IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013
**ISSN: 2320 - 8791**
**www.ijreat.org**

# Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm

**S. Nishanthi**

**Computer Science and Engineering**
**Kalasalingam University**
**Virudhunagar, TamilNadu**

**Abstract**

Wireless Sensor Networks (WSN) are emerging as a new tier within the IT scheme and a rich domain of active analysis involving hardware and system design, networking, and programming models, data management, security and social actors. Wireless sensor networks are compared with wired networks are additional well vulnerable to attacks and intrusions. The intrusion detection is outlined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or abnormal attackers. The watchdog mechanism is defined to evaluate whether a node has abnormal behavior in method of forwarding data. This paper has a tendency to opt for Bio-Inspired Approach. In this paper, the clonal selection principle is implemented and develop the Watchdog based Clonal Selection Algorithm (WCSA).Using this WCSA, the intrusions in the network and monitoring multiple misbehaved nodes. Using this algorithm we can realize intruders and reduce the detector rate, and reduce generator value also will increase in throughput.

***Keywords***—*Wireless Sensor Networks, Watchdog, Cluster, Clonal Selection Algorithm.*

## 1. Introduction

A wireless sensor network consists of a large range of sensor nodes that are densely deployed either within the development or very near it. The position of sensor nodes need not be pre-determined. This permits random deployment in inaccessible terrains or disaster relief operations. On the opposite hand, this additionally implies that sensor network protocols and algorithms should possess self-organizing capabilities. Another feature of sensor networks is that the cooperative effort of sensor nodes. They are fitted with an on-board processor. Sensor networks can give the end user with intelligence and a better understanding of the environment.

The WSN field matures; ways for detecting the anomalies that are inherent to their physically coupled low-end system design can only grow in importance. In fact, providing acceptable tools will effectively detect and respond to anomalies can greatly increase uptake of the technology by stakeholders. Whereas vital work on conventional network management tools exists, WSN counterparts are slow to gain traction within the community. One of the most challenges for WSN anomaly detection is determining where to introduce the intelligence for detecting and localizing anomalies.

Intrusions are unauthorized access to a system resource. The method of intrusion detection involves analyzing and identifying these intrusions to safeguard the system from malicious activities. There are two main kinds of approaches to intrusion detection. The primary approach is misuse detection or signature-based detection, where known security attack signatures are kept and matched against the monitored system. This kind of detection will accurately detect known attacks; however it is unable to detect any new attacks that emerge within the system. The second approach to intrusion detection is anomaly detection, where a traditional profile of the monitored information is established, so anomalies are known as those measurements that deviate from these normal profiles. Thus, anomaly detection is capable of detection new types of security attacks or intrusions that emerge within the system. A problem with this approach to intrusion detection is the high level of false alarms. False alarms will occur during a non-stationary environment, once the normal behavior of the system changes. Hence, a significant issue for anomaly detection is a way to reduce false alarms whereas still being aware of detection security threats.

Due to their severe resource constraints, nodes in wireless sensor networks are prone to attacks. Compromised nodes may drop packets or inject false packets. Misbehavior of those insiders is hard to find and prevent since they have legitimate keys. Watchdog mechanism is an observation methodology used wide in ad-hoc and sensor networks, and it is the base of a majority of misbehavior detection algorithms and trust or reputation systems. The essential plan of watchdog is that a node monitors whether or not its next-hop neighbor forwards the packets it simply sent by

overhearing. If the packet is not forwarded at intervals a certain amount, the neighbor is regarded as misbehaving during this transaction. Once the misbehaving rate surpasses certain threshold, source is notified and following packets are forwarded on different route. If the information flows are equally distributed and node behaves consistently, it will create the judgment of its last-hop with reverse flows. Although literature proposed some propagating mechanisms to form node aware of last-hop past behaviors, exchange of trust data additionally introduces other disadvantages such as communication overhead and potential attacks.

Every node maintains a table of counters for each upstream neighbor. If it finds the upstream node forwards a packet to itself successfully, the counter is increased by 1+α. If it finds the upstream node drops a packet, the counter for it is decreased by β. α and β are reward and punishment parameters respectively. Whenever a packet is forwarded, the counter of that neighbor is decreased by one. Only when the counter is bigger than zero will the node forward the packet for the neighbor. The method will effectively decrease the quantity of injected false information and selfish information.

## 2. Related Works

The watchdog technique [1] permits detecting misbehaving nodes. When a node forwards a packet, the watchdog set within the node ensures that the next node in the path also forwards the packet. The watchdogs will this by listening to all nodes at intervals transmission range promiscuously. If the node does not forward the packet, then it is considered as malicious node. A specific watchdog module is implemented and tested with the large number of nodes. In [2], they determined whether a node exhibits a malicious behavior, the watchdog counts all packets received from its neighbors and the packets should be forwarded. A neighbor trust level can be defined as the ratio between the received packets for forwarding and those effectively forwarded by the neighbor node. Watchdog [3] employs identifier-based checking of use-after-free errors almost entirely in hardware, relying on the software run time only to provide information about memory allocations and deallocations. As pointers can be resident in any registers, conceptually watchdog extends each register with a sidecar identifier register. Watchdog checks to ascertain if the identifier associated with the pointer being referenced is still valid.

The intrusion detection approach [5] modeled on the basis of two bio-inspired concepts namely, negative selection and clonal selection. The negative selection mechanism is the immune system can detect the foreign patterns in the complement space. The clonal selection principle is used to explain the basic features of an adaptive immune response to an antigenic stimulant. It establishes the idea that only those cells that recognize the antigens are selected to proliferate.

## 3. Proposed Scheme

The existing watchdog mechanism is having some limitations. It does not provide the best result if the malicious node is in multi hop distance in the network. The all nodes are having the responsibility of monitoring the neighbors and passing the information about the behavior. It includes lot of communication over head. The Artificial Immune System (AIS) forms the basic solution for various real world problems particularly in the intrusion detection. The clonal selection principle is used by the AIS to define the basic features of an immune response to an antigenic stimulus.

### 3.1 Clonal Selection Algorithm:

The algorithms are inspired by the clonal selection theory of resistance that explains however B and T lymphocytes improve their response to antigens over time known as affinity maturation. It focus on the Darwinian attributes of the theory where selection is inspired by the affinity of antigen-antibody interactions, reproduction is inspired by biological process, and variation is inspired by physical hyper mutation. Clonal selection algorithm is most typically applied to optimization and pattern recognition domains.

The three main features of the clonal selection theory that are created in intrusion detection are:

- Proliferation and maturation on stimulation of cells with antigens;
- Generation of new random genetic changes, subsequently expressed as various antibody patterns, by a form of accelerated physical mutation;
- Elimination of fresh differentiated lymphocytes carrying low affinity antigenic receptors.

The basic Clonal Selection Theory is if an animal is exposed to an antigen, some sub population of its bone marrow derived cells (B

lymphocytes) respond by producing antibodies (**Ab**).Each cell secretes only one kind of antibody, which is specifically for each antigen. By binding to these antibodies (receptors), and with a second signal from accessory cells, such as the T-helper cell, the antigen stimulates the B cell to divide into multiple and mature into terminal (non-dividing) antibody secreting cells, called plasma cells. The different type of cell divisions (called mitosis) generates a clone, that is, a set of cells that are the replica of a single cell. While plasma cells are the most active antibody secretors, large B lymphocytes, which divide rapidly, also secrete **Ab**, at a lower rate. While B cells secrete **Ab**, T cells play a central role in the regulation of the B cell response and are dominating in cell mediated immune responses. Lymphocytes are ends to proliferate and differentiate into plasma cells that also differentiate into long-lived B memory cells.

The following table shows that, how this biological concept are mapped with our network.

Table 1: Mapping Immune System with Network

| ***Immune System*** | ***Network Environment*** |
|---|---|
| Bone marrow and thymus | Primary IDS generates detector sets |
| Antibodies | Detectors |
| Antigens | Network Intruders |
| Self | Normal activities |
| Non-Self | Abnormal activities |

## 3.2 Watchdog based Clonal Selection Algorithm:

Input: S = 'n' number of malicious node from set of sensor nodes.

Output: W = set of clusters which are having watchdog nodes used to find malicious nodes.

Begin

{

1. Create Network topology
2. Assign energy for all nodes
3. Create clusters
4. For all clusters
5. {
   - Select cluster head which is having greater energy

   }
6. For all clusters in hierarchical topology S do
7. For all cluster head enable the watchdog mechanism
8. For all rounds
9. {

   If energy-level < energy-limit

   {
   - Change the cluster head
   - Select node with high energy assign as cluster head //Cloning process

   }

   }
10. For all cluster head

    {
    - Store all the send items
    - Checks whether the forwarded packets are equal or not
    - If not equal send alarm to its cluster members

    }

}

End

In this section, a model is proposed for intrusion detection system in wireless sensor networks. This model follows hierarchical architecture. The whole network is divided into small parts known as clusters. Each cluster indicates the sensory limit of a cluster head node. The cluster head nodes are marked in blue are having the responsibility of monitoring the local nodes which are in the cluster.

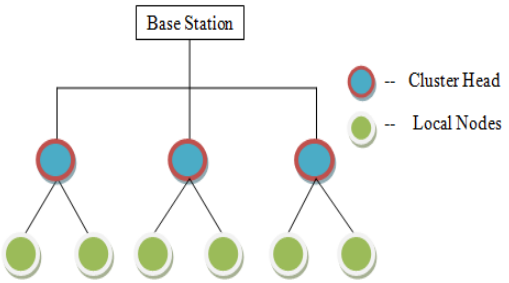


Fig 3.2.1: Proposed Hierarchical Model

The local nodes are marked in green that are under the cluster head. The number of the sensors in the clusters can be different. The network topology can be changing. The cluster head is changed at each interval based on the energy level. The node in the cluster is selected as cluster head which is having greater energy. The technique of detecting abnormality in the first level is handled by the cluster head nodes. The cluster

head is having the responsibility of controlling and receiving the information from their cluster nodes as well as sending alert message to the upper layer which is in base station. Base station is the high level of the proposed model which is directly handled by human.

In wireless sensor networks, a hierarchical topology is used for identifying the network behavior such as normal and malicious status. In this topology, number of sensor nodes is used and to select the cluster head based on their energy level. From this topology, a set of cluster heads are selected ,and the watchdog behavior module will be enabled in the cluster heads. When the cluster head is getting lowest energy with highest intrusions, a watchdog node will be cloned in cluster to detect the intrusion level of the networks.

From the above discussion watchdog that detect the intrusions in the network and repeat this same set of procedure for remaining clusters in network and also the highest level of intrusion can be detected and the corresponding results store it on the buffer or memory. This technique is used to identify the intrusion in network with the multiple clones of the watchdog. That reduce the attacks and to extend the detector rate.

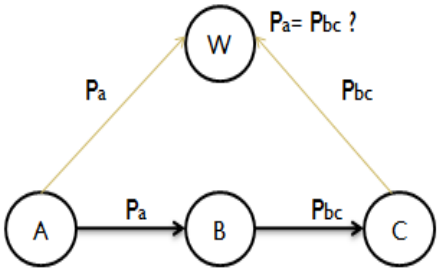


Fig 3.2.2: Process of Cluster Head

In the above figure, W is the cluster head and it acts as watchdog node. It stores all the sent items in every transmission. When the node A sends the packet to node B, watchdog node stores the data packets in its buffer. Now node B forwards the data packet which are sent by node A. Watchdog node checks the node B's sent items whether it is equal or not. If it is not equal, it sends the alert message to other nodes about node B's misbehavior.

## 4. Performance Analysis

The performance of the network was analyzed by suggests that of three parameters such as throughput, packet delivery ratio, dropped packets, over varying number of nodes in the network.

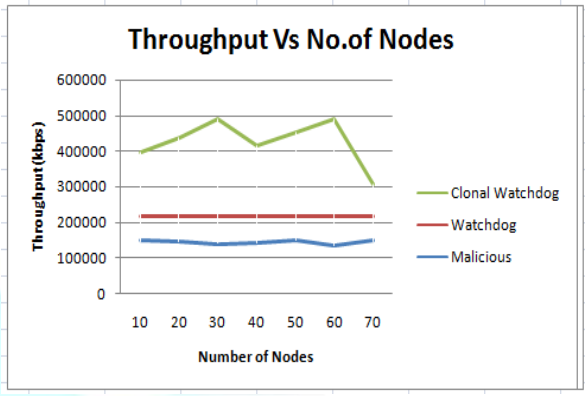


Fig 4.1 Throughput Vs Number of Nodes

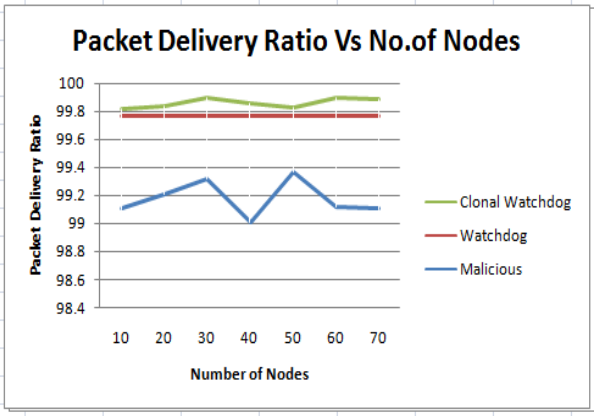


Fig 4.2 Packet Delivery Ratio Vs Number of Nodes

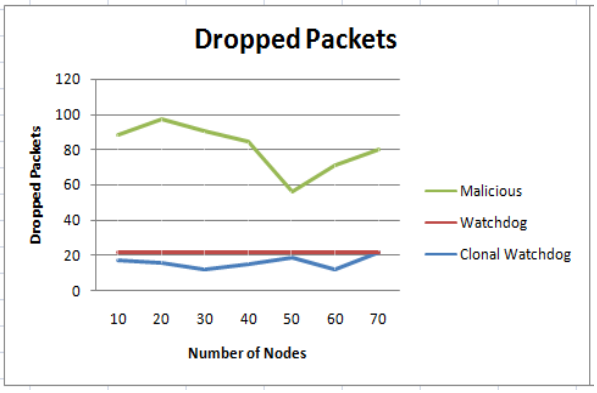


Fig 4.3 Dropped Packets Vs Number of Nodes

## 5. Conclusion

Node's misbehavior is harmful to the performance of WSN. Malicious dropping and excessive packet injecting is that the common misbehaving mode of compromised or selfish

nodes, that cannot be detected with traditional authentication technique. Current watchdog mechanism can only evaluate the behavior of next-hop. With the near one-direction traffic pattern in WSN, there should be some trust propagating mechanism to tackle the problem. The development of an Intrusion Detection System based the clonal selection principle, is considered and a model system has been proposed. The clonal selection algorithm serves to create a comprehensive rule set that can detect most of the intrusions. Thus, I hope that the Intrusion Detection System built on these principles will be able to perform efficiently in real time environments.

## References

[1] Jorge Hortelano, Juan-Carlos Cano, Carlor T. Calafate, Pietro Manzoni, "Watchdog Intrusion Detection Systems: Are They Feasible in MANET?", S/N:46022, August 2010.

[2] Jorge Hortelano, Jan Carlos Ruiz, Pietro Manzoni, "Evaluating the usefulness of watchdogs for intrusion detection in VANETs", December 2010.

[3] Santhosh Nagarakatte, Milo M.K. Martin, Steve Zdancewic, "Watchdog: Hardware for Safe and Secure Manual Memory Management and Full Memory Safety", June 2012.

[4] Ankit Aggarwal, Bhumika Garg, "Survey on Secure AODV for Ad Hoc Networks Routing Mechanism", Vol: 2, March 2012.

[5] Kasthurirangan Parthasarathy, "Clonal Slection Method for Immunity based Intrusion Detection Systems", August 2009.

[6] K. Tamizarasu, M. Rajaram, "An AODV-based Clustering Approach for Efficient Routing in MANET", Vol: 51, No. 15, August 2012.

[7] M. C. Aswathy, Tripti C, "A Cluster Based Enhancement to AODV for Inter-Vehicular Communication in VANET", Vol.3, No.3, September 2012.

[8] A. Forootaninia, M. B. Ghaznavi-Ghoushchi, "An Improved Watchdog Technique based on Power-Aware Hierarchical Design for IDs in Wireless Sensor Networks", Vol.4, No.4, July 2012.

[9] Abderrezak Rachedi, Hand Baklouti "muDog: Smar Monitoring Mechanism for Wireless Sensor Networks based on IEEE 802.15.4 MAC", Vol.1-18 June 2012.

[10] Matthis Becker, Martin Drozda, Sven Schaust, Sebastian Bohlmann, Helena Szczerbicka, "On Classification Approaches for Misbehavior Detection in Wireless Sensor Networks", Vol.4, No.5, May 2009.

[11] Ruchi Bhatnagar, Dr. A. K. Srivastava, Anupriya Sharma, "An Implementation Approach for Intrusion Detection System in Wireless Sensor Network", Vol.02, No.07, May 2010.

[12] Mohammed Korayem, Waleed Abo Hamad, Khaled Mostafa, "A hybrid genetic algorithm and Arificial Immune System for informative gene selection", Vol.10, No.7, July 2010