ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 2, Issue 11, November 2013

Hybrid Intrusion Detection for Anomaly & Misuse Attack using Clustering in Wireless Sensor Network

Mr. Ansar I. Sheikh, Prof. Pankaj Kawadkar, Prof. Hitesh Gupta

Abstract **- Wireless Sensor Networks (WSNs) are employed in variety of platforms that have prospective to be used in different area such as civil area, military & many more. Wireless Sensor Network is commonly set up in absent & unfriendly environments. The WSN security is affected by various threats & physically & logically may damage itself. So it is necessary to protect entire network with the help of mechanism Nowadays Intrusion detection system is most important and well-organized protective methods used against WSN attacks. These have variety of security solutions to be intended with minimum computation and resources. In this paper, hybrid intrusion detection system (HIDS) architecture has been anticipated for wireless sensor networks. Hybrid method, the collection of Cluster-based and Rule-base intrusion detection procedure is used and calculated the performance of this system by analyzing the entire network. The analysis result shows that the scheme performs intrusion detection using hybrid technique and detection graph shows ratings regarding attack , data and detection net with the type of attack and performs efficient improved energy and detection ratio.**

Keyword **- WSN, IDS, clustered HIDS, FPR**

I. INTRODUCTION

Wireless Sensor Networks (WSNs) often considered as a self-structured network of fewer power & least cost sensor nodes have been typically designed to examine monitor for chemical and physical changes in the environment, climatic conditions and disaster regions .The sensor nodes are light and portable sensible device, this can be sense while communication and processing all in critical applications. WSNs find out the route and sense different activities of network with configuration of ad hoc manner for communication. Wireless Sensor Networks (WSN) is research oriented field since long years. The physical cost of WSN system is very low which can gathered full information from every corner of network environment. Each device is collection of sensor having dear-less processor & with low-power telecommunication, lies in using and coordinating a vast number of such devices and allows the implementation of very large sensing activities. Generally, these networks are installed in challenging fields (such as inaccessible terrains) for fine grained monitoring in various applications categories [1]. The flexibility and self-made, fault tolerance, sky-scraping sense consistency, dear-less, and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing. In the near future, these application areas will make sensor networks an integral part of life [2]. WSNs are limited energy , serious and so vulnerable to various routing and malicious attacks is of following categories such as spoofing, sinkhole, selective forwarding, sybil, wormhole, blackhole, and denial of service (DoS) attacks. These have been studied in [3]. Network cryptosystem used to secure entire network with help of firewall installation. Conversely, these mechanisms only create less defensive method for wireless networks. In this system no such prevention mechanism employed to avoid from network break, so it is less secure to involve any mechanism. Therefore, it is needed to develop mechanisms that would be mixed in the previous technique to provide a better tremendous security and guarantee survivability. Hence first step of security is nothing but the development of Intrusion Detection System (IDS). A Lot of IDS have been proposed from several researchers and few of them are discussed in the studied paper. However, all of them showed the concept of high False Positive Rate (FPR) which describes an instance in this IDS falsely generate wrong report about valid as an anomaly. Anomaly detection uses activities that significantly turn number of possible occurrences of attack without seeing focusing on existing intrusion. In this work, our main motive is that to use IDS for Clustered based WSNs which analyze entire network for getting low FPR with high detection accuracy.

II. AN INTRUSION DETECTION SYSTEM (IDS)

Intrusion enters into your system & unauthorized access to the system or network [4]; intrusion is nothing but the collection of different action to destroy the security aspects of a network's resource [5, 6]. Intrusion detection is a process find out unnecessary activities over the network that degrade the performance of network [4]; The purpose of intrusion detection process is reviewing, controlling, analyzing and representing reports from the system and network activities. Intrusion Detection System (IDS), i.e.:

1. The Physical method with defensive mechanism guard the secure information of network system & itself [7, 8];

2. It can be used for network host;

3. Simulating the network flow through the communication port discovering behavior activities done by inner & outer;

4. Identifying non-determent but not fully. Notifying to the security manager about all [6, 7,10].

5. Determining attacker uniqueness

There are three function for IDS are as follows: evaluation, analyzing and reacting [5, 7] to computer system attacks and networks. If IDS work properly, it performs three type of task: 1) basic detection,2) attacks and doubtful task. The IDS work as a network supervisor. It protects system from destruction by giving indication as soon as intruder attack. As studied two types of intrusion detection such as anomaly detection and misuse detection. Anomaly detection assembles normal behavior model and compare these detected behavior. It detection rate is high, but the false positive rate is also high. The misuse detection detects new types of attack by matching with existing behavior of attack and present behavior of attack. It accuracy is high but detection rate is low. Mainly, the misuse detection can detect known attacks, but unknown attacks don't detect. Lot of researchers discuss combined both detection system to gain hybrid benefits of anomaly detection and misuse detection. This hybrid approach can detect unknown attacks with the high accuracy of misuse detection and high detection rate of anomaly detection. The Hybrid Intrusion Detection System (HIDS) builds for gaining the purposes of high detection rate and low false positive rate. In this section, a HIDS is discussed in a CWSN. In sensor network, Cluster head (CH) is nothing but the sensor network but it has greater ability and better capability than other SNs. Also, the CH collects the sensed data from different other SNs in its own cluster. This data is suitable for find out the attackers. However, the CH is used to detect the intruders in our proposed HIDS. This drop off the energy consumption, also capably declines information stores. Therefore, the WSN existence can be long-drawn-out.

IDS REQUIREMENTS IN SN

We give details regarding the requirements of t an IDS system for sensor networks. Each sensor node has many characteristic such as less communication ability, computational resources and a short radio range. Moreover, the attacker can be negotiated with sensor node due to its weakness, who utilizes malicious software to encounter internal attack. In this situation, a distributed architecture provides desirable solution using node cooperation. In particular, an IDS system for sensor networks must support below properties:

1) Local review: An IDS for sensor networks must work with imperfect small and local reviewed data. In sensor networks, audit global data to be collected from different places, so this mechanism relate to the sensor network model.

2) Diminishes resources: An IDS sensor networks should require minimum resources. The wireless networks have dynamic connections, network hardware and devices, i.e. Bandwidth and power are imperfect. Connection can break at any time.

Furthermore, the node require the very few bandwidth for intrusion purposes

3) Trust no node: In IDS, not a single sensor is more secure because, sensor nodes can be very easily compromised. Therefore, IDS must not provide reliable node in environment.

4) Be truly distributed: The collected data is analyzed on different locality. The distributed approach executes many detection algorithm and alert relationship.

5) Be secure: An IDS should hold up unfriendly attack. It regularly observing node and controlling the deeds of embedded IDS agent which stop illegal action of legitimate node from network.

IDS DESIGN CHALLENGES IN WSNS

Followings are varieties of challenges for designing IDS for WSNs; depicted as follows:

- Designing efficient software requires enhancing network lifetime. So it can store as well as install on the sensor nodes, central server and cluster-heads, that saves consumed energy;
- Limited resources [16, 17, 18, 19];
- Inconsistent & frequently failure sensor nodes;
- Application-oriented networks [20];
- It is necessary of screening, sensing, decision making and fast real time intrusion counter reduces damages.
- It is difficult to use time synchronization protocol for time synchronization node.
- Databases challenges: Variable sensed data from SN, cluster and central server is queried for faster indexing sensed data.

III. RELATED WORK

ATTACKS IN WSN

There are two main categories of attacks depend on aim of intrusion [21]. The WSN attack differences are shown in Table 1 [22, 23, and 24]. However, the majority of attack behavior consists of the route updating misbehavior, data transmission manipulation. In the CWSN application, the sensed data is collected by SNs, and is distributed to Cluster Head totally. The total data is then sent to sink from Cluster Head. Therefore, Cluster Head is a main target for attack.

Table 1- types of attacks in WSN

Attack Name	Behavior
Select Forward	Data Forwarding misbehavior
Denial of Service	Data Forwarding misbehavior
Replay routing information ,spoofed	Route updating misbehavior
Sinkhole	Route updating misbehavior
Sybil	Route updating misbehavior
Wormhole	Route updating misbehavior

ANALYTIC TOOL OF INTRUSION DETECTION

In the proposed HIDS, it efficiently detects attack and also keeps away from resource wastes. First of all, the intrusion detection module filter huge packets then whole detection take place. The detection module detects the normalcy of current behavior, as determined by the rules. The detection module determines the current behavior is an attack, and its behavior. Rule-based presents the thoughts of expert [25]. Because complicated knowledge of human thought could hardly be presented with help of algorithm. Hence, a rule-based process is employed to evaluate outcomes. Also, the rules are used when it has been defined.

The rule works on "if... then...” concept that means if "condition” is true and then the “conclusion" will occur.

Many researchers have discussed & proposed different ID systems to protect WSNs. The vulnerabilities associated with wireless networks necessary to include or absorb an IDS in WSNs. [26] defined IDS as an act of monitoring traffic and detecting unwanted activity physically & logically on network. This is achieved by monitoring the traffic flow on the network. Some of examples on anomaly detection systems published are IDES [27],HAYSTACK [28], and the statistical model used in NIDES/STATS [29] which is a more recent approach and presents a better capability anomaly detection system than other MANET network[30].The authors discussed many ways to get details of intrusion from anomaly detection regards attacks; a simple rule can be used to detect node location and sort of attack. A statistical structure has [31] to address in unsupervised anomaly detection that analyzed transmitted packet is determine whether it is normal or abnormal. To do this, encoded packets with many features in traffic mapped to a point A. hence a € A. If packets appear in different region, then it is an abnormal, otherwise, it is normal.

IV SYSTEM ARCHITECTURE

The proposed HIDS has two type of module 1) intrusion detection module 2) decision making module. Intrusion detection module used rule base mechanism to sort out network packet records. Decision making module strict proper action against abnormal node.

SYSTEM ARCHITECTURE AND NETWORK STRUCTURE

Proposed Hybrid Intrusion Detection Model (HIDS) for Cluster Based Wireless Sensor Network (CWSN). Fig.1 shows both modules. First, the Intrusion Detection Agent is used to sort the entering packets and categorize its normalcy or abnormality. Abnormal packets are passed to the decision making module is used to verify the attack introduces and show its type. Ultimately, the decision making module proceeds this information to the main sink and used efficient treatment on intruder node.

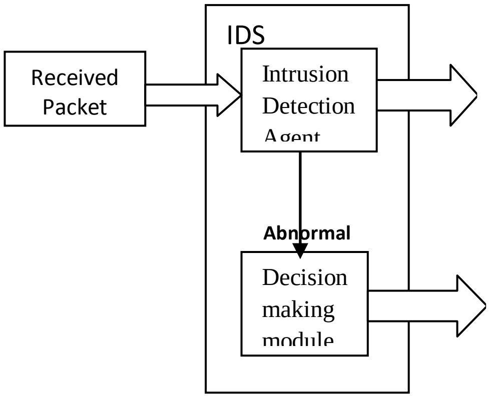


Fig.1. Proposed System Architecture

The hierarchical topology in proposed model, the entire SN divided into clusters having a cluster head (CH) with green color shown in Fig. 3.Here, the sensors nodes are rigid and cluster heads are more powerful than the other sensor nodes. The main motive of this architecture reduces unwanted energy, enhances network life with reduction in network abnormal information. Some of the Cluster-based routing protocols founded in discussion are: LEACH [32], PEGASIS [33] and HEED [34].

In Fig.2, we used three type of node with different colors. Yellow colour shows the Base Station (BS), Cluster Head (CH) with Green colour and all the sensor nodes are indicated by red colour and finally the intruder node with blue colour in the sensor field. In Fig.3, formation of clusters is done using Cluster-based mechanism in WSN.

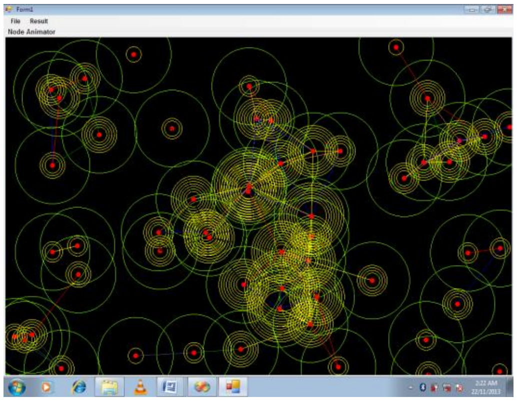


Fig 2: Node deployment in WSN

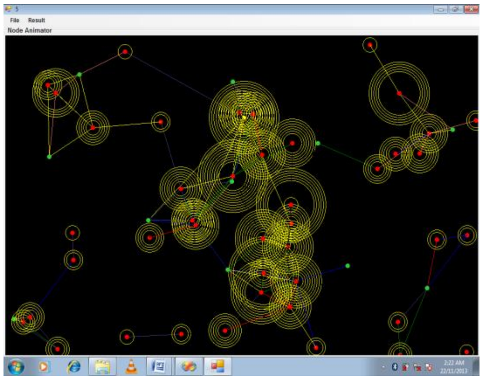


Fig.3. Clustering in WSN

IDS TECHNOLOGIES

In the proposed Hybrid Approach [35], [36], the two techniques i.e. Cluster-Based and Rule-Based techniques are combined together to develop Hybrid Intrusion Detection technique. Hybrid detection, so we can take advantages of both. This combination provides low energy consumption, high security, simplicity, easy operation. Both high low false positive rate and detection rate are achieved by Hybrid IDS.

CLUSTERING

Clustering is defined as collection of sensor nodes form hierarchical of WSN [37]. The network is divided into cluster head & its member node. Cluster head is centre of a cluster. Cluster head forwards information to its member and collected information from them transmit to base station (BS).

Working of Base Station:

All nodes send data through CH to BS.BS keep and the record of all nodes & decide the creation and deletion of node in cluster .It monitors every movement status of node with its network interface hardware as well as cluster. Base station performs MAC tracking and keeps its history also manage MAC database. The BS only responsible for manage the function of any node in the network.

Working of Cluster Head:

Cluster Heads record tracks of all nodes and send to base station periodically for node status. Cluster head send necessary information of all nodes to sink after compressed received data.

RULE-BASED

Rule-based intrusion detection [9] is nothing but protocol consisting data classification which is placed in sequence used according to FIFO principle. The appropriate rule is applied on network monitored data. If rule is found then the data is analogous. This algorithm divided into three phase for intrusion detection .In the first supervise node data. In second phase, node operation failure. In third phase compare number of failure with estimated occasional failure in network. Data alteration, message loss, and message collision are occasional failures. An intrusion indicate anomalous is occurred by raising alarm if the number of failures flagged exceeds than the expected number of occasional failures. The rule base techniques are simple, faster & require minimum data.

POLICY & DEFINITION

Following are three important steps for IDS development in of cluster-based WSN:

(1) Predefined rule select from existing rule set is applied to monitor the feature; (2) compare the information at the target network by pre-select rule to select rules definitively; and (3) parameter set of the selected rules definition with values of the design definitions as follows:

Integrity Rule: to avoid data modification detected by this rule.

Jamming Rule: It identifies the network traffic related to message lower than specified rule. This can also detect communication noise on particular node.

Interval Rule: Failure is introduced if the time interval between the receptions of two consecutive messages is longer or shorter than predefined time. The intruder transmits large packets in order to enhance energy requirement of in the cluster. This rule reduce energy enhancement.

Repetition Rule: The similar packet retransmitted behind limitation. Wormhole and hello flood attack may occur.

Re-send Rule: the monitor listens to receive a message not properly forward to its neighbour. Blackhole and the selective forwarding attack can be detected by this rule . In both attack, the intruder suppresses retransmitted message does not reach to final destination

Delay Rule: Delay in re-sending by subordinate node respect to defined time, it is detected by this rule.

Algorithm 1:

Rules application procedure of IDS

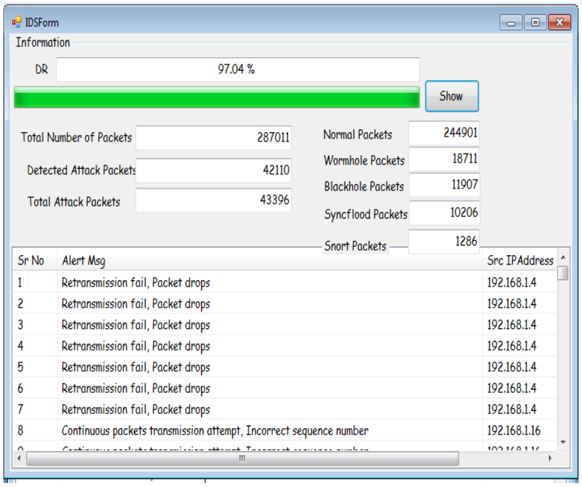
1: for all messages in data structure array do

```
    for all rules specific to the message in descending order by weight do
        apply rule to the message;
        if (message == fail) then
            increment failure counter for the node based on weight ; [failure counter = failure counter + weight ]
            discard message;
            break;
        end if
    end for
    discard message;
end for
```

Algorithm 1 shows the procedure of rules application on messages in the network. The algorithm is used to apply the rule on message. Message failure counter is increases and rejects message, if message fails.

V. NETWORK ANALYSIS AND RESULTS

Visual Studio.Net is used for network simulation in proposed architecture. The simulator can also observe entire topology generated by algorithm LEACH [32] for establishment of node in the WSN as shown in Fig.2. It shows difference between collision of same cluster and check packet error during communication.



DR 97.04 %

Total Number of Packets 287011

Detected Attack Packets 42110

Total Attack Packets 43396

Normal Packets 244901

Wormhole Packets 18711

Blackhole Packets 11907

Syncflood Packets 10206

Snort Packets 1286

Sr No	Alert Msg	Src IPAddress
1	Retransmission fail, Packet drops	192.168.1.4
2	Retransmission fail, Packet drops	192.168.1.4
3	Retransmission fail, Packet drops	192.168.1.4
4	Retransmission fail, Packet drops	192.168.1.4
5	Retransmission fail, Packet drops	192.168.1.4
6	Retransmission fail, Packet drops	192.168.1.4
7	Retransmission fail, Packet drops	192.168.1.4
8	Continuous packets transmission attempt, Incorrect sequence number	192.168.1.16
9	Continuous packets transmission attempt, Incorrect sequence number	192.168.1.16

Fig. 4 Attack Introduction in WSN

In this proposed architecture, the WSN is divided into the no. of small clusters. The hierarchical clustering formation is done with no. of SN. The CH act as current node dynamically after cluster formation, the WSN is called as a Cluster based WSN i.e. CWSN as shown in Fig. 3.Normally, the cluster head having highest energy. Simulation runs with the following simulation parameters:

Table 2 – Proposed Parameters

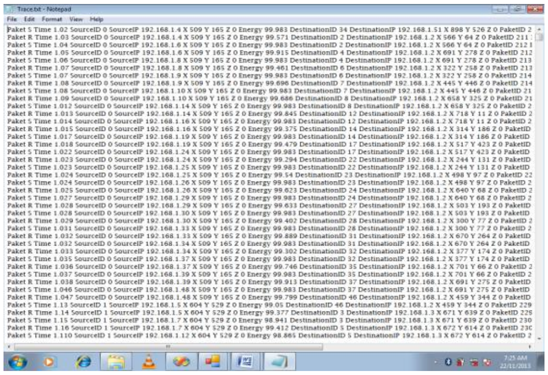
i) Routing Protocol	AODV
ii) Wireless standard	802.11
iii)Total No. of Nodes	55
iv)Traffic category	CBR
v) Simulation Topology	1024cm x 768cm
vi) Simulation Time	101 sec
vii) Packet size	Half Mbytes

Simulation is going on with packet size is 512Kbyte on topology of 1024 cm X 768 cm. The main node of proposed model is called as sink or base station which requires limited resources. Also act as an administrative node provides safety from attackers & take appropriate action on intrusion node. The AODV routing protocol is used for network simulation with Mac layer 802.11. There are 50 nodes in network area having data transmission range is 512 Kbyte for 100 sec. It regularly checks the network performance for above simulation parameter.

The simulation is scurry in different state of affairs, each node has different parameter values injecting malicious packet into normal node in the whole sensor network as shown in Fig. 4. The Fig. shows the false packets in yellow colour around malicious node (Blue) are scattering in the intact network.

Proposed system identifies such nodes and breaks the connection for further communication against malicious node with help of base station.

After the simulation of network, the communication among the nodes has been recorded in text-pad file named as a trace.txt. This trace file keeps every information of each packet in a network. This file is used to determine & analyze the attack activities introduced by intruder node. The trace file is shown in the Fig. 5. These records gets as an input to the Intrusion Detection Engine, filtered using rule base and detection of attacks takes place. The network graphs are shown in the following Fig. Sending and receiving graph shows the sending and receiving of packets in the networks. The networks performance is indicated by Fig. 8. Here attack rating is shown which represents the attacker's packets and data rating shows the total packets sent by all the nodes. Finally the detection of the attacks is shown in Fig. 10 with their ratings and names. The blackhole, wormhole and syncflood attacks have been detected.



```
Paket S Time 1.02 SourceID 0 SourceIP 192.168.1.4 X 509 Y 165 Z 0 Energy 99.983 DestinationID 34 DestinationIP 192.168.1.51 X 898 Y 526 Z 0 PaketID 2
Paket R Time 1.03 SourceID 0 SourceIP 192.168.1.4 X 509 Y 165 Z 0 Energy 99.571 DestinationID 2 DestinationIP 192.168.1.2 X 566 Y 64 Z 0 PaketID 211
Paket S Time 1.04 SourceID 0 SourceIP 192.168.1.6 X 509 Y 165 Z 0 Energy 99.983 DestinationID 2 DestinationIP 192.168.1.2 X 566 Y 64 Z 0 PaketID 212
Paket R Time 1.05 SourceID 0 SourceIP 192.168.1.6 X 509 Y 165 Z 0 Energy 99.915 DestinationID 4 DestinationIP 192.168.1.2 X 691 Y 278 Z 0 PaketID 212
Paket S Time 1.06 SourceID 0 SourceIP 192.168.1.8 X 509 Y 165 Z 0 Energy 99.983 DestinationID 4 DestinationIP 192.168.1.2 X 691 Y 278 Z 0 PaketID 213
Paket R Time 1.07 SourceID 0 SourceIP 192.168.1.8 X 509 Y 165 Z 0 Energy 99.461 DestinationID 6 DestinationIP 192.168.1.2 X 322 Y 258 Z 0 PaketID 213
Paket S Time 1.07 SourceID 0 SourceIP 192.168.1.9 X 509 Y 165 Z 0 Energy 99.983 DestinationID 6 DestinationIP 192.168.1.2 X 322 Y 258 Z 0 PaketID 214
Paket R Time 1.08 SourceID 0 SourceIP 192.168.1.9 X 509 Y 165 Z 0 Energy 99.696 DestinationID 7 DestinationIP 192.168.1.2 X 445 Y 446 Z 0 PaketID 214
Paket S Time 1.08 SourceID 0 SourceIP 192.168.1.10 X 509 Y 165 Z 0 Energy 99.983 DestinationID 7 DestinationIP 192.168.1.2 X 445 Y 446 Z 0 PaketID 21
Paket R Time 1.09 SourceID 0 SourceIP 192.168.1.10 X 509 Y 165 Z 0 Energy 99.686 DestinationID 8 DestinationIP 192.168.1.2 X 658 Y 325 Z 0 PaketID 21
Paket S Time 1.012 SourceID 0 SourceIP 192.168.1.14 X 509 Y 165 Z 0 Energy 99.983 DestinationID 8 DestinationIP 192.168.1.2 X 658 Y 325 Z 0 PaketID 2
Paket R Time 1.013 SourceID 0 SourceIP 192.168.1.14 X 509 Y 165 Z 0 Energy 99.845 DestinationID 12 DestinationIP 192.168.1.2 X 718 Y 11 Z 0 PaketID 2
Paket S Time 1.014 SourceID 0 SourceIP 192.168.1.16 X 509 Y 165 Z 0 Energy 99.983 DestinationID 12 DestinationIP 192.168.1.2 X 718 Y 11 Z 0 PaketID 2
Paket R Time 1.015 SourceID 0 SourceIP 192.168.1.16 X 509 Y 165 Z 0 Energy 99.375 DestinationID 14 DestinationIP 192.168.1.2 X 314 Y 186 Z 0 PaketID
Paket S Time 1.017 SourceID 0 SourceIP 192.168.1.19 X 509 Y 165 Z 0 Energy 99.983 DestinationID 14 DestinationIP 192.168.1.2 X 314 Y 186 Z 0 PaketID
Paket R Time 1.018 SourceID 0 SourceIP 192.168.1.19 X 509 Y 165 Z 0 Energy 99.479 DestinationID 17 DestinationIP 192.168.1.2 X 517 Y 423 Z 0 PaketID
Paket S Time 1.022 SourceID 0 SourceIP 192.168.1.24 X 509 Y 165 Z 0 Energy 99.983 DestinationID 17 DestinationIP 192.168.1.2 X 517 Y 423 Z 0 PaketID
Paket R Time 1.023 SourceID 0 SourceIP 192.168.1.24 X 509 Y 165 Z 0 Energy 99.294 DestinationID 22 DestinationIP 192.168.1.2 X 244 Y 131 Z 0 PaketID
Paket S Time 1.023 SourceID 0 SourceIP 192.168.1.25 X 509 Y 165 Z 0 Energy 99.983 DestinationID 22 DestinationIP 192.168.1.2 X 244 Y 131 Z 0 PaketID
Paket R Time 1.024 SourceID 0 SourceIP 192.168.1.25 X 509 Y 165 Z 0 Energy 99.54 DestinationID 23 DestinationIP 192.168.1.2 X 498 Y 97 Z 0 PaketID 22
Paket S Time 1.024 SourceID 0 SourceIP 192.168.1.26 X 509 Y 165 Z 0 Energy 99.983 DestinationID 23 DestinationIP 192.168.1.2 X 498 Y 97 Z 0 PaketID 2
Paket R Time 1.025 SourceID 0 SourceIP 192.168.1.26 X 509 Y 165 Z 0 Energy 99.623 DestinationID 24 DestinationIP 192.168.1.2 X 640 Y 68 Z 0 PaketID 2
Paket S Time 1.027 SourceID 0 SourceIP 192.168.1.29 X 509 Y 165 Z 0 Energy 99.983 DestinationID 24 DestinationIP 192.168.1.2 X 640 Y 68 Z 0 PaketID 2
Paket R Time 1.028 SourceID 0 SourceIP 192.168.1.29 X 509 Y 165 Z 0 Energy 99.633 DestinationID 27 DestinationIP 192.168.1.2 X 503 Y 193 Z 0 PaketID
Paket S Time 1.028 SourceID 0 SourceIP 192.168.1.30 X 509 Y 165 Z 0 Energy 99.983 DestinationID 27 DestinationIP 192.168.1.2 X 503 Y 193 Z 0 PaketID
Paket R Time 1.029 SourceID 0 SourceIP 192.168.1.30 X 509 Y 165 Z 0 Energy 99.402 DestinationID 28 DestinationIP 192.168.1.2 X 300 Y 77 Z 0 PaketID 2
Paket S Time 1.031 SourceID 0 SourceIP 192.168.1.33 X 509 Y 165 Z 0 Energy 99.983 DestinationID 28 DestinationIP 192.168.1.2 X 300 Y 77 Z 0 PaketID 2
Paket R Time 1.032 SourceID 0 SourceIP 192.168.1.33 X 509 Y 165 Z 0 Energy 99.889 DestinationID 31 DestinationIP 192.168.1.2 X 670 Y 264 Z 0 PaketID
Paket S Time 1.032 SourceID 0 SourceIP 192.168.1.34 X 509 Y 165 Z 0 Energy 99.983 DestinationID 31 DestinationIP 192.168.1.2 X 670 Y 264 Z 0 PaketID
Paket R Time 1.033 SourceID 0 SourceIP 192.168.1.34 X 509 Y 165 Z 0 Energy 99.302 DestinationID 32 DestinationIP 192.168.1.2 X 377 Y 174 Z 0 PaketID
Paket S Time 1.035 SourceID 0 SourceIP 192.168.1.37 X 509 Y 165 Z 0 Energy 99.983 DestinationID 32 DestinationIP 192.168.1.2 X 377 Y 174 Z 0 PaketID
Paket R Time 1.036 SourceID 0 SourceIP 192.168.1.37 X 509 Y 165 Z 0 Energy 99.746 DestinationID 35 DestinationIP 192.168.1.2 X 701 Y 66 Z 0 PaketID 2
Paket S Time 1.037 SourceID 0 SourceIP 192.168.1.39 X 509 Y 165 Z 0 Energy 99.983 DestinationID 35 DestinationIP 192.168.1.2 X 701 Y 66 Z 0 PaketID 2
Paket R Time 1.038 SourceID 0 SourceIP 192.168.1.39 X 509 Y 165 Z 0 Energy 99.913 DestinationID 37 DestinationIP 192.168.1.2 X 691 Y 275 Z 0 PaketID
Paket S Time 1.046 SourceID 0 SourceIP 192.168.1.48 X 509 Y 165 Z 0 Energy 99.983 DestinationID 37 DestinationIP 192.168.1.2 X 691 Y 275 Z 0 PaketID
Paket R Time 1.047 SourceID 0 SourceIP 192.168.1.48 X 509 Y 165 Z 0 Energy 99.799 DestinationID 46 DestinationIP 192.168.1.2 X 459 Y 344 Z 0 PaketID
Paket S Time 1.13 SourceID 1 SourceIP 192.168.1.5 X 604 Y 529 Z 0 Energy 99.05 DestinationID 46 DestinationIP 192.168.1.2 X 459 Y 344 Z 0 PaketID 229
Paket R Time 1.14 SourceID 1 SourceIP 192.168.1.5 X 604 Y 529 Z 0 Energy 99.377 DestinationID 3 DestinationIP 192.168.1.3 X 671 Y 639 Z 0 PaketID 229
Paket S Time 1.15 SourceID 1 SourceIP 192.168.1.7 X 604 Y 529 Z 0 Energy 98.941 DestinationID 3 DestinationIP 192.168.1.3 X 671 Y 639 Z 0 PaketID 230
Paket R Time 1.16 SourceID 1 SourceIP 192.168.1.7 X 604 Y 529 Z 0 Energy 99.412 DestinationID 5 DestinationIP 192.168.1.3 X 672 Y 614 Z 0 PaketID 230
Paket S Time 1.110 SourceID 1 SourceIP 192.168.1.12 X 604 Y 529 Z 0 Energy 98.865 DestinationID 5 DestinationIP 192.168.1.3 X 672 Y 614 Z 0 PaketID 2
```

Fig.5. WSN Network Tracking Records

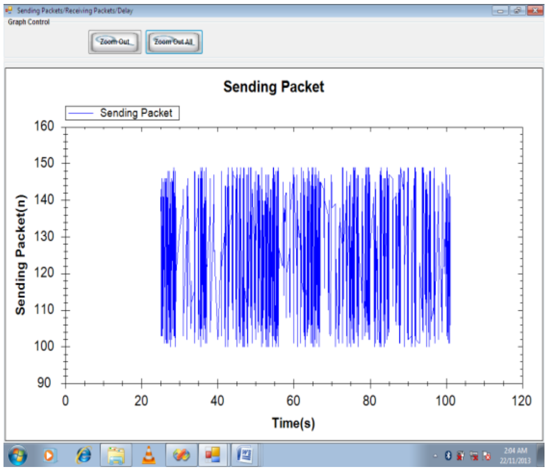


Fig.6 Sending packets graph

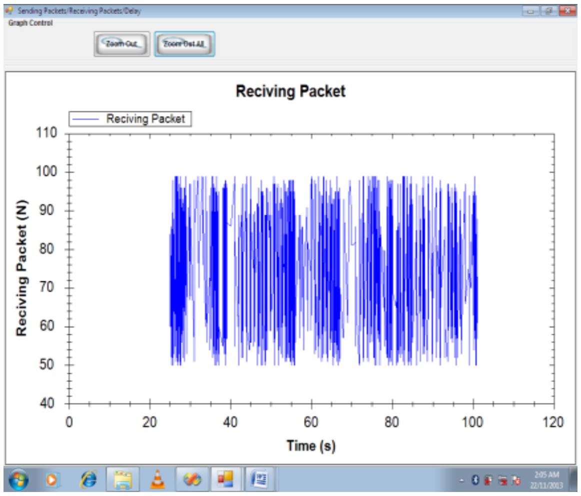
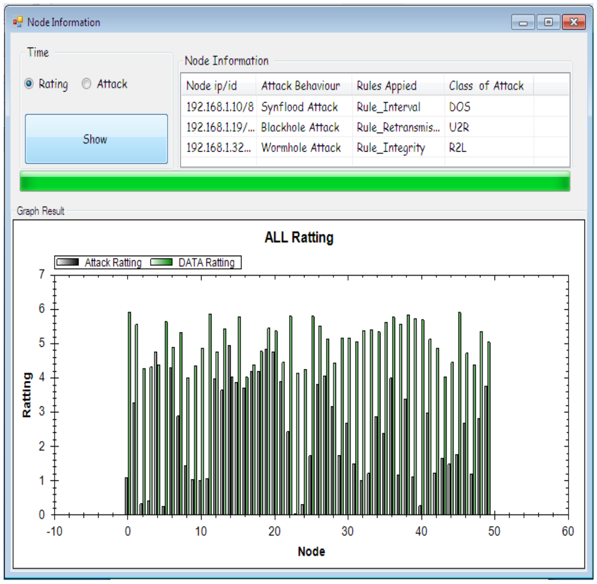
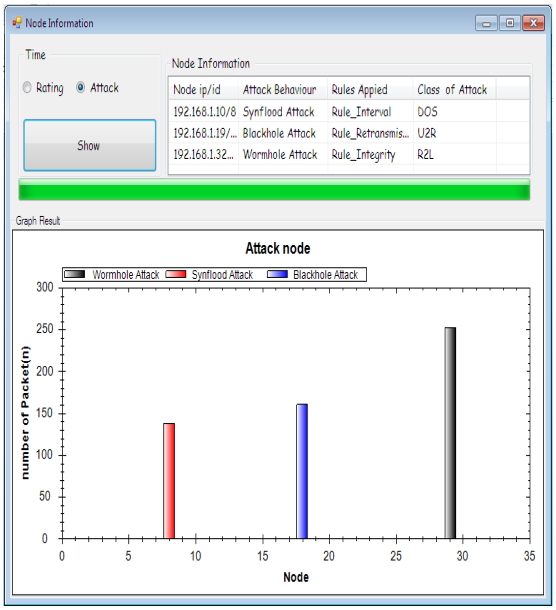


Fig. 7.Receiving packets Graph



Node ip/id	Attack Behaviour	Rules Appied	Class of Attack
192.168.1.10/8	Synflood Attack	Rule_Interval	DOS
192.168.1.19/...	Blackhole Attack	Rule_Retransmis...	U2R
192.168.1.32...	Wormhole Attack	Rule_Integrity	R2L

Fig.8. Attack & data rate graph



Node ip/id	Attack Behaviour	Rules Appied	Class of Attack
192.168.1.10/8	Synflood Attack	Rule_Interval	DOS
192.168.1.19/...	Blackhole Attack	Rule_Retransmis...	U2R
192.168.1.32...	Wormhole Attack	Rule_Integrity	R2L

Fig.9. Intrusion detection Graph

VI.CONCLUSION AND FUTURE WORK

Intrusion detection is a hot concept of the network safety has new kind of defense technology of the network security. Better intrusion detection mechanism has implemented the proposed architecture with using Hybrid Intrusion Detection Technique. This proposed intrusion detection architecture is designed to detect attacks. The aim was to improve the detection rate and decrease the false positive rate with increasing nodes.

This paper includes a proposed hybrid model of intrusion detection for WSN. This detection framework is evaluated and demonstrated for 100 node packet transmitted which detected many more attack such as wormhole, blackhole and sybil. We have simulated network for 55 node for more than 60 second , result as shown in various graph & figures. This could detected attack & reduce energy power consumption is less. So we used the density of the network is high and there is a high probability of collisions in WSNs. The detection modules involve less energy consumption than techniques proposed in previous works because here cluster based technique is used. The model setup creates identified attack behavior into the network and detected attacks. In the future work, advance research on this topic will be performed, with detailed simulation of different attack, to test the performance , make comparison with other current techniques of HIDS. The result will be enhanced our expectation.

REFERENCES

[1]I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: a survey*”, Computer Networks, 38:393-422, 2002.*

[2] J. Kahn, R. Katz, and K. Pister, “Next century challenges : Mobile networking for smart dust”, *In 5th ACM/IEEE Annual International Conference on Mobile Computing (MOBICOM 1999), pages 271278, 1999.*

[3] Chong E., Loo M., Christopher L., Marimuthu P., “Intrusion Detection for Routing Attacks *In Sensor Networks,” The University of Melbourne, 2008.*

[4] R. A. Kemmerer and G. Vigna, “Intrusion Detection: A Brief History and Overview,” *Computer Society, Vol. 35, No. 4, 2002, pp. 27-30. doi:ieeecomputersociety.org/10.1109/MC.2002.10036*

[5] Ch. Krügel and Th. Toth, “A Survey on IntrusionDetection Systems,” *TU Vienna, Austria, 2000.*

[6] A. K. Jones and R. S. Sielken, “Computer System Intrusion Detection: A Survey,” *University of Virginia, 1999.*

[7] K. Scarfone and P. Mell, “Guide to Intrusion Detection and Prevention Systems (IDPS),” *NIST 800-94, Feb 2007.*

[8] G. Maselli, L. Deri and S. Suin, “Design and Implementation of an Anomaly Detection System: an Empirical Approach,” *University of Pisa, Italy, 2002*.

[9] S. Northcutt and J. Novak, “Network Intrusion Detection: An Analyst’s Handbook,” *New Riders Publishing, Thou-sand Oaks, 2002.*

[10] V. Chandala, A. Banerjee and V. Kumar, “Anomaly Detection: A Survey, ACM Computing Surveys,” *University of Minnesota, September 2009.*

[11] R. A. Kemmerer and G. Vigna, "Intrusion detection a brief history and overview," *Computer, 35(4), 2002, pp. 27-30.*

[12] Y. Qiao and X. Weixin, “A network IDS with low false positive rate,” Proceedings of the 2002 Congress on Evolutionary Computation, 2, 2002, pp. 1121-1126.

[13] Y. Qiao and X. Weixin, "A network IDS with low false positive rate," *Proceedings of the 2002 Congress on Evolutionary Computation, 2, 2002,pp. 1121-1126.*

[14] W.T. Su, K.M. Chang and Y.H. Kuo, “eHIP: An energy-efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks,” *Computer Networks, 51(4), 2007,pp. 1151-1168.*

[15] A. Becher, Z. Benenson, and M. Dornseif, “Tampering with motes: Real-world physical attacks on wireless sensor networks,”

Proceeding of the 3rd International Conference on Security in Pervasive Computing (SPC), pp. 104–118, April 2006.

[16] S. Mohammadi, R. A. Ebrahimi and H. Jadidoleslamy, "A Comparison of Routing Attacks on Wireless Sensor Networks," *International Journal of Information Assur-ance and Security, Vol. 6, No. 3, 2011, pp. 195-215.*

[17] M. Saxena, "Security in Wireless Sensor Networks: A Layer-based Classification," Department of Computer Science, Purdue *University,2011.https://www.cerias.purdue.edu/apps/reports_and_papers/view/3106*

[18] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, Alaska, 11 May 2003, pp. 113-127.*

[19] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," *NIST 800-94, Feb 2007.*

[20] J. Yick, B. Mukherjee and D. Ghosal, "Wireless Sensor Network Survey," Elsevier's Computer Networks, *Vol. 52No. 12, 2008, pp. 2292-2330. doi:10.1016/j.comnet.2008.04.002*

[21] W.T. Su, K.M. Chang and Y.H. Kuo, "eHIP: An energy-efficient hybrid intrusion prohibition system for cluster-based wireless sensor networks," *Computer Networks, 51(4), 2007, pp. 1151-1168.*

[22] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks, 1(2-3), 2003, pp. 293-315.*

[23] Y. Wang, G. Attebury and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys & Tutorials, 8(2), 2006, pp. 2-23.*

[24] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," *Computer, 35(10), 2002, pp. 54-62.*

[25] R. A. Kemmerer and G. Vigna, "Intrusion detection a brief history and overview," *Computer, 35(4), 2002, pp. 27-30.*

[26] Tzeyoung M. W., IATAC, "Intrusion Detection Systems," *6th Edition, Information Assurance Tools Report; Aug, 2009*

[27]Lunt T. F., Tamaru A., Gilham F., Jagannathan R., Jalali C., Peter G. N., "A Real-Time Intrusion-Detection Expert Systems (IDES*)", Final technical report, Computer Science Laboratory, SRI International, 1992.*

[28] Smaha, S. E., Haystack, "An intrusion detection system," in Proceedings of the Fourth Aerospace Computer Security Applications Conference, 1988.

[29] Javitz H. S., Valdes A., "The NIDES statistical component: Description and justification," *Technical Rep. SRI International, Comp. Sci. Lab, 1994.*

[30] Yi-an H., Wenke L., "A Cooperative Intrusion Detection System for Ad-Hoc Networks," *Proceedings of the 1st ACM workshop on Security of ad-hoc and sensor networks, Pages 135-147, 2003.*

[31] Eskin E., Arnold A., Prerau M., Portnoy L., and Stolfo S., "A Geometric Framework for Unsupervised Anomaly Detection: Detecting Intrusions in Unlabeled Data*," In Applications of data mining in computer security, Kluwer,2002.*

[32] W. R. Heinzelman, A. Chandrakasan , and H. Balakrishnan, "Energy Efficient Communication Protocol for Wireless Microsensor Networks*", Proceeding of the 33rd Hawaii International Conference on System Sciences, IEEE, 2000, pp.1-10.*

[33] S. Lindsey, and C. Raghavendra, "PEGASIS: Power Efficient Gathering in Sensor Information System*", In Proc. IEEE Aerospace conference, vol.3, 2002, pp.1125-1130.*

[34] O. Younis, and S. Fahmy, "Heed: A hybrid, Energy -Efficient Distributed Clustering Approach for Ad Hoc Sensor Networks", *IEEE Transactions on Mobile Computing, vol.3, No.4, 2004, pp.366-379.*

[35] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network*", Chayang University of Technology, Taiwan, IEEE 2010, pp. 114-118*

[36] K. Q. Yan, S. C. Wang, S. S. Wang and C. W. Liu, "Hybrid Intrusion Detection of Cluster-based Wireless Sensor Network", *Proceedings of International Multi Conference of Engineers and Computer Scientists , Hong Kong, Vol. 1, 2009.*

Ansar I Sheikh is currently doing M.Tech in (CSE) from Patel College of Science & Technology.

Pankaj Kewadkar is Asst. Prof. in PIES, Bhopal. He has published many paper in international journal.