Jamming aware unrestricted data transmission in multi-hop wireless networks

R.Uma Mageswari[1], Dr.S.Baulkani[2]

[1] *Associate Professor, Department of Computer Science and Engineering, Vardhaman College of Engineering (Autonomous), Shamshabad, Hyderabad, Telangana, India.*

[2] *Professor, Department of Electronics and Communication Engineering, Government College of Engineering, Tirunelveli, Tamilnadu, India.*

Email: umaphd71@gmail.com

Abstract- The basic entity of the wireless communication is the electromagnetic waves. Electromagnetic waves carry data that can be used by digital appliances in the wired and wireless network. In Multi-Hop Wireless Network (MHWN) data transmission is performed by the cooperation of neighbor nodes. The functionality of this network is severely affected by jammer, an intended node that blocks the ongoing communication as the media is open in nature. The jammer localization is required to predict the occurrence of jammer and its location in the network. Most of the existing jammer localization techniques only suits for predicting static jammer. The proposed jammer localization is capable of localizing both the static jammer as well as portable jammer. The jammer localization is followed by diverting the data that passes through the jammed area. The proposed Reliable Lookup Algorithm (RLA) enhances the data transmission in the MHWN by the obtained next region information thereby the ongoing data communication is retained. The simulation result proves this proposed work.

Key Words: Portable Jammer, Multi-Hop Wireless Network, Jammer localization, Data transmission.

1. Introduction

Wireless communication's rapid growth is widely involved in the different fields as it utilizes available electromagnetic spectrum for communication. The evolution of wireless communication from electromagnetism was discussed [24] Vinay Kumar Nassa 2011. The ease of use, cheapest price, ease to carry, ubiquitous nature, and adequate consumption has made it admired further. The realistic solution for achieving communication between universal networks is considered as Multi-Hop Wireless Network (MHWN) rather than fixed infrastructure based wireless network, where its services cannot be expanded. In MHWN's the participated device known as nodes which have the capability to communicate with each other without the support of any other external devices in the multi-hop fashion. Due to the open nature of the electromagnetic medium, leads the intruders to easily entered and degrade the functionality of the network [6] Gesic et al. 2016. Especially any form of attack in the wireless network is detected by the degradation in the received SNR i.e. signal-to-noise ratio [1] Adamy 2014. Also jamming attack is categorized under Denail of Service (DoS) attack, since it restricts the communication by denying the channel for legitimate users and is outlined as "any event that removes or decreases the ability of a network to fulfill its intended idea" [27] Wood et al. 2002. Though jamming attack is considered as physical layer attack, this attack can also be made through different layers in the existing protocols stack, thereby its cruel intention of degrading network performance is achieved through available resource usage restriction [17] Pelechrinis et al. 2016.

The current jammer localization algorithm can be categorized as two parts based on the data's used in position identification. First method depends on the range-based and the other is range-free. The Least square method [10] Liu et al. 2010, the Crowd Location method [21] Sun et al. 2011, etc., locates the jammer in the first method. As per [10] Liu et al. 2010, the jammer can be easily localize by using least square problem, that utilizes the variation caused to the range of hearing for the network. In the existing paper [9] Liu et al. 2009 uses VFIL Virtual Force Iterative Localization technique to identify the jammer position by measuring the distance between the nodes in the network and the jammer. The identification of the jammer depends largely on the jammed region's physical properties. Eventhough there are many existing jammer localization techniques are available based on the above two methods, but none of

BUPT

them consider the jammer under mobility i.e. portable jammer. The proposed work consider portable jammer is equipped with motor that support the jammer to roam around the concerned area of Multi Hop Wireless Network.The Portable jammer can strongly differ its point in order to control the jamming signals in physical distribution that will result in a change in network setup. This renders the method of jammer positioning more complicated and difficult. This portability generates discrimination in the above said two methods. In the former method the distance computation is critical, in later the shape of the jammer varies.

In common this portable jammer affects the ongoing communication of the valid users and therefore it is the need to implement certain techniques to come out of its effect. This is only possible when the nodes in the network predict the presence of the jammer followed by portable path. Thereby present limitation in the existing network is overthrown. The steps provided below are included in this paper for the portable jammer detection efficiently. Identifying the right node and to observe the concerned node is the initial step. The second step is to estimate the jammer signal strength. The gather of the data from the concerned concert is the third step and the last step is to supervise the transfer of the concerned node i.e. handover function and fix the location of the jammer.

2. Associated work

This session gives details about the various existing attacks found in MHWN, follow by elaborately explains the main idea behind localization of the jammer and the way by which the target devices are tracked in the Wireless sensor Network.

2.1. Categories of Denial-of-Service attacks (DoS)

DoS attacks are used to prevent network resources from being accessed. This is usually accomplished by flooding the victim system or network with excessive traffic, rendering it incapable of responding to real user inquiries. As per [8] Islam et al. 2020 showcases the various DoS attacks occurs in WSN which is been categorized based on the existing different layers of networks. In the physical layer the attacks were listed as jamming and node tampering attack whereas as in data link layer the attacks were categorized as collision, interrogation and denial of sleep as well as in the network layer the specified attacks were spoofing, black hole attack and hello flood attack. In the transport layer attack were of synchronize flood attack, desynchronized attack and content attack and the last layer known to be application layer gets the attack called as overwhelming sensor node and path-based DoS.

The work done by [7] Hussaini et al. 2019 states there may be some untrusty nodes within the network which creates attack or compromising the network security. They designed the algorithm to detect and localize the untrusty nodes within the WSN and the way to isolate these nodes out of the network during the routing process. In [29] Xu et al. 2005 explained the initial layer jamming and it determines various forms of jammers based on its activity by reserving the channel for the concern duration as reactive jammer, constant jammer, proactive jammer, and random jammer. Apart from the above mention jammers there are many kinds of jammers are available now a day. In [30] Xu et al. 2008 provides mechanism to identify the jammer followed by retreating the interference effect by adopting spectral evasion techniques like channel surfing and spatial retreats thereby communication is achieved in presence of jammer.

2.2. Way to track end nodes inside WSN

Due to the modern IoT boards embedded with lot of location tracking modules analogy added up with the sensors it becomes quite practical to track the location of the end nodes. However, based on the survey from previous articles it's been identified that the following steps are adopted to track the device in WSN which is as per the figure 1.



Figure. 1. Steps for device tracking

In the first module of the diagram reflects the recognition of the end device where the detected is done by certain methods like Passive Infra-red (PIR) in case of the acoustic sensor [23] Vasuhi et al. 2016. The next module which is the reporting Process done after the target node has been successfully identified. The target device is identified using triangulation technology through this measurement details are reported. The last module is the region prediction as per the literature this phase has been using Particel filter, Kalman filter, Hidden Markov model. One can identify the next point of the device

BUPT

movement based on the previous two steps in the WSN. Thus, the target device is traced by repeating these steps in the WSN.

2.3. Localization of the Jammer

According to literature there are numerous works focuses on jammer identification as well as localization. These algorithms are classified as range free and range based localization method. The range free method, functions by analyzing the geographical property of the jammed area. The DCL Double Circle Localization (DCL) algorithm was explained by [4] Cheng et al. 2012, existing mechanism worked on the basis of bounding circle i.e. minimum bounding circle (MBC) and maximum inscribed circle (MIC). Convex hull, is used to calculate the MBC and MIC. The improved PSO algorithm (particle swarm optimization) [16] Pang.et al. 2017, proposed the technique for manipulating the minimum occupying coverage jammed area. This paper [26] Wei et. al. 2017, keenly provides the existing techniques for jammer localization as well as it stated the MHWN performance under jammer done by the analysis of the various researchers. The existing [9] Liu et al. 2009 VFIL algorithm worked to identify the jammer based on the range of nodes changes, here F pull and F push mechanisms are used iteratively to find the jammer position more effectively. This method creates a measured jammed region in circular form. The center of this constructed circle will be fixed as the jammer location and which is predicted to be the actual jammed region.

Only a fewer jammer localization method are fixing up in the recent years, devoid to dedicated devices [17] Pelechrinis et al 2009. The current paper explained that PDR degradation due to the jammer presence in the network when a node comes nearer to the location of jammer, there will be decrease in PDR value. Hence the gradient-descent for PDR estimation-based jammer localization technique must be enabled; it worked based on the network topology's distinct axis in order to identify the jamming. The existing paper [13] Liu et al. 2012 developed the mechanisms to localize the jammer by exploiting neighbor changes. Initially they determined the jamming effect analysis as free-space model by examining the way through which communication range changes with the location of jammer and the power of transmission. Then the estimation of the jammer location was done by solving it as a least-squares (LSQ) problem. It provided the hypothesis, that when the jammer attacked the node, it moves from its hearing range. Then [14] Liu et al. 2012 devised an estimation scheme for jammer localization by introducing ambient noise floor technique as well as for improving localization accuracy an evaluation feedback metrics was formulated to quantify the error in estimation. This existing paper also suggest genetic algorithm to reduce the localization error. In this paper [22] Sun et al. 2011Centroid Localization (CL) technique was proposed, the calculated average for the jammed nodes co-ordinate is used to fix the jammer's location. This above mentioned situation was assumed there by the received signal strength varies by means of jammed nodes which were present in the various locations. Weighted Centroid Localization WCL [2] Blumenthal et al. 2007 suggested that it improves the localization accuracy when compared with CL by assuming further weight metrics to the jammer location, thereby only the exact nearby jammed nodes near to the jammer was used to compute the location of the jammer rather than considering than whole jammed nodes in the network. In [4] Cheng et al. 2012 Double Circle Localization (DCL) algorithm the Convex hull is used to calculate the MBC and MIC. In this existing work [28] Xiong et al. 2012 proposed the robust fault-tolerant algorithm, which discovers the location of the jammer in wireless sensor network. The existing paper [11] Liu et al. 2011 suggested the leverage network topology mechanism and the multiple jammers were identified. Each node modifies its location table based on signal strength and PDR to identify network topology change and this identification localized the jammer. Cheng suggested the M-cluster algorithm which was based on the grouping of jammed nodes with a clustering algorithm, and each jammed node group is used to estimate one jammer location. And the bifurcation points on the skeleton base on skeletonization was used to localize jammers as per X-ray algorithm. According to the paper work was organized as mapping the jammed region, followed by identifying the bifurcation point in the jammed area and finally locate the jammer.

. In summary, the current WSN device has the mechanisms for object tracking. By using this node can spot and track the target device. The target is assisted with the sensing equipments and transmission is reliable in the network. However in the situation of portable jammer tracking, the legal packets transmission may be embarrassed due to jammer. Thereby unpredictability occurs in the data reporting step as well as it causes huge impacts on the process of target identification and tracking.

BUPT

3. Problem formulation

This section illustrates the issues associated with the portable jammer localization in the network as well as the necessity and the way to localize jammer and the hurdles inculcated in the jammer localization.

3.1 Network model

It was suggested in the anticipated system that it must have some static MHWN nodes that know their network spots. It is designed in such a manner that, the portable jammer node is connected via the entity i.e. motor which has the capability to pass through the entire MHWN's defined network area. The area where the nodes can able to sense each other, in which the node can effectively obtain the messages from other nodes and is represented as the node's hearing range. Thus, in this area the signal strength will be better for performing flawless communication. The other nodes that are not available in that concern region are connected by neighbours node. The jammer introduced into this network causes attack and hence reduces the Signal Noise Ratio and this node is represented as the node that has been jammed node, here called as dormant node. The author [14] Lie et al. 2012 adopts this classification of MHWN methodology. Based on the severity of the jammer attack, the MHWN is categorized as three parts.

- **Normal node**. If the node in the network can able to communicate with its neighbour nodes without any interruption and it is signal strength is found to be not degraded then the concern node is marked as Normal Node.
- **Dormant node**. If the node does not receive any message from any of its neighbours node then it is marked as Dormant node.
- **Border node**. The rest of the nodes in the MHWN are represented as Border node.

3.2. Jammer Representation

In order to affect the performance of the MHWN an intruder who purposefully blend with the network is identified here as the portable jammer. This jammer's main task is to makes the medium busy by engaging the concern channel frequency, thereby disturbing the transmission between the nodes which are under its range of transmission. Due to this the receiver signal was affected.

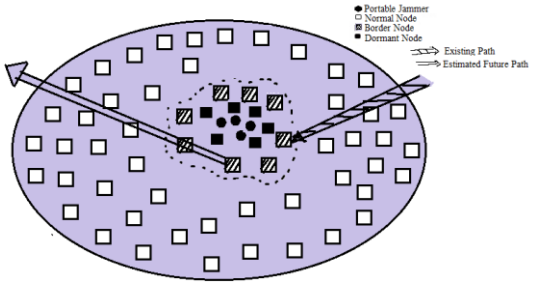


Figure. 2. Model of portable jammer path tracing in MHWN

In figure 2 portrait the structure of the MHWN, where multiple nodes are scattered and are pictures as flat nodes. These nodes have the capability to communicate with each other as these nodes are fixed with omni directional antennas and these communications are highly affected because of the open nature of the electromagnetic media. Until there is no circumstance of signal degradation all the participants' node can communicate with each other and the nodes are treated to be normal nodes. Also, these nodes have the capability to known about its position in the network by the support of GPS devices [3] Bulusu et al. 2000 accommodate with it. If in the network there are 'N' nodes, its coordinates are represented in two-dimension as {($a1$, $b1$), (a2, $b2$), …, (aN, bN)}. Generally, the nodes retain the routing table which holds its neighbor node information and will be updated frequently in a particular interval of time. The dark circular node represents the portable jammer in its motion. Due to its effect in this figure certain nodes are marked as border nodes which have partial communication capability in particular direction due to jammer presence and the rest of the nodes are marked as dormant nodes as they can't participate in the communication because it is fully under the influence of the jammer.

3.3. Signal Strength Measurement and Transmission Model

The wireless transmission follows numerous prototype for channeling, some of them are shadow path loss prototype, free space prototype etc. In the proposed work shadow path model is used to find out sustaining strength for certain distance, and it is also accepted for tracing the signal transmission path [26] Wei et al. 2018.

The Shadow path prototype is provided by applying Equation 1

$$SU_s = CH_s / d_n \quad (1)$$

BUPT

Where the channeling strength is represented as CH_s and the node's sustaining strength is represented as SU_s. In the Equation (1), the connection between CHs and SUs is represented and d denotes the distance between the jammer node and sustain node and n is fading factor.

The relaying of signal and prototype for computation holds mainly on the Received Signal Strength (RSS), which won't need any additional hardware since RSS indicator (RSSI) itself is an indicator for system of regulated communication. The logarithm design format for Equation (1) is represented in the Equation 2.

$$RSSI(d) = 10 \log SUs\ 10 \log CHs - 10n \log d + X\sigma \quad (2)$$

Where, $X\sigma$ is the shadow vanishing parameter and this parameter is represented by standard deviation. The distributed random variable also models the shadow prototype.

4. Proposed system

The Proposed work consider the network as in the figure 2 that holds channeling requirement as specified in the Equation 1 and the jamming prototype used in this work is the shadow path prototype. Also the proposed system uses RSSI for tracing the location of the jammer by following it and compute its path in the concern tracing period 't'. This tracing period is marked into several time slots 't' and during this time slots the analysis of this prototype is done. Thereby the jammer spot is estimated in the MHWN and a moving derived. The proposed work consider that the portable jammer is fixed with an omni directional antenna, thus the effect is recognized by the all the nodes surround it and the speed of the jammer is considered to be moderate, so that it won't damage the performance of the network as well as support for the smooth functioning of the network. The proposed path detection mechanism for portable jammer contains 4 steps, depending on these considerations i.e. i) selection of observing node ii) computation for jammer localization iii) next observing node selection iv) On / Off handover mechanism. Followed-by these steps the next region known to be A*A without jammer effect is identified for the data transmission even though degradation occurs by the portable jammer.

4.1 Node State Categorizations

The state of the node within the MHWN must be detected after the successful identification of the jammer. Based on that the node's state devised into i)Normal Node (NN), ii)Border Node (BN) and iii)Dormant Node (DN). The following algorithm is used to detect the node's state in the concerned timeslot based on the Signal to Noise Ratio (SNR). The threshold value (P) is set based on the signal strength. If the node does not lose any of its neighbour node then it is Normal node during the specific trace period by the observing node. In case the observing node identifies the jammer then that particular node with SNR below the threshold and can't participate in the communication is represented as the dormant node also if the node in the jammer region is represented as Border node if it does not lose any of its neighbor. The count of Border nodes in this algorithm is represented as 'K'.

Algorithm1:

Identification of Node's State:

```
If   N not found a jammer
Then
N=NN
Else
If  N= K &&  ON(SNR) > P
Then
N=NN
Else if
N≠K && ON(SNR )< P
Then
N=DN
Else
N=BN
End
End
End
```

For each period of time, a significant initial work i.e. the detection of dormant nodes due to the effect of jammer, traced the jammer's attack and the localization of the jammer is done. There are many detection methods exists for detection of basic jammers. Based on jamming attack at physical layer, many localization methods are available, which uses the signal strength computation like PDR etc. [25] Wei et al. 2017.

4.2 Observing Node Selection and Handoff process

To identify the portable jammer the proposed system, elects the exact observing node. This observing node identify the region or spot of the portable jammer at each of its tracing timeslot accurately by predicting the affected region with dormant nodes. It is necessary to dynamically regulate the observing nodes, as each observing nodes has only a limited observing area. An observing region denotes the region wherever it gets the jammer signal and discovers the jammer region. The

BUPT

observer node is chosen in such a way as a node among the border nodes. The survival of more than one border nodes in this region is the critical issue, since all these nodes are ready to act as observing node by sending willing to act packet, that increases unwanted overhead. To overcome this Algorithm 2 is proposed.

In this work the value of 'K' plays the major role where 'K' is the count of the border nodes in the particular time slot 't'. During this time period the observing node sends the hello packet to its neighbour node, in case of all the border nodes 'K' receive this hello packet, the nodes in this region are normal and hence they are active to participating in communication, in cased the value of 'K' decreased, it assures one or more than one nodes are affected. But before sending a hello signal to the border node if no other signal from the outside of the border is received by the observing node, then the current observing node cannot act as observing node further. In this situation new observing node should be nominated. The overhead of the observing node will be reduced by these procedures. Figure. 3 represents the observing node's activity.

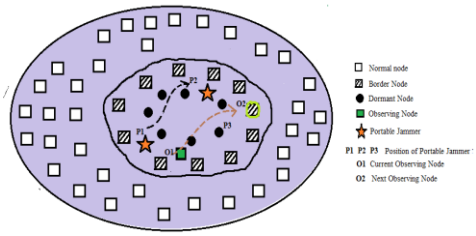


Figure. 3. Observing Node Activity Representation

Whenever the jammer begins to plot a route out of the current observing node's observing region, the tracing task will be reallocated wisely by choosing the next observing node near to the jammer's new location. Accordingly, the process of reallocating the duty of current observing node to the next newly elected observing node is known to be Handoff process. In the above figure 3 the O1 is acting as current observing node, it can able to monitor the jammer within its observing range. The portable jammer is shown in this figure which can able to move from the position P1 to P2. The current observing node has the capability to observe the jammer only up to P2 after that it won't get the signal from jammer, hence the present observing node O1 can't act as the observing node further. Based on the jammer movement the next observing node has to be chosen, here the next position of the jammer is predicted to be P3 therefore the observing node should be chosen to be boundary node near to P3 location. Process of choosing the next observing node from the current i.e. O1 to O2, while doing this all the data collected during its period will be given to the next observing node O2.

Algorithm 2: Selection of Observing node and Handover function:

Observing Node Selection

If BN wants to act as ON
Set t_wait (between 0 to time before sending WILL_ON packet)
End
Sleep(t_wait)
If this BN doesn't receive any other WILL_ON or ON_ENG within t_wait
Mark this node as ON
Else one or more WILL_ON
Select the ON with least time stamp
Mark this node as ON
Else ON_ENG received
Do Nothing
End

Observing Node declaration

If BN doesn't received WILL_ON or ON_ENG within t_wait
Compose WILL_ON packet with its {Node id, Time Stamp}
Broadcast this WILL_ON to its neighbours
Wait for a period > t_wait
Compose ON_ENG packet with {INI_BRO packet's id, Timestamp}
Broadcast the ON_ENG packet to its neighbor
Mark this node as ON
Else
Mark this node as BN
End

Observing Node Handoff

If the ON's RJSS is lower than threshold 'a'
Calculate the moving direction and moving path based on its tracking record
Calculate target position's coordinates
Initiate Handoff process by making the concern node to initiate WILL_ON
If succeeds then
Send ON_ENG to its neighbour nodes
Handover the records from precious ON to the present ON

BUPT

Previous ON becomes border node
End
End

In this algorithm 2 WILL_ON represents the packet willing to act as observing node, ON_ENG represents the packet which specify observing node engagement. These packets are passed into the MHWN nodes just like the transmission of hello packets in the network.

4.3 Reliable Lookup Algorithm (RLA) for Packet Redirection

Due to the prominent signal noise introduces in the channel because of the open nature of the medium the jammer localization become complicated RSS variation by this factor. Thereby efficiency of jammer localization will be reduced to some extent. To overcome this RLA algorithm is proposed. The threshold (β) value is set in this RLA which is the essential metric based on the level of signal strength which is 50% of the original RSS. The 'β' value is fixed based on node hearing range as well as historical evidence on signal loss or path loss exponent information. The progression in tracking the jammer attack is achieved by this threshold value. The observing node (a_o,b_o) estimated their channeling power (P) to calculate the position of each jammer node with its axis (a_j, b_j). If the concerned node relieves a higher level signal than the threshold value, then the erroneous node is discarded. The Figure 4 explains the request for destination and acknowledgement / replay packet format.

Node_ID	Time Slot	(a,b)	A*A(next region detail)

Figure. 4. Packet Format for Des_Req

In the Figure. 4 The Des_Req packet, the field (a,b) is coordinate spot of the destination. This packet format is adopted by [26] Wie et al. 2018 and the extra field A*A is added to obtain next region or next hop based on the concerned signal. The algorithm 1 is used to predict the node's state and is noted in the table for every time slot. The node id list provides the information regarding node's coordinates. Whenever the process of handoff is essential, these available nodes's table list provides the signal strength details in order to make observing node handover process successful.

This proposed mechanism is intended to redirect the data packets with the measured channeling strength obtained from the additional filed in the DES-REQ packet in the particular time slot thereby it act as the layer in the network. In this proposed mechanism, the packets are retransferred from the dormant region to the obtains next region or next hop A*A via observing node without dormant nodes by invoking border nodes which holds the node list containing the signal strength information and uses the information of the future path of this portable jammer by the observing node.

The redirection of the packet using A*A additional field is explained in this following algorithm.

Algorithm 3: RLA Algorithm

Input: Available Maximum number of try H_{max}
If Received Jammer Signal Strength RJSS < β
Evaluate the jammer node direction and trace the path
Calculate the destination axis spot
If current ON's present in the specified region
Evaluate the Destination node
If the flag of A*A =1 then
Build a Des_Req packet to next A*A region
Transmit the Des_Ack packet to the nearest neighbour
Sleep upto the Time period t_wait
Receive Des_Res packet and target node list
Else
Call Algorithm 2 for Handover of ON
If Handover succeeds
Perform the usual task of ON
End
//Packet diversion procedure
Declare HON'=0
If (HON'< H_{max})
Build HO_REQ packet from the list
If (HO_ACK) packet is received
HON'=HON'+1
Else return
End
End
End

In this algorithm HON' represents Handover Node which performs handover of data from dormant area and HO_REQ represents packet for Handover Request and HO_ACK represents packet for Handover Acknowledge. The detail of the handover are carried by the additional A*A field.

BUPT

5. Simulation and result analysis

This section discusses about the simulation setup and the results obtained for the proposed work by using NS-3 simulator

5.1. Simulator NS-3

The network was setup as per the details provide in Table 1. MHWN's performance is evaluated under the proposed portable jammer using NS-3 simulator. The nodes are spread over the entire area of the grid. The portable jammer considered here can travel the entire network and is fixed with an omni directional antenna that covers all the directions. The travelling path is divided into T = 50 separate timeslots.

Log-Distance propagation loss model is an extension of the Friis free space model. It is used to predict the propagation loss for a wide range of environment which is referred from [20]. The log-normal shadowing introduces some kind of randomness into the received signal power.

Table 1. Simulation Parameters (Setup of MHWN)

Notation	Meaning	Parameter
RP	Routing Protocol	DSR
TS	Topology Size Grid (N×N)	where N is from 10 to 20
GD	Grid Distance	1200 m
NN	Number of Nodes	*900*
SN_*ID*	Source Node ID	*#N6*
DN-ID	Destination Node	ID #9
FT	Flow Type	HTTP
PR	Packet Rate	20 pkt/sec
D	Duration	20 sec
NP	Number of packets	200
PS	Packet Size	1088 bytes
MAC	Physical address	IEEE 802.11b
WIM	Wireless Interface Mode	Ad hoc
PLM	Propagation Loss Model	Log-distance Path Loss Model
PDM	Propagation Delay Model	Constant Speed Model
S	Simulator Version	ns-3.11-RC2
L	Deployment range of wireless network	1600 m
P_T	Transmitting power of MHWN node	46.67 dBm
P_J	Transmitting power of the portable jammer	46.67 dBm
P_N	Power of Noise	−60dBm
G	Gain of transmitter and receiver	1
N	Path loss exponent	3
M	Mean of shadow shading	0
Σ	Standard deviation of shadow shading	1

5.2. Experimental results

As per the Table 1 the simulation setup, using this the simulation was done for portable jammer localization and tracing its path followed by packet diversion in the dormant region for achieving better packet delivery rate. Figure 5 shows the arrangement of various nodes in the simulation environment present in the network, as well as the portable jammer moving path.

BUPT

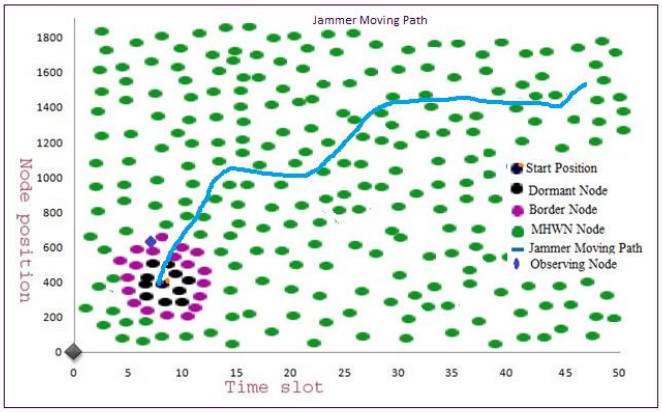


Figure. 5. Arrangement for Simulation

5.3 Measurement Estimate.

The localization of the jammer and the accuracy in path tracing is the primary measure requirement for validating the result. It represents the exactness of the jammer's original location and estimated location in each timeslot.

This was classified as three parts i) based on the position ii) based on the area iii) based on the distance. The proposed system uses the metrics based on position. In order to minimize error AMAE (Adapted Mean Absolute Error) must be computed. According to proposed system at i^{th} time slot, the simulation the Portable Jammer is marked as PJ i.e. (a_j,b_j) and Observing Node ON i.e. (a_o,b_o). The portable jammer position is represented as PJ^1_i.....PJ^n_i , respectively. If it is M observing nodes present in the every time slot 'i' then it is represented as

$$AMAE_i = 1 / M \sum_{j=1}^{M} (||ON_i^j||) \quad (4)$$

The figure 6 shows that the traced jammer position can be robust with the original jammer location of the jammer in each timeslot. The figure 6 shows the result of the traced path for portable jammer obtained by average of every observing node traced value. In this graph the X axis represent the time slot where as the Y axis specifies the node position.

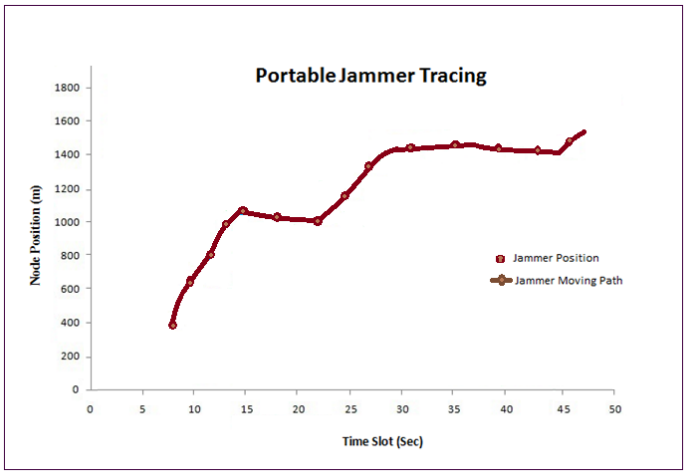


Figure. 6. Proposed Tracing Scheme

5.3 Packet Transmission under Portable Jammer

Figure 7 shows the simulation result for the packet transmission under portable jammer using RLA as well as with usual technique without RLA adoption. The graph is obtained by varying the number of nodes present in the MHWN considered in x axis and number of packets transmitted in y axis where the total packets consider for transmission are 20 packets/Sec.

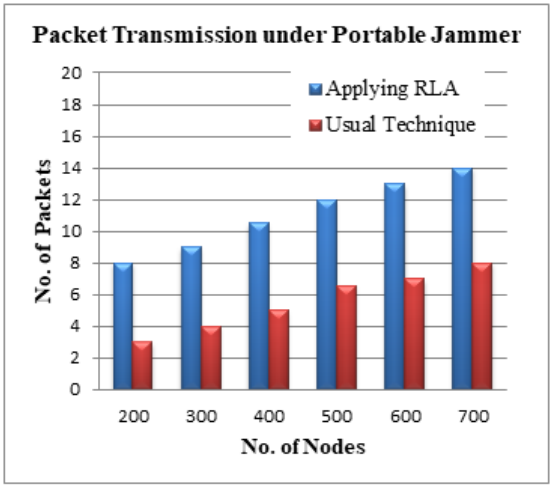


Figure. 7. Packet Transmission under Portable Jammer

6. CONCLUSION AND FUTURE WORK

The proposed work localizes the portable jammer as well as trace its path efficiently which the existing static jammer localizations mostly fails. The proposed RLA divert the data from the jammed region after localizing jammer, thereby the data packets reach its destination node. The proposed system selects the observing node first, and then identifies the location of the jammer followed by tracing its path is done. In case the

BUPT

present observing node can't sense the jammer then handoff process will be achieved in order to elect the next observing node, this is achieved by signal strength degradation. The simulation results show the tracing path of jammer as per these steps. This result showcases that the proposed algorithms have done it by efficiently traced portable jammer meanwhile it also predicts the next hop neighbour or next region information without signal degradation as A*A. Thereby proposed RLA algorithm redirects the data packet transmission. Simulation results compares and shows the packet delivery rate is achieved in the case of adopting RLA algorithm as well as with the usual transmission case. In future the work will focus on considering portable jammer with varying speed as well as diverting the data by considering the energy level of the nodes and path length there by further packet transmission can be improved.

REFERENCES

[1] Adamy, David. *EW 102: a second course in electronic warfare*. Artech house, 2004.

[2] Blumenthal, Grossmann, Golatowski and Timmermann. "Weighted centroid localization in zigbee-based sensor networks." *Proceedings of the IEEE International Symposium on Intelligent Signal Processing, WISP 2007* (2007): 1–6.

[3] Bulusu, Heidemann, and Estrin. "Gps-less low cost outdoor localization for very small devices." *IEEE Personal Communications Magazine* 7.5 (2000): 28–34.

[4] Cheng, Tianzhen, Ping Li, and Sencun Zhu. "An algorithm for jammer localization in wireless sensor networks." *Advanced Information Networking and Applications (AINA), 2012 IEEE 26th International Conference on*. IEEE, 2012.

[5] Cheng, Tianzhen, et al. "M-cluster and X-ray: Two methods for multi-jammer localization in wireless sensor networks." *Integrated Computer-Aided Engineering* 21.1 (2014): 19-34.

[6] Gezici, Sinan, et al. "Jamming of wireless localization systems." *IEEE Transactions on Communications* 64.6 (2016): 2660-2676.

[7] Hussaini, M.M. and Rajalakshmi, A., 2019. "Design and development of a new algorithm for detecting and localization of multiple attacks in wireless sensor network." *Journal of Electrical Engineering*, 19.3 (2019).

[8] Islam, M.NU., Fahmin, et al. "Denial-of-Service Attacks on Wireless Sensor Network and Defense Techniques." *Wireless Personal Communications* 116.3 (2020): 1993-2021.

[9] Liu, Hongbo, et al. "Localizing jammers in wireless networks." *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on*. IEEE, 2009.

[10] Liu, Zhenhua, et al. "Wireless jamming localization by exploiting nodes' hearing ranges." *International Conference on Distributed Computing in Sensor Systems*. Springer, Berlin, Heidelberg, 2010.

[11] Liu, Hongbo, et al. "Determining the position of a jammer using a virtual-force iterative approach." *Wireless Networks*17.2 (2011): 531-547.

[12] Liu, Sisi, Loukas Lazos, and Marwan Krunz. "Thwarting control-channel jamming attacks from inside jammers." *IEEE Transactions on mobile computing* 11.9 (2012): 1545-1558.

[13] Liu, Zhenhua, et al. "Exploiting jamming-caused neighbor changes for jammer localization." *IEEE Transactions on Parallel and Distributed Systems* 23.3 (2012): 547-555.

[14] Liu, Zhenhua, et al. "Error minimizing jammer localization through smart estimation of ambient noise." *Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on*. IEEE, 2012.

[15] Liu, Zhenhua, et al. "An Error-Minimizing Framework for Localizing Jammers in Wireless Networks." *IEEE Trans. Parallel Distrib. Syst.* 25.2 (2014): 508-517.

[16] Pang, Liang, et al. "A novel range-free jammer localization solution in wireless network by using PSO algorithm." *International Conference of Pioneering Computer Scientists, Engineers and Educators*. Springer, Singapore, 2017.

BUPT

[17] Pelechrinis, Konstantinos, et al. "Lightweight jammer localization in wireless networks: System design and implementation." *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*. IEEE, 2009.

[18] Proano, Alejandro, and Loukas Lazos. "Packet-hiding methods for preventing selective jamming attacks." *IEEE Transactions on dependable and secure computing* 9.1 (2012): 101-114.

[19] Rau, Adoor Vikramaditya, et al. "A novel method for jammer localization in large scale sensor networks." *Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference On*. IEEE, 2010.

[20]www.gaussianwaves.com/2013/09/log-distance-path-loss-or-log-normal-shadowing-model/

[21] Sun, Yanqiang, et al. "CrowdLoc: wireless jammer localization with crowdsourcing measurements." *Proceedings of the 2nd international workshop on Ubiquitous crowdsouring*. ACM, 2011.

[22] Sun, Yanqiang, et al. "Catch the Jammer in Wireless Sensor Network." *PIMRC*. 2011.

[23] Vasuhi, S., and Vijay Vaidehi. "Target tracking using interactive multiple model for wireless sensor network." *Information Fusion* 27 (2016): 41-53.

[24] Vinay Kumar Nassa . "Wireless communications: past, present and future." *Dronacharya Research Journal* 3.2 (2011): 50-54.

[25] Wei, Xianglin, et al. "Jammer localization in multi-hop wireless network: a comprehensive survey." IEEE Communications Surveys & Tutorials 19.2 (2017): 765-799.

[26] Wei, Xianglin, et al. "Collaborative mobile jammer tracking in multi-hop wireless network." *Future Generation Computer Systems* 78 (2018): 1027-1039.

[27] Wood, Anthony D., and John A. Stankovic. "Denial of service in sensor networks." *computer* 35.10 (2002): 54-62.

[28] Xiong, Kaiqi, and David Thuente. "Locating jamming attackers in malicious wireless sensor networks." *Performance Computing and Communications Conference (IPCCC), 2012 IEEE 31st International*. IEEE, 2012.

[29] Xu, Wenyuan, et al. "The feasibility of launching and detecting jamming attacks in wireless networks." *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*. ACM, 2005.

[30] Xu, Wenyuan, et al. "Jamming sensor networks: attack and defense strategies." *IEEE network* 20.3 (2006): 41-47.