Ms. Rachana Deshmukh, Prof. Manoj Sharma, Ms. Rashmi Deshmukh / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
www.ijera.com Vol. 3, Issue 4, Jul-Aug 2013, pp.2153-2161

An Intrusion Detection Using Hybrid Technique in Cluster Based Wireless Sensor Network

Ms. Rachana Deshmukh[1], Prof. Manoj Sharma[2], Ms. Rashmi Deshmukh[3]

[1]*Dept. of IT, NRI-Institute of Info Sciences & Tech., Bhopal, M.P., India.*
[2]*Asst. Prof., Dept. of IT, NRI-Institute of Info Sciences & Tech., Bhopal, M.P., India.*
[3]*Dept. of CSE, Dr. Babasaheb Ambedkar College of Engineering & Research, M.S., India.*

Abstract

Wireless Sensor Networks (WSNs) are playing a fundamental role in emerging pervasive platforms that have potential to host a wide range of next generation civil and military applications. Wireless sensor network (WSN) is regularly deployed in unattended and hostile environments. The WSN is vulnerable to security threats and susceptible to physical capture. Thus, it is necessary to use effective mechanisms to protect the network. Intrusion detection system is one of the major and efficient defensive methods against attacks on wireless sensor network. Sensor networks have different characteristics and hence security solutions have to be designed with limited usage of computation and resources. In this paper, the architecture of hybrid intrusion detection system (HIDS) is proposed for wireless sensor networks. In order to get hybrid scheme, the combined version of Cluster-based and Rule-based intrusion detection techniques is used and eventually evaluated the performance of this scheme by simulating the network. The simulation result shows that the scheme performs intrusion detection using hybrid technique and detection graph shows ratings like attack rating, data rating and detection net rating with the attack name and performs better in terms of energy efficiency and detection rate.

Index terms: Wireless Sensor Network, Rule-based & cluster-based intrusion detection, Hybrid, Anomaly detection.

I. Introduction

Wireless Sensor Networks (WSN) is one of the most interesting and promising areas over the past few years. It is often considered as a self-organized network of low cost, power and complex sensor nodes have been typically been designed to monitor the environment for physical and chemical changes, disaster regions and climatic conditions. These networks may be very large systems comprised of small sized, low power, low-cost sensor devices that collect detailed information about the physical environment. WSN's perform both routing and sensing activities and are configured in ad hoc mode for communication.

The sensor nodes are light and portable, with sensing abilities, communication and processing board, and are used for sensing in critical applications. Each device has one or more sensors, embedded processor(s), and low-power radio(s), and is normally battery operated value of sensor networks however, lies in using and coordinating a vast number of such devices and allows the implementation of very large sensing tasks. In a usual scenario, these networks are deployed in areas of interest (such as inaccessible terrains or disaster sites) for fine grained monitoring in various classes of applications [1]. The flexibility and self-organization, fault tolerance, high sensing fidelity, low-cost, and rapid deployment characteristics of sensor networks create many new and exciting application areas for remote sensing WSNs. Following figures(1,2) shows the distinguishing features of simple and cluster-based wireless sensor networks.

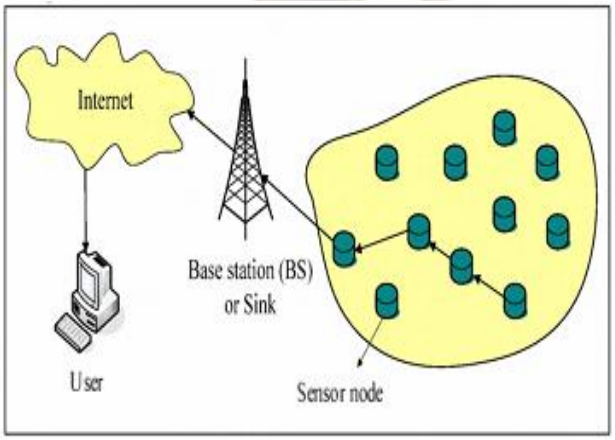

Figure 1. Flat WSN

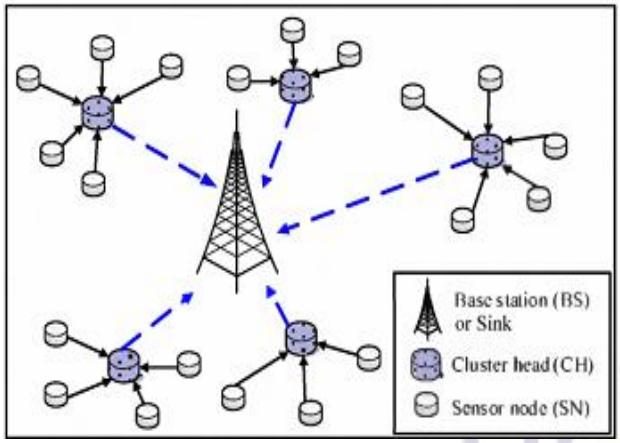

Figure2. Cluster-Based WSN

WSNs are energy constrained, critical and very susceptible to various routing and malicious attack which include spoofing, sinkhole, selective forwarding, Sybil, wormhole, black hole, and denial of service (DoS) attacks. These have been described in [3]. Prevention mechanisms which include authentication, cryptography, and installation of firewalls have been employed to secure networks. However, these mechanisms only pose a first line of defense and do not provide enough security for wireless networks. These mechanism can be exploited because it has been proved that no matter the amount of prevention techniques incorporated into a network, there will always be weak links . Therefore, there is a need to develop mechanisms that will be added to the existing techniques to provide a better security and guarantee survivability. Hence the development of Intrusion Detection System (IDS) referred to as a second line of defense. Many IDS have been proposed from several researchers and some of them are discussed in the related works. However, a number of them suffer from a high False Positive Rate (FPR) which describes an instance where the IDS falsely report a legal activity as an anomaly. Anomaly detection uses activities that significantly deviate from the normal users or programs' profile, to detect possible instances of attacks. It detects new attacks without necessarily been required to know prior intrusions. In this work, our goal is to simulate IDS for Clustered based WSNs by presenting an approach that provides high detection accuracy with a low FPR

II. An Intrusion Detection System (IDS)

Intrusion, i.e. unauthorized access or login (to the system, or the network or other resources) [4]; intrusion is a set of actions from internal or external of the network, which violate security aspects (including integrity, confidentiality, availability and authenticity) of a network's resource [5,6]. Intrusion detection is a process which detecting contradictory activities with security policies to unauthorized access or performance reduction of a system or 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.:

- It is a hardware, software or combination of both systems; with aggressive-defensive approach to protect secrete information, systems and networks [7, 8].
- Usable on host, network [9] and application levels.
- Analyzing traffic, controls communication and ports, detecting attacks and occurrence vandalism, by internal users or external attackers.
- Concluding by using deterministic methods (based on patterns of known attacks) or non-deterministic [8,9] (to detecting new attacks and anomalies such as determining thresholds);
- Informing and warning to the security manager [6,7,10] (sometimes disconnect suspicious communications and block malicious traffic);
- Determining identity of attacker and tracking him/her/it;

The main three functionalities for IDS, including: monitoring (evaluation), analyzing (detection) and reacting (reporting) [5,7] to the occurring attacks on computer systems and networks. If IDS be configured, correctly; it can represent three types of events: primary identification events (like stealthy scan and file content manipulation), attacks (automatic/manual or local/remote) and suspicious events. The IDS acts as a network monitor or an alarm. It prevents destruction of the system by raising an alarm before the intruder starts to attack. The two major modules of intrusion detection include anomaly detection and misuse detection [11]. Anomaly detection builds a model of normal behavior, and compares the model with detected behavior. Anomaly detection has a high detection rate, but the false positive rate is also high. The misuse detection detects the attack type by comparing the past attack behavior and the current attack behavior. The misuse detection has high accuracy but low detection rate. Especially, the misuse detection cannot detect unknown attacks, which are not in the model base. Many researchers discuss the module of hybrid detection to gain both the advantages of anomaly detection and misuse detection [12, 13]. This combination can detect unknown attacks with the high detection rate of anomaly detection and the high accuracy of misuse detection. The Hybrid Intrusion Detection System (HIDS) achieves the goals of high detection rate and low false positive rate. In this section, a HIDS is discussed in a CWSN.

Cluster head (CH) is one of SNs in the CWSN but the capability of CH is better than other SNs [14]. Additionally, the CH aggregates the sensed data from other SNs in its own cluster. This makes a target for attackers.However, the CH is used to detect the intruders in our proposed HIDS. This not only decreases the consumption of energy, but also efficiently reduces the amount of information. Therefore, the lifetime of WSN can be prolonged.

2.1 Requirements for IDS in Sensor Networks

In this section we elaborate on the requirements that an IDS system for sensor networks should satisfy. To do so, one has to consider some specific characteristics of these networks. Each sensor node has limited communication and computational resources and a short radio range. Furthermore, each node is a weak unit that can be easily compromised by an adversary [15], who can then load malicious software to launch an insider attack. In this context, a distributed architecture, based on node cooperation is a desirable solution. In particular, we require that an IDS system for sensor networks must satisfy the following properties:

1) Localize auditing: An IDS for sensor networks must work with localized and partial audit data. In sensor networks there are no centralized points (apart from the base station) that can collect global audit data, so this approach fits the sensor network paradigm.
2) Minimize resources: An IDS for sensor networks should utilize an small amount of resources. The wireless network does not have stable connections , and physical resources of network and devices, such as bandwidth and power, are limited. Disconnection can happen at any time. In addition, the communication between nodes for intrusion detection purposes should not take too much of the available bandwidth.
3) Trust no node: An IDS cannot assume any single node is secure. Unlike wired networks, sensor nodes can be very easily compromised. Therefore, in cooperative algorithms, the IDS must assume that no node can be fully trusted.
4) Be truly distributed: That means data collection and analysis is performed on a number of locations. The distributed approach also applies to execution of the detection algorithm and alert correlation.
5) Be secure: An IDS should be able to withstand a hostile attack against itself. Compromising a monitoring node and controlling the behavior of the embedded IDS agent should not enable an adversary to revoke a legitimate node from the network, or keep another intruder node undetected.

III. Related Work

3.1. Attacks in WSN

Attacks can be classified into two main categories, based on the objectives of intrusion [21]. The comparison of attacks in WSN is shown in Table 1 [22,23,24]. However, the majority of attack behavior consists of the route updating misbehavior, which influences data transmission. In the application of CWSN, the data is sensed and collected by SNs, and is delivered to CH to aggregate. The aggregated data is then sent to sink from CH. Therefore, CH is a main target for attack.

Table1. The different types of attacks in WSN

Attack Name	Behavior
Spoofed, Altered, or Replayed routing information	Route updating misbehavior
Select forward	Data forwarding misbehavior
Sinkhole	Route updating misbehavior
Sybil	Route updating misbehavior
Wormholes	Route updating misbehavior
Denial of Service	Data forwarding misbehavior
Hello floods	Route updating misbehavior
Acknowledgment spoofing	Route updating misbehavior

3.2. Analytic Tool of Intrusion Detection

The proposed HIDS in our research not only efficiently detects attack, but also avoids the waste of resources. First, a large number of packet records are filtered by using the intrusion detection module, and then complete the whole detection. Also with reference to the mode of normal behavior, the detection module detects the normalcy of current behavior, as determined by the rules.

The detection module determines if the current behavior is an attack, and the behavior of the attacks. Rule-based presents the thoughts of expert [25]. Because human thought is very complicated, the knowledge could hardly be presented by algorithms. Therefore, a rule-based method is used to analyze results.Additionally, the rules are logged in a rule base after they have been defined. The basic method of expression of rule is "if... then..." that means if "condition" is established and then the "conclusion" will occur.
With the increasing growth in technology, many researchers have proposed several IDSs to secure WSNs. The vulnerabilities

associated with wireless networks make it imperative to imbibe IDS in WSNs.[26] Defined IDS as an act of monitoring and detecting unwanted actions or traffic on a network or a device. This is achieved by monitoring the traffic flow on the network. Examples of published work on anomaly detection systems are IDES [27], HAYSTACK [28], and the statistical model used in NIDES/STATS [29] which is a more recent approach and presents a better anomaly detection system compared to the others afore mentioned. A process of developing intrusion detection capabilities for MANET was described in [30]. The authors discussed how to provide detailed information about intrusions from anomaly detection by showing that for attacks; as simple rule can be applied to identify the type of attack and the location of the attacking node. A geometric framework has been presented in [31] to address unsupervised anomaly detection such that for example, when a packet is trans mitted and is being analyzed, a decision needs to be made as to whether it is normal or abnormal. To do this, the packet is represented with a set of features which are encoded such that the traffic is mapped to a point a in a feature A, hence a € A. If a packet is seen in separate region where other packets have not been seen, then it is considered an anomalous, otherwise, it is normal.

IV. System Architecture and Network Model

The proposed HIDS consists of an intrusion detection module and decision making module. Intrusion detection module filters a large number of packet records using the rule base technique. Decision making module is used to take an administrative action on the false node with the help of base station.

4.1. System Architecture and Network Structure

Here, the new Hybrid Intrusion Detection Model (HIDS) is proposed for Cluster Based Wireless Sensor Network (CWSN). This consists of two modules as shown in Figure 3. First, the Intrusion Detection Engine is used to filter the incoming packets and classify is as normal or abnormal. The packets identified as an abnormal are passed to the decision making module. The decision-making module is used to determine whether the intrusion occurs and the type of intrusion or attacks behavior. Finally, the decision making module returns this information to the base station to follow-up treatment on intruder node.

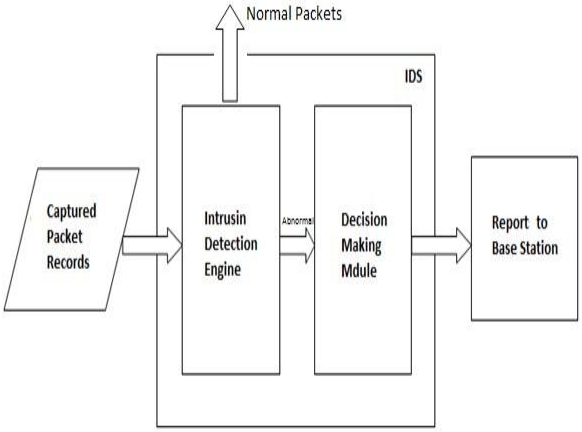

Figure 3. Proposed System Architecture

In this proposed model, we use a hierarchical topology that divide the sensor network into clusters, each one having a cluster head (CH) as shown in Figure 4. Here the sensors nodes are fixed and assuming that the cluster heads having the more energy than the other sensor nodes. The objective of this architecture is to save the energy that allows the network life time prolongation and reduce the amount of information in the network. Some of the Cluster-based routing protocols founded in the literature are: LEACH [32], PEGASIS [33] and HEED [34]. The Figure5 shows the deployment and setting up of the WSN. Here, we used the three types of nodes in the network each of which indicated with different colors. Yellow color shows the Base Station (BS), Green color represents for Cluster Head (CH), all the sensor nodes are indicated by red color and finally the intruder node with blue color in the sensor field. The cluster based technique is used to form clusters in the WSN as shown in the Figure5.

4.2. IDS Techniques Used

In the proposed Hybrid Approach [35, 36], the two techniques i.e. Cluster-Based and Rule-Based techniques are merged to form Hybrid Intrusion Detection technique. Hybrid detection used to gain the advantages of both Cluster-Based approach and Rule-Based approach. This combination provides simplicity, easy to operate, low consumption of energy and provide high safety. The Hybrid Intrusion Detection System (HIDS) achieves the goals of high detection rate and low false positive rate.

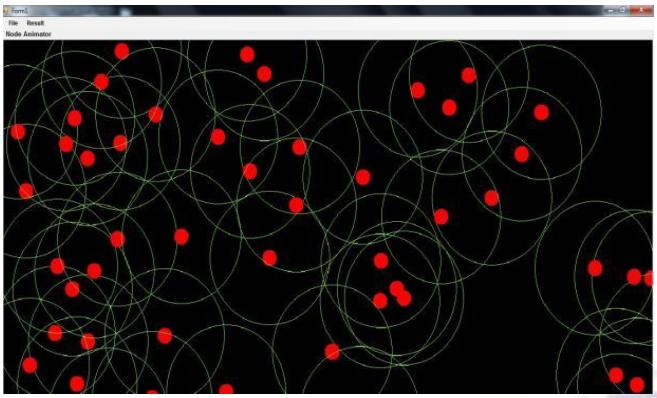

Figure 4: Deployment and Setting up WSN

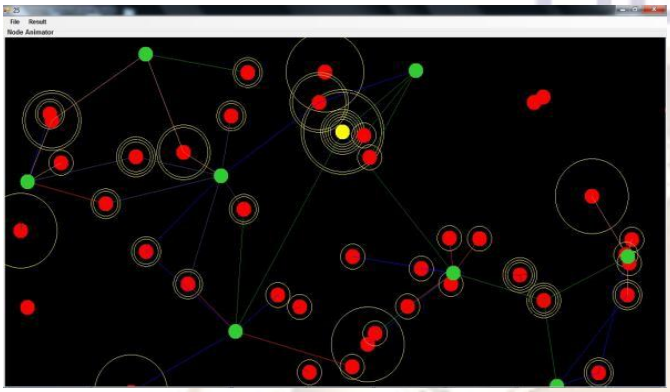

Figure 5. Forming Clusters in WSN

4.2.1. Clusters-Based.

Clustering is known as hierarchical of WSN [37]. To divide the network nodes into head cluster and members of nodes is the basic idea. Cluster head is the centre of a cluster. Through cluster head's information fusion and forwarding to the member node of cluster, other members of nodes transmit to the base station.

Function of Base Station:

1) All nodes are able to send data to BS via Cluster Head.
2) Base station has all the information regarding each Cluster (number and MAC address).
3) The removal or addition of any node in a Cluster is monitored by the Base Station. Poll status of each node is received with MAC address.
4) Base station runs task of MAC address tracking, MAC address history and management of database.
5) The Base Station has the capability to seize the operation of any node in the network.

Function of Cluster Head:

1) Cluster Heads keep track of each node and sends periodic status information to the Base Station.
2) Cluster heads receives data from its nodes and sends necessary information.
3) Cluster Heads (CHs) transmits data to Base Station after performing data reception and compression.

4.2.2. Rule-based.

Rule -based intrusion detection [9] is the collection and classification of data, the data is placed in a queue, using the FIFO principle. In our model while monitoring the network this rules are selected appropriately and applied to the monitored data. If the rules defining an anomalous condition are satisfied, an intrusion is declared. The algorithm has three phases for detecting intrusions. In the first phase monitor nodes monitors the data. In the second phase the detection rules, are applied, in increasing order of complexity, to the collected information to flag failure. The third phase is the intrusion detection phase, where the number of failure flagged is compared to the expected number of the occasional failures in the network. Occasional failures include data alteration, message loss, and message collision. An intrusion alarm is raised if the number of failures flagged exceeds the expected number of occasional failures. The rule base methods are fast, simple and require less data.

Rules and Definition

Development of this IDS to a target cluster-based WSN are divided into three following important steps: (1) pre-select, from the available set of rules, those that can be used to monitor the features defined by the designer; (2) compare the information required by the pre-selected rules with the information available at the target network to select rules definitively; and (3) set the parameters of the selected rules with the values of the design definitions. Definitions of the rules used are presented in the following:

Integrity Rule: to avoid data fusion or aggregation
by other sensor nodes, the message payload must be the same along the path from its origin to a destination. Attacks where the intruder modifies the contents of a received message can be detected by this rule.

Jamming Rule: The number of collisions associated with a message must be lower than the expected number in the network. The jamming attack, where a node introduces noise into the network to disturb the communication channel, can be detected by this rule.

Interval Rule: if the time interval between the receptions of two consecutive messages is longer or shorter than the allowed time limits, a failure is raised. Two attacks that will probably be detected by this rule are the negligence attack and the exhaustion attack. In the negligence attack, the intruder does not send data messages generated by

a tampered node. While in the exhaustion attack, the intruder increments the message - s ending rate in order to increase the energy consumption of other nodes in the cluster.

Repetition Rule: the same message can be retransmitted by a node only a limited number of times. This rule can detect an attack where the intruder s ends the same message several times, thus p r o m o t i n g a denial of service attack.

Radio Transmission Range: all messages listened to by the monitor node must be originated from one of the nodes w i t h i n its c l u s t e r. Attacks like wormhole and hello flood, where the intruder s ends messages to a far located node using a more powerful radio, can be detected by this rule.

Retransmission Rule: the monitor listens to a message, pertaining to one of its neighbors as its next hop, a n d e x p e c t s that t h i s n o d e will forward the received message, which does not happen. Two types of attacks that can be detected by this rule are the black hole and the s elective forwarding attack. In both of them, the intruder suppresssome or all messages that w e r e supposed to be retransmitted, preventing them from reaching their final destination in the network.

Delay Rule: the retransmission of a message by a monitor's neighbor must occur before a defined timeout. Otherwise, an attack will be detected.

Algorithm 1: Rules application procedure of IDS

1: for all messages in data structure array do
2: for all rules specific to the message in descending order by weight does
3: apply rule to the message;
4: if (message == fail) then
5: increment failure counter for the node based on weight; [failure counter = failure counter + weight. 6: discard message;
7: break;
8: end if
9: end for
10: discard message;
11: end for

Algorithm 1 shows the procedure of rules application on messages in the network. The algorithms apply rules on all t h e messages. If m e s s a g e fails according t o t h e r u l e, t h e n t h e f a i l u r e counter will be incremented and discards all the messages.

V. Network Simulation and Results

The above proposed model has been simulated using Visual Studio .Net framework. The simulator can also be used to view the topology generated by the initial s elf organization algorithm LEACH [32] for setting the WSN as shown in Figure 2. A comparison assumed to have the same number of clusters or sensing zones, no packet collisions occurred. It also assumed that there were no packet errors during transmission and reception.

In this proposed architecture, the wireless sensor network is divided into the s mall clusters The hierarchical clustering is used to divide the sensor nodes. After the clustering process finished, the cluster head have been s elected dynamically according to the current status of the nodes and formed the Cluster based WSN as shown in Figure 3. Generally, the node having highest energy left elected as a cluster head. Simulation runs with the following

Simulation parameters

1	**Routing Protocol**	**AODV**
2	**Mac Layer Protocol**	**802.11**
3	**Total No. Of Nodes**	**50**
4	**Traffic Type**	**CBR**
5	**Simulation Topology**	**1024cm * 768cm**
6	**Simulation Time**	**100 sec**
7	**Packet Size**	**512 Kbytes**

Nodes are deployed randomly over an area of 1024 cm X 768 cm. The node closest to the centre of the deployment area is selected as sink or base station (BS), which is resources not limited, secure and safety for any advisory attackers and acts as an administrator for taking appropriate action on the intruder nodes . The network has been simulated with AODV routing protocol with Mac layer 802.11. 50 nodes are taken in the network within the simulation area and constant bit rate of traffic type is us ed. The network performance is observed for the simulation time 100 seconds. The standard packet size is used i.e. 512 Kbytes

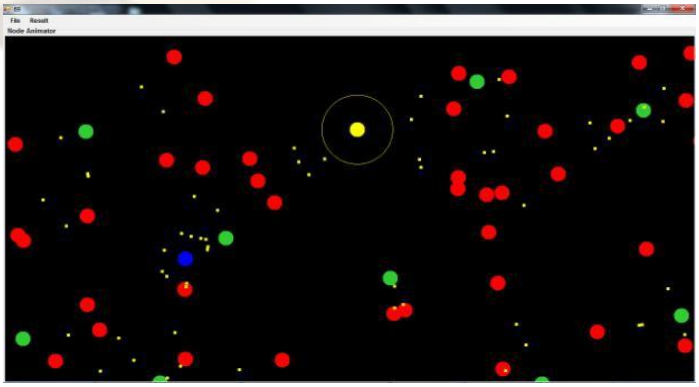

Figure 5. Introducing attacks in WSN

The simulation is run in different scenarios , each scenario has different parameter values , and malicious nodes inject the malicious packets in the whole sensor network as shown in Figure 4. The figure shows the false packets in yellow color a round malicious node (Blue) are spreading in the whole network. Proposed system must recognize these nodes and refuse their connection for next round as an administrative action against malicious nodes with the help of BS.

After the simulation of network, the communication Among the nodes has been traced in trace.txt file. This trace file keeps all the communication records of the network and with the help of these records we can analyze the attack behavior generated by the intruder nodes. The trace file is shown in the Figure 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 figures. Figure 6, 7, 8 shows the s ending, receiving, delay graphs of the network respectively . Sending and receiving graph shows the sending and receiving of packets in the networks. The networks performance is indicated by figure 9. He re attack rating is shown which represents the attacker's packets and data rating shows the amount data transmitted by all the nodes. Finally the detection of the attacks is shown in Figure 10 with their ratings and names . The wormhole, blackhole and s yncflood attacks have been detected.

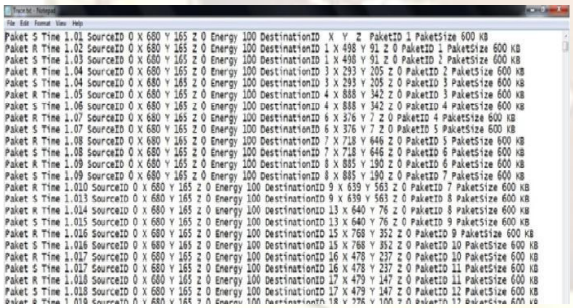

Figure 6. Trace file of WSN Network

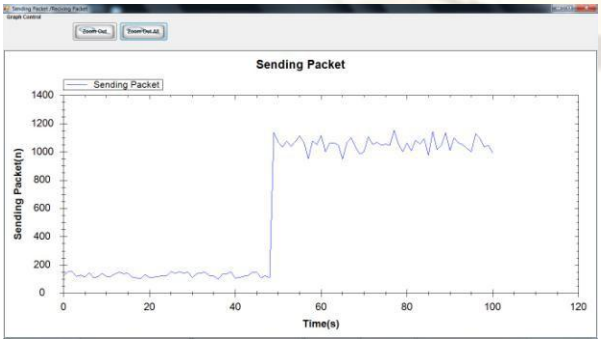

Fig 7: Graph of sending packets in Network

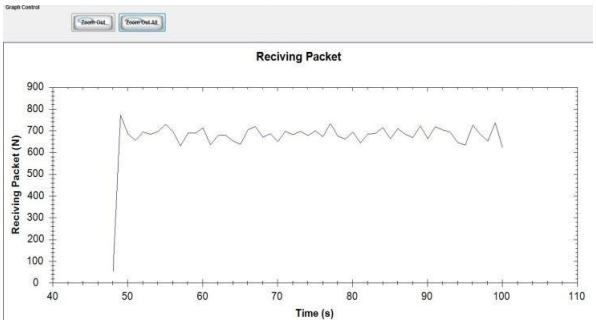

Figure 8. Graph of receiving packets in Network

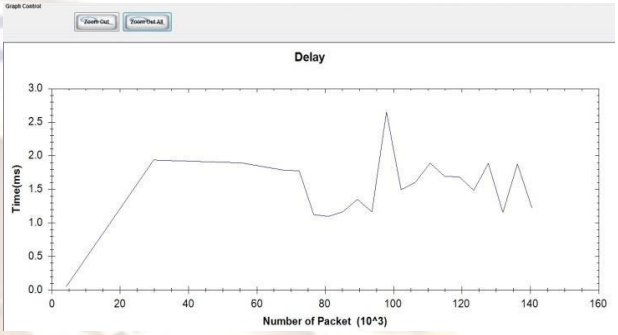

Figure 9. Graph of delay in Network

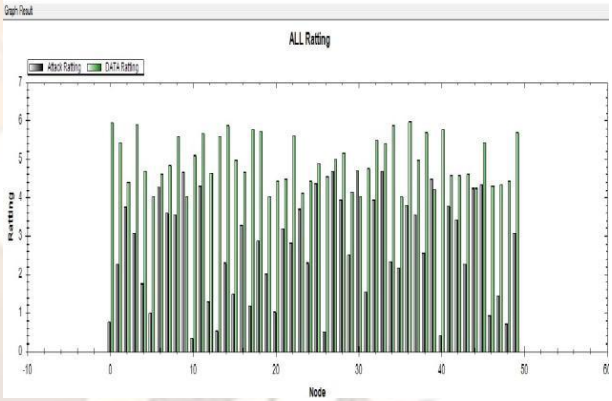

Figure 10. Graph of attack and data rating in WSN

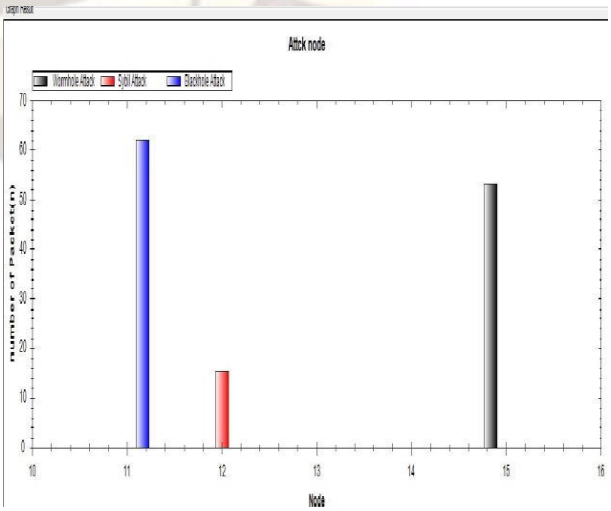

Figure 11. Intrusion detection Graph

VI. Conclusion and Future Work

Intrusion detection is an unavoidable field of the network security research. In our research a new technique based on hybrid detection (i.e. combination of the features of rule-based and cluster-based detection techniques) is used. Hence, a better intrusion detection mechanism is presented in this paper. This proposed intrusion detection architecture determines the presence of an intrusion and also classifies the type of attack. The administrator herein takes the appropriate action on the submitted to it by the cluster head from time- to-time. The aim was to improve the detection rate and decrease the false positive rate.

In the future work, further research on this topic will be performed, with detailed simulation of different attack scenarios, to test the performance of the proposed model and to make comparison with other current techniques of HIDS and also will be able to discover and classify new types of attacks. The result will be available in the near future.

References

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

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

[3] Chong E., Loo M., Chrisom her L., M rimuthu 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," Comp uter Society, Vol. 35, No.4, 2002, p p. 27-30.

[5] Ch. Krügel and Th. Toth, "A Survey on Intrusion Detection Systems," TU Vienna, Austria, 2000.

[6]. A. K. Jones and R. S. Silken, "Computer Sy stem Intrusion Detection: A Survey," University of Virginia, 1999. [7]. K. Scarf one and P. M ell, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST 800-94, Feb 2007.

[8]. G. Maselli, L. Deri and S. Suin, "Design and I mplementation of an Anomaly Detection System: an Empirical App roach," University of Pisa, Italy, 2002.

[9]. S. Northcutt and J. Novak, "Network Intrusion Detection: An Analy st's Handbook," New Riders Publishin g, Thou-sand Oaks, 2002.

[10]. V. Chandala, A. Banerjee and V. Kumar, "Anomaly Detection: A Survey, ACM Computing Survey s," University of Minnesota, September 2009.

[11] R.A. Kemmerer and G. Vigna, "Intrusion detection a brief history and overview," Co mp uter, 35(4), 2002, p p. 27-30.

[12] Y. Qiao and X. Weixin, "A network IDS with low false positive rate," Proceedings of the 2002 Congress on Evolutionary Comp utation, 2, 2002, p p. 1121-1126.

[13] Y. Qiao and X. Weixin, "A network IDS with low false positive rate," Proceedings of the 2002 Congress on Evolutionary Comp utation, 2, 2002,p p. 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," Comp uter Networks, 51(4), 2007, pp.1151-1168.

[15] A. Becher, Z. Benenson, and M. Dornseif, "Tamp erring with motes: Real-world physical attacks on wireless sensor networks," Proceedin g of the 3rd International Conference on Security in Pervasive Computing (SPC), p p. 104–118, April 2006.

[16] S. Mohammadi, R. A. Ebrahimi and H. Jad idoleslamy ,"A Comparison of Routing Attacks on Wireless Sensor Networks," International Journal of Information Assurance and Security, Vol. 6, No. 3, 2011, p p. 195-215.

[17] M. Saxena, "Security in Wireless Sensor Networks: A Layer based Classification," Dep artment of Comp uter Science, Purdue University, 2011. https://www.cerias.p urdue.edu/ap ps/reports_and_p apers/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 M ay 2003, p p. 113-127.

[19] K. Scarfone and P. M ell, "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 Comp uter Networks, Vol. 52, No. 12, 2008, p p. 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," Comp uter 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 n networks," IEEE Communications Surveys & Tutorials, 8(2), 2006, pp. 2-23. [24] A. D. Wood and J. A. Stankovic, "Denial of serv ice in sensor networks," Comp uter, 35(10), 2002, pp. 54-62.
[25] R. A. Kemmerer and G. Vigna, "Intrusion detection a brief history and overview," Comp uter, 35(4), 2002.
[26] Tzeyoung M. W., IATAC, "Intrusion Detection Systems," 6th Edition, Information Assurance Tools Rep ort; 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 rep ort, Comp uter Science Laboratory, SRI International, 1992.
[28] Smaha, S. E., Hay stack, "An intrusion detection system," in Proceedings of the Fourth Aerospace Comp uter Security App lications 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, Pages135-147, 2003.
[31] Eskin E., Arnold A., Prerau M ., Portnoy L., and Stolfo S., "A Geometric Framework for Unsup- ervised Anomaly Detection: Detecting Intrusions in Unlabeled Data," In App lications of data mining in comp uter security , Kluwer, 2002.
[32] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy Efficient Communication Protocol for Wireless Micro sensor Networks", Proceeding of the 33rd Hawaii International Conference on System Sciences, IEEE, 2000, pp.1-10.
[33] S. Lindsey and C. Raghav endra, "PEGASIS: Power Efficient Gathering in Sensor Infor mation System", In Proc.IEEE Aerospace conference, Vo l.3, 2002, p p .1125-1130.
[34] O. Younis, and S. Fahmy, "Heed: A hybrid, Energy - Efficient Distributed Clustering Ap p roach for Ad Hoc Sensor Networks", IEEE Transactions on Mobile Computing, vol.3, No.4, 2004, pp.366-379.
[35] K. Q. Yan, S. C. Wangg, S. S. Wang and C. W. Liu, "Hybrid Intrusion Detection System for Enhancing the Security of a Cluster-based Wireless Sensor Network", Chay ang University of Technology, Taiwan, IEEE 2010, p p .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 MultiConference of Engineers and Comp uter Scientists , Hong Kong, Vo l. 1, 2009.
[37] S. Doumit and D. P. Agrawal, "Self-organized Critically & stochastic learning based intrusion detection system for wireless sensor network". MILCOM2003-IEEE/ACM transactions on Networking, VO l. 11(1), 2003, p p 2-16.