# DETECTING THE COMPROMISED NODE IN ZONE – BASED LEADER ELECTION METHOD IN WSN

Udaya Suriya Rajkumar D.[1] and Rajamani Vayanaperumal[2]
[1]Computer Science and Engineering, Sathyabama University, Chennai, India
[2]Department of Electronics and Communication Engineering, Veltech Multitech, Avadi, Chennai, India
E-Mail: u_suriya@yahoo.com

## ABSTRACT

Since the WSN is not secured in nature, it compromises the sensor node and the physical capture of these nodes is very easy for the intruder nodes. The intruder nodes simply communicate with any node in the zone, thus compromising the nodes and in turn spoiling the nature of the network. To reduce the damages be fallen on the compromised nodes, it should be successfully detected and revoked as soon as possible. Range of node specifies detection systems in wireless ad-hoc and sensor networks have been projected by academicians, of late. In the existing approach Leader based intrusion detection system as well as trust value calculated is used to find out suspect regions where the compromised nodes are ensconced, here the Leader will be elected region wise based on the energy level to detect the attacker and revoke the compromised node. To overcome this as well as to provide high security two new stage approaches are proposed. They are the DPFM-[Data Packet Format Matching] method which detects the attacker node and DAA-[Divert Attention Attacker] method which prevents nodes compromising in the zone. The simulation result shows that the compromising node is eliminated and attacks are controlled in the network.

**Keywords:** zone-based, attacker node, compromising node, detect, prevent.

## 1. INTRODUCTION

Wireless sensor network are too dynamic and the nodes are self-organized. The nodes are placed randomly in anywhere in the network [1]. Since Wireless sensor networks do not have the infrastructure. A node cannot be accompanied to the existing infrastructure. The regions of the wireless sensor network are also dynamic due to the number of nodes in the networks are growing. The entire network can be divided into zones or the regions [2]. A malicious node can occur in the inter zone or in intra zone. The earlier studies discussed about node replication attack. A sensor node is captured by adversary node to extract the information about the node and produces copies of the captured node [13]. Clone nodes are newly formed will be having the same ID as that of the captured node. Clone nodes are treated as legitimate nodes and hence it is very difficult to detect them. Once the clone nodes gain the trust of the sensor nodes, they will perform many malicious activities. Hence it is very important to detect the nodes [3].

Here proposed zone-based node revocation and compromise detection scheme for sensor networks using the two new stage approaches. This paper provides a new technique which can detect and prevent the malicious node in the inter zone or intra zone. The simulation result has shown the proposed approach better than the existing approaches in terms of detecting the malicious node to increase the throughput, energy packet delivery ratio.

This paper includes the Literature Survey related work which was discussed in Section 2. Section 3 presents the Problem Statement. In Section 4, Results and Discussion was discussed and Section 5 presents Conclusion.

## 2. LITERATURE SURVEY

In [4] centralized scheme, the author propound, each node sends a list of its neighbors and their claimed locations to the base station. The base station, then examines the neighbor list to detect the replica nodes. If replica nodes are detected, the base station will revoke the replicated node by flooding the network with an authenticated revocation message. In [5] the identities of the node are checked by simply seeking of each node. The efficiency of this approach promotes the results to prove analytically when the node density is more sufficient in the network. The location information of newly joined nodes is forwarded to the corresponding witness nodes. Witness nodes on the reception of two location claims from the same ID can detect the presence of replica node. Node-To –Network, broadcasting and Deterministic multicast are two distributed approaches. In Node-To-Network Broadcasting each node stores the location information for its neighbors and if it receives a conflicting claim, revokes the offending node. If an adversary can jam key areas or interfere with communication paths, this method cannot achieve 100% detection. Also the total communication cost for each node is high [12]. In Deterministic multicast a nodes location claim is shared with a limited subset of deterministically chosen witness nodes. But this method has high communication cost. Since deterministic, the adversary can also determine the witness nodes. It cannot afford a large number of witness nodes. In [6] authors propose a novel of clustering algorithm for GA based load balanced, and it is for both equal and unequal load on the sensor nodes. In [7] author proposes a novel infiltration detection system based on cross layer communication of, MAC physical layers which has given a new type of IDS. The two WSN models of homogeneous and heterogeneous are considered in [8], which is derived by utilizing two sensor modals like single-sensing detection and multiple-sensing detection. Finally, the WSN enhances the network connectivity, broadcast reach ability and detection probability. In [9] author propounds a hybrid model uses the k-means classifier to ferret out specific incursion, to analyze MAC layer features which can reduce the learning algorithm for the preciseness of the intrusion detection system. The existence types of classifiers on neural networks influence the optimization of detection systems. It propounds opportunistic encryption to increase the throughput optimally within the acceptable security restraints.

In [10] author uses an improved decentralized and customized version of the Dendritic Cell Algorithm, which allows nodes to observe their neighborhood and collaborate to pinpoint their intruders. In [11] authors implement and testing both in simulation and in real sensor platform scenarios. They are compared with each other and also compared with the Negative Selection Theory, implementation in order to showcase its efficacy detecting a denial-of-sleep attack and in energy consumption.

## 3. PROBLEM STATEMENT

Proposed system states how the malicious node is detected eliminated and prevented by applying the two stage approach. The first strategy is detecting the attacker and the compromised node and revoking the node. In the second stage the communication of the attacker node with the other nodes is avoided by diverting the attacker node to the BS; the BS takes care of the attacker node. For the first stage the DPFM is proposed, and for the second stage the DAA is proposed as shown in the system model Figure-1.

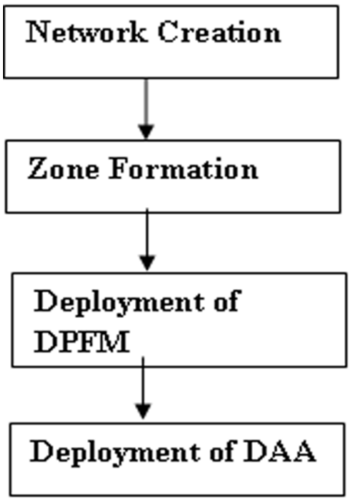

**Figure-1.** System model.

### a) Network creation

In this paper, a network is defined as an area of 1200 x 1200 and is divided into zones with an area of 300 x 300. It can be safely assumed that there are N numbers of nodes deployed randomly throughout the zones in equal number. The communication between the nodes is bi-directional. The network BS is the most trusted entity. There is also an assumption that the BS cannot be compromised by any attacker nodes and that all the nodes knows about their location, ID and placement zone and the nodes are loosely harmonized, which can be obtained by the existing approaches.

### b) Zone formation

The N number of nodes are equally divided and placed randomly in the zones, where the zones are akin to cluster in a network and each zone has its own leader. The sensor nodes can interact and communicate with other nodes through their leader. The attacker node always comes from outside the zone, and is an entirely new node in the network. It is assumed that the attacker node attempts to enter as many zones as possible to compromise as many nodes as possible in each region. Since many nodes are compromised, they start to misbehave in the network and spoil the environment, greatly disrupting the network. Leader node is selected based on the energy level of nodes in the zone. If more than a node has the same energy level, based on the majority voting a node is selected. Zone leader will send a message to one hop neighbors and so on. Nodes respond to the zone leaders by sending a message back. When a node communicates with other nodes in any zone, the zone leader can be monitored the surrounding node. The leader node can be act as a server it should check all the communication in the network.

| From Node-ID | Location | Zone ID | Data | To Node- ID |
|---|---|---|---|---|

**Figure-2.** Data packet format.

The data format given in figure-2 is the common format to be followed by the nodes in the network. Whenever a node inside the network communicates with other nodes in the same network, a data packet is sent. So it is easy to detect any malicious node even ones that cannot communicate in the same data format.

### c) Deployment of DPFM

The proposed approach is detecting and preventing malicious nodes in two different stages. In the first stage while data is transmitted, the data packet is verified by the DPFM, which then checks the data packet format. If the format matches with the template data packet format then it allows the packet to be transmitted. The DPFM should act as a server and should check all the communications in the network. The DPFM is integrated and deployed with the Leader of the Zone, where each node should communicate with other nodes through the zone leader. This data is verified by the zone leader with the help of DPFM. The DPFM detects most of the inside and outsiders in the initial stage itself. The first stage process happens a little late, when a malicious node from outside is allowed to communicate with the insiders of the network and their by detected. The network is saved by preventing the detected malicious nodes from entering.

**d) Deployment of DAA**

In the second stage, when the node as been detected as a malicious node or compromised node the Leader node diverts the un-known node to the BS. The BS executes DAA on the suspected node. Since it is assumed that the nodes in the network knows their location and has information about the neighbors in the zone, if any node comes from outside sending a message, this node is immediately diverted to the BS. The BS eliminates and blocks the node immediately. The complete functionality of the stage1 [DPFM] and stage 2 [DAA] is depicted in given algorithm.

**e) Algorithm for proposed DPFM and DAA**

```
Network G, ∀ G = { $Z_1$, $Z_2$, ….., $Z_n$} // $Z_i$ are zones
For i=1 to NN step n
$Z_i$. node ← node[i]
End I // DPFM starts here
Let tmpNodeArr[] = [NodeID, X, Y, ZoneID]
For j=1 to NN step length(zone)
For I = 1 to length(zone)
Len = tmpNodeArr.length
$Node_i$. Packet → leader(zonei)
For cntr = 1 to Len
Nodeloc = tmpNodeArr[cntr].(X,Y)
If (($Node_i$.Pkt.NodeID = tmpNodeArr[cntr].NodeID
&& ($Node_i$.Pkt.Nodeloc = Nodeloc)) then
$Node_j$.Pkt ←$Node_i$.Pkt
Else declare “ node I is malicious”
Delete node i
End if
End for
End for
// DAA starts here
For I = 1 to NN
If (($node_i$.ID is invalid) or ($node_i$.loc is invalid) or
($node_i$.ZoneID is invalid)) then
Declare “ node is malicious”
$node_i$.msg → $node_j$
Send details of malicious node to BS.
End if
End for
```

## 4. RESULTS AND DISCUSSIONS

The algorithms DPFM, DAA is written in TCL, CC language in the NS-2.34 simulator and investigate the functionality of the proposed approach. Since this paper analyzing WSN, the AODV protocol is integrated with the DPFM, DAA algorithms and the results are obtained and shown below.

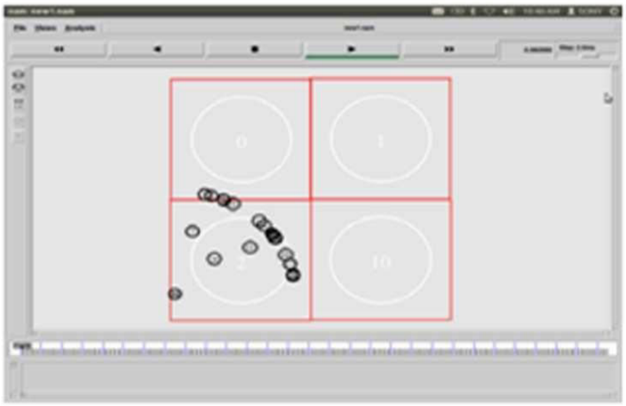

**Figure-3.** Network creation.

The Figure-3 represents a network. Here the network is divided into various types of zones. Each zone contains an equal number of nodes. First the network is formed and the nodes are considered as common to that network. The network then be divided into zones and the common nodes will be moved to the corresponding zone based on the unique ID given to each node for identification. And the main thing is that each zone should contain unique nodes and equal number of nodes.

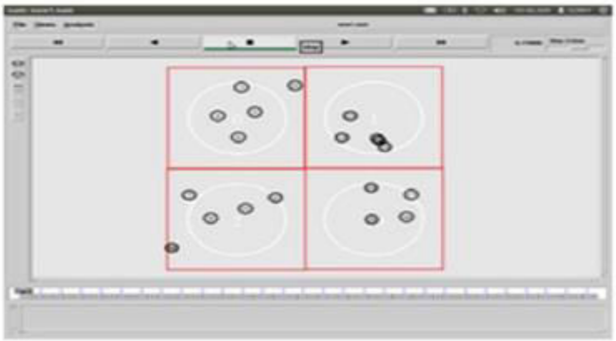

**Figure-4.** Zone formation.

The Figure-4 depicts the zone formation. The whole network is divided into four zones and each zone is named as 0, 1, 2, 3…a soon. After the zone formation the nodes have to be organized for each zone. The nodes are deployed based on an ID. For example, in the above figure zone 0 contains the nodes with IDS 3, 4, and 5 and soon. The Zone-2 contains node-8, node-9, node-10 and node-11 with in the region. Each zone should contain unique nodes only. Duplicate nodes will not be allowed in any zone of the network. The whole network, an every individual node will be controlled and monitored by the base station, which is placed on the top of the network.

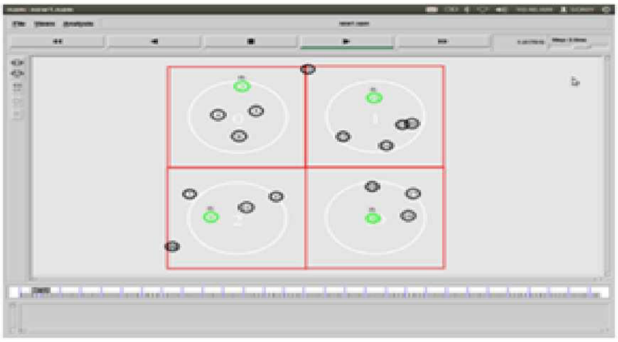

**Figure-5.** Zone leader.

Figure-5 represents the zone leader selection. After deploying the nodes to the zones, zone leader has to be chosen. The zone leader is selected based on above mentioned criteria. The node which is having higher energy level in the particular zone will be selected as the Leader of the zone. The main purpose of the zone leader is to monitor and communicate with the nodes in a particular zone. In the above figure the green color nodes are the zone leaders. The communication between the nodes is bi-directional and the network Base Station is the most trusted entity.

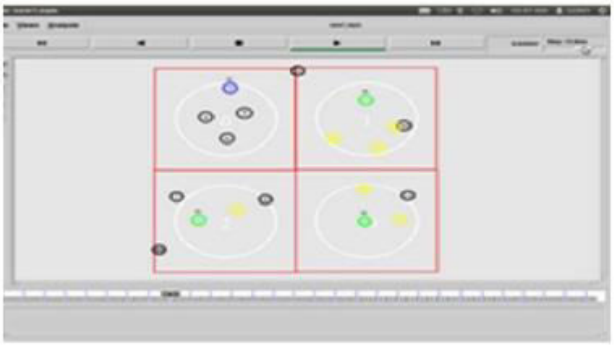

**Figure-6.** Data packet format matching.

Figure-6 represents the function of DPFM. The attacker node always comes from outside the zone, and is entirely new node for the network. It is assumed that the attacker node attempts to enter as many numbers of zones as possible to compromise as many nodes as possible in each sector. Here, node 22 comes from outside of the network as so is treated as an attacker node. This attacker node tries to communicate with as many nodes as possible in that network and in-turn tries to compromise some nodes in that network. These are the things that are monitored by the zone leader.

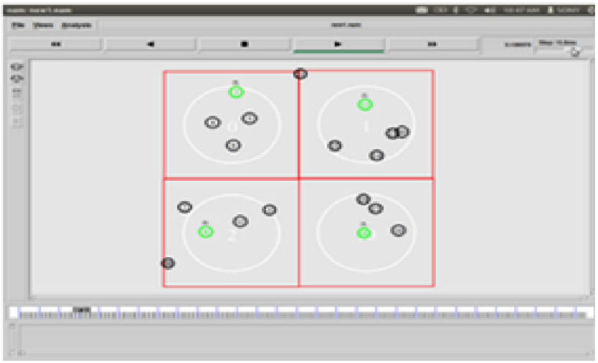

**Figure-7.** DPFM packet matching.

Figure-7 represents the interaction between the attacker and the other nodes in the network through a packet. Basically communication happens in the network by sending packets among nodes. And this is monitored and controlled by DPFM. Communication will be allowed only when the packets are in the correct format. Otherwise the communication will be terminated by DPFM. The zone leader is also used with DPFM to monitor and control the communication among the nodes. Here the attacker node 22, in order to spoil the network tries to compromise the nodes by communicating with the other nodes. This communication is initially restricted by DPFM with the help of a zone leader. To restrict the attacker, the DPFM first checks the template format with the node packet format that comes from outside the network. If the outside node packet matches the template format then DPFM will allow communication among the network otherwise it will restrict the attacker.

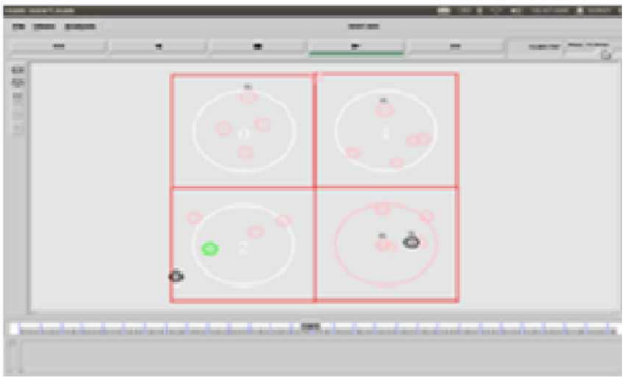

**Figure-8.** DAA function.

The Figure-8 depicts that DAA Divert Attention Attacker Module which is another method used to reject the attacker. DPFM will divert the un-known node to the BS. The BS executes DAA on the malicious node. Since the network model assumes that the nodes in the network knows its location and information about the neighbors in the zone, if any node coming from outside sends the message, it is immediately diverted to the BS. The BS eliminates and blocks the node immediately. Here also node 22 which comes from outside the network is treated as an attacker node. This attacker node will try to communicate with the other nodes in that network. It first tries to compromise some nodes in that network. Here the DPFM first finds the attacker and then sends it to the Base station, thereby protecting the network from any attack. Consider 10 nodes consist of one attacker node out of 100 nodes we are assuming 10 attacker nodes. Here the study detects 9 attack nodes in the overall zone. Here the Figure-9 shows the comparison of average trust value between existing method and proposed DPFN and DAA.

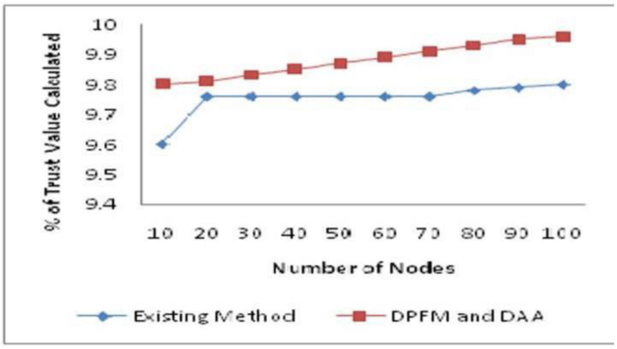

**Figure-9.** Comparison of trust value calculated between existing and proposed DPFM and DAA method.

The packet delivery ratio has been improved after applying DPFM and DAA. That is shown in the below Figure-10.

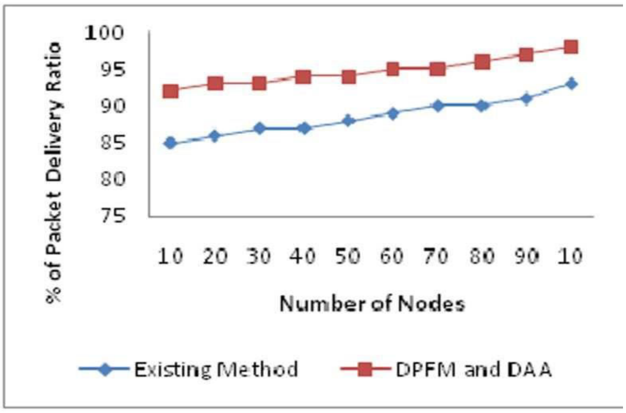

**Figure-10.** Comparison of packet delivery ratio between existing and proposed DPFM and DAA method.

After Deploying the DPFM and DAA the end to end delay also improved. The comparison of end- to end delay has been shown in the Figure-11.

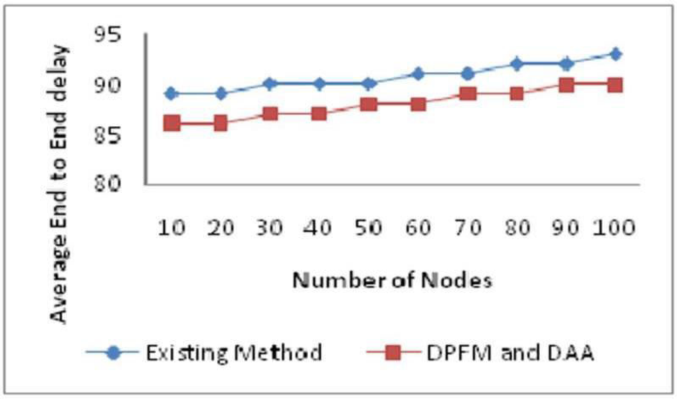

**Figure-11.** Comparison of average end to end delay between existing and proposed DPFM and DAA.

Here the Data packet matches the attacker nearly up to 90%, which means every node which comes from outside is thoroughly checked and the mismatched packets are initially identified and the attackers removed. The total number of nodes and the total number of attacker node in the network. The overall nodes in the network are 100 in that the attacker node will be 10 and the numbers of node detected are 9. It shows that the 90% efficiency of the proposed approach. The comparison of malicious node detection is shown in the Figure-12.

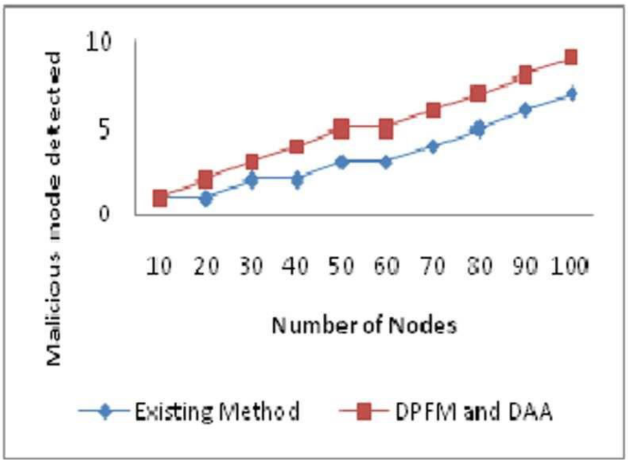

**Figure-12.** Comparison of malicious node detection between existing and proposed DPFM and DAA.

Before the usage of DPFM model the energy consumption was somewhat more. But for DAA the consumption of energy will be in an opposite manner. However in our system DPFM is used only for preventing the unknown user but DAA is used to detect and remove the unknown user in the network. Also the consumption of energy is very low in the proposed system comparing with the existing system.

## 5. CONCLUSIONS

This paper provides more accuracy in detection and prevention with the help of the Monitoring Node.

The DPFM combined DAA algorithms, playing a vital role in the WSN for providing complete security at the maximum. The energy consumption, Trust value calculated, End to End delay, packet delivery ratio and detecting malicious node obtained by our system is best. The efficiency of the approach can be shown through the results produced. In future, instead of multiple algorithms functioning separately, a single algorithm can be developed for both detecting and preventing malicious nodes in inter and intra zone communications.

## REFERENCES

[1] Jennifer Yick, Biswanath Mukherjee and Dipak Ghosal. 2008 “Wireless sensor network survey,” Computer Networks, Vol.52, pp.2292 – 2330, April.

[2] Udaya Suriya Rajkumar, D. Rajamani Vayanaperumal. 2013. “A Leader Based Monitoring Approach for Sinkhole Attack in Wireless Sensor Network,” Journal of Computer Science, Vol.9, pp.1106 – 1116.

[3] Soumitra Das and Pramoc Ganjew. 2014. “Energy Efficient Cluster Based Hierarchical Routing Protocols in Wireless Sensor Network- a Survey,” Multidisciplinary Journal of Research in Engineering and Technology, Vol. 1, pp. 06 – 22, April.

[4] B. Parno, A. Perrig,and V. Gligor. 2005. “Distributed detection of node Replication attacks in Sensor networks,” In Security and Privacy, 2005 IEEE Symposium on, pp. 49 – 63, May.

[5] Rakshith Upparige K R, Sateesh Kumar H. C. 2013. “Reputation Based Zone Trust Detection and Swatt Revocation Method Using SPRT in Sensor Networks,” International Journal of Innovative Research in Science, Engineering and Technology, Vol.2, May.

[6] Pratyay Kuila, Suneet K. Gupta, Prasanta K. Jana “A novel evolutionary approach for load balanced clustering problem for wireless sensor networks,”Elsevier, pp. 2210 – 6502.

[7] Djallel Eddine Boubiche and Azeddine Bilami. 2012. “Cross layer intrusion detection system for wireless sensor network”, International Journal of Network Security & Its Applications, Vol.4, March.

[8]Yun Wang, Xiaodong Wang, Bin Xie, Demin Wang, and Dharma P. Agrawal. 2008. “Intrusion Detection in Homogeneous and Heterogeneous Wireless Sensor Networks,” IEEE Transactions on Mobile Computing, Vol.7, June.

[9] Systems Khalil El-Khatib, Member. 2010. “Impact of Feature Reduction on the Efficiency of Wireless Intrusion Detection”, IEEE Transactions on parallel and Distributed Systems, Vol.21, August.

[10] Jing Deng, and Yunghsiang S. Han. 2008. “Multipath Key Establishment for Wireless Sensor Networks Using Just-Enough Redundancy Transmission”, IEEE Transactions on Dependable and Secure Computing, Vol. 5, July-September.

[11] Helio Mendes Salmon, Claudio M. de Farias, Paula Loureiro, LuciPirmez, SilvanaRossetto, Paulo Henrique de A. Rodrigues ,Rodrigo Pirmez,Fla´via C. Delicato, Luiz Fernando R. da Costa Carmo. 2012. “Intrusion Detection System for Wireless Sensor Networks Using Danger Theory Immune-Inspired Techniques”, June.

[12]Abderrahmane Baadache N., Ali Belmehdi. 2012. “Fighting against packet dropping misbehavior in multi-hop wireless adhoc networks”, Journal of Network and Computer Applications, Vol. 35, pp. 1130 – 1139, January.

[13] Soumya Sara Koshy, Sajitha M. 2003. “Zone Based Node Detection in Wirlesss Sensor Using Trust,” International Journal of Computer Trends and Technology, Vol.4, pp. 2316 – 2340, July.