An Error Minimizing Frame Work for Localizing the Jammers and Analyzing the Strength of Jammers in Wireless Network

Mahamaya Desai and S.V. Sandhya

Abstract--- *In wireless sensor network jammers are one which extremely disturb the communications, which may be intentional or unintentional jamming attacks. To avoid or discard jamming attacks from jammer, jammers location information is used, which helps the defender to defend against jamming attacks. By using indirect measurement method (hearing ranges) only one jammer is determined. In this paper to find multiple jammer in wireless network, we designed and implemented a framework which can localize one or more than one jammers in wireless sensor network with a high accuracy by utilizing direct measurement. Direct measurement uses the Jamming Signals Strength (JSS) which leads to jammers actual or approximation location. To get the global optimal solution, different heuristic search algorithms are used. This paper proposesone more method called Graph plotting method for improving performance as well as monitoring of jammers in network to defend itself from external attacks.*

Keywords--- *Jammer, Localization, Peak Value and Sensor.*

I. INTRODUCTION

THE expanding pervasiveness of remote advancements, consolidated with number of predetermined unlicensed or unwanted bands, which jams the wireless network, prompting inadvertent radio interference over all wireless devices with distinctive or various communiqué technologies yet having the same range. e.g., cordless telephones, wireless network adapters or connectors, etc.[1][2].

- *Jammer*: Jammer is a mobile communication device in mobile computing, which transmits on the same range as cell phones, to create interference that is strong cell tower, interference and block call transmission and cell phone signals. Jammers are usually undetectable and users may experience minimal effect such as poor signal reception. Jammers are illegal in many countries, except in military, government agencies and law enforcement etc., where jammers are largely used to prevent bomb detonation or to isolate suspects in hostage situation.
- *Jamming*: Unexpected interference or malicious jamming attacks cause jamming and if one or more jammers exists together which feature an adverse effect on network performance also referred as jamming.

It is essential to limit jammers for successful deployment of pervasive remote system. Because the location of jammers permit essential physical association of Wi-Fi devices which causes unexpected radio interference, or to avoid jamming attack it empowers extensively variety of defence strategies.

II. LITERATURE SURVEY

Author has discussed about how jamming attacks become most common in past few years, because of the shared nature and the open access to the remote medium. To restore normal network operations, need to find the location of jamming device, Concept of the gradient descent minimization algorithm and Packet Delivery Ratio (PDR) are used[2]. [3], Explained how the wireless communication is vulnerable to radio interference and jamming attacks, which prevent the reception of communications. To address these problems aouthor discussed about Region-based and signal-to-noise ratio (SNR)–based.Based on the level of disturbance caused by jammer. [4], Inthis paper, demonstrated how to evaluate jammers hearing range that is simply by analyzing the network topology, which changes as it goes under jamming attacks. [5], In this paper, again author has discussed about a mechanisms to localize jammers byway of exploiting jamming attacks are especially neighbor modifications. Firstly, he analyzed effect of jamming to inspect how change of communication range adjusts with respect to location of jammer and its power for transmission by using model called free space model. Here they used least-squares (LSQ) problem method. [6], discussed about Jamming attacks and inadvertent radio interference which are standouts amongst the most critical threats. These threats harms the dependability of remote communication between the nodes. In order to protect against jamming attack the jammers position has to be diagnosed first, to do this network is been divided into clusters.[7], in this paper, he discussed about jamming attacks which are easily launched but are difficult to detect. So author used optimal detection method.

III. METHODOLOGY

This paper focusses on the limitations caused by an existing methods. This new framework is designed, which focuses on indirect measurements (eg. node hearing ranges)

Mahamaya Desai, Student, Computer Science and Engineering, SDMCET/VTU, Dharwad, India. E-mail:maya.desai11@gmail.com

S.V. Sandhya, Assistant Professor, Computer Sceince and Engineering, SDMCET, Dharwad, India. E-mail:sandhya.sv@gmail.com

DOI:10.9756/BIJSESC.8231

affected by jamming attacks and jammer localization approaches mostly relay on parameters derived from the affected network topology such as packet delivery ratio, neighbour lists, etc. these methods localizes one jammer and cannot cope up with multiple jammers.

This work focuses on detecting and limiting one or multiple stationary jammers in wireless network. Enhancing the accuracy of jammers localization significantly is the primary objective function. The restrictions generated by indirect estimations of jamming effect are addressed by using direct method of JSS. In this paper, it uses two methods such as one for detecting multiple jammers and one is for defending against jamming attacks by using graph plotting method. To find multiple jammers in wireless network JSS from each node is analyzed and then based on that jammed nodes s been detected and graph plotting method gives the information of frequency and amplitude (peak value) of jamming signal. By this value we can send it back to attacking node to prevent from external attacks. Evaluation metric estimation depicts how nearer the estimated jammers location to their actual locations in the network. This can be estimated with different search algorithms. Traditional approaches tend to meet local minimum and it is difficult to meet global minimum, but this framework provides global optimum answer. To obtain global optimum it uses numerous algorithms which uses stochastic procedures.Specifically, three algorithms are analysed by this paper, such as a GPS (Generalized Pattern Search), SA (Simulated Annealing algorithm) and GA (Generic algorithm). To find the best solution among all possible solutions it uses above heuristic searching algorithms. This approach or framework can localize one or more than one jammers at the same time, regardless of the fact that their jamming locations may overlap. Localizing in this kind of scenario is known to be difficult. In the end it uses one more method called graph plotting framework for identifying jammers signals strength.

Graph plotting is a process of analysing a strength of jammers in wireless network. This paper is intended for collecting data of Radio Frequencies from FPGA board and plotting the data. The collected data is sent over to PC by Ethernet. Embedded systems are part this work, which are used to provide data via TCP/IP. This system works as client-server model and data can be retrieved through requests and responses methods. Graph plotting methods makes use of Real Time Data Acquisition Systems for continuously acquire data (Radio Frequencies), transfer this data from the digitizer to the PC in order that the data is retrieved in real-time. This real time data will be used for visualization, analysis and logging.

IV. Experimental Results

This frame work is basically used for localizing multiple jammers and as well as for decision making, so that data can be easily analysed. Finding highest frequency (peak) value, which is used to send the same frequency with high amplitude back to receiver to jam the signal and to prevent from enemies. This work classify the nodes in the following category

Jammed Node

A jammed nodes are one which cannot reach or communicate with any neighbouring nodes such as unaffected nodes in the wireless network. A node is jammed due to its loss of connectivity to unaffected node. These nodes are useful for measuring of JSS.

Unaffected Node

Unaffected nodes can communicate with all of its neighbouring nodes. Unaffected nodes are one which is not affected by jamming or jammer and these nodes does not contribute to find exact JSS measure.

Boundary Node

A part of its neighbours can be communicated, but not from all of its neighbouring nodes, are called as boundary nodes. These nodes are used in measuring JSS and it also reports the measurements of designated node for localization of jammers in wireless sensor network.

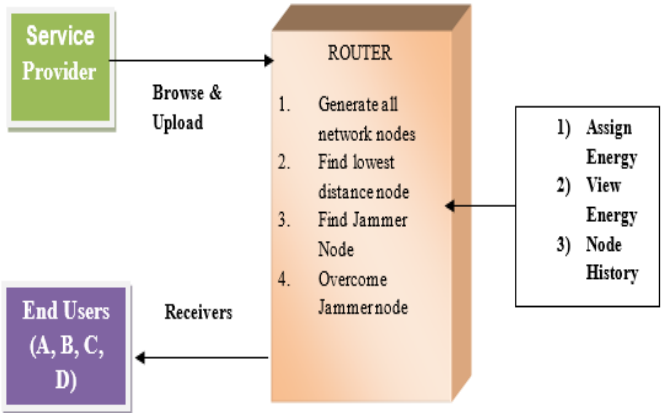

Figure 1 : Architecture Design

In this framework following are the steps to run the application and the figure 1 shows architecture design of this frame work. The service provider browses the data file path and then send to the particular receivers in network. Service provider then send the data file to wireless router present in network and the router will connect to networks, in a network smallest distance sensor node becomes activated and send to particular receiver (a, b, c…) in the network.The Wireless router manages a multiple networks (WNetwork_1, WNetwork_2, WNetwork_3, and WNetwork_4) to provide data storage service. N-number of nodes (N1, N2, N3, N4…) are present in network. Every nodes in network consists of distance and energy (power supply or battery power). Shortest distance sensor node will communicate first. The node consists of lesser energy then that node will be jammed by the jammers and then it will forward to next lesser distance node within the network. The router will show the time delay, jammed nodes, selected neighbour node and also routing path. Receiver receives the data file from the service provider via wireless router. The lesser energy sensor node will be considered as a jammer node.Attributes of this frame work are Wireless sensor networks, Compressive sensing, Jamming nodes, Radio interference, Localization, wireless router, File Management and Receivers.

Results

1. Final outcome of localization of jammer where it depicts the jammed nodes (red in colour with square shape), boundary nodes (green colour) and unaffected nodes (black colour).

Figure 2: Output of Localizing Jammers in Wireless Sensor Network

2. To run graph plotting method, it takes the input from text file which consists of amplitude and frequency. Plotted graph shows the peak value which is used to prevent from external attacks.

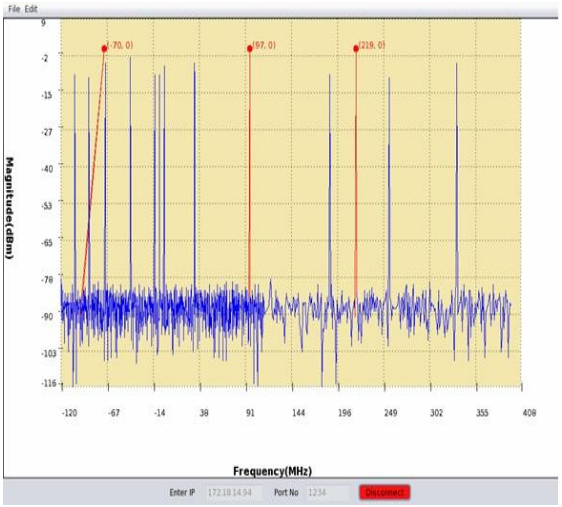

Figure 3: Plotting a Graph for the File Chosen

V. Conclusion and Future Scope

Conclusion

To reduce or decrease estimation errors, jammers needs to be localized properly. Issues of localizing jammers in wireless networks are marked by this project. Issues with Indirect measurement which is used previously can be overcome or solved by using direct measurements, which uses JSS for localizing jammers and also used to detect multiple jammers in the network, if any. Heuristics search algorithms are used for evaluation of JSS as it is challenging task in network because usually jamming signals are embedded with other signals. This framework (plotting of graph) can be used in applications where the real time data has to be plotted, analysed and logged. This frame work can be run on any system because it is completely implemented in java and this is basically used for analysing of data and finding the highest peak value (frequency) which later been used in jamming of signal to prevent from enemy activities. Even the framework discussed in this paper can be used in any applications where the real-time data has to plotted, analysed and logged.

Future Scope

To enhance the estimation accuracy, an error-minimizing framework can be used to localize jammers and this plotting method can be enhanced which can be used for monitoring of jammers in wireless network. In future this can be used for Online signal processing, Real Time Traffic Forecast and Real-time monitoring of explosives using wireless sensor networks.

Acknowledgment

I take this opportunity to express a deep sense of gratitude towards my guide Prof. S.V. Sandhya, for providing excellent guidance, encouragement and inspiration throughout this work. Without her invaluable guidance, this work would never have been a successful one. I would also like to thank or acknowled authors of my base paper "Zhenhua Liu, Hongbo Liu, Wenyuan Xu, and Yingying Chen "An Error-Minimizing Framework for Localizing Jammers in Wireless Networks", *IEEE TPDS*, vol. 25, no. 2, february 2014" is motivation for my work.

References

[1] Z. Liu, H. Liu, W. Xu and Y. Chen, "An Error-Minimizing Framework for Localizing Jammers in Wireless Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 2, Pp.508-517, 2014.

[2] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S.V. Krishnamurthy,"Lightweight jammer localization in wireless networks: System design and implementation", Proceedings of IEEE Global Telecommunications Conference(GLOBECOM), Pp. 1-6, 2009.

[3] H. Liu, Z. Liu, Y. Chen and W. Xu, "Determining the position of a jammer using a virtual-force iterative approach", Wireless Networks (WiNet), Vol. 17, Pp. 531–547, 2010.

[4] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Exploiting jamming caused neighbour changes for jammer localization", IEEE Transactions on Parallel and Distributed Systems, Vol. 23, No. 3, Pp.547-555, 2011.

[5] H. Liu, Z. Liu, Y. Chen and W. Xu, "Localizing multiple jamming attackers in wireless networks", IEEE 31st International Conference Distributed Computing Systems (ICDCS), Pp. 517-528, 2011.

[6] T. Cheng, P. Li and S. Zhu, "Multi-jammer localization in wireless sensor networks", 2011 Seventh International Conference on Computational Intelligence and Security (CIS), Pp. 736-740, 2011.

[7] M. Li, I. Koutsopoulos and R. Poovendran, "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless SensorNetworks", IEEE Transactions on Mobile Computing, Vol. 9, No. 8, Pp. 1119-1133, 2010.

[8] W. Doggett and S. Vazquez, "An Architecture for Real-Time Interpretation and Visualization of Structural Sensor Data in a Laboratory Environment", Proceedings of Digital Avionics Systems Conference (DASC), Vol. 2, Pp. 6D2-1, 2000.

[9] A. Wood, J. Stankovic and S. Son, "JAM: A jammed-area mapping service for sensor networks", IEEE Real-Time Systems Symposium, Pp. 286-297, 2003.

[10] W. Xu, W. Trappe, Y. Zhang and T. Wood, "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, Pp. 46-57, 2005.

[11] A. Goldsmith, "Wireless Communications" Cambridge University Press, 2005.

[12] T. Rappaport, "Wireless Communications-Principles and Practice" Prentice Hall, 2001.

[13] D. Goldberg, "Genetic algorithms in search, optimization and machine learning", Addison-Wesley, 1989.
[14] E. Polak, "Computational Methods in Optimization: A Unified Approach", Academic Press, 1971.
[15] P.V. Laarhoven and E. Aarts, "Simulated Annealing:Theory and Applications" Springer, 1987.

Mahamaya Desai was born in hyderabad, india, in 1993. She recived the B.E degree in information science and engineering from appa institute of engineering and technology college, gulbarga, visvesvaraya technological university belgaum ,karnataka, India in 2014 and the M.Techdegree in computer science and engineering from sdmcetdharwad, visvesvaraya technological university belgaum, karnataka, India in2016. She has done her internship at ecil co. pvt ltd hyderabad. (E-mail:maya.desai11@gamil.com)

S.V. Sandhya was born in Shimoga, Karnataka, India in 1983. She received the B.E and M.Tech in computer science and engineering from JNN college of engineering and technology, shimoga under VTU karnataka, India in 2005 and 2008 respectively. Currently she is pursuing the Ph.D. degree in computer science and engineering.

From 2005 t0 2011 she was lecturer at JNN college of engineering and technology, shimoga, Karnataka, India. She has even completed her internship at ISRO, HQ, Bangalore ,Karnataka,India currently she is working in SDMCET Dharwad, Karnataka, India as Assistant Professor. Her research interest is in Networking. In 2009 she published an ieee paper on "Fault-Tolerant Master-Workers Framework for Map Reduce Applications". (E-mail:sandhya.sv@gmail.com)