ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

A Framework for Detection of Jammers in Wireless Sensor Network

S.Jaipriya

Department of ECE, Kumaraguru College of Technology, Coimbatore, Tamilnadu, India

ABSTRACT: Jammers can severely disrupt the communications in wireless networks, and jammers' position information allows the defender to actively eliminate the jamming attacks. Thus, in this first phase aim to design a framework that can localize one or multiple jammers with a high accuracy. Most of existing jammer localization schemes utilize indirect measurements (e.g., hearing ranges) affected by jamming attacks, which makes it difficult to localize jammers accurately. In first phase exploit a direct measurement the strength of jamming signals (JSS). Estimating JSS is challenging as jamming signals may be embedded in other signals. As such, it devises an estimation scheme based on ambient noise floor and validates it with simulation experiments. To further reduce estimation errors, it define an evaluation feedback metric to quantify the estimation errors and formulate jammer localization as a nonlinear optimization problem, whose global optimal solution is close to jammers' true positions. The proposed explore several heuristic search algorithms for approaching the global optimal solution, and our simulation results show that our error-minimizing-based framework achieves better performance than the existing schemes.

KEYWORDS: jamming, localization, optimization

I. INTRODUCTION

The rapid advancement of wireless technologies has enabled a broad class of new applications utilizing wireless networks, such as patient tracking and monitoring via sensors, traffic monitoring through vehicular ad hoc networks, and emergency rescue and recovery based on the availability of wireless signals. To ensure the successful deployment of these pervasive applications, the dependability of the underneath wireless communication becomes utmost important. One threat that is especially harmful is jamming attacks. The broadcast-based communication combined with the increasingly flexible programming interference of commodity devices makes launching jamming attacks with little effort. For instance, an adversary can easily purchase a commodity device and reprogram it to introduce packet collisions that force repeated back off of other legitimate users and thus, disrupt network communications.

Those defense technologies provide useful methods to alleviate jamming. However, they primarily reply on the network to passively adjust themselves without leveraging the information of the jammer. We take a different viewpoint, that is, networks should identify the physical location of a jammer and use such information to actively exploit a wide range of defense strategies in various layers. For instance, a routing protocol can choose a route that does not traverse the jammed region to avoid wasting resources caused by failed packet deliveries. Furthermore, once a jammer's location is identified, one can eliminate the jammer from the network by neutralizing it. This approach is especially useful for coping with an unintentional radio interferer that is turned on accidentally. In light of the benefits, in this paper, we address the problem of localizing the position of jammers when multiple jamming attackers coexist in a wireless network.

A. Type of Jamming Attack

Although several studies have targeted jamming attacks but definition of jamming was unclear. An assumption is made that jammer transmits RF signal in wireless channel, so that channel is completely blocked and intended receiver may not be able to receive message. Therefore, jammer is an entity who is purposefully trying to interfere with transmission and reception of message across the wireless channel. Recently, several jamming strategies have been introduced. Later, jammers were categorized into four models. They are

- **Constant jammer**
- **Reactive jammer**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

- **Deceptive jammer**
- **Random jammer**

a) Constant Jammer

In this model, jammer continuously emits RF signals and it transmits random bits of data to channel. It does not follow any MAC layer etiquette. Being constant to the transfer it does not wait for channel to become an idle.

b) Deceptive Jammer

In this model, jammer constantly injects series packets to the channel without any gap between subsequent transmissions. It also broadcasts fabricated messages and reply old ones. Jammer will pass preambles out to the network and just check the preamble and remain silent.

c) Random Jammer

In this model, jammer alternates between period of continuous jamming and inactivity. After jamming for t1 units of time, it stops emitting radio signals and enter into sleep mode. The jammer after sleeping for t2 units of time wakes up and resumes jamming. Both time t1 and t2 is either random or fixed.

d) Reactive Jammer

In this model, jammer will stay quite when the channel is idle. As soon as it senses activity on channel, it starts transmitting signal. In order to sense the channel jammer
is ON and should not consume energy.To mitigate jamming attacks many hiding schemes were used. These are

- Strong hiding commitment scheme
- Cryptographic puzzle base scheme
- All-or-nothing transmission

II. LITERATURE SURVEY

Jamming and radio interference are known threats and have attracted much attention. Traditionally, jamming is addressed through conventional PHY-layer communication techniques e.g. spreading techniques. Countermeasures for coping with jamming in commodity wireless networks have been intensively investigated. Defense strategies include the use of error correcting codes to increase the likelihood of decoding corrupted packets, channel hopping to adapt the working channel to escape from jamming, and wormhole-based anti-jamming techniques. Range-based algorithms involve estimating distance to anchor points with known locations by utilizing the measurement of various physical properties, such as RSS.

A. Nodes' Hearing Ranges Based Jammer Detection

Proposed a hearing-range-based localization scheme that also exploits the network topology changes caused by jamming attacks. In particular, to quantify the network topology changes, we introduced the concept of a node's hearing range, an area from which a node can successfully receive and decode the packet[1]. We have discovered that a jammer may reduce the size of a node's hearing range, and the level of changes is determined by the relative location of the jammer and its jamming intensity. Therefore, instead of searching for the jammer's position iteratively, we can utilize the hearing range to localize the jammer in one round, which significantly reduces the computational cost yet achieves better localization performance than prior work.

B. Jammer Detection Based On Signal Strength

One seemingly natural measurement that can be employed to detect jamming is signal strength, or ambient energy. The rationale behind using this measurement is that the signal strength distribution may be affected by the presence of a jammer. In practice, since most commodity radio devices do not provide signal strength or noise level measurements that are calibrated (even across devices from the same manufacturer), it is necessary for each device to employ its own empirically gathered statistics in order to make its decisions[2]. Each device should sample the noise levels many times during a given time interval. By gathering enough noise level Measurements during a time period prior to jamming, network devices can build a statistical model describing normal energy levels in the network.

C. Jammer detection based on generic localization algorithm

Our goal is to exploit the inherent propagation characteristics of the wireless channel in order to expose the presence of jamming devices and localize them. The jamming attacker might be able to hide itself from all but the wireless

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

channel's propagation characteristics[3]. The attributes of the jamming signals (and in particular their spatial properties) can affect measurable attributes (such as the PDR) to varying degrees in different parts of the network, thereby revealing important information with regards to the location of the malicious device. significant performance improvement can be attained with the elimination of the local minima sensitivity. Thus, intelligent ways that can help avoid local-minima regions are needed. One possible way could be to gather all the information with regards to PDR (collected by each legitimate node) and try to fuse these data. A majority rule could subsequently be used in order to decide upon the location of jammer(s). However, since dense-deployment regions might contain most of the nodes, the majority of the votes might still point to a local minimum. Therefore, what is required is a way to increase the confidence of the users' decisions with regards to the location of the jammer. In particular, nodes need to be able to effectively distinguish between jamming interference and heavy, legitimate interference.

D. Neighbor Changes For Jammer Localization

Jamming attacks are especially harmful when ensuring the dependability of wireless communication. Finding the position of a jammer will enable the network to actively exploit a wide range of defense strategies. In this paper, we focus on developing mechanisms to localize a jammer by exploiting neighbor changes[4]. We first conduct jamming effect analysis to examine how the communication range alters with the jammer's location and transmission power using free space model. Then, we show that a node's affected communication range can be estimated purely by examining its neighbor changes caused by jamming attacks and thus, we can perform the jammer location estimation by solving a least-squares (LSQ) problem that exploits the changes of communication range. Compared with our previous iterative-search-based virtual force algorithm, our LSQ based algorithm exhibits lower computational cost (i.e., one-step instead of iterative searches) and higher localization accuracy.
Furthermore, we analyze the localization challenges in real systems by building the log-normal shadowing model empirically and devising an adaptive LSQ-based algorithm to address those challenges.

E. Jammer Detection Based On Virtual-Force Iterative Approach

Wireless communication is susceptible to radio interference and jamming attacks, which prevent the reception of communications. Most existing anti-jamming work does not consider the location information of radio interferers and jammers. However, this information can provide important insights for networks to manage its resource in different layers and to defend against radio interference. In this paper, we investigate issues associated with localizing jammers in wireless networks. In particular, we formulate the jamming effects using two jamming models: region-based and signal-to-noise-ratio(SNR)- based; and we categorize network nodes into three states based on the level of disturbance caused by the jammer. By exploiting the states of nodes, we propose to localize jammers in wireless networks using a virtual-force iterative approach. The virtual-force iterative localization scheme is a range-free position estimation method that estimates the position of a jammer iteratively by utilizing the network topology. We have conducted experiments to validate our SNR-based jamming model and performed extensive simulation to evaluate our approach.

F. Jammer Detection Based RSS Techniques

Location estimation is a critical step for many location-aware applications. To obtain location information, localization methods employing received signal strength (RSS) are attestative since it can reuse the existing wireless infrastructure for localization. Among the large class of localization schemes, RSS-based lateration 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 lateration methods are significantly affected by the unpredictable setup in indoor environments. To improve the applicability of RSS-based lateration methods in indoors, we propose two approaches, regression-based and correlation-based. The regression-based approach uses linear regression to discover a better fit of signal propagation model between RSS and the distance, while the correlation-based approach utilizes the correlation among RSS in local area to obtain more accurate signal propagation.

III. EXISTING METHOD

Jamming and radio interference are known threats and have attracted much attention. Traditionally, jamming is addressed through conventional PHY-layer communication techniques, e.g. spreading techniques. Those PHY-layer techniques provide resilience to interference at the expense of advanced transceivers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Countermeasures for coping with jamming in commodity wireless networks have been intensively investigated. Defense strategies include the use of error correcting codes to increase the likelihood of decoding corrupted packets, channel hopping to adapt the working channel to escape from jamming, and wormhole-based anti-jamming techniques. Received signal strength (RSS) is an attractive approach because it can reuse the existing wireless infrastructure. Based on the localization methodology, the localization algorithms can be categorized into range-based and range-free. Range-based algorithms involve estimating distance to anchor points with known locations by utilizing the measurement of various physical properties, such as RSS. Localize the jamming by measuring packet delivery rate (PDR) and performing gradient decent search. Virtual force iterative localization algorithm (VFIL).Lease-squares-based algorithm that leverages the change of hearing range caused by jamming. Aforementioned algorithms can only localize one jammer and may fail to yield jammers' positions when multiple ones are present.

IV. PROPOSED METHOD

The proposed system estimating JSS is challenging as jamming signals may be embedded in other signals. As such, we devise an estimation scheme based on ambient noise floor and validate it with real-world experiments. To further reduce estimation errors, we define an evaluation feedback metric to quantify the estimation errors and formulate jammer localization as a nonlinear optimization problem, whose global optimal solution is close to jammers' true positions. We explore several heuristic search algorithms for approaching the global optimal solution, and our simulation results show that our error-minimizing-based framework achieves better performance than the existing schemes.

We summarize our main contributions as follows:

Estimating JSS is challenging because the jamming signals are embedded in the regular signals. To the best of our knowledge, our work is the first that directly utilizes the JSS to localize jammers. Our results using direct measurements (e.g., JSS) exhibit significant improvement compared with those using indirect measurements (e.g., hearing ranges).We exploited path loss and shadowing phenomena in radio propagation and defined an evaluation metric that can quantify the accuracy of the estimated locations. Leveraging such an evaluation metric, we formulated the jammer localization problem as an error-minimizing framework and studied several heuristic searching algorithms for finding the best solution.Our error-minimizing-based algorithms can localize multiple jammers simultaneously, even if their jamming areas overlap. Localizing in such a scenario is known to be challenging

To overcome these challenges and increase the localization accuracy, we formulate the jammer localization problem as a nonlinear optimization problem and define an evaluation metric as its objective function. The value of evaluation metric reflects how close the estimated jammers' locations are to their true locations, and thus, we can search for the best estimations that minimize the evaluation metric. Because traditional gradient search methods may converge to a local minimum and may not necessarily yield the global minimum, we adopt several algorithms that involve stochastic processes to approach the global optimum. In particular, we examined three algorithms: a genetic algorithm (GA), a generalized pattern search (GPS) algorithm, and a simulated annealing (SA) algorithm.

The network nodes can be classified into three categories according to the impact of jamming:

1. *Unaffected node*: A node is unaffected if it can communicate with all of its neighbors. This type of node is barely affected by jamming and may not yield accurate JSS measurements.
2. *Jammed node*: A node is jammed if it cannot communicate with any of the unaffected nodes. We note that this type of node can measure JSS, but cannot always report their measurements.
3. *Boundary node*: A boundary node can communicate with part of its neighbors but not from all of its neighbors. Boundary nodes can not only measure the JSS, but also report their measurements to a designated node for jamming localization.

The search-based jammer localization approaches have a few challenging subtasks:

1. EvaluateMetric() has to define an appropriate metric to quantify the accuracy of estimated jammers' locations.
2. MeasureJSS() has to obtain JSS even if it may be embedded in regular transmission.
3. SearchForBetter() has to efficiently search for the best estimation.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

A. Attacker Model

Assume each jammer is equipped with an omni-directional antenna. Thus, every jammer has a similar jamming range in all directions. Identification of jammers' positions will be performed after the jamming attack is detected, and we assume the network is able to identify jamming attacks and obtain the number of jammers, leveraging the existing jamming detection approaches.

B. Localization Evaluation Metric

The definition of the evaluation metric ez, and we show the property of ez as well as its calculation.

Algorithm 1. Jammer Localization Framework
1: p = MeasureJSS()
2: z = Initial positions
3: while Terminating Condition True do
4: ez = EvaluateMetricðz; pÞ
5: if NotSatisfy(ez) than
6: z = SearchForBetter()
7: end if
8: end while

Algorithm 2. Evaluation feedback metric calculation.
1: procedure EVALUATEMETRIC $(\hat{z}, p)$
2: for all $i \in [1, m]$ do
3: $\hat{X}_{\sigma_i} = P_{ri} - P_{fi}(\hat{Z})$
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. Ambient Noise Measure

Ambient noise is the sum of all unwanted signals that are always present, and the ANF is the measurement of the ambient noise. In the presence of constant jammers, the ambient noise includes thermal noise, atmospheric noise, and jamming signals.

$$P_N = P_J + P_w$$

where PJ is the JSS, and PW is the white noise comprising thermal noise, atmospheric noise, and so on. Realizing that at each boundary node PW is relatively small compared to PJ , the ANF can be roughly considered as JSS. Thus, estimating JSS is equivalent to deriving the ANF at each boundary node. In this work, we consider the type of wireless devices that are able to sample ambient noise.

D. Measure Jamming Signal

To derive the JSS, our scheme involves sampling ambient noise values regardless of whether the channel is idle or busy. In particular, each node will sample n measurements of ambient noise at a constant rate. 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.

Algorithm 3. Acquiring the Ambient Noise Floor (ANF). ANF approximates the strength of jamming signals.
1: procedure MEASUREJSS
2: $s = \{s_1, s_2 \dots \dots s_n\} = MeasureRSS()$
3: if $var(s) < varianceThresh$ then
4 $S_a = s$
5: else
6: $JssThresh = \min(s) + \alpha[\max(s) - \min(s)] \Rightarrow \alpha \in [0,1]$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

7: $s_a = \{s_i | s_i < JssThresh, s_i \in s\}$
8: end if
9: return $mean(s_a)$
10: end procedure

The correctness of the algorithm is supported by the fact that sa is not likely to be empty due to carrier sensing, and the JSS approximately equals to the average of sa. The key question is how to obtain sa. To do so, we set the upper bound (i.e., JssThresh) of sc in Algorithm 3 as percentage of the amplitude span of ambient noise measurements.

E. Best Estimation Of Jamming Location

The jammer localization problem can be modeled as a nonlinear optimization problem (defined in Problem 1), and finding a good estimation of jammers' locations is equivalent to seeking the solution that minimizes the evaluation feedback metric ez. In this section, we illustrate the relationship between ez and ed (the distance between thetrue jammer's location and the estimated one), which shows that greedy algorithms that search for successively better solutions are unable to find the global optimal value. Instead, we use several heuristic search algorithms that rely on guided random processes to approach the global optimum without converging to a local minimum. A GA searches for the global optimum by mimicking the process of natural selection in biological evolution. A GA iteratively generates a set of solutions known as a population. At each iteration, 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 inherited. 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 successive 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 (i.e., a solution) has a chromosome of 3n genes, comprising n jammers' coordinates and jamming power levels. We defined the fitness of each individual as ez. The smaller ez is, the better.

V. SIMULATION RESULT

The simulation result had been manipulated by a discrete event simulator targeted for networking research which is known as NS2. It supports for simulation of TCP, routing and multicast protocols over wired and wireless network.

A. Packet delivery ratio: It illustrates the amount of delivered data to the destination. Compared to the existing system (red line) the proposed system (green line) claims that there is a constant improvement in the packet delivery even after the packets are routed in alternate path.

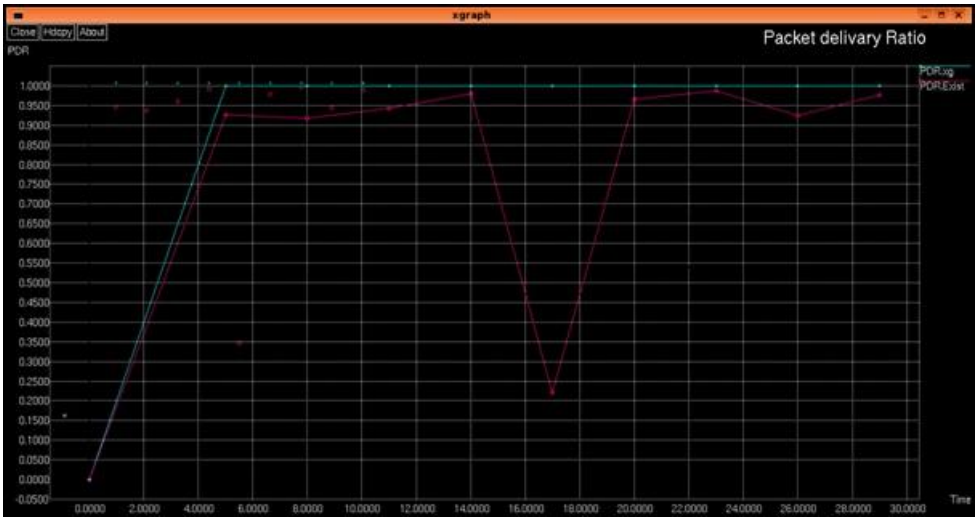

Fig.1. packet delivery ratio

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

B. Packet drop ratio: It illustrates the amount of packet that fails to reach the destination. The quality of a wireless sensor network is determined by this factor. On comparing the existing system (red line) with proposed system (green line) the later has the least amount of packet loss.

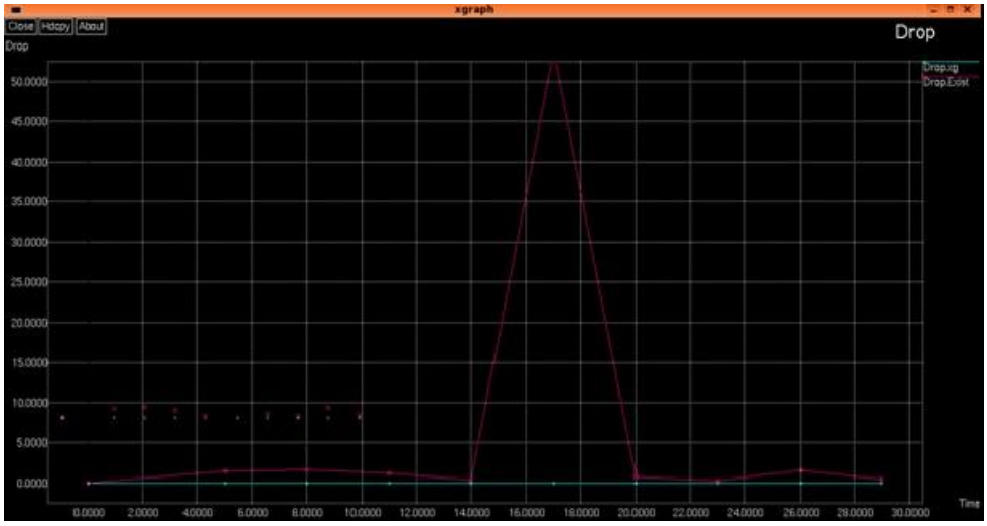

Fig.2. packet drop ratio

C. Throughput: It determines the amount of work that the network can do in a given period of time. It usually measured as data packets per time slot. The proposed system shows effective improvement in throughput.

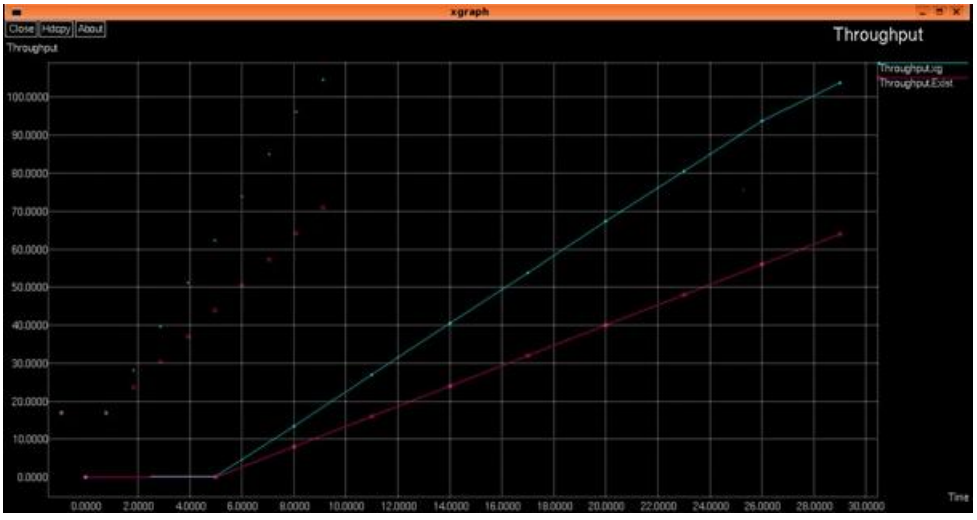

Fig.3. performance throughput

VI. CONCLUSION

The problem of localizing jammers in wireless networks, aiming to extensively reduce estimation errors. The jammers could be several wireless devices causing unintentional radio interference or malicious colluding jamming devices who coexist and disturb the network together. Most of the existing schemes for localizing jammers rely on the indirect measurements of network parameters affected by jammers, for example nodes' hearing ranges, which makes it difficult to accurately localize jammers. In this work, we localized jammers by exploiting directly the JSS. Estimating

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

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. The scheme samples signal
strength regardless of whether the channel is busy or idle and estimates the ANF by filtering out regular transmission (if any) to obtain the JSS.

REFERENCES

[1] K. Pelechrinis, I. Koutsopoulos, I. Broustis, and S.V. Krishnamurthy, "Lightweight Jammer Localization in Wireless Networks: System Design and Implementation," Proc. IEEE GLOBECOM, 2009.
[2] H. Liu, Z. Liu, Y. Chen, and W. Xu, "Determining the Position of a Jammer Using a Virtual-Force Iterative Approach," Wireless Networks, vol. 17, pp. 531-547, 2010.
[3] 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.
[4] 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.
[5] 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.
[6] 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.
[7] 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.