International Journal of Scientific Research in Computer Science and Engineering
Vol.10, Issue.6, pp.30-39, December (2022)

Research Paper

E-ISSN: 2320-7639

To Identify the Untrustworthy Leader of a Hierarchical Wireless Sensor Network Using Received Signal Strength

Md. Ibrahim Abdullah[1*], Md. Atiqur Rahman[2], Mohammad Alamgir Hossain[3], Md. Shohidul Islam[4], Md. Shamim Hossain[5]

[1,2,3,4,5]Department of Computer Science and Engineering, Islamic University, Kushat-7003, Bangladesh

[*]*Corresponding Author: ibrahim25si@yahoo.com, Tel.: +880-1712501961*

Available online at: www.isroset.org

Received: 21/Sept/2022, Accepted: 23/Nov/2022, Online: 31/Dec/2022

***Abstract*–** There are a multitude of privacy and safety concerns that arise as a result of wireless sensor nodes being carelessly put in potentially hazardous regions. An adversary has the capability of either seizing a node that is located in an area that is not under their control or introducing a node that is acting under the guise of a genuine node. The lack of adequate security in sensor networks presents a substantial barrier to many potential applications. A form of protection known as intrusion detection can be utilized to thwart attacks of this nature. Because of this, traditional methods of intrusion detection cannot be utilized in a sensor network due to the restricted resources of individual nodes. In this paper, we have presented a method to detect intruder in hierarchical wireless sensor networks using a sensor fusion algorithm. This method is intended to be utilized in situations in which malevolent nodes are performing the duties of Cluster Head. Clustering is an approach that sensor networks take in order to produce their detections. A technique that only requires a modest amount of communication yet is nevertheless capable of thwarting an attack on a hierarchical routing system has been described.

***Keywords*–** Wireless Sensor Network, Security, LEACH, Malicious Node, RSS, Hello Flood attack.

I. INTRODUCTION

Over the course of the past few years, wireless sensor networks (WSNs) have steadily risen to the status of one of the most interesting and potentially fruitful fields. This network is made up of a vast number of minuscule sensor nodes, each of which possesses a constrained amount of power, bandwidth, memory, and processing capabilities [1]. Because sensor nodes have their own built-in restrictions, the network may become more susceptible to errors and malicious attacks as a result. The open nature of wireless transmission, the unstable communication channels, and the limits of resources in radio range, processing speed, memory and power make it difficult to implement security mechanisms in WSN [2].

Because of its straightforward architecture, the WSN device can be compromised in a variety of different ways. Despite the use of encryption and authentication, malicious actors are still able to monitor and manipulate the communication that passes via WSNs. To make matters even worse, it is exceedingly difficult to defend sensor nodes from physical attacks in hostile unattended situations. This is due to the fact that nodes can be physically shifted, damaged, or tampered with through direct physical access. Attackers on WSN have been categorized, according to Roosta et al. [3]. Wood [2] discusses potential DoS attacks that could be launched against WSNs. Finding novel security solutions that are appropriate for node design and protocols is the primary problem faced by researchers working in this area of the field. This security system should be able to identify intruders with a minimum amount of communication by detecting any abnormal behaviors exhibited by sensor nodes. Owing to the fact that wireless communication is the primary driver of energy usage [1]. Misbehaviors may be displayed by a node whenever a problem occurs or as the result of malicious activity by sensors that have been exploited [4]. By evaluating the activity of the nodes, it is possible to identify inappropriate activities in any scenario.

Karlof [5] has presented a comprehensive examination of the vulnerabilities that are present in the routing of WSNs. According to the findings of their research, standard protocols for sensor networks are insecure because of their inherent simplicity. The routing algorithms proposed for sensor networks do not consider security techniques because of the limited capabilities of sensor nodes. Because sensor networks are subject to a different set of criteria than standard wireless ad hoc networks, the routing in these networks also operates differently [6].

In reference number [7], a comparison is made between the Comparative Received Signal Strength (CRSS) Algorithm and the vector algorithm to determine which one is superior for the task of indoor localization. Therefore has been demonstrated that the superior

performance of the vector algorithm can be attributable to the aforementioned parameters. This is because CRSS is ambiguous, and it requires a bigger number of access points as well as a higher working frequency. A variant of the k-nearest Neighbor technique that is based on the signal matching approach has been developed in [8]. This variation was evaluated using a single test case, and the results showed that it offered an improvement in accuracy.

However, range-based techniques determine an estimate of the distance that separates each pair of nodes by approximating the gap. Global Positioning System (GPS) [9], time difference of arrival (TDoA) [10,11], time of arrival (ToA) [12], acoustic energy [13], angle of arrival (AoA) [14], and received signal strength indicator (RSSI) [15] are the range-based approaches that are utilized for estimating distance the most frequently. However, despite its high cost, additional hardware requirements, and significant energy consumption when applied for LoS applications in the vast outdoors, GPS is still the most preferred alternative. In addition, such applications are not encompassed by the scope of the WSNs that were taken into consideration for this research. When doing TDoA-based distance measuring, synchronization across the various nodes that are essential is of the utmost importance. This is a very inefficient approach in terms of both the amount of energy it consumes and the amount of money it costs, as it requires two signals to be delivered at different speeds in order to achieve synchronization. In a similar line, accurate ToA calls for clocks that have a high resolution in addition to their precision. In addition to this, it is necessary to have an accurate figure for the speed at which signals are transmitted. Because AoA is a directed method for determining the distance between two points, it requires a more expensive antenna to capture the incoming signal from a particular direction. In this study, RSSI-based localization will be used to complete the task of localizing target nodes because of its independence from the antenna array, synchronization requirements, and any other ancillary gear.

The received signal intensity at a node is influenced both by the power of the signal that was broadcast and the terrain of the path that the signal took. This effort will take into account the possibility of path loss as well as node separation [16]. Path loss can be caused by a number of different phenomena, including signal reflection, diffraction, and scattering [17]. Along the path that the signal takes as it is propagated, there is also some attenuation that occurs. The received signal strength indicator, also known as RSSI, is a metric that represents, in decibels, the strength of a signal at a particular node. There are a number of factors, including the relative motion of the transmitter and/or receiver, that have the potential to influence the RSSI [18,19,20] at a particular node. It is essential to keep in mind that the RSSI can be impacted at any time by the movements of items in the propagation environment [21,22], even if the devices themselves continue to remain stationary. This is something that must be kept in mind. It is difficult to construct a straightforward linear relationship between signal distance and node distance since RSSI depends on a number of different variables simultaneously. Therefore, a methodical and accurate strategy is required in order to calculate the distance between undiscovered nodes and locate their locations. The localization of a target node is essential for figuring out which path through a network will take the least amount of time and will deliver a data package to its destination.

The focus of this work is on attacks that are made against hierarchical routing protocols used in WSNs. In this architecture, some of the nodes were responsible for processing and sending information to the Base Station (BS) in the form of Cluster Heads, while the others were in charge of performing the sensing. As a result of CH's ability to aggregate and fuse the sensed information of its members and serve as an intermediary router to BS, The function of CH is significantly more significant than that of other nodes. If hostile nodes operate as CHs, it has the potential to disrupt the operation of the entire network [5]. The detection method that was proposed placed an emphasis on this susceptible point of security for hierarchical WSN and built a detection approach for a CH when it behaves in an unusual manner.

The remaining parts of this work are structured as described below. In the following section, clustering strategies for hierarchical routing protocols are discussed. In Section 3, we discuss the security breach as well as the work that is directly tied to it. Proposed detection mechanism detailed in part 4. The simulation will be presented in full in this section, and the findings will be discussed. In section 6, we will explore the findings and compare them to other work that is closely related. In the seventh and final section, we will offer some concluding thoughts.

II. CLUSTERING TECHNIQUE OF WSN

The formation of clusters in WSN is typically determined by the energy reserves of the sensors and the proximity of the sensors to the CH. LEACH [23] is the first hierarchical routing approach for WSNs. In this approach, a small number of sensor nodes are chosen at random to function as CHs. The remaining nodes all connect to one of these CHs. LEACH is entirely decentralized and does not call for any familiarity with global network architecture. In LEACH, the role of CH is shared among the nodes on a rotating basis in order to ensure that the energy load is evenly distributed after each predetermined time interval. The methodology behind this method of clustering is referred to as dynamic clustering [23]. The operation of LEACH is divided into two phases: I the setup phase, during which CHs are chosen and clusters are organized; and ii) the steady state phase, during which sensing data are transmitted.

During the setup phase, certain nodes will choose to act as CHs, at which point they will broadcast an advertisement

to the remaining nodes. A node will choose its cluster leader based on the received signal power of the advertisements it has received from CHs after it has received those CHs' advertisements. The node will then send a message to the CH it has targeted with the correct ID. On the other hand, a CH will only begin the process of creating its cluster if it has received messages from nodes that are interested in participating. After the cluster has been formed, the individual nodes that make up the cluster will start to sense and relay data to the CHs. The CH is responsible for aggregating or compressing the data of its members before sending it to the BS.

In PEGASIS [24], each node broadcasts a power signal to its neighbors, and then gradually decreases the strength of the signal until it is only received by a single node, identifying that node as its nearest neighbor. After that, every node will only connect with its immediate neighbor and will take turns transmitting data per round. Each node in the network combines the data it has acquired with its own data, and then uses multihop transmission to send the combined set of data to the next node in the network. This process replaces the formation of cluster leaders, which is done in LEACH. The TEEN [24] algorithm, which is an improvement upon the LEACH algorithm, enables reactions to extreme and abrupt changes in the network. The clustering method is comparable to LEACH in that it also considers the strength of the received signal. Therefore, the signal strength that a CH receives from a WSN cluster is the most crucial attribute to consider while constructing a WSN cluster.

III. SECURITY BREACH AND RELATED WORKS

Karlof [5] describes two hypothetical attacks that can be used against hierarchical routing protocols used in WSN: the HELLO Flood and the Selectively Forwarding. It is a requirement of many protocols that nodes announce themselves to their neighbors by broadcasting HELLO packets. A node that receives such a packet may believe that it is within normal radio range of the sender of the packet. An attacker can carry out a HELLO flood attack by broadcasting routing or other information with sufficient transmission power to persuade every node in the network that the adversary is one of its neighbors. When a node chooses an enemy node as part of its message route, the malicious node may either operate as a black hole by refusing to forward any of the messages it receives or it may selectively forward some messages to the wrong receiver while dropping the rest. In this study, we discuss the security vulnerability that occurred with the hierarchical routing protocols, and we suggest a detection system that is based on the received signal strength [26].

This is the first time that Junior et al. [27] offer a technique for detecting rogue nodes based on the signal intensity of sent messages. He mulled over the possibility of utilizing a geographic routing technique in which every node knows its position using GPS or another positioning technology. This work has a good amount of success in detecting malicious nodes. The fact that each node must obtain information about its position from the surrounding nodes is a drawback of this approach. J. Wang et al. [28] suggested a method to detect Sybil attacks based on RSS, paired with additional characteristics such that the nodes' ID number, position information, and nodes' power value, etc. The routing technique utilizes a hierarchical structure. M. A. Hamid presented a protection mechanism against the HELLO flood assault in [29]. The HELLO flood attack is defended against in this work by the introduction of bidirectional verification and multi route routing using a shared secret across sensor nodes. Each node in this network is able to compute a pairwise key using the shared secrets. The process of key production and distribution is the primary focus of this piece of art.

IV. PROPOSED DETECTION TECHNIQUE

In this section, the method for detecting suspicious CH that conducted attacks through the clustering technique of hierarchical wireless sensor networks is described.

Network Model

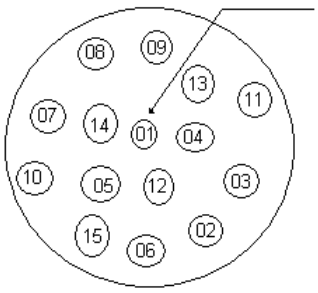
We are going to make the assumption that WSNs are static, homogenous (meaning that all of the nodes have the same hardware and software), and symmetric (meaning that node A can only connect with node B if and only if node B can communicate with A). The initial configuration of each node is the same [27]. (e.g., energy, transmission power, antenna height and antenna gain). Within this sensor area, they are able to identify each individual node thanks to their IDs. The Two-Ray Ground Model is used to describe the propagation of radio waves (Eq. –1).

$$P_r = \frac{P_t \times G_t \times G_r \times h_t^2 \times h_r^2}{L \times d^4} \quad (1)$$

In equation–1, P_t and P_r are transmitted and received power, G_t and G_r are Antenna Gain of the transmitter and receiver, h_t and h_r are Antenna Height of the transmitter and receiver, L is the system loss factor not related to propagation and d is the distance between transmitter and receiver [30]. It is assume that a node can be easily measure signal strength of a received signal. All nodes transmit packets with same power P_t to other nodes otherwise inform to recipient about transmitted power. Communication pattern within a cluster is single-hop and CHs to BS may be multihop depends on distance between them.

In addition to this, we take into consideration the fact that a node cannot be corrupted within a given amount of time after its deployment. Because when a person or agent deploys nodes in a sensor field, an adversary is unable to capture or tamper with any nodes on her presence without being detected. During this period of time, tm nodes will send a HELLO message to all of their neighbors in order to compile a database of neighbors that will be known as

the neighbor database. It consists of at least two fields, which are the Node ID and the Received Signal Strength (RSS) when it comes to receiving messages from its neighbors (fig. 1). A node will need a few seconds in order to construct a neighbor database [31]. The behavior of a node is considered abnormal if the node gets any message from its neighbors with a higher signal power than the value in the neighbor database. It is possible for a foe to seize control of this node and use their superior transmission power to win over further nodes. The clustering procedure will continue once tm has passed. A CH or elect status can be declared by a node using a manner similar to that used in LEACH [23]. A node may check the transmitted power of any other node within its radio range by simply sensing the wireless medium; this is because the wireless medium is broadcast in nature.



Node 01 Neighbor Database

Node ID	Reveive Power
14	3.21
04	3.11
...	.....
10	1.62

Fig. 1 All of node-01's radio-neighboring nodes, together with the neighbor-database they generate automatically at tm.

Trust Model

When evaluating the reliability of this detection method, we consider the following trust factors [27] [28]:

- The base station is stored in a secure location, so that it cannot be tampered with in any way.
- BS is the authority and controller of all activities that take place within WSN, and it does not have any resource limitations.
- There are no trust requirements placed on sensor nodes despite the fact that they are vulnerable to node capture threats. The BS is the authoritative source for any authentication and decision.

CH Detection Technique

We make the assumption that an adversary is capable of seizing a valid node or introducing a node with the correct ID. We look at two different methods of clustering: the dynamic clustering [23] methodology and the fixed clustering technique. In fixed clustering, the CH property of a node will not be altered until either the CH has died due to a shortage of power or an administrator modifies the CH property. The following is how the proposed detection technique for dynamic clustering actually works:

When a node receives CH advertisement from one or more nodes, the node will first validate the node ID and signal strength of the advertisement with its neighbor-database. If the node ID is already stored in the database, then it will compare the strength of the advertisement signal to the database of its neighbors. It is a sign of inconsistency if the node observes that the CH advertisement has sufficient power beyond the permitted range. Since there is no movement among the nodes, and each node always transmits packets with the same power P_t, as explained in section 4.1. The irregularity in the propagation of radio waves is to blame for any slight differences that may exist.

If the currently acquired signal strength is lower than the value in the neighbor database, then it is considered acceptable. On the other hand, if it is sufficiently large, the node needs to determine whether or not it is acceptable. The permissible power ratio is defined by us as ((present RSS - neighbor–database RSS) / neighbor–database RSS). If one node discovers that another node within its radio range is transmitting at higher signal intensity than usual, then this must be considered an anomaly. It is validated by the node using the information from other nodes.

The node will check the inconsistency of that CH by sending a message to all of its adjacent nodes. It provides a counterpoint to support the inconsistent behavior of the neighbors. The node was referred to as the sending node. The value of the counter increases whenever a supporting reply message that is called a supporting-message from neighbors is received. Because a radio receiver may detect high power from a sender due to some imbalance in the transmission hardware or irregularity in the propagation of radio waves or both, we take into consideration this form of verification from neighbors. The voting method reduces the amount of times that a false detection is made, as demonstrated in [32] and [33]. If the majority of nodes in close proximity to CH are able to detect a high transmission power from CH, then we can safely say that this is an abnormality.

Any suspicious behavior exhibited by a node ought to be picked up locally by the members or neighbors of a CH given that the technique for cluster formation is local. If the sending-node counter value is more than a certain threshold, also known as the suspicious threshold, it broadcasts to the other nodes the information that the CH is potentially malicious. The node communicates with the BS by sending a message concerning the suspicious behavior of the CH.

In the method known as fixed clustering, randomly selected member nodes of a cluster check the CH transmission power at regular intervals after being organized into a cluster. A random number r is produced by each node after a period of time that has been determined. If r is greater than rth, which is referred to as the random threshold, a node will only verify the CH power it possesses. When a node makes the decision to check the CH power, it does so by sensing the wireless medium and determining the strength of the signal sent by its CH. The current value of CH signal power is evaluated by the node and compared to the database of its neighbors. If the node detects that the received signal intensity from CH is now greater than the permissible power ratio, it will broadcast a message to all of its neighboring nodes

requesting that they check the power supplied by CH. It enables a supporting-message counter for its neighbors to use. Only the nodes that are part of the same cluster as you will check the CH transmitting power of your neighbors; the remaining nodes will ignore the message. When the counter value of the node goes beyond the suspicious threshold, a notice is sent to the BS as well as the other nodes.

Algorithm for neighbor–database of a node:

Step 1: A node sends Hello message to all its neighbors with its ID.
Step 2: The nodes within radio range reply with their ID.
Step 3: Node creates a table of neighbors for every received message with Node ID and signal strength of the message.

Algorithm for dynamic clustering:

Step 1: When a node *n* receives CH advertisement it checks this node ID and signal strength of the advertisement with neighbor–database.
Step 2: If the CH Node ID in its neighbor–database and signal strength of the CH advertisement within acceptable power ratio, do nothing.
Step 3: If node *n* detect CH signal power more than acceptable power ratio, send message to all neighbors to check the CH power.
Step 4: *n* set a counter to count for supporting message.
Step 5: Nodes within radio range of *n* check this CH power if it receives any message from this CH, otherwise ignore the message.
Step 6: If any neighbor node finds CH transmitted power exceeds acceptable power ratio, it sends a packet to node *n*, otherwise send nothing.
Step 7: *n* increases its counter after receiving of each message. When the counter value exceeds suspicious threshold, it informs other nodes and BS.

Algorithm for fixed clustering:

Step 1: After each time interval t_i, all nodes generate a random number *r*. Nodes (n_1, *n2*...), whose value of *r* greater than r_{th}, checks their CH power.
Step 2: If a node (say n_1) detects signal power of its CH is greater than acceptable power ratio, it broadcast this to all neighbors.
Step 3: n_1 open a counter to count for supporting message from neighbors.
Step 4: Neighbor nodes, which are member of n_1–cluster, check their CH power otherwise overlook the n_1 message.
Step 5: If a member node finds that CH transmitting power greater than acceptable power ratio, it sends a message to n_1, otherwise send nothing.
Step 6: n_1 increases the counter after reception of each supporting message.
Step 7: When the counter value exceeds suspicious threshold, it informs other nodes and BS.

Figure 2 (a), (b), and (c) depict the pseudo code for the suggested approach (c).

```
for node n: i to N
    send Hello_Msg_i to all n;
    open neighbor-database_ni(DB_ni);
    for node j to N (j≠i)
      if node j receive Hello_Msg_i
        send Hello_Msg_j to i;
      end if;
      measure RSS_j of Hello_Msg_j;
      insert value of j and RSS_j in DB_ni;
    end for
end for
```

Figure 2(a). Pseudo code for neighbor database

```
if node n_i receive CH_ADV of node n_j
    check j and RSS_j in DB_ni;
    if (j ∈ DB_ni)
      if (RSS_j > RSS_j(DB_ni))
        if ( check RSS_j > acceptable_power_ratio)
          open a counter c_i;
          send Msg_sus_j to all neighbor;
          for all neighbor n: k to m
            if (n_k receive CH_ADV of node n_j)
              if (check RSS_j > acceptable_power_ratio)
                send Msg_sus_j to node n_i;
              end if
            end if;
            increase c_i= c_i+1;
          end for;
          if (c_i≥ suspicious_threshold)
            send Msg to BS and other nodes about n_j;
          end if
        end if
      else
        start clustering process;
      end if
    end if
    if (j ∉ DB_ni)
      send Msg to BS and other nodes about n_j;
    end if
end if
```

Figure 2(b). Pseudo code for dynamic clustering

```
node n_i open a time couter t_n
    t_n >time_intervl t_i
    generate random number r;
    r > r_th
      check CH RSS_CH ;
      open a counter c_i;
      if (RSS_CH > acceptable_power_ratio)
        send Msg_sus_CH to all neighbor;
        for all neighbor n: k to m
          if (n_k ∈ CH)
            if (check RSS_CH > acceptable_power_ratio)
              send Msg_sus_j to node n_i;
            end if
          else
            do nothing;
          end if;
          increase c_i= c_i+1;
        end for;
        if (c_i≥ suspicious_threshold)
          send Msg to BS and other nodes about n_j;
        end if
      end if
```

Figure 2(c). Pseudo code for fixed clustering

V. SIMULATION DETAILS AND RESULTS

During simulation, the parameters of Mica2 [34] and its radio chip CC1000 [26] are utilized. They are detailed in Table 1 below. If the signal power of the packet is less than the receiver sensitivity, also known as the **receiver threshold** P_{Th} [26], a node won't be able to receive any packets sent by other nodes. We are working under the assumption that the nodes are distributed throughout the sensor field in a random manner. Every node decreased their transmission power (P_t) until it was 0 dBm. We decided to choose such a large amount due to the fact that the proposed work detects anomalies based on signal strength. By employing a high transmitted power, a foe attempts to attract the nodes in the sensor field. Therefore, the adversary-node is required to configure the transmitted power to be higher than the agreed-upon transmitted power P_t. The adversary-node will quickly lose its power as a result of this strategy. The figure in 3 depicts the typical number of nodes that are a given node's neighbors for a variety of sensor field sizes and densities of nodes. Fig. 3 is going to employ in order to determine the best possible value for the suspicious threshold.

Table 1. Parameters used in simulation

Transmitter Power – P_t	0 dBm
Antenna Gain – G_t, G_r	1
Antenna height – h_t, h_r	8.2 cm
System Loss – L	1
Receiver threshold – P_{Th}	– 98 dBm
Center frequency	868 MHz
Minimum time – t_m	10 Sec [15]
Acceptable power ratio	2%
Data sending Rate / Node	1 packet / 30 sec.
Cluster Time	1 hour
Malicious CH Power	1, 2, 3, 4, 5 dBm

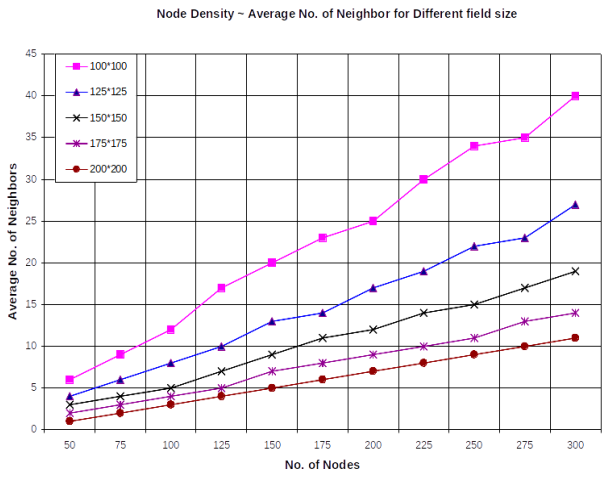


Figure 3. Average no. of neighbors of a node for different area

At start, every node will build its own neighbor database immediately following deployment, well under the time limit tm. After this, some nodes are chosen among the nodes that have been deployed in the sensor field to act as CHs, as shown in [23]. A CH will be selected at random to act as the malicious node. It has been decided to boost the transmission power of the harmful CH from 0 to 5 dBm. If a node determines that a CH is transmitting with a power ratio that is unacceptable, then it will open a counter to receive supportive messages from its neighbors. This CH is considered to be suspicious whenever its counter value is equal to or higher than the suspicious threshold. It was a successful investigation and detection. It is an example of unsuccessful detection where a node determines that a CH has transmitted more than the permitted power ratio but that the counter value is lower than the suspicious threshold.

Dynamic Clustering

For the purpose of making decisions regarding the detection of suspicious activity, we take into consideration two distinct kinds of suspicious threshold: (i) the dynamic suspicious threshold and (ii) the fixed suspicious threshold. The number of a node's neighbors is a factor that influences the dynamic suspicious threshold. The values of it change depending on the node you're looking at because each node has its own neighbor database. The importance of having a fixed suspicious threshold is established through the results of an empirical study of WSNs. The values of it are determined by the size of the sensor field and the typical number of nodes that surround a node. The field area and node density that are employed to identify potentially harmful CH during dynamic clustering are detailed in Table 2. In this particular instance, the typical number of nodes that are a node's neighbors is 17. (Fig. 3). The detection rate of a malicious CH is depicted in figures 4 and 5, which show the rate of detection for a dynamic suspicious threshold and a fixed suspicious threshold, respectively, for varying levels of transmitted power.

Table 2: Field area and node density for dynamic clustering

Sensor Field Area	100m × 100m
No. of Nodes	125
Average No. of Neighbor	17

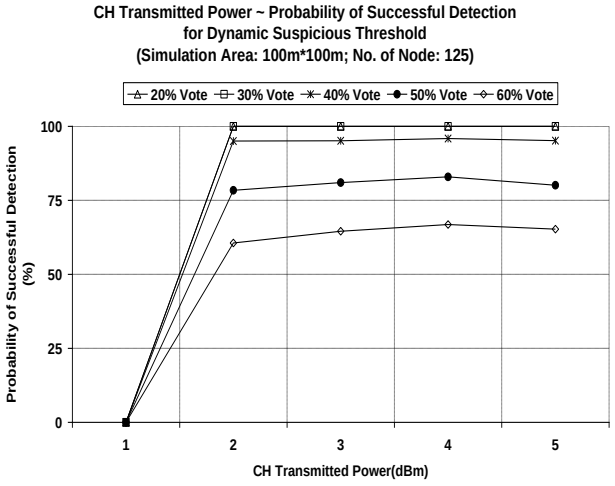


Figure 4. Detection probability for dynamic suspicious threshold

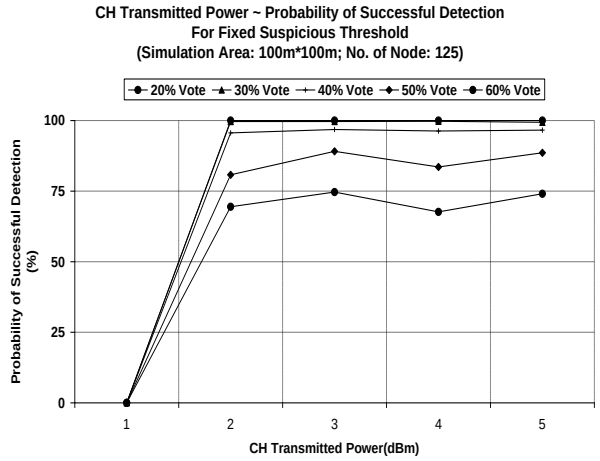


Figure 5. Detection probability for fixed suspicious threshold

It can be observed from figures 4 and 5 that the detection probability is almost the same for both a dynamic suspicious threshold and a fixed suspicious threshold. It is quite close to one hundred percent for both the 20% and the 30% suspicious threshold. In other circumstances, the detection rate drops since nearby neighbors aren't sending any supporting messages. A node that is located a significant distance from CH may not be able to successfully identify the high transmission power of CH since the receiving power is inversely proportional to the fourth power of distances (eq.-1). Additionally, nodes are unable to detect a 2% change in the signal strength while CH is transmitting at 1 dBm.

5.2 Set a Suspicious Threshold

It has been discovered through empirical research that, as a result of the random deployment of nodes, there are occasions when 20% or 30% of a node's neighbors are almost equal to 1. Because of this, the dynamic suspicious threshold could result in erroneous detection. The value of 20% and 30% no. of average neighbors (fig. 3) of a node are around 3 and 5 respectively for the area that was employed in the simulation. A node needs two more supporting messages from its neighbors in order to pass the 20% suspicious threshold. This value could also result in false detection if these three nodes are located within a certain distance of one another. As a result, the suspiciousness threshold for the region and nodes listed in Table 2 is set at thirty percent of neighbors who support messages. This value will serve as the basis for the fixed clustering.

5.3 Fixed Clustering

In this particular instance, the probability of detection is determined by the individuals who make up a CH. The results of an empirical investigation for the average number of member nodes associated with a CH are presented in Figure 6. In this scenario, the same region and nodes as those used in dynamic clustering are taken into consideration. The parameters that were used for fixed clustering are provided in Table 3. Every time a CH is randomly identified as being malicious, the transmitting power of that CH is increased from 0 to 5 dBm. The successful detection is seen in Figure 7 and occurs when 30% of the member nodes in a cluster identify their cluster head as being suspicious. It approaches a perfect score.

Table 3. Parameters for fixed clustering

Sensor Field Area	100m × 100m
No. of Nodes	125
Average No. of Neighbor	17
Random threshold r_{Th}	0.9
Percentage of CH	8%
Average No. Nodes/CH	10
Suspicious threshold	30% of Nodes per CH
Malicious CH Power	1, 2, 3, 4, 5 dBm
Simulation Time	1 hour
Checking time interval	5 minutes

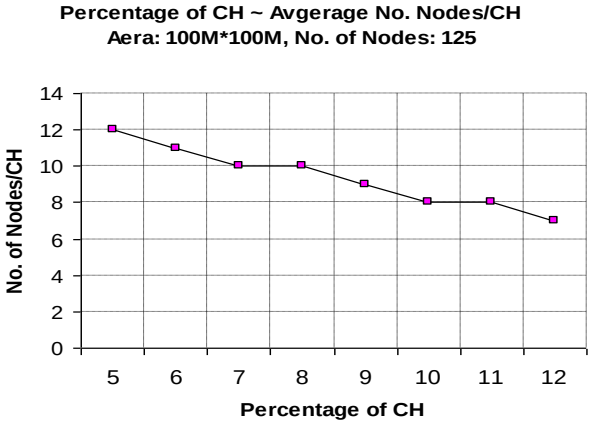


Figure 6. Average member nodes per CH for 100m*100m

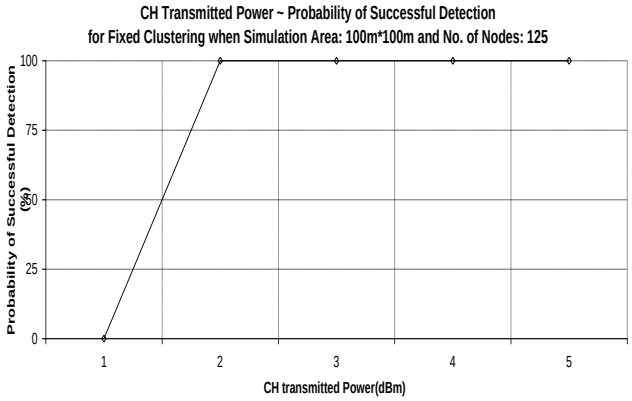


Figure 7. Detection probability of malicious CH for fixed clustering

5.4 Packet Transmission Overhead

Instead of measuring the amount of energy consumed, we look at how many extra packets a node needs to send out in order to identify a potentially malicious CH at the 30% threshold. Figure 8 depicts the packet overhead for dynamic clustering on a per-node basis, taking into account the area and nodes listed in Table 2. When a new cluster is formed with a malicious CH, the overhead is

measured per node to determine the total amount. When a node joins a cluster using dynamic clustering, it will only transmit one packet to the cluster head. A node will send 120 data packets to its CH in the course of one hour of cluster time. Therefore, a node will transmit 121 packets in the absence of any form of intrusion detection technique. According to figure 8, it has been discovered that a node will send a maximum of five additional packets if it finds any suspicious CH while the cluster is being set up. An hour has a maximum overhead of around 4% every packet, regardless of which node it comes from.

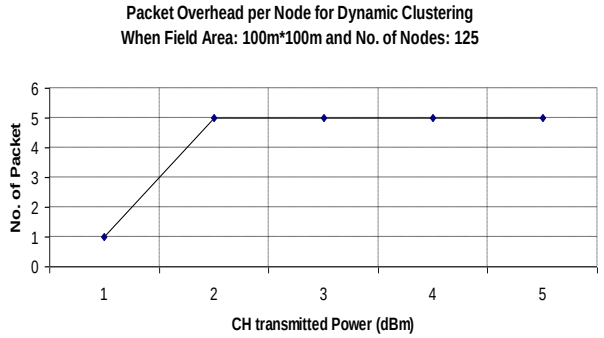


Figure 8. Packet overhead when new cluster start at Dynamic Clustering

Figure 9 illustrates the packet overhead that is incurred by each node during an hour of fixed clustering while a member node observes the activity of its cluster head. In order to calculate the overhead of the packets, we take into account the characteristics provided in Table 3. During the regular course of one hour's worth of simulation time, send 120 packets to its CH. If a node's CH is questionable, it will send an average of 9 extra packets than usual. The maximum amount of overhead that can be incurred by packets for each node is around 7.5%.

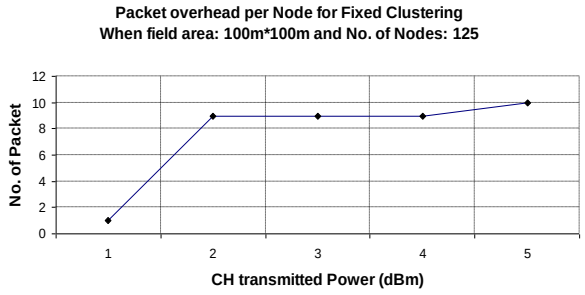


Figure 9. Packet overhead of fixed clustering for an hour

VI. DISCUSSION

The signal intensity that a node got from a CH is the most important criterion that needs to be considered in the suggested method for detecting suspicious CHs. As part of this research, sensor nodes collaborate with their surrounding nodes to identify a malevolent CH. This is the first piece of research that utilizes receiving signal power in order to identify a malicious CH in a hierarchical sensor network. The nodes monitor the amount of power that is being transmitted by their cluster leader. In other words, a node will identify a potentially malicious CH based on the strength of the received signal. According to the results of our simulation, the probability of the suggested plan being successful is heavily dependent on the encouraging messages received from its surrounding areas (fig. 4 and fig. 5). The rate of success decreases as the suspiciousness threshold increases. Therefore, the location of the nodes is of paramount importance.

The proposed method has a comparatively little impact on the communication overhead. For dynamic clustering, the fee is 4%, whereas the fee for fixed clustering is 7.5%. (sec–5.4). If a node detects any anomaly in the signal it is receiving, then it is necessary for it to communicate with other nodes. The neighbor database is stored on each node in this work. This database is an integral component of the routing method. As a result, the suggested work will not result in any additional storage overhead.

The security risks posed by sensor networks are substantially influenced by the routing method that they use [5]. However, because there are many distinct classes of routing techniques, an intrusion detection technique that was created for one category of routing is ineffective in other categories of routing. In addition, the dangers posed by wireless sensor networks to information security take many different forms. Therefore, a singular solution is not feasible. The receive signal power and the routing mechanism of hierarchical sensor networks are both utilized in the proposed detection technique. Comparing our work to other intrusion detection strategies that employ receive signal power and detect intruders for hierarchical routing techniques is one of the things that we do in this study.

Junior et al. [11] technique introduced for the first time to detect malicious nodes, which is based on the signal intensity of transmitted messages. He gave some thought to the geographical routing strategy, in which each node is aware of its position thanks to the use of GPS or another positioning technology. This experiment demonstrates a high degree of success in identifying malicious nodes. It is close to one hundred percent for high node density. The disadvantage of this approach is that each node needs to determine its position based on the positions of the other nodes.

A method to detect a Sybil attack synthetically was proposed by J. Wang et al. [28], and it is based on RSSI, combined with parameters such as the nodes' ID number, position information, and nodes' power value, etc. The methodology of the routing is hierarchical. An about 90% success rate can be expected when trying to identify a Sybil node. If the distance between nodes is more than a certain threshold, the success rate will be drastically lowered. Because of this approach, a Sybil node—a node that uses numerous identities—can be avoided. However, it is unable to defend hierarchical sensor networks from other types of routing attacks.

M. A. Hamid presented a defense against the hello flood attack [29]. In this work, a defense against a HELLO flood attack is developed by introducing bidirectional verification and multi way routing between sensor nodes while making use of a shared secret. In this case, every node is capable of computing a pairwise key using shared secrets. The concept of key distribution and key generation is essential to this body of work. The work that we have proposed is contrasted with many other intrusion detection techniques in Table 4.

Table 4. Comparison of the proposed work

Technique	Routing technique	Key Parameters	Defend Attacks	Success rate	Remarks
Junior's Scheme	Geographic	Received Signal Power	Hello Flood Attack	Almost 100%	• Depend on knowing node position • Success rate depend on node density. • Can prevent Hello Flood Attack but not Sybil, bogus routing information • Low communication overhead.
J. Wang's Scheme	Hierarchical	Received Signal Power	Sybil Attack	Average 90%	• Success rate depends on proximity between nodes. • Can prevent Sybil attack but not Hello Flood, Sink Hole etc. • Low power consumption
Hamid's Scheme	Hierarchical	Key Distribution	Hello Flood Attack	Not defined	• Need shared secret keys • Authentication technique identified intruder • Need multipath routing so high communication overhead • Success depend on no. of keys maintained by a node • High memory overhead due to store shared keys • Can prevent Hello Flood, Sink Hole etc but not Sybil attack.
Proposed Scheme	Hierarchical	Received Signal Power	Hello Flood Attack, Sinkhole Attack	Almost 100%	• Do not need information about node position. • Success rate depend on no. of neighbor nodes. • Low communication overhead. • No memory overhead • Can prevent Hello Flood Attack, Sinkhole Attack but not Sybil attack.

VII. CONCLUSION

A method for the detection of malicious CH in hierarchical wireless sensor networks is presented in this body of work. Using this strategy, normally functioning nodes in the nearby area are able to identify potentially malicious CH activity. Because of radio irregularities and hardware, our method has the drawback of a node's potential to receive an excessive amount of power from another node. The voting method lessens the likelihood of false detection but cannot eradicate it entirely. The mechanism for detecting suspicious cluster heads protects against a wide variety of routing attacks, including the Hello Flood attack and selective forwarding. The detection method is able to determine whether or not an adversary has attempted to lure nodes to their network through wormholes, sinkholes, or other similar mechanisms by employing a powerful transmitter. In a heterogeneous sensor network, the cluster heads are chosen from among some particularly resource-dense nodes. In the event that these exceptional nodes initiate a Hello Flood attack, the proposed method will be able to identify it by checking the cluster head signal power at regular intervals. Any method of authentication will incur a significant amount of additional compute and communication overhead. In order to reduce the burden of such communication, the base station will only verify the legitimacy of those nodes for which it has received a message indicating potentially malicious behavior. As part of our ongoing research, we are expanding the detection method to accommodate mobile nodes as well as other types of routing for WSN. In addition to this, we have an interest in developing a secure protocol for sensor

networks and protecting the network from other types of denial of service attacks such as Sybil, Wormhole, and others.

REFERENCES

[1] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. "A survey on sensor networks", *IEEE Communications Magazine,* **40(8):102–114**, August **2002**.

[2] A. D.Wood, J. A. Stankovic, "Denial of service in sensor networks," *Computer,* vol. **35**, no. 10, pp. **54–62, 2002**.

[3] T. Roosta, S. Shieh, S. Sastry, "Taxonomy of Security Attacks in Sensor Networks and Countermeasures", *In Proc. of the 1st Int. Conference on System Integration and Reliability Improvements,* **vol 25, p. 94, 2006**.

[4] S. Rajasegarar , C. Leckie , M. Palaniswami, "Distributed anomaly detection in wireless sensor networks**"** *in Proceedings of Tenth IEEE International Conference on Communications Systems **IEEE ICCS,*** **2006**.

[5] C. Karlof, D. Wagner, "Secure Routing in Sensor Networks: Attacks and Countermeasures," *in Ad Hoc Networks,* volume 1, issues 2--3 (Special Issue on Sensor Network Applications and Protocols), Elsevier, September, **pp 113-127, 2003**.

[6] J. N. Al-Karaki, A. E. Kamal. "Routing techniques in wireless sensor networks: a survey", *Elsevier Ad Hoc Networks Journal,* **pp. 325–349, 2005**.

[7] H.A. Obeidat, Y.A.S. Dama, R.A. Abd-Alhameed, Y.F. Hu, R. Qahwaji, J.M. Noras, S.M.R. Jones, "A comparison between vector algorithm and CRSS algorithms for indoor localization using received signal strength," *Applied Computational Electromagnetics Society Journal,* **vol. 31 pp. 868–876, 2016.**

[8] X. Wang, P. Xu, W. Xue, "Research on online signal matching of indoor positioning based on AL-KNN algorithm," *In Proceedings of International Applied Computational Electromagnetics Society Symposium* China, **pp. 1–4, August 2017**.

[9] N.M. Drawil, H. M. Amar, O. A. Basir, "GPS localization accuracy classification: A context-based approach", *IEEE Transaction of Intell. Transp. System,* **vol. 14, pp. 262–273, 2013**.

[10] Y. Zhang, W. Wu, Y. Chen, "A Range-Based Localization Algorithm for Wireless Sensor Networks," *Journal of Communication Network,* **vol. 7, pp. 429–437, 2005**.

[11] H. Xiong, Z. Chen, B. Yang, R. Ni, "TDOA localization algorithm with compensation of clock offset for wireless sensor networks", *China Communication,* **vol. 12, iss. 10, pp. 193-201, 2015**.

[12] H. Shen, Z. Ding, S. Dasgupta, C. Zhao, "Multiple source localization in wireless sensor networks based on time of arrival measurement," *IEEE Trans. Signal Processing,* **vol. 62, pp. 1938–1949, 2014.**

[13] X. Sheng, Y. H. Hu, "Maximum likelihood multiple-source localization using acoustic energy measurements with wireless sensor networks," *IEEE Trans. Signal Processing,* **vol. 53, pp. 44–53, 2005.**

[14] M. Malajner, D. Gleich, P. Planinšič, "Angle of arrival measurement using multiple static monopole antennas," *IEEE Sens. Journal,* **vol. 15, pp. 3328–3337, 2015.**

[15] W. Mardini, Y. Khamayseh, A. A. Almodawar, E. Elmallah, "Adaptive RSSI-based localization scheme for wireless sensor networks," *Peer-to-Peer Networking and Applications,* **9, pp. 991–1004, 2016**.

[16] C. W. Trueman, D. Davis, B. Segal, "Relationship between the path loss exponent and the room absorption for line-of-sight communication," *The Applied Computational Electromagnetics Society Journal,* **vol. 24**, **Iss. 4**, **pp. 361–367, 2009**.

[17] S. Kurt, B. Tavli, "Path-Loss Modeling for Wireless Sensor Networks: A review of models and comparative evaluations," *IEEE Antennas Propagation Magazine*,**59, pp. 18–37, 2017.**

[18] M. Meenalochani, S. Sudha, "Fuzzy based estimation of received signal strength in a wireless sensor network," *In Proceedings of the ACM International Conference Proceeding Series; Association for Computing Machinery*, NY, USA, **pp. 624–628, 2015.**

[19] M. Meenalochani, S. Sudha, "Jammed Node Detection and Routing in a Multihop Wireless Sensor Network Using Hybrid Techniques," *Wireless Personal Communication, Springer,* **104, pp. 663–675, 2019**.

[20] S. MakalYucedag, A. Kizilay, "Time domain analysis of ultra-wide band signals from buried objects under flat and slightly rough surfaces," *Applied Computational Electromagnetics Society Journal,* **28(8), pp. 646–652, 2013.**

[21] A. Al Sayyari, I. Kostanic, C.E. Otero, "An empirical path loss model for Wireless Sensor Network deployment in a concrete surface environment," *In Proceedings of the IEEE 16th Annual Wireless and Microwave Technology Conference, WAMICON,* NY, USA, **pp. 13–15, April 2015**.

[22] M. Passafiume, S. Maddio, M. Lucarelli, A. Cidronali, "An enhanced triangulation algorithm for a distributed RSSI-DoA positioning system," *In Proceedings of the 13th European Radar Conference, EuRAD, London,* **UK, pp. 185–188, 2016**.

[23] W. R. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy efficient communication protocol for wireless microsensor networks," *in 33rd Annual Hawaii International Conference on System Sciences,* **pp. 3005–3014, 2000**.

[24] S. Lindsey, C. S. Raghavendra, "PEGASIS: Power Efficient GAthering in Sensor Information Systems," in the *Proceedings of the IEEE Aerospace Conference,* **pp. 3-1125-3-1130, 2002**.

[25] A. Manjeshwar and D. P. Agrawal, "TEEN: A Protocol for Enhanced Efficiency in Wireless Sensor Networks," in the Proceedings of the *1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco,* **CA, April 2001.**

[26] Chipcon. SmartRF CC1000: http://www.chipcon.com/files/CC1000_Data_ Sheet_2_1.pdf, 2003.

[27] Waldir R. P. J´unior, T. H. de Paula, F. H. C. Wong, "Malicious Node Detection in Wireless Sensor Networks", *Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04),* 2004.

[28] J. Wang, G. Yang, Y. Sun, S. Chen, "Sybil Attack Detection Based on RSSI for Wireless Sensor Network", *International Conference on Wireless Communications, Networking and Mobile Computing,* **pp. 2684-2687, 2007.**

[29] M. A. Hamid, M. Mamun-Or-Rashid, C. S. Hong, "Routing Security in Sensor Network: HELLO Flood Attack and Defense", *Proceedings of IEEE International Conference on Next-generation Wireless Systems,* **pp. 77 – 81, 2006**.

[30] T. S. Rappaport. "Wireless communications: principles and practice", **Prentice Hall, 2nd edition, 2002**.

[31] J. Polastre, J. Hill, D. Culler, "Versatile low power media access for wireless sensor networks," *in SenSys '04: Proceedings of the 2nd international conference on Embedded networked sensor systems*. **USA: ACM Press, 2004**.

[32] T. Park and K. Shin, "LiSP: A lightweight security protocol for wireless sensor networks," in *ACM Transactions on Embedded Computing Systems,* **Vol. 3, No. 3, pp. 634-660, August 2004**.

[33] K. Ren, W. Lou, Patrick J. Moran, "A Proactive Data Security Framework for Mission-Critical Sensor Networks," *in Proceeding IEEE Military Communications conference, MILCOM 2006,* **pp. 1-7, 2006.**

[34] MICA2: Crossbow Technologies Inc. 100 3317.73 http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/MICA2_Datasheet.pdf , **2009**.

