International Journal of Engineering Applied Sciences and Technology, 2019
Vol. 4, Issue 6, ISSN No. 2455-2143, Pages 283-288
Published Online October 2019 in IJEAST (http://www.ijeast.com)

NETWORK TRAFFIC ANALYSIS AND MULTI-LAYER INTRUSION DETECTION IN WIRELESS SENSOR NETWORK

Mrs. M. Vidhya
Asst. Professor
Panimalar Institute of Technology
Chennai

Mr. N. Rajesh
Asst. Professor
Panimalar Institute of Technology
Chennai

Mrs. K. Suja Rajeswari
Asst. Professor
Panimalar Institute of Technology
Chennai

Abstract - This paper will mentioned at the character and structure of wireless sensor network attacks at different layers of OSI model that may be accustomed establish and answer such attacks. The numerous intrusion detection systems (IDS) are planned to shield WSNs over the network traffic. Be that as it may, of these frameworks are work in a solitary layer of the OSI model and doesn't consider the association and coordinated effort between these layers and also doesn't the board the system traffic. In this manner these frameworks are mainly wasteful in WSN. The arranged work of our cross layer intrusion detection to detect malicious attack at different layer of OSI model and control the network traffic over network using wireshark tool. The objective of our proposed system is an Identifying attack streams and understanding the nature of network traffic will be discussed through the use of and their operation and contribution to fighting malicious network activity will be evaluated by Wireshark tool then detect and prevent the attack by intrusion detection system.

Keywords: **Wireless Sensor Network (WSN), Intrusion detection Systems (IDSs), Wireshark.**

I. INTRODUCTION

A Wireless sensor system is often characterized as a system of gadgets that may impart the information assembled from an ascertained field through remote connections. The knowledge is distributed through varied hubs, and with a passage, the knowledge is related to totally different systems like remote local area network. WSN could be a remote system that contains of base stations and quantities of hubs (remote sensors). These systems are used to screen physical or natural conditions like sound, weight, temperature and co-operatively go data through the system to a primary space[1]. Sensing element arranges that delineate the parcel of security assaults, for instance, self-sorting out condition, down and out battery power stockpile, restricted information transmission support, seized capacities mistreatment open remote medium, multi jump traffic causing, and reliance on totally different hubs. Security assaults are often consigned into 2 sort's for instance dynamic and uninvolved assault [2]. Uninvolved assault are troublesome to acknowledge and straightforward to dam. Dynamic assaults are easy to spot and troublesome to show away.

Intrusion detection system (IDS) could be a piece of discovering, analyzing and uncovering a bootleg framework [3]. It fine could also be habituated to acknowledge sundry varieties of harmful exercises that may collaboration the protection and notwithstanding obstruction the hubs. IDS are to screen clients' exercises and system execution at varied layers could be a principle objective in WSNs that is known by some bearing is wandered from their commonplace mien as a trespasser.

II. RELATED WORK

In this section present the existing techniques are,

a. Anomaly –based IDS*:* Anomaly IDS is utilized for little estimated WSNs any place couple of center point talks with the base station are talked in regards to in [4]. It will build up novel ambushes exclusively along these lines can't recognize the exceptional attacks. It's light-weight in nature however will deliver an a great deal of false alerts.

b. Signature based IDS*:* Signature IDS is utilized for significant measurable WSNs, any place bigger security threats and attacks will cut value get ready activities. It will't locate the novel ambush along these lines can essentially recognize existing attacks

[5] so it's need an a great deal of benefits and calculations when put alongside oddity based IDS.

c. Hybrid IDSs: Hybrid IDSs is utilized for Brobdingnagian and reasonable WSNs. It will recognize novel and for certain comprehended ambushes since it's every peculiarity based and signature-based IDS however it needs an a great deal of assets and calculations [6].

d. Cross layer IDS: Cross layer IDS basically will set up the different layer attacks and what is more breaks the standard layer oversees yet it's devoured the more vitality [7].

III. PROPOSED WORK

In this section, describing the planned work of Network Traffic Analysis in Wireless Sensor Network using Wireshark. Network Sniffers are programs that catch low-level bundle data that is transmitted over a network[8]. Partner assaulter will investigate this information to get important data like client ids and passwords. Network sniffing is that the strategy for catching data bundles sent over a system. Sniffing are regularly used to;

- Capture touchy data like login accreditations
- Eavesdrop on visit messages
- Capture records are transmitted over a system

Sniffing the network using Wireshark

Wireshark arrange investigation device at one time alluded to as Ethereal, catches bundles continuously and show them in comprehensible configuration. Wireshark incorporates channels, shading committal to composing, and elective alternatives that license you delve profound into system traffic and look at singular bundles. the most things to catching bundles, sifting them, and reviewing them and Wireshark to look at a suspicious program's system traffic, examine the traffic stream on your system, or investigate system issues.

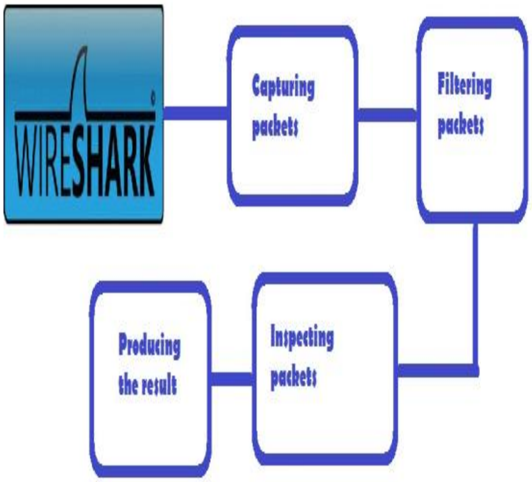


Fig. 1 Block diagram of proposed work.

Capturing Packets

The Figure.2 demonstrated the important part of catching bundles consequently interfaces and moreover catches traffic on remote system so click on remote interface. Wireshark catches each bundle sent to or from your framework.

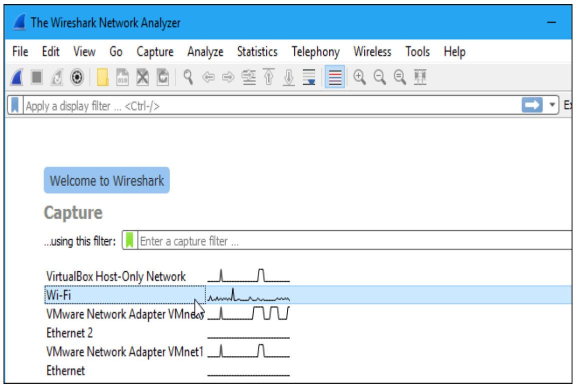
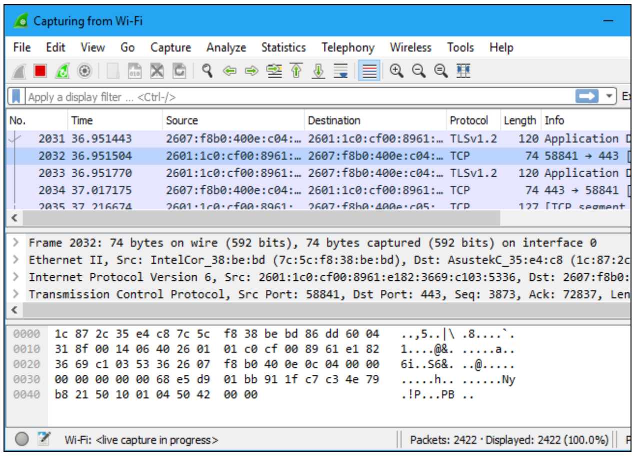

The Wireshark Network Analyzer
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
VirtualBox Host-Only Network
Wi-Fi
VMware Network Adapter VMnet
Ethernet 2
VMware Network Adapter VMnet1
Ethernet

Fig. 2 Wireshark Network Analyzer WiFi Window.

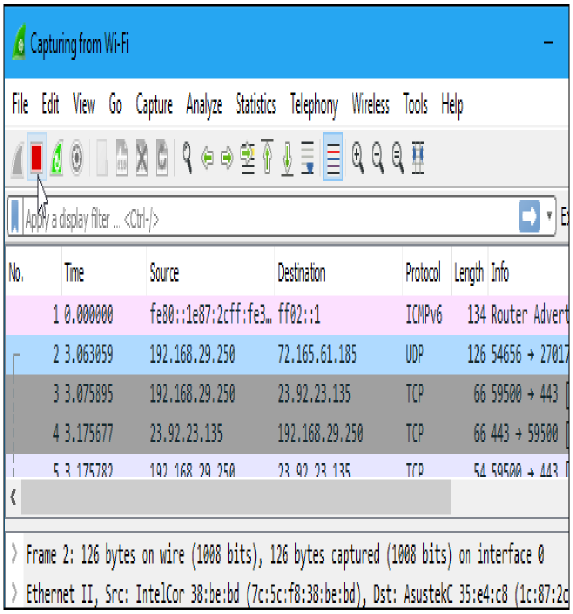
The wanton mode empowered of course and sees all the contrary bundles on the system instead of exclusively parcels routed to our system connector. to check whether unbridled mode is empowered, click Capture > decisions and confirm the "Empower indiscriminate mode on all interfaces" checkbox is initiated at extremely modest of this window is appeared in beneath fig.3



```
Capturing from Wi-Fi
Apply a display filter ... <Ctrl-/>
No.   Time      Source                Destination           Protocol Length Info
 2031 36.951443 2607:f8b0:400e:c04:… 2601:1c0:cf00:8961:… TLSv1.2   120 Application D
 2032 36.951504 2601:1c0:cf00:8961:… 2607:f8b0:400e:c04:… TCP        74 58841 → 443 [
 2033 36.951770 2601:1c0:cf00:8961:… 2607:f8b0:400e:c04:… TLSv1.2   120 Application D
 2034 37.017175 2607:f8b0:400e:c04:… 2601:1c0:cf00:8961:… TCP        74 443 → 58841 [
 2035 37.216674 2601:1c0:cf00:8961:… 2607:f8b0:400e:c05:… TCP       127 [TCP segment

> Frame 2032: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
> Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c
> Internet Protocol Version 6, Src: 2601:1c0:cf00:8961:e182:3669:c103:5336, Dst: 2607:f8b0:
> Transmission Control Protocol, Src Port: 58841, Dst Port: 443, Seq: 3873, Ack: 72837, Len

0000  1c 87 2c 35 e4 c8 7c 5c  f8 38 be bd 86 dd 60 04   ..,5..|\ .8....`.
0010  31 8f 00 14 06 40 26 01  01 c0 cf 00 89 61 e1 82   1....@&. .....a..
0020  36 69 c1 03 53 36 26 07  f8 b0 40 0e 0c 04 00 00   6i..S6&. ..@.....
0030  00 00 00 00 00 68 e5 d9  01 bb 91 1f c7 c3 4e 79   .....h.. ......Ny
0040  b8 21 50 10 01 04 50 42  00 00                     .!P...PB ..

Wi-Fi: <live capture in progress>        Packets: 2422 · Displayed: 2422 (100.0%)
```

Fig. 3 Capturing Packet.

Snap the red "Stop" button near the most elevated left corner of the window once you wish to forestall catching traffic appeared in fig.4 Wireshark uses hues to detect the classifications of traffic at a look. As a matter of course, light purple is transmission control convention traffic, light-weight blue is UDP traffic, and dark recognizes parcels with mistakes.

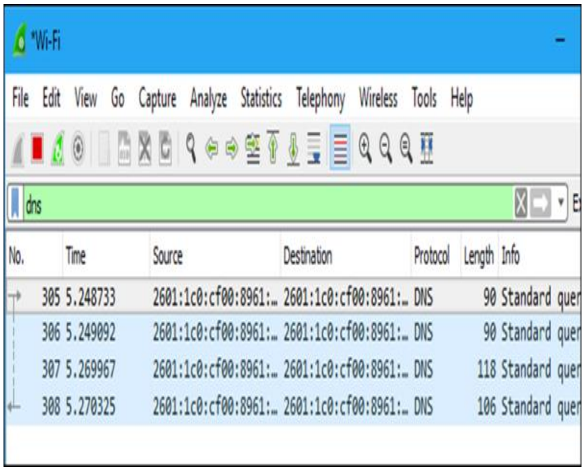


```
Capturing from Wi-Fi
Apply a display filter ... <Ctrl-/>
No. Time     Source               Destination    Protocol Length Info
  1 0.000000 fe80::1e87:2cff:fe3… ff02::1        ICMPv6   134 Router Advert
  2 3.063059 192.168.29.250       72.165.61.185  UDP      126 54656 → 27017
  3 3.075895 192.168.29.250       23.92.23.135   TCP       66 59500 → 443 [
  4 3.175677 23.92.23.135         192.168.29.250 TCP       66 443 → 59500 [
  5 3.175782 192.168.29.250       23.92.23.135   TCP       54 59500 → 443 [

> Frame 2: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
> Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c
```

Fig. 4. Capturing Traffic over WiFi

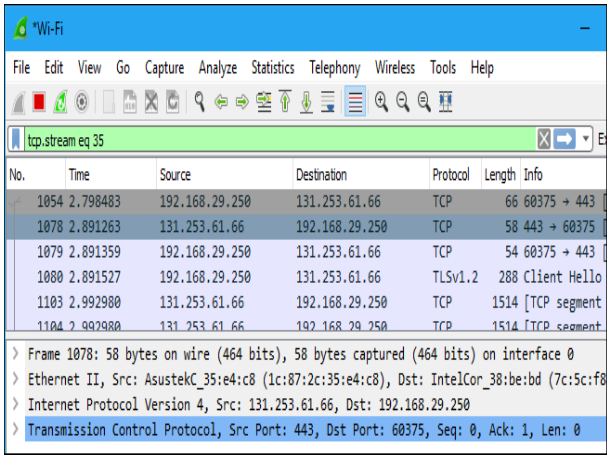
Filtering Packets

The most fundamental gratitude to apply a channel is by composing it into the channel box at the most elevated of the window and clicking Apply or squeezing Enteric appeared in fig .5 we can moreover snap Analyze > show Filters to pick a channel from among the default channels encased in Wireshark. From here, we can include our own custom channels and spare them to just access them inside the future and right-click a parcel and pick Follow > transmission control convention Stream at that point see the total TCP voice correspondence between the customer and server and furthermore click elective conventions in the Follow menu to learn the full discussions for different conventions is appeared in fig.6



```
*Wi-Fi
dns
No. Time     Source               Destination          Protocol Length Info
305 5.248733 2601:1c0:cf00:8961:… 2601:1c0:cf00:8961:… DNS       90 Standard quer
306 5.249092 2601:1c0:cf00:8961:… 2601:1c0:cf00:8961:… DNS       90 Standard quer
307 5.269967 2601:1c0:cf00:8961:… 2601:1c0:cf00:8961:… DNS      118 Standard quer
308 5.270325 2601:1c0:cf00:8961:… 2601:1c0:cf00:8961:… DNS      106 Standard quer
```

Fig. 5. Filtering DNS Packet



```
*Wi-Fi
tcp.stream eq 35
No.  Time     Source         Destination    Protocol Length Info
1054 2.798483 192.168.29.250 131.253.61.66  TCP        66 60375 → 443 [
1078 2.891263 131.253.61.66  192.168.29.250 TCP        58 443 → 60375 [
1079 2.891359 192.168.29.250 131.253.61.66  TCP        54 60375 → 443 [
1080 2.891527 192.168.29.250 131.253.61.66  TLSv1.2   288 Client Hello
1103 2.992980 131.253.61.66  192.168.29.250 TCP      1514 [TCP segment
1104 2.992980 131.253.61.66  192.168.29.250 TCP      1514 [TCP segment

> Frame 1078: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0
> Ethernet II, Src: AsustekC_35:e4:c8 (1c:87:2c:35:e4:c8), Dst: IntelCor_38:be:bd (7c:5c:f8
> Internet Protocol Version 4, Src: 131.253.61.66, Dst: 192.168.29.250
> Transmission Control Protocol, Src Port: 443, Dst Port: 60375, Seq: 0, Ack: 1, Len: 0
```

Fig. 6. Filtering TCP Packet

Inspecting Packets

Snap a parcel to choose it and burrow right down to peruse its subtleties and also right-click one among the important part and utilize the Apply as Filter various leveled menu to make a channel bolstered it appeared in fig7.Wireshark is utilized to redress arrange convention usage, look at security issues and inspect organize convention internals. Fig.7 Inspecting Packets.

Intrusion Detection at layer

Wireshark won't manipulate things on the network, it'll solely "measure" things from it. Wireshark doesn't send packets on the network or do alternative active things (except name resolution, however that may be disabled)

The design of cross layer that works articulation and relationship of 3 neighboring layers within the OSI show i.e. system, raincoat and physical layers is planned. Fig.8 shows the flow chart of intrusion detection at every layer [9][11].

- ***Intrusion detection at network layer:*** Intrusion detection system is to see whether or not it's presence of the sending hub within the routing table. On the off likelihood that it's no betokens then lunch the persona non grata caution. The routing is procedure of separate the most effective manner within the system. The eq. (1) depicted as metric worth

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

Where, x1, x2, x3: weights of hop range, stability, traffic load

H: hop range

Stability=0.1* node+ Packet Count

Load=queue/total buffer

Intrusion detection at MAC layer: to get the wellspring of the bundle that might be gotten by driving data. The main data utilizes the bounce consider metric. On the off probability that it's no betokens then lunch the persona non grata alert commonly go to the ensuing layer. A skip is one a player inside the way among supply and objective Routing data uses jump consider the measurement.

- ➢ Hop Count = scope of Routers information from supply to goal

- ***Intrusion detection at physical layer:***

he validity of contestant hub are checked by action its RSSI (Received Signal Strength Indicator) worth. RSSI speaks to the entire got control. The got power Pr is delineated as in identical.

$$Pr=Pt*(1/d)n \qquad (1)$$

Here, Pr - receiving power,

Pt - transmitted power,

d - Distance among sender and recipient hub

n - Transmission issue whose value relies upon the spread environment.

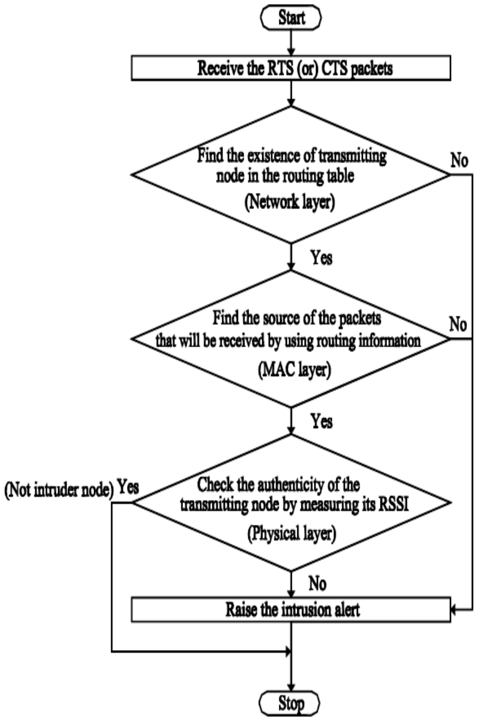

Start
Receive the RTS (or) CTS packets
Find the existence of transmitting node in the routing table (Network layer)
No
Yes
Find the source of the packets that will be received by using routing information (MAC layer)
No
Yes
(Not intruder node) Yes
Check the authenticity of the transmitting node by measuring its RSSI (Physical layer)
No
Raise the intrusion alert
Stop

Fig. 8 Flow chart of intrusion detection layers

IV. RESULT AND DISCUSSION

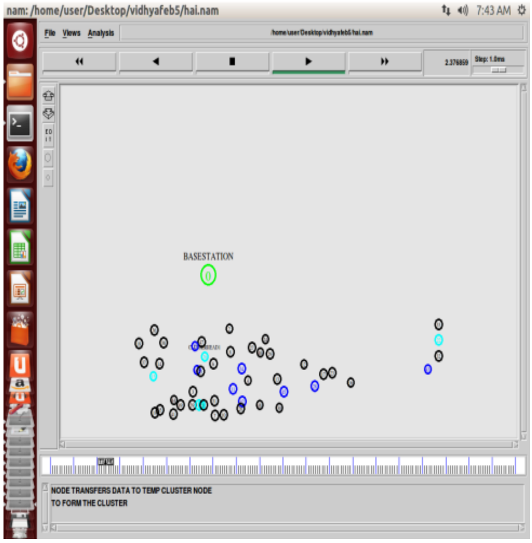
Survey of intrusion detection is executed by using the network simulator NS2

Creating of Sensor Network

For making sensor arrange we are going to utilize Wi-Fi hub of NS-2 the reproduced model is built on fifty hubs then we will create sinks hubs that get data from sensor hub appeared in Fig.9

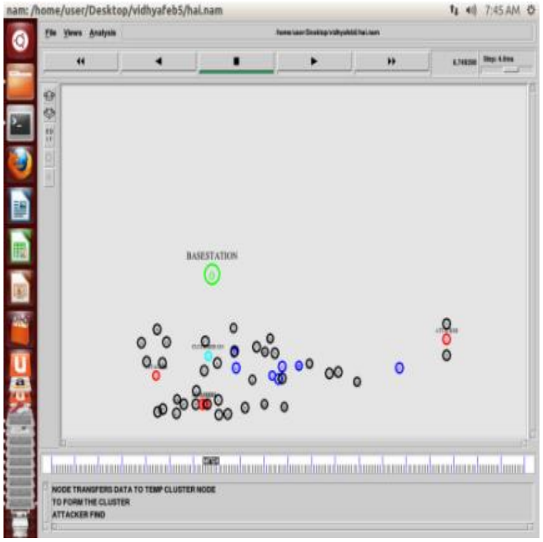
First could be a Base Station (BS) that is accustomed to making the bunch and winnows the Cluster Head (CH) which has most noteworthy vitality hold inside the group [10].

The course of action of chains of hub relies upon directing information sent by all systems then all the system hubs can transmit and store up data to their CH through the chain of close to hubs, Then CHs are assume the liability of sending and got information on to the BS and utilize 2 famous steering conventions of different methodology - AODV. A scheming vitality hub we will apply vitality module of NS-2 on each hub that is lessening the undesirable hub so vitality are spared is appeared in Fig.10.


nam: /home/user/Desktop/vidhyafeb5/hai.nam
7:43 AM
File
Views
Analysis
/home/user/Desktop/vidhyafeb5/hai.nam
2.376859
Step: 1.0ms
BASESTATION

NODE TRANSFERS DATA TO TEMP CLUSTER NODE
TO FORM THE CLUSTER

Fig.9 Node Transmission



NODE TRANSFERS DATA TO TEMP CLUSTER NODE
TO FORM THE CLUSTER
ATTACKER FIND

Fig.10 attacker nodes are detected and prevented

V. PERFORMENCE ANALYSIS

Initially computed the number of entrant nodes detected throughout simulation progresses. Allow us to surmise that assailer nodes goal and assail indiscriminately network nodes when being in purposeless period. The Fig. 11 shows that result.

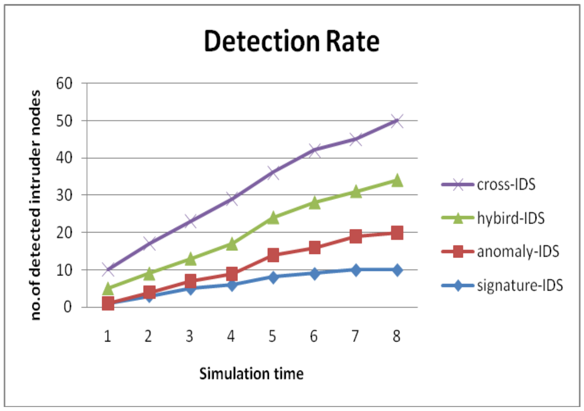


Fig. 11 Number of detected intruder nodes v/s simulation time

VI. CONCLUSION

This paper present idea of coming up with a security mechanism have to be compelled to think about the wireless sensing element network attacks at totally different layers. Anomaly-predicated IDSs are used for minute sized WSN however it will engender a lot of pretend alarm. Signature-predicated IDSs are used for relatively sizably voluminous-sized WSNs still it's some expenses like change and inserting inchoate signatures. The most objective is security, the planned cross layer intrusion detection system dedicated for WSNs. Our methodology is associate characteristic attack streams and understanding the character of network traffic are mentioned through the utilization of and their operation and contribution to fighting malicious network activity will be evaluated by Wireshark tool then discover and stop the attack by cross layer intrusion detection system.

VII. REFERENCES

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

[2] Padmavathi ,G and D, Shanmugapriya. (2009), “A survey of attacks, security mechanisms and challenges in wireless sensor networks,” International

Journal of Computer Science and Information Security, vol. 4, no. 2.

[3] Onat,I and A, Miri(2005), "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.

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

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

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

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

[8] S. Ansari, Rajeev S.G. and Chandrasekhar H.S(2003), "Packet Sniffing: A brief Introduction", IEEE Potentials, Dec 2002- , Volume:21, Issue:5, pp:17 – 19

[9] M.Vidhya, Prof.Srinivasan, R,Sudha,"MULTI LAYER INTRUSION DETECTION AND PREVENTION IN WSNs USING SELF HEALING MODULE(2015)" International Journal of Science, Engineering and Technology Research (IJSETR Volume 4, Issue 3,pp.424-429, ,ISSN:2278-7798 .

[10] Su, C.C, K.M. Chang, Y.H. Kue, and M.F. Horng.(2005), "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.

[11] M. Vidhya, A. Irudaya paul raj Vinod & A. Porselvi(2017) "Cross Layer Intrusion Detection System in WSNs using Self Rejuvenating Module", Engineering and Scientific International Journal (ESIJ), ISSN 2394-7187,Volume 4, Issue 1.