DESIGN OF AN INTRUSION DETECTION SYSTEM TO DETECT THE BLACK HOLE ATTACK USING LESS ENERGY CONSUMPTION IN WSN

Bhupinder Singh
Dept. of Computer Science Engineering, Punjabi University, Patiala, India
Email: ebhupinder@gmail.com

ABSTRACT

In recent years, the applications based on the wireless sensor networks are growing day by day. Wireless sensor network is collection of sensor nodes. These sensor nodes monitor the physical conditions like sound, temperature, vibrations etc. The Wireless Sensor network are weak against many types of attacks. One of the main attack is Black Hole attack. The Black Hole attack in sensor nodes, it sends the false routing information but show that it has original route information and it increase the packet dropping chance and it is very hard to detect and prevent.

In this paper, a new intelligent intrusion detection system has been proposed and implemented to reduce the false alarm rate present in the existing Intrusion Detection System. The final contribution of this paper is the proposal of a new cluster and trust based routing technique in which the trust score evaluation is carried out to detect the intruders effectively in WSN.

Keywords: Wireless Sensor Networks, Intrusion Detection System, Black Hole Attack, Proposed IDS to Detect the Attack,

I. INTRODUCTION

Wireless sensor network is group of sensor nodes. WSN can be defined as a self-configured wireless network to monitor physical or environmental conditions, such as sound, vibration, pressure, temperature, motion or pollutants [1]. They are self-organizing, self-healing and decentralized in nature. The main objective of sensor nodes to collect selective data from its surrounding environment and transmit it to the sink.

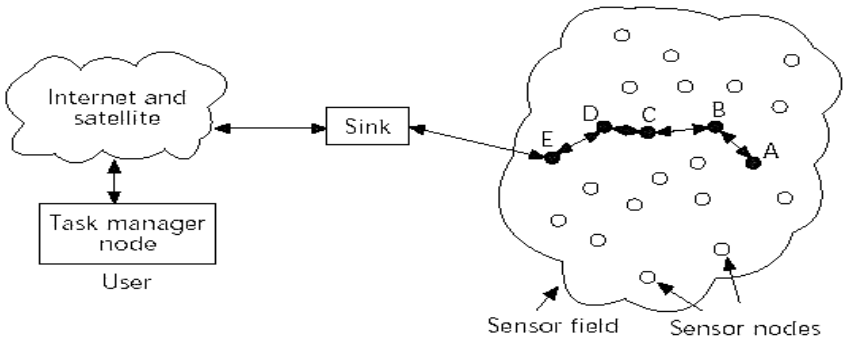

Figure 1: Wireless Sensor Network Architecture

The various components of sensor nodes are microcomputer, memory, transceiver and power source. The microcomputer can be used for processes and store the sensor output. The transceiver receives data from a

central point or computer and transmit data to another computer. WSN have wide range of applications like healthcare, military, agriculture, hospitality management, mobiles etc. To protect Wireless Sensor Network from the various weakness, the many security mechanisms like authentication, cryptography and security mechanism have been proposed but they cannot deal with providing security towards many attacks. These techniques are used to detect only the outsider attack but cannot detect insider attack. So, to detect the insider attack we need another type of detection techniques, known as IDS (Intrusion Detection System).

II. INTRUSION DETECTION SYSTEM

Intrusion is an unwanted activity in the system and it is totally harmful for system. The Intrusion Detection System [5,15] provide protection against the unwanted or unauthorized activity in the system. Intrusion Detection System is providing protection against both insider and outsider intrusion. But it will less effective against the insider intrusion. For example, a cryptographic mechanism provide protection against the outsider intrusion, but it will not effective against the insider intrusion. the purpose of intrusion detection process is reviewing, controlling, analysing and representing reports from the system and network activities [10]. IDSs are divided into three different techniques, including Misuse Based Detection Technique, Anomaly Based Detection Technique and Hybrid Based Technique.

A. Misuse Based Detection Technique

Misuse Based Detection Technique [5,14] is one of the commonly used method of Intrusion Detection. it is also known as signature based technique. The signature of known threats is stored in the system and when the threats matched with the signature then it finds the intrusion in the system. This technique is very effective for known threats and provide the alarm system to user if known threats are detected.

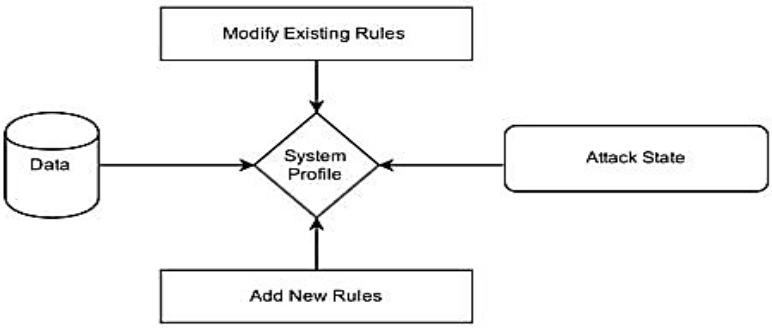

Figure 2 Misuse Based Detection Technique

B. Anomaly Based Detection Technique

Anomaly Detection overcomes the limitation of Misuse Based Detection technique. The Anomaly Based Detection Technique [9,14] is very effective for unknown threats in the system. However, in the Anomaly Based Detection technique the system will raise the alarm once the behaviour of the network traffic patterns does not match with its normal traffic patterns. The false positive rate is one the main disadvantage of Anomaly Based Detection Technique.

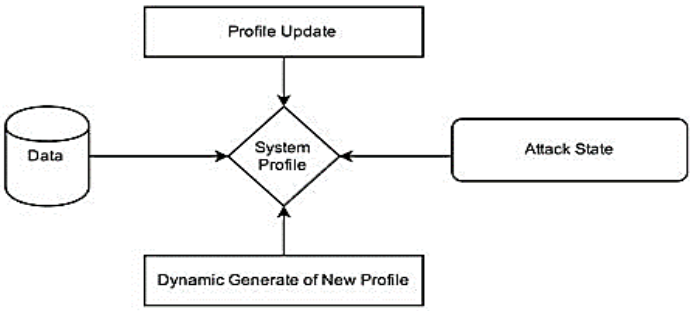

Figure 3 Anomaly Based Detection Technique

C. Hybrid Based Detection Technique

It is also known as Specification Based Technique. This technique is a combination of both Misuse Based Technique and Anomaly Based Technique. Both techniques have advantages and disadvantages. This technique combination of two detection modules, one for detecting the known attack and another for detecting the unknown attack [10]. But this hybrid technique is usually not favour in WSN as this consumes more resources and energy. this technique also contains three different modules it is classified as Analysis modules, Monitoring modules and Response modules.

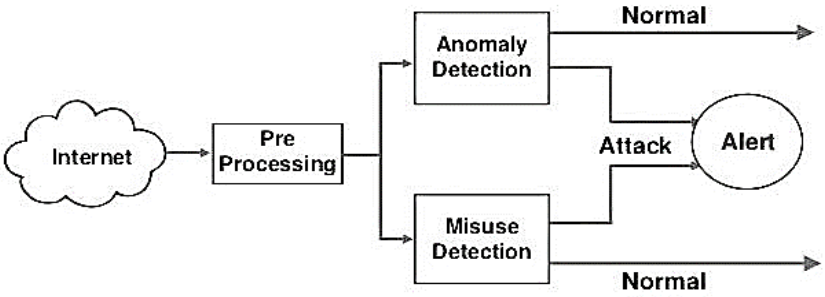

Figure 4 Hybrid Based Detection Technique

III. BLACK HOLE ATTACK

The Black Hole Attack [3] is one of the security threats in wireless sensor network. In the black hole attack, the malicious node acts as unwanted or false node in the network. It sends the false routing information but show that it has original route information. The black hole attack can increase the packet dropping chance and it is very hard to detect and prevent, a node which is called malicious node will absorb all the network traffic towards them and discard all the packet.

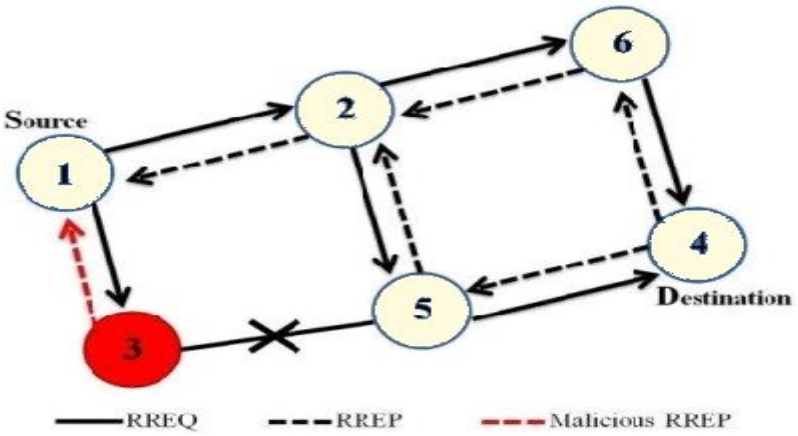

Figure 5 Black Hole Attack

In figure 5 the node 1 sends RREQ message to every nearby node. When RREQ message is received by malicious node, then it sends RREP message to source node. The Source node accepts the reply message from node 2 which is called malicious node and transfer packets. The black hole attack can be divided into two types, i.e. internal and external black hole attack. the internal attack occurs inside from the network. Its route from sender to receiver, showing in the figure 5 the external black hole attack occurs outside from the network.

IV. PROPOSED IDS TO DETECT THE ATTACK

The Algorithm and Flowchart of proposed IDS scheme represents the steps followed by the contributing nodes in the communication to identify the black hole attack in the nodes and to block the attacker nodes to provide the secure communication.

Algorithm:

```
For Each Node Blackhole=0;
Receive Reply (Packet Q) {
    If (BLACKHOLE=1 AND Q has pass in Route Table) {
        Select End_Point_Seq_No from routing table
            If (Q. End_Point_Seq_No > End_Point_Seq_No) {
                If (RREP Not Sent)
                Then Blackhole=1;
                ELSE
                    Update entry of Q in routing table
                    Unicast data packets to the route specified in RREP
                BLACKHOLE=0;
            }
            ELSE {
                Discard RREP
            }
    }
    ELSE {
        If (Q. End_Point_Seq_No >= Src_Seq_No) {
            Make entry of Q in routing table
        }
    ELSE {
```

Discard this RREP

}}}

Flowchart:

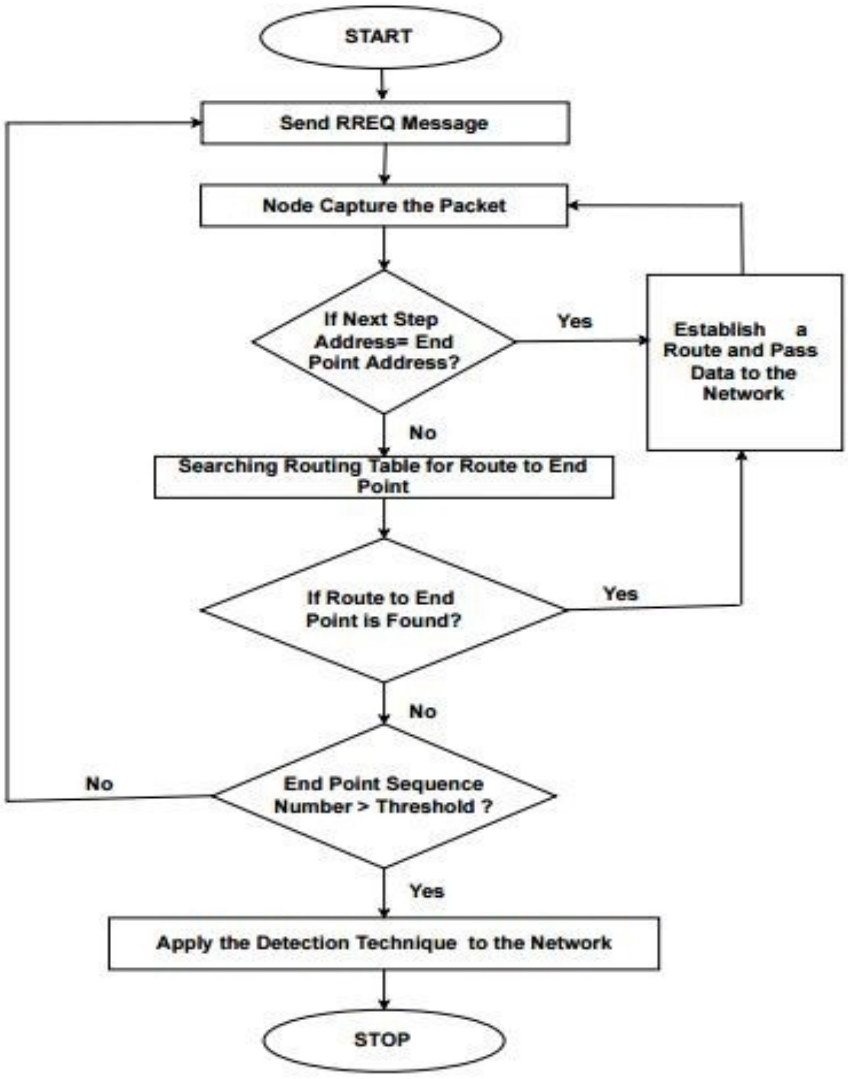

Figure 6 Proposed Flowchart

V. SIMULATION ENVIRONMENT

We used network Simulation OPNET Modeler 14.5 in our evaluation. The OPNET is a discrete event driven simulator. It simulates the network graphically and its graphical editors mirror the structure of actual networks and network components. The modeler uses object oriented modelling approach. The nodes and protocols are modelled as classes with inheritance and specialization.

The simulation parameters are given below in Table 1.

Table 1 Network Parameters

Parameters	Value
Simulator	OPNET 14.5
Traffic Type	Constant Bit Rate (CBR)
Simulation Area	1200*1200
Number of Nodes	120
Simulation Time	500 secs
Routing Protocol	OLSR
Hello Interval	2 secs
TC Interval	5 secs
Data Rate (bps)	11 Mbps

VI. PERFORMANCE PARAMETERS

The main aim of performance metrics should be introduced to estimate the required results. Following are the various performance metrics used for OLSR routing protocol to estimate the required results.

Throughput: Throughput indicates the how much useful data can be transmitted per unit time. It represents the total number of bits forward from wireless LAN layers to higher layers in all WLAN nodes of the network.
Network Load: Network load is increasing with respect to time period which is responsible for network errors.
Hello Traffic Sent: A hello message exchange between all neighbours nodes of OLSR protocols. A hello message mainly contains link state information.
Media Access Delay: Media Access Delay is the media transfer delay for multimedia and real time traffics data packets from sender to receivers.

VII. RESULTS

The simulation results are shown in this section in the form of graphs. Graphs show comparison between proposed IDS and existing IDS scheme. The six scenarios are run for 500 sec. and corresponding results are described in this section.

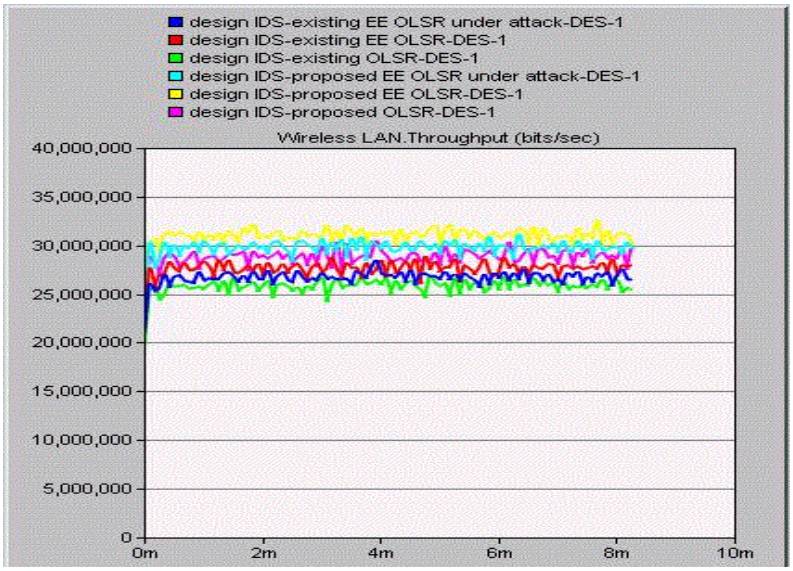

Figure 7 Throughput

Throughput is the rate of successful message delivery over a communication channel. The data these messages belong to may be delivered over physical or logical link, or it can pass through a certain network node. The Figure 7 show that maximum Throughput value for proposed EE-OLSR around 28,905,401.6 seconds. The results show that proposed EE-OLSR has more Throughput i.e. maximum packets are received at the receiver and has better performance.

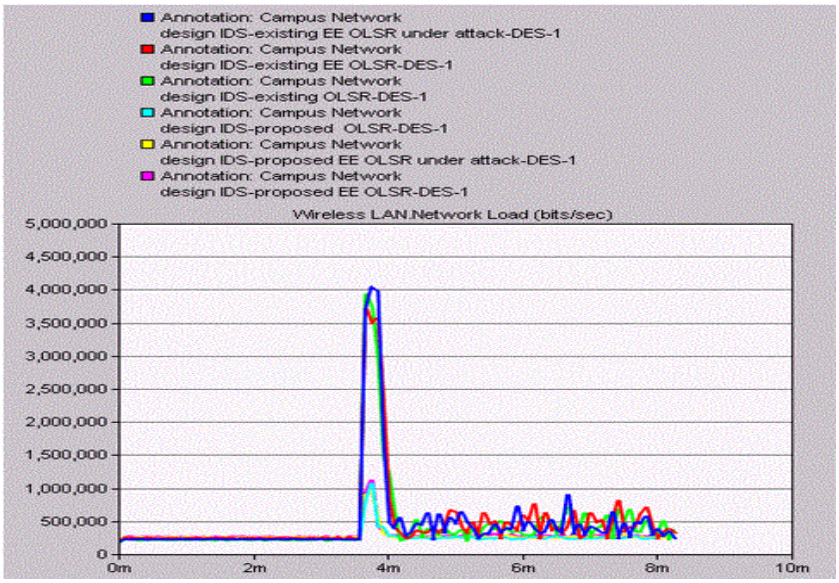

Figure 8 Network Load

Figure 8 shows the Network Load performance of proposed and existing IDS. As the number of malicious nodes increase the Network Load but taking the average value for all the nodes, the performance shows that the Network Load is reduced i.e. proposed EE-OLSR shows better results i.e. Network Load are higher for existing EE-OLSR under attack that is around 4,035,449.6 seconds but lower in proposed EE-OLSR that is around 1,130,675.2 seconds.

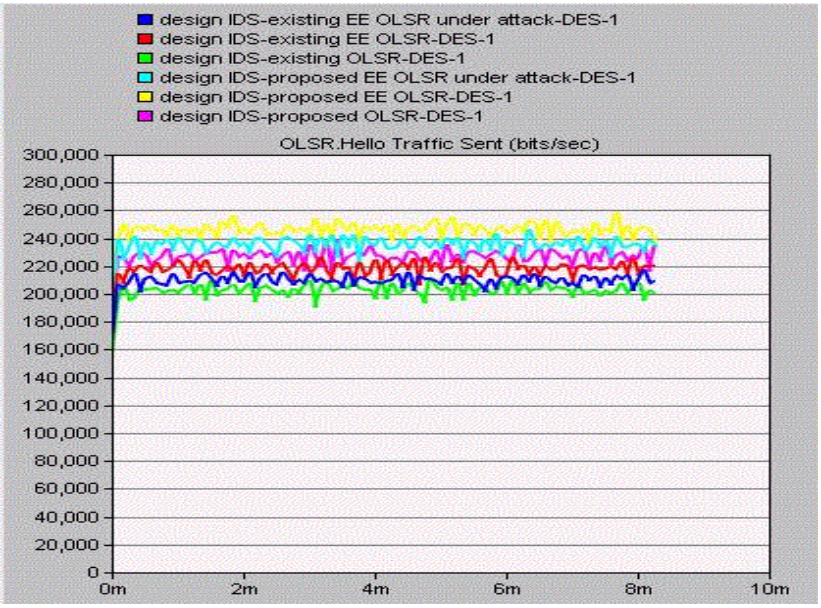

Figure 9 Hello Traffic Sent

Figure 9 shows Hello Traffic Sent, we can see that Hello Traffic Sent bits per second are higher in proposed IDS and smaller in existing IDS. The Hello Traffic Sent of EE-OLSR increase with rising number of sensor nodes but performance of EE-OLSR decreased when it is working under the attack situation i.e. Hello Traffic Sent are higher for proposed EE-OLSR that is around 226,802.2 seconds.

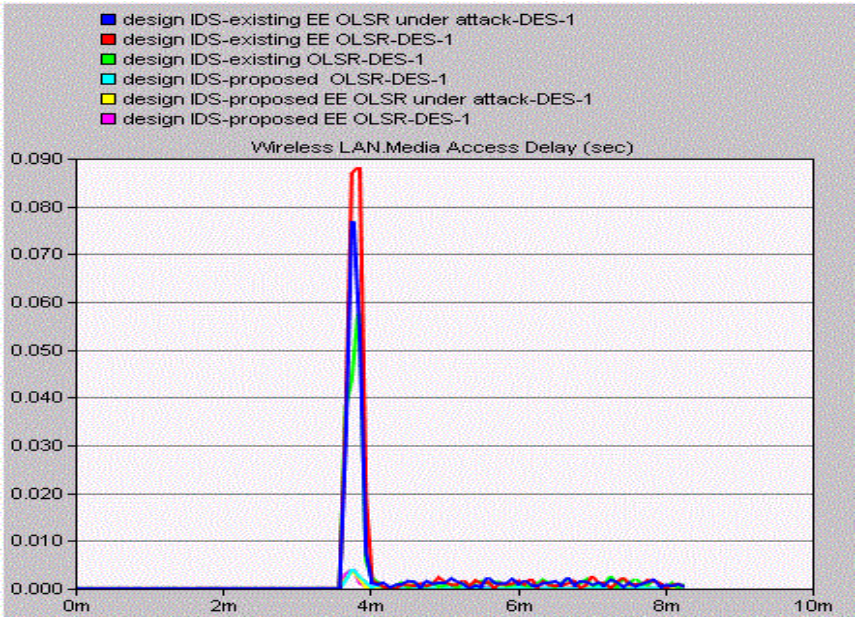

Figure 10 Media Access Delay

In Figure 10, we have plotted Media Access Delay which very important for multimedia and real time traffic; it is vital for any application where data is proccessed online. Media Access Delay is low for propossed EE-OLSR that is around 0.0041169 second. However Media Access Delay is higher for existing EE-OLSR under attack that is around 0.07691 seconds

VII. CONCLUSION

As security is the major issue in WSN. Any node can easily communicate the other node. The unwanted node is the main security threat that effects the performance of the routing protocols. In the existing work, a comparison of the routing protocols for WSN is discussed. Also, OLSR over Wireless Sensor Network is simulated with different topology changes. Even though, the black hole attack can be happening in the sensor nodes due to network issues for this reason we implement an Intrusion Detection System to detect the black hole attack on the sensor nodes. Detection of intruder in the sensor nodes is the main matter of concern. In this paper, we evaluated the four-performance measure i.e. Throughput, Network Load, Hello Traffic Sent and Media Access Delay with Mobility model.

In future work by applying some modern techniques such as genetic algorithm and fuzzy sets to reduce false positive rate and produce suitable results and implementing our proposed architecture on a simulator.

REFERENCES

[1] M.A. Matin and M.M. Islam, "Overview of Wireless Sensor Network" pp. 03-24, 2012.

[2] Kamaldeep Kaur and Parneet Kaur, "Wireless Sensor Network: Architecture, Design Issues and Applications" International Journal of Scientific Engineering and Research (IJSER) vol. 2 issue 11, pp. 2347-3878, November 2014.

[3] Padmalaya Nayak, V. Bhavani and B. Lavanya, "Impact of Black Hole and Sink Hole Attacks on Routing Protocols for WSN" International Journal of Computer Applications (IJCA) vol. 116, No. 4, pp. 42-46, April 2015.

[4] Abirami.K and Santhi.B, "Sybil attack in Wireless Sensor Network" International Journal of Engineering and Technology (IJET) vol. 5 No 2, Apr-May 2013.

[5] Manali Singh, Khushbu Babbar and Kusum Lata Jain, "A Survey on Intrusion Detection System in Wireless Sensor Networks" International Journal of Wireless Communications and Networking Technologies (IJWCNT) vol. 3, No. 3, Apr-May 2014.

[6] Keshav Goyal, Nidhi Gupta and Keshawanand Singh, "A Survey on Intrusion Detection in Wireless Sensor Networks" International Journal of Scientific Research Engineering & Technology (IJSRET) vol. 2, Issue 2, pp 113-126, May 2013.

[7] Amrit Pal Singh and Manik Deep Singh, "Analysis of Host-Based and Network-Based Intrusion Detection System" I.J. Computer Network and Information Security (IJCNIS) vol. 6, No. 8, pp. 41-47, August 2014.

[8] L. Sheeba, "A Brief survey on Intrusion Detection System for WSN" International Journal of Computer Trends and Technology (IJCTT) vol. 40, No. 3, October 2016.

[9] V. Jyothsna and V. V. Rama Prasad, "A Review of Anomaly based Intrusion Detection Systems" International Journal of Computer Applications (IJCA) vol. 28, No. 7, September 2011

[10] Megha Gupta, "Hybrid Intrusion Detection System: Technology and Development" International Journal of Computer Applications(IJCA) vol. 115, No. 9, April 2015.

[11] Hossein Jadidoleslamy, "A High-Level Architecture for Intrusion Detection on Heterogeneous Wireless Sensor Networks: Hierarchical, Scalable and Dynamic Reconfigurable" pp. 241-261, 2011.

[12] Djallel Eddine Boubiche and Azeddine Bilami, “Cross Layer Intrusion Detection System for Wireless Sensor Network” International Journal of Network Security & Its Applications (IJNSA) vol. 4, No. 2, March 2012.

[13] Alexandros Tsakountakis, Georgios Kambourakis and Stefanos Gritzalis, “Towards effective Wireless Intrusion Detection in IEEE 802.11i” Third International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Istanbul, pp 37-42, 2007.

[14] Piya Techateerawat and Andrew Jennings, “Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks” IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology Workshops, Hong Kong, pp 227-230, 2006.

[15] Md. Safiqul Islam, Razib Hayat Khan and Dewan Muhammad Bappy, “A Hierarchical Intrusion Detection System in Wireless Sensor Networks” International Journal of Computer Science and Network Security (IJCSNS), vol. 10, No. 8, August 2010.

[16] Paul Brutch and Calvin Ko, “Challenges in Intrusion Detection for Wireless Ad-hoc Networks” IEEE Proceedings of Workshop on Security and Assurance in Ad hoc Networks, pp 368 - 373, Jan. 2003.