M. and Zaborszky, J. John Wiley & Sons, Inc. © 2000, p. 756.

[2] Modeling and Evaluation of Intrusion Tolerant Systems Based on Dynamic Diversity Backups. Meng, K. et al. Proceedings of the 2009 International Symposium on Information Processing (ISIP'09). Huangshan, P. R. China, August 21-23, 2009, pp. 101–104

[3] Characterizing Intrusion Tolerant Systems Using A State Transition Model. Gong, F. et al., April 24, 2010.

[4] Energy Assurance Daily, September 27, 2007. U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability, Infrastructure Security and Energy Restoration Division. April 25, 2010.

[5] CENTIBOTS Large Scale Robot Teams. Konoledge, Kurt et al. Artificial Intelligence Center, SRI International, Menlo Park, CA 2003.

[6] Handling Communication Restrictions and Team Formation in Congestion Games, Agogino, A. and Tumer, K. Journal of Autonomous Agents and Multi Agent Systems, 13(1):97–115, 2006.

[7] Robotics and Autonomous Systems Research, School of Mechanical, Industrial and Manufacturing Engineering, College of Engineering, Oregon State University

[8] D. Dietrich, D. Bruckner, G. Zucker, and P. Palensky, "Communication and computation in buildings: A short introduction and overview," IEEE Trans. Ind. Electron., vol. 57, no. 11, pp. 3577–3584, Nov. 2010.

[9] V. C. Gungor and F. C. Lambert, "A survey on communication networks for electric system automation," Comput. Networks, vol. 50, pp. 877–897, May 2006.

[10] S. Paudyal, C. Canizares, and K. Bhattacharya, "Optimal operation of distribution feeders in smart grids," IEEE Trans. Ind. Electron., vol. 58, no. 10, pp. 4495–4503, Oct. 2011.

[11] D. M. Laverty, D. J. Morrow, R. Best, and P. A. Crossley, "Telecommunications for smart grid: Backhaul solutions for the distribution network," in Proc. IEEE Power and Energy Society General Meeting, Jul. 25–29, 2010, pp. 1–6.

[12] L. Wenpeng, D. Sharp, and S. Lancashire, "Smart grid communication network capacity planning for power utilities," in Proc. IEEE PES, Transmission Distrib. Conf. Expo., Apr. 19–22, 2010, pp. 1–4.

[13] Y. Peizhong, A. Iwayemi, and C. Zhou, "Developing ZigBee deployment guideline under WiFi interference for smart grid applications," IEEE Trans. Smart Grid, vol. 2, no. 1, pp. 110–120, Mar. 2011.

[14] C. Gezer and C. Buratti, "A ZigBee smart energy implementation for energy efficient buildings," in Proc. IEEE 73rd Veh. Technol. Conf. (VTC Spring), May 15–18, 2011, pp. 1–5.

[15] R. P. Lewis, P. Igic, and Z. Zhongfu, "Assessment of communication methods for smart electricity metering in the U.K.," in Proc. IEEE PES/IAS Conf. Sustainable Alternative Energy (SAE), Sep. 2009, pp. 1–4.

[16] A. Yarali, "Wireless mesh networking technology for commercial and industrial customers," in Proc. Elect. Comput. Eng., CCECE,May 1–4, 2008, pp. 000047–000052.

[17] M. Y. Zhai, "Transmission characteristics of low-voltage distribution networks in China under the smart grids environment," IEEE Trans. Power Delivery, vol. 26, no. 1, pp. 173–180, Jan. 2011.

[18] V. Paruchuri, A. Durresi, and M. Ramesh, "Securing powerline communications," in Proc. IEEE Int. Symp. Power Line Commun. Appl., (ISPLC), Apr. 2–4, 2008, pp. 64–69.

[19] Q.Yang, J. A. Barria, and T. C. Green, "Communication infrastructures for distributed control of power distribution networks," IEEE Trans. Ind. Inform., vol. 7, no. 2, pp. 316–327, May 2011.

[20] T. Sauter and M. Lobashov, "End-to-end communication architecture for smart grids," IEEE Trans. Ind. Electron., vol. 58, no. 4, pp. 1218–1228, Apr. 2011.

[21] K. Moslehi and R. Kumar, "Smart grid—A reliability perspective," Innovative Smart Grid Technologies (ISGT), pp. 1–8, Jan. 19–21, 2010.

[22] Southern Company Services, Inc., "Comments request for information on smart grid communications requirements," Jul. 2010

[23] R. Bo and F. Li, "Probabilistic LMP forecasting considering load uncertainty," IEEE Trans. Power Syst., vol. 24, pp. 1279–1289, Aug. 2009. [24] Power Line Communications, H. Ferreira, L. Lampe, J. Newbury, and T. Swart (Editors), Eds. New York: Wiley, 2010.

[25] G. Bumiller, "Single frequency network technology for fast ad hoc communication networks over power lines," WiKu-Wissenschaftsverlag Dr. Stein 2010.

[31] G. Bumiller, L. Lampe, and H. Hrasnica, "Power line communications for large-scale control and automation systems," IEEE Commun. Mag., vol. 48, no. 4, pp. 106–113, Apr. 2010.

[32] M. Biagi and L. Lampe, "Location assisted routing techniques for power line communication in smart grids," in Proc. IEEE Int. Conf. Smart Grid Commun., 2010, pp. 274–278.

[33] J. Sanchez, P. Ruiz, and R. Marin-Perez, "Beacon-less geographic routing made partical: Challenges, design guidelines and protocols," IEEE Commun. Mag., vol. 47, no. 8, pp. 85–91, Aug. 2009.

[34] N. Bressan, L. Bazzaco, N. Bui, P. Casari, L. Vangelista, and M. Zorzi, "The deployment of a smart monitoring system using wireless sensors and actuators networks," in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), 2010, pp. 49–54.

[35] S. Dawson-Haggerty, A. Tavakoli, and D. Culler, "Hydro: A hybrid routing protocol for low-power and lossy networks," in Proc. IEEE Int. Conf. Smart Grid Commun. (SmartGridComm), 2010, pp. 268–273.

[36] S. Goldfisher and S. J. Tanabe, "IEEE 1901 access system: An overview of its uniqueness and motivation," IEEE Commun. Mag., vol. 48, no. 10, pp. 150–157, Oct. 2010.

[37] V. C. Gungor, D. Sahin, T. Kocak, and S. Ergüt, "Smart grid communications and networking," Türk Telekom, Tech. Rep. 11316-01, Apr 2011.