iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** VIII **Month of publication:** August 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Framework for Focusing Jammers Localization with Minimum Errors and Higher Accuracy in Wireless Networks

B.Janani[1], A.K.Puneeth Kumar[2]
[1]M.Tech CSE Student, [2]Asso.Prof, Research Scholar
Dept of CSE, SEAGI, Tirupati,

Abstract: ***Jammers can rigorously interrupt the communications in wireless networks as well in radio interferences, the jamming attacks can be destructively eliminate by the protector thus permits by the jammer location information. In this paper we explore to design a framework for focusing jammers with minimum error and higher definitiveness. For measuring the estimation errors, an evaluation of feedback metric can be explained. Almost the existing jammers-localization methods utilizes some of indirect measurements like hearing ranges that can be easily affected by jamming attacks, which does not localize the jammers accurately, Instead that we use direct measurement techniques as strength of jamming signals(JSS) .We used estimation scheme based on ambient noise floor. Also we examine several heuristic technique search algorithms for approaching the global favourable solution, and our results show that our error-minimizing-based framework achieves better performance than the previous methods.***
Keywords: Wireless Networks, jamming Localization, jammer attacks, Estimating jamming signals, ANF

I. INTRODUCTION

The increasing ubiquitous of wireless networks in commercial and military applications, which needs the reliable network deployment because of physical arrangement of wireless networks which makes threat, most likely threats are jamming attacks or radio interference. A defender can add the false messages to diminish the network communication. The defender could be a device which protests the user to gain the access for the communication. Some of the parameter approaches to find the jammers location are packet delivery ratio [1],neighbor lists[2],and nodes hearing ranges[3].
Our contribution is to design a framework for focusing the multiple jammers localization with higher accuracy. We proposed the direct measurement of strength of jamming signals; generally jamming signals are embedded with regular networks. Some commonly used RSS associated with packet does not correspond to JSS, to overcome this we advise a scheme that effectively estimating the JSS utilizing the measurement of ambient noise floor (ANF).
The ability to estimate the JSS, we consider the jamming location for different reasons:
After the network deployment the jammers start to disturb in WSN.
No detailed prior intimation about the jammers transmission is available
Multiple jammers may collude and disturb the network communication together.

A. Kind Of Jammer Attacks In Wireless Networks

A jammer is used to continuously emits RF signal by which a wireless channel get filled so that legitimates traffic will get completely blocked. The most commonly all jamming attack get characterized by their communications which are not capable of being acted with MAC protocols.

B. Models in Jammer Attack

In wireless network jamming attacks are categorized in four groups.
Constant jammer
Deceptive jammer
Random jammer

Volume 3 Issue VIII, August 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Reactive jammer

1) Constant Jammer: In this jammer, it is continuously emitting a radio signal and sending out random bits to the channel. As, It does not following any MAC layer etiquette and not waiting for the channel to become indolently.

2) Deceptive Jammer: In this jammer, continually regular packets get injected to the channel and packets deceiving the Usual nodes and normal nodes just checking the preamble and remaining noiseless.

3) Random Jammer: In this jammer, it alternately sleeping and jamming after jamming for t_j time units of time between them, it turning off its radio and entering into sleeping mode. After going to sleep for t_s units of time, it wakes up and resuming jamming constant or deceptive. t_j and t_s are randomly or fixedly intervals energy conservation.

4) Reactive Jammer: In the reactive jammer, Jammer stayed quiet when the channel indolent and it starts transmitting a radio signal as soon as it senses activity on the channel.

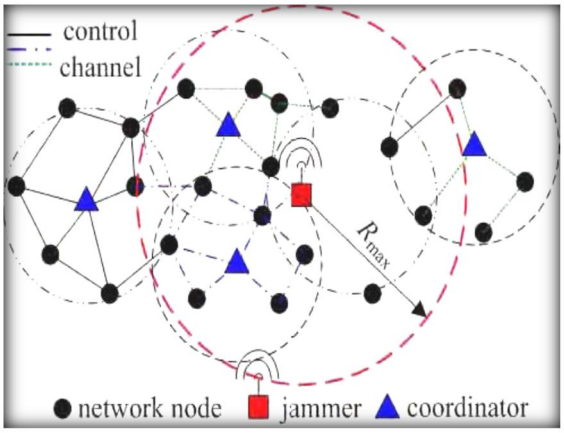


Figure: jammer attack

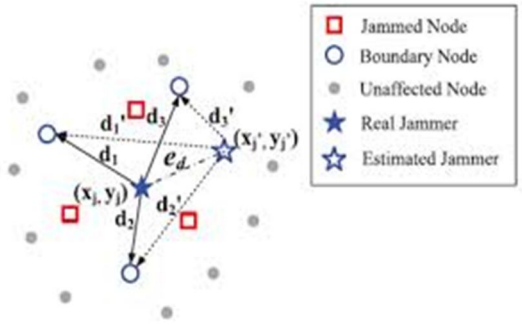
C. Network Node Classification In Jamming

These nodes are classified into three categories according to the impact of jamming.

1) Unaffected Node: The node can be unaffected if it communicates with all its neighbors.This type of nodes hardly affected by jamming which could not yield accurate JSS measurements.

2) Jammed Node: A node becomes jammed if it cannot communicate with any unaffected nodes,which could measure JSS but cannot always report measurement.

3) Boundary Node: This node can communicate with part of its neighbors not all of its neighbours.which could not measure JSS but reports their measurements to designated node for jammer localization.



II. LITERATURE SURVEY

A. Neighbor Changes for Jammers Localization

In this thesis describes about developing mechanisms to localize a jammer by exploiting neighbor changes. In First pass conduct jamming effect analysis to examine how the communication range alters with the jammer's location and transmission power using free-space model. Then, showed that a node's affected communication range can be estimated easily find within the communication range and performed jammers location by solving a least-squares (LSQ) problem that exploits the changes of communication range.

1) Advantage: Least Square (LSQ) method gives location of jammer with high accuracy when compared to the previous work like iterative search based virtual force algorithm.

2) Disadvantage: Based on LSQ, can able to find a location for single jammer, it does not explain about multiple jammers localization.

B. Localizing Multiple Jamming Attackers

The impact of jammers localization caused neighbor changes, in this work the jammers position should be identified and exploited for building a wide range of defense strategies to alleviate jamming, addressed the problem of localizing multiple jamming attackers coexisting in wireless networks by leveraging the network topology changes caused by jamming. Also systematically analyze the jamming effects and develop a framework that can partition network topology into clusters and can successfully estimate the positions of multiple jammers even when their jamming areas are overlapping.

1) Advantage: Jammers position can be easily find by partitioning network topology into cluster mode, which can be easily find the positions even when they are overlapping.

C. Multi-Jammer Localization

The existing countermeasures mainly focus on designing new communication mechanisms to survive under jamming, an alternative solution is to first localize the jammer(s) and then take necessary actions. By developing x-rayed jammed-area localization (X-ray) algorithm which skeletonizes jammed areas and estimates the jammer locations based on bifurcation points on skeletons of jammed areas. The results demonstrate that with one run of the algorithms, X-ray is efficient in localizing multiple jammers in WSN with small errors.

D. RSS-Based Localization For Improving Localization Accuracy

Among the large class of localization schemes, RSS-based localization methods have the advantage of providing closed-form solutions for mathematical analysis as compared to heuristic-based localization approaches. However, the localization accuracy of RSS-based localization methods are significantly affected by the unpredictable setup in indoor environments.

E. Jamming Localization By Exploiting Nodes' Hearing Ranges

By developing mechanisms to localize a jammer, first conducted jamming effect analysis to examine how a hearing range, for example the area from which a node can successfully receive and decode the packet, modify with the jammer's location and transmission power. It shows that the pretend hearing range can be estimated purely by inspect the network topology changes caused by jamming attacks. Hence solved the jammer location estimation by constructing a least-squares problem, which utilize the changes of the hearing ranges.

III. ALGORITHM FOR JAMMERS LOCALIZING FRAMEWORK

The several heuristic search algorithms for approaching the global optimal solution. The search based jammers localization approaches have a few challenging subtasks.

Evaluate Metric () which defines an appropriate metric to quantify the accuracy of estimated jammers locations.

Measure JSS () Which obtain JSS even if it may be embedded in regular transmission.

Search for Better () which obtains efficiently search for the best estimation.

Algorithm: Jammers localization framework

In this algorithm, formulating the evaluation feedback metric using collected jss measurements.

1: p =Measure JSS()
2: z=Initial positions
3: while Terminating Condition True do

4: e_z = EvaluateMetric(z,p)
5: if NotSatisfy(e_z) than
6: z = SearchForBetter()
7: end if
8: end while

A. Network Classification

We classify the network nodes based on the level of disturbance caused by jammers, and identify the nodes that can participate in jammer localization, e.g., the ones that can measure and report the JSS. Essentially, the communication range changes caused by jamming are reflected by the changes of neighbors at the network topology level. Thus, the network nodes could be classified based on the changes of neighbors caused by jamming. We define that node B is a neighbor of node A if A can communicate with B prior to jamming. The network nodes can be classified into three categories according to the impact of jamming: unaffected node, jammed node, and boundary node.

B. Evaluation Metric

Essentially, our jammer localization approach works as follows. Given a set of JSS, for every estimated location, we are able to provide a quantitative evaluation feedback indicating the distance between the estimated locations of jammers and their true locations. For example, a small value of evaluation feedback indicates that estimated locations are close to the true ones, & vice-versa.

1) Single Jammer: Assume a jammer J located at (x_J, y_J) starts to transmit at the power level of P_J , and m nodes located at {(x_i , y_i)}i∈[1,m] become boundary nodes. To calculate e_z , each boundary node will first measure JSS locally and we denote the JSS measured at boundary node i as Pr_i . Then the current estimation of the jammers j's location can be calculated.

*2) Multiple Jammers:*Similar to single jammer, we assume n jammers located at {(xJi , yJi)}i∈[1,n] start to transmit at the power level of {PJi }i∈[1,n] separately at the same time, and m nodes located at {(xi , yi)}i∈[1,m] become boundary nodes. To calculate e_z , each boundary node measures JSS locally and we denote the JSS measured at boundary node i as Pri which is a combined JSS from multiple jammers. We can include all the variables to be estimated, i.e., current estimation of the n jammers locations and the transmission powers, calculated in a form of matrix.

Algorithm 2 Evaluation feedback metric calculation.

1: **procedure** EVALUATEMETRIC($\hat{\mathbf{z}}$, p)
2: **for all** $i \in [1, m]$ **do**
3: $\hat{X}_{\sigma_i} = P_{r_i} - P_{f_i}(\hat{\mathbf{z}})$
4: **end for**
5: $e_z = \sqrt{\frac{1}{m}\sum_{i=1}^{m}(\hat{X}_{\sigma_i} - \hat{\bar{X}}_{\sigma})^2}$
6: **end procedure**

C. Measure JSS

Calculating JSS is equivalent to obtaining the average of the Ambient Noise Floor (ANFs), i.e., mean (s_a). In most cases, $s_c = \emptyset$ and $s_a \subset s$. In a special case where no sender has ever transmitted packets throughout the process of obtaining n measurements, $s_c = \emptyset$ and $s_a = s$. The algorithm for calculating the ANF should be able to cope with both cases. A regular node will take n measurements of the ambient noise measurements. It will consider the ANF as the average of all measurements if no sender has trans- mitted during the period of measuring; otherwise, the ANF is the average of s_a , which can be obtained by filtering out sc from s. The intuition of differentiating those two cases is that if only jamming signals are present, then the variance of n measurements will be small; otherwise, the ambient noise measurements will vary as different senders happen to transmit. The correctness of the algorithm is supported by the fact that s_a is not likely to be empty due to carrier sensing, and the JSS approximately equals to the average of s_a. The algorithm for acquiring the ambient noise floor ,In particular each node is denoted as sample *n* measurements of ambient noise at a constant rate and denote them as a s=[s1,s2,s3,……s_n]

Algorithm for Acquiring a ambient noise floor,approximates the strengthen of jamming signals.

1: procedure MEASUREJSS
2: $s=\{s1,s2,\ldots..,s_n\}$= MeasureRss()
3: if var(s)<varianceThresh then
4: $s_a=s$
5: else
6: JssThresh=min(s)+α[MAX(S)-MIN(S)] ►$\alpha\epsilon[0,1]$
7: SA={SI|SI<jSSTHRESH , $s_i \epsilon s$}
8: endif
9: return mean(s_a)
10: end procedure

D. Best Estimation

The jammer localization problem can be modeled as a non-linear optimization problem and finding a good estimation of jammers locations is equivalent to seeking the solution that minimizes the evaluation feedback metric e_z. We use several search algorithms that rely on guided random processes to approach the global optimum without converging to a local minimum.

E. Algorithms

A (Genetic algorithm) GA [6] searches for the global optimum by mimicking the process of natural selection in biological evolution. A GA emphasis to generate a set of solutions known as a population. At each repetition, a GA selects a subset of solutions to form a new population based on their "fitness "and also randomly generates a few new solutions. As a result, the "fitter" solutions will be genetic. At the same time, new solutions will be introduced to the population, which may turn out to be "fitter" than ever. As a result, over ensuing generations, a GA is likely to escape from local optima and "evolves" toward an optimal solution. In the application of searching for the best estimation of jammers' locations, each individual has chromosome of 3n genes, comprising n jammers' coordinates and jamming power levels. We defined the fitness of each individual as e_z. The smaller e_z is, the better.

A (Graph processing system)GPS algorithm [7] works similarly to the gradient descent algorithm. However, at each iteration, instead of making a step toward the steepest gradient, a GPS checks a set of solutions around the current solution, looking for the one whose corresponding function value is smaller than the one at the current solution. If a GPS finds such a solution, the new solution becomes the current solution by the next step of the algorithm. By searching for a mesh of solutions, a GPS is likely to find a consequence of solutions to an optimal one without converging to a local minimum.

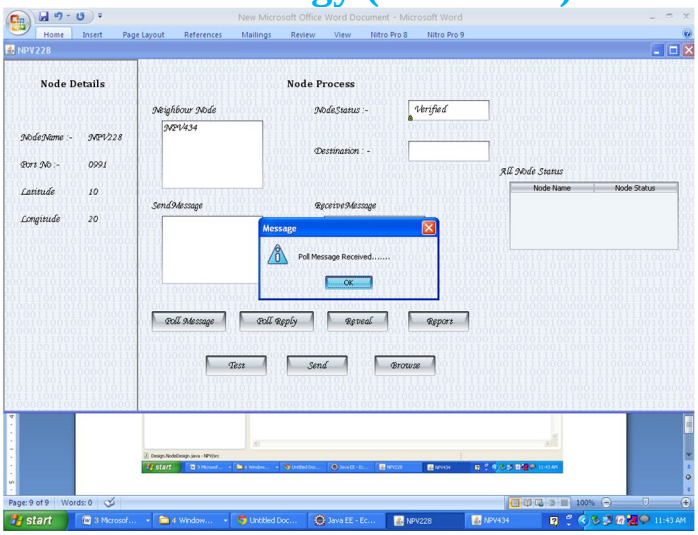
A (Simulated annealing) SA algorithm [8] searches for the optimal solutions by modeling the physical process of heating a material and then controlled lowering the temperature to decrease defects. At each iteration, the SA algorithm compares the current solution with a randomly generated new solution. The new solution is selected according to a probability distribution with a scale proportional to the temperature and it will replace the current solution according to a probability governed by both the new object function value and temperature. By accepting "worse" solutions occasionally, the algorithm avoids being trapped in local minima, and it is able to explore solutions globally.

IV. EXPERIMENTAL RESULTS

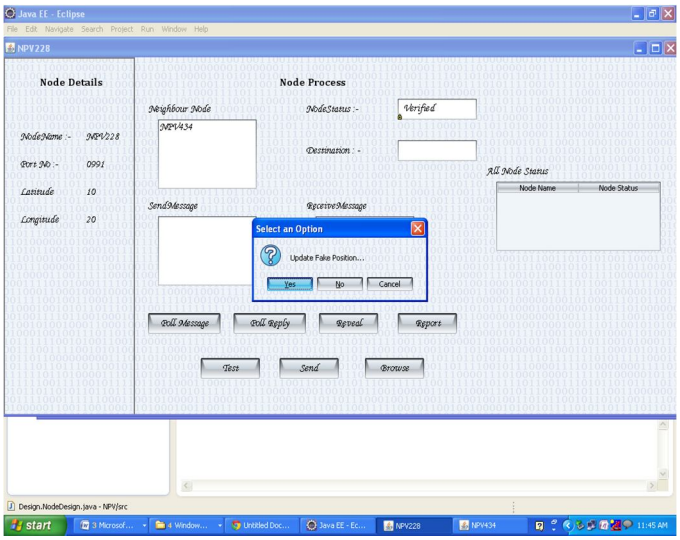
This system model is implemented using java platform. The system is designed with set of nodes among which one node acts as source and another acts as authorized designation node. The source node is authorized before it is communicates with destination node. A file is transferred from source to destination with security mechanism. Because of this error reduction scheme is used for transferring the file between the nodes, the data is send with more secured way by identifying the jammers and finding the best route in the network nodes to reach the destination node.

A. The Source Node Gets Authorized Before It Communicates With Destination Node.(i.e. Poll Message Received)

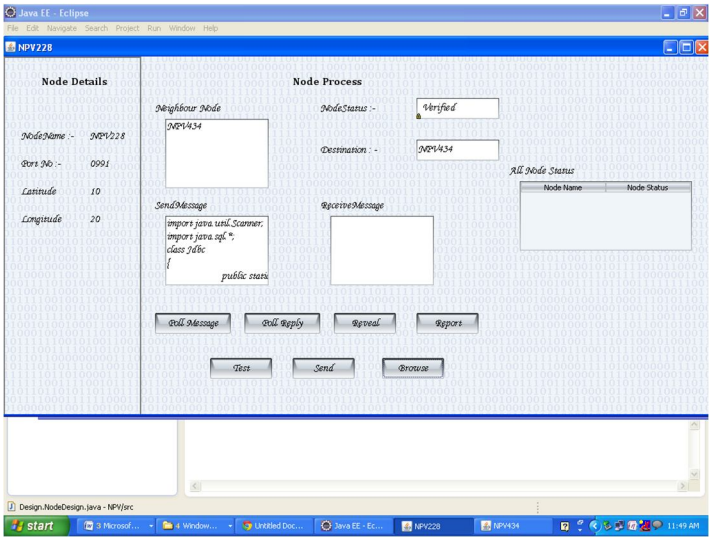
Volume 3 Issue VIII, August 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)



B. Node Which Becomes The Faulty Node (i.e. Updating Fake Position)

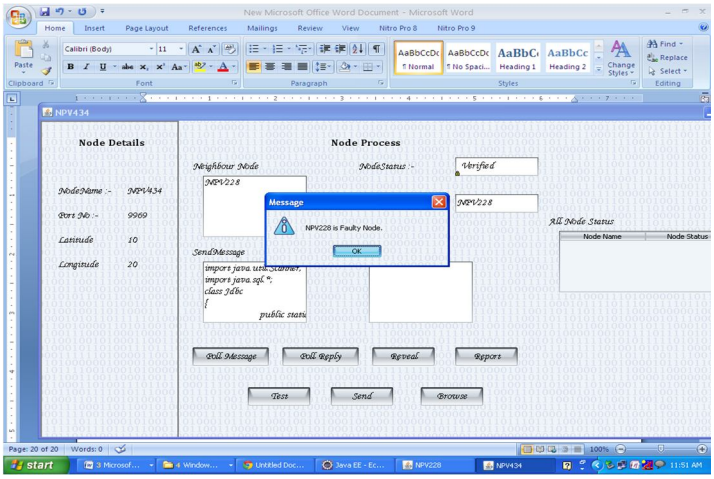


C. Transferring A File From Sender Node To Receiver Node (i.e.. Source Node To Destination Node)



Volume 3 Issue VIII, August 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

D. The File Cannot Be Delivered To The Destination Node Because Its Finds The Node Is Faulty Node (i.e. Jammed Node).



V. CONCLUSION

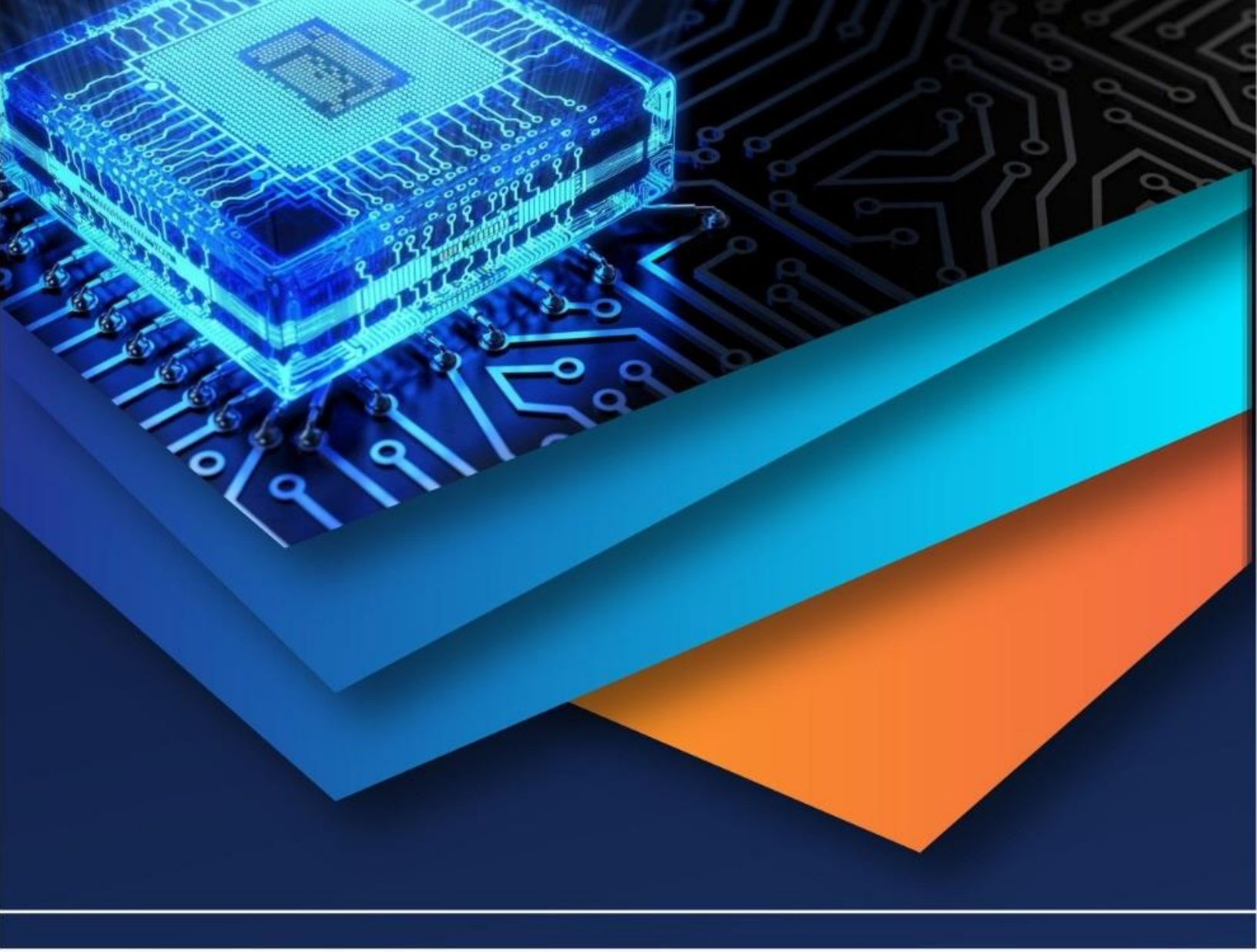
Jamming is still an important research problem. We addressed the problem of localizing jammers when comparing to the previous work the localization of jammers gives less accuracy and chances for packet loss. In this work, we addressed the problem of localizing jammers in wireless networks , pursue to extremely reduce estimation errors with higher accuracy. Estimating JSS is considered challenging because they are usually embedded with other signals. Our estimation scheme smartly derives ANFs as the JSS utilizing the available signal strength measuring capability in wireless devices. For further improving the estimation accuracy, we designed an error minimizing framework to localize jammers. In particular, we defined an evaluation feedback metric that quantifies the estimation errors of jammers' positions. We treated the evaluation feedback metric as the objective function for the error minimizing purpose. We examined that our framework gives the localization of jammers with high accuracy when compared to the previous work.

VI. FUTURE WORK

Our future concept, Network Intrusion detection and Countermeasure selection in virtual network systems to establish a begin set up, a defense-in-depth intrusion detection framework. Some of the intrusion prevention scheme is 1.Frequency hopping 2.Spatial retreats 3.PHY layer anti-jamming techniques. By using this prevention schemes we can gain accurate localization of jammer for better attack detection, incorporates attack graph analytical procedures into the intrusion detection processes.

REFERENCES

[1] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Exploiting Jamming-Caused Neighbor Changes for Jammer Localization," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 3, pp. 547-555, Mar. 2012.
[2] H. Liu, Z. Liu, Y. Chen, and W. Xu, "Localizing Multiple Jamming Attackers in Wireless Networks," Proc. 31st Int'l Conf. Distributed Computing Systems (ICDCS), 2011.
[3] T. Cheng, P. Li, and S. Zhu, "Multi-Jammer Localization in Wireless Sensor Networks," Proc. Seventh Int'l Conf. Computational Intelligence and Security (CIS), 2011.
[4] J. Yang, Y. Chen, and J. Cheng, "Improving Localization Accuracy of RSS-Based Lateration Methods in Indoor Environments," Ad Hoc and Sensor Wireless Networks, vol. 11, nos. 3/4, pp. 307-329, 2011.
[5] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Wireless Jamming Localization by Exploiting Nodes' Hearing Ranges," Proc. IEEE Int'l Conf. Distributed Computing in Sensor Systems, 2010.
[6] D. Goldberg, Genetic Algorithms in Search, Optimization and Machine Learning. Addison-Wesley, 1989.
[7] E. Polak, Computational Methods in Optimization: A Unified Approach. Academic Press, 1971.
[8] P.V. Laarhoven and E. Aarts, Simulated Annealing: Theory and Applications. Springer, 1987.
[9] Google scholar: Denial of service attacks in wireless networks: The case of jammers.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY