Enhancing the QoS of Sensor Nodes through Advance Pattern Detection Technique

Aarti Kumari[1], Neha Shrivastava[2], Nitin Kali Raman[3]
[1]M. Tech. (ECE), [2,3]Asst. Professor (Dept. of ECE)
DPG Institute of Technology & Management, Gurugram, Haryana

Abstract **-** The history of sensor network technology originates in the first distributed sensing idea implementations. The continuous work of researchers and engineers over sensor networks which lately became wireless sensor networks (WSNs). Wireless sensor network is one of the growing technology for sensing and performing the different tasks. Such networks are beneficial in many fields, such as emergencies, health monitoring, environmental control, military, industries and these networks prone to malicious users' and physical attacks due to radio range of network, un-trusted transmission, unattended nature and get access easily. We have compared the results of back-propagation technique with Hop-field neural network. The comparison shows that results of hop-field are better than the back propagation. Here, the packet delivery ratio and through-put are increased and end-to-end delay is decreased. This thesis also explores solutions to efficiently recover collisions in WSNs. In future neuro-fuzzy and fuzzy applications can be apply to avoid the collision using these parameters.

Keywords **-** wireless sensor networks, packet delivery ratio, throughput, end-to-end delay

I. INTRODUCTION

Wireless sensor networks consist of individual nodes that are able to interact with the environment by sensing or controlling physical parameters. These nodes have to collaborate to fulfill their tasks. The nodes are interlinked together and by using wireless links each node A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that is able to communicate and collaborate with each other collaborate in order to achieve a common goal. Sensor nodes operate in hostile environments such as battle fields and surveillance zones. Due to their operating nature, WSNs are often unattended, hence prone to several kinds of novel attacks. WSNs have attracted a lot of attention recently due to their broad applications in both military and civilian operations. Many WSNs are deployed in unattended and often hostile environments such as military and homeland security operations. Therefore, security mechanisms providing congeniality, authentication, data integrity, and non-repudiation, among other security objectives, are vital to ensure proper network operations.

A. Sensor nodes - Sensor nodes are the network components that will be sensing and delivering the data. Depending on the routing algorithms used, sensor nodes will initiate transmission according to measures and/or a query originated from the Task Manager. According to the system application requirements, nodes may do some computations. After computations, it can pass its data to its neighboring nodes or simply pass the data as it is to the Task Manager. The sensor node can act as a source or sink/actuator in the sensor field. The definition of a source is to sense and deliver the desired information.

Hence, a source reports the state of the environment. On the other hand, a sink/actuator is a node that is interested in some information a sensor in the network might be able to deliver.

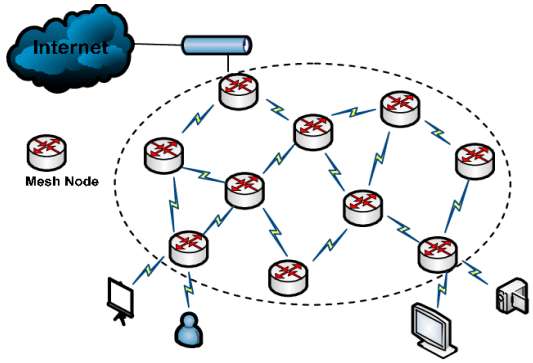

Figure 1**:** Illustration of sensor network and backbone infrastructure.

B. System Components and Operations in a Wireless Sensor Network -

i). Communication Architecture: In this section, we will explore the left black box in Figure 1, i.e. the sensor field. The components and operations between sensor nodes within the sensor field would be explored. We first describe the wireless sensor network architecture and the communication protocols for the wireless sensor network. This is essential to understand the hardware and software level power savings strategies. One of the intension of this report is to provide a survey of the sensor nodes in literature and recommend the appropriate hardware based on the specific application. We can refer to [4-7] for more information in the detail composite of the hardware.

ii). Sensor Node: As mentioned earlier, the sensor field constitutes sensor nodes. Typically, a sensor node can perform tasks like computation of data, storage of data, communication of data and sensing/actuation of data. A basic sensor node typically comprises of five main components and they are namely controller, memory, sensors and actuators, communication device and power supply (see Figure 2). A controller is to process all the

relevant data, capable of executing arbitrary code. Memory is used to store programs and intermediate data. Sensors and actuators are the actual interface to the physical world. These devices observe or control physical parameters of the environment. The communication device sends and receives information over a wireless channel. And finally, the power supply is necessary to provide energy. In wireless sensor networks, power consumption efficiency is one of the most important design considerations. Therefore, these intertwined components have to operate and balance the trade-offs between as small energy consumption as possible and also the need to fulfill their tasks.

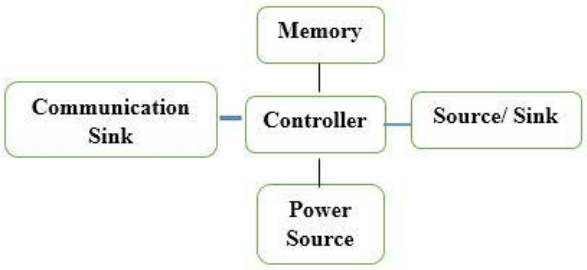

Figure 2: Overview of sensor node hardware component.

II. BACKGROUND

Xu, Q., et al. (2018) investigates twin attractors in a two-neuron- based non-autonomous Hopfield neural network (HNN) through numerical analyses and hardware experiments. Stability analysis of the DC equilibrium point is executed and an unstable saddle-focus is found in the parameter region of interest. The stimulus-associated dynamical behaviors are numerically explored by bifurcation diagrams and dynamical map in two-dimensional parameter-space, from which coexisting twin attractor's behavior can be observed with the variations of two stimulus-associated parameters. Moreover, breadboard experiment investigations are carried out, which effectively verify the numerical simulations.

Rebentrost, P., *et al.* (2018). Quantum computing allows for the potential of significant advancements in both the speed and the capacity of widely used machine learning techniques. Here they employ quantum algorithms for the Hopfield network, which can be used for pattern recognition, reconstruction, and optimization as a realization of a content-addressable memory system. They show that an exponentially large network can be stored in a polynomial number of quantum bits by encoding the network into the amplitudes of quantum states. By introducing a classical technique for operating the Hopfield network, they can leverage quantum algorithms to obtain a quantum computational complexity that is logarithmic in the dimension of the data. They also present an application of our method as a genetic sequence recognizer.

Bao, B., *et al.* (2017) present simplifying connection topology of Hopfield neural network (HNN) with three neurons, a kind of HNN-based nonlinear system is proposed. Taking a coupling-connection weight as unique adjusting parameter and utilizing conventional dynamical analysis methods, dynamical behaviors with the variation of the adjusting parameter are discussed and coexisting multiple attractors' behavior under different state initial values are investigated. The results imply that the HNN-based system displays point, periodic, and chaotic behaviors as well as period-doubling and tangent bifurcation routes; particularly, this system exhibits some striking phenomena of coexisting multiple attractors, such as, a pair of single-scroll chaotic attractors accompanied with a pair of periodic attractors, a pair of periodic attractors with two periodicities, and so on. Of particular interest, it should be highly significant that a hardware circuit of the HNN-based system is developed by using commercially available electronic components and many kinds of coexisting multiple attractors are captured from the hardware experiments. The results of the experimental measurements have well consistency to those of MATLAB and P-Spice simulations.

Yang, J., *et al.* (2017) Memristor is a nanoscale electronic device that exhibits the synaptic characteristics in artificial neural network. Some valuable memristor-based synaptic circuits have been presented. However, the circuitry implementations of some simple neural network are still rarely involved before. This paper contributes to construct a novel memristive Hopfield neural network circuit. On one hand, an improved memristor bridge circuit is employed to realize synaptic operation which better performs zero, positive and negative synaptic weights without requiring any switches and inverters, and P-spice implementation scheme is also considered. On the other hand, the proposed bridge circuit greatly simplifies the structure of neural network, and reduces the conversion process between current and voltage signal. Furthermore, the associative memory in binary and color images is demonstrated on the basis of the proposed memristive network. A series of numerical simulations are designed to verify associative memory capability, and experimental results demonstrate the effectiveness of the proposed neural network via the cases of single-associative memory and multi-associative memory.

Patel (2017) Wireless Sensor Network (WSN) is a small wireless sensor nodes wireless network. Sensors are used to monitor physical or environmental conditions. Wireless sensor networks are especially used in military and civilian applications. Since the wireless sensor network is generally posted in unsafe areas because they are dangerous for different types of attacks. One of the harmful attacks is cyber-attack, in which a node claims to illegally identify multiple. In this case, legal node will share the data in an awful node and the data will be lost. Therefore, such attacks require network protection. This paper has to study, discuss and analyze various techniques to detect cyber-attacks in wireless sensor networks. Various protocols that were affected by cyber-attacks were also studied and analyzed.

Cabeza, R. T., *et al.* (2016) Most of the existing artificial neural network models use a significant amount of information for their training. The need for such information could be an inconvenience for its application in fault diagnosis in industrial systems, where the information, due

to different factors such as data losses in the data acquisition systems, is scarce or not verified. In this chapter, a diagnostic system based on a Hopfield neural network is proposed to overcome this inconvenience. The proposal is tested using the development and application of methods for the actuator diagnostic in industrial control systems (DAMADICS) benchmark, with successful performance.

Duan, S., *et al.* (2016) present novel systematic design of associative memory networks is addressed in this paper, by incorporating both the biological small-world effect and the recently acclaimed memristor into the conventional Hopfield neural network. More specifically, the original fully connected Hopfield network is diluted by considering the small-world effect, based on a preferential connection removal criteria, i.e., weight salience priority. The generated sparse network exhibits comparable performance in associative memory but with much less connections. Furthermore, a hardware implementation scheme of the small world Hopfield network is proposed using the experimental threshold adaptive memristor (TEAM) synaptic-based circuits. Finally, performance of the proposed network is validated by illustrative examples of digit recognition.

Singh (2016) has developed several protocols for wireless sensor networks. Most of them have the same capabilities similar to the network, every node has the same capabilities of the same processing power, storage, energy and the same. In real situations, nodes are different processing time, storage and energy values. In this way, the performance is set to be recognized as a diffused Wireless Sensor Network (H-WSN) routing protocol. WSN nodes in two modes, i.e., advanced nodes (high energy) and in the normal node. The node battery does not drain until the sensor works the network. In addition, once the battery will be deployed nodes for some harsh environment, it is hard to fill battery nodes. In this article, it is that the Leach's, Fair and SEP three massively accepted WSN routing protocols have been presented against their energy patterns in the diffused scene. The initial features of the initially randomized energy-based weapons are introduced to Center Noodle. All simulations are done in the obligation. Various parameters are used to use the utility of the H-WSN routing protocol. The simulation results show that there is no clear winner for all matters, but in most cases, leach protocols on comparison Fair SEP and better results, such as round reduction dead nodes, and base-up packet transmission rate and cluster head increase provides .

III. PROPOSED ALGORITHM

Create a network having 18 node arranged in circular fashion.
Select source and destination and the sensor node from the nodes.
While(data is not received by destination)
repeat
If(sensor node detect collision)
Then
Apply pattern recognition neural network to change the position of the node at which collision is detected.
And start transmission from source node again.
Else
Transmit the data from one node to another.
End if
End while
Exit

IV. RESULT AND DISCUSSION

The performance of each classifier in terms of packet delivery ratio, end2end delay, and throughput was compared. For better understanding of results comparison, we introduce these criteria.

Packet delivery ratio- It expresses the ratio of the total number of publication messages received by each subscriber node, up to the total number of publication messages generated by all publisher nodes of the events to which the subscriber node has subscribed.

It can be calculated by the following formula:

PDR= ((total packets-loss)/total packets)*100.

a) End2End Delay- The delay of a packet in a network is the time it takes the packet to reach the destination after it leaves the source.

b) Throughput – Throughput is the number of packet that is passing through the channel in a particular a unit of time. This performance metric show the total number of packets that have been successfully delivered from source node to destination node and it can be improved with increasing node density.

The amount of samples generated by the network as response to a given query is equal to the number of sensors, k, that are present and active when the query is received.

It can be calculated by the following formula:

Throughput=total packets/End2EndDelay

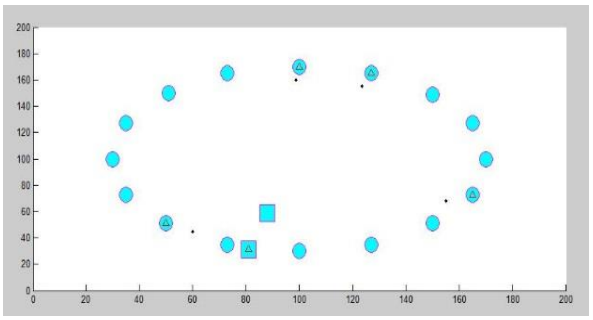

Figure 3: Simulation of WSN

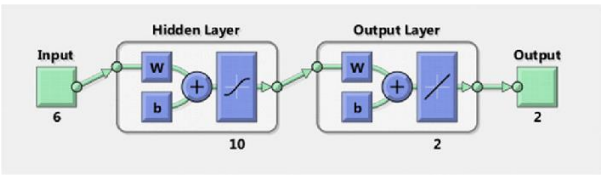

Figure 4: Neural network execution

Result: Command Prompt
Packet Transmitted = 170
Packet Drop = 6.000
PDR= 9.99e+03
E2edelay= 0.172
Throughput= 989.145

Figure 5: Output PDR, e2e Delay, and Throughput

V. CONCLUSION AND FUTURE WORK

Wireless sensor networks (WSNs) are innovative large-scale wireless networks that consist of distributed, autonomous, low-power, low-cost, small-size devices using sensors to cooperatively collect information through infra-structure-less ad-hoc wireless network. The development of wireless sensor networks was originally motivated by military applications such as battlefield surveillance. However, wireless sensor networks are now used in many civilian application areas, including environment and habitat monitoring, healthcare applications, home automation, and traffic control. Security plays a fundamental role in many wireless sensor network applications. Because sensor networks pose unique challenges, security techniques used in conventional networks cannot be directly applied to WSNs because of its unique characteristics. First, sensor nodes are very sensitive of production cost since sensor networks consist of a large number of sensor nodes argued that the cost of a sensor node should be much less than one dollar in order for sensor networks to be feasible. Therefore, most sensor nodes are resource restrained in terms of energy, memory, computation, and communication capabilities. Normally sensor nodes are powered by batteries, and recharging batteries are infeasible in many circumstances. Energy consumption becomes a key consideration for most sensor network protocols. Second, Sensor nodes may be deployed in public hostile locations, which make sensor nodes vulnerable to physical attacks by adversaries. Generally, adversaries are assumed to be able to undetectably take control of a sensor node and extract all secret data in the node. Furthermore, the scale of sensor networks is considerably large, and the network topology is dynamically adjusted, because some nodes may die out of running out of energy or failure, and new nodes may join the network to maintain desirable functionality. At last, sensor networks use insecure wireless communication channel and lack infrastructure. As a result, existing security mechanisms are inadequate, and new approaches are desired. Since large number of sensor nodes are densely deployed, neighbor nodes may be very close to each other. Hence, multi hop communication in sensor networks is expected to consume less power than the traditional single hop communication. Furthermore, the transmission power levels can be kept low, which is highly desired in covert operations.

VI. REFERENCES

[1]. Akyildiz, W. Su, Y. Sankarasubramanian, E. Cayirci, "A Survey on Sensor Networks", IEEE Communications Magazines, August 2002.

[2]. Y. Hu, A. Perrig, and D. Johnson, "Wormhole detection in wireless ad hoc networks," 2002. [Online]. Available: citeseer. ist.psu.edu/hu02wormhole.html

[3]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures" Ad Hoc Networks, vol. 1, no. 2, 2003

[4]. Blackert, W.J., Gregg, D.M., Castner, A.K., Kyle, E.M., Hom, R.L., and Jokerst, R.M., "Analyzing interaction between distributed denial of service attacks and mitigation technologies", Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24 April, 2003, pp. 26 – 3.

[5]. P fleeger, C. P. and P fleeger, S. L., "Security in Computing", 3rd edition, Prentice Hall 2003

[6]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and counter measures," Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, vol. 1, no. 2–3, pp. 293– 315, September 2003.

[7]. J. Suh, Mike Horton, "Powering sensor networks", Potentials, IEEE, August/September 2004.

[8]. K. L. Chee, P. K. Sivaprasad, S.V. Rao, J.G. Lim, "Clock Drift Reduction For Relative Time Slot TDMA Based Sensor Networks", Personal Indoor and Mobile Radio Communications, PIMRC 2004. 15th IEEE International Symposium, Pages: 1042 – 1047, Vol.2, 5-8 Sept. 2004.

[9]. M. Hempstead, N. Tripathi, P. Mauro, G. Y. Wei, David Brooks, "An UltraLow Power System Architecture for Sensor Network Applications", Intelligent Sensors, Sensor Networks and Information Processing Conference, Proceedings of the 2004 14-17 Dec. 2004, Pages: 13 – 18, 2004.

[10]. S. K. Jayaweera, "An Energy-efficient Virtual MIMO Communications Architecture Based on V-BLAST Processing for Distributed Wireless Sensor Networks", Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. First Annual IEEE Communications Society Conference, Pages: 299 – 308, October 2004

[11]. Wang, B-T. and Schulzrinne, H., "An IP trace back mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2-5 May 2004, pp. 901 – 904.

[12]. Culpepper, B.J. and Tseng, H.C., "Sinkhole intrusion indicators in DSR MANETs", Proc. First International Conference on Broad band Networks, 2004, pp. 681 – 688

[13]. John Paul Walters, Zhengqiang Liang, Weisong Shi, Vipin Chaudhary, "Wireless Sensor Network Security: A Survey", Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006

[14]. Tahir Naeem, Kok-Keong Loo, "Common Security Issues and Challenges in Wireless Sensor Networks" and IEEE 802.11 Wireless Mesh Networks, International Journal of Digital Content Technology and its Applications, Page 89-90 Volume 3, Number 1, year 2009

[15]. Sinchan Roy chowdhury, Chiranjib Patra," Geographic Adaptive Fidelity and Geographic Energy Aware Routing in Ad Hoc Routing", Special Issue of IJCCT Vol.1 Issue 2, 3, 4; 2010 for International Conference [ACCTA-2010], 3-5 August 2010.

[16]. Mauro Conti, Roberto Di Pietro,Luigi Vincenzo Mancini, and Alessandro Mei, "Distributed Detection of Clone Attacks in

Wireless Sensor Networks" IEEE Transaction on dependable & secure computing vol.8 n0.5 September 2011.

[17]. Cabeza, R. T., Viciedo, E. B., Prieto-Moreno, A., & Vega, V. M. (2016). Fault Diagnosis with Missing Data Based on Hopfield Neural Networks. In *Mathematical Modeling and Computational Intelligence in Engineering Applications* (pp. 37-46). Springer, Cham.

[18]. Duan, S., Dong, Z., Hu, X., Wang, L., & Li, H. (2016). Small-world Hopfield neural networks with weight salience priority and memristor synapses for digit recognition. *Neural Computing and Applications*, *27*(4), 837-844.

[19]. O. Singh, V. Rishiwal and M. Yadav, "Energy trends of routing protocols for H-WSN," *2016 2nd International Conference on Advances in Computing, Communication, & Automation (ICACCA) (Fall)*, Bareilly, 2016, pp. 1-4.

[20]. Bao, B., Qian, H., Wang, J., Xu, Q., Chen, M., Wu, H., & Yu, Y. (2017). Numerical analyses and experimental validations of coexisting multiple attractors in Hopfield neural network. *Nonlinear Dynamics*, *90*(4), 2359-2369.

[21]. S. T. Patel and N. H. Mistry, "A review: Sybil attack detection techniques in WSN," *2017 4th International Conference on Electronics and Communication Systems (ICECS)*, Coimbatore, 2017, pp. 184-188.

[22]. Xu, Q., Song, Z., Qian, H., Chen, M., Wu, P., & Bao, B. (2018). Numerical analyses and breadboard experiments of twin attractors in two-neuron-based non-autonomous Hopfield neural network. *The European Physical Journal Special Topics*, *227*(7-9), 777-786.

[23]. Rebentrost, P., Bromley, T. R., Weed brook, C., & Lloyd, S. (2018). Quantum Hopfield neural network. *Physical Review A*, *98*(4), 042308

[24]. V. Arnaudov, "Unified Management of Heterogeneous Sensor Networks In the Atlantis Framework", Department of Computer Science, Brown University.

[25]. M. Sims, C. Goldman, V. Lesser, "Self-Organization through Bottom-up coalition formation", University of Massachusetts.