IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Detection of Intrusion in Wireless Sensor Networks with Low Power Consumption

A. Saran Kumar[1], M. Sangeetha[2]

M.E. Student, CSE Department, Kumaraguru College Of Technology, Coimbatore, India[1,2]

Abstract: In a network or a system, any kind of unauthorized or unapproved activities are called Intrusions. An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network. An IDS inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. They act as the first line of defense for our computer systems. New intelligent Intrusion Detection Systems (IDSs) which are based on sophisticated algorithms with less power consumption rather than current signature-based detections are in demand. In this paper, we propose a solution using LEACH protocol to detect intrusion with low power consumption and also to increase the level of security. LEACH (Low Energy Adaptive Clustering Hierarchy) is one of the most interested techniques that offer an efficient way to minimize the power consumption in sensor networks to identify the intrusions. In Watchdog-LEACH, some nodes are considered as watchdogs and some changes are applied on LEACH protocol for intrusion detection. Watchdog-LEACH is able to protect against a wide range of attacks and it provides security and energy efficiency.

Keywords: IDS, Leach, AODV, Watch dogs.

I INTRODUCTION

Intrusion detection is needed in today's computing environment because it is impossible to keep pace with the current and potential threats and vulnerabilities in our computing systems. The environment is constantly evolving and changing fueled by new technology and the Internet.

To make matters worse, threats and vulnerabilities in this environment are also constantly evolving. Intrusion detection products are tools to assist in managing threats and vulnerabilities in this changing environment. In a worst-case scenario, an intrusion may cause production downtime, sabotage of critical information, theft of confidential information, cash, or other assets, or even negative public relations that may affect a company's stock price.

Intrusion detection products are tools that can assist in protecting a company from intrusion by expanding the options available to manage the risk from threats and vulnerabilities. Intrusion detection capabilities can help a company secure its information. The tool could be used to detect an intruder, identify and stop the intruder, support investigations to find out how the intruder got in, and stop the exploit from use by future intruders. The correction should be applied across the enterprise to all similar platforms. Intrusion detection products can become a very powerful tool in the information security practitioner's tool kit. Also, the intrusion detection products must consume less energy to detect detections as energy plays a great role in today's environment.

II LITERATURE SURVEY

2.1 EXISTING SYSTEM:

List clustering change (LCC) algorithm is proposed to minimize the frequency of cluster head change where cluster stability is the major consideration under certain circumstances. But, this algorithm is robust in an environment in which the network topology changes frequently and also consume high power to detect intrusion. It has low routing overhead and latency. However, the load distribution would be unfair for all nodes.

The lowest ID (LID) clustering algorithm is a 2-hop clustering algorithm. Here a node periodically broadcasts the list of nodes that it can hear (including itself). A node, which only hears the nodes with IDs higher than itself from the 1-hop neighborhood, declares itself as the cluster head. It then broadcasts its ID and cluster ID. A node that can hear two or more cluster heads is a gateway node, otherwise it is an ordinary node or a cluster head. In LID based greedy algorithms, a unique identity is assigned to each node and chooses the node with lowest identity as cluster head. The LID clustering algorithm is more stable in an environment in which the network topology changes frequently. The drawback of LID is that there may be quick power drainage of the cluster head node and Gateway nodes.

Highest-connectivity (HCN) clustering algorithm elects the node with the highest connectivity (degree) in a neighborhood as the cluster head. The connectivity of a node is the number of links to its 1-hop neighbors. HCN

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

and Lowest-ID (LID) are based on the Linked Cluster Algorithm. As compared to LID algorithm, HCN incurs a higher message overhead because more information about connectivity is exchanged. Thus, the throughput is low in HCN approach.

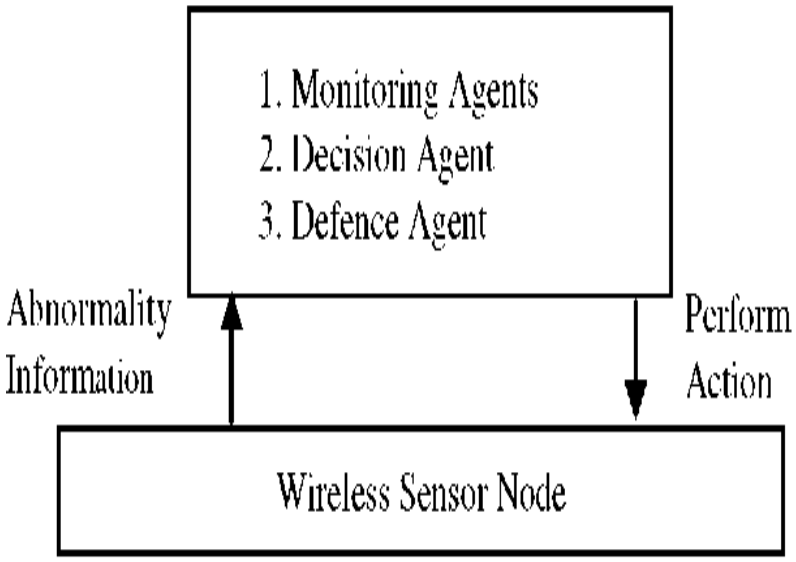
2.2 PROPOSED SYSTEM:

A new intelligent based intrusion detection system using LEACH protocol is proposed. The reason we need network protocol such as LEACH is due to the fact that a node in the network is no longer useful when its battery dies. This protocol allows us to space out the lifespan of the nodes, by using less energy for detecting intrusions. Also LEACH protocol uses stochastic cluster head selection algorithm. Depending on the network configuration an increase of network lifetime and its nodes by about 30 % can be accomplished.

III SYSTEM ARCHITECTURE

3.1 WIRELESS SENSOR NETWORK:

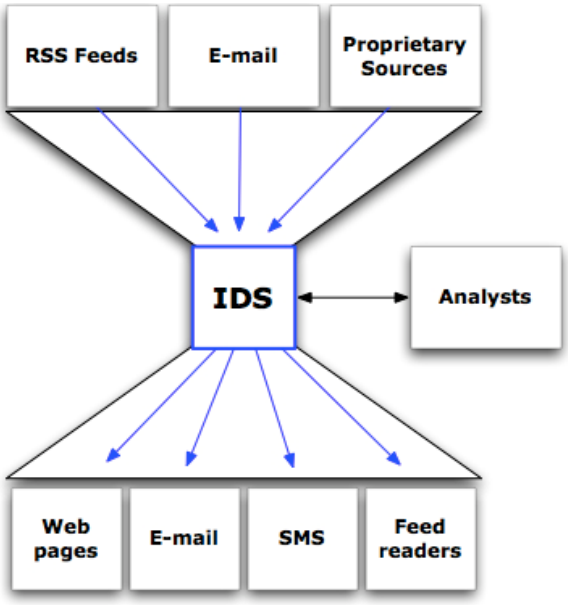
A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor all activities of the system and cooperatively pass their data through the network to a main location. The more modern networks are bi-directional, also enabling control of sensor activity. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size.



3.2. INTRUSION DETECTION SYSTEM:

An IDS is a security countermeasure. It monitors things looking for signs of intruders. The most important activity of the system is intrusion detection. IDS monitor packets on a network and compare them with a database of signatures or attributes for known malicious threats. This is similar to the way in which most antivirus systems detect viruses.

An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (virus, worms, and Trojan horses). The IDS that is being designed must satisfy the requirements like: must not introduce new weakness to the system, should be transparent, should be reliable, minimize false positives and false positives in the detection phase, must run continuously.



IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

3.3 TYPES OF IDS:

- Network based intrusion detection system (NIDS)
- Host-based intrusion detection system (HIDS)
- Protocol-based intrusion detection system (PIDS)
- Application protocol-based intrusion detection system (APIDS)

IV FUNCTIONAL DIAGRAM

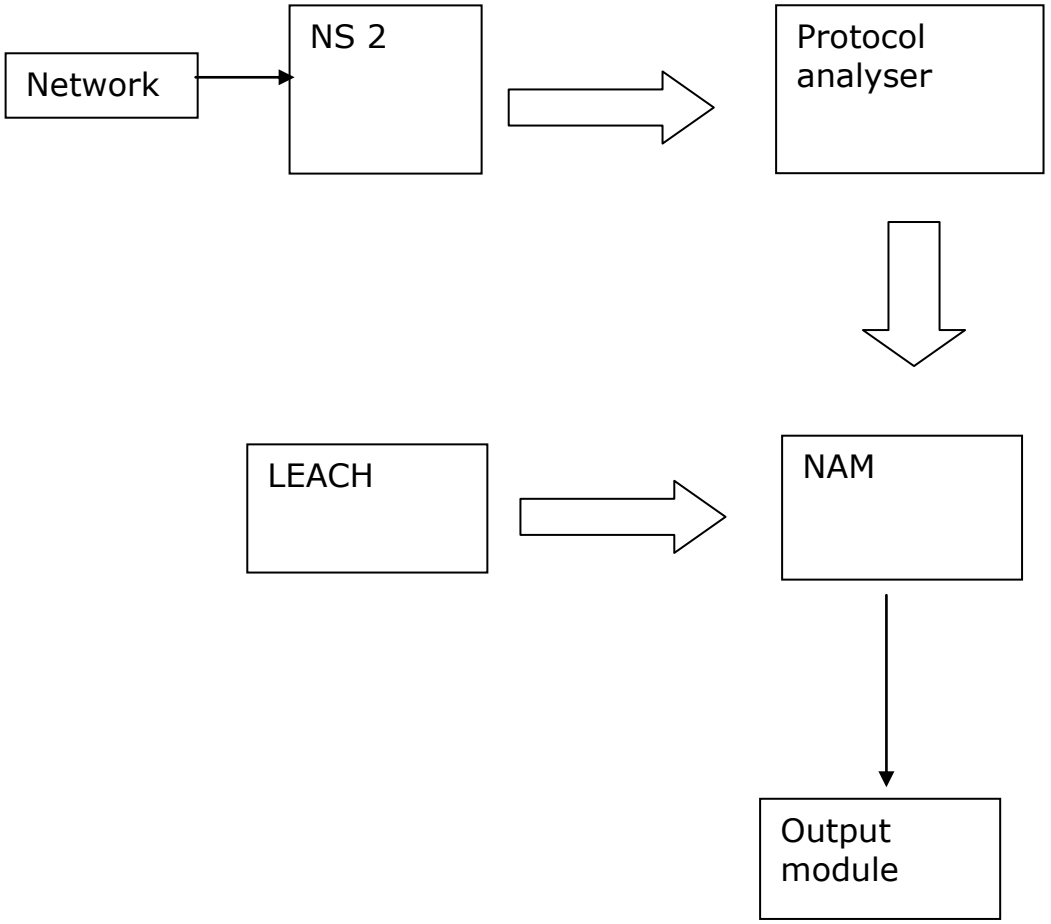


Fig. 4.1. Function Diagram for Intrusion Detection System

4.1 LEACH PROTOCOL:

LEACH is a hierarchical protocol in which most nodes transmit to cluster heads, and the cluster heads aggregate and compress the data and forward it to the base station (sink). Each node uses a stochastic algorithm at each round to determine whether it will become a cluster head in this round. LEACH assumes that each node has a radio powerful enough to directly reach the base station or the nearest cluster head, but that using this radio at full power all the time would waste energy. The operation of LEACH is split into two phases: set-up and steady.

During the set-up phase, each sensor node chooses a random number between 0 and 1. If this is lower than the threshold for node n, T(n), the sensor node becomes a cluster-head. The threshold T (n) is calculated as:

$$T(n) = P/(1- P*(r \bmod(1/P))) \quad \text{for all n belongs G}$$
$$T(n) = 0 \quad \text{for all n not belongs to G}$$

where P as the cluster-head probability, r as the number of the current round and G as the set of nodes that have not been cluster-heads in the last 1/P rounds. Nodes that have been cluster heads cannot become cluster heads again for P rounds, where P is the desired percentage of cluster heads. Thereafter, each node has a 1/P probability of becoming a cluster head in each round. At the end of each round, each node that is not a cluster head selects the closest cluster head and joins that cluster. The cluster head then creates a schedule for each node in its cluster to transmit its data.

Nodes that have been cluster heads cannot become cluster heads again for P rounds, where P is the desired percentage of cluster heads. Thereafter, each node has a 1/P probability of becoming a cluster head in each round. At the end of each round, each node that is not a cluster head selects the closest cluster head and joins that cluster. The cluster head then creates a schedule for each node in its cluster to transmit its data.

The steady phase is of longer duration in order to minimize the overhead of cluster formation. During the

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

steady phase, data transmission takes place based on the TDMA schedule, and the cluster-heads perform data aggregation/fusion through local computation. The BS receives only aggregated data from cluster heads, leading to energy conservation. After a certain period of time in the steady phase, cluster-heads are selected again through the set-up phase.

For a micro sensor network we make the following assumptions: (i) The base station (BS) is located far from the sensors and immobile. (ii) All nodes in the network are homogenous and energy-constrained. (iii) All nodes are able to reach BS. (iv) Nodes have no location information. (v) Symmetric propagation channel. (vi) Cluster-heads perform data compression.

The energy needed for the transmission of one bit of data from node u to node v, is the same as to transmit one bit from v to u (symmetric propagation channel). Cluster-heads collect n k-bit messages from n adjacent nodes and compress the data to cn k-bit messages which are transmitted to the BS, with c $\leq$1 as the compression coefficient.

4.2 WATCH DOGS:

Watchdogs are the basis of inherent Intrusion Detection Systems. They have the advantage of using only local information and therefore, they are robust to most of the attacks. Intrusion detection systems (IDS) aim at monitoring the activity of the nodes in the network in order to detect misbehavior. A basic module in the construction of such systems is the watchdog, a component used for the detection of selfish nodes and malicious attackers. When a node forwards a packet, the watchdog ensures that the next node in the path also forwards the packet. When a node forwards a packet, the watchdog set in the node ensures that the next node in the path also forwards the packet. The watchdog does this by listening to all nodes within transmission range promiscuously. If the next node does not forward the packet then it is tagged as misbehaved. A match confirms that the packet has been successfully forwarded, causing the neighbor's trustworthiness to be increased. If a packet is not forwarded within a timeout period, then a failure tally for the node responsible for forwarding the packet is incremented. If this tally exceeds a predetermined threshold, then the node is termed as malicious.

V SNAPSHOTS

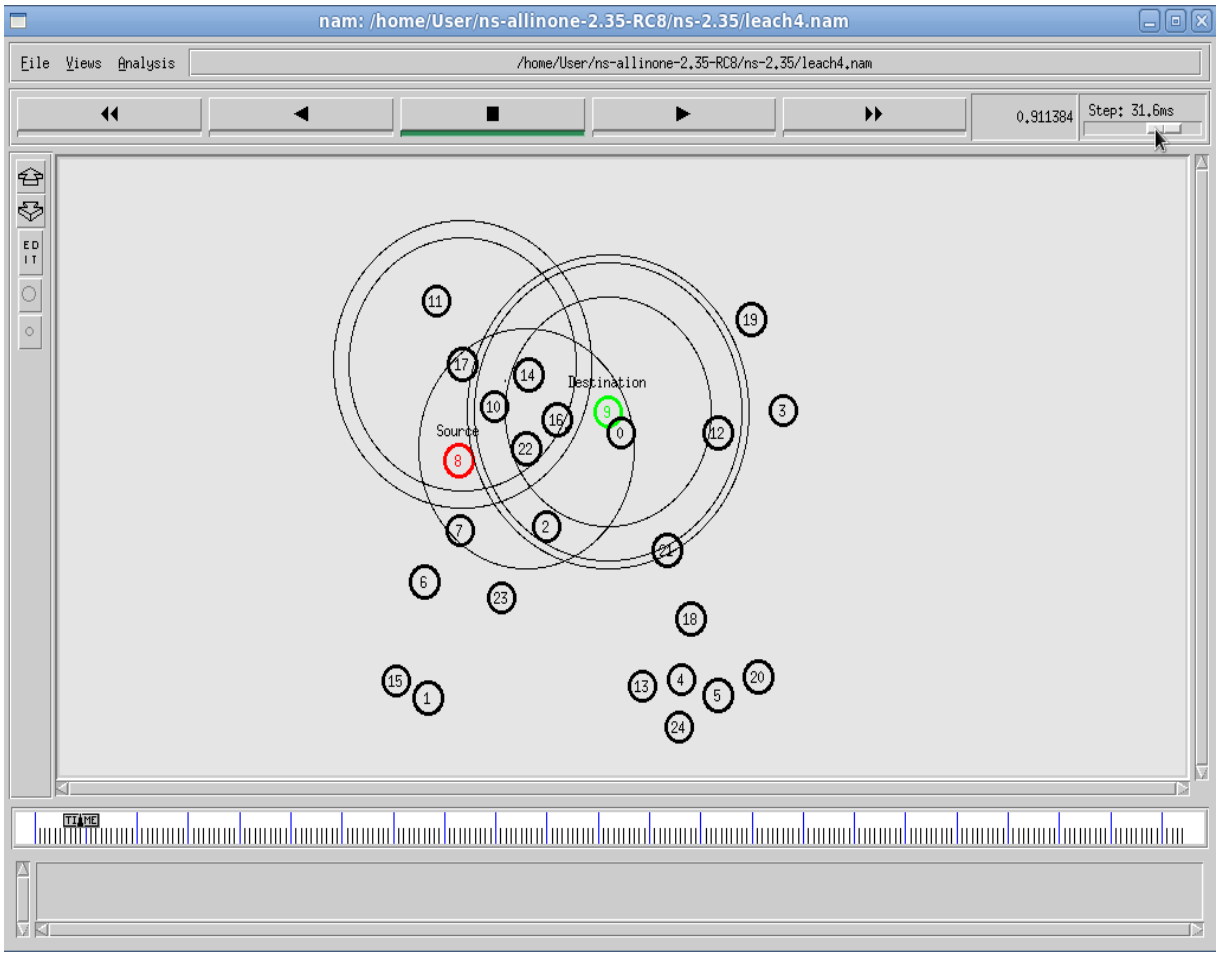


Fig.5.1 WSN transmission

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

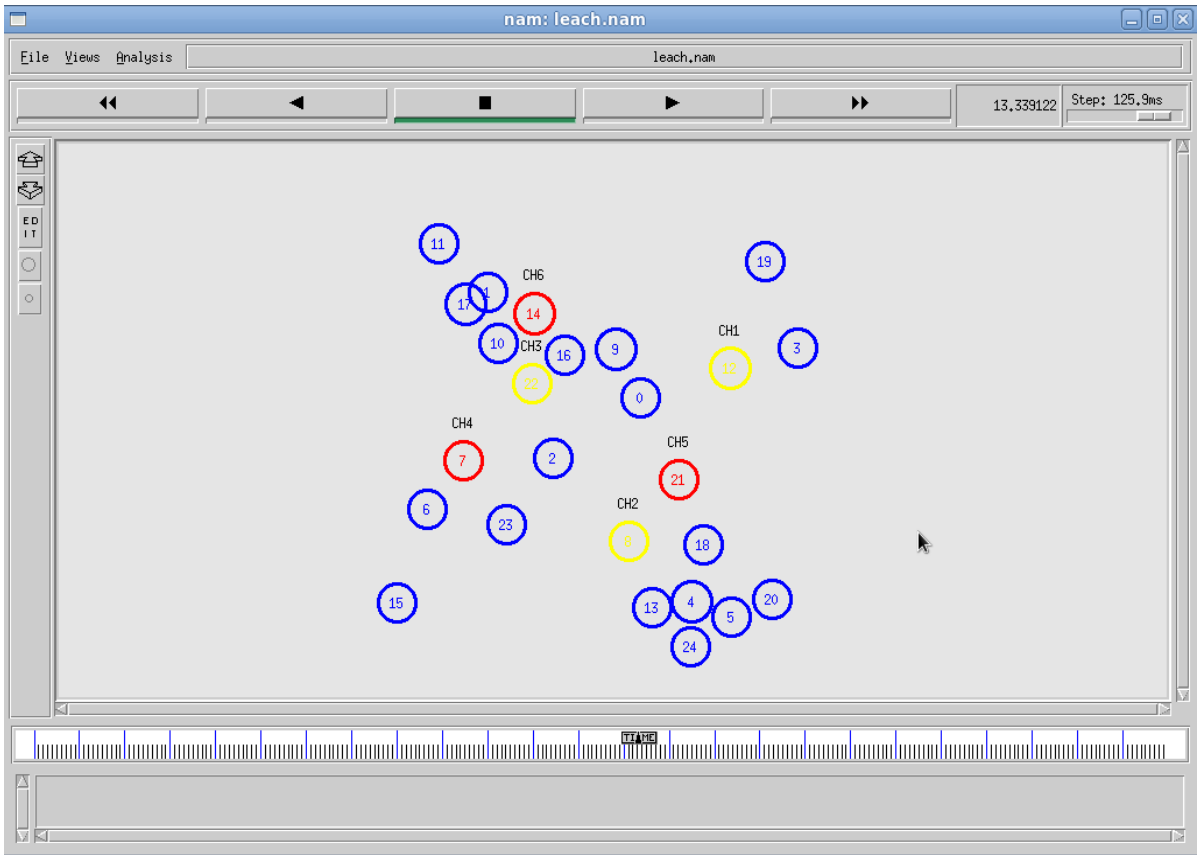


Fig. 5.2 Cluster head selection

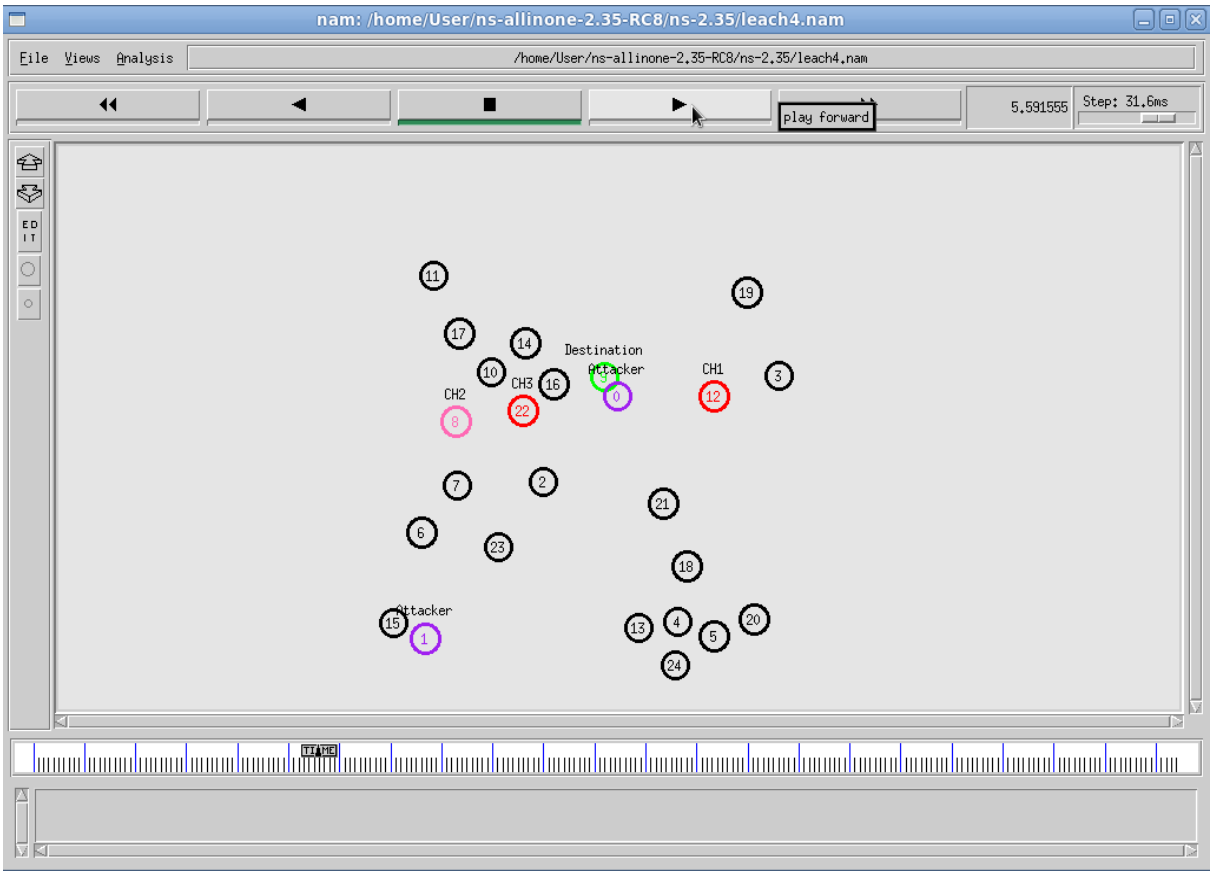


Fig. 5.3 Detection of intrusions by watch dog

DOI 10.17148/IJARCCE.2017.6236

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

Number of nodes	LEACH	AODV
25	0.9254	0.3
50	0.8363	0.5
75	0.8065	0.6
100	0.7876	0.7
200	0.6543	0.9
300	0.4214	1.4

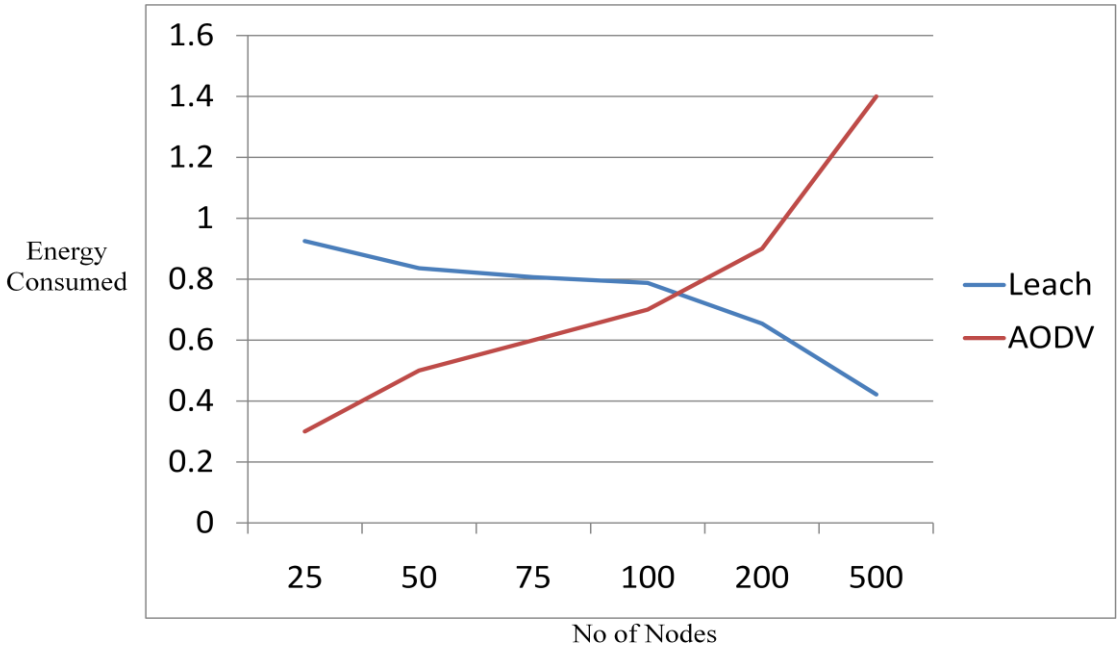


Fig. 5.4 Graph showing energy consumption for different number of nodes

VI CONCLUSION AND FUTURE ENHANCEMENT

The main goal of this project was to detect live intrusions. Detecting intrusions with low power consumption plays a great role in today's environment. In future, improvements can be done to detect intrusions with very less power and measures can be taken to optimize intrusions and also to prevent intrusions in the wireless networks as data exchanges are taking place through wireless environments in today's environment.

REFERENCES

[1] Tapolina Bhattasali, Rituparna chaki," A Survey of Recent Intrusion Detection Systems for Wireless Sensor Network", Advances in network security and applications, Springer, 2011.
[2] http://www.ACSIJ.org .
[3] A journal on "Energy efficient intrusion detection system for WSN" by Syeda Gauhar Fatima, Dr. Syed Abdul Sattar, Dr. K. Anita Sheela, December 2012.
[4] Aleksandar Lazarevic, Aysel Ozgur, "A Comparative Study of Anomaly Detect Schemes in Network Intrusion Detection", Department of Computer Science, University of Minnesota.
[5] R. Min, M. Bhardwaj, S. Cho, E. Shih, A. Sinha, A. Wang, A. Chandrakasan, "Low-power wireless sensor networks", VLSI Design 2001, Invited Paper, Bangalore, January 2001.
[6] Sinha, A. Chandrakasan, „Dynamic power management in wireless sensor networks", IEEE Design & Test of Computers, March-April 2001, S. 62-74.
[7] L. Zhong, R. Shah, C. Guo, J. Rabaey, "An ultra low power and distributed access protocol for broadband wireless sensor networks", IEEE Broadband Wireless Summit, Las Vegas, May 2001.
[8] V. Rodoplu, T. H. Meng, "Minimum energy mobile wireless networks", IEEE Jour. Selected Areas Comm., August 1999, pp. 1333-1344.
[9] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, Energy-efficient communication protocol for wireless microsensor networks", Proceedings of the 33rd International Conference on System Sciences (HICSS '00), January 2000.