ISSN: 2321-7782 (Online)
Volume 3, Issue 8, August 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Anomaly Based Intrusion Detection System

Gurpreet Kaur[1]
Research scholar
MMICT & BM
MMU Mullana, (Haryana)
India

Rshma Chawla[2]
Assistant Professor(Computer Science),
M.M. University,
Mullana, Ambala (Haryana)
India

Abstract: Wireless Sensor Networks are facing assorted vulnerability attacks and security issues from multiple dimensions as well as directions. A number of wireless network attacks can be projected to damage various aspects and security points of the networks. The wireless attacks include DDoS Attack, Sybil Attack, Wormhole Attack, Blackhole Attack, etc. Wireless Sensor Networks are having major role in rising invasive platform for various applications such as corporate, military, banking, financial and many other sectors. It is necessary to prevent sensor network from these attacks for security purpose. Now days, intrusion detection system is the most important and well organized protective methods used against WSN. To prevent malicious nodes from joining the sensor network, access control is required in the design of sensor network protocols. The network signals are collected by sensor nodes in such a way that an unauthorized entity cannot make arbitrary queries and thus the illegitimate access can be denied with the detailed logging of the access. This research paper proposes secure IDS for WSN using access control mechanism. The proposed approach accesses the problem of high false positive rate and tries to manage as well as log the misuse and anomaly detection given to an idea for a precise solution.

Keywords: Intrusion Detection System, Network Security, Vulnerability Analysis, WSN Security

I. Introduction

A Wireless Sensor Network (WSN) consists of distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location. The modern networks are bi-directional, also enabling control of sensor activity. The development of wireless sensor networks was motivated by military applications .Now days such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on. The typical WSN scenario consists of a number of sensor nodes which vary from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver with an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The propagation technique between the hops of the network can be routing or flooding.

Various applications of Wireless Sensor Networks includes Health Care, Area Monitoring, Environmental and Earth Monitoring, Air Quality Monitoring, Air Pollution Monitoring, Forest Fire Detection, Landslide Detection, Water Quality Monitoring, Natural Disaster Prevention and many others.

The main characteristics of a WSN include:

- » Power consumption constrains for nodes using batteries or energy harvesting
- » Ability to cope with node failures

- Mobility of nodes
- Communication failures
- Heterogeneity of nodes
- Scalability to large scale of deployment
- Ability to withstand harsh environmental conditions
- Ease of use in the flexible environment

CLUSTERING IN WIRELESS SENSOR NETWORK

Clustering involves grouping nodes into clusters and electing a CH. Members of a cluster can communicate with their CH directly. The key objectives of clustering includes

- Allows Aggregation for collaborative data transfer
- Limits data transmission
- Facilitate the reusability of the resources
- CHs and gateway nodes can form a virtual backbone for inter cluster routing
- Cluster structure gives the impression of a smaller and more stable network
- Improve network lifetime
- Reduce network traffic and the contention for the channel
- Data aggregation and updates take place in CHs

II. Network Intrusion Detection System (NIDS)

Network intrusion detection system (NIDS) is considered as a compelling barrier against system based assaults coordinated to PC systems [1]. This system is considered as a dependable source to distinguish assaults designs, noxious activities and unapproved access to a domain. To keep pernicious nodes from joining the sensor system, access control component are exceptionally required with leaving IDS. It figures out what one will permit another to do regarding assets and articles interceded by the previous. Access control for the most part needs a verification. Validation is a procedure to separate one gathering from another. An Authentication builds up the personality of a client to some piece of the system intricacy by prerequisite of a secret key. Access control is security benefit in remote sensor system. WSN must have the capacity to approve and award clients right to access to the system.

In WSN Scenario, the sensor nodes gather the data from its encompassing surroundings and transmit it to sink node. Sensor nodes are asset limitations. A more broad verification can be PC to PC or procedure to handle and is common in both bearings. It is a developing territory of interdisciplinary research between individuals in the electrical designing software engineering, and among their different controls. It is assembled of a few hundred or even thousand nodes, where every node is joined with one or numerous sensors [2]. Each sensor node of system is utilized to radio handset, a smaller scale controller, a sensor and so forth. Thusly, there is a need to create instrument that will be added to the current systems to give a superior security and insurance survivability. In bunched remote sensor system, because of heterogeneous nature of sensor system the ability of focus head is more noteworthy than general sensor system. The improvement of IDS alluded to as a second line of resistance. Numerous IDS have been proposed by a few scientists. Be that as it may, Most of them experience the ill effects of a high false positive rate (FPR) which portrays an occasion where IDS erroneously report a lead action.

Intrusion is the accumulation of distinctive activity to crush the security parts of a system's asset. Intrusion detection is a procedure to discover superfluous exercises over the systems that corrupt the execution of system[15]. There are three capacities for IDS as takes after: assessment, dissecting and responding. Irregularity detection observes not for known intrusion - the sign yet rather for variations from the norm in the movement. Abnormality detection amasses typical conduct model and look at these distinguished conducts. Its detection rate is high, however false positive rate is likewise disturbing. Conversely of mark detection the intrusion detection choice is framed on the premise of learning of a model of the meddlesome procedure. It ought to be noticed that these indicators attempt to recognize proof of nosy action independent of any foundation activity, i.e. ordinary conduct. The abuse detection identifies new sorts of assault by coordinating with existing conduct of assault and present conduct of assault. Its exactness is high however detection rate is low.

The WSN have security services like authentication, confidentially and availability. It is essential to protect WSNs from attacks and threats [12]. They have limited energy and thus are vulnerable to various routing and malicious attacks like spoofing, wormhole, sinkhole, black hole, denial of service (DOS) attacks.

On the basis of above literature some of the designing challenges in IDS for WSN are as follows:

- Repeated failures and unreliable sensor nodes.
- High false alarm rate.
- High energy consumption.
- Reduce the amount of information in the entire network.
- Application oriented.
- Authentication - It ensures that the retrieval & sending of data is done by authorized parties by identifying its origin.

III. Access Control Mechanism

Access control is needed to identify the identity of user by authentication or authorization. Authentication involves verification of IP address, machine, time etc. If a user is allowed to access the system at all or not. Authorization assumes that the identity of user is known. It determines some specification is allowed. Access control is divided into DAC (discretionary access control) MAC (mandatory access control) RBAC (role based access control) categories. MAC is developed in an atmosphere of military setting and of national security .DAC has its roots in academic, commercial and laboratories research .The RBAC model is an emerging approach to access control that is attracting much attention from both the scientific community and industry.

MAC - It governs access based on the sensitivity level of user and data. It accesses the data granted only if the security levels of user and data satisfy certain constraints[13]. Where the environment is multi layered it will use. In military domains users and files are classified into different levels of hierarchy and user access files. It check the accessibility based on constraints one is read property, star property .Access is allowed when both the constraint are satisfied .Access is checked only if the user is in the same category.

DAC - It governs the access to the information on the basis of the user's identity and authorization. It specify for each user and each data in the system. The access modes are followed by the user to allow the data. Each request of a user to access the data is to be checked[5]. The main advantage of DAC its users can access privileges and burden of security administrator is reduced as resource .User and administrator jointly manage permission. The disadvantage is that it is not appropriate for multilayer systems where information flow is restricted.

RBAC - It has access rights that depend on the role of user. Users are associated with roles. Roles are associated with permission. A user has permission only if the user has an authorized role which is associated with that permission. For Example - Oil Companies

All these models are described as follows –

Table 1 - Classification of Access Control Models

MODELS	**Work**	**Advantage**	**Disadvantage**	**Applications**
DAC	User Identify and Authorization	Higher Security with privileges	Not appropriate for multilayered systems	Corporate Sector
RBAC	Restricted Access	Reduced Complexity and Higher Efficiency	Cost Effective	Banking and Finance
MAC	Security in hierarchy	Simplified	Confidentiality Issues	Defense

IV. Related Work

Mourabit [2] described the proposal for an intrusion detection system architecture that uses multi agent system. It is an effective choice for many research and application areas due to several reasons, including improvements in latency, reducing network load and threat assessment.

Singla D. [3] addressed the security issues, goals, and attacks on WSN because wireless sensor networks are more vulnerable. Several techniques are being developed by the many researchers to handle attacks. WSN applications, security requirements as well as the challenges are significant for understanding the core principles of WSN.

Jadidoleslamy H. [4] proposed the design which has been a comprehensive view of this issue by presenting complete and comprehensive intrusion detection architecture (IDA). The main contribution of this architecture is the hierarchical structure i.e. It is designed and applicable in one or two levels, consistent to the application domain and its required security level. This paper designs a questionnaire to verify the proposed system. The prepared questionnaire includes some questions about different properties of IDA. This work also discusses the high level and general requirements of IDS which focused on IDSs performance and functionality.

Chodhary R. [5] presented access control mechanism of geospatial data are. Then the issue of security mechanism of authorization of different model is explained. Access control mechanism and its types including DAC, MAC and RBAC are explained in this research paper.

Ansar.S [6] depicted the overview of WSN intrusion detection and types of intrusion detection methodology with the comparative security of existing method. This work proposes hybrid intrusion detection for cluster WSN. This paper analyzes rule based multi agent based & hybrid approach are explained.

Deshmukh R. [7] proposed the architecture of hybrid intrusion detection system (HIDS) in 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 rating like attack rating, data mining, and detection net rating with attack name and performs better in terms of energy efficiency and detection rate.

Chokle V. [8] explained the number of attack pattern on number of nodes of sensor network. The generalized approach that can be applicable for both computationally and memory restricted devices. This work proposes the intrusion detection system for network. The proposed distributed learning algorithm for the training of reaches high accuracy for detecting the normal & anomalous behavior.

Chand A. [9] presented the security issues of WSNs with the major functions. The paper works on the anomaly detection model detects including attack and misuse detection model.

Ali N.[10] presents current intrusion detection system and some open research problems related to WSN security. Overview of security in wireless sensor network and Intrusion Detection are described in this paper. The differentiation of the Signature, Anomaly & Hybrid Intrusion Detection are explained in the manuscript.

Rashida.S [11] proposes a novel distributed intrusion detection system using multi agent in order to decrease false alarms and manage misuse and anomaly detects. Intrusion detection is the process of monitoring and analyzing the data events occurring in a computer and or network system to detect attacks and other security problems. Implementation including security and efficiency is the crust of this paper.

V. Problems In The Existing System

IDSs use agents as their lowest level element for data collection and analysis .In existing architecture [11] architecture both techniques of IDS anomaly detection and misuse detection is used. It consists of seven modules-Tracker, Anomaly detection module, Misuse Detection module, Monitor, Signature Generator, Inference Detection module and Countermeasure Module combining the results of the three Detection Modules. The author proposed a novel distributed intrusion detection system using multi agent in order to decrease false alarms and manage misuse and anomaly detects. Three types of possible values of intrusions are Low, High and medium .The major problem discussed by the author is that the Detection of intrusions at the inference module is delayed until all necessary information gets from the agents and does not specify any access control mechanism to allow for different users to have different levels of access to the IDS.

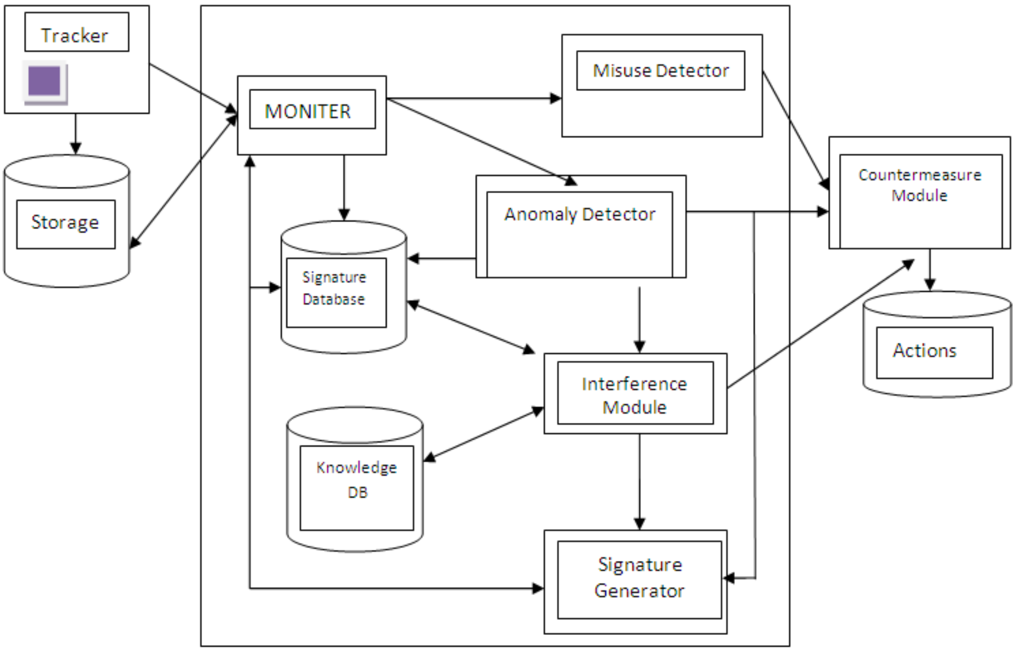

Figure 1 - Existing Architecture [11]

Challenges of Existing IDS with WSN:-

- Detection of intrusion at inference module is delayed until all the necessary information gets them from the agents.
- Architecture does not specify Access Control Mechanism to allow for different users to have different levels of access to the IDS.

» Inference module is single point of failure .It stops the working of entire anomaly detector. It stops producing useful information.

VI. Proposed Work And Research Methodology

This section proposes a pragmatic and unique architecture of anomaly based Intrusion detection system with clustered wireless sensor network using access control mechanism. Following is the working of proposed architecture that is depicted in figure 2:

Clustering - The wireless sensor system is partitioned into assorted clusters. The various leveled clustering is utilized to separate the sensor hubs. The system has one cluster head and its part hub. It advances data to its member& gathered data from them transmits to base station. Cluster head records tracks of all hubs & sent to base station intermittently for hub status.

Access control module:- It is utilized that the client has been effectively confirmed preceding implementation of access control through situation. It takes the information from sensor and should be coordinated into every bundle that is conveyed. Approval accepting character of client is known; figure out if some detail is permitted. Trustworthiness of the substance of every bundle must be guaranteed credible. It is done by DAC strategy. The DAC approach directs access to documents and host. It represents client access in light of client personality or approval. By utilizing this access control it assess some condition. It assesses the pre and solicitation result condition.

Pre conditions determine what must be valid keeping in mind the end goal to concede the asked for operation. In the event that there is no pre condition, the approval status set to genuine. Generally the pre - conditions are assessed and the outcome is put away in the approval status. On the off chance that the solicitation – request conditions are available in the strategy, the conditions are assessed and result is put away in security database. On the off chance that approval is not conceded the solicitation is rejected and in this situation the uncommon log is kept up by the server to stay informed regarding further comparable marks of the assaults. Conversely on the off chance that it is approve then it will forward the information to monitor.

Monitor : - It is utilized to channel the approaching parcels and group it as ordinary or irregular. Screen contrasts got information & watches and then mark standards of typical example of conduct. The screen utilized a rule based strategy to examine the parcels and depict which bundles are unusual. In this manner, a model of typical conduct is set up. In the event that monitor discovers any match then sends proper message for known assault to misuse detector. On the off chance that screen does not discover any match then send information to Anomaly detector for discovering abnormality.

Misuse Detector: - It deals with system and caught the information globally . It investigates the information. It goes about as independent IDS and identify the assaults for itself just without consulting another IDS. In the event that approaching information is identified as an assault, it recognizes the known assaults in system if there is a closeness between the got information and assault signature in the database then it send the report to reaction module.

Anomaly detector - It is utilized to recognize the new or unknown assaults. It is traditionally put on the host and gathers the information from sensor to break down the information to distinguish unknown assaults. It checks the conduct of the information & groups it as assault or normal information [14]. It looks upward the information in knowledge base solution. On the off chance that it finds any irregularity then it will send the information to inference module.

Inference module:- It is the essential segment of information models. It goes about as thinking procedure. It controls the part of elements that are running. It checks the realness of information on system. It chooses by learning and rules in information base and security information base. A learning base contains instances of information sorts, which are identified with client's activities. On the off chance that the approaching information is distinguished assault then it sends the report to security information base. The RBAC module is having the abnormal state secured access rights which rely on upon the part of client and by this approach the clients are connected with roles . A client has permission just if the client has an approved part which is connected with that authorization.

Reaction module:- If the indicator decides the outcome to be suspicious, the reaction module will take the corrective measures to keep malicious activities from being executed. It utilize the reaction approach characterizes activities to be performed by response module occurrence reaction. It is enables the use of policies that tighten or loosen defense in response to network attacks or the apparent probability of an assault at a specific purpose of time.

Security database:- This data is gathered from different sources that can be of many types are including client action profile portray "ordinary" client conduct and are utilized as a part of oddity recognition to identify suspicious exercises that lost from the profiles. It portrays the activities needed for occurrence reaction to contain and control the assault. The activities may incorporate creating cautions, adjusting the conduct of the application and conforming the action profiles to incorporate new values so as to keep the profiles up to information.

Signature Data base: It makes lead or marks and makes new section in mark information base. At that point it sends suitable message to screen to reanalyze the assault. It records empower IDS to have an arrangement of mark criteria or guidelines which they can be utilized to think about bundles as go through the host.

Various Advantages of the proposed architecture are given below:

Advantages of proposed framework includes

- » The users can self-manage access privileges.
- » The overhead of security administrator is significantly reduced as resource users and administrator jointly manage permission.
- » Supporting new privileges is easy.
- » Achieve the goals of high detection rate and low false positive rate.
- » High Level Security and Integrity is maintained in the proposed system
- » The System is having multi-layered security and confidentiality with the logging of assaults and reducing the upcoming vulnerabilities.
- » The Detection of Intrusion at inference module is not delayed until all the necessary information gets them from the agents.

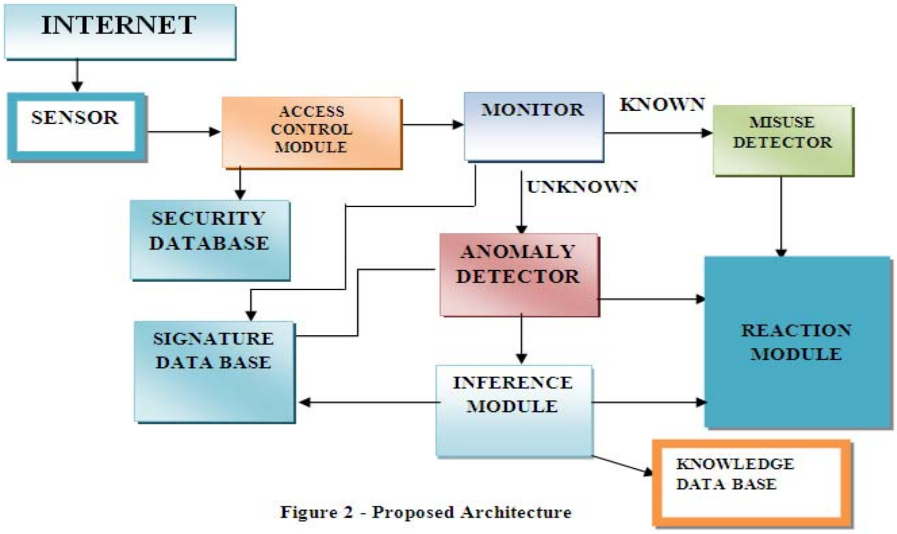

Figure 2 - Proposed Architecture

FLOW CHART OF THE PROPOSED WORK

Flowchart of the propped architecture is shown in fig 4

Start from initial node N

S: Sensor Node

ACM: Access Control Module

M: Monitor

AD: Anomaly detector

MD: Misuse detector

IM: Inference module

RM: Reaction module

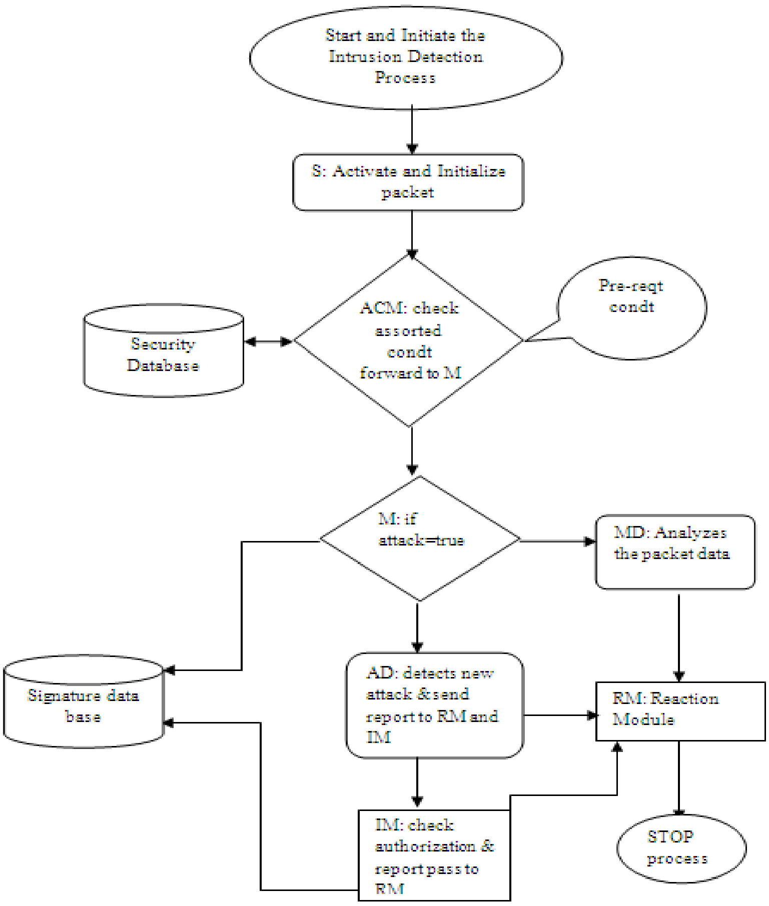
Start and Initiate the Intrusion Detection Process
S: Activate and Initialize packet
Security Database
ACM: check assorted condt forward to M
Pre-reqt condt
M: if attack=true
MD: Analyzes the packet data
Signature data base
AD: detects new attack &send report to RM and IM
RM: Reaction Module
IM: check authorization & report pass to RM
STOP process

Figure 4- Flowchart of Proposed Architecture

S: gather the information &forward to ACM

ACM: check the pre-reqst condition

If (pre=true)

Grant reqst

Else

Rejected

```
M: Compare received data =signature
    If (attack=true)
    Send to MD
    Else
    Send to AD
MD: Analyzes the data on network
    If (data=attack)
    Send report to RM
    Else
    Stop
AD : Detects new or unknown attack
    If(attack =anomaly)
    Send report to RM
    Else
    Forward to IM
IM: Check authorization on network side[Multi layered  security protocol]
    If (data packet=attack)
    Send report to signature data base and reaction module
    Else
    Forward for further process
     //it uses two level of detection.
    //a .Anomaly detector, b.Infernce module
RM: classify data traffic on network side
  If (attack =true)
  take predictive action
  Else
  Rejected data send to security data base.
 //matches the attribute based on machine learning algorithm.
//fuzzy set used at this level for max.association rule   mining
```

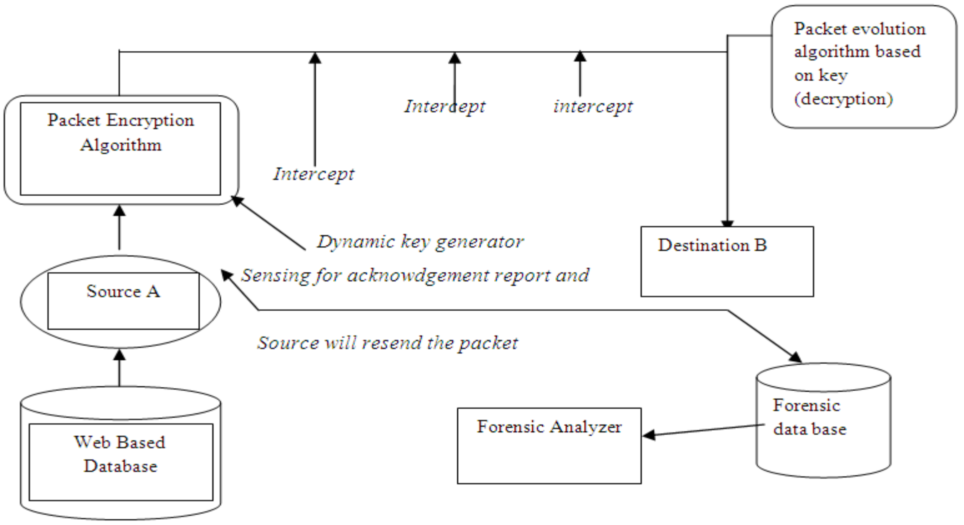
Packet evolution algorithm based on key (decryption)
Intercept
intercept
Packet Encryption Algorithm
Intercept
Dynamic key generator
Destination B
Source A
Sensing for acknowdgement report and
Source will resend the packet
Forensic data base
Forensic Analyzer
Web Based Database

Figure3.Working Model of Intrusions Detection and logging

The figure 3. Shown that the working model of Intrusions Detection and logging .This model is secured and supports the non-delay transmission of packets as there is the forensic analyzer for detailed logging. The forensic analyzer keeps track of all the data packets and their acknowledgement. If the packet is delayed due to intrusion, its timestamp and intrusion type is logged. Using this approach, the further delay is avoided because the system is already having that signature. An access control Mechanism is used for check the authenticity of packet, the Transmission of Encrypted Packet C_i using the specified Path and encrypted packet is implies to the destination path. The detailed algorithmic approach -access control mechanism in internal level is following :.

Detailed Algorithmic approach – Access Control Mechanism in internal level

```
Step 1: Activate and Initialize the Wireless Protocol Enabled Packet $P_i$ at Source $S_i$ for transmission to Destination $D_i$
Step 2: Packet Encryption Module $PE_k$ based on Dynamic Key k Generation, once the Packet moves from Source $S_i$
$C_{i\,:}= PE_k\ (P_i)$
Step 3: Transmission of Encrypted Packet $C_i$ using specified Path/Route $R_i$
$C_i \rightarrow\ D_i\,[R_i]$
Step 4: Authentication of Packet on Receiving and Access Mode End
IF ( $C_i\ = PD_k\ (C_i)$     // Packet Decryption Module $PD_k$ to decrypt the packet at destination
BEGIN
    a) DEST [i] := $PD_k\ (C_i)$
    b) Successful Delivery of Packet
    c) ACK sent to Source $S_i$ // Acknowledgement ACK i
    d) s delivered to Source in case of Success
END
ELSE
BEGIN
```

a) A record will be inserted in the Forensic Database. The Interception Table will consist of the Structure (Id, Interception Type, Timestamp of Interception). // Acknowledgement ACK is sent to Forensic Database in case of Failure Attempt

b) Source S_i senses the Forensic Database.

Select All Records from Forensic Database

IF (true)Then

print “Failure Delivery, Retransmit the packet”

c) GOTO Step 1

d) Update Forensic Analyzer Database for taking remedial actions.

END

Step 5: Detailed Logging and Forensic Analysis of the Access Control

a) Retrieve Records for analysis of interceptions.

b) Analyze the type T_i of Intercept

c) Perform the remedial measure for avoiding the stored interception or intrusion type

Performance Parameters of the Proposed Approach

The proposed framework and architecture is effective and having higher efficiency in terms of multiple parameters including

» Turnaround Time

» Throughput

» Less Packets Loss

» Overall Security

» Integrity

Table 3 - Pragmatic Comparison between Classical and Proposed Approach

Approach → **Parameter** **↓**	**Classical Approach**	**Proposed Approach**
Levels of Security	Single Level Security with less integrity based communication	Multilevel security with dynamic hash algorithms
Delay	High	Less
Jitter	High	Moderate
Fault Tolerance	No	Yes
Access Rights	No Specifications	Multiple Layers of Access Rights to implement elevated security
Metaheuristic Adaptive	No	Yes
Network Implementation	Specific types of networks can be implemented	Any type of network can be analyzed
Assorted Assaults Taxonomy Identification	No	Yes

Self-Learning and Adaptive Nature	Moderate	High
Forensic Compatibility	No	Yes
Machine Learning Compliant	No	Yes

VII. Simulation Aspects in MATLAB

The proposed model can be simulated in MATLAB for detection, analysis, logging and avoidance of the intrusions in wireless scenario.

MATLAB includes the biograph toolbox that can be used for the dynamic generation of wireless scenario and connection. A dynamic key using hash functions can be generated for secured transmission against intrusions. The proposed working model of the intrusion detection will keep track of each data transmission and their detailed report.

VIII. Conclusion And Future Work

The development of Intrusion detection and prevention systems are prevalent and having huge literature on multiple sources. As the domain is very huge and diversified, this stream is having scope of developing new and effective algorithms using hybrid, parallel and other metaheuristic approaches.

Intrusion detection system with clustered wireless sensor network using access control mechanism. The proposed research work presents an improved framework for enhanced security scheme to integrate access control and intrusion detection in CWSN. With respect to the assorted wireless network problems, the new framework of IDS is proposed which solve the existing security issues and system vulnerability problems.

For future scope of the work meta heuristic techniques can be used in hybrid as well as parallel approaches to better and efficient results.

References

1. Khanum, S., Usman, M., & Alwabel, A. A. (2012). “Mobile agent based Hierarchical Intrusion Detection System in Wireless Sensor Networks”. International Journal of Computer Science Issues (IJCSI), Vol 9 No 1,pp, 101-108.

2. El mourabit, Yousef. (2014). “A mobile agent approach for IDS in Mobile Ad Hoc Network”. I JCSI International Journal of Computer Science, Vol 1 No-2, pp.148-152.

3. Singla D. (2014),"Analysis of security attacks in Wireless Sensor Network”, International Journal of software and web services (IJSWS), Vol 1.No-2, pp 26-30

4. J.doleslamy.(2011).”Hierarchical Intrusion Detection Architecture for Wireless Sensor Networks”, International Journal of Network Security and its Applications (IJNSA), Vol 3 No.5, pp.131-154.

5. Chaudhary R, K. V. (2014). “A Survey on Secure Access Control Mechanism of Geospatial Data”,. International Journal of Computer Science, Vol. 2, No 2, pp.5-9

6. Sheikh, M. A. I., Kewadkar, M. P., & Gupta, M. H. (2013),”Analytical Study on Hybrid Approach towards Intrusion Detection System for Wireless Sensor Network”. International Journal of advanced Research in Computer and Communication Engineering Vol 12.No 10, pp.1-9

7. Deshmukh R, M. R., Deshmukh, M. R., & Sharma, M. (2013).,”Rule-Based and Cluster-Based Intrusion Detection Technique for Wireless Sensor Network”, International Journal of computer science and mobile computing, Vol 2,No 6,pp 200-208

8. Mr.vivek A chokle,(2015),"Intrusion prevention and detection in Wireless Sensor Network",Internatioanl journal on recent and innovation trends in computing & communication ,Vol 3,No 2,pp 1-11

9. Lonkar, M. T. H., & Tiwari, M. R(2005),”. Enhancing the Security of a Cluster-based Wireless Sensor Network Using Hybrid Intrusion Detection System.”IEEE International Conference On Wireless Sensor and Mobile Computing networking and Communication. Vol 2,No 2.pp.1-9

10. Alrajeh, N. A., Khan, S., & Shams, B. (2013). “Intrusion detection systems in Wireless Sensor Networks- a Review” International Journal of Distributed Sensor Networks, Vol 2,No 2.pp55-62

11. Rashida, S. Y. (2013). “Hybrid architecture for distributed Intrusion Detection System in Wireless Network. “International Journal of Network Security & Its Applications (IJNSA), Vol 5 No.3, pp 45-54.

12. Abdullah, M. Y., & Hua, G. W. (2009).”Cluster-Based Security for Wireless Sensor Networks. In Communications and Mobile Computing, 2009. CMC'09. WRI International Conference on, Vol. 3, pp. 555-559

13. Sandhu, R., & Samarati, P. (1997). “Authentication, access control and intrusion detection.”The Computer Science and Engineering Handbook, Vol. 1, pp 929-939

14. A.Wani, R.Chawla,(2015),"Effective and reliable countermeasure for detecting DDoS attack in IDS",International Journal of engineering research and Technology (IJERT),Vol.4,No.3,pp-536-542

15. G.kaur, R.Chawla,(2014),"Comparative analysis of anomaly based Intrusion Detection Techniques",IJITE,Vol 2,No12,pp 71-81

16. A. Singh, D.Junega,(2010),"Agent Based Preventive Measure for UDP flood Attack in DDoS attacks", International Journal of Engineering Science and Technology ,Vol,2,No 8,pp- 3405-34

17. D.Junega, R.Chawla,(2009),"An Agent Based Framework to counter attack DDoS Attacks", International Journal of wireless Networks and communications,Vol.1,No 2,pp193-200.