Circuits and Systems, 2016, 7, 2613-2621
Published Online July 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.79226

Scientific Research Publishing

A Coincered Node Based Localization of Jammers in Wireless Sensor Networks

Balamurugan Perumal, Sharmila Vadivel, Mummoorthy Arulappan

K. S. R College of Engineering, Tiruchengode, India
Email: balamuruganp16@yahoo.co.in

Received 10 March 2016; accepted 5 April 2016; published 28 July 2016

Abstract

Jammers can awfully interfere with the wireless communications. The transmission and reception of wireless communication is blocked by the jammer. The intruder will place the jammer in a well topological network area and they can easily track the information. It will help them to block the signal transmission and reception. Now, the intention is to track the position of the jammer where it is fixed. The existing methods rely on the indirect measurements and the boundary node to find the jammer's position which degrades the accuracy of the localization. To improve the efficiency, this paper proposed an efficient method namely Coincered Node Based Localization of jammers to find the position of the jammer with high level of accuracy. The proposed system uses the direct measurements, which is the jammer signal strength. The effectiveness can also be increased by using the coincered node that will stumble across the true position of the jammer. The proposed work is compared with existing methods. Then the proposed mechanism proves better to find the jammer location. The simulation results estimate that the accuracy of the localization achieves better performance than the existing schemes.

Keywords

Wireless Sensor Network, Jamming, Jammer Localization, Jammer Signal Strength, Coincered Node

1. Introduction

The wireless communication has a tremendous improvement and its pervasiveness impact has many changes in the real world. The increasing technologies in wireless networks is not limited to the decade years, day by day the performance and also the power of the signal reaches its high level. Jamming is a behavior that is purposefully blocking the signal transmission. Jammer is a device that is used to block the nodes, which has antenna and certain level of equipment. Once the jammer is fixed in certain area, it is called as jammed region. This region

How to cite this paper: Perumal, B., Vadivel, S. and Arulappan, M. (2016) A Coincered Node Based Localization of Jammers in Wireless Sensor Networks. *Circuits and Systems*, **7**, 2613-2621. http://dx.doi.org/10.4236/cs.2016.79226

will intentionally block the area to knock out the signals which has normal transmission and reception. The blocked region nodes cannot communicate with their neighbor nodes and also to the base station. There are different types of jammers which could be classified as constant jammers, reactive jammers, deceptive jammers and random jammers.

Constant Jammers: These type of common jammer continually emits the radio signal and never mind whether the channel is idle or not.

Reactive Jammers: This type of jammer stays quiet at the transmission process and starts emitting the signal at the reception process.

Deceptive Jammers: This type of jammers continually emits the valid packets with its header and also not considers the gap between the packets.

Random Jammers: The radio signals alternates between the sleeping and the jammed mode. It stays quiet when the channel is idle.

1.1. Related Works

The problem of detecting jammers was deliberated by Wood *et al*. [1]. Later, same was deliberated by Xu *et al*. [2] and they presented some jamming models and discovered the necessity for superior detection algorithms to detect jamming. In the context of sensor networks [3] [4], jamming detection was studied. Also, jamming detection was studied networks involving frequency hopping [5].

Pelechrinis *et al*. [6] proposed to localize the jamming by measuring packet delivery rate (PDR) and performing gradient decent search. However, they did not present performance evaluation. Liu *et al*. utilized the network topology changes caused by jamming attacks and estimated the jammer's position by introducing the concept of virtual forces. The virtual forces are derived from the node states and can guide the estimated location of the jammer towards its true position iteratively. Both jamming localization algorithms are iterative-based, while our algorithm leverages the neighbor changes caused by jamming attacks to localize jammers in one round.

Xu *et al.* [2] experimented to examine radio interference attacks from both sides of the issue: First, we study the problem of conducting radio interference attacks on wireless networks, and second we examine the critical issue of diagnosing the presence of jamming attacks.

Liu *et al.* [7] Wireless Networks (WiNet) performed simulation results have shown that the virtual-force iterative approach is effective in localizing the jammer with high accuracy and outperforms the existing centroid based methods.

Bahl *et al.* [8] utilized the network topology changes caused by jamming attacks and estimated the jammer's position by introducing the concept of virtual forces. The virtual forces are derived from the node states and can guide the estimated location of the jammer towards its true position iteratively. Both jamming localization algorithms are iterative-based, while our algorithm leverages the neighbor changes caused by jamming attacks to localize jammers in one round.

The presence of jammer in a region will degrade the performance of the wireless networks. So, the localization of jammer is made at the effective area where the signals can be blocked [1]. The unintentional interference will enable the signals in a wide range of military strategies.

1.2. Our Contribution

In this work, our goal is to intentionally stumble across the accuracy of jammer localization. The existing localization mostly rely on the PDR values [2], Neighbor aware lists [9], Sending and hearing ranges [7] and calculating the jammer signal strength at boundary nodes [10]. These PDR values [2], Neighbor aware lists [9], Sending and hearing ranges [7] are an indirect measurement that is derived from the affected network topology [11] [12]. The strength of affected nodes is not participated to ensure their own values.

The recent existing method uses direct measurements with the boundary nodes which will not reflect the original signal strength of jammer [10]. But the coincered node will report the original strength of jammer of how much it is affected. The signal strength can be calculated using the distance find out between all other jammed nodes and the estimated position of jammer. A designated jammed node will collect all values of coincered node. The sink coincered node compares the values of all nodes and estimate the smallest distance. If the distance is relatively small, the estimated location is closer to the true position of the jammer.

1.3. Organization of the Paper

The remainder section of this paper is organized as follows. We depict the jammed model in Section 2. In section 3, we proposed a new system and there is an overview of the localization algorithm with the subtask of calculating coincered node estimation. Furthermore, measuring signal strength is depicted in Section 4. In Section 5, to estimate the true position of the jammer an evaluate feedback metric is calculated. Next, we present the simulation and results in Section 6. In Section 7, the paper is concluded finally. The related work is already discussed in Section 1.

2. Effect of Jamming

There are different types of jammer strategies that will disrupt the communications. Here we concentrate on constant jammer which will continually emit the radio signals and block the region whether it is idle or not [1]. These types of jammers will keep disturbing the communication of network.

By using Omni-directional antenna, every jammer has similar range in all other jammed regions. This identification of finding jammers will overcome the existing jamming localization algorithms [2] [6] [7]. The node in the network has been classified based on the disturbance of jammer to the network area. They are the Normal node, Coincered node and the boundary node.

Normal node: These nodes are able to communicate with all other nodes.

Coincered node: These nodes are blocked nodes, where it cannot communicate with all other nodes.

Boundary node: These nodes can partially communicate with their neighbors. It can report the measurement to the nodes.

Figure 1 depicts the classification of nodes based on the proximity of the jammer where circles are coincered node, triangles are boundary nodes and stars are the unaffected nodes.

3. The Proposed System

To overcome the weaknesses discussed in above section a novel method is proposed against reactive jamming attack in Wireless Sensor Network. The proposed framework is listed below and also shown in **Figure 2**.

Step 1: Initialize spare message transmission between intruder detection nodes.

Step 2: Monitor Network Communication for any interruption.

Step 3: Check whether jamming using jamming detection algorithm.

Step 4: Find the coincered node.

Step 5: Then apply localizing algorithm to locate and trap the reactive jammer in the region of duplicate communication.

Step 6: Continue the real transmission without any jamming attack.

3.1. Localization Algorithm

The proposed system has an essential play on coincered node instead of boundary node. So, the steps involved in our localization approach concentrates the procedure on coincered node. A smaller value of the distance indicates that the location of the estimated jammer is closer to the true position of the jammer.

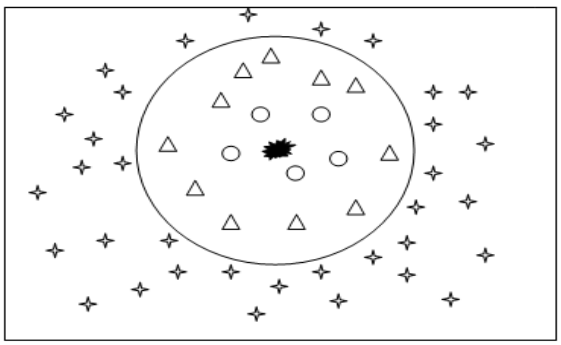

Figure 1. Classification of network nodes.

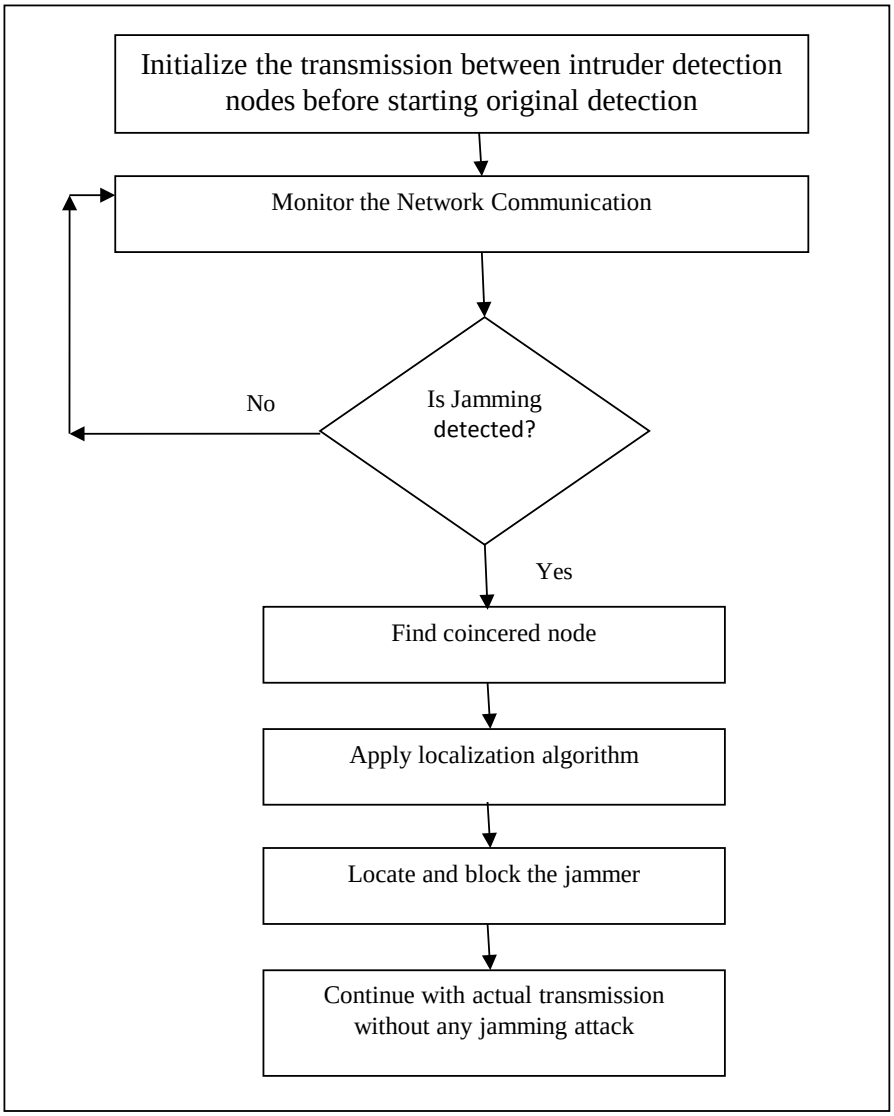

Figure 2. The proposed framework flowchart.

The few challenging subtasks involved in the formulation are as follows.
1. Coincerednode ( ) has to set the threshold value using adaptive clear channel assessment.
2. MeasureVal ( ) has to obtain the distance between the nodes to find out the signal strength of jammer.
3. EvaluateVal ( ) is to quantify the accuracy of the location of the estimated jammer position.

Algorithm 1. Jammer Localization Algorithm

```
C = Coincerednode( )
d = measureval( )
while (C>d) do
        e_v = evaluateval(c,d)
        returne_v
end while
```

This section focuses on the coincered node to measure the distance of nodes to find the signal strength. We delay the discussion of the measureval ( ) to Section 4 and the final evaluateval ( ) to the Section 5.

3.2. Coincered Node

In general, once these nodes are blocked the signals are also blocked. There is no communication between the nodes. It is the nodes that intentionally blocked by the jammer for unintentional radio interference. Since it is affected by jammer, the signal strength of jammer is much better when compared with the boundary node. The jammed nodes are liable to measure the reports by using the clear channel assessment value [7].

The adaptive clear channel assessment is one of the component of the carrier sense multiple access (CSMA) in many wireless networks [7]. In this each network node, either jammed or boundary node is subject to transmit the packets. The threshold value is set for a node once it is jammed the device samples the signal strength of jammer. The sample value is the last report by the jammed node using the threshold value is predetermined. The value from the node is allowed to calculate the distance between the estimated positions of jammer.

Consider the example; if $X_1, X_2, ...X_j$ the jammed nodes, then each node have to measure the threshold value once it is jammed. Therefore we obtain the formula for threshold value is given as

$$C = \{X_j \mid \forall X_j \in N_j, X_j > \gamma\} \tag{1}$$

where C is the coincered node, X_j is the jammed node, N_j is the number of jammed nodes and γ is the threshold value. The threshold value is set by the adaptive clear channel assessment in the network topology. The value of each coincered node is return to measure the signal strength by finding the distance between the particular node and estimated position of the jammer.

4. Measuring Signal Strength

The signal strength of jammer can be calculated by measuring the distance between each jammed node and estimated location. The previous existing method uses ambient noise floor which is readily available as commodity devices [11]. The ambient noise floor will sample the values and it is measured at each node. In theoretically, the ambient noise is the signals of unwanted values present always in the network area. The ambient noise floor is the measurement of these ambient noise values. It is yet challenging, the proposed system calculates the distance of all jammed nodes with the estimated position.

Algorithm 2. Acquiring the distance of node approximates the signal strength of jammer

Procedure **MeasureVal**

$X = X_1, X_2, ...X_j$ =MeasureVal ( )

If val(x) < threshold *then*

$X = \{X_j \mid X_j < threshold\ X_j \in X$

End if

Return mean(x)

End procedure

The Algorithm 2 depicts the values must be calculated for all coincered nodes. The mean value of x is return to the evaluate values as the actual parameter d to estimate the true position of jammers.

5. Localization Evaluate Values

In this section, it defines the metric value and the distance calculated for the smallest error value. The first process in the evaluate value is to collect all reports from the coincered nodes. A designated node will gather the x and d values to evaluate the distance. Each jammed node locally reports their values to the designated node. The rough estimation is refined by this evaluate feedback algorithm.

The property of the e_y is given as follows, the larger value of e_y indicates that the estimation position of jammer error is larger. When the estimated jammer location is equal to the value of e_y, then it indicates the true

position of jammer. Here we illustrate the property of e_y in **Figure 2**, where there are three jammed nodes are $(j1, j2, j3)$ values that are away from jammer j.

The distance calculated between the jammed node and the estimated position is denoted as d_1, d_2, d_3. After the algorithm evaluates the values of the nodes, the new distance is denoted as $d_1^{'}, d_2^{'}, d_3^{'}$, which indicates that is the distance calculated between the jammed nod and the true position of the jammer. **Figure 3** shows the estimation of jammer location by the proposed approach.

Algorithm 3. Evaluation of Localizing Jammer

Procedure $EVALUATEVAL(c,d)$

for all $i \in [1,n]$ do

$$d_i = \sqrt{(x_j - x_i)^2 + (y_j - y_i)^2}$$

end for

$$e_y = \sqrt{\frac{1}{n}\sum_{i=0}^{n}(x_j - x_i)^2}$$

end procedure

The evaluation of the localizing jammer is given by the values

$$e_y = \sqrt{\frac{1}{n}\sum_{i=0}^{n}(x_j - x_i)^2} \tag{2}$$

One of the biggest advantages of this technique is that the difference always makes the estimation error always small. This will indicates that the true position of jammer can be estimated with high level of accuracy.

6. Simulation and Results

6.1. Simulation Environment

The NS-2 simulation environment offer great flexibility in investigating the characteristics of sensor networks because it already contains flexible models for energy constrained wireless networks. This model includes features for node movements and energy constraint with a wireless sensor network in a square field with various sizes. The nodes are randomly distributed in this area. The simulation parameters are shown in **Table 1**.

6.2. Results

The transmission range of the jammer is fixed at 45 feet. To adjust the density of the sensor network, on one

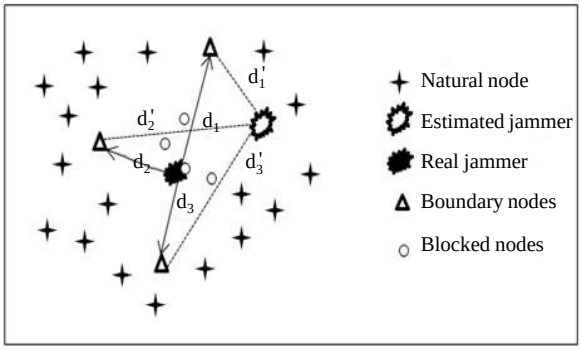

Figure 3. Estimation of jammer localization.

Table 1. Simulation parameters.

Parameter	Value
Network area	500 m × 500 m
Transmission range	45 feet
Number of nodes	50
Link capacity	500 pkts/s
Jamming Transmission power	1.5 db
Maximum jammer speed	5 m/s
Packet error rate	1.16

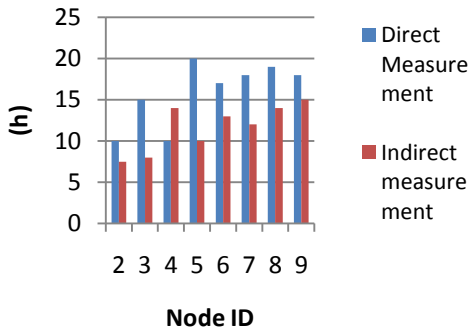

Figure 4. Measurement of individual node.

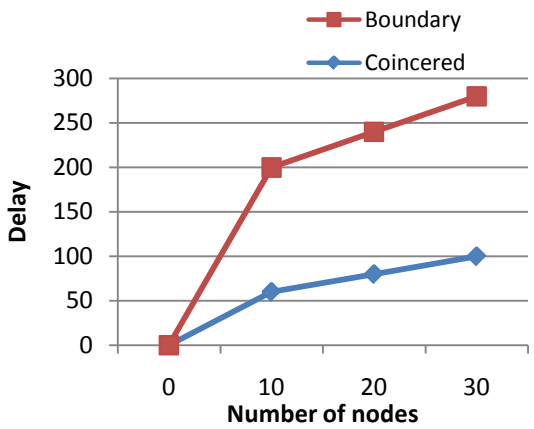

Figure 5. Delay reduced in coincered approach.

hand, varied the total number of the nodes N in simulation environment; on the other hand, extended the area of the sensor network in simulation from 300 feet. Impact of jammer's transmission range on localization error when N = 200. The impact of node density on localization error when the transmission range is 45 feet is estimated. The wireless model essentially consists of the core and the additional simulations features of Ad hoc networks. The node object is a split object. The C++ class node is derived from parent class Node. Therefore a node thus has the basic additional functions of the node from where it is derived.

In **Figure 4**, the localization of jammer has its high accuracy based on the performance of algorithm under the different network densities and various jammed regions. The multiple network nodes surround the jammer which is at the center of the simulation area. The localization error has a metric value to evaluate the accuracy of the position of jammer.

The Direct Measurement based networking has improves the accuracy of the nodes of 80%. There is better accuracy of localizing the jammer with direct measurement comparing to the indirect measurement.

Figure 5 shows the delay reduced in coincered approach. The accuracy of localizing a jammer with transmission

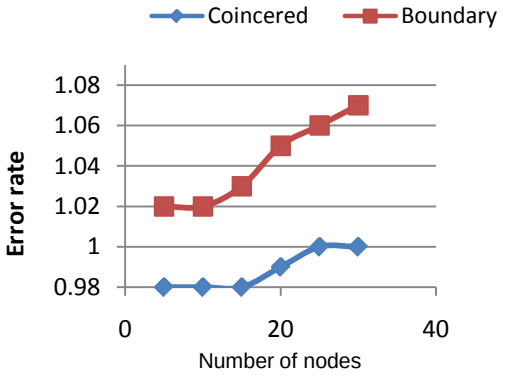

Figure 6. Error analysis of nodes.

range changes from 30 feet, 45 feet to 60 feet. The simulation is run under certain conditions to obtain the better result to localize the true position jammers.

Figure 6 shows the error analysis of nodes and error rate. Error analysis of coincered node is efficient when compared to boundary node analysis. The smallest distance between the estimated location of the jammer and the true location of the impact of jammer's transmission range is calculated.

7. Conclusion

In this paper, the performance of the direct measurement to detect and localize the jammers in network is improved. Our intensive goal is to increase the efficiency by calculating the distance between the coincered nodes and the estimated position of the jammer. The algorithm forms an approximate jammed region, and hence the center of jammed region is treated as the estimated position of jammer. The future enhancement of this paper is to concentrate on localizing the multiple jammers in the network with high level of accuracy for better enrichment.

References

[1] Wood, A.D., Stankovic, J.A. and Son, S.H. (2003) JAM: A Jammed-Area Mapping Service for Sensor Networks. *Proceedings of the* 24*th IEEE International Real-Time Systems Symposium*, 286-297.

[2] Xu, W., Trappe, W., Zhang, Y. and Wood, T. (2005) The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks. *Proceedings of ACM MobiHoc*, Urbana Champaign, 25-27 May 2005, 12 p.

[3] Çakıroğlu, M. and Özcerit, A.T. (2008) Jamming Detection Mechanisms for Wireless Sensor Networks. In: *InfoScale*'08: *Proceedings of the* 3*rd International Conference on Scalable Information Systems*, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), Brussels, 1-8.

[4] Mraleedharan, R. and Osadciw, L.A. (2006) Jamming Attack Detection and Countermeasures in Wireless Sensor Network Using Ant System. *Proceedings of the SPIE in Wireless Sensing and Processing*, **6248**, 62480G. http://dx.doi.org/10.1117/12.666330

[5] Chiang, J.T. and Hu, Y.-C. (2007) Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks. In: *MobiCom*'07: *Proceedings of the* 13*th Annual ACM International Conference on Mobile Computing and Networking*, ACM, New York, 346-349. http://dx.doi.org/10.1145/1287853.1287901

[6] Pelechrinis, K., Koutsopoulos, I., Broustis, I. and Krishnamurthy, S.V. (2009) Lightweight Jammer Localization in Wireless Networks: System Design and Implementation. *IEEE Global Telecommunications Conference*, Honolulu, 30 November 2009-4 December 2009, 1-6.

[7] Liu, Z., Liu, H., Xu, W. and Chen, Y. (2012) Exploiting Jamming-Caused Neighbor Changes for Jammer Localization. *IEEE Transactions on Parallel and Distributed Systems*, **23**, 547-555. http://dx.doi.org/10.1109/TPDS.2011.154

[8] Bahl, P. and Padmanabhan, V.N. (2000) RADAR: An In-Building RF Based User Location and Tracking System. *Proceedings of the* 19*th Annual Joint Conference of the IEEE Computer and Communications Societies*, **2**, 775-784.

[9] Liu, H., Liu, Z., Chen, Y. and Xu, W. (2010) Determining the Position of a Jammer Using a Virtual-Force Iterative Approach. *Wireless Networks*, **17**, 531-547. http://dx.doi.org/10.1007/s11276-010-0295-6

[10] Liu, Z., Liu, H., Xu, W. and Chen, Y. (2014) An Error-Minimizing Framework for Localizing Jammers in Wireless Networks. *IEEE Transactions on Parallel and Distributed Systems*, **25**, 508-517.

[11] Liu, H., Liu, Z., Chen, Y. and Xu, W. (2011) Localizing Multiple Jamming Attackers in Wireless N*etworks. Proceedings of the* 31*st International Conference on Distributed Computing Systems* (*ICDCS*), Minneapolis, 20-24 June 2011, 517-528.

[12] Cheng, T., Li, P. and Zhu, S. (2011) Multi-Jammer Localization in Wireless Sensor Networks. 17*th International Conference on Computational Intelligence and Security* (*CIS*), Hainan, 3-4 December 2011, 736-740.