Ensuring Network Security through the Use of the Honeypot Technique

Ensuring Network Security through the Use of the Honeypot Technique

By

Rajalakshmi Selvaraj
and Kuthadi Venu Madhav

Cambridge
Scholars
Publishing

Ensuring Network Security through the Use of the Honeypot Technique

By Rajalakshmi Selvaraj and Kuthadi Venu Madhav

This book first published 2020

Cambridge Scholars Publishing

Lady Stephenson Library, Newcastle upon Tyne, NE6 2PA, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN (10): 1-5275-4143-6
ISBN (13): 978-1-5275-4143-6

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1. 1 BACKGROUND

A 'wireless sensor network' (WSN) is defined as a group of hubs sorted into a useful network. Every hub contains handling capacity and may contain numerous sorts of memory, have an RF handset, have a force source, and suit different sensors and actuators (Butun, Morgera and Sankar 2014). In the wake of being sent in a specially appointed manner, the hubs convey remotely and frequently self-sort out. WSNs have uncommon components in contrast with past remote systems, which had sensor hubs with lower quality, hub arrangements with denser levels and computation, restrictions of capacity (Liu and Yu 2008) and overwhelming vitality. These elements create more difficulties in the application and advancement of WSNs. These WSNs have been broadly utilized around the world in recent years.

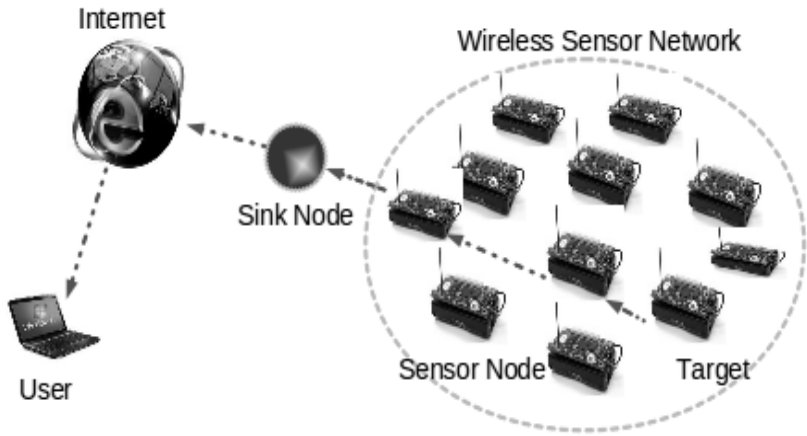

Figure 1.1 Basic structure of a wireless sensor network

Sensor hubs in a WSN perform in a territory of interest and work with less power, less cost and, furthermore, with few capacities. Despite the fact that the size of these sensor hubs is small, they are given radio handsets, sensors and implanted microchips. As can be seen from Figure 1.1 (Yu, Luo and Min 2010), sensor hubs transmit over a short separation by means of a remote medium and team up to fulfill a typical assignment that is then sent to the client through the sink hub, for instance, the control of a mechanical procedure, the observation of a front line, or the checking of an environment. Sensor systems have accompanying one-of-a-kind qualities and requirements in contrast to conventional remote correspondence systems, for instance, cell frameworks and MANET (Shen, Li, Xu and Cao 2011).

Dense node deployment: In a field of interest, sensor hubs are normally vigorously conveyed.

Power of sensor nodes: Batteries control the sensor hubs in a sensor system, so in certain circumstances it is hard to energize the batteries in a sensor system.

Calculation, basic vitality and capacity confinements: Sensor hubs in a sensor system are vigorously confined in their calculation, vitality and capacity ranges.

Setup: Sensor hubs in the sensor systems by and large perform haphazardly with no arrangement. They autonomously coordinate themselves in the event that they perform in a system.

Settled application: For a specific application, by and large, only the system is arranged and performed. The requirements of the outline of a system may change with its use.

Deceitful sensor nodes: In sensor systems, sensor hubs for the most part perform in the most exceedingly terrible situations and perform with no data. This causes disappointments for the sensor hubs.

Interminable change of topology: The topology of the system perpetually changes if there is hub disappointment.

Numerous-to-one traffic pattern: This activity example is exhibited in a few utilizations of sensor systems. In this activity, design information is spilled out of numerous sensor hubs to one particular sink.

Information redundancy: Sensor hubs in sensor systems are performed in an area of interest and take an interest in understanding a standard detection assignment in most sensor system applications. Consequently, the detected information in the sensor hubs has a clear level of excess.

With respect to the system and the arrangement of the system, the components of sensor systems and the requirements of different applications majorly affect the expectations of the system outline. The primary points of the system outline are delineated below.

Size of the tiny node: Among the points of the system outline, the reduction of the hub size is an essential one. Many sensor hubs in the sensor systems by and large perform in a most exceedingly terrible environment. Hub sending can be encouraged, and the force, utilization and expense of sensor hubs can additionally be diminished by decreasing the hub's size.

Minimal cost of the hub: The second vital point of the system outline is minimizing the hub's cost. Since numerous sensor hubs in the sensor systems by and large perform in a most exceedingly awful environment and the system cannot reuse those sensor hubs, it is fundamental to minimize the sensor hubs' cost so that the system expense is minimized.

Minimum consumption of power: A major and imperative point in the sensor system outline is reducing power utilization. Sensor hubs in the sensor systems are fueled by batteries and it is hard to revive the hubs, so the goal should be for the life span of the system and its sensor hubs to be drawn out.

Setup: Sensor hubs in the sensor systems for the most part perform with a range of energy with no arrangement. They coordinate themselves freely in the event that they perform in a system and, if there is a disappointment of the hubs, the topology of the system may change.

Versatility of the sensor organizers: The quantity of sensor hubs in the sensor system is adaptable so that the composed conventions for the system can be versatile enough to adapt to different system sizes.

Unwavering quality of the sensor systems: Data ought to be conveyed with no intrusion in the utilization of the sensor system. To convey this solid information with no intrusion, the planned protocols of the system ought to give blunder redress and control plans.

Deficiency sufferance: Disappointments of sensor hubs in the sensor system occur because of the noticeably bad surroundings and undesirable operations, so the goal is that they should be flaw tolerant.

Security: Sensor hubs in the sensor systems perform in a most exceedingly terrible environment and thus are prone to attacks, particularly in various military applications. In such circumstances, to shield a sensor hub from illicit access or the information/data in the sensor system from dangerous attacks, effective security plans must be presented.

Channel utilization of the sensor system: Due to its restricted transmission capacity, a sensor system's use of the channel gets diminished so that planned conventions can be presented for effective channel use.

QoS Support: Different utilizations of sensor systems may have different qualities of service (QoS) as far as bundle misfortune and idleness of conveyance in sensor systems are concerned.

1.1.1 WSN Intrusion Detection

An undesirable action in the system is called an 'intrusion'. Intrusion recognition is a noteworthy improvement and exploration theme that influences secrecy, accessibility and honesty. The Intrusion Detection System (IDS) runs in order to recognize undesirable intrusions for wired systems, thus it helps to accomplish a wide security method (Rao and Nayak 2014). To create an intrusion detection system for wired systems, there are distinctive methodologies and techniques, yet a few strategies are not practical for remote systems. Because of the varying quality of remote sensor organizers, the IDS made for wired systems is not appropriate for WSNs. The isolation of the dangerous, unordinary hub from the system is the real technique of the IDS in a WSN. An IDS actualized for a WSN is vital in order to find surprising, performing, not performing or damaging hubs (Li, Li, Fu and Ming 2010). Other vital perspectives for WSN security are physical security and remote transmission: above all, flagging and spying remote assault transmissions. The actualized intrusion location framework ought to evaluate the flagging and spying. Fundamental capabilities for an IDS in a WSN are physical security and distinguishing harmed hubs. This point affords the respectability of the information and directs it through the entire system safely (Li, Pandit, Katneni and Agrawal 2012).

1.1.2 Attacks on wireless sensor networks

Security assaults on wired systems are unique in relation to those on a WSN (Jabez and Muthukumar 2015). These varieties are produced using specific properties of a WSN. The vitality of a WSN is its real key, and its security includes classification, accessibility and uprightness parts. Elements of these security nuts and bolts are clarified below.

Classification: Confidentiality is the real component in the digital security worldview. At the base of this is the information transmitted in WSN systems. The information ought to be scrambled by the system to give it confidentiality. Encryption strategies such as symmetric and deviated ones can serve this encryption process. In contrast with symmetric encryption, deviated encryption is more grounded because of its private key methodology. WSN overseers ought to be certain about conveying their key when they utilize symmetric encryption. The overseer can be cautioned by a dependable and advantageous IDS about system security, or they can build up a safe key administration structure in their WSN.

Uprightness: Uprightness means information shielded from change by unapproved and undesired parties. Executives ought to be certain about uprightness to ensure their WSN is working appropriately. In a WSN, offering uprightness requires extra assets for calculation and creates additional bytes for sent information, so the engineering of the IDS can offer a noteworthy component of honesty.

Vitality: Sensors of WSNs have restricted computational assets and have constrained vitality. A WSN watches situations, and the life of the sensor is key to giving it additional time, and heads of WSNs avoid lessening the life of the battery of the sensor. Confronting this vitality approach is even more important for WSNs with regard to the parts of digital security administration. Some digital assaults are described below.

Denial of Service (DoS) Attacks: A major part of DoS assaults is to try to render an online administration inaccessible. Because of the qualities of WSNs, DoS assaults can be modified, and it is through the different qualities of WSNs that assailants give structure to their intrusions. Limited calculations and confined memory are frailties of WSNs, and these are exploited by gatecrashers. The equipment of the sensor hubs is another constraint of WSNs, and this is used by aggressors to benefit them. Assailants look to bring about WSN non-performances because of the way that WSNs work. The physical layer is a layer that can be influenced by

other assaults. Sensors can be harmed because of the expansion of physical layer assaults.

Confusion: The steering data of WSNs can be changed by confusion assaults, and the entire WSN is adversely affected by these confusion assaults. The primary stage of this assault is to send the message back the wrong way. Some methodologies are described below to help us recognize confusion assaults.

- Utilizing hashed bundles of information results. Extra vitality is not required by this technique.
- Making and using a verification device between the transmitter and the recipient. This technique happens a great deal less in its execution.
- Utilization of secure multi-bounce steering. This strategy is not proficient enough to distinguish harmed hubs.

Specific Forwarding: Although harmed hubs act like a customary hub and send parcels, a few bundles are dropped in this sort of assault. In contrast with the dark opening/sinkhole assaults, specific forwarding is more grounded. The following gatherings are countermeasures for specific forwarding assaults:

- Detection in the light of acknowledgment.
- Detection with the utilization of the data of neighborhoods.
- Utilizing a multi-information stream to combat the assault.

Sinkhole Attack: In this sort of assault, a spurious hub is presented by an aggressor in the system. This spurious hub is utilized to launch an assault, which is called a sinkhole assault. Solicitations by the hubs for directions are observed by the aggressor. This assault's approach is targeted on the information join layer.

Sybil Attack: The Sybil assault is a harmed hub that performs the acknowledgment illegitimately. To acquire the expressed request in the WSN scientific categorization (Huang, Liao, Chung and Chen 2013), all hubs in the system need to perform with the assistance of different hubs. Harming this association is the principal point of this assault. The following are types of Sybil assaults:

- Indirect and direct correspondence
- Stolen characters and fabricated characters

- Non-synchronous and simultaneous assaults

A harmed hub can point hubs at the participation procedure, the routing convention and the component used for location with this assault.

Wormhole Attack: Without utilizing the system cryptographically, the system can be influenced by this assault on the WSN (Han, Jiang, Shen, Shu and Rodrigues 2013). Data are recorded at one harmed hub by an assailant, and the hub is then burrowed to some other area by the aggressor.

HELLO Flood Attacks: In a remote sensor system, in order to distinguish the closest hub for routing conventions, a few bundles called 'HELLO Parcels' are sent to the neighboring node. To polarize different sensors, this sort of digital assault utilizes bundles, particularly gatecrashers, as they have a substantial radio and handling force and can send HELLO parcels to a lot of sensors by squeezing an entire segment of the system. A sensor that gets parcels can expect the gatecrasher to be an ordinary hub.

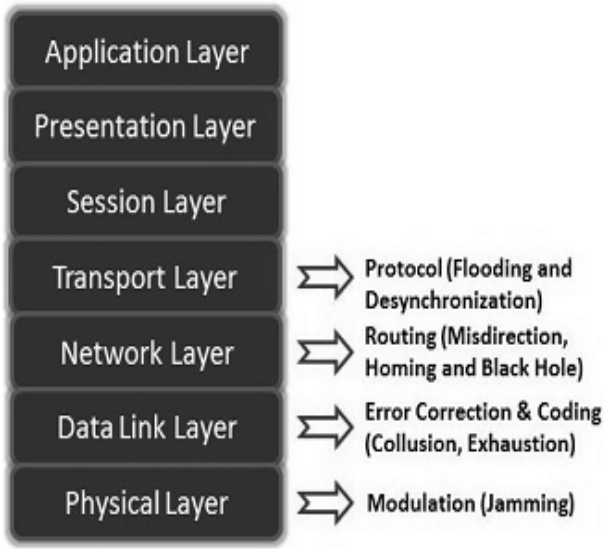

Figure 1.2. DoS Attack Types on WSN Layers (Muntjir, Rahul and Alhumyani 2017)

In Figure 1.2, DoS assaults will assault the physical layer of the WSN. Confusion assaults, specific forwarding assaults and sinkhole attacks appear

as system layer assaults. Wormhole attacks will assault the data link layer of the WSN layer. High flood attacks will assault the transport layer of the WSN layer.

1.1.3 Classification of IDS for WSNs

In order to recognize internal or external digital assaults, the IDS can be characterized as programming or equipment devices that check the system. The objectives of the IDS are recognizing assaults, counteracting assaults by giving discouragement to the assailants, gathering proof from the system, serving situational mindfulness, and obtaining association policies (Coppolino, D'Antonio, Romano and Spagnuolo 2010). The IDS' design has four fundamental segments, which are the sensor, detector (analyze engine), knowledge base, and response component. In Figure 1.3, the sensor gathers information from the monitored system and the detector breaks down the gathered information to identify intrusions. The knowledge base serves to identify the marks of an assault and the response component deals with the reactions to assaults. As indicated by the screening activity, the procedure of the framework IDS is either named a 'Network-Based IDS' (NIDS) or a 'Host-Based IDS' (HIDS). A NIDS is on a circulated system and screens system activity to recognize intrusions that can be on this system. A HIDS is on a particular PC and screens the intrusions that can be on this machine. NIDS sensors can be in any part of a system. The consolidation of both a NIDS and a HIDS is named a 'Hybrid Framework'. In order to identify intrusions, there are two methodologies that are separated into two strategies, and are named 'anomaly detection' and 'misuse detection'.

Anomaly Detection: When a system exercises something that is unique in relation to typical framework practices, anomaly detection frameworks attempt to recognize that exercise. A few procedures of anomaly detection are portable specialist-based insights, data mining, and neural networks. In Figure 1.4, anomaly detection functions admirably for obscure assaults, however now and then its false ready rate can be high. The anomaly detection procedure gets reviewed information individually, looks at the information to choose whether there are any inconsistencies or not, and in the end, if there is any irregularity, it warns the framework with a reaction message (Dhakne and Chatur 2015).

Misuse Detection: This is a mark-based recognition. This strategy has a learning base, including marks of known assaults and feeble purposes of the framework. Misuse detection is extremely fruitful for identifying known assaults, however its downside is that it struggles to detect new obscure assaults.

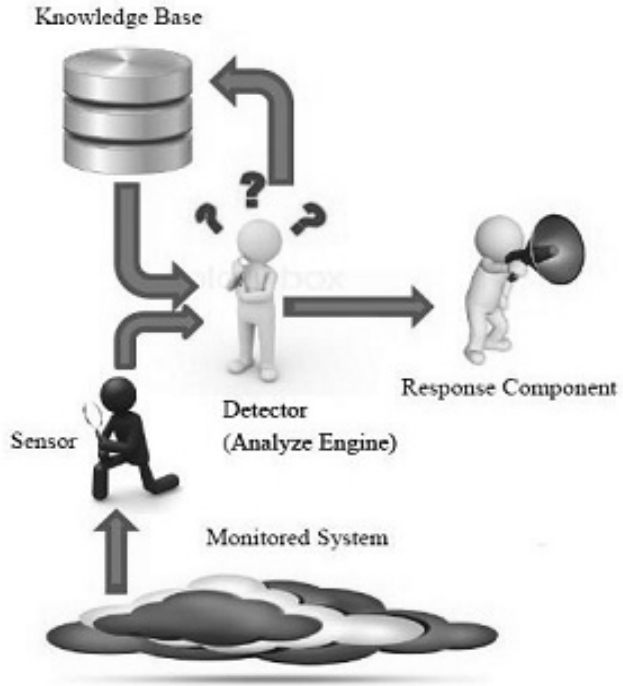

Figure 1.3. Basic structure of the IDS

Figure 1.4. Structure of anomaly detection

1.1.4 IDS approaches in WSNs

Because of the structure of WSNs, security dangers happening in the remote sensor system are not quite the same as wired system dangers and limitations; it has, for example, a restricted battery life. A WSN has distinctive IDS approaches. All groupings of discovery methodologies made by various analysts happen from open IDS scientific classifications (misuse detection, anomaly detection). The order of methodologies is as follows: intrusion sort, interloper sort, discovery procedures, wellspring of the gathered information, investigating areas of the gathered information, utilization recurrence. The interloper sort is assembled into two classifications in a system. These classifications are inside interloper (narrow-minded or vindictive hub) and outer interloper (an outside assailant attempting to access the framework). The intrusion can be made by taking information, supplying false information and thus adjusting the framework, denying access to the framework, or affecting the vitality proficient as per the intrusion type in a WSN. A few papers also bring up cross-breed or determination-based discovery for location approaches. Fathinavid and Aghababa (2012) note that in determination-based recognition, security tenets are held to distinguish specific assaults and to examine hub practices. In the event that any circumstance occurs in which these rules are attacked, then the framework decides that there is an intrusion. The IDS methodology is isolated into two sections, which are unified IDS and conveyed IDS, as indicated by investigating areas of the gathered information.

Anomaly detection approaches in WSNs: Different types of anomalies are gathered as oddities of WSNs. Association issues existing in WSNs are portrayed by system peculiarities. Unusual and startling additions and removals are the data that show whether there is any intrusion or not. These signs are depicted as broadcast storms, episodic connectivity, a loss of connectivity, and routing loops. Equipment or programming issues on the sensors are called node anomalies. The disappointment of sun-based boards and power issues cause the signs of hub abnormalities. Jumbled information sets cause data anomalies in WSNs. These inconsistencies can be created from sensor or ecological issues. Different anomalies can be characterized as not fitting to another sort of oddity seen previously. These methodologies can be sorted as measurable-based, simulated insusceptible framework-based, machine learning-based, information mining-based and diversion hypothesis-based (El-Alfy and Al-Obeidat 2014).

WSN misuse detection methods: This is otherwise called signature-based IDS and is effective for recognizing known assaults (Yu and Tsai 2008).

The disadvantage of the misuse detection approach is that it cannot recognize new obscure assaults or assaults that do not have predefined rules. For WSNs, utilizing the misuse detection system is an unpredictable undertaking in light of the imitations of WSNs. For example, keeping indications of assaults is extremely troublesome and is not viable.

Hybrid detection approaches in WSNs: A hybrid methodology can be refined, like that which stays out of the anomaly and misuse recognition methods, or that which consolidates anomaly and misuse detection techniques (Sun, Shan, Wu and Xiao 2013).

1.2 PROBLEM STATEMENT

There are numerous existing research studies on intrusion detection in WSNs. Here we describe the disadvantages of existing systems.

Network Anomaly Detection & Intrusion Reporter (NADIR): At the Los Alamos National Laboratory, the NADIR was produced for use by the research facility in its internal PC security system. Therefore, with the issues and hierarchical needs of the Los Alamos National Laboratory in mind, the NADIR was imagined. It was not by any means planned as a widespread IDS. Data are gathered from three different types of administrative hubs, which is a truly tedious and progressive, continuous process.

Distributed Intrusion Detection System (DIDS): When utilizing DIDS, there are three principal segments: 1) a DIDS director, which is capable of breaking down all the information received from the two different segments and distinguishing conceivable assaults. The DIDS director investigates material from the host screens and the LAN screens that report to it and conveys the outcomes to the SSO; 2) a LAN screen, which screens all movement in a LAN section and reports unapproved or suspicious exercises in the system to the DIDS director; and 3) a succession of host monitors, in which the reviewed information is gathered and dissected. At that point it transmits the significant data to the DIDS director. Communications manager and framework manager are the two principal people reporting to the director. Information from the host screens and LAN screens is gathered by the communications manager and conveyed to the framework manager for further handling. Inductions about the security condition of the framework and every individual host are drawn by the framework manager. The framework manager gathers the data for presentation (Cárdenas, Berthier, Bobba, Huh, Jetcheva, Grochocki and Sanders 2014).

After an intrusion, it takes a very long time to advise the director through the screens, so it is an excessively protracted procedure, making it impossible to be a standard IDS. In a substantial system, it is exceptionally hard to keep constant contact between the screens as there can be such a large number of them. It is a various leveled procedure and a disappointment at any time may make the entire framework powerless.

Graph-Based Intrusion Detection System (GrIDS): In huge systems, in order to help with intrusion recognition, GrIDS prepares the creators by proposing a strategy for building diagrams of system action. Hosts on the systems are spoken to as hubs and associations between these hosts are spoken to as edges between these hubs in the diagram. In a substantial system, GrIDS is tedious and difficult to actualize. The framework director is completely detached from the discovery-based plan, in which the restorative activities are rendered unapproachable.

Co-Operating Security Managers (CSMs): CSMs have six segments: 1) a local intrusion detection component (IDS), which performs intrusion detection for the neighborhood host; 2) a security manager (SECMGR), which co-ordinates the conveyed recognition intrusion between CSMs; 3) an intruder handling part (IH), which takes action when an interloper is discovered; 4) a Graphical User Interface (GUI), which allows security heads to associate with individual CSMs; 5) a command monitor (CMNDMON), which catches the orders executed by clients and sends them to the IDS; and 6) a TCP communication (TCPCOM), which enables TCP correspondence between CSMs. An intrusion is only taken care of after the successful fulfillment of all six criteria, so CSMs are tedious. CSMs are not relevant for a quick review of vast quantities of information. On the off chance that the system size gets larger, it is difficult for CSMs to speak with the administrators.

Event Monitoring and Enabling Responses to Anomalous Live Disturbances (EMERALD): EMERALD has been proposed as a structure for adaptable and dispersed intrusion detection between operable PCs and a system. Internal aggressors are not identified by EMERALD, as it believes the hubs of the internal system (Cheng, Chi and Lau 2011). It requires message passing. It does not go for a high review investigation speed.

Autonomous Agents For Intrusion Detection (AAFID): The AAFID works with three parts: operators, handsets and screens. The framework is self-sufficient and requires no human specialist, yet at the same time it has a few issues. Screens are single purposes of disappointment in the AAFID control

part. All the handsets that it controls stop delivering helpful data when a screen stops working. There are issues of consistency and duplication of data when copied screens are utilized, creating repetition. The AAFID design does not indicate access control components or take into account diverse clients having different levels of access to the IDS. The AAFID delays the recognition of intrusions at the screen level until all the fundamental data arrive from the specialists and handsets. This is an issue that is common to every single conveyed IDS.

Intrusion Detection and Rapid Action (INDRA): This utilizes a trusted system (Bao, Chen, Chang and Cho 2012) and creates alerts inside the system to advise about the suspected hosts. The biggest frailty of the framework is that INDRA needs trust, since intrusions may arise from any place, even from inside the trusted system. The likelihood of a false alert wins, which may put the entire framework in a precarious state. On the off chance that it originates from a trusted system, INDRA cannot adapt to the assault.

The following components should be considered in order to outline the proficiency of an IDS:

Time consumption: Additional time is required to recognize an intrusion more plausibly and make the interloper less effective, so a large and dependable IDS ought to be less protracted.

Multiple attack stability: Multiple intrusions are not liable to happen at the same time, but this scenario might still occur and none of these frameworks propose any system to handle numerous intrusions in this way.

Kind of reaction: The reaction can be either uninvolved or dynamic. The ideal path is to utilize a mixed reaction.

System association end: To identify or control an interloper, the use of an IDS appears to be very extreme, yet the best IDS ought not to require any sort of system association end.

Message spreading troubles: A decent IDS ought to be free from this issue in light of the fact that, at whatever point there is a need for a message to spread, there remains a chance of a false alert predicament.

Information handling: An IDS can incorporate or appropriate information handling. In any case, utilizing both can be far superior.

Trust issue: At each conceivable hub of the system, a perfect framework ought to be fit for recognizing intrusions. Altogether, a decent IDS should not utilize a trusted system.

A various leveled framework is not generally great: To work together with the lower level parts, a framework that has a progressive plan typically needs additional time. A novel IDS therefore ought to be variously leveled as little as could be expected under the circumstances.

The less reliance, the more productivity: There remains a possibility of a bottleneck when the segments of IDS are subject to each other. In the event that a solitary part falls flat, the entire framework may crumble. So there ought to be as little reliance as could be expected under the circumstances.

1.3 OBJECTIVES OF THE STUDY

The major aim is to determine how to detect attackers and hackers as well as how to gather information about the hackers. The captured data will be utilized for the upcoming investigations. We are proposing a novel concept known as a virtual honeypot, which will recognize and capture network intrusions.

Honeypot system

A honeypot is a data framework system set up as a decoy to distract hackers in order to gain access to information (Sokol, Husak and Liptak 2013). This definition incorporates two general concepts: 1) a honeypot can be any kind of PC asset because the expression data framework asset is extensively and purposefully characterized; and 2) a honeypot can be a work station, a gadget, a server or a whole system, and will be a distraction to capture an attacker. During the action performed by the attacker, sufficient information and data are extracted and verified. Honeypots can be utilized for generation or exploration reasons. A honeypot is also utilized for danger moderation generation. Most generation honeypots are imitations of particular working frameworks or administrations. As a result of assaults created via robotized instruments used to haphazardly search for and assume control of defenseless frameworks, systems and frameworks are secured by these honeypots. The checking procedure from these assault apparatuses can be backed right off by running a generation honeypot, squandering their time in this manner. Assaults can be closed and brought down by some generation honeypots, for instance, sending the aggressors an affirmation parcel with a window size of zero. At the point that the window size starts to build, the assault is put into a "hold" status in which it can just send

information. Figure 1.5 demonstrates the engineering of the honeypot framework. The honeypots are open to the approaching aggressors as opposed to blocking them and occupy their attention with a false database instead of a genuine database and restrict the capacity of the assailants.

Figure 1.5 demonstrates the framework outline of the honeypot architecture. Firstly, a firewall protects the whole system. At that point, the whole framework is secured by a switch, and compartmented information layers are isolated from systems inside the association and outside clients or operating systems. An instrument called the honeynet secures the association system, which is a system of PCs' support in the honeypot design. IDSs are actualized in the framework for additional security and recognition. To deal with the logs made by the honeynet, a checking control framework is utilized. An observing control framework is additionally used to screen all the approaching sections in the system.

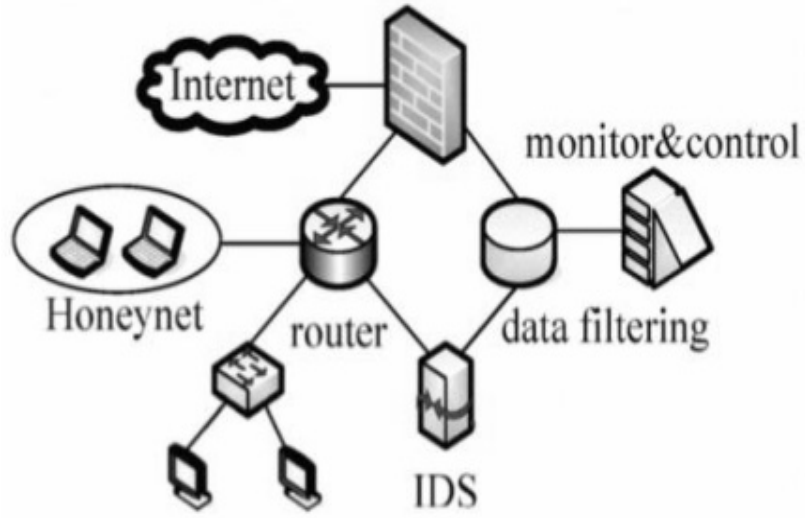

Figure 1.5. System design of honeypot architecture

1.3.1 Classification of Honeypots

Honeypots can be classified into two types.

Low-interaction honeypots*:* These are frequently utilized for generation purposes. As can be seen from Figure 1.5, low-interaction honeypots restrict

their communication and work parameters by copying certain administrations and working frameworks. The honeypot constrains the assailant's exercises to the level of imitating.

Advantages:

1) Simple to set up and maintain.

2) The potential dangers are diminished by the restricted imitation permitted in low-interaction honeypots. In the case of low-interaction honeypots, it is a façade application that gives a bogus picture of an objective host. A façade assembles data about the assailant when it is tested or assaulted. As exteriors frequently require negligible establishment exertion and hardware, they offer basic, simple sending and can imitate an expansive assortment of frameworks.

High-interaction honeypots*:* As high-interaction honeypots (Yu, Luo and Min 2010) include genuine working frameworks and applications, they are more mind-boggling. In the event that the aim is to gather data about hackers on a specific FTP server or administration, a genuine FTP server will be assembled. No limitations are placed on the aggressors' conduct as they are given genuine frameworks to connect with, and in order to catch broad insights about the full degree of a hacker's techniques, directors are permitted. To keep an attacker from further damaging data and servers, the honeypot framework itself, i.e. the system associated with the honeypot, should be separated in the worst-case scenario.

A characteristic of high-interaction honeypots is the conciliatory sheep, which is a framework purposefully left helpless against an assault. The honeypot will occasionally be inspected to figure out whether it has been traded off and, assuming that this is the case, what was done to it. A system sniffer placed close to the honeypot can gather extra information, for example, a point by point hint of charges sent to the honeypot. In any case, the honeypots themselves are "live" and in this manner introduce a conceivable bouncing off point for an aggressor. With the specific end goal of disengaging and controlling the honeypot, extra organization considerations must be made, for example, a method of firewalls or other system control technology, or the total separation of the honeypot from the internal system. All created outcomes are precisely as they would be for a genuine framework in light of the fact that conciliatory sheep are themselves genuine frameworks. Be that as it may, significant authoritative overheads,

for example, the establishment of a fully working framework and a manual, are required by conciliatory sheep (Sokol, Husak and Liptak 2013).

The second characteristic of high-interaction honeypots is an authentic working framework that gives data, regulations and control. Here, proficient security engineers have altered the working framework and portion, not at all like the conciliatory sheep model. The qualities of both conciliatory sheep and façades will be consolidated by these systems. They give a complete duplicate of an authentic framework that is prepared for assailants, like the conciliatory sheep framework, and at the same time (like façades) they are fluently available and hard to sidestep. The honeypot innovation is additionally utilized for concentrating on spam and email reaping exercises. Honeypots have been conveyed to concentrate on how spammers distinguish open mail transfers. To find out the reasons why spam messages were received, spam emails are received and broken down. Likewise, by utilizing an email address, an email trap can be set up, committed simply to getting spam messages.

1.3.2 Strategies of honeypot deployment

The organization ought to deliberately want to amplify the qualities of honeypots and minimize the dangers involved. At that point, assault-related data can be gathered by the honeypot. Nonetheless, if an effective attack happens on the honeypot inside the system, that compromised honeypot system may be exploited to check for other potential flaws in the system. This is the primary issue of initiating the honeypot inside the creation framework. This would not happen in other honeypot arrangement techniques as the entire honeynet can itself be an invented system (Abduvaliyev, Pathan, Zhou, Roman and Wong 2013). A specific measure of information, for example the site core of a web server, may have to be reproduced in the honeypot to cover the honeypot. Another strategy is to assemble a honeynet, which is a system of honeypots that mimics and imitates an authentic system.

1.4 JUSTIFICATION

The current work introduces the honeypot framework aided by the IDS. These techniques are regarded as the main terms for defensive functions. This methodology is also regarded as the flexible security mechanism, and it also eliminates the stealing of information by attackers. The proposed methodology includes the main functionalities in order to confuse attackers as well as gather the framework's information, then direct them onto the

wrong path. This process differentiates the attacker's movements with new techniques and applications. The intruders may have a place within the black hat group and attempt to take over the information that was stolen from the framework, aided by data like the TCP address, IP address, and so on. After gaining information about the attacker, the next action of the honeypot framework will be to protect the user's information and secure the information from the attackers. The honeypot framework plays a major role in identifying intruders.

1.5 OUTLINE OF THE CHAPTERS

Chapter 1 describes the introduction of the topic, the background, problems identified, etc.

Chapter 2 gives a review of recent literature on the topic.

Chapter 3 depicts the inspiration for this examination/target work.

Chapter 4 delineates a major technique for honeypots utilizing intrusion detection systems.

Chapter 5 depicts an ant-based DDoS detection technique using roaming virtual honeypots.

Chapter 6 discloses how to upgrade intrusion detection system performance by using a FireCol Protection Services-based honeypot system.

Chapter 7 delineates the Efficient Approach to Protect the Network and Intrusion Prevention (EIDPS).

Chapter 8 clarifies an effective ODAIDS-HPS approach for preventing, detecting and responding to DDoS attacks.

Chapter 9 is the conclusion of this work and recommends some conceivable future improvements.

CHAPTER 2

LITERATURE SURVEY

2.1 INTRODUCTION

Intrusion detection is a major part of wired and wireless sensor networks. Intrusions will occur due to the dangers in and attacks on the networks. To prevent these intrusions, many intrusion detection techniques such as present or system located, initial or irregularity located, energetic or submissive observing, concurrent or interlude processing and, finally, integrated or circulated applications have been presented. IDS has become a necessity due to the significance of preserving privacy and obtaining reliability for our most appreciated possession, which is data. Many research papers have been published based on these intrusion detection techniques.

In this chapter, related research works on IDSs are presented. Here, these related works are classified as follows:

1) Anomaly-based IDS
2) Distributed approach for IDS
3) Trust-based IDS
4) Cluster-based IDS
5) Intelligent IDS
6) IDS in MANET
7) IDS for Heterogeneous WSNs
8) Game theoretic approaches for ID
9) IDS for various attacks
10) Agent-based IDS
11) Traffic analysis-based IDS
12) Immunity-based IDS
13) Optimized algorithms used for IDS
14) Data mining approaches for IDS
15) Energy-efficient IDS

2.2 ANOMALY-BASED IDS

Intrusion detection is concerned with detecting executions that make an effort to violate information security. The security policy of an information system is violated by the intrusion, which is an activity. IDS, therefore, is an attempt aimed at curtailing the excesses of the intruders. IDS is either misuse-based or anomaly-based depending on the model of its application. Idowu *et al.* (2013) have projected a new but vigorous algorithm called a membrane algorithm for NP-complete optimization problem solving using the P-system paradigm. Systems try to prevent intrusion attempts, and the IDS is neither needed nor anticipated by the monitoring system. Logging details about incidents and recording trials is the main ID and prevention system for attainable incident identification. For other desires, like issues' identification with security strategies and discouraging singles and previously documented threats from overstepping security strategies, Intrusion Detection and Prevention Systems (IDPSs) are additionally used by organizations. Given the security infrastructure of every organization, IDPSs have become essential. Jabez and Muthukumar (2015) have proposed an innovative scheme named "outlier detection", where the irregularity of the dataset is estimated by the NOF.

El-Alfy and Al-Obeidat (2014) have proposed a scheme for "anomaly-based intrusion detection" using a "fuzzy classification" scheme together with a selection of greedy parameters. Based on the content, time and host, the projected method attributes have superiority in dealing with different kinds of attributes and compressing TCP/IP network traffic basic packet headers. At the same time, the selection of the greedy parameter algorithm allows the selection of the finest attribute group that was most significantly aimed at detecting intrusive events to decrease the dimensional and computational complexity, and different network components of the constructed system are enabled to be virtual in order to develop open system infrastructures such as radar links, informal wireless links, and cloud calculating and shrewd networks.

Modeling normal user activities is an important issue in intrusion irregularity detection. The technique of conventional data mining is applied generally to finite audit datasets for the purpose of normal behavior extraction from user activities. In audit datasets, these methods model stagnant user behavior. Park *et al.* (2010) have projected an "anomaly intrusion detection" scheme which uninterruptedly uses the normal behavior of an operator above the review file stream. A set of characters is used to represent the features of a movement in this paper. Each cluster, in the

proposed method, represents the regularity scale of the actions with respect to the feature. To improve the performance of irregularity detection, different statistics of actions corresponding to the detected clusters were also demonstrated in this paper.

When detecting a new attack, irregularity intrusion detection plays a significant part in an IDS by identifying any variation from the normal profile. Lin *et al.* (2012) have projected an efficient algorithm with a selection of features and decision rules applied to irregularity or "asymmetry intrusion detection". The benefits of "simulated annealing" (SA), the "decision tree" (DT), and SVM are taken as key ideas in this paper. SA and SVM can find the best-chosen attributes to increase the accuracy of irregularity intrusion detection in the proposed algorithm. The decision rules for new attacks are obtained by analyzing the information after expending SA, the KDD'99 dataset and the DT, and the accuracy of classification also improved in this paper. In addition, SA spontaneously adjusted the best restriction settings for the DT and SVM.

El-Ghali and Masri (2009) have presented a new method for identifying failures of software security, the major aim of which is simplifying the detection and restoration of security weaknesses. The proposed method of this paper depended on the online capture of performances and profiling, offline performance replay and evaluation. The flow analysis, known as a "fine-grained dynamic data flow analysis", was engaged by this proposed approach in combination with anomaly detection. The proposed goal of this paper, also called "information flow anomaly detection", was detected in various security failures, including ones that concern intrusions of privacy and ones that do not. A prototype tool called DynFlow implemented the method for Java byte code programs.

The security of the WSN is an important objective for many researchers. IDSs played a major role in detecting and avoiding security attacks. Maleh *et al.* (2015) have presented a hybrid, inconsequential intrusion detection system. To reduce energy consumption, their IDS worked on the superiority of cluster-based architecture. This system used anomaly detection and a group of signature rules to identify mischievous behaviors and afford a global lightweight IDS based on the "SVM algorithm".

Sun *et al.* (2013) have presented a combination of ID and "system monitoring modules" in the background of WSNs. To identify corrupted data, they proposed an extended Kalman filter (EKF)-based appliance. Specifically, by monitoring the activities of its neighbors and by using the

EKF to forecast their future situations (real in-network aggregated standards), each node aimed to fix a normal range of upcoming transmitted collected values. Due to the potential coarse environs, high packet loss rate and recognized insecurity, this task is challenging. The authors explained how to utilize the EKF to solve the challenge of making valuable local detection mechanisms. They presented how to obtain an abstract inception by means of diverse combination utilities (mean, total, maximum, and minimum). They also applied an algorithm integrating progressive summation and a generalized possibility ratio to improve detection understanding. Finally, they explained how they offered native discovery methods that work mutually with the "system monitoring module" to distinguish between mischievous actions and reserve actions to overwhelm the restrictions of native discovery mechanisms.

The difficulties of misinterpretation, misdetection and the absence of a real-time reaction to the outbreak are the most significant challenges to intrusion detection. For intrusion detection, numerous information excavating methods are used, such as grouping, cataloging and union law recognition. The anticipated hybrid method of the paper offered by Ravale *et al.* (2015) combined information excavating methods such as the RBF kernel function and the K-means clustering algorithm of the Support Vector Machine as a sorting unit. Reducing the number of features related to each data point was the central point of the projected method in this paper. In terms of detection rate and accuracy, the suggested method worked well when employed with the KDDCUP'99 dataset.

In WSNs, safety matters are most important. WSNs are vulnerable to certain kinds of occurrences as they are composed of inexpensive and minor devices and are positioned in exposed and isolated surroundings. Yan *et al.* (2010) have suggested an IDS formed in the sphere of the group head. The suggested IDS was a hybrid IDS. It had variances as well as an abuse finding unit. The aim of this paper was to increase the finding rate and reduce the untrue progressive degree by utilizing the benefits of abuse finding and variance finding. However, an executive element was used to assimilate the identified outcomes and to state the kinds of occurrences.

2.3 DISTRIBUTED APPROACH FOR IDS

Krishnan (2015) has conveyed that a dispersed self-adjusting IDS depends on designable mobile factors that can represent a vital link in the defense against major security assaults. Krishnan has presented an "intrusion detection model" that is prepared as a blend of the two forms of IDS: the