AN ANTI-JAMMING TECHNIQUE BY JAMMER LOCALIZATION FOR MULTI-CHANNEL WIRELESS SENSOR NETWORKS

Maoyejatun Hasana[1] and Hossen Asiful Mustafa[2]

[1]Department of Computer Science and Engineering, Asian University of Bangladesh, Dhaka, Bangladesh
[2]Institute of Information and Communication Technology (IICT), Bangladesh University of Engineering and Technology (BUET), Dhaka, Bangladesh

ABSTRACT

A jamming attack is a serious security threat for Wireless Sensor Networks (WSN) in which adversaries intentionally emit radio frequency signals to corrupt ongoing transmission. Several anti-jamming techniques have been devised as countermeasures against jamming attacks. These techniques detect jamming relying on the parameters such as Packet Delivery Ratio (PDR), Packet Send Ratio (PSR), Received Signal Strength Indication (RSSI), and Signal-to-Noise Ratio (SNR). On the other hand, energy efficiency is a significant issue for WSN and is a dominating factor for network lifetime. To prolong the network lifetime, WSN is organized into clusters where each cluster head transmits aggregated data to the base station directly or using multi-hop. In this research work, a jamming attack in a clustering-based WSN is investigated. Jamming attack in a clustered WSN affects drastically and makes clusters ineffective. As a result, WSN may experience delay in transmission, and a reduction in network throughput. To overcome jamming attacks, an effective jamming localizing scheme is proposed where parameters such as Jamming Signal Strength (JSS), PDR, etc., are considered in detecting jamming attacks, and then the jammed region is localized by finding convex hull using detected jammed nodes. To continue transmission in the presence of jamming, a cluster-based multi-channel assignment technique is also proposed to avoid the channels that are thwarting transmission efficiency and to select a new channel for the jammed cluster dynamically. The simulation results reveal the efficiency of the proposed scheme in identifying the presence of the jammer in the network, reduction in packet loss due to jamming attack, and this improving throughput.

KEYWORDS

Network Protocols, Wireless Sensor Network, Jamming Attack, Anti-jamming technique

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are large-scale networks with low-cost, small-size, low-power, and limited processing sensor nodes which are densely and randomly deployed in various kinds of environments such as medical and health care, environment and ecological monitoring, home and building automation, industrial monitoring, and battlefield [1], [2]. WSNs have generated tremendous interest among researchers because of their potential usage in a wide variety of applications. Despite many opportunities the wireless sensor networks provide, using WSN technology comes with great challenges. Handling such a wide range of applications raises some key issues of WSNs that need to be addressed, namely- energy efficiency [4], [5], fault-tolerance [30], scalability, and security [41].

Sensor nodes are battery-powered and are expected to be used heavily in remote and inaccessible areas where frequent changing or recharging of batteries is inconvenient, impractical, or even impossible. Therefore, minimizing the energy consumption of the sensor nodes is a challenging issue that needs to be taken into consideration. Thus, using solutions for prolonging the lifetime of the sensor nodes is crucial in WSN. Several studies show that the energy consumption due to collisions, overhearing, over-emitting, and idle listening [31] is greater than that of sensing or processing sensed data [7]. Without any energy-efficient scheme, sensor nodes would deplete energy faster than expected; so it is essential to guarantee to conserve energy so that the network lifetime can be extended to reasonable times.

Clustering [3] WSN is an effective way to minimize energy consumption by sending aggregated data toward the base station in order to reduce the number of messages transmitted to the base station. Some of the popular clustering schemes such as LEACH [23], PEGASIS [24], TEEN [37], APTEEN [38], HEED [39], TL-LEACH [25], and EEUC [26]. Security threats such as jamming attacks in a clustered WSN invalidate the original purpose of clustering, i.e., increase the energy consumption of the sensor network and thus degrade the network's overall performance. A jamming attack is one kind of Denial-of-Service (DoS) attack in WSN, which disrupts the existing wireless communications by decreasing the signal-to-noise ratio at the receiver sides through the transmission of interfering wireless signals [32]. Most of the existing works [6-12] focus on the detection of jamming attacks and localization of the jammer, but they do not discuss efficient data transmission in the presence of jamming attacks. Hence, a secured energy-efficient scheme is necessary to ensure smooth data transmission and the durability of the sensor network in the presence of jamming attacks. The basic idea is to use a different channel when the cluster detects that it is jammed and to avoid the jammed region while sending aggregated data to BS using multi-hop. The specific contributions of this work are as follows:

- A cluster-based jamming detection scheme is presented which, unlike most centralized jamming detection mechanisms, is a semi-distributed jamming detection technique. The BS does not need to worry about the presence of the jammer. The task of detecting jamming attacks is entirely assigned to the Cluster Heads (CHs), which makes it an efficient and fast jamming detection scheme over centralized and distributed jamming detection schemes.
- Instead of finding the true position of a jammer, an approximate jamming region is computed by the CHs of jammed clusters so that CHs can avoid the jammed region while sending aggregated data to BS using multi-hop. A method based on finding a convex hull is used to estimate the jamming region. Because the CH estimates the jammed region that only falls inside its cluster, the energy consumption of calculating the jammed area is minimized.
- A cluster-based multi-channel assignment scheme is presented. Instead of waiting for the decision of BS to change the channel during jamming attacks, this scheme is faster to change the channel of the jammed cluster, thus providing an efficient data transmission.
- Finally, a set of experiments is conducted on real sensor motes to see the performance of the proposed scheme.

The rest of the paper is organized in the following manner. Section 2 reviews the background related to various clustering techniques for energy-efficient routing and existing anti-jamming techniques for seamless data transmission. Section 3 presents the proposed multi-channel anti-jamming technique. Section 4 presents the performance analysis of the proposed anti-jamming technique through simulation results. Performance evaluation in terms of network throughput, PDR, packet loss, latency, and energy efficiency is investigated. Finally, Section 5 draws conclusive remarks on the results.

2. BACKGROUND AND RELATED WORK

2.1. Jamming Attacks in WSN

Wireless communication, which is susceptible to radio interference, is vulnerable to serious security threats such as jamming. There are several types of jammers that may be used to disrupt wireless transmission. In [22], Xu et al. proposed four types of jammer models, namely: constant jammer, deceptive jammer, random jammer, and reactive jammer. Localizing a jammer is an important task, which not only allows the network to actively exploit a wide range of defense strategies but also provides important information for network operations in various layers. For example, a routing protocol can choose a path that does not fall in the jammed region to avoid energy consumption caused by failed packet deliveries. Moreover, once a jammer's location is identified, one can eliminate the jammer from the network by removing it physically or choosing an appropriate technique to isolate it.

2.2. Jammer Localization and Defense Strategies

Localization [12] is defined as the estimation of the position of an unknown node, sometimes with the help of nodes with known positions. Localization in WSNs is not only an important component for a variety of emerging applications, including military applications [13], healthcare [14], environment monitoring [15], etc., but also a key issue for detecting and localizing jammers. Generally, the localization techniques are devised considering the network size, usage of anchor nodes, indoor localization, and mobility of the sensor nodes. Range-based approaches measure distance by using an angle of arrival (AoA) [27], time of arrival (ToA) [27], time difference of arrival (TDoA) [27], received signal strength (RSSI) [16] and measure the effectiveness of jamming using packet delivery ratio (PDR), packet send ratio (PSR) [28], and signal-to-noise ratio (SNR) [29]. Range-free approaches use connectivity information among the sensor nodes to determine the position of unknown nodes.

Pelechrinis et al. [6] proposed jammer localization by measuring PDR. The authors observed that PDR has lower values when a jammer is very close to victim nodes. A gradient descent search is used to locate the adversarial node. In [40], signal-to-jamming-plus-noise ratio (SJNR) at a targeted node is used to localize the jammer. The minimum value of SJNR indicates the presence of a jammer. In [8], a reactive jammer is localized by measuring PDR. The observed PDR at time t is calculated by counting the ratio of correctly received packets over the total number of transmitted packets. To determine the number of correctly received packets, the receiver checks the frame check sequence of all received packets and if it is correct, increments a counter. In [9], Sun et al. proposed a jammer localization scheme, CrowdLoc, by collaboratively collecting the measurements of RSS. CrowdLoc works in three phases. The sensor nodes at the boundary of the jamming region are termed Crowds, which measure RSS of the jammed area. Crowds, in turn, make a network to share the recorded measurements of RSS. Finally, Crowds as Estimator estimates the position of the jammer using Range-based Jammer Localization (RJL) which first estimates the distance between the jammer and the sensing node by using Equation 1 and then evaluates the approximation value of the jammer's position using linear approximation.

$$d_i = 10^{\frac{(-r_i + PL_R + X_g)}{10\lambda}} . d_R \qquad (1)$$

Where r_i refers to the recorded RSS value at the ith sensing node, PL_R is the path loss at the reference distance d_R, and λ is the path loss exponent. X_g is a normal random variable with zero mean, reflecting the attenuation caused by flat fading, and d_i refers to the estimated distance between the jammer and the i-th sensing node.

Catch the Jammer (CJ) [10] is an efficient jammer localization scheme where sensor nodes collaborate with each other to compute the coordinates of the jammer based on the received signal strength. CJ uses Jammed Area Mapping Service [11] to receive the coordinates of the victim nodes, and based on the victim nodes' location information, CJ constructs a convex hull and then selects a pair of nodes that has a maximum diameter. CJ identifies the midpoint of diameter as the jammer's estimated position.

Zhu et al. [17] proposed three anti-jamming techniques for different jamming conditions. In severely jammed areas, the nodes adopt a heavy anti-jamming technique, whereas in slightly jammed areas, the nodes adopt light anti-jamming techniques. Based on jamming conditions, transmission power adjustment, error correcting code, and channel hopping are used as anti-jamming techniques. Mustafa et al. [18] addressed the problem of multipath selection under the jamming condition and proposed a jamming resilient path availability algorithm. Liu et al. [19] addressed the jammer localization problem as a non-linear optimization problem and proposed jammer localization by exploiting the JSS directly. Rahman et al. [20] proposed a fast mapping technique for the jammed region where based on the received notification from sensor nodes, the base station maps the jammed region. Liu et al. [21] addressed the problem of localizing a jammer and solved this problem by proposing an adaptive Least Squares (LSQ)-based algorithm that estimates the jammer's location by utilizing the changes in hearing range and sending a range of neighboring nodes caused by jamming.

To address jamming, Xu et al. [22] proposed a two-phase strategy: retreat from the interferer and compete with the interferer; power control and code throttling are used to compete against jammers; channel surfing and spatial retreats are used as evasion defense strategies. Two types of channel surfing are presented- coordinated channel switching and spectral multiplexing. In a coordinated channel switch, the entire network changes its channel to a new channel. In spectral multiplexing, nodes located within a jammed area move to safe regions and stay connected with the rest of the network. However, if the sensor nodes are stationary, spectral multiplexing cannot be used, and switching the entire network to a new channel may introduce latency as the network size increases.

Ganeshkumar et al. [33] presented a jamming detection framework to detect the intrusion of jammer and the presence of jamming in a cluster-based WSN. The authors used PDR and RSSI as the jamming detection metrics and proposed a three-step framework, such as verification, validation, and auditing, to detect both jammer intrusion and jamming. Every CH has to maintain look-up tables for verification, validation, and auditing. The verification step uses the look-up tables to determine the type of source node and identify whether the source node is a legitimate node, a new node, or a jammer node. When the source node moves from one cluster to another, the validation step authenticates whether the source node belongs to any of the available clusters or not. The auditing step determines the behavior of the members in a cluster by observing the PDR and RSSI periodically.

This research work focuses on detecting and mitigating jamming attacks in a cluster-based sensor network and proposes a multi-channel anti-jamming technique that allows clusters to transmit data in the presence of the jammer.

3. THE PROPOSED MCALJ: MULTI-CHANNEL CLUSTERING-BASED ANTI-JAMMING BY LOCALIZING JAMMER

The proposed multi-channel clustering-based anti-jamming technique for WSNs by localizing jammer (MCALJ) is divided into four phases. These are cluster formation, jammer localization, channel selection, and data transmission in the presence of jammer in the network. MCALJ considers a clustering network where the organization of clusters and selection of CHs algorithms are derived by modifying LEACH [23] and EEUC [26]. An efficient multi-channel clustering-based anti-jamming technique has been developed to switch channels for the jammed cluster and continue data transmission in the presence of jamming. MCALJ reduces packet loss, increases network throughput and packet delivery ratio, and reduces energy consumption under jamming conditions.

The first phase is the cluster formation phase where CHs are selected based on the residual energy of each node, and each CH finds one or more neighbors who are nearer to the BS. Sensor nodes join a cluster based on the received signal strength from a CH. In the jammer localization phase, the jammed region is identified so that CH avoids the jammed region while transmitting data to BS via one or more CHs. In the channel selection phase, the channel selection algorithm is presented. In the data transmission phase, both intra-cluster and inter-cluster communications are discussed.

3.1. Cluster Formation

3.1.1. System Model

Let N nodes be uniformly deployed over a certain area by $G = (V, E)$, where V is the set of all vertices $(V = v_1, v_2 .... v_n)$ and E is the set of edges which represent the possible direct communication link between sensor nodes. *BS* represents the Base Station. The base station is placed on the top center of the monitoring area. The following assumptions are taken into consideration:

a) Sensor nodes are deployed uniformly in a 2-dimensional plane.
b) Sensor nodes are equipped with an omnidirectional antenna.
c) Intra-cluster communication is one-hop and inter-cluster communication is multi-hop since sensor nodes may not be able to communicate directly with the base station due to their limited transmission range.
d) A unit disk model is used as a radio model, and radio signal propagation is considered as free space propagation. In the unit disk model, two sensor nodes can communicate with each other if their Euclidean distance $d(u, v)$ is not greater than the transmission range.
e) Deployed sensor nodes are homogeneous, i.e., they have the same radio coverage radius R.
f) Sensor nodes know the position of the base station.
g) Sensor nodes are not equipped with GPS.
h) A jammed node cannot be a cluster head.

The cluster-based WSN works in two phases: the setup phase and the steady-state phase. The setup phase includes the selection of CHs, finding neighbor CHs who will act as relay CHs, and giving cluster members a fixed time slot for sending data. In the steady-state phase, intra-cluster communication and inter-cluster communication take place. In this work, unequal clusters are considered. The CHs near the BS have smaller clusters than the CHs that are far from BS. This is because CHs nearer to BS are likely to spend high energy than the farther CHs, as the

communication between CHs is considered multi-hop. A CH near to BS not only aggregates data from its cluster members but also acts as a relay node for the CHs which are far from the BS.

3.1.2. Cluster Head Selection

The cluster head selection is based on the residual energy of each node, and the task of being cluster head is rotated among sensor nodes in each round trip. During the setup phase, a sensor node becomes tentative CH with a probability less than T_p, which is a random number between 0 and 1. Each tentative CH then starts a competition to become a CH by sending a competition head packet, *CompeteHeadPkt*, across the network. The tentative CH n_j, who receives the competition head packet from the tentative CH n_i, checks if n_i falls inside its competition range. If it is, it marks the n_i as a competitor. If a tentative CH has one or more competitors, it sorts them according to their residual energy and compares its residual energy with the competitor who has the highest residual energy. Finally, the tentative CH with higher residual energy becomes a final CH. The competition range of a sensor node is a function of its distance to the base station. Two tentative CHs compete with each other to become the final head if they fall in each other's competition range. Suppose, R_{max} is the maximum competition range which is predefined. The competition range of a sensor node is calculated using Equation 2.

$$R_c = (1 - \beta\ (d_{max} - d(n_i, BS))/(d_{max} - d_{min}))R_{max} \qquad (2)$$

Here, d_{max} and d_{min} are the maximum and minimum distance between sensor nodes and BS, respectively, $d(n_i, BS)$ is the distance between node n_i and *BS*, and β is a constant coefficient between 0 and 1. With a proper choice of d_{max}, d_{min}, R_{max} and β, *the* sensor network's energy consumption can be mitigated as fewer clusters in a large network can have greater energy consumption. On the other hand, more clusters in a small network can also have greater energy consumption. By setting d_{max}, d_{min}, R_{max} and β, the size of the cluster can be calculated. The final cluster heads are selected from tentative cluster heads by using Algorithm 1.

Algorithm 1 Cluster Head Selection

1: μ = uniform(0, 1)
2: **if** $\mu < T_p$ then
3: *isTentativeHead* = True
4: **end if**
5: **if** *isTentativeHead* == True then
6: Send *CompeteHeadPkt*(ID_i, R_{ci}, RE_i)
7: **end if**
8: **if** $d(n_i, n_j) < R_{ci}$ OR $d(n_i, n_j) < R_{cj}$ then
9: Add n_j to COMPETITORS(n_i)
10: **end if**
11: Sort COMPETITORS(n_i) according to residual energy
12: *FinalHead* = COMPETITORS(n_i) with the highest residual energy
13: **End**

3.1.3. Identifying Relay Cluster Heads

Since the network is large, the farther CHs from BS will not be able to send the aggregate data to BS directly. In this case, aggregate data must be sent via one or more CHs. When a CH has data to send to BS, it finds one or more relay CHs that have a smaller distance to BS than it has. If it finds two or more such CHs, it will select one of them based on their residual energy and send aggregate data through that CH. The idea is adopted from PEGASIS [24] where sensor nodes

form a chain to send data to BS. Here, instead of every node forming a chain, CHs form a chain to send aggregate data to BS. A CH finds relay CHs by using Algorithm 2. A CH selects a relay CH among its neighbor CHs which has the higher residual energy. A CH n_j, is a neighbor of the CH n_i, if they are within each other's hearing range and the n_j's distance to BS is also less than n_i's distance to BS. If it is, then the CH n_i considers CH n_j as one of its neighbors. After finding all such neighbors, CH n_i chooses the relay CH based on the residual energy.

3.2. Jammer Localization

3.2.1. Jamming Model

A jammer is defined as an individual who is intentionally obstructing legal wireless communication. It is treated as an active attacker depending upon its intentions and actions. In this work, the jamming model consists of a constant jammer which is placed close to a sensor node and continuously sends a high rate of packets in high transmission power so that sensor nodes find the channel busy all the time and cannot send legitimate data to CH.

Algorithm 2 Relay CHs Selection

For each cluster head $n_i \in N_{CH}$
  Calculate $d(n_i, n_j)$
  Calculate d(n_i, BS) and $d(n_j, BS)$
  if $d(n_i, n_j) <= k*R_{ci}$ AND $d(n_j, BS) < d(n_i, BS)$ then
    Add n_j in CHNeighbor(n_i)
  end if
Sort CHNeighbor(n_i) according to residual energy
End

3.2.2. Jamming Detection

There are various jamming detection techniques discussed in the literature. A jamming attack can be detected using received signal strength, carrier sensing, packet delivery ratio, packet send ratio, signal-to-noise ratio, energy consumption amount, etc. In this work, jamming signal strength (JSS) with packet rate are used as jamming detection metrics. Here, the packet rate is the rate at which a legitimate node is getting jammed packets, and it is termed as Bad Packet Rate (BPR).

Under jamming conditions, the sensor nodes can be classified into three categories: (i) highly jammed nodes, (ii) loosely jammed nodes, and (iii) non-jammed nodes. Sensor nodes that are very close to a jammer and unable to access the channel completely are termed as highly jammed nodes. Loosely jammed nodes are boundary nodes of a jammed node. Due to the path-loss and shadowing phenomenon in radio signal propagation, some of the boundary nodes of the jamming area are considered as loosely jammed nodes. Loosely jammed nodes are capable of accessing the channel with some interference. Non-jammed nodes are unaffected nodes by jamming as they are outside of the jamming region.

Algorithm 3 Jamming Detection Algorithm

μ = uniform(0,1)
JSS = measureRSS()
BPR = measureBPR()
if $JSS \geq \tau_{jss}$ then
  isJammed = TRUE

```
6:      end if
7:      if  isJammed == TRUE and BPR > τ_bpr  then
8:          channelState = BAD
9:          SEND_SOS()
10:         changeChannel()
11:     end if
12:     if  JSS < τ_jss  AND BPR > τ_max  then
13:         isJammed = TRUE
14:           SEND_SOS()
15:           changeChannel()
16:       end if
17:    end if
```

Algorithm 3 shows the proposed jamming detection procedure. At any time t_j, a sensor node may start receiving packets with high received signal strength. If the RSS is higher than the predefined threshold value τ_{jss}, it then primarily detects jamming. Receiving high RSS does not always mean jammed, so for a time duration t_d, the sensor node checks whether it is getting an unusually bad packet rate. If it is getting unusual BPR for a time duration t_d, it considers itself jammed and sends a jammed packet, namely an SOS packet, with high energy to its CH. An SOS packet consists of measured jamming signal strength, link quality information, and coordinates of the jammed node. It may happen that the jamming signal is below the predefined threshold value, but some nodes are still getting unusual BPR. In this case, if a node is getting BPR greater than a predefined number of packets, τ_{max}, it considers itself jammed and sends the SOS packet across the network so that it reaches its CH.

Since the intra-cluster communication is one hop, the SOS packet should reach directly to CH; however, because of the presence of a jammer, the transmission range of jammed nodes may reduce to a certain level which in turn may prevent the SOS packet from reaching directly to CH. So, there may happen two scenarios: CH received the SOS packet, or CH did not receive the SOS packet. If the cluster members start receiving channel-switching packet and start operating in the new channel, it means CH received the SOS from the jammed nodes. In this case, both highly and loosely jammed nodes will not receive the jammed packets anymore.

But, if CH did not receive the SOS packet for some reason, then loosely jammed nodes would not receive the channel switching packet from the CH. In this case, loosely jammed nodes that are still getting high BPR will send SOS packets to their CH.

Using Equation 3, CH maps the received JSS to a numerical value: 0 or 1, where 1 represents the current channel as bad, and 0 represents the current channel available.

$$Channel_{avail} = \begin{cases} 1 & when\ JSS_i > \tau_{jss}\ \text{OR BPR} > \tau_{max} \\ 0 & otherwise \end{cases} \quad (3)$$

After receiving all $Channel_{avail}$ from its cluster members, CH changes the current channel using Algorithm 4. CH calculates a decision factor, d_f, which is the ratio of the total number of received $Channel_{avail}$ from the jammed cluster members and the total number of cluster members. If d_f is lower than the acceptable jamming J_a, CH switches to a new channel and sends a channel-switching packet across the network.

Algorithm 4 Channel Availability

```
for each cluster member i ϵ CH_j
    if JSS_i > τ_jss OR BPR > τ_max then
        countJSS++
    end if
end for
d_f =(countJSS / countClusterMembers)*100%
if d_f ≥ J_a then
    Send ChannelSwitchingPkt(currentChannel, newChannel)
    changeChannel()
end if
```

3.2.3. Jammer Localization

Localizing jamming attacks is challenging but important for building a secure wireless sensor network. This work focuses on localizing the jamming region rather than locating the true position of a jammer. An estimated position may be calculated from the derived jamming region. By identifying the jammed region, a CH may avoid the jammed region while sending aggregated data to BS via one more CHs. When a node detects jamming, it sends an SOS packet to its CH, as discussed earlier. This SOS packet consists of the location of the jammed node, measured JSS, and link quality information. The CH extracts the received SOS packets to get the coordinates of jammed nodes and sorts the jammed nodes by their JSSs. A jammed node is near the jammer if the measured JSS is higher than a threshold τ_{jss}. If the JSS is close to receiver sensitivity, then the jammed node is around the boundary of the jamming region. The CH then eliminates the highly jammed nodes from the jammed nodes stack. After reducing the jammed nodes, the CH sorts the location of the jammed nodes by their y-coordinates and finds the convex hull, which is a set of jammed nodes that form the smallest convex polygon where every jammed node is either on the boundary of the polygon or inside the polygon. Highly jammed nodes are being eliminated from the stack to avoid unnecessary computation during finding a convex hull.

To find a convex hull, Graham Scan Algorithm [42] is used. The algorithm proceeds with a jammed node with the lowest y-coordinate. Suppose J_0 is the node with the lowest y-coordinate. The remaining jammed nodes (J_1, J_2, J_3,…,J_n) are sorted by their polar angles relative to J_0 from smallest to largest. The iteration starts from J_0 in counterclockwise order by finding a node that makes a left turn. Figure 1 shows the process of finding the convex hull for the jamming region. If a jammed node makes the right turn, it is eliminated from the hull and adds the node which makes the left turn. J_3 is making the right turn so it is eliminated from the hull, and J_4 is added to the hull. The found convex hull is regarded as the jammed region, which encloses all jammed nodes, including the jammer.

The position of the jammer is localized in two steps. First, an approximate position of the jammer is calculated by finding the mean of the vertices of the convex hull, which is essentially the center of the region. Let the coordinates of jammed sensor nodes are $(X_1, Y_1), (X_2, Y_2), (X_3, Y_3), \ldots (X_N, Y_N)$. So, by Equation 4, the estimated position of the jammer is,

$$(\overline{X_e}, \overline{Y_e}) = \left(\frac{\sum_{j=1}^{N} X_j}{N}, \frac{\sum_{j=1}^{N} Y_j}{N}\right) \quad (4)$$

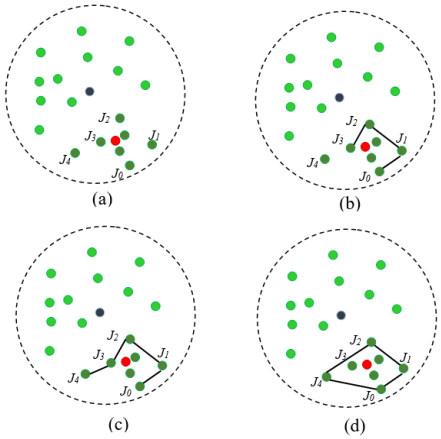


Figure 1: Convex hull for the jammed region.

Since the boundary nodes of the jammed region may not be getting the same JSS, it is highly unlikely that the center of this region is the accurate position of the jammer. So, to localize the jammer accurately, a parameter called localization adjustment metric α is considered, which is defined as the relative difference between receiver sensitivity and the least JSS received by a jammed node. A boundary node of the jammed region may get higher signal strength than its signal sensitivity. In this case, this boundary node is not an actual boundary node since the estimated jammed region is shrunk. So, considering the center of the jammed region as the position of the jammer is inaccurate. The localization adjustment metric α is used here to minimize the error in localizing the jammer. If a jammed node J's signal sensitivity is S_{rj}, and the least JSS received by J is JSS_{minj}, then α_j is calculated from Equation 5,

$$\alpha_j = \frac{S_{rj} - JSS_{minj}}{S_{rj}} \quad (5)$$

The new estimated position of the jammer is found by adding or subtracting α from Equation 4. From Friis's free space transmission equation [3], it can be derived that RSS is inversely proportional to the distance from the sender to the receiver. Since α is a unit-less parameter, and is the relative difference of jammed signals from the jammer to the jammed sensor nodes, making adjustments using α can give a better estimation of the jammer's position. After making all adjustments, the final estimation of the jammer's position is considered by calculating the mean of all adjusted positions of the jammer.

3.3. Channel Assignment Technique

In each round, each node acquires a common channel which if jammed, is used as a relay channel. Under jamming condition, each CH and its cluster members choose its own channel dynamically using Equation 6. A pseudorandom function, Linear Congruential Generator (LCG) is used for effective and dynamic channel assignment. This function ensures that the jammer cannot identify the new channel selected by a jammed node easily.

$$X_{n+1} = (aX_n + c) \bmod m \quad (6)$$

Here, X_{n+1} is the new operating channel, X_n is the first channel, a is a multiplier which is the round number in this work, c is an increment and m is the total number of channels that the network uses. During network initialization, the sensor nodes acquire a default channel as the

operating channel and relay channel. When a CH finds that its cluster is jammed, it changes channel using Equation 6. Since this work is considering real sensor mote such as TelosB mote with CC2420 2.4GHz IEEE 802.15.4 compliant RF transceiver, so here X_n is 2400MHz. Since the channel spacing for CC2420 is 5MHz which means channels are non-interfering with 5MHz space, so c is 5. Let m is 11 channels with 5MHz space each, e.g., 2410, 2415, 2420, 2425. The value of m controls the number of channels that can be used in the network. The CH of jammed cluster selects channel as follows:

$$X_1 = (2 \times 2400 + 5) mod\ 11 = 9$$

The jammed nodes also select the channel using the same parameter, so they have the same channel that of their CH. For the first round, the operating channel and the relay channel are same. For the subsequent rounds, the relay channel is the channel that is used as the operating channel in the previous round. Since the round number is increasing, so in each round a new channel is selected dynamically for the jammed clusters.

3.4. Data Transmission

Data transmission is time slotted and can be intra-cluster and inter-cluster. Data transmission for intra-cluster is time slotted. During steady state phase, each cluster members of a cluster send data to its CH using its slot so that no collision occurs in transmitting data. Figure 2 shows cluster members are sending data to CH using time slot. A CH aggregates all incoming data from its cluster members and combines them into a single packet. It then sends this aggregated packet to BS via one or more CHs using its inter-cluster slot. When the network is not jammed, CHs use the network's operating channel for sending aggregated data. When a cluster is jammed, it operates using another channel which is different from its neighbor's operating channel. On the other hand, if the jammed region falls in between the sending CH and relay CH, then it may not be able to send the aggregated data because that relay CH may be using the same operating channel that is being used by the jammer.

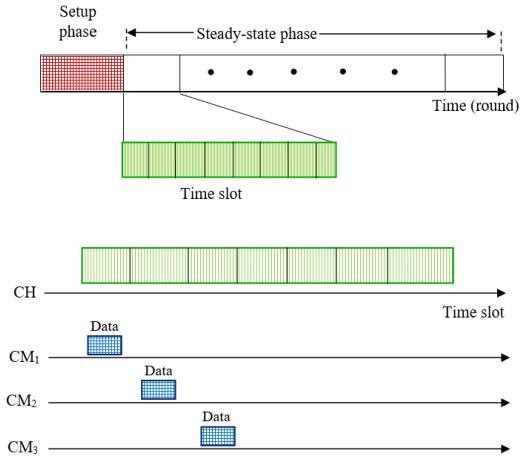


Figure 2: Intra-cluster communication

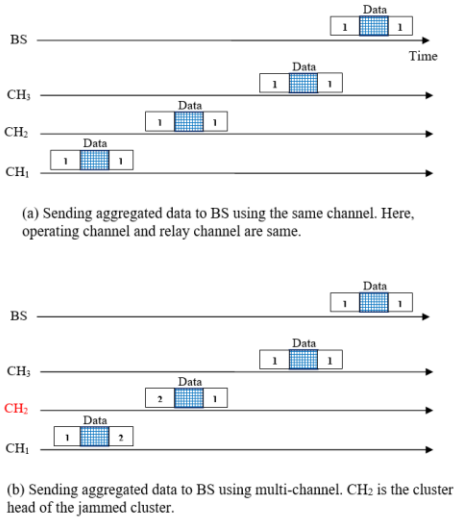


Figure 3: Inter-cluster communication

To provide seamless data transmission under the threat of the jammer, a jammed CH is not only required to change its current operating channel, but also it needs to choose a relay CH whose path from sending CH does not fall in between jammed region and is next least distant from the

BS. During channel changing phase, the CH of jammed cluster informs its neighbor CHs that it is going to use relay channel for aggregated data transmission and chooses a time slot for sending and receiving aggregated data. The CH of jammed cluster selects a relay CH from the available neighbor CHs list and sends aggregated data via relay CH.

Figure 3(a) shows an example of transmitting aggregated data from a CH to BS when the network is not jammed and Figure 3(b) shows data transmission between a jammed cluster and the BS. Here, the cluster head of jammed cluster, CH_2 is using channel 2 for intra-cluster communication and when it has data to send to BS via CH_3, it switches to CH_3's channel which is channel 1. If other CHs need to send data via CH_2, they switch to CH_2's channel. Here, CH_1 needs to send through CH_2, so it switches to channel 2 and sends the aggregated data.

4. EXPERIMENTAL RESULTS

To assess the performance of the proposed scheme, simulations of non-jammed, jamming, and anti-jamming scenarios are performed in a multi-hop clustering based WSN using Castalia simulator [34] that runs on the top of OMNET++ [35]. The average energy consumption in the network, average delay, Packet Loss Ratio due to jamming, Packet Delivery Ratio (PDR), and network throughput have been calculated. The simulation parameters are listed in Table 1.

Table 1: Simulation Parameters

Parameter	Value
Simulation Duration (s)	100
Number of Nodes	100
Network Dimension (m^2)	400x100
Real Radio	CC2420
Initial Energy (J)	18720
Slot length (ms)	20
Round length (s)	30
Percentage of CHs	5-15
Jammer's Type	Constant Jammer
Number of Jammers	1-3
Jammer's Packet Rate	500

4.1. Simulation Environment

The proposed scheme simulated with various number of jammers. The following simulation assumptions are made: (i) sensor nodes are considered to be homogeneous, with respect to transmission power and receiver sensitivity, (ii) sensor nodes are stationary, meaning once they are jammed, cannot escape the jammed region because of no mobility, (iii) for simplicity, the transmission range of the sensor nodes is assumed to be a perfect circle, (iv) jammer's transmission range as well as transmission power can vary, and (v) a jammer is constantly sending high rate of packets with high energy.

4.2. Simulation Results

The simulation results are compared in terms of packet delivery ratio (PDR), packet loss rate due to jamming, network throughput, average delay and energy consumption with respect to transmission power. The simulation is carried out for 100s with repetition of 100 times.

4.2.1. Packet Delivery Ratio (PDR)

PDR is defined in [36] as the ratio of the number of legitimate packets that has been successfully delivered and acknowledged by the destination node to the number of packets sent by the transmitting node. PDR is a good metric to detect the different forms of jamming attacks. Figure 4 shows that under jamming condition, for 50% times the average PDR is 28%; 53% when the network is not jammed; and 48% when the anti-jamming technique is applied. The CDF performance curves shows that anti-jamming technique increases the PDR and is very close to non-jammed scenario.

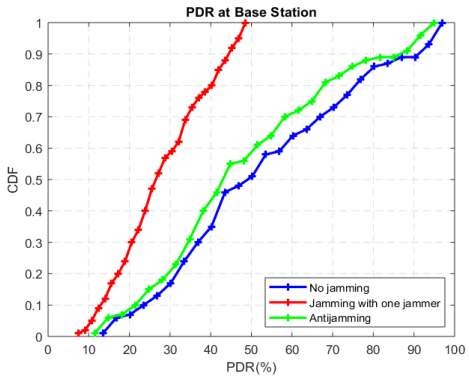
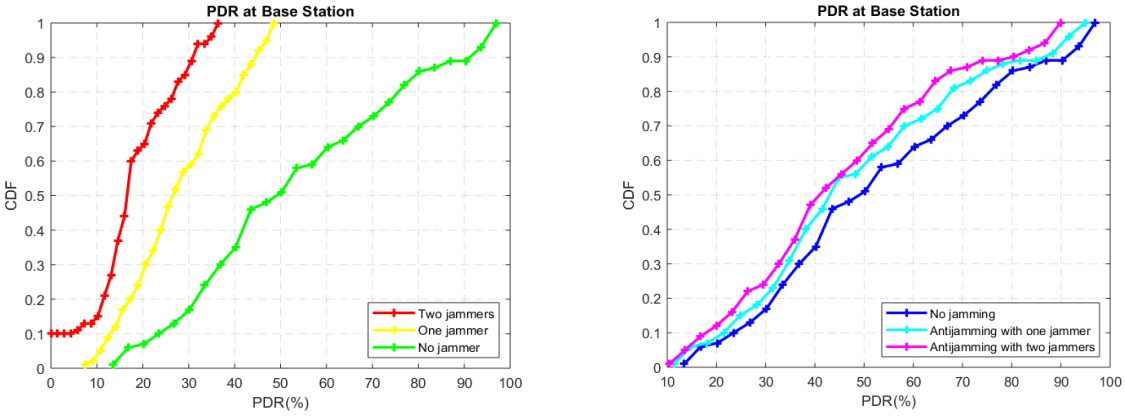


Figure 4: Impact of PDR for non-jammed, jammed and anti-jamming with jamming scenarios.

Figure 5(a) shows the effect at packet delivery ratio when jammers are increased. For two jammers scenario, 90% times the PDR falls below 31%; for one jammer scenario, 90% times the PDR is decreased to 45% compared to non-jammed scenario. After applying anti-jamming technique, the PDR is increased for both one jammer and two jammers scenarios and is very close to non-jammed scenario as shown in Figure 5(b).



(a) (b)

Figure 5: Impact of PDR (a) in case of no jammer, one jammer and two jammers, and (b) in case of no jamming, anti-jamming with one jammer, and anti-jamming with two jammers.

To check whether the PDR of jamming attacks varied significantly from the PDR of anti-jamming technique or not, an F-test has been performed. The result from the F-test reveals significant variances ($P<0.05$) in PDR between jamming attacks and anti-jamming technique.

Moreover, F-test has also been performed for the PDR between two more groups: non-jammed and jammed; and non-jammed and anti-jamming technique to see whether PDR varies significantly or not. Significance variance is observed in PDR between non-jammed and jammed networks. However, there is not enough evidence ($P>0.05$) to conclude that there is a significant variance in PDR between non-jammed and anti-jamming technique which indicates similar variance in PDR between non-jammed and anti-jamming technique.

4.2.2. Packet Loss Ratio

The packet loss ratio in radio level is calculated by dividing total packet loss due to interference by the total RX packets. The total number of RX packets is the sum of the failed packets with interference, failed packets because of received signal is below sensitivity, failed packets because nodes are not in receiving state, received packets despite interference and received packets with no interference.

Figure 6 shows application level packet loss with respect to different jamming transmission power. For 0dBm transmission power, the packet loss due to jamming is close to 86%, where in anti-jamming with jammer case, the packet loss is almost consistent for all transmission powers with a slight increase for 0dBm jamming transmission power. In anti-jamming scenario, the packet loss for 0dBm is 49% which is very low compared to packet loss due to jamming.

In non-jammed scenario as shown in Figure 7(a), the average packet loss is 2.8% while no jammer is present in the network which is very negligible. In Figure 7(b), the average packet loss due to jamming is 7% of total RX packets and packet loss increases drastically if more than one jammer is present in the network as shown in Figure 7(c). In two jammers case, the average packet loss is 15% of total RX packets.

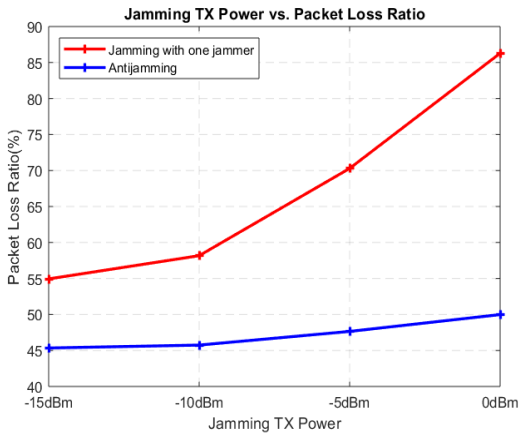
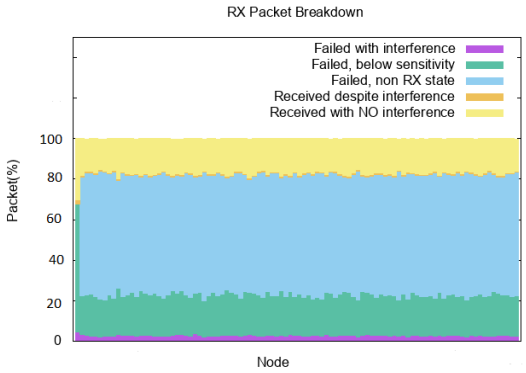
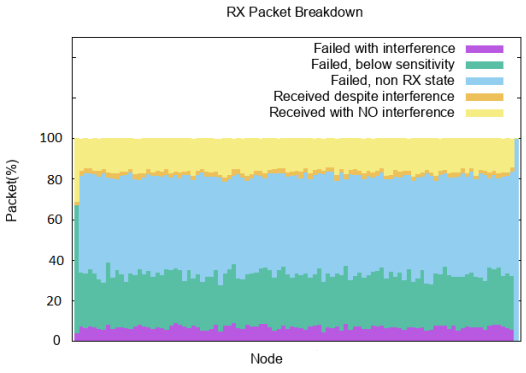


Figure 6: Packet loss ratio due to jamming with respect to different transmission power.

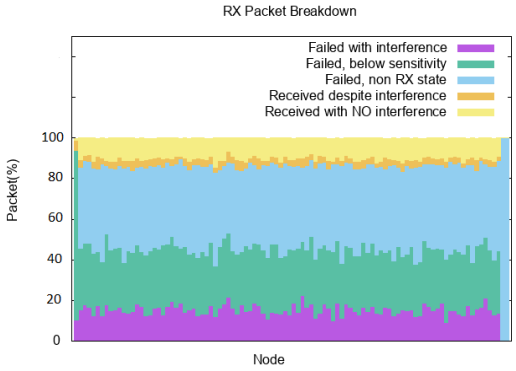
After applying anti-jamming technique for both one jammer (Figure 7(d)) and two jammers (Figure 7(e)) shows significant reduction in packet loss. For anti-jamming with one jammer scenario, the average packet loss is 3.2% which is very close to non-jammed scenario and anti-jamming with two jammers scenario, the average packet loss is 5.2% which is much lower than two jammers case. So, the proposed anti-jamming technique gives a better performance in reduction of packet loss due to jamming.



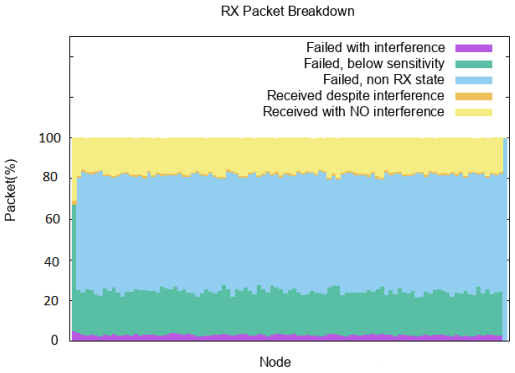
(a) Packet loss due to interference in non-jammed scenario.



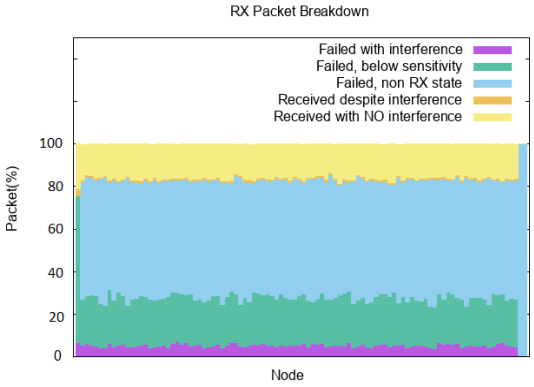
(b) Packet loss due to interference in jammed scenario



(c) Packet loss due to interference in two jammers case.



(d) Packet loss due to interference in jammed network with anti-jamming.

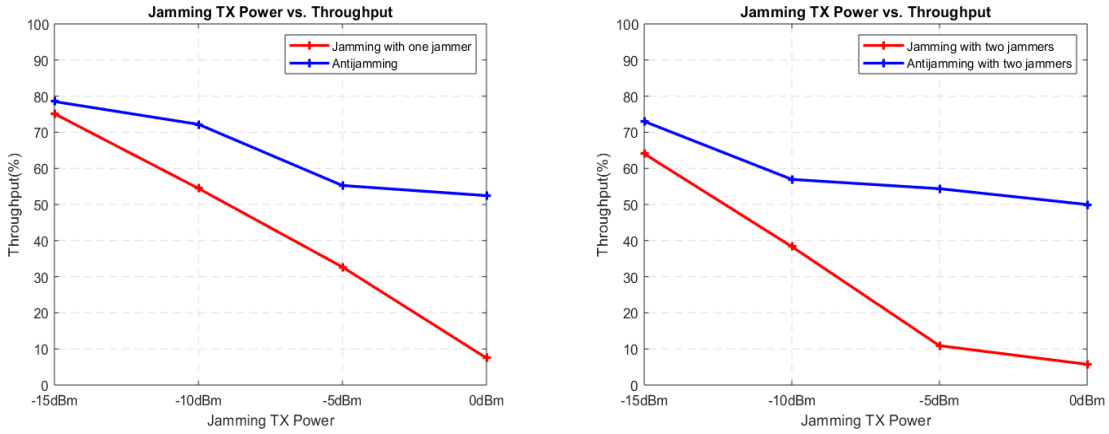


(e) Packet loss due to interference in anti-jamming with two jammers.

Figure 7: Packet loss due to interference when jammer is present in the network in (a) non-jammed, (b) jammed with one jammer and (c) jammed with two jammers, (d) anti-jamming with a jammer scenario, and (d) anti-jamming with two jammers scenario.

4.2.3. Throughput

Throughput is defined as the total number of received packets from the source to the destination with a certain period of time. Figure 8 shows application level throughput at base station with respect to different jamming transmission power.



(a) (b)

Figure 8: Application level throughput of the network (a) in jammed and anti-jamming with one jammer and (b) in jammed and anti-jamming with two jammers scenarios for jammer's transmission powers: 0dBm, -5dBm, -10dBm, and -15dBm.

The throughput of the network in jammed case decreases with the increase in jamming transmission power. When the jamming transmission power is maximum which is here in this case, 0dBm, the throughput of the network is 7.5%, whereas the throughput of network is 52% when anti-jamming technique is used. The Figure 8(a) shows that when the jamming power decreases the throughput of the network increases, because the jamming power is not strong enough. In anti-jamming with a jammer case, the throughput of the network is better for all jamming transmission powers.

In Figure 8(b), for 0dBm jamming transmission power, the throughput of the network in two jammers case decreases rigorously which is 5% whereas the in anti-jamming with two jammers case, the throughput of the network is almost same as the throughput with anti-jamming with one jammer case.

4.2.4. Average Delay

Average delay is defined as the sum of the duration of all successfully reached packets at the base station divided by the total number of received packets by the base station. The Figure 9 shows the average delay for non-jammed, jammed and anti-jamming with a jammer scenario. The average delay reduces when a jammer is present in the network. The reason behind reduction in average delay is that the most of the packets cannot reach to base station due to jamming. So, this definition of delay is sometimes deceiving. Because it does not consider the presence of jammers in the network which thwarts in reaching the packets in the base station.

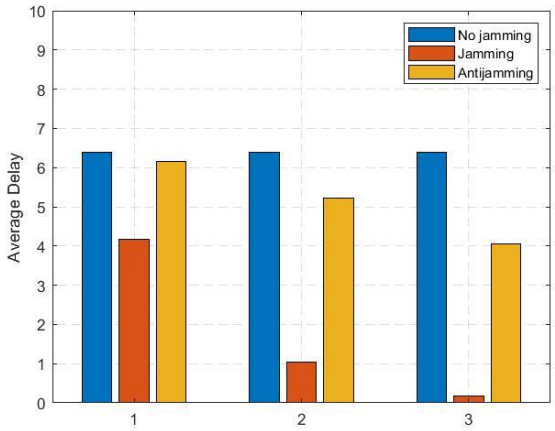
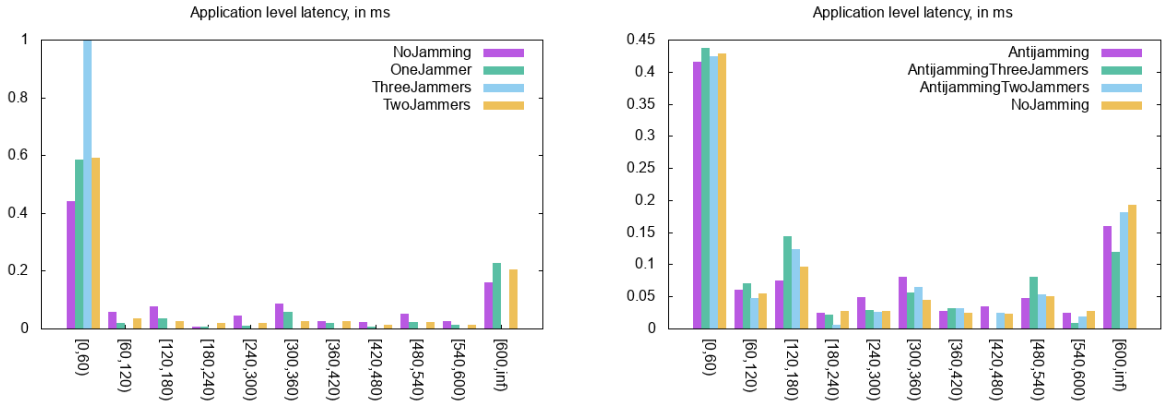


Figure 9: Average delay for (1) non-jammed, jammed with one jammer, anti-jamming in presence with one jammer, (2) non-jammed, jammed with two jammers and anti-jamming in presence with two jammers, (3) non-jammed, jammed with three jammers, and anti-jamming in presence of three jammers scenarios.

To show real picture of delay, an application level latency histogram is constructed for jamming scenarios and anti-jamming with jammers scenarios (Figure 10). Figure 10(a) shows that most of the packets are received with under 60ms latency, which means that they are transmitted after their creation. There is a little variability in other buckets meaning packets received per node due to jamming is very low. This is why delay for jamming cases are lower.



(a) (b)

Figure 10: Latency Histogram (a) for non-jammed, one jammer, two jammers and three jammers cases and (b) for non-jammed, anti-jamming with one jammer, anti-jamming with two jammers and anti-jamming with three jammers cases.

On the other hand, Figure 10(b) shows the latencies when anti-jamming technique is used. In anti-jamming cases, most packets are received with under 60ms latency and some packets are received with variable latencies. Very few packets fall in the last bucket at [600, inf) which is ignorable. It shows that anti-jamming technique with three jammers is performing better than other cases.

4.2.5. Energy Consumption

Average energy consumption of the network is defined as the total energy consumed by the all sensor nodes divided by the total number of nodes. Figure 11 shows the average energy consumption of the network for different transmission power in a non-jammed, jamming and anti-jamming scenario. The energy consumption increases when transmission power increases and the maximum energy is consumed for two jammers case which means with the increased number of jammers in the network, the energy consumption will also increase. Although the energy consumption of anti-jamming techniques is greater than non-jammed network but it is lower than the jammed network. So, the proposed technique is performing better in jammed cases in terms of energy efficiency.

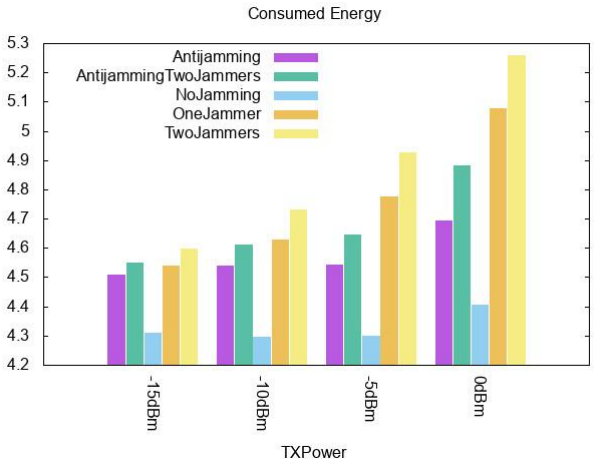


Figure 11: Average energy consumption of the network for non-jammed, a jammer, two jammers, anti-jamming with one jammer, and anti-jamming with two jammers.

5. DISCUSSION

The proposed anti-jamming technique can be integrated in any type of clustered protocol. For deployment, different types of hardware can be used as no special hardware is necessary for our proposed scheme. The deployment challenges are regular challenges in a WSN such as coverage area, environment, power, weather, etc. [43], [44]. Other than this, there is no additional challenges for our proposed technique as we do not use additional hardware. The limitation of our scheme is the overhead of the additional control packets. Also, the proposed scheme cannot mitigate the jamming effect 100%. However, the proposed scheme still improves the overall performance of the network in the presence of jamming.

6. CONCLUSION

This research work explored the various kinds of jamming attacks in WSN with more emphasis on the constant jamming attack. This type of jamming attack mainly increases the energy consumption of the sensor nodes by keeping the nodes in receive state when they are expecting receiving legitimate packets. This reduces the lifespan of the network. Hence, a multi-channel clustering based anti-jamming technique has been introduced and analyzed. The proposed technique is able to produce better performance in terms of PDR, network throughput and latency. Although there is not much improvement in conservation of energy but it still shows

lower energy consumption in case of jamming. The simulation results prove that a considerable improvement as opposed to schemes with no anti-jamming technique.

Future work includes improving the proposed technique in terms of energy conservation, and testing it with other classes of jamming attacks. A further study regarding mobility of sensor nodes will be useful to discover the effect of jamming attack in the proposed technique. In future, both the mobility of sensor nodes and jammers in the proposed technique will be investigated and adjustment of this work will be made.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] Kandris, D., Nakas, C., Vomvas, D., & Koulouras, G., "Applications of wireless sensor networks: an up-to-date survey," Applied system innovation, vol. 3, no. 1, pp. 14, 2020.

[2] Abdulkarem, M., Samsudin, K., Rokhani, F. Z., & A Rasid, M. F., "Wireless sensor network for structural health monitoring: A contemporary review of technologies, challenges, and future direction," Structural Health Monitoring, vol. 19, no. 3, pp. 693-735, 2020.

[3] Karl, H., Willig, A., "Protocols and Architectures for Wireless Sensor Networks," John Wiley & Sons, 2005.

[4] Wang, J., Gao, Y., Liu, W., Sangaiah, A. K., & Kim, H. J., "Energy efficient routing algorithm with mobile sink support for wireless sensor networks," Sensors, vol. 19, no. 7, pp. 1494, 2019.

[5] Koskela, P., Energy-Efficient Solutions for Wireless Sensor Networks, Ph.D. Thesis, University of Oulu Graduate School, University of Oulu, 2018.

[6] Pelechrinis, K., Koutsopoulos, I., Broustis, I., Krishnamurthy, V., S., "Lightweight Jammer Localization in Wireless Networks: System Design and Implementation," GLOBECOM, IEEE, pp. 6, 2009.

[7] Pantazis, A., N., Nikolidakis, A., S., Vergados, D., D., "Energy-Efficient Routing Protocols in Wireless Sensor Networks: A Survey", IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 551-591, 2012.

[8] Giustiniano, D., Lendersy, V., Schmittz, B. J., Spuhler, M., and Wilhelm, M., "Detection of Reactive Jamming in DSSS-based Wireless Networks," Proceedings of the sixth ACM Conference on Security and Privacy in Wireless and Mobile Network, pp. 43-48, April 17-19, 2013.

[9] Sun, Y., Wang, X., Önen, M., Molva, R., "CrowdLoc: Wireless Jammer Localization with Crowdsourcing Measurements," Proceedings of the 2nd International workshop on Ubiquitous Crowdsourcing, ACM, pp. 33-36, September 18, 2011.

[10] Sun, Y., Molva. R., Önen, M., Wang, X., Zhou, X., "Catch the Jammer in Wireless Sensor Network," IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications, pp. 5, September 11-14, 2011.

[11] Wood, D. A., Stankovic, A., J., and Son, H. S., "JAM: A Jammed-Area Mapping Service for Sensor Networks," IEEE Real-Time Systems Symposium, pp. 13, December 5, 2003.

[12] Chowdhury, S., J., T., A Distributed Cooperative Algorithm for Localization in Wireless Sensor Networks Using Gaussian Mixture Modeling, M.Sc. Thesis, The University of Toledo, 2016.

[13] ðurišić, P., M., Tafa, Z., Dimić, G., Milutinović, V., "A Survey of Military Applications of Wireless Sensor Networks," Mediterranean Conference on Embedded Computing (MECO), IEEE, pp. 4, June 19-21, 2012.

[14] Kulkarni, P., Ozturk, Y., "Requirements and Design Spaces of Mobile Medical Care," ACM SIGMOBILE Mobile Computing and Communications, vol. 11, no. 3, pp. 12-30, July, 2007.

[15] Ramesh, V., M., "Wireless Sensor Network for Disaster Monitoring," Wireless Sensor Networks: Application-Centric Design, pp. 20, 2010.

[16] Patwari, N., Location Estimation in Sensor Networks, Ph.D. Thesis, Electrical Engineering and Computer Science, The University of Michigan, 2005.

[17] Zhu, Y., Li, X., Li, B., "Optimal Adaptive Anti-jamming in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, pp. 9, 2012.
[18] Mustafa, A., H., Zhang, X., Liu, Z., Xu, W., Perrig, A., "Jamming-Resilient Multipath Routing," IEEE Transactions on Dependable and Secure Computing, vol. 9, pp. 852-864, 2012.
[19] Liu, Z., Liu, H., Xu, W., Chen, Y., "An Error Minimizing Framework for Localizing Jammers in Wireless Networks," IEEE Transactions on Parallel and Distributed Systems, vol. 25, pp. 11, 2014.
[20] Rahman, N., Wright, M., Liu, D., "Fast and Energy-Efficient Technique for Jammed Region Mapping in Wireless Sensor Networks," https://arxiv.org/abs/1401.7002 [Last access on 15 July, 2023].
[21] Liu, Z., Liu, H., Xu, W., Chen, Y., "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization," IEEE Transactions on Parallel and Distributed Systems, pp. 14, 2012.
[22] Xu, W., Ma, K., Trappe, W., Zhang, Y., "Jamming Sensor Networks: Attack and Defense Strategies," IEEE, pp. 41-47, 2006.
[23] Heinzelman, R., W., Chandrakasan, A., Balakrishnan, H., "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," IEEE, pp. 10, 2000.
[24] Lindsey, S., Raghavendra, S., C., "PEGASIS: Power-Efficient Gathering in Sensor Information Systems," IEEE, vol. 3, pp. 6, 2002.
[25] Loscrì, V., Morabito, G., Marano, S., "A Two-Levels Hierarchy for Low-Energy Adaptive Clustering Hierarchy (TL-LEACH)," IEEE, pp. 1809-1813, 2005.
[26] Li, C., Ye, M., Chen, G., Wu, J., "An Energy-Efficient Unequal Clustering Mechanism for Wireless Sensor Networks," IEEE, pp. 8, 2005.
[27] Boukerche, A., Oliveira, A.,B., F., H., Nakamura, F., E., Loureiro, A., F., A., "Secure Localization Algorithms for Wireless Sensor Networks," IEEE, pp. 96-101. April, 2008.
[28] Saeed, S., Analysis of Jamming attacks on Wireless Sensor Networks, M.Sc. Thesis, University of Hertfordshire, September, 2015.
[29] Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., and Pantziou, G., "A Survey on Jamming Attacks and Countermeasures in WSNs," IEEE Communications Surveys & Tutorials, vol. 11, no. 4, pp. 42-56, 2009.
[30] Mohapatra, H., & Rath, A. K., “Fault-tolerant mechanism for wireless sensor network,” IET wireless sensor systems, vol. 10, no. 1, pp. 23-30, 2020.
[31] Catarinucci, L., Colella, R., Fiore, D., G., Mainetti, L., Mighali, V., Patrono. L., Stefanizzi, L., M., "A Cross-Layer Approach to Minimize the Energy Consumption in Wireless Sensor Networks," International Journal of Distributed Sensor Networks, no. 268284, pp. 11, 2014.
[32] Grover, K., Lim, A., Yang, Q., "Jamming and Anti-jamming Techniques in Wireless Networks: A Survey," International Journal of Ad Hoc and Ubiquitous Computing, pp. 197-215, 2014.
[33] Ganeshkumar, P., Vijayakumar, K., P., Anandaraj, M., "A novel jammer detection framework for cluster-based wireless sensor networks," EURASIP Journal on Wireless Communications and Networking, pp.1-25, 2016.
[34] Boulis., A., "Castalia: A simulator for Wireless Sensor Networks and Body Area Networks," NICTA: National ICT Australia, March, 2011.
[35] Varga., A., "OMNET++: Modeling and Tools for Network Simulation," pp. 35-59, 2010.
[36] Osanaiye, O., Attahiru S. Alfa, S., A., Hancke, P., G., "A Statistical Approach to Detect Jamming Attacks in Wireless Sensor Networks," Sensors, no. 1691, pp. 1-15, May, 2018.
[37] Manjeshwar, A., Agrawal, P., D., "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," Proceedings 15th International Parallel and Distributed Processing Symposium, IEEE, pp. 1-8, April, 2000.
[38] Manjeshwar, A., Agrawal, P., D., "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," Proceedings of the International Parallel and Distributed Processing Symposium, IEEE, 2002.
[39] Younis, O., Fahmy, S., "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks," IEEE Transactions on Mobile Computing, vol. 3, no. 4, pp. 366-379, 2004
[40] Guo, J., Zhao, N., Yu, F., R., Zhang, S., Yang, Z., and Leung, C.M., V., "Disrupting Anti-jamming Interference Alignment Sensor Networks with Optimal Signal Design", IEEE, pp. 4, 2017.

[41] Farahani, G., "Energy Consumption Reduction in Wireless Sensor Network Based on Clustering," International Journal of Computer Networks & Communications (IJCNC), vol. 11, no. 2, pp. 33-51, March, 2019.

[42] Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (1990). 33.3: Finding the convex hull. Introduction to Algorithms, 955-956.

[43] Amutha, J., Sharma, S., & Nagar, J., "WSN strategies based on sensors, deployment, sensing models, coverage and energy efficiency: Review, approaches and open issues," Wireless Personal Communications, vol. 111, pp. 1089-1115, 2020.

[44] Priyadarshi, R., Gupta, B., & Anurag, A., "Deployment techniques in wireless sensor networks: a survey, classification, challenges, and future research issues," The Journal of Supercomputing, vol. 76, pp. 7333-7373, 2020.

AUTHORS

Maoyejatun Hasana received B.Sc. degree in Computer Science and Engineering from International Islamic University Chittagong, M.Sc. degree in Information and Communication Technology from Bangladesh University of Engineering and Technology (BUET). She is currently pursuing Ph.D. degree in Computer Science and Engineering at Bangladesh University of Engineering and Technology (BUET). She is holding a lecturer position at the Department of Computer Science and Engineering at Asian University of Bangladesh. Her research interests include wireless sensor networks, network security and human-computer interaction.

Dr. Hossen Asiful Mustafa is currently serving as Associate Professor at the Institute of Information and Communication Technology, Bangladesh University of Engineering and Technology (BUET). Dr. Mustafa received his Ph.D. degree from the University of South Carolina, USA in 2014. His research interests include Wireless Networks, Cyber Security, Distributed Systems and Data Science. He has several publications in top journals and conferences including IEEE TDSC, ACM CCS, USENIX Security, IEEE CNS, etc. Dr. Mustafa also worked in the industry in research and development for five years and has expertise in systems, security, and software development.