INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078

(Volume 7, Issue 4 - V7I4-1461)
Available online at: https://www.ijariit.com

A study of Wireless Sensor Network security attacks and Intrusion Detection Techniques

Nitu Singh Gahlawat
neetu8448@gmail.com
BRCM College of Engineering and Technology, Bahal, Haryana

Praveen Kantha
pkantha@brcm.edu.in
BRCM College of Engineering and Technology, Bahal, Haryana

ABSTRACT

Nowadays, remotely impromptu sensor systems have gained popularity in both commercial and military situations. In any case, security is a critical problem for IoT systems due to its distribution in an open and unprotected environment. Also, because the encryption component is still insufficient to support the sensor protection from malicious attacks, a framework for detecting interruptions should be given. While interruption counteraction is an effective and successful strategy against attacks, there may be some assaults for which no established avoidance technique exists. Therefore, apart from protecting the framework against known attacks, the interruption detection framework collects critical data about attack strategies and aids in developing an interruption counteraction framework. Along with checking attacks against remote IoT devices, this article analyses the various activities to interrupt the discovery framework against remote sensor organizations. In this article, we offer a system for recognizing interruptions in a progressive structural plan that is tailored to the existing requirements and constraints of remote, specifically appointed sensor organizations. We used grouping components to construct a four-level progressive organization that increases network adaptability to large geological regions and employs both abnormality and abuse detection techniques for interruption finding in this suggested interruption location framework engineering. In addition, we offer a strategy-based location instrument and an interruption reaction, as well as a GSM cell concept for engineering interruption identification.

Keywords: *Wireless Sensor Network, Intrusion Detection System, sequential design .*

1. INTRODUCTION

Several intrusion detection systems for use in Wireless Ad hoc networks have been demonstrated or are being developed. Many of them work in a conveyed climate, that means individuals operate independently on single hubs and look for anomalies in their peers' activities to find interruptions. There is now a lot of study towards preventing and detecting intruders and gatecrashers in Wireless Sensor Networks, but there has been very little work done for strategic reasons. As a result, the organization's chairman will have a difficult time identifying interruptions. As an end, they need the hubs to use a greater amount of processing power, battery reinforcement, and space available, making Intrusion Detection System more expensive or unfeasible for the overwhelming majority of applications. Numerous Intrusion Detection System make use of adapting experts in appropriate climates [8]. The Versatile Agent maintains sensor mobility, efficient routing of interruption data throughout the enterprise, and eliminates network dependency on explicit hubs. However, this component is not well-known for Intrusion Detection System due to the diverse specialists' acquired security flaws and considerable load. A subset of the Intrusion Detection System is attacked explicit, limiting them to a certain type of assault [1].

Several of them feature a system that enables Intrusion Detection System to make use of a computer's tremendous processing speed, massive storage capacity, and infinite battery life [21]. The majority of Intrusion Detection System methods collect data for intrusion detection by evaluating framework log records, network traffic, or bundles inside the enterprise. Some distinguish between disruption and gaining further data, for example, the type of assaults, the location of the gatecrasher, and so forth. Although many IDS systems are offered in Wireless impromptu organization, only a small number of them are suitable for Wireless Sensor networks due to their asset constraints. While most IDS are designed to identify assaults at the directing layer only [7] [21], they are rapidly being upgraded to detect attacks at additional system management layers. The bulk of structures are built on inconsistency detection [18] [2], which examines the accurate assessment of hub location exercises.

2. WIRELESS SENSOR NETWORK - AN OVERVIEW

The term "sensor network" refers to a framework that involves the combination of sensors and actuators, as well as a few generally helpful figuring components. A sensor structure may have hundreds or even thousands of sensors; they may be mobile or fixed in location, and they may be connected to a control or display [7]. A "remote hoc sensor network," according to the National Institute of Standards and Technology (NIST), is "a network of the period spreading over a geographical region" [8].

It mainly serves as a conduit for another organisation or a route of communication with persons [21]. For talking to additional wireless devices, an access point may have an infinite supply of force and high data transfer links. Remote sensor hubs, on the other hand, must employ low power, poor transfer speeds, and short reach connections. This distant detector network is made up of IoT gadgets that detect information about their mood and broadcast it to the base station, which acts as a centralize control and information gathering personality. Base stations, in general, are great equipment with a large storage ability for incoming data.

In the first place, in the impromptu organization, each hub is generally held and overseen by a human client. While in sensor organization, every intersection is free, and the base station constrains correspondence. Different privacy concerns and threats that are addressed for distant impromptu organizations can be applied to WSN. This has been discussed in previous investigations. However, due to the structural differences between WSNs and small, particularly appointed organizations, the security component used for small, specially appointed companies cannot be sent directly to WSNs. Secondly, remote sensor requires more computing resources and resources than properly designed hubs. Thirdly, detector networks are extremely reliable, for example, when it comes to estimating actual data (like temperature, sound, and so on). Finally, sensor network hub thickness is more than that of spontaneous organizations.

The design aspect of Wireless Sensor Networks allows for the basic demand of security assaults in Wireless Sensor Networks to be met:

Table 1: Threats and Attacks in WSN

Attacks	Brief Description
Attack on Information in transit	Data that will be sent can be changed, adjusted, replayed, parodied, or evaporated by assailant.
Hello flood	Aggressor with high radio reach sends more Hello bundle to declare themselves to enormous number of hubs in the huge network convincing themselves as neighbor.
Sybil attack	Counterfeit numerous characters to assault on information trustworthiness and openness.
Wormhole attack	Communicate data between two WSN hubs stealthily.
Network partition attack	Dangers to openness however there is a way between the hubs.
Black Hole Attack	The aggressor retains every one of the messages.
Sink Hole Attack	Similar to black hole. Exception: the attacker advertises wrong routing information
Selective Forwarding	The aggressor advances messages based on some pre-chosen measure
Simple Broadcast Flooding	The attacker floods the network with broadcast Messages.
Simple Target Flooding	The attacker tries to flood through some specific nodes.
False Identity Broadcast Flooding	Similar to simple broadcast flooding, except the attackerdeceives with wrong source ID.
False Identity Target Flooding	Like basic objective flooding, aside from the aggressor misleads with wrong source ID.
Misdirection Attack	The attacker misdirects the incoming packets to a distant node.

3. EXISTING CHALLENGES

As a result, an IDS is required that can detect assaults both in and out of, known and unknown, with a minimal risk of false warnings. Existing IDS systems for sensor networks, for example, lack features such as high handling power, gigantic capacity capacities, and endless battery reinforcement, to name a few. Existing methods of identifying interrupts are incapable of protecting WSN from both internally and externally adversaries. None of them are finished. For example, most techniques present grouping techniques without defining how they will be structured or how they will interact with the remainder of the framework. Apart from their remote partner, the bulk of present IDSs operate wired design. The engineering of WSNs is much more complicated than the design of, particularly designated remotes.

3.1 IDS Design

Distributed and cooperative: Any built-in function, on the other hand, has its unique IDS. Then they work together to create a worldwide IDS. With several remote sensor nodes, this idea is especially well-organized and structured, as a world IDS is launched in response to an uncertain disruption detected by a single hub. In [11], remote specially appointed organization design is characterized into three fundamental classification which can be acclimated to Intrusion detection system in WSN engineering.

Intrusion Detection System can be classified into two groups based on the information collection component:

- Host-based Intrusion Detection System examines log documents (applications, operating systems, and so on) before comparing and logging the current mark of known attacks from an internal data collection.
- Organization-based Intrusion Detection System, on the other hand, operates in a variety of ways.

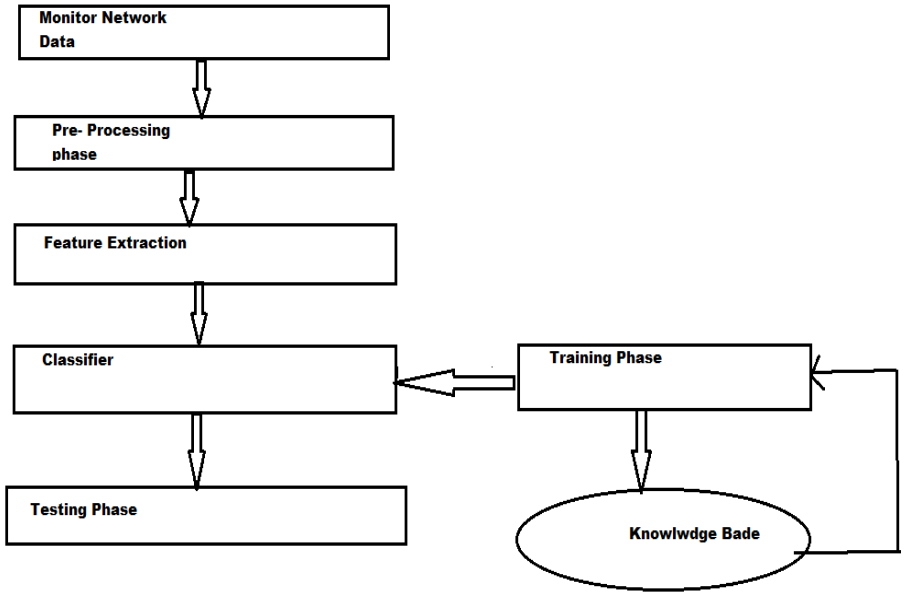

Figure: Design of Intrusion Detection System

Hierarchical: This engineering has been proposed for the multifaceted remote organization. Bunch head distinguishes assaults as part hubs that might reroute, adjust or drop a bundle in transmission. Simultaneously all bunch heads can help out focal base station to shape a worldwide IDS. The network is divided into a group with batch heads in this case. The group head functions as a small base station for the bunch's hubs. It also adds up data from the part hubs on harmful exercises.

Stand alone: Every hub goes about as an autonomous IDS. It recognizes assaults for itself just without imparting any data to another IDS hub of the framework, even doesn't help out different frameworks. Thus, all interruption discovery choices depend on data accessible to the individual hub. Therefore, its impact is excessively restricted. This engineering is most appropriate in a climate where every hub is fit for running an IDS [11].

The First idea is to access data among specialists. Cryptography, a ballot component, or trust, depending on the organization's asset requirement, can be used to send data between specialists.

The second consideration is how to alert users. Clients, for the most part, are in front of Base stations. As a result, numerous calculations can be used to provide information to the base station. Tesla, for example, uses a secure transmission computation.

In a Wireless Sensor Network, there are a variety of IDS approaches (WSN). We'll look at some of the most popular Wireless sensor IDS models here.

Table 2: Comparative study on existing IDS

Name of the Intrusion Detection System	Data Collection Mechanism	Detection technique	Handled attacks	Network Architecture
Hybrid IDS for Wireless Sensor Network [6]	Networkbased	Anomalybased	Selective forwarding, sinkhole, Hello flood and wormhole attacks	Hierarchical
Decentralized IDS in WSN[5]	Networkbased	Anomaly based	Repetition, Message Postpone, Active attacks, Sinkhole, Data Alteration, Plugging, Message Negligence, and Selective Forwarding are all terms used to describe how data is altered.	Distributed
Intrusion Detection in Routing attacks in Sensor Network [1]	Host based	Anomalybased	DoS, active sinkhole attacks, and passive sinkhole.	Distributed
Intrusion Detection with a Wireless Channel	Host based	Signaturebased	Flooding, Wormhole, Black hole assault, selective forwarding, and misdirection are all examples of duplicate nodes.	Distributed
IDS for WSN based on self-organized critical and random learning [2]	Host based	Anomalybased	In this IDS paradigm, there is no indication of which attacks it can withstand and which it cannot.	Distributed

3.2 Our Model

The Base station will detect and manage regional hubs. We propose a new IDS architecture in this paper that attempts to reduce the force required of sensor hubs by delegating the work of interruption location to three-layer hubs via a strategy-based organizational structure for executives. A multi-leveled overlay design is used in the model (HOD). Each sensor hub space was separated into hexagonal localities (like GSM cells).

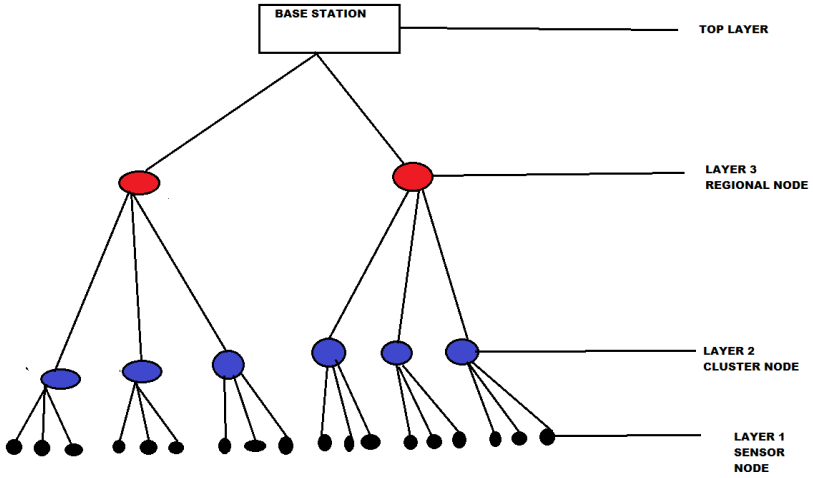

Figure: Designing a Layered Overlay

3.3 Detection Entities

The Base Station is the most advanced level of engineering that necessitates human intervention. It will gather data from local hubs and send it to clients according to their preferences. Before transmitting the combined alarm to the upper layer ground station, the Local Node will check and collect data from surrounding group leaders. It doesn't have a screen like the group hubs, but it does include all of the IDS functions. It enhances the capabilities of the sensor network. The entire region will be divided into many portions if a high number of sensor hubs are accessible at the leaf level.

For the sensor hubs, Cluster Node serves as a screen hub. For each hexagonal region, one bunch hub has been assigned. It will collect data from sensor hubs, break it down, and total it before sending it to the local hub. It is more impressive than sensor hubs since it includes interruption discovery capability.

Sensor networks can be used for two purposes: sensing and routing. In the centre of sensor hubs and group hubs, each sensor hub will detect the climate and trade information. Because sensor hubs have so many asset requirements, this model does not include an IDS module in the leaf level sensor hubs.

3.4 Policy-based IDS

PDP encrypts or decrypts the available Information for a subordinate gadget arrangement and creates the necessary PEPs. The PEP carries out the PDP's selection of sensible substances [12]. These characteristics enable organizations to reorganize their frameworks in response to changing situations brought about by computerization. Thus, if a disappointment occurs, the framework enables one segment to acquire control of the administration portion of another part. One of the primary architectural advantages of the progressive building is that each hub may forcefully acquire control over another hub's usefulness, therefore ensuring longevity. A nimble specialist structure guarantees that new administrative capabilities are dynamically implemented. Strategy systems can be utilised to achieve durability, adaptability, and self-governance in a large WSN when Structured Network Management is used.
Each intermediate supervisor has a specified region, known as an Area or Group specialist, who gathers, prepares, and transmits data from its allocated area to the proper authorities.A hierarchical network the board integrates the advantages of two executive models (Central and Distributed) [14] and utilizes middle-of-the-road hubs (Regional and Cluster) to appropriate recognition endeavours.

Each of the moderate hubs is also utilized to distribute orders/information/messages from the principal layer supervisor to the hubs within its region. It should be noted that there is no direct relationship between moderates. However, the leaf level sensor hubs are all constructed with increased energy and capacity on the more significant level.

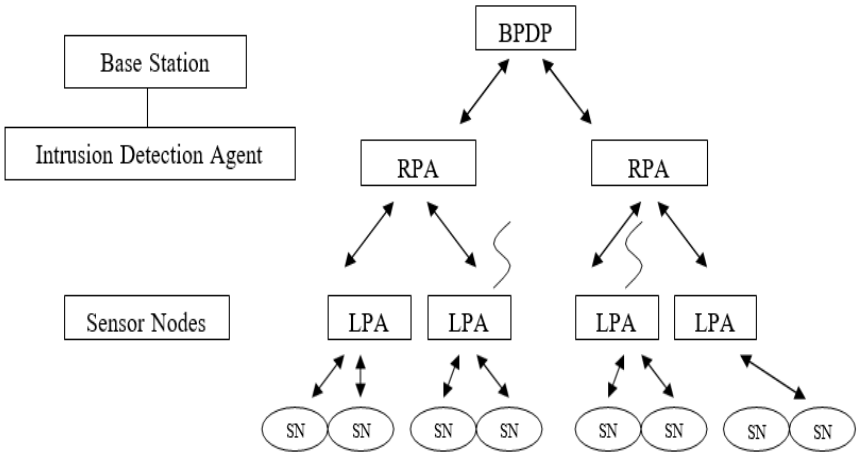

Figure: IDS Network Monitoring Layered Structure

The proposed engineering includes numerous segments that analyse configurations to achieve approach-based administration for IDS:

(a) A Base Policy Selection Point (BPDP),
(b) Different Policy Selection Modules (PDMs), and
(c) A Policy Enforcement Point (PEP).

Low-level Sensor Nodes are Policy Implementation Stations. PDMs (Policy Decision Modules) are components that do sophisticated computations in critical areas. LPAs and RPAs function similarly to PDMs. LPA is more notable than sensor hubs since it interacts with sensor hubs LPAs execute neighborhood strategy-controlled arranging, sifting, checking, and revealing, which reduces board transfer speed and processing complexity from lower-level system traffic, allowing for improved network execution and interruption recognition. An RPA can handle a large number of LPAs.

For the Base, a Point of Decision The engineering's controlling aspect is policy. It executes the Intrusion Detection Tool's (IDT) arrangements or interruption rules, which include gathering events, assessing irregularity conditions, and applying new principles, calculations, edge esteems, and so on. IDT supports the specialist's setups and approaches being created, erased, adjusted, and evaluated. It can, for example, introduce new elements to RPA and LPA, such as a new signature of interruption, as well as edit or delete existing compounds.

3.5 Agent for Regional Policy

Point of Decision for the Base Policy
Regional Policy Agent
Local Policy Agent
Sensor Node

3.6 Intrusion Detection Agent Structure (IDA)

The following situation reflects the various levels of engineering for the WSN strategy board. It consists of many different layered levels, each of which has an Intrusion Detection Agent (IDA). An IDA comprises four parts: a preprocessor, a signature processor, an anomaly processor, and a postprocessor. The following figure illustrates the functionalities. The four types of policy decision are:

(a) The Base Policy Decision Point (BPDP)
(b) The Regional Policy Agent (RPA),
(c) The Local Policy Agent (LPA), and
(d) The Sensor Node are nodes (SN).

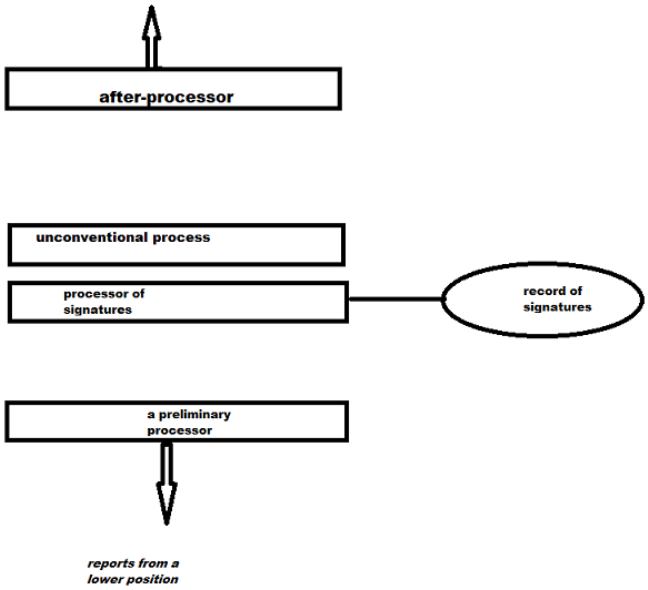

Figure: Intrusion Detection Agent Structure

The processor's compiler either gathers the sensor's organization traffic or receives information from the underlying transport Intrusion Detection Agent system when the lower-level detector isn't even an LPA. To justify the organization's status to the specialist's higher layer processor, the sensor traffic data is subsequently connected to a collection of items known as an upgrade vector.

The Identity Classifier compares the preprocessor's findings to known assault marks using a framework or knowledge base called the Signature Record of known unapproved noxious costs and potential behaviors. If no match is found, the abuse interruption should be determined, and the identity processor should provide the relevant data to the next higher layer for further processing.

Anomaly, the processor examines the vector returned by the preprocessor to detect anomalies in network traffic. Typically, a quantifiable approach or automated reasoning is used to identify this type of attack. The data set contains a profile of typical activity

elicited by the Base station. If the workouts generated by the preprocessor deviate significantly from the standard shape or exceed some defined limit value, esteem assaults are recorded.

3.7 IDS node selection

It is a waste of energy to set up each hub as an Intrusion Detection System. As a result, reducing the number of hubs required to perform interruption detection is critical. Three systems are presented within [15], including the option of Intrusion discovery hub. In any group, no gatecrasher is allowed to enter the focal station. This type of model protects the most inside area of the body before fighting back to the outer region. A portion of the organization's core defense selects an Intrusion Detection System hub around a halfway mark.

In this paradigm, the spread defense does indeed have a specialized hub choice calculation that comes after the casting a ballot computation from [16]. The tree chain of command is used to determine the hub. This prevents intruders from slipping further join group from outside the group 's boundaries. The hub is chosen via boundary defense along the group's limit edge.

If there should be an occurrence of the small-medium, gotten signal strength has a connection with the distance between hubs. Hub altering and obliteration is another actual layer assault that can be forestalled by setting hubs in got the place. The Local Policy Agent's Anomalous processor will next examine whether the obtained esteem is shocking at the time of checking. If this is the case, robotic process automation will be reprimanded by the production of sufficient caution.

During the statement interaction, the Received Signal Strength Indicator will be recorded by the Cluster hub's Local Policy Agent as an incentive for the communication between Array link and lower sensor sends hubs, as well as sensor to sensor hub.

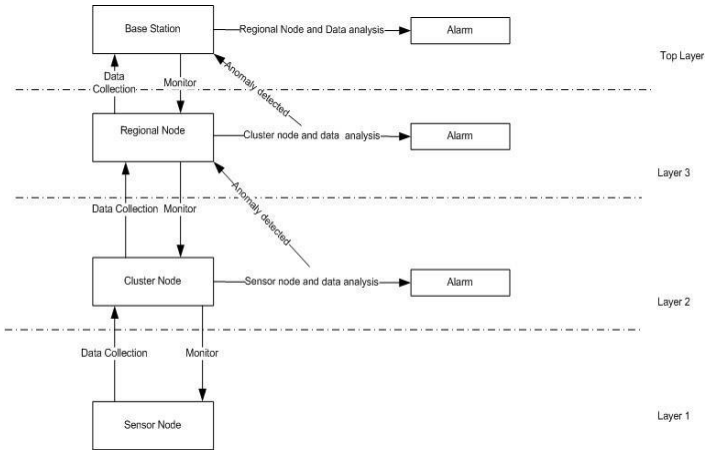

Figure: Process of IDS

During this space each sensor hub approaches the radio recurrence channel without obstruction. Crash, rejection of rest, and parcel replay are examples of Connection Layer assaults. To detect the irregularity, social, mobile, analytics, and cloud, as well as Time Division Multiple Access, can be used. Time Division Multiple Access (TDMA) is a computerized transmission method in which each group hub assigns different schedule openings for different sensor hubs in its area.

Application Layer utilizes three level of hubs or stations and they are defined in:

- base station
- local hub
- bunch hub.

Sensor layer will be checked by upper layer bunch hub and group hubs will be observed by local hub. lastly the high-level base station will screen the local hubs.

The following Network Layer course is used to determine if the parcel carefully comes from the optimal course. If a package is delivered to its destination in a non-optimal manner, the Anomaly Processor can detect possible interruptions based on established criteria.

3.8 Intrusion Response

There are contrasts between interruption location and interruption anticipation. In the event that a framework has interruption counteraction, it is expected that interruption identification is inherent.

For interruption response, there are two alternative procedures: Policy-based reaction or fast response [20]. (Base Policy Decision Point) BPDP and PDM are both active participants in the system. Disruption can be found in both Set and Global nodes Then again Policy put together reaction works with respect to more broad extension. It considers the dangers revealed in the ready, requirements and destinations of the data arrangement of the organization. It alters or makes new guidelines in the arrangement store to forestall an assault later on. The Policy choice point of the base station, as well as other arrangement choice modules, engage in the reaction system in our suggested Intrusion Detection System. Interruptions are distinguished consequently as per the approach carried out by Base Policy Decision Point. Re-activity is likewise programmed yet manager may re-plan the engineering agreeing prerequisites. Intrusion Detection Systems (IDSs) are meant to cause disruption in order to obtain permissions, while Intrusion Detection System

(IPSs) try to block access from the start. "While an IDS sits outside the queue of traffic and notices, an IPS sits immediately in line of organization traffic and can obstruct the actual assault," says the IPS.

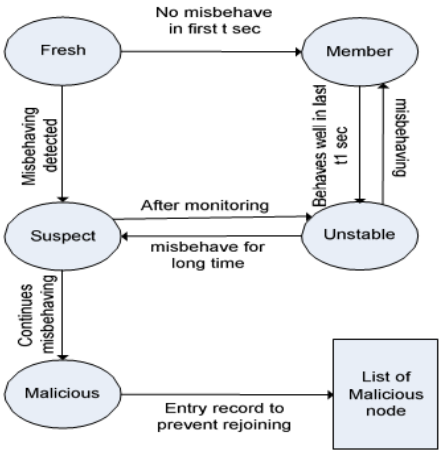

Figure: Intrusion Detection Activity

One of the primary points that each framework is expected to deliver is survivability. Base stations, we feel, will not disappoint. However, owing to disappointment or power exhaustion, national or group hubs may be inaccessible. Control of Array ports and sensor networks sharing a regional hub will naturally be moved to the adjacent node in this manner.

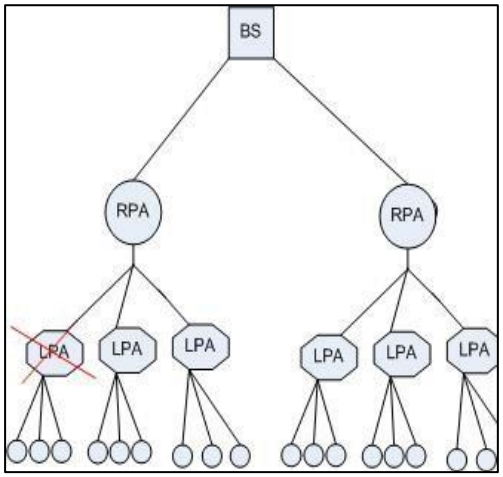

Figure: Failure of cluster nodes

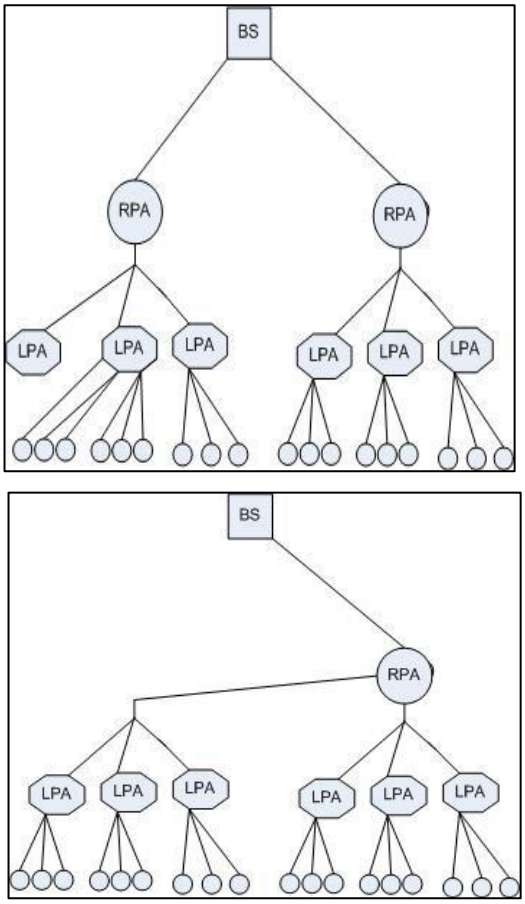

Figure: The demise of a local network

The regional hub and the base station have a direct connection. So, whenever a Local link bombs, the Access Point can identify the problem and choose one of its adjacent ports relative to a reference criterion in the BPDP. In reality, in the basic model, the main platform has direct or indirect connections to everything of their peripheral centers. Similarly, assuming any bunch hub comes up short, neighbor group hub won't be educated about its disappointment. So, for this situation regional hub will make a vital move of choosing reasonable neighbor group hub. Then BPDP must provide the bombed hub's strategy, rules, or marks to the chosen new neighbor regional hub.

4. CONCLUSION

Interruptions and insecurity risks are common in wireless communication. We offer a unique Intrusion Detection System for a specially assigned sensor network based on a progressive overlay scheme in this research. In addition, as suggested by the proposed design, we offer a reaction instrument. In the way it represents the all-out assignment of recognizing interruption, our IDS plan

complements other relevant plans. Our concept integrates the entire task of interruption finding into a multiple command chain, resulting in a structure that is extremely energy efficient. Each screen only needs to screen a handful of hubs within its reach; thus, it doesn't need a lot of effort. Because of the various leveled model, the recognition framework works in an extremely organized manner and can distinguish any interruption successfully. We regard group hubs or geographical hubs to be more spectacular than regular device hubs in this paper.

Strategy based instrument is an incredible way to deal with mechanizing network the executives. The administration framework for interruption discovery and reaction framework depicted in this paper shows that a very much organized decrease in administration traffic can be reachable by strategy the executives. This strategy-based design redesigns versatility and re-configurability of organization the executive's framework which has a decent commonsense exploration an incentive for enormous topographically appropriated network climate.

5. FUTURE WORK

This study presents a very next solution for a four-layer interruption finding framework for Sensor nodes using several tiered strategies. So, there's plenty of room for more exploring around here. The suggested IDS architecture is extremely expandable, in that additional recognition calculations can be linked to strategy as new assaults or assault designs are identified. Scenes for future works could include:

- The current concept can be applied by looking into the secure communication connecting the baseline terminal regional hub, and group hub.
- Development is a Risk Analysis Network in the director nodes to improve the interruption detection framework's response capabilities.
- Instead of physically identifying the group hub and local hub, there will be a political decision measure that will identify the group hub and territorial hub as a result of the election plan.
- On that article, I focus on the overall concept of a structural plan for Intrusion Detection System and how the board framework might be applied to the framework. In any situation, a detailed assessment of the identification and action plan is required.
- More firmly establishing board elements of director position.
- Therefore, a full detailed assessment is expected to quantify Intrusion Detection System existing capabilities in terms of assets and strategy, allowing for potential straightens updates.
- Overall, more complete examination is expected to quantify the current proficiency of Intrusion Detection System, as far as assets and strategy, so upgrades of its future version(s) are conceivable.

6. REFERENCES

[1]. Chong Eik Loo, Mun Yong Ng, Christopher Leckie, Marimuthu Palaniswami. Intrusion Detection for Routing Attacks in Sensor Networks, International Journal of Distributed Sensor Networks, Volume 2, Issue 4 December 2006 , pages 313 - 332 DOI: 10.1080/15501320600692044.

[2] S. Doumit and D.P. Agrawal, "Self-organized criticality & stochastic learning-based intrusion detection system for wireless sensor network", MILCOM 2003 - IEEE Military Communications Conference, vol. 22, no. 1, pp. 609-614, 2003

[3]. [C.-C. Su, K.-M. Chang, Y.-H. Kuo, and M.- F. Horng, "The new intrusion prevention and detection approaches for clustering-based sensor networks", in 2005 IEEE Wireless Communications and Networking Conference, WCNC 2005: Broadband Wirelss for the Masses - Ready for Take-off, Mar 13-17 2005.

[4]. A. Agah, S. Das, K. Basu, and M. Asadi, "Intrusion detection in sensor networks: A non- cooperative game approach", in 3rd IEEE International Symposium on Network Computing and Applications, (NCA 2004), Boston, MA, August 2004, pp. 343346.

[5]. A. da Silva, M. Martins, B. Rocha, A. Loureiro, L. Ruiz, and H. Wong, "Decentralized intrusion detection in wireless sensor networks", Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks- 2005.

[6]. OTran Hoang Hai, Faraz Khan, and Eui-Nam Huh, "Hybrid Intrusion Detection System for Wireless Sensor Network", ICCSA 2007, LNCS 4706, Part II, pp. 383–396, 2007. Springer-Verlag Berlin Heidelberg 2007.

[7]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications (Anchorage, AK, May 11, 2003).

[8].National Institute of Standards and Technology, "Wireless ad hoc sensor networks", web: http://w3.antd.nist.gov/wahn_ssn.shtml, retrieved 12th January,2008.

[9]. Sumit Gupta "Automatic detection of DOS routing attach in Wireless sensor network" MS thesis, Faculty of the Department of Computer Science University of Houston , December 2006

[10] Rodrigo Roman, Jianying Zhou , Javier Lopez, "Applying Intrusion Detection Systems to wireless sensor networks ",Consumer Communications and Networking Conference, 2006. CCNC 2006. 3rd IEEE, 8-10 Jan. 2006 Volume: 1, On page(s): 640- 644 ISBN: 1-4244-0085-6

[11]. P.Bruth and C. Ko, "Challenges in Intrusion detection for wireless ad hoc networks" in Application and the Internet Workshop =s, 2003 proceedings,2003 Symposium on, PP.368373,2003.

[12]. R. Chadha, G. Lapiotis, S. Wright, "Policy-Based Networking", IEEE Network special issue,March/April 2002, Vol. 16 No. 2, guest editors.

[13]. Linnyer Beatrys Ruiz□Jose Marcos Nogueira and Antonio A. F. Loureiro. MANNA: A Management Architecture for Wireless Sensor Networks□ IEEE Communications Magazine, 2003.2b: http://w3.antd.nist.gov/wahn_ssn.shtml, retrieved 1[68]. Zhou Ying, Xiao Debao, "Mobile agent based Policy management for wireless sensor network", ISBN: 0-7803-9335-X/05, 2005 IEEE.

[14]. W. Chen, N. Jain and S. Singh, "ANMP: Ad hoc Network Management protocol", IEEEJournal on Selected Areas

in Communications17(8) (August 1999) 1506-1531.
[15]. Piya Techateerawat, Andrew Jennings, "Energy Efficiency of Intrusion Detection Systems in Wireless Sensor Networks", Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT 2006 Workshops)(WI-IATW'06) 0-7695-2749-3/06.
[16] O. Kachirski and R. Guha. "Intrusion Detection Using Mobile Agents in Wireless Ad HocNetworks", *Proceeding of the IEEE Workshop on Knowledge Media Networking*, pp. 153-158, 2002.
[17]. D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", IEEE Pervasive Computing, vol. 7, no. 1, 2008, pp. 74-81.
[18]. V. Bhuse, A. Gupta, "Anomaly intrusion detection in wireless sensor network" Journal of HighSpeed Networks, Volume 15, Issue 1, pp 33-51, Jan 2006.
[19]. Bharat Bhargava, Weichao Wang. Visualization of Wormholes in Sensor Networks. New York,NY, USA: ACM Press, 2004.
[20]. P. Albers *et al.*, "Security in Ad Hoc Networks: a General Intrusion Detection Architecture Enhancing Trust Based Approaches," *1st Int'l. Wksp. Wireless Info. Sys.*, Ciudad Real, Spain, Apr. 3–6, 2002.
[21]. Zhou, L. and Haas, Z. J., "Securing ad hoc networks", IEEE Network, Volume 13, Issue 6, Nov.-Dec. 1999, pp. 24 – 30. January,2008.FZhang, Y. and Lee W "Intrusion detection in Wireless Ad hoc Networks", The 6th annual international conference on Mobile computing and networking.

