ISSN No:-2456-2165

Intrusion Detection Algorithm for Mitigating Sinkhole Attack on Leach Protocol in Wireless Sensor Network: A Case of Iprc-Huye Campus

(Area of Focus: Wireless Sensor Network)

UMUHOZA Epiphanie, Dr. Wilson MUSONI(PhD),
Mastersof Science with honors in Information Technology, at University of Kigali, Rwanda

Abstract:- Wireless Sensor Network deploys tiny sensor devices to sense physical parameters and transmits periodically to a central station called sink nodes or base station. In several fields nowadays, wireless sensor networks are frequently used, especially in environmental applications, military applications, etc. Since, wireless sensor network is deployed in hostile environment; security forms a major concern for the network. In WSN protocol stack, the network layer poses many security threats. Sinkhole attack is among the serious network layer threat which attracts the entire traffic towards itself and drops or selectively forwards the data packets. This attack will lead to lose many data and performance degradation of the wireless sensor network. Nowadays, sinkhole security attack is still being a problem on the network of sensors. Therefore, this thesis proposes an intrusion detection algorithm for mitigating sinkhole attack on Wireless Sensor Network which uses a clustering-based routing protocol namely LEACH for its routing operation in IPRC-Huye Campus. In the suggested technique, the intrusion ratio (IR), which is determined by the IDS agent using detection metrics like the quantity of packets sent and received was used to detect if there is a sinkhole or not. The calculated numerical or non-numerical value depicts legitimate or unlawful activities. The simulation results demonstrate how the sinkhole node significantly affects network performance by dropping all the packets that it receives from the cluster members. The IDS agent warns the network to halt the data transfer as soon as the sinkhole is detected. Our proposed algorithm checked one network security which is sinkhole attack.As a result, it may be resistant against sinkhole attacks. The simulation results for the recommended algorithm are also shown, and they show that it performs well in comparison to the existing networking without an intrusion detection algorithm in terms of minimal computing both complexity and low energy usage. The approach was also numerically simulated and examined using MATLAB.

Keywords:- *Intrusion Detection Systems, Joint Request Packet, Hierarchical Wireless Sensor ,Denial Of Service, Intrusion Detection, Network Based Intrusion Detection Systems, Signature Based Intrusion Detection System, Demand Signal Repository, Sinkhole Message Modification nodes.*

I. INTRODUCTION

Wireless Sensor Network is constituted of many deployed sensors that are responsible for gathering data from the physical environment around and send it to the sink node (base station). The sensor nodes have limited resources like CPU, battery energy and memory, but its short-range wireless communication to communicate with the base station and with each other. The base station manages the normal operating of the network, and also performs the processing of the collected data and storing them (Kumar, 2017).

Regarding that wireless sensor networks are characterized with low resources like low processing power, low communication resources, low memory and are powered by a battery, to make use of these scarce resources properly when building the wireless sensor network protocols, various trade-offs are present. To overcome the issue of low resources, clustering schemes are deployed in sensor networks to ensure efficient resource usage and reduce communication overheads, reducing the system's overall energy usage and keeping interference low among the sensor nodes (Jubair, 2021).

Security is most crucial problem in wireless sensor networks due to their nature. The low processing and low memory constraints prohibit the deployment of a protocol with security mechanisms in it. The environment in which wireless sensor networks are implemented makes them susceptible to sinkhole attacks. One of the deadliest assaults is the sinkhole attack, when a false node publishes a phony routing update, such as the quickest route to a sink node, to disrupt network traffic (Ali, 2020).

In WSN, two types of network models are available. Distributed model structure that constitutes a homogeneous network in which all nodes have the equal in terms of energy resources, calculation and memory, and another one is hierarchical model where all nodes do not have the same roles and therefore the same resources, the simulation results of energy consumption in each architecture, show that the hierarchical one is more efficient than flat (Oudani, 2018). It is the why that, this thesis is based on the hierarchical routing protocols.

ISSN No:-2456-2165

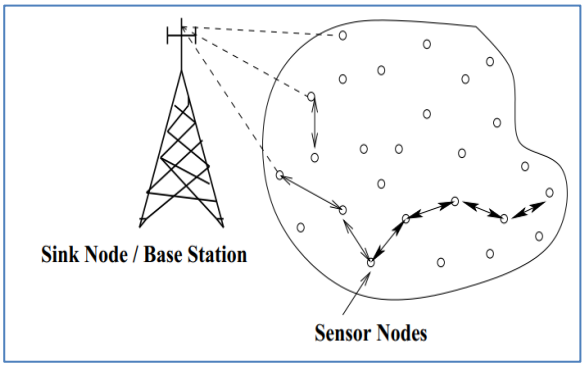


Fig. 1: A distributed wirelesssensor network

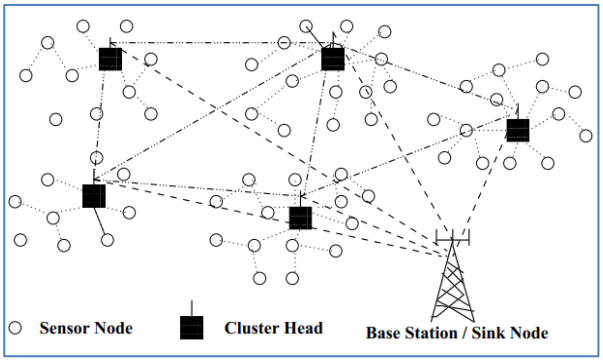


Fig. 1: A hierarchical wireless sensor network

Through the technique of information pooling in the Cluster Head (CH), Low Energy Adaptive Clustering Hierarchy (LEACH) routing is specifically used to lower the data transmission rate in wireless sensor networks. By reducing energy used for communication, this method lowers the energy requirements of the sensor nodes. In order to improve load balancing and extend the network's service life, clustering is also deployed. By ensuring that the CHs' responsibilities are balanced, clustering works to prolong the life of the network.

II. BACKGROUND TO THE STUDY

Indian paper writers, in their paper (Waoo, 2021) stated that a wireless network is made of small devices known as sensors are a group of interconnected, inexpensive, and elegant computing sensors. These sensors are used today in all advanced sectors, including the development and deployment of smart environments.

These smart sensors get geographically distributed within network in such a way and embedded by the process to ecological devices with various purposes like measuring and monitor environment effectively like temperature, sound, humidity, pollution levels, wind. The sensor nodes of the network using radio signals can interact and exchange information among themselves.

Wireless sensor networks continue to offer crucial services for numerous applications, including monitoring, data collecting, and data transmission from dangerous areas to safer locations, according to (Jibreel, 2022). The energy-efficient routing protocols, which are primarily created for such uses, have improved this.

Extensive research on sensor routing protocols and their threats is available in (Wagner, 2003). In WSN, LEACH Protocol is employed as its energy-efficient routing protocol to make the most of the network's limited resources. A technique for grouping the sensor nodes into a grouping hierarchy mostly based on weight attributes is called hierarchical clustering. Security is very crucial concerning of the various hierarchical protocols that have been researched (Sharma, 2011).

An energy-efficient protocol called LEACH relies on hierarchical clustering to function. In 2002, this procedure was suggested by (Balakrishnan, 2002). They came up with a novel approach to WSNs that use hierarchical clustering that makes use of random CH rotation based on the features of a node, including its energy and bandwidth. In contrast to conventional clustering procedures, to ensure that energy is spread fairly throughout the network, LEACH calls for the random and dynamic rotation of CHs, which keep the CH on the same node throughout the routing process. The representation below demonstrates the LEACH protocol's operations. The initialization stage and the steady state stage are the two periods in which the protocol operates. Each sensor network member chooses a number drawn at random between 0 and 1 to take part in the first round of voting. This sensor node is chosen as a CH if the value is less than the threshold value T (n) (Saini, 2013).

Active and passive attacks are two major categories into which various security concerns in WSN are categorized. In an active attack, the compromised node modifies the data while it is being transmitted. Denial of service, alteration, impersonation, fabrication, and other threats are now being used. A passive attack involves an infected node that observes the data transit rather than altering it. Eavesdropping, traffic monitoring, and enemy camouflage are a few examples of passive attacks. Low level and high-level security measures are the two categories into which these attacks are categorized by security measures. Authentication, privacy, and key establishment are all parts of the low-level system. Safe group administration, a system for detecting intrusions, and safe data aggregation are all components of the high-level method. (Padmavathi, 2009). The IDS work as a second line of defense for the network and notifies it when dangers are present. According to (Ajala, 2018), Rwanda is currently putting its 2050 vision into action, concentrating on the SDGs and making industrial production one of the primary drivers of economic growth. IoT technologies are anticipated for usage in smart industries, taking ICT into consideration. In this line also, IPRC-Huye has introduced the technology of using wireless sensors network to monitor water tank levels in whole campus

III. METHODOLOGY

A. Data Collection Methods and Instruments/ Tools

The practice of gathering information using specified procedures in order to react to the study's predetermined research subject is known as data collecting. Considering general purpose of this research thesis, which design a sinkhole attack mitigation intrusion detection system technique for wireless sensor networks, the work defined on

this research is methodology deliberates to observe a quantitative research strategy.

The chosen method manner that a quantitative inquiry approach deliberates of being accompanied inside the design and circumstance of the study.

Since the study requires use of simulation platforms, primary data and secondary data were collected using questionnaires and interview.

B. Data analysis

The process of developing answers through examination and interpretation is known as data analysis. Data analysis is critical for understanding survey and administrative results and providing data information. Data analysis is expected to provide enlightenment on the topic under study and respondents' perceptions, as well as to enrich readers' knowledge of the topic under study and to pique their interest in that range of the studyData analysis is the key of quantitative research. The research data results were obtained and interpreted by simulating WSN that uses LEACH protocol to transmit data. The simulation was done using MATLAB software.

➢ *Data processing*

Data processing were mainly done through simulations and graphical interpretation of the current mechanisms and systems in use. The aim of this analysis helps the researcher to record and comprehend “as is” the state of the current WSNs security set-up environment and intrusion detection algorithms.

➢ *MATLAB*

was used to simulate network topologies. It was also used along with the already off-the-shelf protocols to carry out network modifications.

MATLAB stands for MATrixLABoratory and the software is built up around vectors and matrices. MATLAB is an excellent tool for solving algebraic and differential equations as well as for numerical integration, which makes it very useful for linear algebra. MATLAB offers robust graphic capabilities and can create appealing 2D and 3D images. It is one of the simplest programming languages to use for creating mathematical programs. It is also a programming language. Additional tool boxes for signal processing, image processing, and optimization are available in MATLAB (Chidiebere, 2017).

C. Research Design

In this study, experiments based on the algorithm were carried out. Results from experiments were compared with control samples. Samples input data were used to test the variations in the results. At the end correlation research was conducted to compare variables of the new results. Because we don’t have continuous data, random data samples were assumed. This research was carried out in IPRC-Huye campus. This was the case study of this research thesis because it is a place where we can find sufficient and appropriate infrastructure.

The below, there is a figure that explains the proposed IDS algorithm.

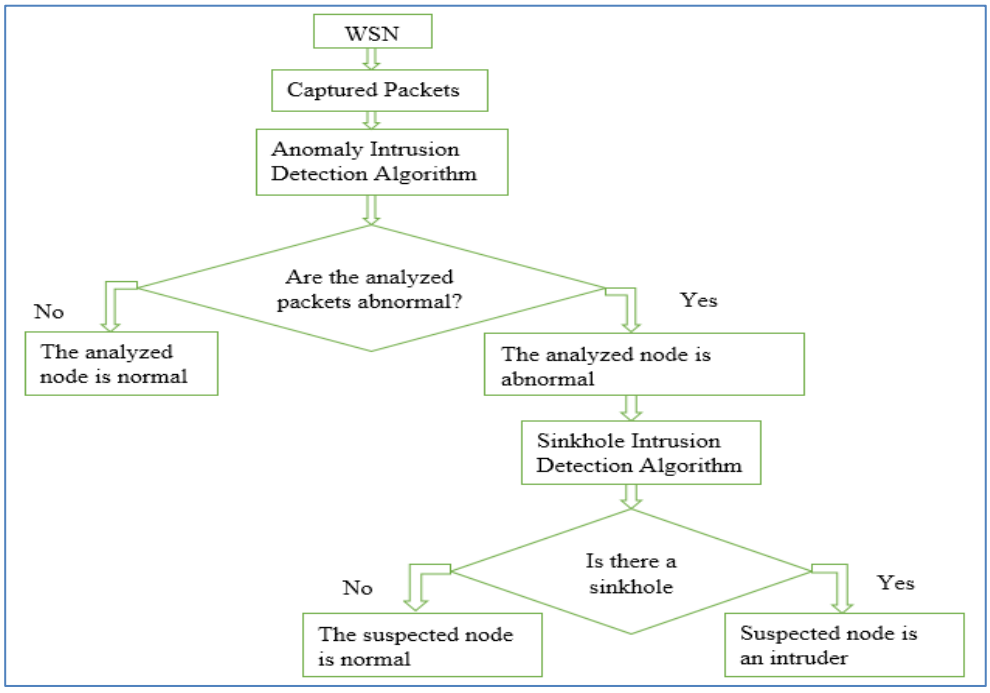


Fig. 3: Process of proposed IDS algorithm

D. CONCEPTUAL FRAMEWORK

A conceptual framework, often referred to simply as a "framework," is a structure or a set of interrelated concepts that provide a basis for understanding, analyzing, and discussing a particular topic or area of study. It serves as a theoretical foundation that helps researchers, scholars, or professionals conceptualize, organize, and frame their research or work within a specific field or discipline.

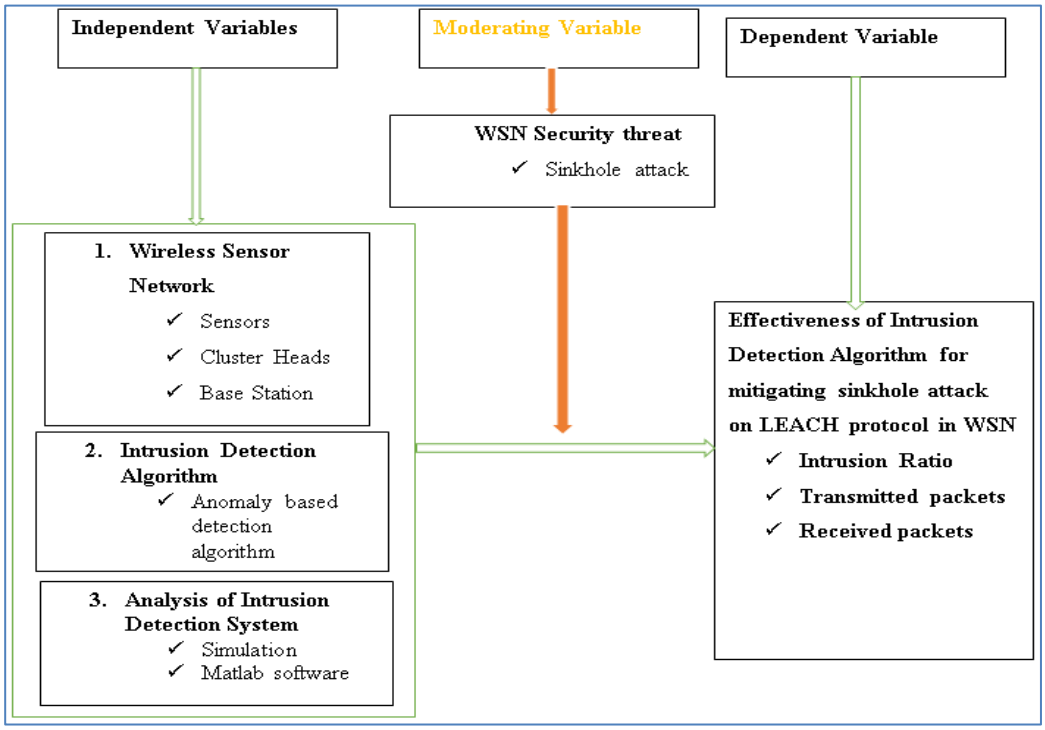


Fig. 4: Conceptual Framework

E. Ethical considerations

Ethical consideration helps in protecting the data obtained within this research. The researchers' responsibility to be truthful and respectful to all people affected by their study or the results report constitutes research ethics. Researcher is generally administered by several ethical regulations. The researcher will respect the values of people who deal with. Gathering data was only facilitating me to accomplish the academic task and to contribute to the promotion of quality of education. Data was treated confidentially and nobody among respondents blamed of his/her answer.

F. Data analysis

According to the data collected from questionnaires and interview conducted at IPRC-Huye Campus, the used technologies to detect wireless sensors network threats are not efficient to enhance the performance of the network. 90 per cent of the total respondents showed that they have experienced with the issues of the sinkhole attack. The table below shows the overview of the answers from different respondents.

Table 1: Feedbacks from Respondents

Department	*n*	Answers	
		Users experiencing sinkhole attack	Users not experiencing sinkhole attack
Staff	5	5	0
ICT Personnel	5	5	0
IT Students	206	195	21
TOTAL	216	205	21
%	100%	90%	10%

As presented in the table above, all 216 respondents in IPRC-Huye Campus answered the questionnaires and interviews as we have planned. Going through the feedbacks, all staff and ICT Personnel experienced the issue of sinkhole attack in the wireless sensor network. And also, among 206 IT students, 195 students experienced a sinkhole attack while 21 of the IT students did not experience sinkhole. According to the statistics, 90% of the all respondents experienced a sinkhole attack while 10% does not experience a sinkhole threat in the WSN.

IV. DATA PRESENTATION

Findings are presented by respecting objectives of the research study.This section presents the data collected and analyzed into graphs for staff, ICT Personnel and IT students.

A. Staff

The data collected from staff department showed that all staff targeted in the research have experienced with sinkhole attack as shown on the below graph.

ISSN No:-2456-2165

Fig. 5: Staff Data Presentation

The figure above shows that 100 percent of the research targeted staff have experiencing a sinkhole attack in WSN. The long bar represents n=5(100%) of the staff experiencing sinkhole attack while the staff that have not experienced sinkhole attack have no bar which means that there are no users not experiencing sinkhole attack.

B. ICT Personnel

The data recorded from ICT Personnel showed that all targeted users in the research have experienced with sinkhole attack as shown on the below graph.

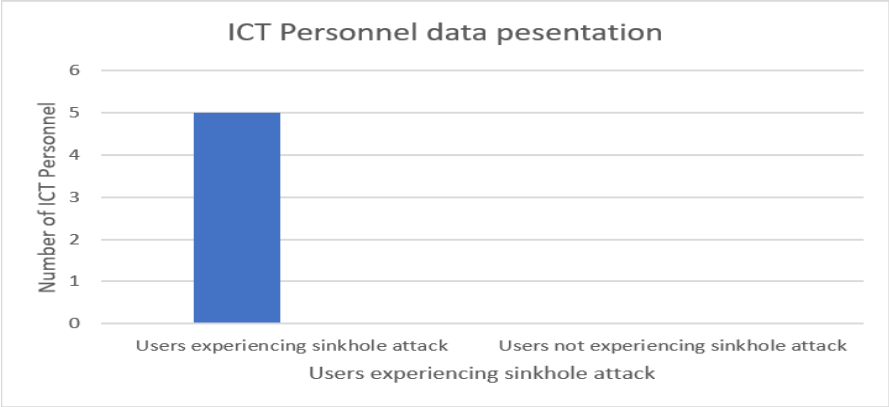


Fig. 6: ICT Personnel Data Presentation

The figure above shows that 100 percent of the research targeted users have experiencing a sinkhole attack in WSN. The long bar represents n=5(100%) of the ICT Personnel experiencing sinkhole attack while the ICT personnel that have not experienced sinkhole attack have no bar which means that there are no users not experiencing sinkhole attack.

C. IT Students

The data recorded from IT students showed that all IT students have experienced a sinkhole attack as shown on the below graph.

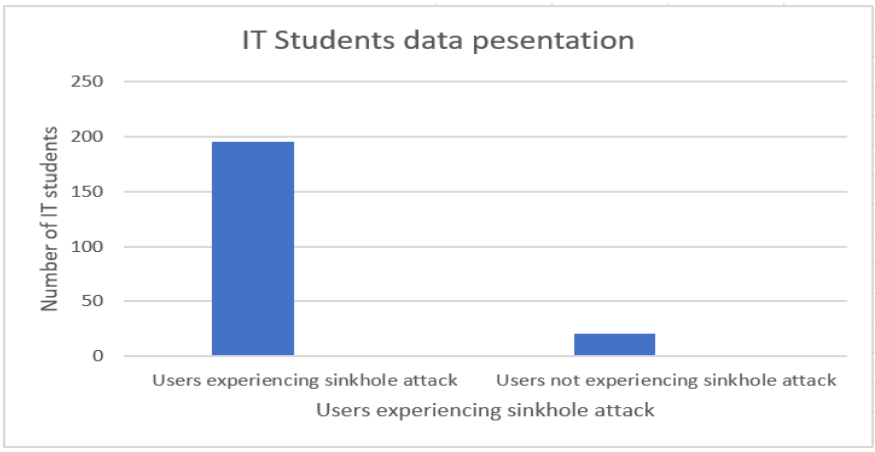


Fig. 7: IT Students Data Presentation

ISSN No:-2456-2165

The figure above shows that 94.66 percent of the targeted IT students have experienced a sinkhole attack in WSN while 5.33 percent does not. The long bar represents n=195(94.66%) of the IT students experiencing sinkhole attack while the IT students that have not experienced sinkhole attack have small bar representing 5.33%. This concludes that there is a serious issue of sinkhole attack in wireless sensor network of IPRC Huye Campus. In the following sections of the study, we proposed a solution the issue of sinkhole attack in the wireless sensor network.

D. Proposed intrusion detection system algorithm model design

The IDS act as the network's second highest line of defense and notifies it when threats are present (Ranjeeth, 2015). This research study focuses on the high-level protection system, specifically the IDS, to find malicious nodes. By claiming to be the node closest to the base station, the infected node attracts packets and modifies those traveling through it to start the attack. In the majority of sensor network routing protocols, no measures are started to detect security assaults.

This study's main goal was to develop an intrusion detection algorithm that reduce the effects of a sinkhole attack on a WSN that uses the LEACH protocol for routing and to provide a security mechanism to prevent it. A WSN may experience sinkholes due to both internal and external attacks. The sinkhole attack is effectively detected by the suggested IDS technique. The performance of the intrusion detection technique is statistically validated, and simulations support its precision and effectiveness. A clustered node map was employed in the proposed model to carry out the concept. In the proposed model, a clustered node map was used to implement the idea. I this case, the network model involved having a group of nodes forming a cluster.

E. Cluster Formation

Clustering is the process of maintaining a small number of logical assemblies made up of physical network nodes while the network is in use. Clusters are the logical assembly. During the initial cluster construction, it can spot compromised nodes and eliminate them. The first line of protection for secure clustering is removing the vulnerable nodes during cluster creation. The clustering is driven by the minimization of energy for all the sensors.

Based on the relative distance from nodes, clusters are formed. Data transfer from a cluster to a base station is done by a CH. Energy consumption in this model is relatively low. Clustering helps in quick discovery of routes because only cluster heads do communicate with the Base station.

The illustration below shows how the communication will be in the cluster. It is a single-hop node-to-cluster communication. The wireless sensor network structure is made up 30 node sensors that are linked to one base station. Those sensors are grouped into three clusters. This network structure helps the sensors to consume low power energy while transmitting data into the network.

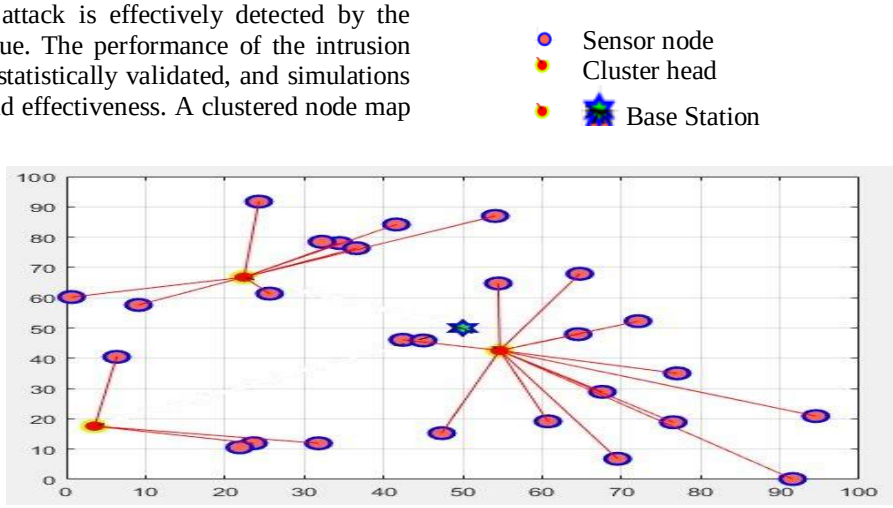


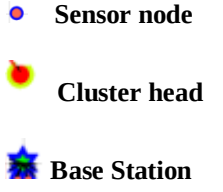
Fig. 8: Transmission between Sensor nodes and cluster head

LEACH rotates cluster heads in a dynamic and random manner, as opposed to conventional clustering algorithms, which retain the head as the same node, to ensure that energy is consistent across all sensor nodes, according to Kumar's analysis of the cluster formation in wireless sensor networks (Kumar, 2017).

F. Cluster Head Selection

The WSN divides clusters, each having a coordinator (cluster head) responsible for gathering the data from the nodes and sending it to the sink (base station). The cluster heads can be selected hazardly or based on one or more criteria. Selection of cluster head largely affects WSNs lifetime. The ideal cluster head is the one which has the highest residual energy, the maximum number of neighbor nodes, and the smallest distance from the base station. Here there are three clusters and cluster head for each cluster.

We employed a single hop cluster-to-Base station transmission hierarchy in the suggested communication paradigm. According to the diagram below, the Cluster Head sent the data it had gathered immediately to the base station.



ISSN No:-2456-2165

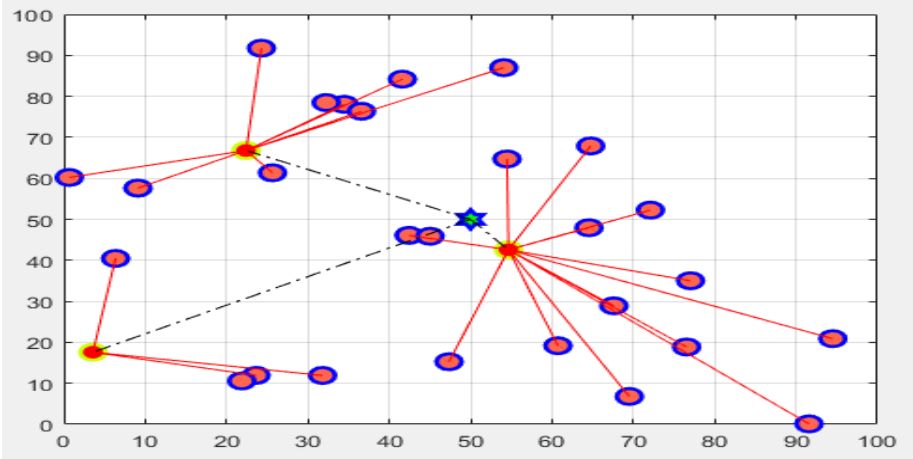


Fig. 9: Transmission of data from sensor nodes to CH and from CH to BS

During the steady state phase, each node transmits its data to the appropriate CH at the appropriate time. The CH performs data aggregation and transmits the data to the BS or to the CH that is nearest to it when the BS is outside of its transmission range. Because of this, CHs are the only nodes that directly interface with the BS. A cluster node's radio is only in the active state while it is in their time slot; otherwise, it enters the sleep mode, forcing sensor nodes to conserve energy.

G. Intrusion Detection at CH Level

The intrusion detection at CH level is conducted by BS, reducing the possibility of being deceived by CHs and decreasing the energy consumption of CHs. The trust calculation of each CH is different from SN. The malicious SN discovery, which also detects by a threshold of trust of CHs, is comparable to the harmful CH discovery. Where CHS is the set of CH in WSN, the BS computes and stores the trust value of each CH and chooses a threshold trust as the. The BS evaluates each CH's trust value within the WSN and compares it to the established threshold, classifying any CH whose trust value is below the threshold as malicious or compromised.

H. Intrusion Detection at Sink node

Since sink nodes are typically targeted by sinkhole attacks, the focus of this research project is on designing an intrusion detection method for minimizing sinkhole attacks on wireless sensor networks that transmit data utilizing low energy adaptive clustering hierarchy as the routing protocol. Through the modification of routed data, this kind of attack can bring down the entire wireless sensor network. When a wireless sensor network employs the LEACH protocol, the entire network is split up into sensor clusters. Cluster heads receive data transmissions from sensors first before sending them to the base station. Based on the energy levels of the sensors and the proximity to the base station, cluster heads are chosen at random by a base station.

A sink node is a cluster head node that is close to the base station and has a high level of energy. Because it is the quickest data transmission path to the base station, a sensor node targeted by a sinkhole security threat will pose as a real sink node and promote its routing protocol to other sensors in the network. Then, after receiving data from sensors, a sinkhole modifies the information (message) before sending it to the base station. According to (Fessant, 2010), if a sinkhole attacker node is deployed successfully, there will be three possibilities: messages may be lost (dropped by the attacker node), messages may be delayed, or messages may be modified. On the basis of these three observations, three types of sinkhole attacker nodes are possible:

- Sinkhole message modification nodes (SMD): Before sending the messages to the subsequent node, sinkhole attacker nodes change the messages.
- Sinkhole attacker nodes dump the messages, occasionally even on purpose, using sinkhole message dropping nodes (SDP).
- Sinkhole attacker nodes may delay message forwarding by acting as sinkhole message delay nodes (SDL).

I. Anomaly based IDS algorithm design

Security is the top priority in a wireless network, and because sinkhole attacks are so relentless, they exceed all other threats. In order to ensure security, efforts were concentrated on identifying the likelihood of a sinkhole attack in a sensor network using LEACH, comprehending the ramifications of the assault, and developing an IDS to mitigate the consequences (Arumugam, 2018).

➢ *Introduction*

CH is selected in the LEACH process depends on the energy value, which has a threshold dependency. Understanding the network's clustering pattern is the aim of the initial inquiry. The attacker then launches an attack employing a group of nodes, like a sinkhole attack on a network using LEACH routing. By examining the parameters, particularly the number of clusters (nC) and cluster members (SNi), values are projected. The CHs at various locations are believed to be compromised by the values during the attack process. Due of routing assaults' impact on the WSN, the hackers employ two additional attack paths.

➢ *Launching of Sinkhole Attack*

This attack aims to compromise (nC) nodes that are accessible throughout the network, each compromised node being a member of the cluster. As a result, the compromised nodes take control of the regular sensor nodes and project their energy readings as being higher than the necessary level

to become CHs. Each infected CH or sinkhole node can drop or modify the packets to complete the security breach since the compromised CHs receive data packets from the regular nodes during the steady state period.

In the latter launch, a compromised sinkhole attack was used to modify the network's cluster members' data. Instead of compromising the (nC) cluster for each round of the selection process, CH is compromised in order to initiate the sinkhole attack. In this case, it would be malevolent for one CH to operate as a sinkhole. Although there is a minimal performance cost for each data transport, the exploited sinkhole assault extends the harmful activity. As a result, it has been acknowledged as a difficult challenge.

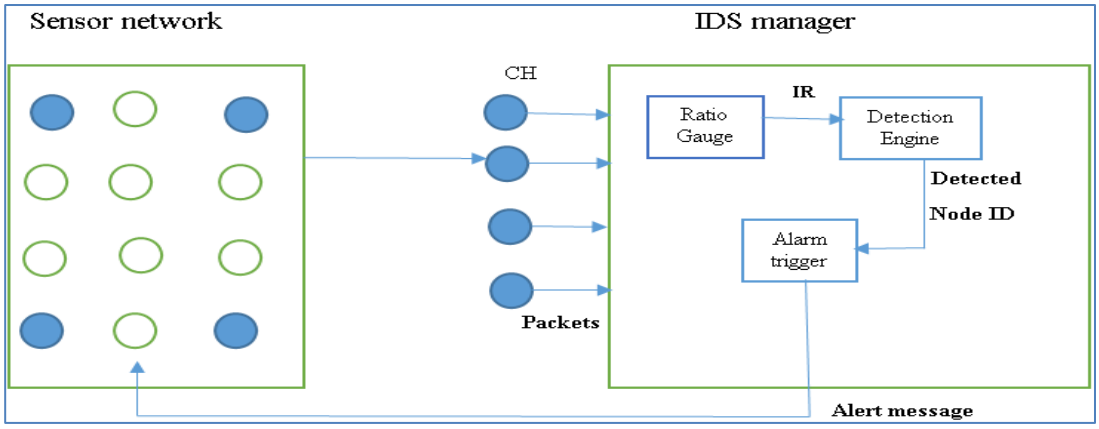


Fig. 10: Anomaly based IDS architecture

The suggested IDS anomaly-based approach assumes that the sinkhole nodes, which are infected nodes, will arbitrarily or selectively discard packets that originate from the reliable sensor nodes. After the CH gathers the data from the cluster member, the BS reviews it. By listening to the transmissions of the cluster nodes and CH nodes, the IDS agent running in the BS gathers the packets. The IDS agent's ratio gauge module uses data taken from the network to calculate the intrusion ratio (IR). The packet received, packet transmitted, and CH node IDs (Ni) values are used to calculate the IR. The value of IR transmitted to the detecting engine through the ratio gauge to check the availability of a compromised node to initiate the warning. The following is a list of the algorithm used.

Begin

Sn is the sensor network

PTi be the total packets transmitted by the i^{th} CH in Sn

PRi is the total packets received by the i^{th} CH in Sn

Ni is the Cluster Head Node ID

IR is the Intrusion Ratio for the i^{th} CH

Repeat

Time delay (100)

For $\forall$ (Ci) Receive (PRi, PTi and Ni) packets from the CHs'

Calculate IR where IR = PRi/PTi

If IR tends to ∞, then

Corresponding Ni is the sinkhole node

Isolate Ni

Send warning message to the remaining cluster member nodes about Ni

Else

Corresponding Ni is the normal CH

End if

End for

Fig. 11: IDS Proposed Algorithm

The BS's IDS agent module continuously scans data packets made up of PRi, PTi, and Ni for intrusions in accordance with the aforementioned IDS algorithm. The intrusion ratio (IR) is checked by the IDS agent using the CH node identifier Ni, CH packet transmission value PTi, and CH packet reception value PRi. If the ratio of PRi to PTi contains a number, it means that a portion of the packet was kept to ensure that "the malicious activity is not existing." The matched CH is a sinkhole node that has completely rejected all data packets that might have otherwise led to a black hole attack had (IR = infinite).

However, it might be able to launch a targeted forwarding assault if PRi and PTi values significantly diverge. The aforementioned technique aims to lower the intrusion ratio in order for the intruder node to be separated in the following data transmission cycle and blocked from the CH selection procedure by the BS.

The proposed IDS approach notifies each cluster member in turn to stop further data transfer. The network's energy efficiency is greatly enhanced by this approach. It is easy to calculate the ratio gauge, which speeds up the computation and lowers the computational complexity. Less communication is required between the BS and sensor networks when using the suggested IDS approach. Despite the sensor network's growing node density, the suggested IDS system efficiently alerts the threat deduction.

➢ *Intrusion Detection Mathematical Model*

An easy-to-build mathematical model was used to examine the efficiency of the IDS approach. Numerous sensor nodes that are dispersed unevenly throughout the network make up the sensor network (Sn). Let Sn consist of SN1, SN2, up to SN30 sensor nodes. Let Ci stand in for the cluster that comprise the sensors. The Ni is a unique cluster of the CH of Ci. The sensor nodes integrate with the cluster during the setup phase after the CHs have been selected, depending on the transmission range.

In order to calculate the values for packets received(PRi) and packets transmitted (PTi) for a certain CHCH (Ni), the BS keeps track of the transmission of the cluster members and the CH.

The following equation is used to mathematically represent the ratio of intrusion (IR):

$$IR = \frac{\text{PRi}}{\text{PTi}} \quad (2)$$

For the detection of sinkhole attacks, the IR value can take one of two possible values: *n* or *infinite*. Based on the value of IR, the IDS agent assesses if a CH is malicious or not. In the case where the IR value is a number *(n)*, the packets are not entirely destroyed. If PTi = 0, which indicates the existence of evil activity, is true, then the IR value is infinite (∞). The values of the IR are shown by the equation below:

$$IR = \begin{cases} n \rightarrow Ni \text{ is a normal node}, \forall \text{n } \in integer \\ \infty \rightarrow \text{Ni is a sinkhole node} \end{cases} \quad (3)$$

J. Intrusion Ratio calculations

➢ *Cluster C1*

The intrusion ration (IR) is determined using the following formula for the CH $(N1)$ in the cluster$C1$:

$$IR1 = \frac{PR1}{PT1} \quad (4)$$

Sinkhole attack in cluster C1 of the IPRC-Huye campus was checked in consideration of two situations such as under attack and no attack.

- **Under sinkhole attack.** We have four cluster members in cluster C1of the network such as $SN1$, $SN2, SN3$, and $SN4$ and one cluster head $CH\,N1$ as well as a few representative input values.

Let the $CH\,N1's\,PR1$ value be 80 and its $PT1$ value be 0(no packets transmitted). Then, equation (4) calculates the IR value of the $CH\,N1$ as follows:

$$IR1 = \frac{80}{0} \quad (5)$$

$IR1$ = *Infinite*

This indicates that the $CH\,N1$ is a sinkhole node because it loses all 80 packets. This can be explained using the MATLAB simulation graph below.

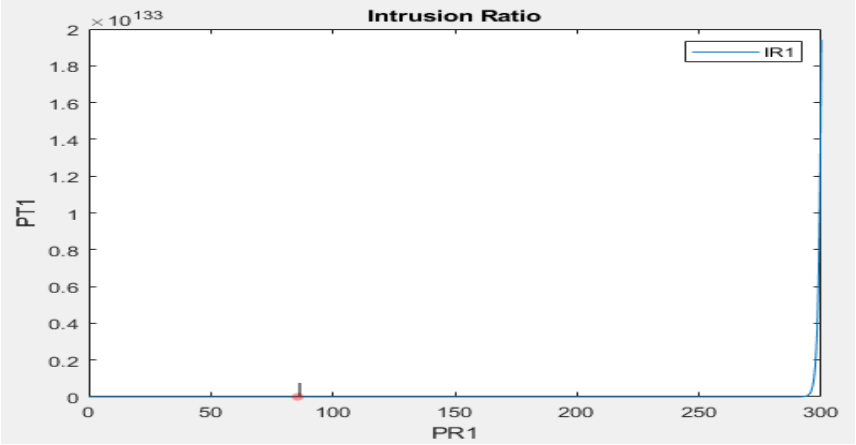


Fig. 12: Sinkhole attack on Cluster Head 1

ISSN No:-2456-2165

As the graph 20 above showing, PR1value which is 80 was received from sensor nodes to the cluster head on cluster one, but the cluster head one did not transmit any transmitted data. This means that all received packets were lost. In this situation, there was a sinkhole attack on the wireless sensor network of IPRC-Huye campus.

- **No sinkhole attacks.** Take into account a $CH\ N1$and $SN1$, $SN2$, $SN3$, and $SN4$.

Let the $CH\ N1's\ PR1$ value be 80 and its $PT1$ value be 76. The $CH\ N1's\ IR$ value is :

$$IR1 = \frac{80}{76}$$

$$IR1 = 1.05$$

For no sinkhole attack, the value of the ratio of intrusion is a numerical value. This means that the cluster head is a regular one since it forwards packets. The figure below shows the obtained results using MATLAB simulation in case there is no sinkhole attack.

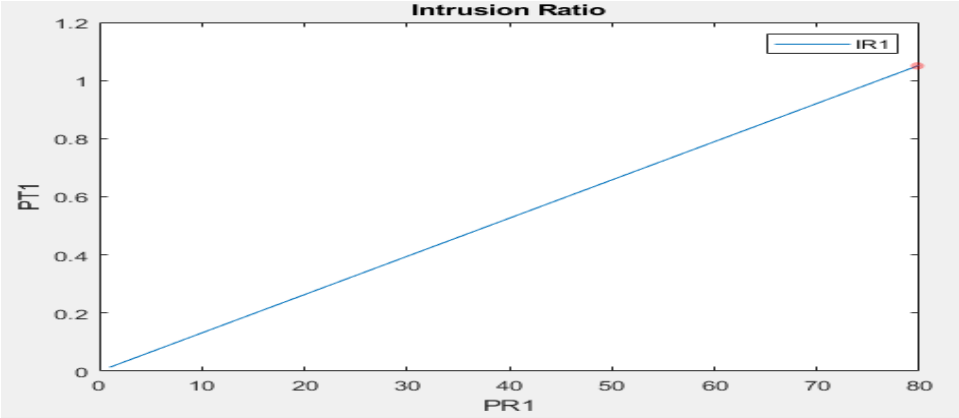


Fig. 13: No Sinkhole attack on Cluster Head 1

Referring to the figure 13, PR1value which is 80 was received from sensor nodes to the cluster head on cluster one, and the cluster head retransmit data to the base station (sink node). This means that all or many received packets were retransmitted to the sink node. In this situation, there was no sinkhole attack on the cluster one of wireless sensor network of IPRC-Huye campus.

➢ *Cluster C2*

The intrusion ration (IR) was calculated using the following formula for the $CH\ (N2)$ in the cluster $C2$:

$$IR2 = \frac{PR2}{PT2} \qquad (6)$$

Sinkhole attack in cluster C2 of the IPRC-Huye campus was checked in consideration of two situations such as under attack and no attack.

- **Under sinkhole attack.** We have four cluster members in cluster C2 of the network such as $SN1$, $SN2$, $SN3$, and $SN4$ and one cluster head $CH\ N2$ as well as a few representative input values.

Let the $CH\ N2's\ PR2$ value be 50 and its $PT2$ value be 0. Equation (6) calculates the IR value of the $CH\ N2$ as:

$$IR2 = \frac{50}{0} \qquad (7)$$

$$IR2 = Infinite$$

This indicates that the $CH\ N2$ is a sinkhole node because it loses all 50 packets. The simulation results of intrusion ratio in the cluster two of wireless sensor network of IPRC-Huye campus are presented in the figure below.

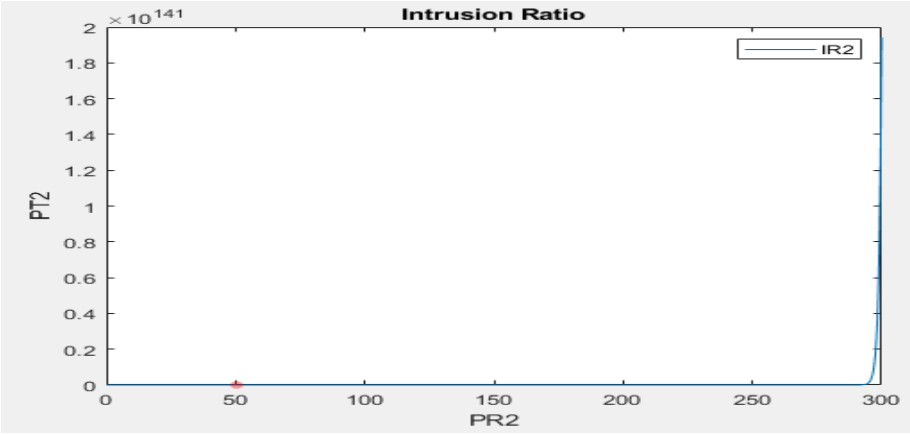


Fig. 14: Sinkhole attack on Cluster head 2

As the above graph shows, PR2 value which is 50 was received from sensor nodes to the cluster head of cluster one, but the cluster head one did not retransmit any transmitted data to the base station. This means that all received packets were lost. In this situation, there was a sinkhole attack on the cluster head 2 of wireless sensor network of IPRC-Huye campus.

- **No sinkhole attacks.** Take into account a $CH\ N2$ and 4 cluster members $SN1$, $SN2$, $SN3$, and $SN4$.

Let the $CH\ N2's\ PR2$ value be 50 and its $PT2$ value be 49. The $CH\ N2's\ IR$ value is:

$$IR2 = \frac{50}{49}$$

$$IR2 = 1.02$$

The intrusion ratio is a number for situations without a sinkhole assault. Thus, since it forwards packets, the cluster head is a typical node. Below are the simulation findings.

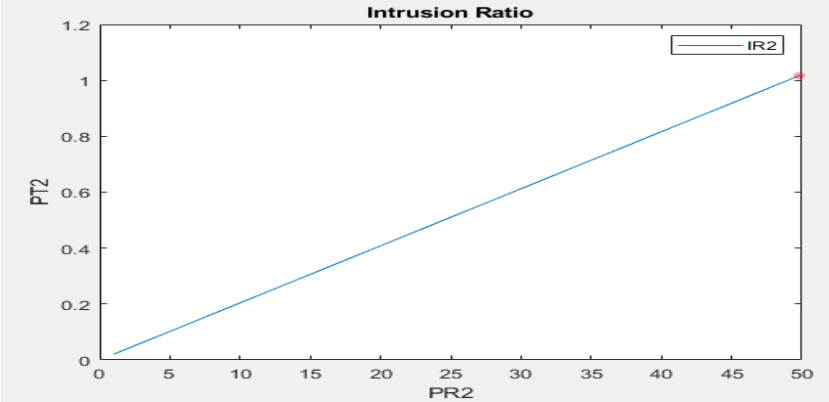


Fig. 15: No Sinkhole attack on Cluster head 2

According to the simulation's output in Figure 23, sensor nodes on Cluster 2 transmitted a PR2 value of 50 to the cluster head, who then retransmitted the information to the base station (sink node). This indicates that many or all of the packets that were received were sent back to the sink node. There was no sinkhole assault on the IPRC-Huye campus' wireless sensor network's cluster one in this instance.

➢ *Cluster C3*

We calculated the intrusion ratio (IR) using the following formula for the $CH\ (N3)$ in the cluster $C3$:

$$IR3 = \frac{PR3}{PT3} \quad (8)$$

Sinkhole attack in cluster C3 of the IPRC-Huye campus was checked in consideration of two situations such as under attack and no attack.

- **Under sinkhole attack.** We have four cluster members in cluster C3 of the network such as $SN1$, $SN2$, $SN3$, and $SN4$ and one cluster head $CH\ N3$ as well as a few representative input values.

Let the $CH\ N3's\ PR3$ value be 235 and its $PT3$ value be 0. Equation (8) calculates the IR value of the $CH\ N3$ as:

$$IR3 = \frac{235}{0} \quad (9)$$

$$IR3 = Infinite$$

This indicates that the $CH\ N3$ is a sinkhole node because it loses all 235 received packets. The figure below shows the simulation findings for the intrusion ratio in cluster two of the IPRC-Huye campus' wireless sensor network.

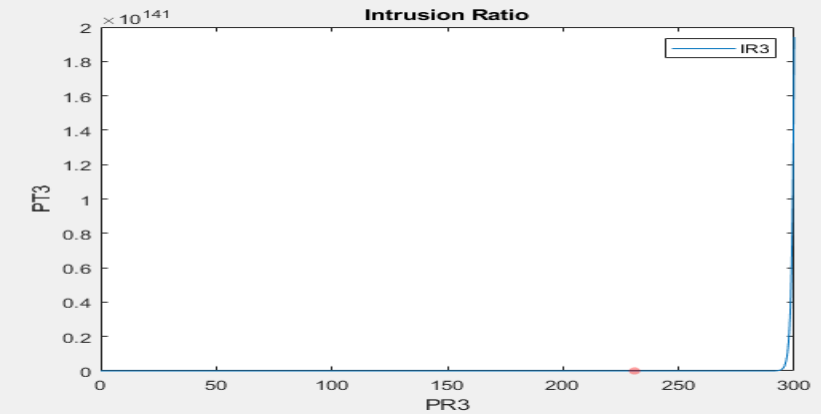


Fig. 16: Sinkhole attack on Cluster Head 3

As shown in the graph above, sensor nodes communicated a PR3 value of 235 to cluster head 1 of cluster 1, but the cluster head 1 did not retransmit any of the transmitted data to the base station. This implies that every packet that was received was lost. In this instance, the cluster head 3 of the IPRC-Huye campus' wireless sensor network was attacked by a sinkhole.

- **No sinkhole attacks.** Take into account a $CH\ N3$ and 4 cluster members $SN1$, $SN2$, $SN3$, and $SN4$.

Let the $CH\ N3's\ PR3$ value be 235 and its $PT3$ value be 220. The $CH\ N3's\ IR$ value is:

$$IR3 = \frac{235}{220}$$

$$IR3 = 1.06$$

For no sinkhole attack, the intrusion ratio is a numerical value. This means that the cluster head is a regular one since it forwards packets.

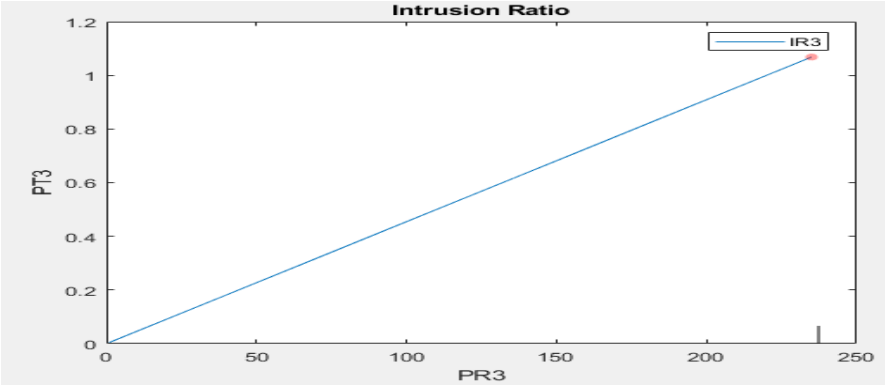


Fig. 17: No Sinkhole attack on Cluster Head 3

The simulation's output is shown in Figure 17, where sensor nodes on Cluster 3 sent the cluster head a PR3 value of 235, who subsequently sent the data back to the base station (sink node). This suggests that the most, if not all, of the received packets were forwarded to the sink node. In this case, the wireless sensor network cluster one of the IPRC-Huye campus was not attacked by a sinkhole.

All of the CHs in the network go through the same IR estimate process. Due to network link issues, there is some minor packet loss. The ratio gauge within the IDS agent gathers local data to determine the IR value, so the suggested IDS detects and prevents the sinkhole attack efficiently based on the values of intrusion ratio calculated by a base station.

V. CONCLUSIONS OF THE STUDY

In conclusion, the primary goal of this project was to develop an intrusion detection system algorithm for preventing sinkhole attacks on Wireless Sensor Network's LEACH protocol. As presented in previous chapter, we designed, developed an intrusion detection algorithm that mitigates a sinkhole attack in WSN of IPRC-Huye campus. We finally conclude that the existed intrusion detection algorithms are not efficiency to detect a sinkhole in the network. And also, by conclusion, the designed intrusion detection algorithm detects and prevents sinkhole attack in the wireless sensor network of the IPRC-Huye campus.

VI. RECOMMENDATIONS

A. IPRC-Huye Campus

As the designed intrusion detection algorithm detects sinkhole attack in the network, I would like to recommend IPRC-Huye Campus to implement the algorithm in the wireless sensor network to avoid the loss of data transmitted and fraudulent.

B. Future Researches

This research study was conducted only in IPRC-Huye campus. Other researchers should further study on other remaining campuses available in Rwanda. They could also work on other organizations that have wireless sensor networks.

REFERENCES

[1.] Admavathi, G. (2009). Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks . *International Journal of Computer Science and Information Security*.

[2.] Adwok, J. (2015). Probability Sampling - A Guideline for Quantitative Health Care Research. *Te ANNALS of AFRICAN SURGERY* , 95.

[3.] Agrawal. (2008). Intrusion detection in homogeneous and heterogeneous wireless sensor networks . *IEEE Transactions on Mobile Computing*.

[4.] Ajala. (2018). Abbreviations and Acronyms," Eur. Muslims their Foreign Policy Interest.

[5.] Aley. (2014). A Review On Intrusion Detection Schemes In Wireless Sensor Network.

[6.] Ali, M. (2020). Addressing Sinkhole Attacks In Wireless Sensor Networks - A Review . *International Journal of Science&Technology*.

[7.] Almomani, I. (2020). Integrating Software Engineering Processes in the Development of Efficient Intrusion Detection Systems in Wireless Sensor Networks. *Multidisciplinary Digital Published Institute*.

[8.] Antony Arthur, Beverley Hancock. (2009). *Introduction to the Research Process.*

[9.] Anzola, J. (2018). A Clustering WSN Routing Protocol Based on k-d Tree Algorithm. *Multidisciplinary Digital Publishing Institute*.

[10.] Arumugam. (2018). Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks. *Journal of Sensors*.
[11.] Asher. (1984). Theory-building and data analysis in the social sciences.
[12.] B. Zhanga, L. D. (2014). Sinkhole attack detection based on redundancy mechanism in wireless sensor networks.
[13.] Bagci, F. (2016). Energy-efficient communication protocol for wireless sensor network.
[14.] Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. *IEEE Transactions on Wireless Communications*.
[15.] Banerjee, A. (2009). Anomaly Detection: A Survey, ACM Computing Surveys. *University of Minnesota*.
[16.] Byungura, J. C. (2015). E-learning management system for thesis process support from a supervisor perspective: The case of SciPro System at University of Rwanda.
[17.] Chandala, V. (2009). Anomaly Detection: A Survey, ACM Computing Surveys. *University of Minnesota*.
[18.] Chen, C. (2010). "Intrusion detection of sinkhole attacks in large-scale wireless sensor networks. *IEEE international conference on wireless communications, networking and information security (WCNIS)*.
[19.] Chidiebere, O. (2017). Introduction to MATLAB for Researchers and Engineering Students. *Journal of Scientific and Engineering Research*.
[20.] Cukier, M. (2009). Evaluating Attack Resiliency for Host Intrusion Detection Systems. *Information Assurance and Security Journal*.
[21.] D'Antonio. (2010). An intrusion detection system for critical information infrastructures using WSN . *In Critical Infrastructure (CRIS), 2010 5th International* .
[22.] Denscombe. (2010). The Good Research Guide: for Small-scale Social Research.
[23.] Deri, L. (2002). Design and Implementation of an Anomaly Detection System: an Empirical Approach. *University of Pisa, Italy*.
[24.] Dewal. (2015). Security Attacks in Wireless Sensor Networks: A Survey. In Cyber Security.
[25.] Dimitriou, T. (2008). Intrusion Detection Sinkhole Attacks in Wireless Sensor Network In Networking and Communications. *IEEE International Conference on Wireless and Mobile Computing*.
[26.] ElDow, A. (2021). A Combined Model for Continuous Intention to Use E-Learning System. *International Journal of Interactive Mobile Technologies (iJIM)* .
[27.] Fessant, F. L. (2010). A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis. *Computer Communications*.
[28.] Ghassemi, F. (2017). An adaptive sinkhole aware algorithm in wireless sensor networks .
[29.] Guechari, M. (2012). Dynamic solution for detecting Denial of Service attacks. *IEEE International Conference on Communications*.
[30.] Gupta. (2018). Modified and Efficient LEACH Protocol for Hybrid Clustering Scenario in Wireless Sensor Networks.
[31.] Hussain. (2017). A Survey on Security Challenges in Wireless Sensor Networks.
[32.] Ilker Etikan, S. A. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*.
[33.] Irmak, E. (2017). A hybrid trust based intrusion detection system for wireless sensor networks . *International Symposium on Networks, Computers and Communications (ISNCC)*.
[34.] Jadidoleslamy, H. (2011). A High-Level Architecture for Intrusion Detection on Heterogeneous Wireless Sensor Networks: Hierarchical, Scalable and Dynamic Reconfigurable. *Scientific Research*.
[35.] Jibreel, F. (2022). An Enhanced Heterogeneous Gateway-Based Energy-Aware Multi-Hop Routing Protocol for Wireless Sensor Networks. *Multidisciplinary Digital Publishing Institute*.
[36.] Jokhio. (2013). Light-Weight Framework For Security-Sensitive Wireless Sensor Networks Applications.
[37.] Jubair, A. M. (2021). Optimization of Clustering in Wireless Sensor Networks: Techniques and Protocols. *Applied Sciences*.
[38.] Karlof, C. (2003). Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications*.
[39.] Khonsari. (2014). Detection and Mitigation of Sinkhole attacks in wireless sensor networks . *Journal of Computer and System Science*.
[40.] Kirshenblatt. (2006). Part 1, "What Is Research Design. The Context of Design." Performance Studies Methods Course syllabus. New York University, spring.
[41.] Koffka Khan. (2012). Security in Wireless Sensor Networks. *Double Blind Peer Reviewed International Research Journal*.
[42.] Kothari, C. (2004). *Research Methodology, Methods & Techniques(SECOND REVISED EDITION)*. Jaipur(India): NEW AGE INTERNATIONAL(P) LIMITED PUBLISHER.
[43.] Kristin. (2021). Statistical and qualitative data analysis software. .
[44.] Krontiris. (2008). *Intrusion Prevention and Detection in Wireless Sensor Networks.*
[45.] Krontiris, I. (2008). *Intrusion Prevention and Detection in Wireless Sensor Networks.*
[46.] Krügel, C. (2000). A Survey on Intrusion Detection Systems. *TU Vienna, Austria*.
[47.] Kumar, S. (2017). Analysis of sinkhole attack in leach based wireless sensor network. *International Journal of Pure and Applied Mathematics*.
[48.] Lamba, S. (2020). How to Detect and Mitigate Sinkhole Attack in Wireless Sensor Network . *International Journal of Engineering Research & Technology (IJERT)*.
[49.] Lee. (2000). Foundations of behavioural research.
[50.] Li, C. (2010). Security of Wireless Sensor Networks: Current Status and Key Issues, in Smart Wireless Sensor Networks.

[51.] M.Thala. (2017). Analysis on sinkhole attack in LEACH based Wireless Sensor Network. *International Journal of Pure and Applied Mathematics*.
[52.] McCombes. (2020). An introduction to sampling methods. .
[53.] Mell, P. (2007). Guide to Intrusion Detection and Prevention Systems (IDPS). *NIST*.
[54.] Mentzas, G. (2001). Modelling business processes with workflow systems: an evaluation of. *International Journal of Information Management, 21(2)*, 123-135.
[55.] Murphy, M. (2016). *Population definitions for comparative surveys in education.* Australia.
[56.] narim, E. (2005). An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse Detection in Computer Networks. *Expert Systems with Applications*.
[57.] Ndiaye, M. (2017). Software Defined Networking for Improved Wireless Sensor Network Management: A survey .
[58.] Novak, J. (2002). Network Intrusion Detection: An Analyst's Handbook. *New Riders Publishing, Thousand Oaks,*.
[59.] Oliveira. (2007). The Security Of Clustered Sensor Networks.
[60.] Optimization of Clustering in Wireless Sensor Networks: Techniques and Protocols. (2021). *Applied Sciences*.
[61.] Oteafy. (2014). Evolution of Wireless Sensor Networks,‖ in Dynamic Wireless Sensor Networks.
[62.] Oudani, H. (2018). LEACH and PGASIS Protocols in wireless sensor network: Study and Simulation. *European Journal of Advances in Engineering and Technology*.
[63.] Padmavathi, G. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *International Journal of Computer Science and Information Security*.
[64.] Panda, J. (2023). Localization and Detection of Multiple Attacks in Wireless Sensor Networks Using Artificial Neural Network. *Wireless Communications and Mobile Computing*.
[65.] Perrig, A. (2004). The Sybil Attack in Sensor Networks: Analysis & Defenses.
[66.] Poza-Lujan, J. (2019). Distributed Architecture to Integrate Sensor Information: Object Recognition for Smart Cities.
[67.] Qiang. (2009). A Routing Protocol Combining Multi-Hop Transmissions And Single-Hop Transmissions. *In Proceedings of the 2009 Pacific-Asia Conference on Circuits Communications and Systems*.
[68.] Rafeh, R. (2013). A novel agent-based approach to detect sinkhole attacks in wireless sensor networks.
[69.] Ranjeeth. (2015). Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks. *Journal of Sensors*.
[70.] Reddy, C. (2019). An Empirical Study on Support Vector Machines for Intrusion Detection. *International Journal of Emerging Trends in Engineering Research*.
[71.] Rehman, A. (2019). Sinkhole Attacks in Wireless Sensor Networks: A Survey.
[72.] Reza. (2015). Optimizing LEACH clustering algorithm with mobile sink and rendezvous nodes.
[73.] Saini, S. (2013). Simulation of low energy adaptive clustering hierarchy protocol for wireless sensor network. *International Journal of Advanced Research in Computer Science and Software Engineering.*
[74.] Sengul, C. (2009). Cryptographic protocols to fight sinkhole attacks on tree based routing in WSN. .
[75.] Sharma, S. (2011). A survey on secure hierarchical routing protocols in wireless sensor networks. *In Proceedings of the International Conference on Communication, Computing and Security*.
[76.] Sharmila, S. (2011). Detection of sinkhole attack in wireless sensor networks using message digest algorithms. *International conference on process automation, control and computing*.
[77.] Sheela, D. (2011). A non-cryptographic method of sinkhole attack detection in wireless sensor networks. *International conference on recent trends in information technology* .
[78.] Shin, S. (2010). An Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial Sensor Networks. *IEEE Transactions on Industrial Informatics*.
[79.] Singh, A. S. (2014). SAMPLING TECHNIQUES & DETERMINATION OF SAMPLE SIZE IN APPLIED STATISTICS RESEARCH: AN OVERVIEW. *International Journal of Economics, Commerce and Management*, 14.
[80.] Singh, S. (2008). Countering Sinkhole and Blackhole Attacks on Sensor Networks using Dynamic Trust Management. *In Computers and Communications.*
[81.] Suin, S. (2002). Design and Implementation of an Anomaly Detection System: an Empirical Approach. *University of Pisa, Italy*.
[82.] Tiwari, V. (2021). Challenges in Sinkhole Attack Detection in Wireless Sensor Network. *Indian Journal of Data Communication and Networking (IJDCN)*.
[83.] Vigna, G. (2002). Intrusion Detection: A Brief History and Overview. *Computer Society*.
[84.] Wagner. (2003). Secure routing in wireless sensor networks: attacks and countermeasures," Ad Hoc Networks".
[85.] Wang, Y. (2013). Gaussian versus uniform distribution for intrusion detection in wireless sensor networks. *IEEE Transactions on Parallel and Distributed Systems*.
[86.] Waoo, A. A. (2021). Challenges in Sinkhole Attack Detection in Wireless Sensor Network. *Indian Journal of Data Communication and Networking (IJDCN)*.
[87.] Wazid. (2017). *Design and Analysis of Intrusion Detection Protocols for Hierarchical Wireless Sensor Networks.*
[88.] Wittaya, T. (2009). Detection of Sinkhole Attack in Wireless Sensor Networks .
[89.] Yang, S. (2019). Research on routing optimization of WSNs based on improved LEACH protocol. *Journal on Wireless Communications and Networking*.

[90.] Yu, Y. (2014). Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications*.
[91.] Zanero, S. (2004). *Unsupervised Learning Techniques for an Intrusion Detection System.* New York.
[92.] Zheng, J. (2009). Introduction to Wireless Sensor Networks,‖ in Wireless Sensor Networks.