A Novel Technique To Avoid Collision Through Integrated System Of Hopfield Neural Network And Synthesis Of Pattern For Wsn

Ankita Ojha[1], Priyesh Chaturvedi[2]

Post Graduate Scholar[1], Assistant Professor[2]

Department of Electronics and Communication Engineering

VITS, Satna, MP, India

[1]ankita.ojha1@gmail.com

Abstract:

We present an overview of embedded network applications and discuss requirements arising from this analysis. Furthermore, we discuss selected in-network processing techniques and point out the analogy between Hopfield neural and back propagation networks. In the following neural networks are introduced in the sensor network Context. We describe the motivation and the practical case for neural networks in the sensor networks context, and evaluate early results achieved with our test implementation. We argue that there is a high potential with these paradigms which promise a strong impact on the future research, especially if applied as a hybrid technology.We are implementing this for WNS for finding Collision in Sensor network and also try to find out the throughput value of the data that is transmitted over the sensor network. Further whole simulation executed on MATLAB command prompt and the GUI constructed in the whole research. It finds a typically great and higher value of all term like throughput, E2Edaly and PDR for packet delivery. So deployment of neural network with high PARAM value will give better solution for randomization of testing of WSN for detecting the collision so further avoidance of dropping packets. As per the proposed research it has find on testing the GUI on seven times for earlier and seven times for proposed. It has clear that on delivering the 1280 packet has been send out and 105 packet lost in earlier where as on the same delivering of packet data only 51 number of packet loss. So in numeric data it has very appreciable result for proposed work.Almost double whence compared to earlier. So it is very clear when a neural network has been applied with high PARAM value it has great improvement in minimizing the packet loss due to very active pattern recognition technique that will rectify the packet loss problem as well. Consequently a slight improvement in end to end delay as well in throughput. So the proposed systems do the great work for collision detection during transmission and avoidance.

Keyword: *WSN,Hopfield Network,ANN,PARAM*

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. 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.

LITERATURE SURVEY

RishavDubey, Vikram Jain, Rohit Singh Thakur, SiddharthDuttChoubey in (2012) proposed "Attacks in Wireless Sensor Networks".[1]The authors proposed that Wireless Sensor Networks is an emerging technology. 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 .In this research they investigate how wireless sensor networks can be attacked in practice.

Rajkumar, Sunitha K.R and Dr. H.G Chandrakanth (2012) surveyed on"A Survey on Security Attacks in Wireless Sensor Network".[2]A wireless sensor network (WSN) has important applications such as remote environmental monitoring and target tracking. This has been enabled by the availability, particularly inrecent years, of sensors that are smaller, cheaper, and intelligent. These sensors are equipped with wireless interfaces with which they can communicate with one another to form a network. In this paper we deal with the security of the wireless sensor networks. Staring with a brief overview of the sensor networks, and discusses the current state of the security attacks in WSNs. Various types of attacks are discussed and their countermeasures presented. A brief discussion on the future direction of research in WSN security is also included.

WazirZada Khan Yang Xiang Mohammed Y Aalsalem, in (2011) proposed "Comprehensive Study of Selective Forwarding Attack in Wireless Sensor Networks".[3]Sensor networks are becoming closer towards wide-spread deployment so security issues become a vital concern. Selective forwarding attack is one of the harmful attacks against sensor networks and can affect the whole sensor network communication. The variety of defense approaches against selective forwarding attack is overwhelming. In this research they had described all the existing defensive schemes according to our best knowledge against this attack along with their drawbacks, thus providing researchers a better understanding of the attack and current solution space. Also classifies proposed schemes

according to their nature and defense. Nature of scheme classifies into Distributed and Centralized. Defense of scheme classifies into detection and prevention.

Chaudhari H.C. and Kadam L.U. (2011) research on "Wireless Sensor Networks: Security, Attacks and Challenges".[4]The significant advances of hardware manufacturing technology and the development of efficient software algorithms make technically and economically feasible a network composed of numerous, small, low-cost sensors using wireless communications, that is, a wireless sensor network. Sensor networks have great potential to be employed in mission critical situations like battlefields but also in more everyday security and commercial applications such as building and traffic surveillance, habitat monitoring and smart homes etc. However, wireless sensor networks pose unique security challenges.

PROBLEM FORMULATION AND METHODOLOGY

3.1 How Collision Occur 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 [40]. 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.

3.2 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.

3.3 Feed Forward Back Propagation

ANN's are biologically inspired computer programs to simulate the way in which the human brain process information. It is a very powerful approach for building complex and nonlinear relationship between a set of input and output data. The power of computation comes from connection in a network. Each neuron has weighted inputs,

simulation function, transfer function and output. The weighted sum of inputs constitutes the activation function of the neurons. The activation signal is passed through a transfer function which introduces non-linearity and produces the output. During training process, the inter-unit connections are optimized. Once the network is trained, new unseen input information is entered to the network to calculate the test output. There are many backpropagation algorithm are used in the neural network but mostly used feedforward back propagation neural network (FBNN).

3.4 Hopfield Neural Network

The Hopfield neural network is a simple artificial network which is able to store certain memories or patterns. Hopfieldneural 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 (V_0,V_1,V_2…V_i) where is number of units and is the activation level of unit.

RESULT AND DISCUSSION

In this section, 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

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.

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.

Throughput=total packets/End2EndDelay.

SIMULATION RESULTS

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.

5.1 Comparison Table between Earlier and Proposed Work.

Table 5.1: Result come out by Hopfield neural network

Test Condition	Packet Transmitted	Packet Drop	PDR	E2Edelay	Through Put
Test 1	170	6	99.96	0.160	1056.99
Test 2	170	9	99.94	0.188	902.22
Test 3	210	9	99.95	0.113	1853.47
Test 4	150	0	100	0.058	2547.29
Test 5	170	10.5	99.93	0.158	1069.84
Test 6	200	7.5	99.96	0.110	1810.46
Test 7	210	9	99.95	0.110	1900.92

Table 5.2: Result come out by earlier base algorithm

Test Condition	Packet Transmitted	Packet Drop	PDR	E2Edelay	Through Put
Test 1	190	24	99.87	0.159	1194.36
Test 2	200	15	99.92	0.112	1784.72
Test 3	150	0	100	0.057	2641.04
Test 4	180	9	99.95	0.110	1623.73
Test 5	190	30	99.84	0.158	1195.16
Test 6	190	18	99.90	0.161	1173.90
Test 7	180	9	99.95	0.115	1552.85

As per the comparison of above two tables it is clearly shown that the overall performance of all parameters of result of table 5.1 is clearly much better that the earlier. This will give a better test condition for WSN for generating the actual condition.

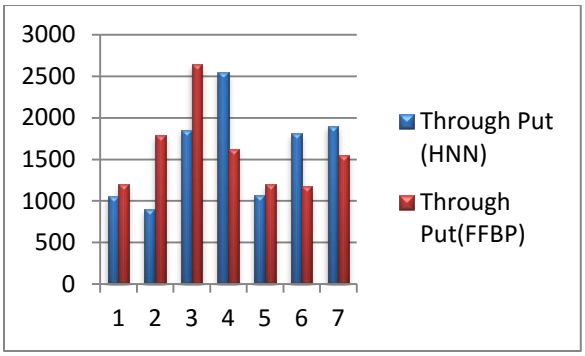

Fig 5.1: Comparison Table

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 akey 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.

Reference:

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

[2] Rajkumar, Sunitha K.R and Dr. H.G Chandrakanth "A Survey on Security Attacks in Wireless SensorNetwork", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622www.ijera.com Vol. 2, Issue4, July-August 2012, pp.1684-1691.

[3] WazirZada Khan Yang Xiang Mohammed Y Aalsalem, "Comprehensive Study of Selective Forwarding Attackin Wireless Sensor Networks", I.J. Computer Network and Information Security, 2011, 1, 1-10 Published OnlineFebruary 2011 in MECS (http://www.mecs-press.org/).

[4] Chaudhari H.C. and Kadam L.U. "Wireless Sensor Networks: Security, Attacks and Challenges". InternationalJournal of Networking Volume 1, Issue 1, 2011, pp-04-16 Available online at:http://www.bioinfo.in/contents.php?id=108.

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

[6] Kalpana Sharma, M K Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA SpecialIssue on "Mobile Ad-hoc Networks" MANETs, 2010.

[7] S. K. Jayaweera, "An Energy-efficient Virtual MIMO Communications Architecture Based on V-BLASTProcessing 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.

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

[9] Sinchan Roy chowdhury, ChiranjibPatra," 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.

[10] 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