MULTI LAYER INTRUSION DETECTION AND PREVENTION IN WSNs USING SELF HEALING MODULE

M. VIDHYA	V. SRINIVASAN	R.SUDHA
II M.E. (CSE) Department of Computer Science & Engineering, Annamalai University Annamalainagar – 608 002, Tamil Nadu, India.	Professor and Head Department of Computer Science & Engineering, Annamalai University Annamalainagar – 608 002, Tamil Nadu, India.	M.E(CSE),Web Designer Department of MCA AVC College of Engg, Mayiladuthurai-609305 Tamil Nadu, India.

ABSTRACT

Wireless sensor network (WSN) have been vulnerable to various kinds of security threads due to open wireless medium so intrusion detection system (IDS) is best solution for that and it can effectively detect different types of intrusion.IDS identifying attack efficiently but it cannot able to any fixing the action. In this paper we propose multi layer intrusion detection and prevention using self healing algorithm, which responsible of detecting and preventing the network from attackers.

Keywords: **wireless sensor network (WSN), intrusion detection systems (IDSs), Cross Layer Intrusion Detection Agent (CLIDA), Security, Self healing module, Self healing algorithm.**

I.INTRODUCTION

Wireless Sensor Networks (WSNs) have been collected of sensor nodes and sinks. Sensor nodes are having the power of self-healing and self-organizing. They have been decentralized and distributed in environment where information transmitted through multi hop intermediate nodes. The basic objective of a sensor node is to gather information from its surrounding atmosphere and convey to the sink [1]. WSNs have several applications and are used in situation such as detecting changed climate, monitoring atmosphere and environment, and various other surveillance and military applications. Regularly sensor nodes are deployed in areas where wired connections are not possible. WSNs are implemented in physical cruel and intimidating situation where nodes are always exposed to physical security risks damages. Moreover, self-organizing environment, low down battery power supply, restricted bandwidth support, distributed functions using open wireless medium, multi hop traffic forwarding, and dependency on other nodes are such characteristics of sensor networks that expose it to a lot of security attacks at all layers of the OSI model.

Intrusion detection systems (IDSs) process of discovering, analyzing and reporting an illegal network [2]. IDS can play important role in detecting and preventing security attacks. An Intrusion Detection System is used to detect several types of malicious behavior that can compromise the security and trust of mainframe. Our aim is, to avoid the contact and retain path of the intruder's challenges and intrusions. An IDS is a mechanism to detect malicious activities. The primary functions of IDS are to monitor users' activities and network behavior at different layers [3].

II. RELATED WORK

In this section we are going to discuss about existing techniques are,

a. Anomaly –based IDS*:* Anomaly IDS is appropriate for small-sized WSNs where few nodes communicate with the base station have been discussed in [4] .It can detect novel attacks and cannot detect well-known attacks. It's lightweight in nature however they can create a more false alarms.

b. Signature based IDS*:* Signature IDS is appropriate for relatively large sized WSNs, where more security threats and attacks can compromise network operations. It's required more resources and computations as compared to anomaly-based IDS. It can detect well-known attacks and cannot detect the novel attacks [5].

c. Hybrid IDSs*:* Hybrid IDSs is appropriate for large and sustainable WSNs. It have combination of both anomaly-based and signature-based IDS, so it can detect novel and existing attacks but required more resources and computations [6].

ISSN: 2278 – 7798

d. Cross layer IDS: Cross layer IDS only can detect the multi layer attacks and to breaks the traditional layer rules but it's consume the more energy [7].

III. Security in WSNs

Security attacks against WSNs can be classified as active and passive [8]. Passive attacks are hard to detect and easy to prevent. Active attacks are easy to detect and hard to prevent [9].

The security goals are classified into two goals: main and secondary [10, 11].

Main goals

- Confidentiality
- availability,
- integrity and
- Authentication.

Secondary goal

- Self-organization,
- secure localization,
- Time synchronization and
- Resilience to attacks

IV.PROPOSED WORK

In this section, present proposed work of Multi layer intrusion detection and prevention [12] using self healing algorithm. The function of intrusion detection system is to detect intruders while they try to communicate with the network node. Fig. 1shows the details of block diagram of proposed work.

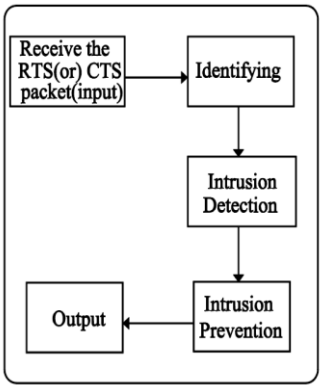

Fig. 1 Block diagram of proposed work.

A. INTRUSION DETECTION AT LAYERS

When RTS or CTS packets are received, IDS check if it's one of neighbor node in the routing table using the cross layer intrusion detection agent (CLIDA).Its containing the certain monitor nodes which responsible of checking their neighbor nodes and discover the intruder

CLIDA Architecture: CLIDA is the entity via which the layers and applications communicate. It's including two parts which are interaction interface and cross-layer data module. Fig. 2 shows the CLIDA Architecture and these details are illustrate in sections 1 and 2.

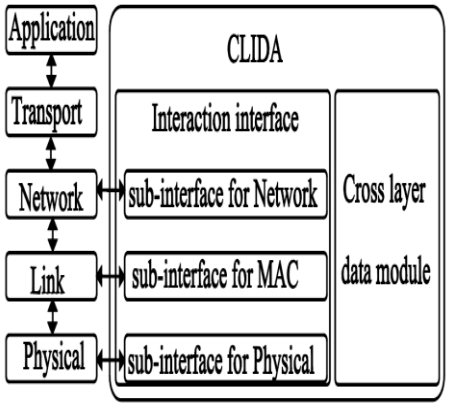

Fig. 2 Architecture of CLIDA

1) ***Interaction interface:*** It's making easy the communication between the layers and their functions on the one side and the CLIDA agent on the other side. Its main objective is the management of sub-interfaces which provide access to the layers. Every sub interface describes technique for reading and writing to ease the management of limits of the related protocol. Through these techniques have been made the collection and / or updating data i.e. calculated RSSI, direction-finding board.

2) Cross-layer data module: The Cross-layer data module corresponds to data to make them rapidly accessible by all layer protocols. This module provided data's are the origin of any Cross-layer adaptation and optimization and also maintaining up to date data via Cross layer interaction interfaces.

- ***Intrusion detection at network layer:*** To check the existence of the transmitting node in the routing table. If it's no means then lunch the intruder alert.

ISSN: 2278 – 7798

- ***Intrusion detection at MAC layer:*** to find the source of the packet that will be received by routing information. The routing information uses the hop count as metric. If it's no means then lunch the intruder alert.
- ***Intrusion detection at physical layer:*** The authenticity of intruder node will be checked by measuring its RSSI *(*Received Signal Strength Indicator) value. RSSI represents the entire received power. The received power P_r is represented as in eq. (1)

$$P_r=P_t*(1/d)^n \quad (1)$$

Here, P_r - receiving power, P_t - transmitted power, d-Distance between sender and receiver node n - Transmission factor whose value depends on the propagation environment.

B. INTRUSION PREVENTION

An intrusion detection system recognizing the attacks efficiently but it couldn't able to do any fixing action. In later than IDS, introduces the self healing module is shown in Fig.3.

Self healing module: It able to fixing the network by using self healing algorithm [13] is shown in Fig.4.

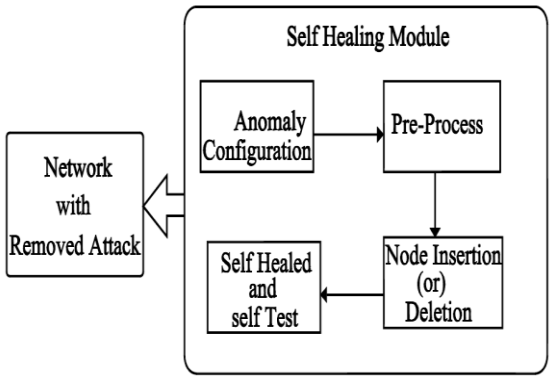

Fig. 3 Self healing module

Steps:

- To identify the anomaly configuration.
- Pre-processing.
- Feature extraction.
- Self healing test.

1) Anomaly configuration: Anomaly-based intrusion protection devices work by identifying network activity that is out of the ordinary and unexpected, such as zero-day hacker attacks. Fitting and configuring a system that will recognize unexpected activity requires an understanding of the activity that is expected. Network is configured using cross layer based intrusion detection system. Through this any attacks in the network can be monitored.

2) Pre-processing: Our aim is to reduce the power consumption in resource constrained devices such as wireless sensors. We reduce the noise level by pre-processing inside the sensor node then send a reduced sampled data to the Base Station (BS). Input data cleaning by removing noise and incomplete data is proposed. Unwanted parameters like noise and incomplete data makes the task of intrusion detection difficult. It increases overlapping behaviour of normal and intrusion data.

3) Feature extraction: An exchange message with neighbour nodes and those messages are containing information about route regeneration. It's used to reduce the false positive rate and increasing efficiency of detection rates.

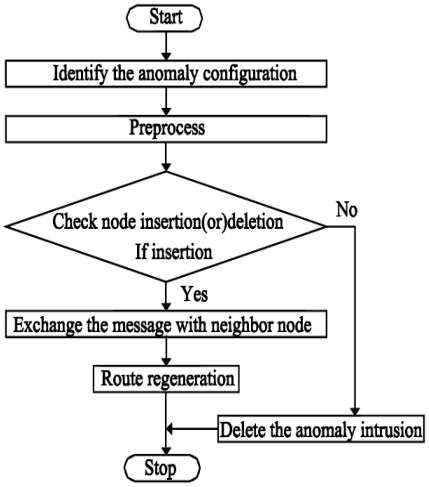

Fig. 4 Self healing algorithm.

V. RESULT AND DISCUSSION

Analysis of intrusion detection is executed by using the network simulator NS2. In this execution, our simulated model is built on 50 nodes spread randomly on a square surface is shown in Fig.5

First node is a Base Station (BS) which duty of forming the cluster and election of Cluster Head

ISSN: 2278 – 7798

(CH) which has greatest energy reserve in the cluster [14].

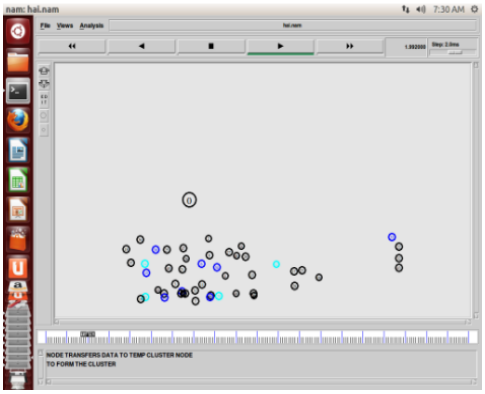

Fig.5 Node Creation

An establishment of chains of node depends on routing information sent by all networks then all the network nodes will broadcast gathered information to their CH via the chain of neighbouring nodes, Then CHs will be take the responsibility of transmitting received information directly to the BS. Fig.6 is shows that result.

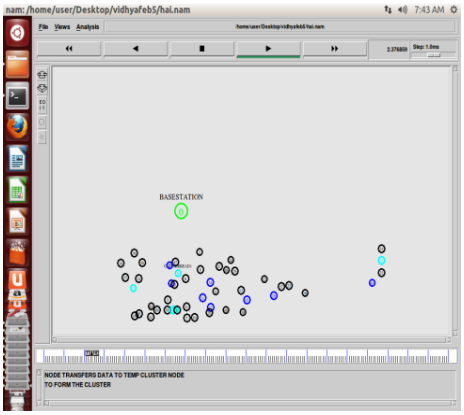

Fig.6 Cluster Formation

During the transaction the intruder node tries to play the role of CH role in order to make sinkhole attack [15] which is to lure traffic a compromised node in that case IDS containing monitor which responsible of monitoring their neighbour and find intruder and also they have eavesdrop to the communication in their radio range and use the buffer which is store to precise communication ground that might be helpful for IDS running with sensor nodes. Thus the intrusion will be detected and corrupted. In addition data will not be sent, connection will not be established and also an anomaly alarm will be report to BS .These are shown in figures (Fig. 7 and 8)

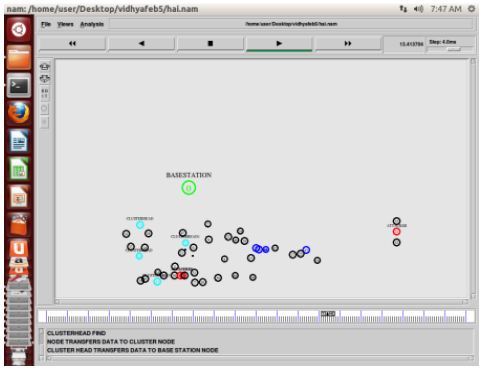

Fig.7 Node Transmission

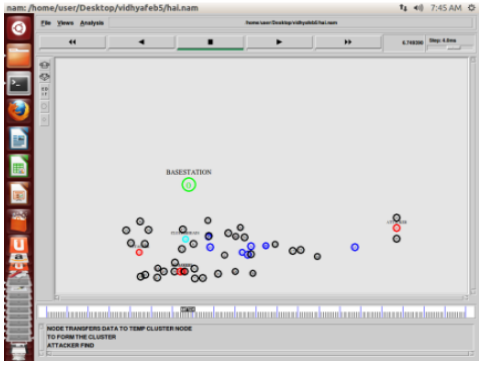

Fig.8 attacker nodes are detected and prevented

VI.PERFORMENCE ANALYSIS

Initially we calculated the number of intruder nodes detected during simulation progresses. Let us assume that attacker nodes goal and attack randomly network nodes after being in random time period and then send RTS packet to each tow frame time. The Fig. 9 shows that result.

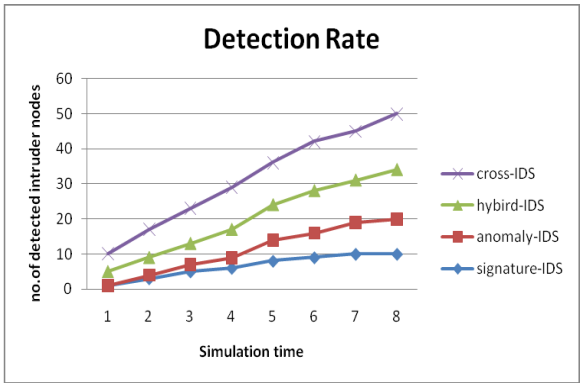

Fig. 9 Number of detected intruder nodes v/s simulation time

ISSN: 2278 – 7798

The possibility of detection of an intruder, P_{Det} based on two aspects: no. of attacked nodes in a cluster and likelihood of a missed detection of an attacked node. The number of nodes attacked is given as Z. In the proposed method the intruder nodes are not only detected if the compromised nodes don't accept any packet from the malicious node. Then the likelihood of a missed detection is equivalent to the likelihood of a collision occurring in a transmission link $P_{Col.}$

Binomial rule in eq. (2)

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \qquad (2)$$

By using the Binomial rule we can define the possibility of identifying an intruder as in eq. (3)

$$P_{Det} = \binom{Z}{1} (1 - P_{col}) P_{col}^{Z-1} \qquad (3)$$

Basing on equation 4 we can calculate the possibility of identifying M intruder in the network in eq. (4)

$$P_{Det} = \binom{Z}{M} (1 - P_{col})^M P_{col}^{Z-M} \qquad (4)$$

The whole network can identify the attackers and the possibility of identifying augments gradually with the expansion of the number of attacked nodes and the declining of collusion amount. Let us consider the attacker node attacks all nodes within its communication range. Then the average number of attacked node by an intruder can be equal to eq. (5)

$$Z = (N-1)\, \pi\, r^2/v \qquad (5)$$

Where: v is the area of the region, N is the no. of nodes in that region and r is the intruder transmission radius.

The proposed IDS are energy efficient. To approximate the total energy consumed by our IDS, for that calculate the consumed energy of IDS on each attacked node in eq. (6)

$$EC_i = E_{rx} + E_p + E_{sx} \qquad (6)$$

Where: EC_i is the energy consumed to identify the intrusion node i, E_{rx} is receiving of packet from intruder, E_p is the processing of intruder detection and E_{sx} is the sending the alarm message. After that, the total energy consumed by our IDS to protect the network from M attacker (j) nodes is indistinguishable to eq. (7)

$$Energy\_IDS = \sum_{j=0}^{j=M} \sum_{i=0}^{i=Z} ERi \qquad (7)$$

We can reduce the unnecessary active node which helps us to reduce the energy consumption.Fig.10 shows the result.

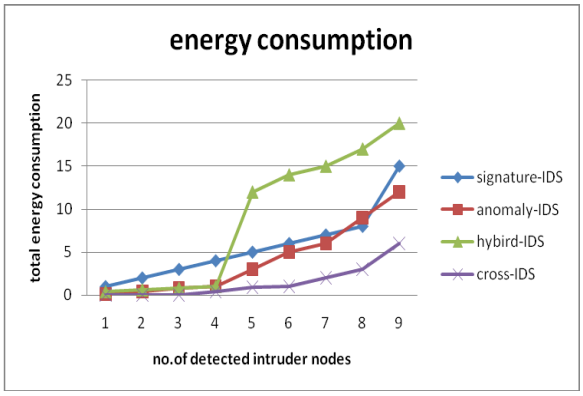

Fig. 10 Energy Consumption v/s the no. of detected intruder

VII. CONCLUSION

While designing a security mechanism, we should consider the some degrees of resources of WSNs. Anomaly-based IDSs are trivial in nature; still they are generating more fake alarm. Signature-based IDSs are appropriate for comparatively large-sized WSNs; still they have some expenses such as updating and inserting new signatures. Our main objective is security, so our proposed multi layer intrusion detection system dedicated for wireless sensor networks. Our approach is to develop single cross layer intrusion detection system that operates on dissimilar layers of the OSI model and to identify dissimilar types of attacks on various layers of the OSI model. The simulation results demonstrate the performance provided by our IDS in terms of detecting and preventing the various intrusion attacks.

REFERENCES

[1] Culler, D. E and Hong, W., "Wireless Sensor Networks", Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[2] Onat,I and A, Miri), "An intrusion detection system for wireless sensor networks," In Proceeding of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications , Vol. 3, Montreal, Canada, pp. 253–259,2005.

[3] Ioannis Krontiris, Tassos Dimitriou, and Felix C. Freiling., "Towards intrusion detection in wireless

ISSN: 2278 – 7798

sensor networks," In Proceedings of the 13th European Wireless Conference, 2007.

[4] Bhuse, V and A. Gupta., "Anomaly intrusion detection in wireless sensor networks," Journal of High Speed Networks, Vol. 15, No. 1, pp. 33–51,2006.

[5] Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad, "Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks", IEEE Sensors Journal, Vol. 12, No. 10, October 2012

[6]. K.Q. Yan, S.C. Wang, C.W. Liu, "A Hybrid Intrusion Detection System of Cluster-based WirelessSensor Networks", Proceedings of the International Multi Conference of Engineers and Computer Scientists 2009, Vol IIMECS 2009, Hong Kong (March 18 - 20, 2009).

[7]Mingbo Xiao,Xudong Wang,Guangsong Yang, "Cross-Layer Design for the Security of Wireless Sensor Networks," Proceedings of the 6th World Congress on Intelligent Control and Automation , June 21 - 23, Dalian, China, 2006.

[8] Padmavathi ,G and D, Shanmugapriya., "A survey of attacks, security mechanisms and challenges in wireless sensor networks," International Journal of Computer Science and Information Security, vol. 4, no. 2, 2009.

[9] Camtepe,S and B. Yener., "Key distribution mechanisms for wireless sensor networks: a survey," Rensselaer Polytechnic Institute, Troy, New York, Technical Report 05-07, 2005.

[10] Dimitriou, T and I. Krontiris.,(2006) "Security in Sensor Networks," CRC Press, ch. k Processing in Sensor Networks, pp. 275–290, 2006.

[11] Ganeriwal. S, S. Capkun, C.-C. Han, and M. Srivastava., "Secure time synchronization service for sensor networks," in Proceedings of the 4th ACM workshop on Wireless security (WiSe '05), pp. 97–106, 2005.

[12] Su, C.C, K.M. Chang, Y.H. Kue, and M.F. Horng., "The new intrusion prevention and detection approaches for clustering-based sensor networks," in Proceedings of 2005 IEEE Wireless Communications and Networking Conference (WCNC'05), Vol. 4, New Orleans, L.A.,pp. 1927-1932, 2005.

[13] Jothilakshimi, K, G. Usha, Dr.S.Bose., " A Framework of cross layer based anomaly intrusion detection and self healing model for MANET,"in Proceeding of International Conference on Recent Trends in Information Technology(ICRTIT),pp. 429-433.2013.

[14] Boubiche ,D, A.Bilami., "HEEP (Hybrid Energy Efficiency Protocol) Based on Chain Clustering", Int. J. Sensor Networks, Volume 10 Issue 1/2, pp. 25 – 35, 2011.

[15] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos.,"Intrusion detection of sinkhole attacks in wireless sensor networks. In Algorithmic Aspects of Wireless Sensor Networks," Vol.4837, pp. 150–161. Springer Berlin / Heidelberg, 2008.

ISSN: 2278 – 7798