COLLISION DETECTION DUE TO MALICIOUS NODE IN WSN THROUGH HOPFIELD NETWORK

Pooja Balyan[1], Mrs Rasmeet Kaur[2]
[1]M.Tech (ECE), [2]DPGITM, Gurgaon

ABSTRACT: Wireless sensor networks monitor dynamic environments that change rapidly over time. This dynamic behavior is either caused by external factors or initiated by the system designers themselves. To adapt to such conditions, sensor networks often adopt machine learning techniques to eliminate the need for unnecessary redesign. Machine learning also inspires many practical solutions that maximize resource utilization and prolong the lifespan of the network. In this paper, we present an extensive literature review over the period 2002-2014 of machine learning methods that were used to address common issues in wireless sensor networks (WSNs). The advantages and disadvantages of each proposed algorithm are evaluated against the corresponding problem. We also provide a comparative guide to aid WSN designers in developing suitable machine learning solutions for their specific application challenges. 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.

I. OVERVIEW

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 is able to communicate and collaborate with each other.

A. Architecture of WSN:

For example, they might spoof, alter or replay routing information to interrupt the network routing [1]. As shown in Figure 1.1, the wireless sensor network and the classical infrastructure comprises of the standard components like sensor nodes (used as source, sink/actuators), gateways, Internet, and satellite link, etc.

B. 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 [2].

II. LITERATURE SURVEY

Rishav Dubey, Vikram Jain, Rohit Singh Thakur, Siddharth Dutt Choubey in (2012) proposed "Attacks in Wireless Sensor Networks".[24]

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".[25]

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".[26]

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".[27]

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.

III. PROBLEM FORMULATION AND METHODOLOGY

A. 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.

B. 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. [41],

C. 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 back propagation algorithm are used in the neural network but mostly used feed forward back propagation neural network (FBNN).

D. 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.[42]

IV. 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.
It can be calculated by the following formula:
Throughput=total packets/End2EndDelay

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 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.

REFERENCES

[1] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures” 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] M. Sims, C. Goldman, V. Lesser, “Self-Organization through Bottom-up coalition formation”, University of Massachusetts.
[4] Suh, Mike Horton, “Powering sensor networks”, Potentials, IEEE, August/September 2004.
[5] K. L. Chee, P. K. Sivaprasad, S.V. Rao, J.G. Lim, “Clock Drift Reduction For Relative Time Slot TDMABased Sensor Networks”, Personal Indoor and Mobile Radio Communications, PIMRC 2004. 15th IEEE International Symposium, Pages: 1042 – 1047, Vol.2, 5-8 Sept. 2004.
[6] M. Hempstead, N. Tripathi, P. Mauro, G. Y. Wei, David Brooks, “An Ultra Low 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.
[7] 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
[8] I. Akyildiz, W. Su, Y. Sankarasubramanian, E. Cayirci, “A Survey on Sensor Networks”, IEEE Communications Magazines, August 2002.
[9] Sinchan Roychowdhury, 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] TahirNaeem, 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
[11] John Paul Walters, Zhengqiang Liang, Weisong Shi, VipinChaudhary, “Wireless Sensor Network Security: A Survey”, Security in Distributed, Grid and Pervasive Computing Yang Xiao (Eds), Page3-5, 10-15, year 2006
[12] Pfleeger, C. P. and Pfleeger, S. L., “Security in Computing”, 3rd edition, Prentice Hall 2003
[13] 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.
[14] C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures,” Elsevier’s AdHoc Networks Journal, Special Issueon Sensor Network Applications and Protocols, vol. 1, no. 2–3, pp. 293– 315, September 2003.
[15] Karlof, C. and Wagner, D., “Secure routing in wireless sensor networks: Attacks and countermeasures”, Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003, pp. 293-315.

