EARLY WARNING AND PREDICTION OF MALICIOUS NODE AND INTERNAL ATTACKS ON WIRELESS SENSOR NETWORK

J COMPONENT PROJECT REPORT

SLOT A1

Submitted by

SATHWIK GUNUGANTI
gunuganti.sathwik2019@vitstudent.ac.in
19BCT0055

YASH SHARMA
yash.sharma2019a@vitstudent.ac.in
19BCT0195

HARSH AGARWAL
harsh.agarwal2019@vitstudent.ac.in
19BCT0206

AKASH GOYAL
akash.goyal2019@vitstudent.ac.in
19BCT0222

Course Code: BCT3001

Course Title: Internet of Things

Under the guidance of

S. Ananda Kumar

B.Tech

in

Computer Science and Engineering

VIT –Vellore Institute of Technology

VIT®
Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

TABLE OF CONTENTS

1. Abstract:

As we as a whole realize that the innovation is projected to be close to people very soon in light of its comprehensive development. Presently a-days, we see a ton of utilizations that are making our lives agreeable like savvy vehicles, shrewd homes, brilliant traffic the executives, brilliant workplaces, shrewd clinical conference, shrewd urban communities, and so on

All such offices are in the scope of an average person in view of the headway in Information and Communications Technology (ICT). In view of this headway, new figuring and correspondence conditions like the Internet of Things (IoT) came into picture. Part of exploration work is in progress in the IoT area which helps for the general advancement of the general public and makes the lives simple and agreeable. In any case, in the asset compelled climate of Wireless Sensor Network (WSN) and IoT, it is practically incomprehensible to set up a completely solid framework. As we are pushing ahead extremely quickly, innovation is turning out to be increasingly more helpless against the security dangers. Later on, the quantity of Internet associated individuals will be not exactly the savvy protests so we really want to set up a vigorous framework for keeping the previously mentioned conditions safe and normalize it for the smooth conduction of correspondence among IoT objects.

Malignant assaults like refusal of-administration greatly influence the organization exercises of remote sensor organizations. These assaults exploit network layer weaknesses and influence every one of the layers of the organization. Inconsistency based interruption identification framework (AIDS) is intended for checking such erratic assaults yet it creates high bogus up-sides. In the proposed concentrate we plan powerful and productive AIDS which utilize fluffy and neural organization (NN) based instruments. The proposed framework can be executed in every hub as it is lightweight and doesn't burn-through much overhead. Likewise it can autonomously screen the nearby hub's conduct and distinguish whether a hub is trust, doubt or adversary. The utilization of a prepared NN channels the bogus alerts produced because of fluffy rationale applied in the initial step in this way improving the framework precision.

Cybercriminals increase their endeavors with complex procedures while protectors bit by bit update their normal safety efforts. Aggressors frequently have a drawn out interest in their objectives. Because of various factors like scale, engineering and ineffective traffic anyway it makes it hard to distinguish them utilizing run of the mill interruption identification methods. Digital early admonition frameworks (CEWS) target cautioning such endeavors in their incipient stages utilizing fundamental markers. Plan and execution of such frameworks includes various examination difficulties like nonexclusive arrangement of pointers, knowledge gathering, vulnerability thinking and data combination.

Keywords: Residual Energy - Wireless Sensor Network - NS2 - Intrusion Detection System - Attacks - Man in the middle - Black hole attack

2. Introduction:

These days, remote sensor organizations (WSNs) have become perhaps the most helpful innovations and have drawn increasingly more consideration from researchers . Inferable from the capacities of information procurement, handling, and transmission, the sensor hubs can be conveyed in numerous application situations, like ecological checking, war zone discovery, modern wellbeing observing and medical care, and so forth Be that as it may, because of the automated climate and the attributes of energy-obliged, the sensors are powerless against different assaults.

By catching some typical hubs, the aggressors can change their conduct and afterward embed bogus information or choices to delude the decision-production of the entire organization. Likewise, the sensor hubs might be issue inclined to non-pernicious mistakes, like deficient lingering energy and deficiencies of remote handsets or parts.

Remote sensor networks are made out of a few sensors conveyed in regions where the point is to gather information and forward it for the investigation. It has turned into an undeniably fascinating field of examination with regards to taking care of such testing certifiable issues, like natural observing , military applications, topographical detecting, traffic signal, and home computerization.

Remote Sensor Networks (WSNs) establish quite possibly the most encouraging third-thousand years technology and have a wide scope of utilizations in our general climate.

WSNs have begun to converge with the Internet of Things (IoT) through the presentation of Internet access capacity in sensor hubs and detecting capacity in Internet-associated gadgets. Accordingly, the IoT is giving admittance to tremendous measures of information.

Various insightful sensors with fundamental computational and remote correspondence abilities are as of now installed into different gadgets and instruments around the world. Since their number is developing quickly, it very well may be normal that remote sensor hubs will endlessly dwarf ordinary PCs and other organized gadgets sooner rather than later. Remote sensor organizations (WSNs) were the subject of escalated innovative work during the last decade [1–3]. Because of severe asset limitations (both power and computational) the execution of ordinary Internet convention engineering in WSNs used to be stayed away from the outset, bringing about various non interoperable arrangements. Further improvement of WSNs normally prompted endeavors to interconnect and coordinate a WSN with traditional IP organizations. These endeavors brought about specific systems and transformation norms that empower the utilization of the IP in a WSN climate.

3.1 Literature Review:

The author had proposed an efficient security methodology by the implementation of Hamming residue method. For simplicity, Hamming code as (7, 4) had been chosen along with the quadratic residues of 7 to improvise the security. However, one can choose any Hamming code and residues based on the network requirements[1]. The entire technique is stored in IPV6 packet header such that all the non-malicious nodes will produce the security code within the specified time to live (TTL). However, it will take more time than TTL for malicious nodes to analyze the security code generation technique. Hence, this method can easily detect the rival node, improving the packet delivery ratio (PDR) and reducing the delay in the network. This method provides the security to WSNs against the malicious attacks without any key distribution mechanism.[2]

In digital communication, Hamming codes are used to detect and correct the errors; as a result, all the communication systems are aware of these codes. WSNs are autonomous and require less energy consumption, and such codes can be used to secure WSN system without any additional infrastructure.[1] In the presented approach by the author, initial security bits (users define) are used and a set of additional security check bits is appended to it for generating the security codeword. Depending on the security codeword length “n” and a number of initial security bits “k,” Hamming codes (n, k) (such as (6, 3) and (7, 4) codes) can be used or many more.

The presented approach is validated by simulating the results using Network Simulator 2 (NS2) and comparing this approach with the approach that already exists. Different parameters were considered for simulation such as Node count, Simulation period, Layer, Antenna used, Type of queue, MAC protocol, etc.[3] The node count is taken between the range of 2 and 150; however, by the use of Hamming code (7, 4), the maximum number of nodes possible is 15. It is observed that overhead of the proposed approach is less when compared with the other two approaches used for comparison, the proposed approach has a significant effect on the data transfer. The acceptable limits for video and audio packets are 150 ms and 400 ms respectively. The proposed approach is valid up to 15 hops as the example of (7, 4) Hamming code is presented. However, the number of hops can be increased by increasing their initial security bits length and security codeword length as per the Hamming code.[1]

The security of wireless sensor networks is improved by the Hamming residue technique. The presented approach is simple and very much effective if more number of rival nodes exists at different hops in the network.[3] As at each node, a new security codeword is generated, which makes the proposed method more efficient, enhances the confidentiality among the nodes, and can easily detect the rival node in the network. The presented approach also reduces the mathematical complexity which in turn increases the PDR by minimizing the delay.

The authors have proposed an efficient and secure malicious node detection model based on a hybrid clustering network for WSNs, which was based on the clustering process using one cluster head and mobile trusted nodes[2]. Firstly, the ESMCH model was described with all used algorithms then they analyzed the energy computation and security mechanism. The performance is calculated based on delay, packet delivery ratio, drop and throughput. ESMCH model is more secure against some attacks like Man-in-the-Middle Attack and Black hole Attack. By simulation results using NS2 the authors could prove that the ESMCH model is better in performance and security than these compared models (DCSDA, ECCDSA, and E2HRC) which could help in providing considerable security and reducing energy consumption to increase the network lifetime.[4]

The ESMCH model had been classified according to clustering head selection, the energy model and security mechanism. The network consists of one cluster head. Other nodes are sub-divided into sub-clusters. Each cluster in the network consists of some main nodes as cluster head node (CH), child nodes (CN) and mobile nodes (MN). The cluster head node suffers from transferring the data directly to the Super-cluster head (SCH) due to the distance. To address these issues, mobile sink nodes are introduced.[4] The mobile sink mode acts as an intermediate between the cluster head and Super-cluster head. Each cluster has one or more mobile sink nodes consistent with the number of child nodes located in the cluster head.

In this research, the ESMCH proposed two algorithms named as Intelligent based Secured Fuzzy Clustering algorithm (ISFC) and Balanced Load Sub-cluster head selection to decrease the distance between the nodes and reduce energy consumption.[3]

Balancing the load between sensor nodes is a great challenge for the long run operation of wireless sensor networks. When a sensor node becomes overloaded, the prospect of higher latency, energy loss, and congestion becomes high.[4] The balanced load cluster head selection aims at decreasing the energy consumption and increasing the network lifetime by introducing load balancing concept in it. If a few cluster nodes are heavily loaded, it leads to faster energy consumption and to get the normal depletion of energy. The balanced load cluster head selection is initiated. The distance between normal child nodes and cluster head plays a major part in energy consumption. So, balanced load cluster head selection leads to nominal energy depletion of each node is presented in the network by creating transmission with closer nodes by a balanced load among the cluster heads.[4]

The security services in WSN have to protect the data conveyed over the network and the assets from attacks and bad conduct of nodes.[4] In the proposed ESMCH model, the authors had sought to achieve the security and their security mechanism is based on using Elliptic curve cryptography. The user creates the secret keyKs. Since two keys are created in EECC which are private key (PRK) and public key (PUK). The secret key is undergoing XOR operation. In each transmission round, an encryption key is generated for every SN. The designed encryption key is of 176-bitto overcome the memory constraints of the sensor network. These techniques have led to better security in the proposed model.[6]

In the paper by Zinaida BENENSON[7] a,1 , Peter M. CHOLEWINSKI b , Felix C. FREILING the author presented a framework which provides concepts to clarify two important aspects of the security analysis in wireless sensor networks:

What should be protected? Here they offer a set of generic classes of requirements which can be used to structure and refine a set of concrete security requirements. They highlighted the main differences between security requirements in classical systems and security requirements in wireless sensor networks.[7]

Against what are we protecting the system? Here we offer a set of generic attacker models which can be used to choose and refine particular attacker models for individual systems.

Wireless Sensor networks provide unique opportunities of interaction between computer systems and their environment.[8]Considering the Internet as an example, it is extremely difficult to add security to systems which were originally designed without security in mind.

The structure given is as follows:

They first give an overview of security goals in sensor networks, i.e., they approach the question “what to protect”.

Then they created a report on experiments in attacking wireless sensor networks.

Building on these experiences they developed a generic set of attacker models, i.e.they had approached the question “against whom to protect”.

Finally, they briefly discussed protection mechanisms i.e., they approached the question “how to protect”.

Thus, in order to design a WSN secure against those node capture attacks described in this research paper, the following steps should be applied: • Take standard precautions for protecting microcontrollers from unauthorized access;

• Choose a hardware platform appropriate for the desired security level, and keep up-to-date with new developments in embedded systems security; • Monitor sensor nodes for periods of long inactivity;

• Allow for revocation of the authentication tokens of suspicious nodes.

They had described security goals, adversary models and protection mechanisms which are relevant and specific for sensor networks. They also answered some of the interesting problems like

• Realistic adversary models should be derived with respect to existing and future applications. Here, experiences with GSM and WLAN security (and security failures) can be used as a guideline, but every application needs to define its own adversary model to be able to talk about security.

• As cross-layer integration is especially important for resource-constrained sensor nodes, careful design decisions must be taken concerning which security means to put into which layer.

So,overall they tried to convey that the security goals of sensor networks will be probabilistic and depend on the strength of the adversary.

In [4] by Waldir Ribeiro Pires J´unior Thiago H. de Paula Figueiredo Hao Chi Wong Antonio A.F. Loureiro the author provided a solution to identify malicious nodes in wireless sensor networks through detection of malicious message transmissions in a network.

A wireless sensor network (WSN) consists of a set of compact and automated devices called sensing nodes. A sensing node is a computational device that has memory, battery, processor, transceiver, and a sensing device.

Wireless sensor networks can collect data from the environment where they are embedded. The data are often first processed by the sensor nodes and then sent over non-secure channels to the sink node for further processing.

Under the model described in the given paper, any node can obtain two values on any transmission it hears.[8] The first value is the expected signal strength of the received signal, which can be computed using the transmission power that was agreed upon for message transmissions in the system and the distance between the node that hears the transmission and the source of the transmission itself. The second value is the actual signal strength detected at the listener's transceiver.

Here they developed a wireless sensor network simulator to create an environment to evaluate their work which is a discrete event simulator written in Java. A network generator was built, which generates networks comprised of n nodes plus one malicious node, all located in an S S square field.. Each node has randomized x and y coordinates. No two different nodes share the same coordinates. Networks with 50; 100; 150; : : : ; 500 nodes in 179 179 m2 fields were generated and used as input to the simulator. For each network with a given number of nodes, 200 network topologies were created. As all networks we consider are in a 179 179 m2 field, the density is measured in number of nodes.[9]

On the basis of the given model they also created graphs comparing-

(i) .Detection rate vs. network density

(ii) Detection rate vs. transmission power multiplier

(iii) Detection rate vs. maximum ratio difference

(iv) Detection rate vs. Message check probability

Their proposed scheme can be easily integrated into other protocols. It would interface with the rest of the system through an API that provides information about whether a node or a message is regarded as suspicious. The MNDSS protocol does not have heavy requirements in terms of the underlying hardware; low-precision devices can be used, as the scheme works well even for relatively high values of maximum ratio difference.[10]

Determination of a malicious node's location requires some degree of cooperation between nodes, so that they may together pinpoint the approximate location of the adversary.[11]

When a node receives a message and considers it as suspicious, it may coordinate with its neighbors to try to locate the origin of the message by using the signal strength detected by its own receiver and the signal strength received by other nodes.A minimum of three nodes should be sufficient in finding the approximate region where the adversary is located.

WSN suffers from several attacks, intrusion and security vulnerabilities. Intrusion detection system (IDS) is one of the essential security mechanism against attacks in WSN. Through this we present a comparative evaluation of the most performant detection techniques in IDS for WSNs, the analyzes and comparisons of the approaches are represented technically, followed by a brief. Attacks in WSN also are presented and classified into several criteria. To implement and measure the performance of detection techniques we prepare our dataset, based on KDD'99, into five steps, after normalizing our dataset, we determined normal class and 4 types of attacks, and used the most relevant attributes for the classification process. We propose applying CfsSubsetEval with BestFirst approach as an attribute selection algorithm for removing the redundant attributes. The experimental results show that the random forest methods provide high detection rate and reduce false alarm rate. Finally, a set of principles is concluded, which have to be satisfied in future research for implementing IDS in WSNs [5].

It has become clear that we cannot achieve the satisfactory level of security in WSN only by using cryptographic techniques, as these techniques fall prey to insider attacks. The attacker can compromise and retrieve the cryptographic material of a number of nodes . In order to counter this threat some additional techniques such as the intrusion detection system (IDS) has to be deployed [5].

There are two basic approaches in IDS according to the used detection techniques :

Misuse detection technique compares the observed behavior with known attack patterns (signatures). Action patterns that may pose a security threat have to be defined and stored in the system. The advantage of this technique is that it can accurately and efficiently detect instances of known attacks, but it lacks an ability to detect an unknown type of attack [5].

Anomaly detection: The detection is based on monitoring changes in behavior, rather than searching for some known attack signatures. Before the anomaly detection based system is deployed, it usually must be taught to recognize normal system activity (usually by automated training). The system then watches for activities that differ from the learned behavior by a statistically significant amount. The main disadvantage of this type of system is the high false positive rate. The system also assumes that there are no intruders during the learning phase [5].

The key challenge of evolving intrusion detection system in WSN is to identify attacks with high accuracy, and satisfied the required constraints and challenges, to prolong the lifetime of the entire network. This aims could be attained from several ways. Firstly paying much more attention to detection techniques used for attacks detection is characterized by efficiency and ability. Secondly, reconstructing detection mechanism with a distributed manner, to reducing the communication overhead [15].

Aggressors perform numerous continuous accursed Internet exercises, including subtle surveillance, low and slow filtering, and testing, to distinguish freedoms to infiltrate and dispatch takes advantage of.[9] These exercises can be subjective and arbitrary, as opposed to coordinated or vital. How could the "heroes" distinguish vital covert surveillance to recognize future assaults? Is it conceivable to recognize aggressors' aim and foresee their conduct, or are their exercises so undirected that they're indistinct from that of arbitrary examining worms? In this portion of On the Horizon, I depict a few parts of the Worminator project (http://worminator.cs.columbia.edu), a joint effort of scholarly foundations seeking after R&D of insightful prescient and proactive innovations that identify, report, and guard against early preattack cyberevents—explicitly network observables—that are antecedents to pernicious exercises during a later assault stage. The task expects to quantify and fundamentally build the admonition time for a zeroday assault (an assault against an unreported weakness) to give security experts and chiefs time to make preventive strides and for computerized versatile reaction instruments to reconfigure IT foundations to limit the effect and misfortunes. Worminator tends to two expansive regions: edge discovery and early admonition of potential worm spreads and forerunners to zero-day assault against a got site, and the effect on network anomalydetection frameworks to find potential new malignant assaults that have pierced the edge guards, including mechanizing the age of zero-day assault marks. The critical prerequisite for these pursuits is a dispersed arrangement of sensors that can precisely distinguish subtle surveillance exercises at network entryways' outside edges[6].

Nowadays, wireless sensor networks (WSNs) have become one of the most useful technologies and attracted more and more attention from researchers . Owing to the capabilities of data acquisition, processing, and transmission, the sensor nodes can be deployed in many application scenarios, such as environmental monitoring, battlefield detection, industrial safety monitoring and health care, etc. However, due to the unmanned environment and the characteristics of energy-constrained, the sensors are vulnerable to various attacks. By capturing some normal nodes, the attackers can change their behavior and then insert false data or decisions to mislead the decision-making of the whole network. In addition, the sensor nodes may be problem prone to non-malicious errors, such as inadequate residual energy and faults of wireless transceiver or components, and then, result in unreliable data generation [7].

Taking into account of energy consumption and secure routing, many studies combine the construction of trust model with the clustering management mechanism of nodes. Proposed a group-based trust management mechanism and applied it to clusterstructured wireless sensor networks. The calculation of trust value is achieved by monitoring the communication behavior between neighbor nodes, including member node’s trust, cluster head’s trust, cluster trust, and base station trust. The trust model can effectively resist malicious node attacks and protect malicious nodes from defamation and defamation attacks as well as keep energy-efficiency. Proposed a trust evaluation model based on the autonomous behavior of sensor nodes. Sensor nodes acquire direct or indirect trust values by monitoring the behavior of neighbor nodes. Cluster heads calculate comprehensive trust values according to D-S evidence theory. By trust evaluation, malicious nodes can be effectively identified and malicious nodes can be restricted to become cluster heads. designed a distributed trustbased cluster head election mechanism. The trust table was constructed by monitoring the transmission process of neighbor nodes, and the trust degree was calculated [7].

Multidimensional trust indicators are derived from communication between adjacent sensor nodes, and direct and indirect trust values will be estimated based on the corresponding behaviors of those sensor nodes. To improve the validity of trust quantification and ensure the objectivity of evaluation, the entropy weight method is applied to determine the proper value of the weight. In our future work, we will devote to evaluate the trust level of sensor nodes in clustered WSNs and combine the trust model with secure data fusion. Besides, some professional techniques, e.g., fuzzy logic or pattern recognition, will be employed and discussed to reduce the fuzziness of behavior evidences [7].

In Research Paper[8] by Muhammad R Ahmed, Xu Huang, and Dharmendra Sharma

WSN is a great development in communication technology in recet years.It requires minimal energy,weak coputation capabilities,wireless communication.But as there are many advantages it also ensures some limitations such as WSNs are vulnerable to many internal and external attacks.So we are going to implement some ideals and propose some models to prevent these attacks to happen for WSNs based on OSI model.However, the resource constrains in the sensor nodes of a WSN and multihop communications in open wireless channel make the security of WSN even more heavy challenge. Since sensor nodes can (or have to) also be deployed in the hostile environment without any temper resistant protection. The nodes deployed in a network are relatively easy to be compromised, which is the case that the nodes are out of the system control and an adversary can easily get full access to those nodes. Hence, all the data could be modified and restored in those targeted nodes, including the cryptographic keys. Thus, developing new security mechanisms are necessary as the nodes under traditional security mechanisms based on conventional authentication become inefficient and an adversary is able to lunch attacks with a legitimate status of the network [2]. The node is called compromised node when an attacker gain a control of the node and appears as a legitimate node, after a network deployment done.

A WSN has three major properties that made the security mechanism challenging.

a. Resource Constraints

b. Operational Environment, and

c. Wireless Multihop Communication.

All of the above mentioned attacks has the common purpose that is to compromise the integrity or workability of the network that they attack. In order to make the network function the network need to saved internally and externally. This work will give a understanding the internal attacks of WSN to the researchers.

Provisioning internal security is a significant task in WSN. In this paper we have presented a foundation of OSI layer based internal attacks of WSN. This will lead the researchers to develop the resilient security mechanism by considering internal attacks induced in WSN.

In paper by WEI SHE, QI LIU , ZHAO TIAN , JIAN-SEN CHEN , BO WANG , (Member, IEEE), AND WEI LIU

In wireless sensor networks, we consider dividing the nodes into bs,sn and sensor . The sensor monitors the indicators of the area in real time, collects monitoring data, understands the running status, and uploads the integrated data to the associated sn through the cellular link; sn collects all the monitoring data uploaded by the sensor in the transmission range, analyzes the running status of the sensor in real time, and collects the results to the bs center through the backhaul network[11]. As shown in the lower part, we map the operating framework of the wireless sensor network into the Consortium Blockchain. There are four main types of nodes in the Consortium Blockchain: contract issuing node, CA node, verification node and common nodes. bs is the contract publishing node, responsible for publishing intelligent contracts, as the issuer of activities. The sn serves as both CA node and verification node. CA node provides digital certificate-based identity information to members of the Consortium Blockchain community (Each sn and the sensor in the communication range is an alliance), and can generate or cancel a member's identity certificate. On the basis of clear membership, the organization can implement the management of authority control. The verification node is served by the pre-selected sn. It is mainly responsible for receiving the monitoring data collected by the common node, processing the smart contract, checking the legality of the transaction data, and updating and maintaining the node data and the account status in the blockchain organization. Among them, the smart contract is a piece of code that is deployed on the distributed ledger, which can control the received external information. In particular, the generation of each block is determined by all pre-selected nodes, and stored in Cmndb.

The sensor is a normal node and only uploads the collected monitoring data, regardless of the accounting process. [12]Therefore, based on their common characteristics, the overall structure of the wireless sensor network can be mapped into the Consortium Blockchain network, and then the detection of malicious nodes in the blockchain network. The blockchain trust model (BTM) for malicious node detection in WSNs is formalized as follows:

Malicious Node Detection Method in Smart Contracter:

Because the evaluation of malicious nodes is subjective and uncertain, in this paper it takes the state of node, processing delay, forwarding rate and response time as the evaluation indicators of malicious nodes to improve the credit degree of nodes. In order to better describe the state of the sensor node in the network environment, it is divided into working state and non-working state. If the sensor nodes are not working, we directly remove from the network; otherwise, collect the following three factors:

a: DELAYED TRANSMISSION (DT) FACTORS

b: FORWARDING RATE (FR) FACTOR

c: RESPONSE TIME (RT) FACTOR

WSN POSITIONING METHOD IN SMART CONTRACT:

Sensor location data is very important for WSNs in certain scenarios. When a disaster occurs (e.g. an earthquake, a forest fire, a natural gas leak), Wireless sensor network-based monitoring does not mean much if it only knows that a serious incident has occurred but does not know its specific location. Therefore, all sensor location information contained in the entire WSNs is stored in the sensor node. However, because the number of sensors in WSNs is too numerous, it is difficult for sensor network systems to obtain location information of all nodes at an early stage.[13] In this paper, the terminal node in a network is grouped into two, namely anchor node-set (AN) and unknown locations nodeset (ULN). Among them, AN represents a special class that knows its own location, and ULN represents a class of nodes that do not know their locations. Every node has a same node location list (NLL) which has node ID and location. The initial list only contains the location information of the anchor node. In order to obtain the location information of all nodes, this paper proposes a quadrilateral measurement (QM) method in [35], which can acquire nodes of unknown locations, and then improve the unified NLL.

Nowadays, the malicious node detection in WSNs mostly adopts the way of one-time centralized decision-making. According to this method, the original data cannot be traced back, the detection process is difficult to reproduce and check, and the problems of error and false positives are difficult to avoid. In this paper, through 3D space it is realized by using block chain intelligent contract and WSNs quadrilateral measurement for localization of the detection of malicious nodes in, and the consensus results of voting are recorded in the blockchain distributed. The simulation results show that the model can effectively detect malicious nodes in WSNs and ensure the traceability of the detection process.

In Research Paper[10] Intrusion Detection for Wireless Sensor Network Based on Traffic Prediction Model Han Zhijie, Wang Ruchuang

In this article, the authors first propose an efficient traffic prediction algorithm for sensor nodes using the Markov model . Based on this algorithm, a distributed anomaly detection scheme, TPID (Traffic Prediction Based Intrusion Detection), was developed to detect attacks that have a stronger impact on packet traffic, e.g. Ex. B. Selective redirect attacks , DOS attacks. With TPID, each node acts independently when predicting traffic and detecting a failure. No special hardware or node cooperation is required. The scheme is evaluated and compared with other methods in experiments. The results show that the proposed scheme achieves a high recognition rate with less computing and communication costs.

WSN, short for Wireless Sensor Network, can implement complex and extensive environmental monitoring and monitoring tasks in a variety of application areas, making it a high application in military and national defense, as well as environmental monitoring has, traffic management, disaster rescue and many other areas.[12] WSN's wireless transmission, properties that nobody cares about and other natural ones, make it vulnerable to all kinds of attacks. One of the most damaging attacks is scam and 4,444 denial of service (or DoS) attacks. Under the premise of masking as much as possible, the above tries to produce the monitoring results incorrectly so that the monitoring results are unreliable. The latter tries to damage the local network or even the general functioning of the network, so the facilities are not available. When WSN was used on the scene in important missions, such as the success or failure of the entire mission.[13]

In this paper, we've delivered a singular anomaly detection primarily based totally protection scheme for huge scale sensor networks primarily based totally on Markov version. If every node can construct a easy Markov version of visitors predict, those data can later be used to discover adjustments in them. We have proven that, via way of means of searching at a surprisingly small range of acquired packet functions, a node can successfully discover an interloper impersonating a valid neighbor. In our implementation, we taken into consideration the paradox detection set of rules achieved at every node separately. Low-complexity cooperative algorithms may also enhance the detection and containment process. Different routing, medium-get right of entry to and dispensed manipulate algorithms will introduce specific functions. More studies is wanted to decide higher node functions addressing precise vulnerabilities and to expand stepped forward detection algorithms with sensor.

In paper[11] Malicious attack detection in underwater wireless network detection by Mohammad R Ahmad, Syeda Manjia Tahsien, Mohammad Aseeri.

Underwater Wireless Sensor Network (UWSN) is one of the most promising technologies for observing the oceans. Underwater sensor applications have several areas, ranging from the oil industry to aquaculture. Some of the UWSN applications include equipment verification, underwater ecosystem monitoring, natural disaster and fault prediction, mission exploration and exploration, and the study of marine life. Given the properties and application platform of UWSN, UWSN security is a critical issue and received a lot of attention from researchers. To have a functional UWSN to extract the authentic data, security and protection mechanisms are crucial. Malicious node attacks have prevailed and are the main challenges for UWSN. Various research has been done to protect UWSN from malicious attacks, but most of the work relies on a defined pre-deployment threshold or training data set. It is a complication and a challenge for the UWSN that without an established security foundation, a UWSN is required to detect malicious attacks. In this whitepaper, we support Vector Machines in identifying malicious attacks on a UWSN. SVM gives good results and its training time is.[14]

Wireless Sensor Network (WSN) is a cutting-edge technology for collecting data through the collaboration of distributed and autonomous nodes. Lately, this technology has attracted more attention than before, largely due to its superiority in terms of wide application and lower cost. [12] Typically, a WSN includes a large number of low-cost, low-power, multifunctional detection devices that are equipped with short-range wireless communication capabilities. The sink or base station has high processing power, increased memory, storage, and analysis performance. All data from the node is transmitted to the receiver via wireless communication means; the process is carried out autonomously.

The research presented in the document is examined and a novel algorithm is modeled to find malicious attacks to protect UWSN. We use the Support Vector Machine (SVM) method to evaluate attacks in UWSN, since SVM takes less time to train. Malicious nodes always retain the anomaly attribute. We use the abnormal attribute of a node to identify the bad node. In general, the behavior of a malicious or compromised node is always different from that of a normal node. Typically this happens with both the physical and transmission parameters of the compromised node, even though the compromised node is attempting to act as a legitimate node. In this we use the behavior of the neighbor node to evaluate the suspicious node with SVM. With this evaluation, we have identified malicious attacks on underwater wireless sensor networks that are shown in the result and in the simulation.

In paper[12] HYBRID NODE WATCHING TECHNIQUE BASED DOS FLOODING ATTACK DETECTION IN WIRELESS SENSOR NETWORK L. Sheeba and V.S. Meenakshi

Intrusion detection is the most concentrated research topic in the wireless sensor network, where the presence of intrusion activity on the is more difficult to find when there is no centralized architecture to monitor. One of the most common attack activities on the wireless sensor network is floating denial of service (DoS) attacks. DoS Flood attacks would send large amounts of fragmented messages to the end node at to compromise the functionality of that node. Some of the top 4,444 DoS flood attacks found on the network are 4,444 ICMP flood attacks, 4,444 synchronous flood attacks, UDP flood attacks, and 4,444 web attacks. All these networks would send a huge number of messages, such as B. Internet control message packets, synchronous messages, UDO messages, respectively, to the web servers in order to impair their normal operation by consuming energy resources and so on. In previous research, the Sybil and DDoS attacks were identified and prevented by introducing method , namely the Privacy Related Anonymous Authentication (PAAM) method. However, these investigation methods reduced the detection rate of the attack with the presence of DoS flood attacks. This is focused on and solved in this thesis by introducing a method, namely the Hybrid Node Observation Technique (HNWT). This investigation technique seeks to find the variation in the data and control messages transmitted between the end nodes to find the presence of flood attacks. This is done through trusted nodes that are optimally selected by using the cat swarm algorithm. These optimally selected nodes monitor data transfer behavior to predict the presence of malicious nodes. The general implementation of this research is done in the NS2 simulation environment , from which it has been shown that the proposed research technique tends to have a higher attack detection.

We also discussed HYBRID NODE WATCHING TECHNIQUE FOR DOS FLOODING ATTACK DETECTION, OPTIMAL MONITORING NODE SELECTION BASED ON TRUST VALUE, HYBRID WATCHING TECHNIQUE FOR DOS FLOODING ATTACK DETECTION, PERFORMANCE ANALYSIS OF UDP FLOODING ATTACK, PERFORMANCE ANALYSIS OF WEB ATTACK.

In this research work, the Hybrid Node Observation Technique (HNWT) is presented for the precise detection of DDoS flood attacks. This research technique seeks to find the variation in the data and control messages transmitted between the end nodes to find the presence of flood attacks. This is done through trusted nodes , which are optimally selected by the Cat Swarm algorithm. These optimally selected nodes monitor the transmission behavior of data to predict the presence of malicious nodes. The general implementation of this research is done in the NS2 simulation environment, from which it has been shown that the proposed research technique tends to have a higher attack detection.

In paper[13]Malicious Node Detection in Wireless Sensor Networks using Weighted Trust Evaluation Idris M. Atakli, Hongbing Hu, Yu Chen* SUNY – Binghamton Binghamton, NY 13902, USA.

When deployed in a harsh environment, individual nodes in a wireless sensor network (WSN) can be restricted due to restrictions such as: It is important to identify and isolate compromised nodes to avoid being misled by forged information injected by the adversary through compromised nodes. However, due to poor scalability and high communication overhead, it is challenging to efficiently secure flat topology networks. In addition to a hierarchical WSN architecture, in this article we proposed a new scheme based on a weighted trust score to detect malicious nodes. The hierarchical network can reduce the communication overhead between the sensor nodes by using the cluster topology. Through intensive simulations, we verified the correctness and efficiency of our detection.

In this article, we proposed a new weighted scoring scheme to detect compromised or misbehaving nodes in wireless sensor networks. The basic idea of is that the FNs grant trust values to each of the nodes at the trust level of the cluster. It is much easier and less complex to keep track of the nodes, and it is more difficult to compromise most of the node unless an attacker is compromising the base stations. With very good scalability, our approach can be applied to both small WSNs and WSNs with more than nodes. The only difference when applied to larger WSNs is to increase the number of FNs. In essence, it could be treated as a node grouping problem. Although various investigations report that addresses the problem of detecting malicious nodes in the WSN, it is difficult to compare the performance of each one. As introduced in Section 2, the design assumptions and experimental settings are very different. In particular, the lack of a comparable benchmark makes it meaningless to compare the results, i. H. the detection rate, to compare. Our approach is based on the assumption that base stations are reliable. In fact, if the adversary can gain control of the base stations, they can carry out any attack against the WSN. This is an interesting open problem, but it is outside the scope of this paper. Another critical assumption is that most of the sensor nodes are functioning properly. If the number of compromised nodes is greater than the number of normal nodes, the legal nodes are reported as malicious and quarantined. In fact, in this document we only reported preliminary results that confirmed the accuracy and effectiveness of our solution. A more detailed analysis regarding the performance of our system is examined in Research in progress and other questions to be answered.

In the Given the Research Paper the Author has explained about the layer wise attacks which take place in the Wireless Sensor Network.

In every network where sensitive data is safely sent in the required direction, security is a must. WSNs (wireless sensor networks) are networks developed in hostile environments for many uses. Regardless of the application, WSNs must collect a huge quantity of sensitive data and transfer it to an authorised authority, usually a sink. Through internet access in sensor nodes and internet-connected devices, WSN has merged with the Internet of Things (IoT). The amount of data acquired by IoT is tremendous, and WSN eventually collects it through the Internet. It's difficult to create a secure sensor network due to a variety of resource restrictions, but having a secure WSN is critical for a safe IoT. The majority of existing security measures are ineffective with WSN.As described in Communication, some of the issues in IoT include:

Wired and wireless communication, such as LPWAN, ZigBee, and others, are employed in IoT.

Scalability: An IoT network consists of numerous nodes, making naming, addressing, and controlling a large number of such devices difficult.

Heterogeneity: The Internet of Things (IoT) is a network of numerous devices from various families, such as actuators, sensors, switches, gateways, mobile phones, and so on. Different algorithms, protocols, and circuits are used by different devices.

Energy Consumption: In both WSN and IoT, energy consumption is a major restriction. As a result, researchers are always battling to build an algorithm for IoT and WSN that has the fewest processing needs.

Interoperability: An IoT network is made up of a variety of devices that communicate and interact with one another. As a result, a predetermined standard for data interchange is always required.[15]

Self-awareness: IoT devices should automate automatically with as little human involvement as possible.[19]

In the Given the Research Paper the Author has explained us how to handle the Inside Attacks in Wireless Sensor Network.Wireless sensor networks are a relatively new data collection and processing technique. A sensor network typically comprises of a large number of sensor nodes with limited resources.These nodes take measurements of physical phenomena, process data, make reports, and communicate those reports to a central information processing unit called a sink through multihop communication. Depending on the circumstance, numerous sensor nodes collaborate to acquire and analyse data, for example, to estimate the average temperature in a given area.Sensor networks may be applied to a wide range of applications. Sensor networks, which originated in military research and are now widely employed in civil applications such as critical infrastructure monitoring, are increasingly being used in civic applications.

They offer concepts and procedures to deal with insider threats in wireless sensor networks in this thesis. This thesis makes a two-fold contribution. To begin, they suggest a new generic taxonomy to categorise the various methods to insider threat protection. Second, we offer a number of security practises to guard against insider threats.[16]

The established security strategy distinguishes techniques to guard against insider attacks in their classification.

The applied mechanisms have been subclassified.The findings might serve as a foundation for future protocol development.The protocols suggested in the second section of this thesis cover a wide range of topics.[14]

To begin, they offer a protocol to guard against a major Denial-of-Service attack in which an adversary injects or repeats a large number of bogus messages in order to overwhelm numerous message forwarding nodes and (completely) exhaust their limited energy resources. To filter out such signals, most proposed techniques use threshold-based algorithms.[20]

In this research paper the author told us about the intrusion detection system in Wireless Sensor Networks.Due to the open wireless channel, multihop decentralised communication, and deployment in hostile and physically unprotected places, WSNs are subject to a variety of security assaults. Multihop distributed operations are one of the fundamental elements of a WSN, which adds to the complexity of security attack detection and prevention. An intrusion is defined as any illegal action carried out by attackers in order to harm network resources or sensor nodes. In wireless networks, a single flawless defence is neither practicable nor attainable, as there are always some architectural defects, software vulnerabilities, or design faults that might be exploited by attackers. It's considered a passive defence since it doesn't try to prevent assaults; instead, it warns network administrators about potential attacks ahead of time so they can halt or mitigate the damage.[21]

IDS, in general, is made up of three primary components

The monitoring component is utilised to keep track on local happenings as well as neighbours. This component is primarily responsible for tracking traffic patterns, internal events, and resource use [18].

(ii) The key component is the analysis and detection module, which is based on a modelling method. The operations, behaviour, and activities of the network are examined, and choices are made about whether they are harmful or not.

(iii) The alarm component is a response-generating component that creates an alarm when an incursion is detected.[22]

3.2 Survey Table:

Protocols/models	**Parameters**				
	Parameter 1	**Parameter2**	**Parameter 3**	**Parameter 4**	**Parameter 5**
Hamming Residue Method	**Node Count**	**Layer**	**Antenna**	**Type of Queue**	**MAC Protocol**
ESMCH Model	**Node Count**	**Coverage Area of nodes**	**Trust Value of nodes**	**Trust value of path**	**Routing Protocol**
Malicious Node Detection in WSN	**Network density**	**Malicious node multiplier**	**Maximum ratio difference**	**Message check probability**	**Transmission Power Multiplier**

Attacks in WSN	**Node Count**	**Layer based**	**Active and Passive Attacks**	**Adversary presence**	**Adversary intervention**
IDS using data mining Algo	**Node Count**	**Layer**	**Misuse detection technique**	**Anomaly detection**	**Dawson proactive routing protocol**
Weight Assignment for Malicious node	**Node Count**	**Data repetition rate**	**Packet size abnormality**	**Data correlation**	**Volatility of transmission delay**
Taxonomy of internal attacks in WSN	**Node Count**	**Layer based**	**Sensor based platform OSI built**	**Security attack & DoS attack**	**Increase in Bandwidth & routing protocol**
Blockchain Trust model for Malicious detection	**Node Count**	**Based on Smart Contract**	**Blockchain Intellegent contract**	**NCQ & BTM**	**Enhanced LEACH protocol**

3.3 Problem Definition:

Wireless sensor networks are randomly deployed and responsible for monitoring geographical area wide. In WSN, the aggregation of data is very complex because of its limited power and computing capabilities. Issue in data aggregation is that the data may be passed on to malicious nodes. All the existing data aggregation techniques undergo security issues because of the transfer of large amounts of data.

Deployed in a hostile environment, individual nodes of a wireless sensor network (WSN) could be easily compromised by the adversary due to the constraints such as limited battery lifetime, memory space and computing capability. It is critical to detect and isolate the compromised nodes in order to avoid being misled by the falsified information injected by the adversary through compromised nodes. However, it is challenging to secure the flat topology networks efficiently because of the poor scalability and high communication overhead. On top of a hierarchical WSN architecture.

Different kinds of attacks happen on these wireless sensor networks which cause a lot of havoc and destruction to all the people and applications it is deployed for. Attackers constantly try to attack and hack into the network to gain sensitive data regarding the model or application at which wsn has been deployed by the engineers. Many different attacks are possible on such networks like man in the middle attacks, balck hole attack, wormhole attack, etc. These attacks prove to be very harmful to the network and can cause a lot of destruction like a WSN deployed in an earthquake station if hacked can cause catastrophe.

Rather than conventional remote organizations, uncommon security and execution issues must be cautiously considered for sensor networks . For instance, due to the unattended nature of sensor organizations, an aggressor could patch different assaults and even trade off sensor gadgets without being distinguished. In this manner, a sensor organization ought to be strong against assaults, and in case an assault succeeds, its effect ought to be limited. As such, compromising a solitary sensor hub or not many sensor hubs ought not crash the whole organization.

4. Proposed Method:

In our proposed method, we have tried to implement an Intrusion Detection System for a wireless sensor network using a programming language. In our model, there is also a simulation for a scenario using the NS2 simulator.

An Intrusion Detection System(IDS) would be best for the detection of malicious nodes in a Wireless Sensor Network(WSNs) as it will discover the hostile nodes in an efficient manner and with a better accuracy than other approaches. So, we have designed an IDS which will detect the malicious nodes in the network.

Residual energy was one of the main factors which was considered in designing this system. As all kinds of attackers try to hack into the nodes already present in the network, it tends to reduce the energy of nodes drastically.

We have implemented a two-layer network protocol to detect abnormal Wireless Sensor Nodes by monitoring their power levels and get rid of it if necessary. This includes lower level and upper level implementation. The network can be attacked in the simulation, and our IDS can detect the compromised node and remove it from the route.

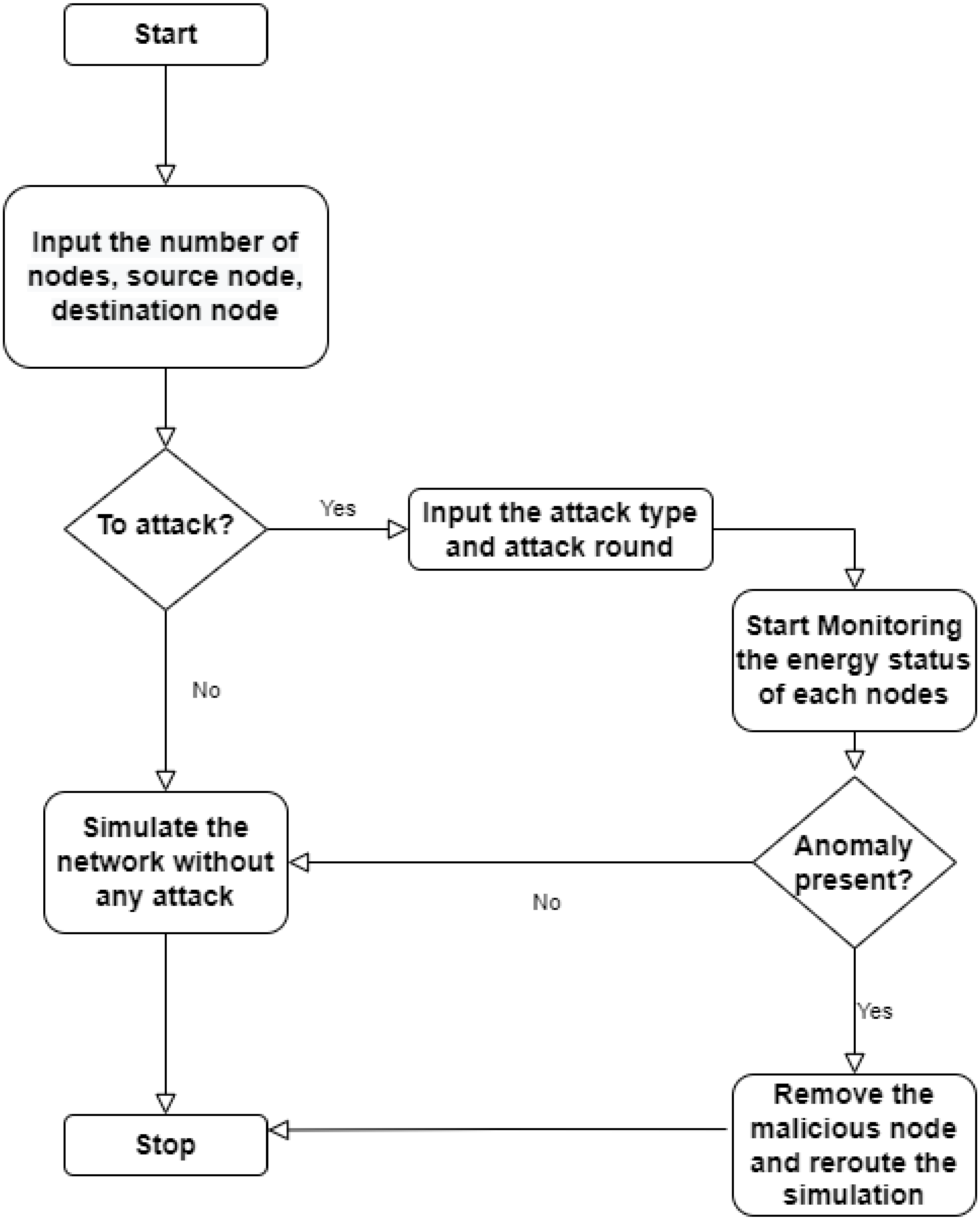
LowerLevel is used to form and reform the network. Node defines attributes of each node, which includes the coordinates of each node and distance to other nodes.
UpperLevel is used to monitor the route and it changes the route when one node in the route is compromised. Whether a node is compromised or not is decided by its residual energy, which is monitored by its child node. AdjustPsend is a class in the JAVA to show the energy status of a node.

Attack is the class for attacking strategy. This part contains 3 kinds of attacks:

1: jamming - 0% energy left
2: man-in-the-middle - 30% energy left
3: physical damage

Node discharges as they are used continuously but as they are attacked, their energy decreases at a much faster rate. So, energy is continuously monitored to check any malicious activity.

4.1. Flowchart:

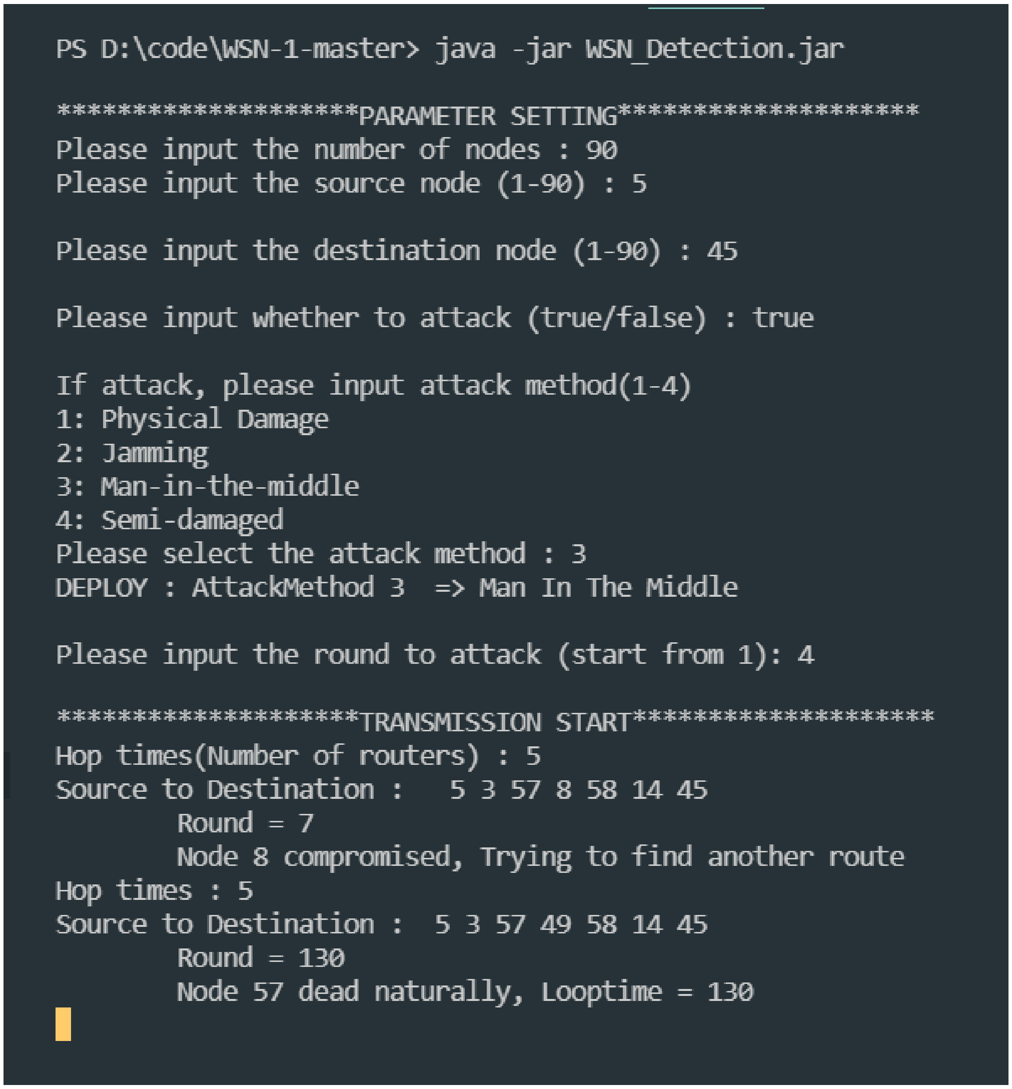

Start
Input the number of nodes, source node, destination node
To attack?
Yes
Input the attack type and attack round
Start Monitoring the energy status of each nodes
No
Simulate the network without any attack
Anomaly present?
No
Yes
Remove the malicious node and reroute the simulation
Stop

4.2 Algorithm:

- **Step1: Get the input of all the network parameters like number of nodes, source node, destination node.**
- **Step2: Get the condition whether to attack or not in the network.**
- **Step3: If an attack has to be done on the network, get the attack parameters like attack type and round at which the node which will be infected.**
- **Step4: Start the simulation of the network using the conditions specified by the user and start the monitoring of residual energies in the network.**
- **Step5: If the attack is not present, directly assign the energies to each node in the network and route the packets from source to destination until any node in the route dies naturally.**
- **Step6: If an attack is present, the node will be infected at the round specified by the user and the monitoring of the nodes present in the route will search for any anomalies.**
- **Step7: If any anomaly is present with any node, the infected node will be removed from the network and transmission halts for some time until a new route is discovered.**
- **Step8: Once the new route is discovered and established, the transmission will resume and will continue until any node in the route dies naturally of the lack of energy.**
- **Step9: Simulation of the same network has been done for a particular scenario in NS2 using NSG for the generation and nam for the animation of the simulation for both malicious and non-malicious networks.**

5. Implementation:

- **Java programming language has been used to implement the intrusion detection system.**
- **Java AWT and swing has been used to develop the window based application to show the current network and routing path along with malicious and other nodes.**
- **NS2 simulation has also been used to animate the network with and without malicious nodes.**
- **NSG (Network Simulation Generator) has been used to design the network and to generate the respective tcl file.**



```
PS D:\code\WSN-1-master> java -jar WSN_Detection.jar

********************PARAMETER SETTING********************
Please input the number of nodes : 90
Please input the source node (1-90) : 5

Please input the destination node (1-90) : 45

Please input whether to attack (true/false) : true

If attack, please input attack method(1-4)
1: Physical Damage
2: Jamming
3: Man-in-the-middle
4: Semi-damaged
Please select the attack method : 3
DEPLOY : AttackMethod 3  => Man In The Middle

Please input the round to attack (start from 1): 4

********************TRANSMISSION START********************
Hop times(Number of routers) : 5
Source to Destination :   5 3 57 8 58 14 45
        Round = 7
        Node 8 compromised, Trying to find another route
Hop times : 5
Source to Destination :  5 3 57 49 58 14 45
        Round = 130
        Node 57 dead naturally, Looptime = 130
```

Fig:1

- **As we can see in fig.1, we have implemented a Wireless Sensor Network using total number of nodes as 90, source node as 5, destination node as 45, and attacking strategy as Man in the middle attack. The malicious node was set to attack at round number 4 . Our IDS was able to detect the malicious node in the network at round number 7 and that particular node was removed and a new route search has been initiated and found.**

  The new route will run and transmit the data packets until and unless any node dies in the network due to lack of energy. In this example the node 57 dies after round 130 naturally.

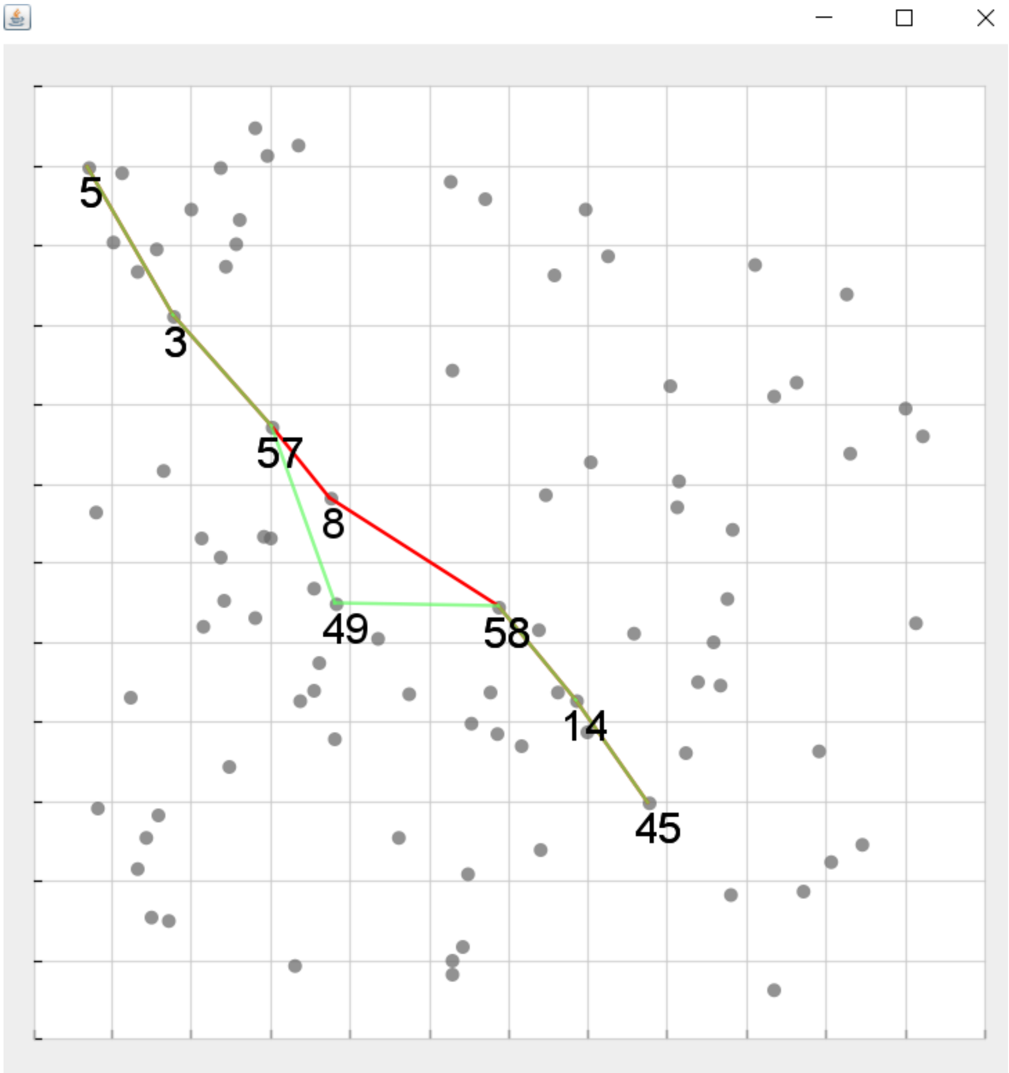


Fig:2

The fig.2 shows the simulation of parameters specified in fig1. We can see that node 8 is compromised and a new route has been discovered and transmission begins.

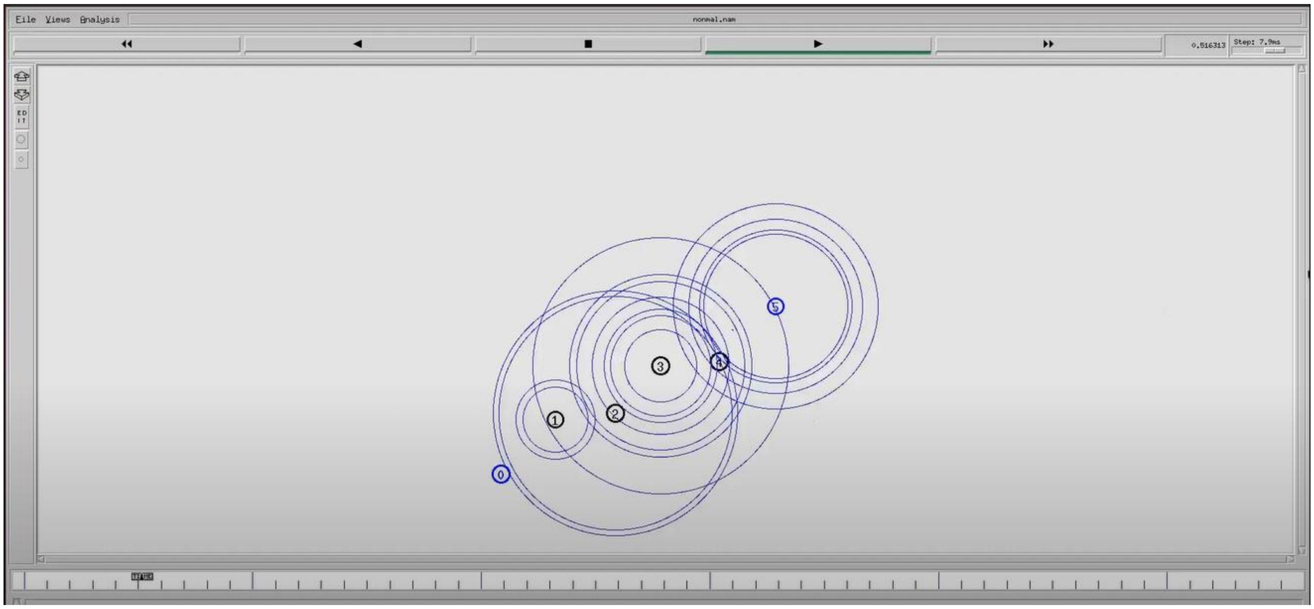


Fig.3

The fig.3 shows the animation of simulation of non-malicious networks. It is clearly visible that packet transmission is taking place continuously and without any interference.

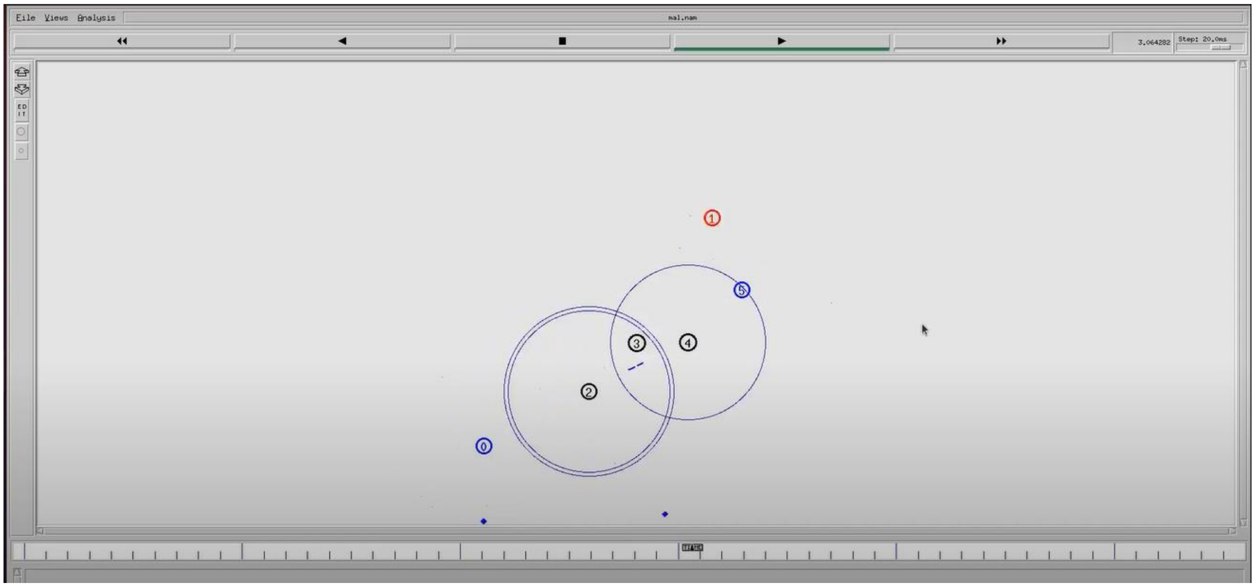


Fig.4

The fig.3 shows the animation of simulation of malicious networks. It is clearly visible that node 1 is detected as malicious and is removed from the network.

6. Results and Discussion:

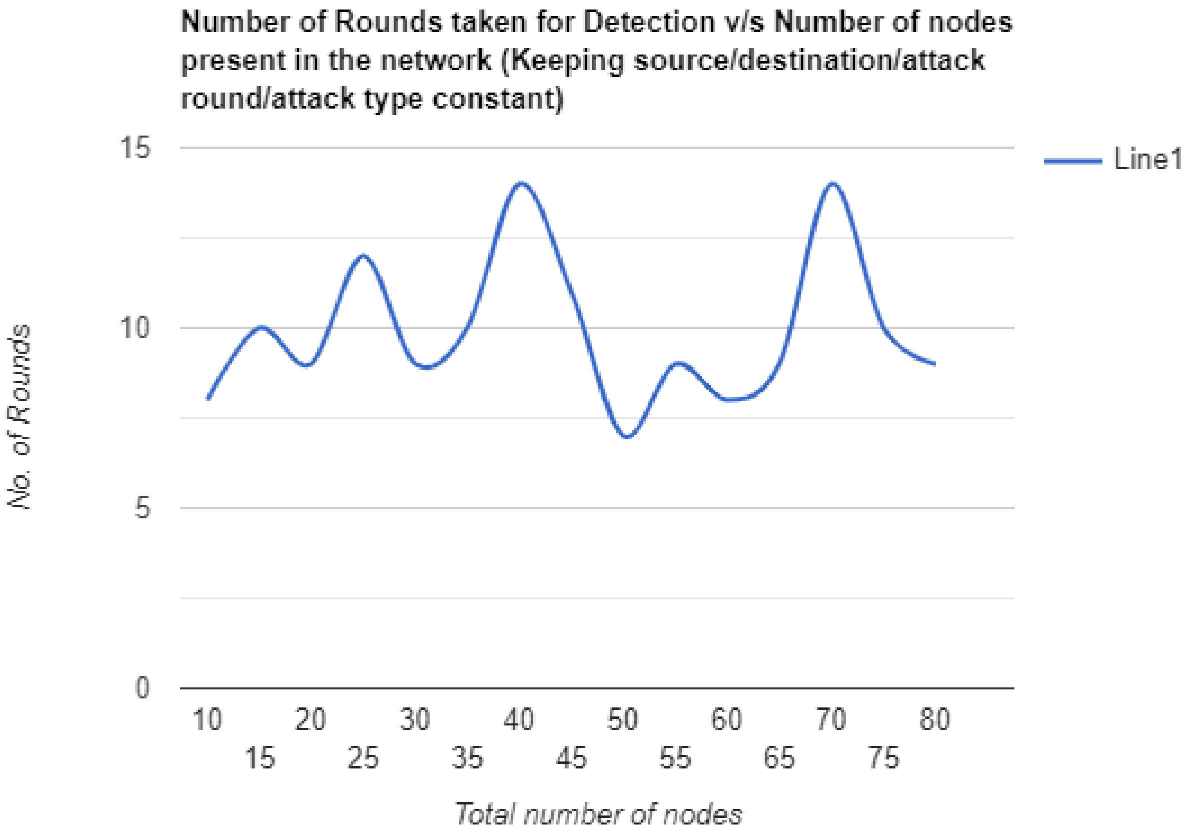


Fig.5

<u>The fig.5 shows the relation between number of rounds taken for detection by number of nodes present in the network (keeping source/destination/attack round/attack type constant)</u>

From this graph we conclude that if we increase the number of nodes in our network the loop time generally gets increase. But on an average the total number of rounds to detect our nodes is between 10-15. This is because everytime we increase our nodes the topology of our network changes.

We have taken the source and destination constant for the simulation and attack type and attack round is also constant. Only the total number of nodes is changing for the entire duration. As we have initialized the attack round as 5, the malicious nodes are getting detected around the round number 11.

It is seen that everytime we attack any nodes its energy decreases accordingly the node will be infected at the round specified by the user and the monitoring of the nodes present in the route will search for any anomalies. If it detects any anomalies

the infected nodes gets detached from the network accordingly losing the residual energy.

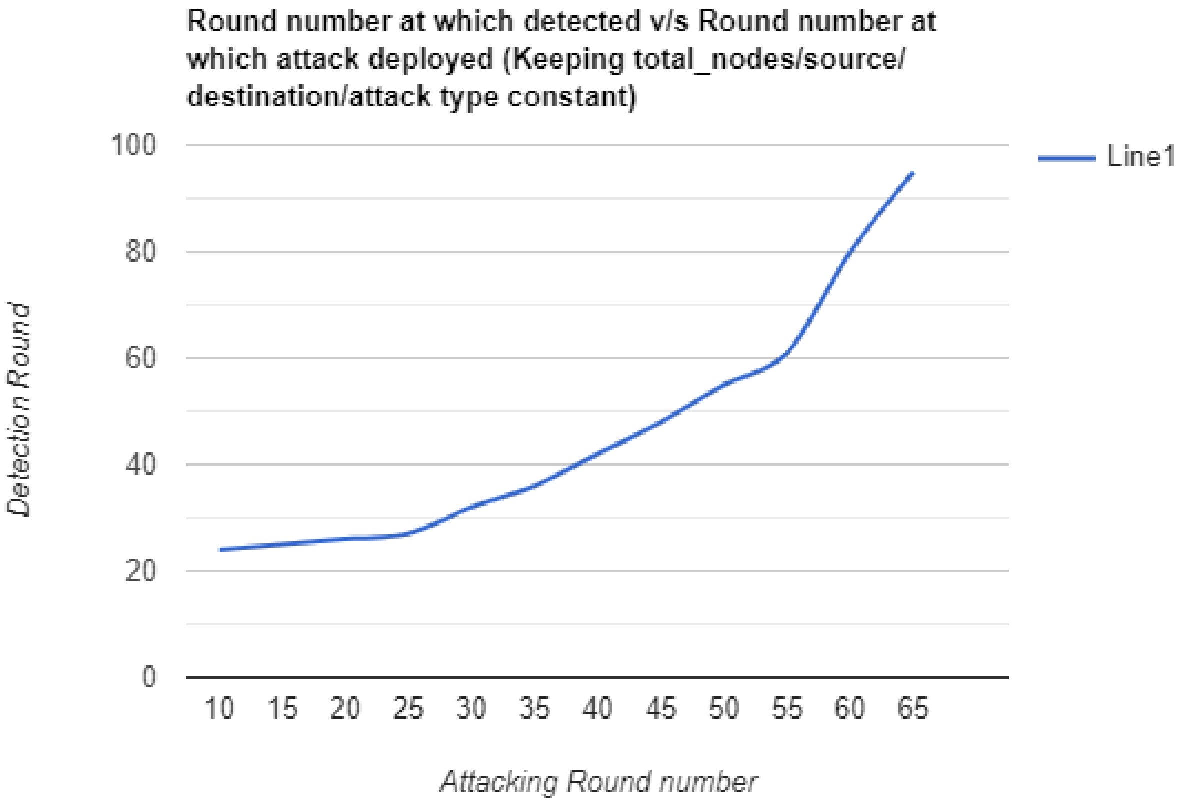


Fig.6

<u>The fig.6 shows the comparison between the round number at which the malicious node detected vs the round at which the node is attacked.</u>

From this graph, it has been inferred that as the node is attacked at a later stage of time in the simulation of the network, it becomes difficult to detect whether the node is malicious or not. As the simulation progresses, the nodes' residual energy starts to decline and when the attacker attacks the network, the change in energy is much less as it would be if an attack has taken place in the initial phases of the simulation. It is clearly visible in the graph that when the attack is taking place between the rounds 10-50, it usually takes on an average of 10 rounds to detect the malicious node and removal of it from the network.

But as we have increased the attack round for larger values than 50, it is clearly visible that it is taking much more time to detect the anomaly and the change in residual energy. Since the difference in residual energies of non-malicious nodes and

the malicious node is much less after round number 50, it has been of greater difficulty to detect the attack. For our scenario, the source node is 5 and destination was 62. The attack is Man in the middle attack and total number of nodes is 90.

7.1. Conclusion:

In this paper, the detection of malicious nodes in wireless sensor networks has been done by an Intrusion Detection System using the residual energy of the nodes. The model which was implemented to detect any malicious node is working fine and giving good results. It is automatically detecting the malicious nodes by the use of predefined parameters and able to remove that node from the route of an ongoing transmission.

Our model is able to reroute the ongoing transmission using the detection mechanism to detect and remove the malignant node in the network successfully. The basic idea was to check any sudden decline in the energy of the nodes present in the network. All the nodes in our model have some finite amount of energy which is set to drain at a particular rate in the due course of simulation. As the attacker attacks on the network, the node's energy declines at a much faster pace and gets detected by the simulation program and detection system.

The response time for the detection of malicious nodes from the round of injection was on an average of 2-5 rounds of simulation and total energy of the node present just before the destination node was drained completely after ~138 rounds of packet transmission.
Our IDS was able to detect the malicious node successfully and in simulation it is possible to remove that detected node from the network.

7.2. Future Work:

As the future work of this project, we intend to add other parameters like transmission anomalies, sequence numbers, etc to enhance the detection strategy of our IDS. We will try to inculcate different attacks like blackhole attacks, etc in our simulation also. We will also try to enhance our system by logging the information captured during the simulations and create a simulation which will help the developers and implementers of WSNs to provide more security to their network.

We will try to integrate Machine Learning (Neural Network) in our current project, so that this system will be able to attain nearly ~100% accuracy and much less response time than the current version.

8. References:

[1] M. Alotaibi, “Security to wireless sensor networks against malicious attacks using Hamming residue method,” Eurasip J. Wirel. Commun. Netw., vol. 2019, no. 1, 2019, doi: 10.1186/s13638-018-1337-5.

[2] A. M. Morsi, T. M. Barakat, and A. A. Nashaat, “An efficient and secure malicious node detection model for wireless sensor networks,” Int. J. Comput. Networks Commun., vol. 12, no. 1, 2020, doi: 10.5121/ijcnc.2020.12107.

[3]Y. Sei and A. Ohsuga, “Malicious node detection in mobilewireless sensor networks,” J. Inf. Process., vol. 23, no. 4, pp. 476–487, 2015, doi: 10.2197/ipsjjip.23.476.

[4]J. Sen, “Security in wireless sensor networks,” Wirel. Sens. Networks Curr. Status Futur. Trends, pp. 407–460, 2016.

[5] Y. El Mourabit, A. Toumanari, A. Bouirden, and N. El Moussaid, “A comparative evaluation of intrusion detection techniques in wireless sensor network,” J. Theor. Appl. Inf. Technol., vol. 76, no. 1, pp. 27–35, 2015.

[6] Stolfo, S. J. (2004). Worm and attack early warning: piercing stealthy reconnaissance. IEEE security & privacy, 2(3), 73-75.

[7] X. Yin and S. Li, “Trust evaluation model with entropy-based weight assignment for malicious node’s detection in wireless sensor networks,” Eurasip J. Wirel. Commun. Netw., vol. 2019, no. 1, 2019, doi: 10.1186/s13638-019-1524-z.

[8] X, Huang, M, Ahmed, D, Sharma, “The node became compromised when an attacker gain control of the node that acts as a legitimate node, after network deployment”, 2011 Ninth IEEE/IFIP International Conference on Embedded and Ubiquitous Computing. October 2011 Melbourne, Australia

[9]] T. Qiu, K. Zheng, M. Han, C. L. P. Chen, and M. Xu, ‘‘A data emergency-aware scheduling scheme for Internet of Things in smart cities,’’ IEEE Trans. Ind. Informat., vol. 14, no. 5, pp. 2042–2051, May 2018. doi: 10.1109/TII.2017.2763971.

[10] Agah A , Das S K, Basu K, Asadi M. Int rusion detection in sensor networks : A non cooperative game approach/ / Proceedings of t he 3rd IEEE International Symposium on Network Computing and Application (NCAA̧04) . Cambridge ,MA , 2004 : 3432346.

[11] M. R. Ahmed, X. Huang, and H. Cui, "Mrakov Chain Monte Carlo Based Internal Attack Evaluation for Wireless Sensor Network," Int. J. Comput. Sci. Netw. Secur., vol. 13, no. 3, pp. 23-31, Mar. 2013.

[12] E. Fadel, V.C. Gungor, L. Nassef, N. Akkari, M.A. Malik, S. Almasri and I.F. Akyildiz, “A Survey on Wireless Sensor Networks for Smart Grid”, Computer Communications, Vol. 71, pp. 22-33, 2015.

[13] R. Chen, J. M. Park, and K. Bian, “Robust Distributed Spectrum Sensing in Cognitive Radio Networks,” Technical Report TR-ECE-06-07, Dept. of Electrical and Computer Engineering, Virginia Tech., July 2006.

[14] Alrajeh, Nabil Ali, Shafiullah Khan, and Bilal Shams. "Intrusion detection systems in wireless sensor networks: a review." International Journal of Distributed Sensor Networks 9.5 (2018): 167575.

[15] Mostefa, Benfilali, and Gafour Abdelkader. "A survey of wireless sensor network security in the context of Internet of Things." 2017 4th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM). IEEE, 2017.

[16] Ahmed, Adnan, et al. "A secure routing protocol with trust and energy awareness for wireless sensor network." Mobile Networks and Applications 21.2 (2016): 272-285.

[17] Ahmed, Adnan, et al. "Energy-aware and secure routing with trust for disaster response wireless sensor network." Peer-to-Peer Networking and Applications 10.1 (2017): 216-237.

[18] Shen, Wen, et al. "A new energy prediction approach for intrusion detection in cluster-based wireless sensor networks." International Conference on Green Communications and Networking. Springer, Berlin, Heidelberg, 2018.

[19] Sinha, Somnath, and Aditi Paul. "Neuro-fuzzy based intrusion detection system for wireless sensor network." Wireless Personal Communications 114.1 (2020): 835-851.

[20] Sherasiya, Tariqahmad, Hardik Upadhyay, and Hiren B. Patel. "A survey: Intrusion detection system for internet of things." International Journal of Computer Science and Engineering (IJCSE) 5.2 (2016): 91-98.

[21] Pawar, Mohandas V., and J. Anuradha. "Detection and prevention of black-hole and wormhole attacks in wireless sensor network using optimized LSTM." International Journal of Pervasive Computing and Communications (2021).

[22] El Mourabit, Yousef, et al. "Intrusion detection techniques in wireless sensor network using data mining algorithms: comparative evaluation based on attacks detection." International Journal of Advanced Computer Science and Applications 6.9 (2015): 164-172.