Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.214 – 221

RESEARCH ARTICLE

Energy Efficient Neural Network Technique to Recover Collision in WSN

Jyotsna[1], Vikram Nandal[2]

[1]M.tech, CSE Dept., R.N College of Engineering & Management

[2]Assistant Professor, R.N College of Engineering & Management

[1] jyotsnasharma1989@gmail.com, [2] vikramcselive.com

Abstract: Wireless Sensor Networks (WSN) are highly distributed self-organized systems. The basic idea of sensor network is to disperse tiny sensing devices; which are capable of sensing some changes of incidents/parameters and communicating with other devices, spread over a specific geographic area for some specific purposes like environmental monitoring, surveillance, target tracking etc. By combining sensing technology with processing power and wireless communication makes it lucrative for being exploited in abundance in future. Wireless sensor networks are equipped with only Omni-directional antennas, which can cause high collisions. Packet collision causes packet loss and wastes resources in wireless networks. In this paper we are proposing an approach that avoids the collision using Hopfield neural network and increases the packet delivery ratio and throughput of the network.

Keywords: WSN, packet collision, Hopfield network

I. INTRODUCTION

In these days, wireless sensor network emerging as a promising and interesting area. Homogeneous and Heterogeneous nodes are used in wireless sensor network where a wireless medium is used by the nodes to communicate with each other. A hundred to thousands of nodes can be deployed in the sensing region to sense the environment. These nodes work cooperatively and send sensed information to the sink. A Wireless Sensor Network (WSN) is a collection of sensors with limited resources that collaborate in order to achieve a common goal. Sensor nodes operate in hostile environments such as battle fields and surveillance zones [1]. 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 nonrepudiation, among other security objectives, are vital to ensure proper network operations.

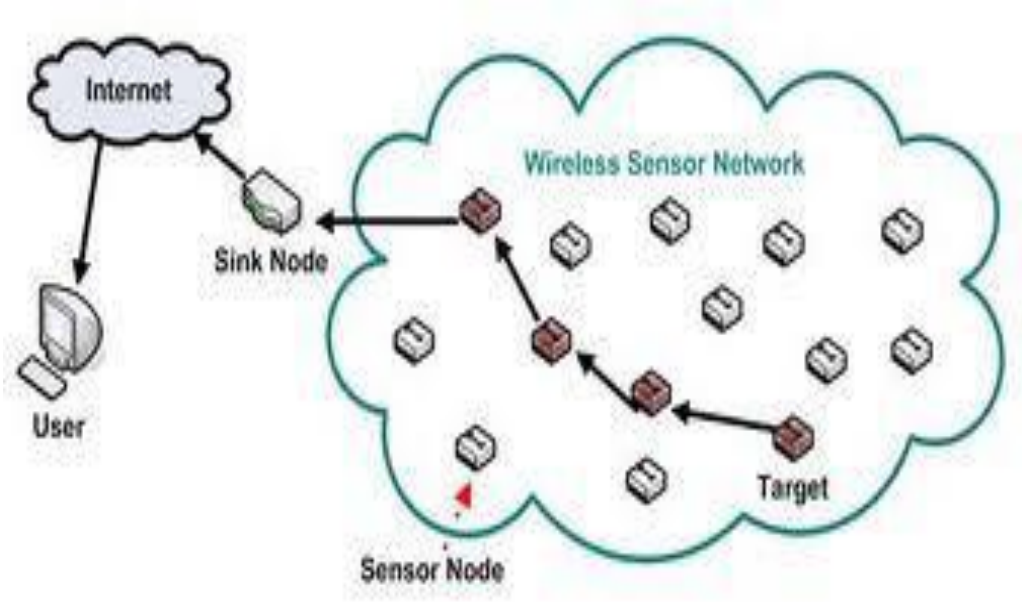

Fig 1. Basic Architecture of Wireless Sensor Network

Wireless sensor network can be categorized into two types:

1) Unstructured WSN- The nodes are densely deployed and also the nodes can be deployed in ad-hoc manner in the sensing area or region.
2) Structured WSN – Sensor node developments of some or all nodes are preplanned. The nodes placement is also planned.

As can be seen in figure 1usually sensor nodes are scattered in a sensor field, this is an area where the sensor nodes are deployed. Sensor nodes coordinate among themselves to produce high-quality information about the physical environment. Each of these scattered sensor nodes has the capability to collect and route data either to other sensors or back to an external BS(s). A BS may be a fixed or mobile node capable of connecting the sensor network to an existing communications infrastructure or to the internet where a user can have access to the reported data.

II. RELATED WORK

Frank Oldewurtel in 2005 proposed an overview of embedded network applications and discusses requirements arising from this analysis. Furthermore, they discussed selected in-network processing techniques and point out the analogy between neural and sensor networks. Phillip Reindl and Kendall Nygard, 2007 proposed "Defending Malicious Collision Attacks in Wireless Sensor Networks".[6]. They discussed that Security is an important issue for sensor networks deployed in hostile environments, such as military battlefields. The low cost requirement precludes the use of tamper resistant hardware on tiny sensor nodes. Hence, sensor nodes deployed in open areas can be compromised and used to carry out various attacks on the network. Raghavendra V. Kulkarni, in 2009 worked on "Neural Network Based Secure Media Access Control Protocol for Wireless Sensor Networks"[5]. This research discussed an application of a neural network in wireless sensor network security. It presents a neural network approach against the denial-of-service attacks launched by adversaries. The MLP enhances the security of a WSN by constantly monitoring the parameters that exhibit unusual variations in case of an attack/collision. Jiyong Son , Seoul and Hwan-JooKwak, in 2011 introduced "Back propagation neural network based real-time self-collision detection method"[4]. This research proposed a back propagation neural network based real-time humanoid self-collision detection method which eliminates the repetition of detection computation for same and similar motion sets. The proposed system is able to reduce self-collision detection computation time significantly, because of the

pattern recognition capability of the neural network. RishavDubey, Vikram Jain, Rohit Singh Thakur, SiddharthDuttChoubey in (2012) proposed "Attacks in Wireless Sensor Networks"[3]. WSN has limitations of system resources like battery power, communication range and processing capability. WSNs are used in many applications in military, ecological, and health-related areas. These applications often include the monitoring of sensitive information such as enemy movement on the battlefield or the location of personnel in a building. One of the major challenges wireless sensor networks face today is security, so there is the need for effective security mechanism.

III. COLLISION PROBLEM IN WSN

Collision occurs when two or more nodes attempt to transmit a packet across the network at the same time. The transmitted packets must be discarded and then retransmitted, thus the retransmission of those packets increases the energy consumption and the latency. Collision attack is a type of DOS attack which occurs on Data Link Layer. Packet Collision occurs when two or more close stations attempt to transmit a packet at the same time. This can result in packet loss and impede network performance. Many CSMA based MAC protocols are proposed in Wireless Sensor Network (WSNs) to avoid collisions, such as B-MAC [5]. These protocols can efficiently reduce collisions, but intrinsically cannot eliminate all collisions, because of hidden terminal problems, as well as collisions when multiple nodes sense the medium free at the same time. Furthermore, the consequences of packet collisions are serious to WSNs. Collisions can cause the loss of critical control information from base stations, and applications may fail.

Collision Attack: In the collision attack [2], the adversary sends his own signal when he hears that a legitimate node will transmit a message in order to make interferences. In theory, causing collisions in only one byte is enough to create a CRC error and to cripple the message. The advantages of a collision attack are the short power energy consumed and the difficulty to detect it (the only evidence of collisions attacks is incorrect message). In fact, such an attack can target specially the ACK control message causing an exponential back-off in some MAC protocol. According to attack attributes, first the intention of the collision attack is to exhaust the battery by using the channel of communication indefinitely. Then in the movement class, the attacker does not really need particular technical capabilities and it can be launched by anyone in the network, the vulnerability is the data integrity requirement and the layer used is the link layer. The target is general logical and can be at the same time against internal service like power management and against provided services, for example the communication service. Finally the result can be partial degradation if the attack is launched in certain region in the network or total degradation if the attack is applied in multiple precise locations in the network.

In next section, we have proposed a neural network approach using Hopfield networks to avoid collision in wireless sensor networks.

IV. COLLISION AVOIDANCE APPROACH

a. Role of Neural Network in WSN:

Although neural network and sensor network are normally viewed as two radically different subjects, they do share one thing in common. The most fundamental way of exchanging information in both kinds of networks is one-to-many communication, i.e., the broadcast. In a biological neural network, a firing neuron sends an action potential to all neurons that are connected to it by synapses, each of which may impose different delay and amplification to the transmitted signal. Similarly, a communication node in a sensor network broadcasts its signal to all nodes within its transmission range. The proposed computing with time paradigm applies to networks in which a broadcast is a Communication primitive, such as neural networks in biology or wireless networks in telecommunication. Another example of such a paradigm is computing with action potentials proposed by Hopfield et al. [7], who observed that

analog information can be encoded into firing times of action potentials and that the timings of these action potentials can be used to carry out a vector matching algorithm. The ability to perform broadcast-based communication was not explicitly mentioned as a requirement. There must be certain moments at which distributed neurons observe the same events, as if each of them would own a local clock and these clocks were synchronized from time to time by such events. Broadcast naturally provides plenty of such synchronization points. The purpose is to look for an optimum value by associating the firing times with a certain variable in such a way that the smaller this variable is the more desirable the property of the corresponding neuron is. Hence, the neuron firing earliest will naturally be the one whose property variable has the minimum value among the neurons being compared. Hence, the essence here is to introduce competition, instead of superposition in Hopfield's approach, to select a winner that possesses the desired optimality.

b. Hopfield Neural Network:

The Hopfield neural network is a simple artificial network which is able to store certain memories or patterns. Hopfield neural network model is a fully interconnected network of binary units with symmetric connection weights between the units. The nodes in the network are vast simplifications of real neurons - they can only exist in one of two possible states - firing or not firing. At any instant of time a node will change its state depending on the inputs it receives from itself and the other nodes. The dynamics of the Hopfield network can be described formally in mathematical terms. The activation levels of binary units are set to zero and one for "off" and "on," respectively. Starting from some initial configuration (V0,V1,V2…Vi) where is number of units and is the activation level of unit. The behavior of network is determined by an appropriate energy function. This function is based on neuron states, weights and bias value derived from problem data. Update rule of neurons is defined based on energy function [8]. HN shows promising characteristics such as associative memory, robustness and error correction capability to overcome this drawback [9-11]. Associative memory means that a pattern is not stored on any individual neuron but is a property of the whole network. Thus, the weights within the HN store the average correlations between all pattern components across all patterns. The network presented with a partial or corrupted pattern can then use the correlations to recreate the entire pattern. The HN itself is robust since it performs pattern completion in case of missing data and pattern correction in case of corrupted data due to the association ability. The HN is a single layer fully connected feedback network with no direct feedback connections, i.e. each single neuron is not directly connected to itself. Furthermore, it shows symmetric (bidirectional) weights, i.e. the weights between all single neurons are equal in either direction. Figure 2 depicts the HN, which is presented with the sensor input pattern containing readings of three sensors. After iterative processing the optimized, i.e. completed or corrected pattern can be used to build a data packet, which is represented by the dashed box.

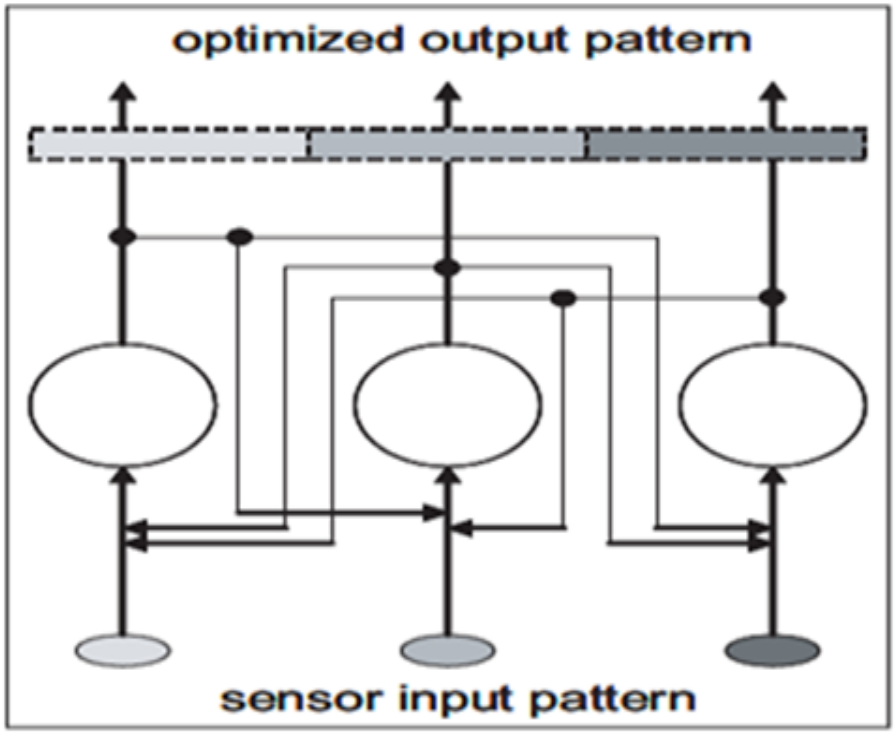

Figure 2: The Hopfield network applied to the single sensor node.

c. COLLISION AVOIDANCE USING HNN:

Wireless communication often suffers from bad channel conditions. One has to deal with erroneous or even lost data packets by signal processing algorithms or other techniques such as retransmission. In this context the HNN shows promising characteristics such as associative memory, robustness and error correction capability to overcome this drawback. HNN uses the concepts of associative memory, pattern completion and error correction. Here Associative memory means that a pattern is not stored on any individual neuron but is a property of the whole network. By using partial or corrupted pattern, it can then use the correlations to recreate the whole pattern/network then it performs pattern /network completion for whole network. The HN itself is robust in case of missing data, and pattern correction in case of corrupted data to remove the collided packet from the network due to the association ability. The HN is a single layer fully connected feedback network with no direct feedback connections, i.e. each single neuron is not directly connected to itself[12-14].

PROPOSED ALGORITHM:

1. **Create a network having 18 node arranged in circular fashion.**
2. **Select source and destination and the sensor node from the nodes.**
3. **While(data is not received by destination)**
4. **repeat**
5. **If(sensor node detect collision)**
6. **Then**
7. **Apply pattern recognition neural network to change the position of the node at which collision is detected.**
8. **And start transmission from source node again.**
9. **Else**
10. **Transmit the data from one node to another.**
11. **End if**
12. **End while**
13. **Exit**

Based on our proposed algorithm, network is simulated using Matlab and as can be seen in figure above, no collision occurs among nodes and all 18 nodes are received at receiver side without collision.

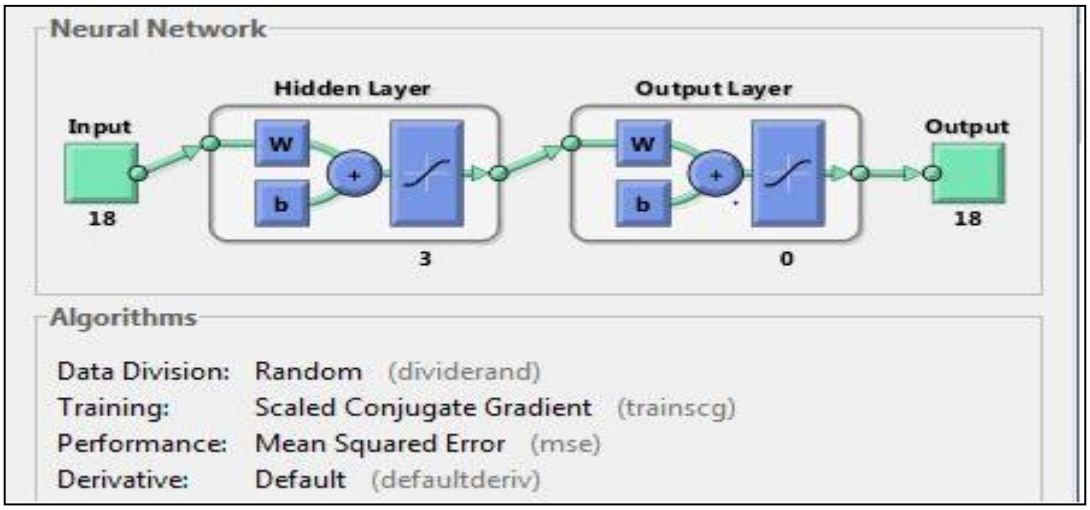

Fig 2. Matlab simulation for Neural Network Approach

V. RESULTS

In this section, we present some graphical results obtained using Hopfield neural network approach to avoid collision. Results obtained are in terms of packet delay and throughput obtained. Also we have compared results of Hopfield with back propagation network to prove how efficient is Hopfield neural network in case of energy preservation by avoiding collision in WSNs. Figure 3 shows that end-to-end delay in case of Hopfield network is less as compared to back propagation network.

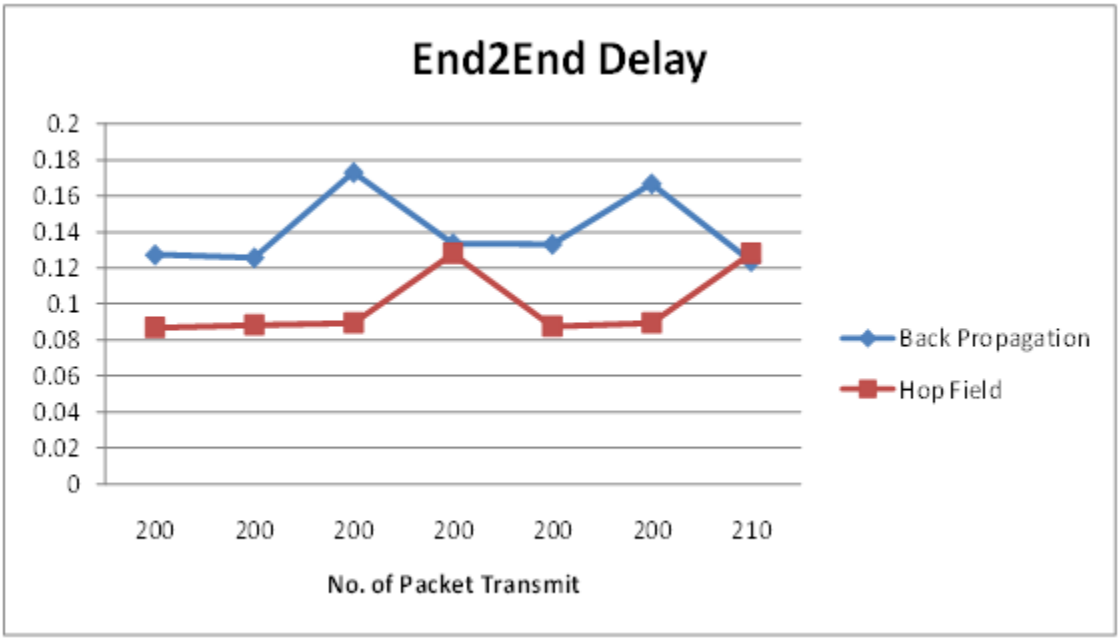

Figure 3: Graph for End2End Delay over no. of Packet Transmit

Figure 4 shows throughput obtained through Hopfield networks is much greater than back propagation networks.

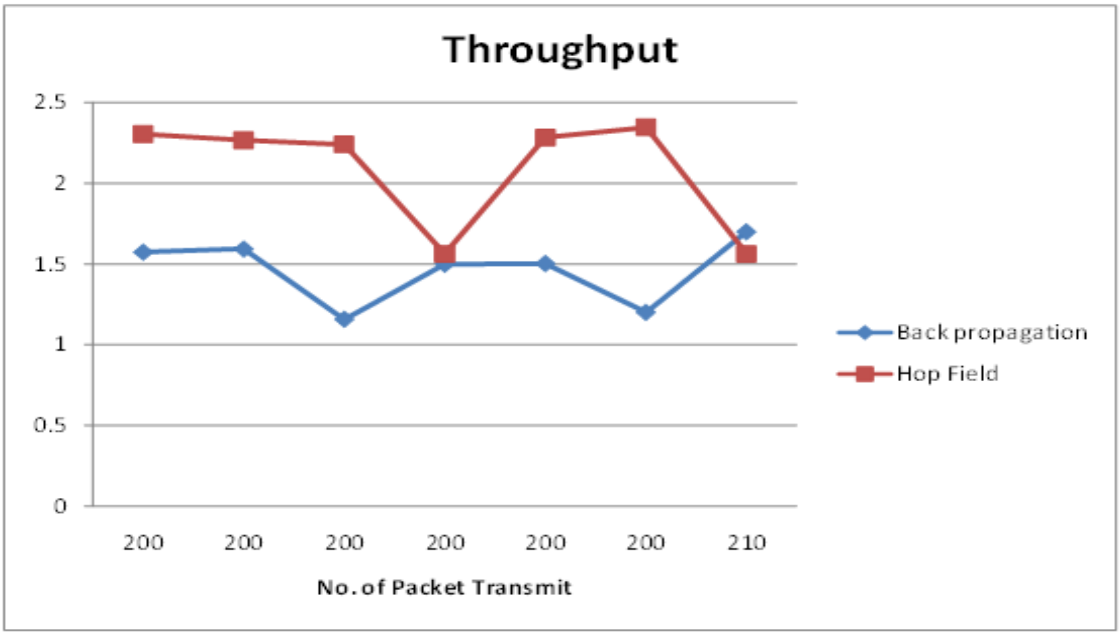

Figure 4: Graph for Throughput over No. of Packet Transmit

VI. CONCLUSION

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 main feature of WSN that makes it unique is its flexibility in terms of the shape of the network and mobility of the sensors. In this paper, we have obtained throughput, delay and packet delivery ratio of networks according to no. of packet transmit using hop-field neural network. 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.

REFERENCES

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

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

[3] RishavDubey, Vikram Jain, Rohit Singh Thakur, SiddharthDuttChoubey,"Attacks in Wireless Sensor Networks" ,International Journal of Scientific & Engineering Research, Volume 3, Issue 3, March-2012- ISSN 2229-5518.

[4]JiyongSon ; Dept. of Electr. Eng., Korea Univ., Seoul, South Korea ; Hwan-JooKwak ; Gwi-Tae Park ,member IEEE proposed some work" Back propagation neural network based real-time self-collision detection method"2011.

[5] Raghavendra V. Kulkarni, "Neural Network Based Secure Media Access Control Protocol for Wireless Sensor Networks" Senior Member, IEEE," 2009.

[6] Phillip Reindl and Kendall Nygard , "Defending Malicious Collision Attacks in Wireless Sensor Networks". Department of Computer Science North Dakota State University Fargo,2007.

[7]Hopfield, J. J., Brody, C. D. and Roweis, S. (1998) Computing with action potentials. Proceedings of Advances in Neural Information Processing Systems10, Denver, CO, 1-6 December, pp. 166-172. MIT Press, Cambridge, MA.2.

[8] H. He, Z. Zhu, "A Neural Network Model to Minimize the Connected Dominating Set for Self-Configuration of Wireless Sensor Networks," IEEE Transaction on neural networks, vol. 20, No. 6, pp. 973-982, 2009.

[9]Hopfield, J. J., Brody, C. D. and Roweis, S. (1998) "Computing with action potentials. Proceedings of Advances in Neural Information Processing Systems"10, Denver, CO, 1-6 December, pp. 166-172. MIT Press, Cambridge, MA.2.

[10] Simon X. Yang, Member, IEEE,proposed some work "Neural Network Approaches to Dynamic Collision-Free Trajectory Generation"2001.

[11],K. Jamieson, H. Balakrishnan, proposed some work "A mac protocol for event-driven wireless sensor networks"2003.

[12] L. Fausett, Fundamentals of Neural Networks. Prentice Hall, 1994.

[13] D. J. C. MacKay, Information Theory, Inference, and Learning Algorithms. Cambridge University Press, 2003.

[14] J. J. Hopfield, "Neural networks and physical systems with emergent collective computational abilities," Proc. of National Academy of Sciences, 1982.

