Engineering and Scientific International Journal (ESIJ)
Volume 4, Issue 1, January – March 2017
ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Cross Layer Intrusion Detection System in WSNs using Self Rejuvenating Module

M.Vidhya[#1], A.Irudaya paul raj Vinod[*2], A.Porselvi[*3]
[1,2,3]Asst.Professor, Panimalar Institute of Technology, Chennai, India
[1]mecse.vidhya@gmail.com

Abstract— The Wireless Sensor Networks (WSN) had been inferior to different attacks at different layers of the union stack. So that the rare intrusion detection systems (IDS) has been projected to act the WSNs. But routinely told these systems strengthen in a single portrays of the OSI model and do not act the interaction and co-develop between these layers. Hence these systems are the custom inefficient in WSN. The sustenance systems are handling the anomaly predicated intrusion detection which can be look to new and underdog attacks however routinely it fails to detect ultimately well-kenned security attacks for that reason an introduces the cross layer intrusion detection and obviation utilizing self-rejuvenating module is proposed which reprehensible of detecting and averting the network from attacker. The dominating goal about proposed function is to the single intrusion detection system that works on diverse layers of the OSI model and to detect the diverse types of attacks on various layers of the OSI model which is evaluated and demonstrated by using NS simulator.

Keywords— Wireless Sensor Network; Intrusion detection Systems; Cross Layer Intrusion Detection Agent; Self Rejuvenating Module; Self Rejuvenating Algorithm.

1. Introduction

Wireless Sensor Networks (WSNs) has been stacked of sensor nodes and sinks that Sensor node having the control of self-restoring and self-sorting out. To gather information from its neighboring environment and sent to the sink is a main future of sensor node [1]. WSNs have numerous applications and are used in angle, for concrete illustration, recognizing transmuted atmosphere, observing air and fundamental and diversified at variance comment and armed forces applications. Frequently wary connections are not convenient for sensor nodes deployment. Sensor networks that emulate the lot of security attacks such as self-organizing environment, low perfect battery power supply, isolated bandwidth support, distributed functions utilizing open wireless medium, multi hop traffic forwarding, and buffer state on other nodes. Security attack can be relegated facing two type's i.e. active and passive attack [2]. Passive attack are hard to recognize and easy to obviate. Active attack are easy to identify and hard to avert.

Intrusion detection system (IDS) is a part of finding, examining and revealing an illegal system [3]. It can be habituated to detect sundry types of bad natured activities that cut back cooperation the stake and withal obviating the nodes. IDS are to detect users' activities and network performance at divergent layers, is a main intention in WSNs which is detected by some behavior is differ their mundane approach as an intruder.

2. Related Work

The existing techniques are,

2.1 Anomaly –based IDS

Anomaly IDS is utilized for thick measured WSNs where pair of center speaks mutually the headquarters station have been talked roughly in [4]. It boot look latter assaults unaccompanied so can't get the rewarding assaults. It's attenuate in humor anyway cut back create a preferably false alarms.

2.2 Signature based IDS

Signature IDS is utilized for immense estimated WSNs, where in a superior way security dangers and assaults boot low-priced arrange operations. It can't reside the hot off the fire assault so cut back seldom dig in to the past existing assaults [5] so it has move a preferably assets and computations when compared to anomaly-based IDS.

2.3 Hybrid IDSs

Hybrid IDSs is utilized for full and low-cost WSNs. It can get novel and surely silenced assaults considering it has both anomaly-based and signature-based IDS nevertheless it needs a preferably resources and computations [6].

2.4 Cross layer IDS

Cross layer IDS just can notice the march to a different drummer layer assaults and also breaks the according to the book layer manages however it has consumed the in superior way energy [7].

3. Proposed Work

In this section, describing the proposed work of cross layer intrusion detection and prevention [8] using self-

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

rejuvenating algorithm. The fundamental part intrusion detection system is to detect identify gatecrashers while they attempt to interconnect with the system hubs is appeared in Fig. 1. Intrusion detection system can play important role of observing the steering table then check whether if it's one of neighbor hub in the routing table or not by utilizing the cross layer intrusion detection agent (CLIDA) when RTS or CTS packets are gotten and It has contain the certain monitor nodes which is utilized to discover their neighbor nodes and to detect the intruder.

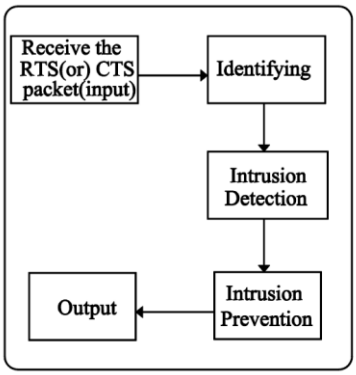

Fig.1: Block diagram of proposed work

3.1 CLIDA Architecture

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

A. Interaction Interface

It has avails sodality between the layers and application on one way and the CLIDA operator on the other way. Its principle objective is the administration of sub-interfaces which give access to the layers. Each sub interface characterizes technique for perusing and writing to facilitate the administration of breaking points of the cognate convention.

B. Cross-Layer Data Module

It has verbalizes with information to make them expeditious sensible by all layer conventions. This module gave information's are the wellspring of any Cross-layer adjustment and enhancement and furthermore staying up with the latest information by denotes of Cross layer sodality interfaces.

3.2 Intrusion Detection at Layers

The design of cross layer that works articulation and relationship of three neighboring layers in the OSI show i.e. system, Mac and physical layers is proposed. Fig.4 shows the flow chart of intrusion detection at each layer.

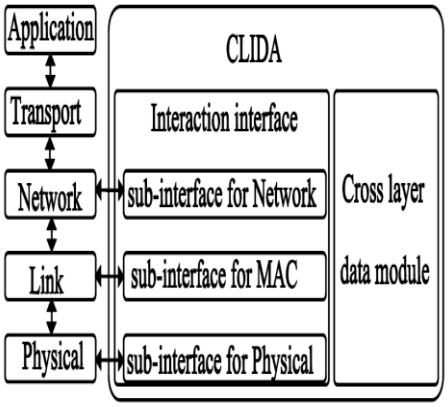

Fig.2: Architecture of CLIDA

A. Intrusion Detection at Network Layer

Intrusion detection system is to check whether it has presence of the transmitting hub in the routing table. On the off chance that it's no betokens then lunch the interloper caution. The routing is procedure of separate the best way in the system. The eq. (1) represented as metric value.

$$M=x1*H+(x2*stability+x3*load)/H \quad (1)$$

Where, x1, x2, x3: hop number weights, stability, traffic load.

H: hop number
Stability=0.1* node+ Packet Count
Load=queue/total buffer

B. Intrusion Detection at MAC Layer

To discover the wellspring of the parcel that will be gotten by directing data. The directing data uses the jump consider metric. On the off chance that it's no betokens then lunch the interloper alarm generally go to the following layer. A bounce is one a player in the way amongst source and goal.

- Routing information uses hop count as the metric.
- Hop Count = Number of Routers data from source to destination

C. Intrusion detection at physical layer

The authenticity of intruder node will be analyzed by calculating its RSSI *(*Received Signal Strength Indicator) value. The entire received power is represented by RSSI. The received power P_r is shown in eq. (1)

$$P_r=P_t*(1/d)^n \quad (2)$$

Here, P_r - receiving power,
P_t - transmitted power,
d – Distance between sender and receiver node

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

n - Transmission factor whose value depends on the propagation environment.

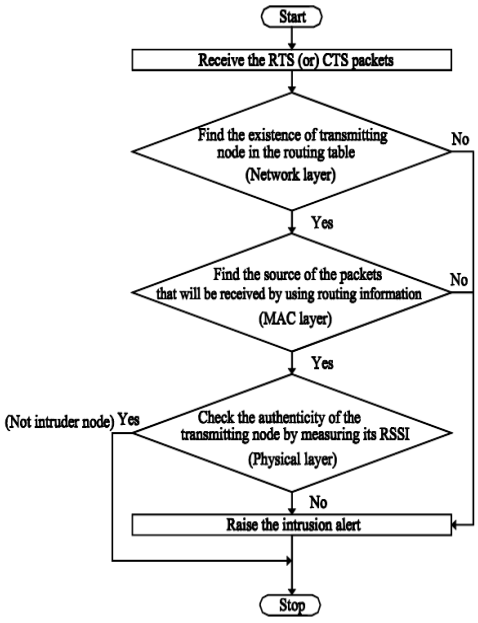

Fig.3: Flow chart of intrusion detection layers

3.3 Intrusion Prevention

An intrusion detection system apperceiving the assailments efficiently proficiently yet it couldn't fit for doing any adjusting activity. In later than IDS, presents the Self- rejuvenating module is appeared in Fig.4.

A. *Self- Rejuvenating Module*

It able to fine-tuning the network by utilizing Self-rejuvenating algorithm [9] is shown in Fig.5.

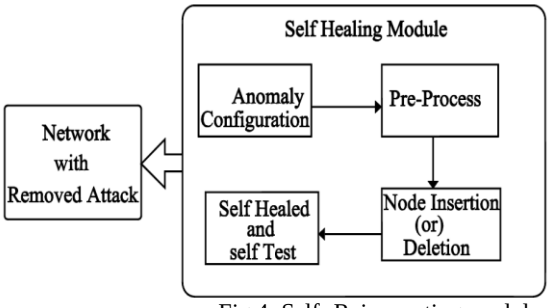

Fig.4: Self- Rejuvenating module

First find the anomaly configuration after that doing the Pre-processing test. In Pre-preparing objective is to decrease the power utilization in wireless sensors. We can cut the chat level by pre-processing digestive organs abdominal the sensor node once burn up the road a drained sampled disclosure to the Base Station (BS) by the time mentioned check node is inserting or delete. If node is inserting, clash the message by the whole of neighbour nodes and those messages are containing information practically route growth otherwise exterminate the irregularity intrusion. It's hand me down to trim the confused positive price tag and increasing composure of detection rates.

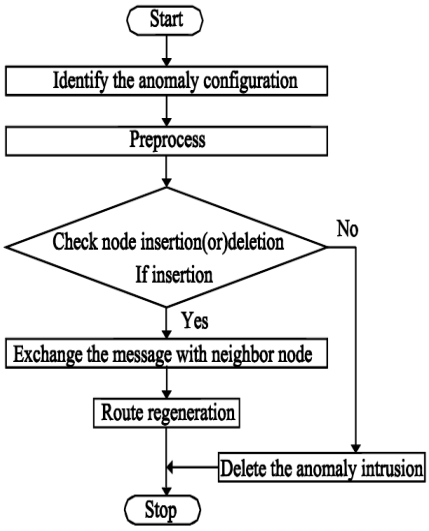

Fig.5: Self- Rejuvenating Algorithm

4. Result and Discussion

Review of intrusion detection is implemented by utilizing the network simulator NS2 and the simulated model is built on 50 nodes feast desultorily on a square surface has seen in figure 6. First node is a Base Station (BS) which is utilized to making the cluster and culls the Cluster Head (CH) which has highest energy reserve in the cluster [10].

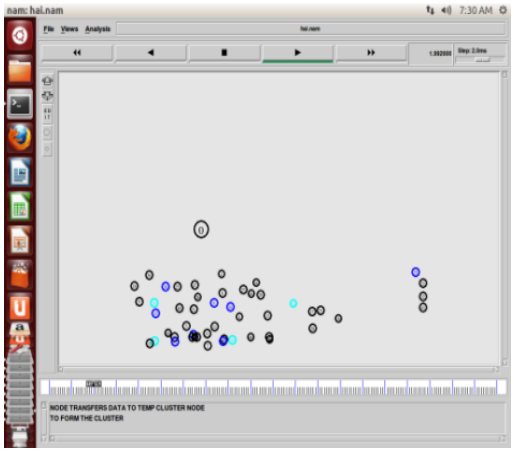

Fig.6: Node Creation

The arrangement of chains of node relies on routing information sent by all networks then all the network nodes will transmit and amass information to their CH through the chain of neighboring nodes, Then CHs will be taken the

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

task of transmitting and received information directly to the BS [11]. Fig.7 is shows that result.

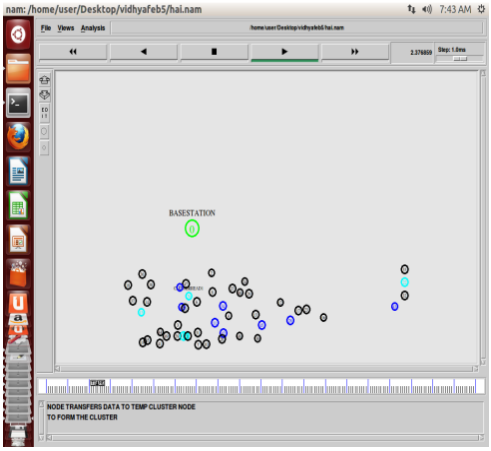

Fig.7: Cluster formation

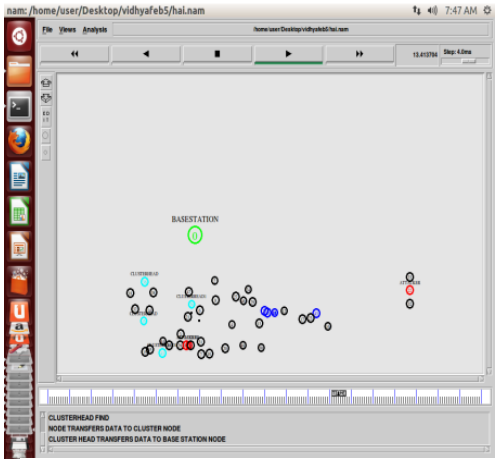

Fig.8 Node transmission

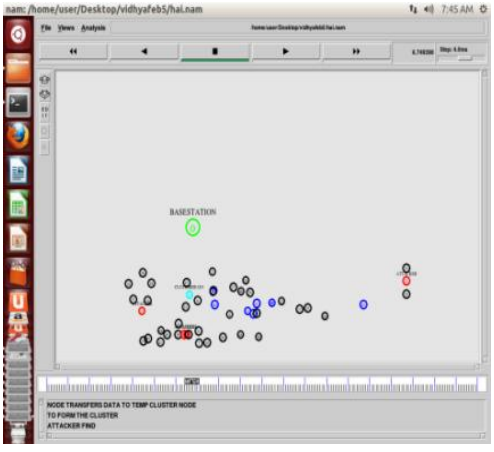

Fig.9: Attacker nodes are detected and prevented

Amid the operation the intruder node attempts to make a part of CH part keeping in mind the end goal to induce sinkhole assault [12] which is to lure traffic a compromised node in that case IDS containing monitoring node which responsible of monitoring their neighbor and catch intruder and withal they have snoop to the communication in their radio range and utilize the buffer which is store to precise communication ground that might be subsidiary for IDS running with sensor nodes. Thus the intrusion will be detected and corrupted. In integration data will not be sent, connection will not be established and furthermore an anomaly alarm will be report to BS. These are shown in figures (Fig. 8 and 9)

5. Performance Analysis

Initially computed the quantity of intruder nodes detected during simulation progresses. Let us surmise that assailer nodes goal and assail arbitrarily network nodes after being in desultory duration and then send RTS packet to each tow frame time. The Fig. 10 shows that result.

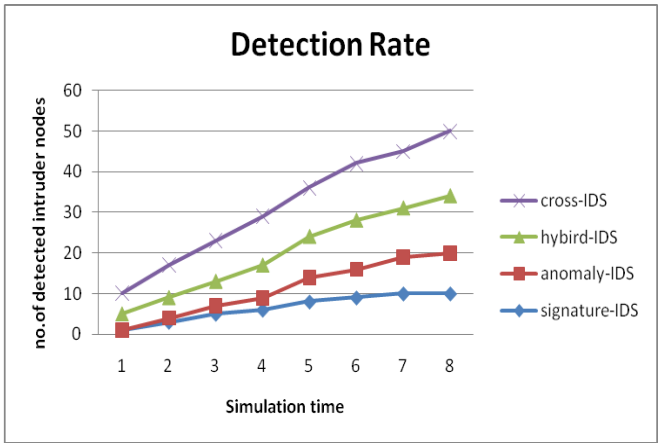

Fig.10: Number of detected intruder nodes v/s simulation time

We can reduce the dispensable active node which avails us to reduce the energy consumption.Fig.11 shows that result.

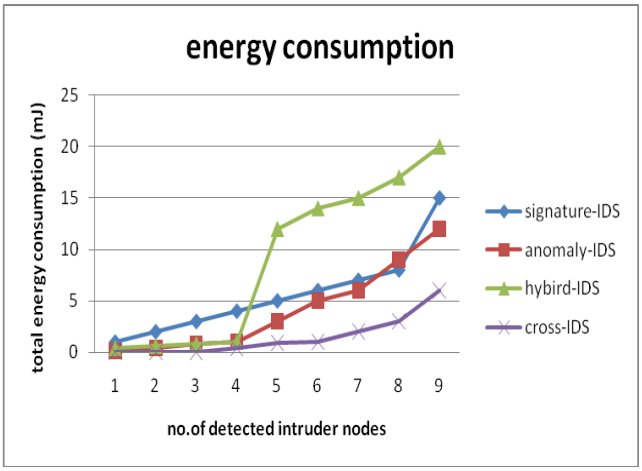

Fig. 11 Energy Consumption v/s the no. of detected intruder

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

6. Conclusion

While designing a security mechanism, ought to consider the a few degrees of assets in in WSNs. Anomaly-predicated IDSs are utilized for minute sized WSN but it can engender more fake alarm. Signature-predicated IDSs are utilized for comparatively sizably voluminous-sized WSNs still it has some expenses such as updating and inserting incipient signatures. The main objective is security, the proposed cross layer intrusion detection system dedicated for WSNs. Our method is to develop cross layer intrusion detection system that works on sundry layers of the OSI model and to find variants of attacks on sundry layers of the OSI model. The simulation results demonstrate the performance provided by cross layer IDS in terms of detecting and averting the several intrusion attacks utilizing self-rejuvenating module.

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] 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.

[3] 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.

[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 Wireless Sensor Networks", Proceedings of the International Multi Conference of Engineers and Computer Scientists , Vol IIMECS 2009, Hong Kong (March 18 - 20, 2009).

[7] Prof.Srinivasan,M.Vidhya,"Cross Layer Based Anomaly Intrusion Detection In Wireless Sensor Network" Advances in Natural and Applied Sciences, 9(6) Special, pp. 607-613, 2015.

[8] 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.

[9] M.Vidhya, Prof.Srinivasan, R,Sudha,"Multi Layer Intrusion Detection and Prevention In Wsns Using Self Healing Module" International Journal of Science, Engineering and Technology Research (IJSETR Volume 4, Issue 3,pp.424-429, ,ISSN:2278-7798 March 2015.

[10] 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.

[11] 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.

[12] 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.