International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Optimization of an Error Minimizing or Localizing Jammers in Wireless Networks

S. Rajeswari

Assistant Professor in MCA, Sree Saraswathi Thyagaraja College, Pollachi, India

Abstract: ***Wireless networks have already grown considerably and will certainly go on doing so, consequently the security and secrecy has become a critical issue. Earlier research efforts have mostly solved this problem: (i) efficient detection and elimination of cheating node, (ii) range-based localization without using radio coverage and (iii) range-based localization in the presence of cheating node. The proposed system guarantees an upper bound on the localization jamming error. Most of the malicious node detection techniques are based on consensus building or geometric estimation, and are rather restrictive with high false-positive or false-negative rate. In this paper is the design and implementation of an efficient and lightweight jamming localization algorithm. Our technique control scheme guarantees stability robustness to multiple jamming nodes in different channels and changeful presented bit-rate (PBR) bandwidth. It also achieves two expectant goals, i.e. it ensures convergence of queue length to the desired steady-state value and satisfies a weighted fairness condition. The higher priority queue results in reducing the input delay of packets which results in traffic control mechanisms, the scheduling is assigned on FIFO scheduling mechanisms. The algorithm good performance of jamming location. Simulation results show that the control system is rapid, robust, and adaptive and the quality of service (QOS) is guaranteed.***

Keywords: Mobile Ad Hoc Networks, jamming aware traffic allocation, multipath source routing, optimization CDMA.

1. Introduction

Distributed localization or location discovery in wireless networks is the problem of determining the location (in a distributed fashion) of a (mobile) device in the network with respect to some local or global coordinate system. Localization protocols in wireless networks can be categorized into two broad types: i) range-based and ii) range-free protocols [2]. In range-based techniques, a node computes its location by first estimating distances to neighboring nodes, whereas range-free techniques, typically, do not involve any distance estimation by the target node. Range-based techniques can be further classified as (a) anchor or beacon-based and (b) anchor-free protocols. Anchor-based algorithms such as [3]–[10], among others, need special beacon or anchor nodes that are strategically placed in the network and know their own location using GPS. The mobile target node first estimates its distance to a set of neighboring beacon or anchor nodes by using well-known techniques such as Received Signal Strength Indicator (RSSI) [11], Time of Arrival (ToA) [12], and Time Difference of Arrival (TDoA) [13]. The target node then applies constraint satisfaction or optimization techniques, such as, trilateration or multilateration, in order to compute its location. A two dimensional anchor-based localization process by trilatering distance estimates to three anchor nodes is depicted in Figure 1(a). Anchor-free schemes do not involve specifically marked anchor nodes.

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 coexisting a wireless network

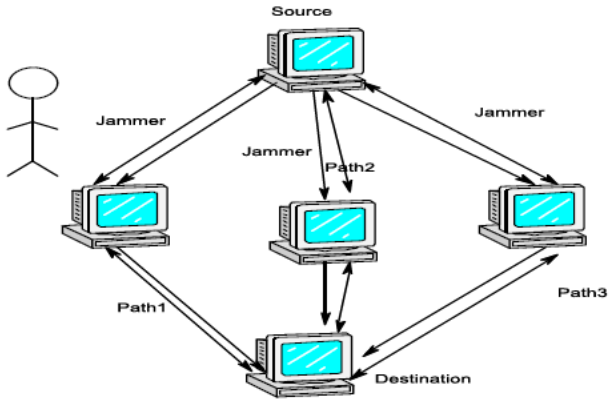

Figure 1: Distance-based (range-based) localization (a) Trilateration (b) Cheating Jammer anchors

Although anchor-based schemes are popular and generally perform well, a majority of these techniques operate under the assumption that anchor nodes behave honestly during the localization process. This theory is not valid in non trustworthy wireless environments where anchor nodes could cheat by manipulating the distance estimation process, as shown in Figure 1(b), and thus affecting the overall accuracy of the location estimated by the target node. Many existing techniques overcoming this problem of cheating in range based localization protocols exist in the literature [1], [14]–[23]. these proposals have primarily followed one of the following two approaches. The first approach is to localize in the presence of cheating anchor nodes and securely verify that the determined location is within some maximum error bound. The second approach calls for efficiently detecting and eliminating measurements emanating from cheating anchors before location determination. Localization schemes following the first

approach often need to satisfy certain necessary network conditions (e.g., in terms of the total number of malicious anchors) and are constrained by the resulting large localization errors. Localization schemes following the second approach suffer from the non-triviality of the detection and elimination process in a distributed networking environment.

We are motivated by the fact that radio signal jamming has traditionally always been considered as an adversarial tool that is used for disrupting network protocols. In this work, we would like to follow a reverse ideology and use jamming in order to protect network protocols such as location discovery. Our focus in this paper is on the explicit rate feedback framework. Over the years, many congestion control algorithms have been proposed on control theoretic principles in this framework. This algorithm, however, requires a complex online tuning of control parameters to ensure stability and to damp oscillations under different network conditions. An integral sliding mode controller (ISMC) is introduced, which can overcome the adverse effect by the multiple propagation delays and keep stable robustness with respect to uncertainties of ABR bandwidth. The proposed sliding surface includes a predictor which consists of not only the current state but also the past control input during the period of delay. The predictor is applied to map the original system into an input-delay free form, and then the ISM technique is used to minimize the effects of the changeful available bit rate bandwidth. We construct this controller on a solid analytical basis and simulation results show that our algorithm indeed achieves another two goals for a variety of networks scenarios: 1 tracking, which is to keep the queue size close to a certain desired size. By choosing this level sufficiently larger than zero and sufficiently smaller than the buffer size, nonlinear effects may also be avoided and the outgoing how rate may be kept close to the full capacity (thus achieving the maximum utilization of the network). 2 weighted fairness, which means allocating different percentages of the obtainablepower to different sources. Thus, weighted fairness may be used as a pricing tool.

The rest of the paper is organized as follows. Section 2, gives an overview of related work. Section 3 presents proposed approach. In Section 4, deal with some topologies to validate proposed approach. Conclusion is presented in Section 5.

2. Related Work

The first approach to secure distance-based localization is to detect cheating anchors and eliminate them from consideration. The existing a technique eliminating malicious anchor data, called attack-resistant Minimum Mean Square Estimation (MMSE), which leverages on the fact that malicious location references are usually inconsistent with the benign ones. The second approach is to design techniques that are robust enough to tolerate the cheating effect of malicious anchors. Existing system develop the CRICKET system that eliminates the dependence on beacon nodes by using communication hops to estimate the network's global layout, and then apply force-based relaxation to optimize this layout. Concepts from coding theory have also been used to secure distributed range-based localization. Some proposed framework for providing robust location detection in wireless sensor networks using the theory of Identifying Codes (ID-Codes). In this framework, high powered transmitters are fitted in such a way that each localizable point on the terrain is covered by a unique set of transmitters.

Each node localizes itself by mapping the set of neighborhood transmitters to the corresponding location. Similarly, have used the theory of Error Correcting Codes (ECC) for robust localization in sensor networks. For each localizable point, the authors used distances from a fixed set of neighboring nodes to that point as a "codeword" for that point such that the "distance" between any two code words is fixed. Thus, any cheating behavior by the participating nodes can result in an illegal codeword and can be detected and corrected. Contrary to this, in our work, we use orthogonal codes or chips for only eliminating cheating nodes, and not for detecting cheating. Related outline an OCS and CDMA based technique for mobile location discovery in Line Of Sight (LOS) and Non-Line of Sight (NLOS) scenarios. In this technique, all anchors are assigned identifiers by using a set of orthogonal codes that are broadcast periodically and synchronously. The mobile target detects the three strongest broadcast signals and estimates its location by calculating the Time Difference of Arrival (TDoA) with respect to these anchors. The authors showed that the use of OCS for localization helps to cancel the interference at the mobile target caused by simultaneous transmission of the anchors. However, they do not address any security issues related to cheating anchors.

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s [15]. Recently, several alternative jamming strategies have been demonstrated [11], [12], [1], [2]. Xuet. al. Categorized jammers into four models, (a) a constant jammer that continuously emits noise, (b) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, (c) a random jammer that alternates between periods of continuous jamming and inactivity, and (d) a reactive jammer who jams only when transmission activity is detected. Intelligent attacks which target the transmission of specific packets were presented in [8], [3]. Thuente considered an attacker who infers eminent packet transmissions based on timing information at the MAC layer. Law et. al. considered(a) (b) selective jamming attacks in multi-hop wireless networks, where future transmissions at one hop were inferred from prior transmissions in other hops. However, in both [8], [4], real-time packet classification was considered beyond the capabilities of the adversary. Selectivity was achieved via inference from the control messages already transmitted.

Channel-selective jamming attacks were considered in [4], [5]. It was shown that targeting the control channel reduces the required power for performing a DoS attack by several orders of magnitude. To protect control channel traffic, control information was replicated in multiple channels. The "locations" of the channels where control traffic was broadcasted at any given time, was cryptographically protected. In [9], we proposed a randomized frequency

hopping algorithm, to protect the control channel inside jammers. Finally, Popper et. al. proposed a frequency hopping anti-jamming technique that does not require the sharing of a secret hopping sequence, between the communicating parties [10].

3. Proposed Approach

In this proposed approach the problem of localizing identify based on power adaptation which is the best of our knowledge. The jammer going to increases the jammer packet the proposed system eliminates the input delays. The control scheme guarantees constancy robustness to multiple time delays in different channels and changeful available bit-rate bandwidth. It also achieves two hopeful goals, i.e. it ensures convergence of queue length to the desired steady state value and satisfies a weighted fairness condition.This simulation results show that the bandwidth control system is rapid, robust, adaptive and the quality of service (QOS) is guaranteed.

3.1 The Network Model

The network consists of a mobile device MT, also referred to as the mobile target node, moving over an application area. MT wants to estimate its own location by using distance estimates to a set of neighboring (and stationary) anchor nodes who know their own location. In practice, there can be multiple target nodes, but here currently assume a single target node in order to simplify the current exhibition. The mobility of the target node is application dependent only consider the movement of the target node over the topology area. Without loss of generality, we assume that MT is momentarily static during the localization process. Deployed over the application area, are a fixed number (nodes n) of stationary anchor nodes that know their own location and can assist the target node in its location estimation. Let these nodes be denoted asB_1,……B_n. For simplicity, assume that the locations of the target node MT and the anchor nodes can be expressed in the two-dimensional coordinate system as a vector (x; y) where, y $\in \mathbb{R}$. Each of the anchor nodes and the MT possesses anomni-directional radio transceiver.

3.2 Adversary Model

We assume that, amongst a total of n anchors in the network, a maximum of anchors are malicious or cheating nodes. The set of the entire malicious node is denoted by A. All anchors that are not malicious are assumed to be honest, i.e., they execute the proposed localization protocol correctly. Although many types of attacks are possible in radio frequency based positioning systems. In this proposed system focus on distance manipulation attacks. In these attacks, anchor nodes cheat by manipulating the distance between themselves and the target node, for example, either delaying or manipulating the signal strength of the localization messages depending on the distance estimation technique used in the localization protocol. In addition to the stage separately, a malicious anchor can also plan with other malicious anchors. In order to effectively communicate with the MT on the CDMAbased data channel, all anchors need to transmit localization messages to the MT. Coordinating with each other helps the malicious anchors in selecting different data transmission, thus avoiding interference and data corruption at the target node. Malicious data transmitted using an incorrect message will be directly discarded at the target, and thus not included in the location calculation process. It is also reasonable to assume that the malicious node does not possess the secret group keys and other cryptographic materials shared only by the honest node only know the message. Moreover, the malicious node are not able to receive (and maintain) a table of valid during a particular time period because the updates are encrypted with a group key known only to honest anchors.

3.3 Proposed Localization Protocol

A mobile node can receive the messages required for localization from the locators in the network. One is that the locators periodically broadcast their messages, which lets the mobile node hear them. The other is an event-driven method which the mobile node requests and the locators respond to it.

Due to the same reason and its mobility, it is not reasonable for the mobile node to use the slow power adaptation technique to communicate with the locators. In these techniques all the mobile node broadcast the location request message with maximum transmission range. Suppose consider the jammer location L1 and L2 receive the message. The entire node response message with location information.

3.3.1 Estimator of jammer location

After receive the response message from the entire node. Here calculate the P_{JM} jamming power.

$$P_{JM} - \frac{1}{(4\pi)^2} G_s . G_R . P_S . \left(\frac{\tau}{D_{SR}}\right) \qquad (1)$$

Where GS is the antenna gain of S, GR is the antenna gain of R, PS is the transmitting power of S is the wavelength of radio wave, ABR is the distance between S and R, and n is the loss exponent. After derive the ABR for L1's transmission to a recipient locator L2, while under jammer J's interference as

$$\gamma_{L_1/J(P_{L1})} = \frac{P_{L_1 L_2}}{P_{J L_2}} \qquad (2)$$

Where n is the loss exponent.

3.4. Multiple attackers in wireless networks

The multiple jamming attack detection of jamming localization, we use two jammer and two locators. Experiments varying with the configuration of locators and jammer. The measurement and the estimated jamming location in each configuration. The actual jammer location is denoted by the point J and the two locators are denoted by the point L1 and L2. E. Note that a locator sometimes fails to deliver location information even with the maximum power (e.g. the case where L2 sends to L1 in the first configuration, the case where L1 sends to L2 in the third configuration), since its transmission power is not enough to defeat the jammer for the receiver in the given configuration. The result, however, shows the discrepancy

between the two jammer location due to measurement errors and fading effects. To compensate this gap between the theory and the practice, we proposed a technique based on the relative radius of each node. If the radii of the two node are similar, it means with high probability that the distances between the jammer and each locators are similar. On the other hand, if a radius is greater than the other, then it implies with a high probability that the jammer is located closer to the node with a smaller curve.

ABR based on searching algorithms that are particularly helpful when multiple jammers create one connected jamming area. We evaluated the performance of our multi-jammer localizer through simulation using large-scale size topology setups with various distances between jammers.

4. Evaluation

We present simulation results for our proposal on securing anchor-based localization

Table 1: Network parameters

Simulator	NS2
Protocol	MAODV
Simulation area	1000m X 1000m
Simulation duration	200 Second
Number of nodes	80
Transmission range	250 m
Movement model	Randomwalk Model
MAC Layer Protocol	IEEE 802.11
Pause time	100 sec
Maximum speed	20 m/s
Packet rate	4 packets/sec
Traffic type	Constant bit rate Error
Packet Size	512 bytes/packet

4.1 Performance Metrics

PDR is the ratio of the number of data packets received by the destination node to the number of data packets sent by the source mobile node. It can be evaluated in terms of percentage (%). This parameter is also called "success rate of the protocols", and is described as follows:

$$PDR = \left(\frac{SendPacketno}{Receivepacketno}\right) \times 100$$

Throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node.

$$X = \frac{C}{T}$$

Where X is the throughput, C is the number of requests that are accomplished by the system, and T denotes the total time of system observation.

Average end-to-end delay Average end-to-end delay signifies how long it will take a packet to travel from source to destination node. It includes delays due to route discovery, queuing, propagation delay and transfer time.

$$D_{end-end} = N(d_{trans} + d_{prop} + d_{proc}$$

Where dend-end= end-to-end delay, dtrans= transmission delay,dprop= propagation delay,dproc= processing delay,dqueue= Queuing delay and N= number of links.

This metric is useful in understanding the delay caused while discovering path from source to destination.

5. Performance Comparison

The simulation results are shown in the following section in the form of line graphs. Performance of regular AODV and minimum delay routing protocol MAODV based on the varying number of nodes in chain topology is done on parameters like packet delivery ratio, good put and throughput.

Table 3: Packet Delivery Ratio

Protocols	*jammers*						
	1	**2**	**3**	**4**	**5**	**6**	**7**
JSS	54	50	64	79	84	88	91
ABR with FIFO	65	67	85	83	87	94	98

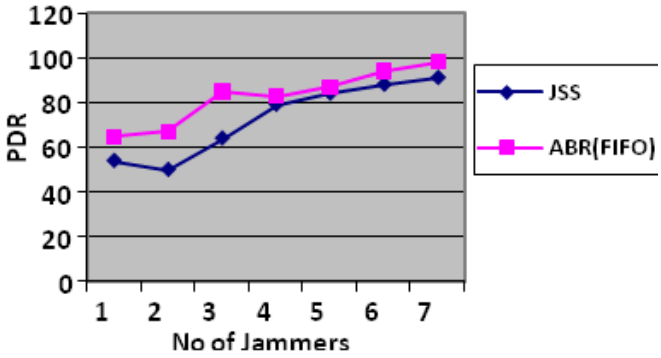

Figure 2: Shows packet delivery ratio against the number of jammers. It shows that the ABR based FIFO protocol has a better PDR compare to JSS.

Table 4: Compare Throughput

Protocols	*jammers*						
	1	**2**	**3**	**4**	**5**	**6**	**7**
JSS	5.1	6.4	7.5	8.2	8.7	9.1	9.5
ABR(FIFO)	5.8	6.9	7. 6	9.1	10.3	11.7	12.4

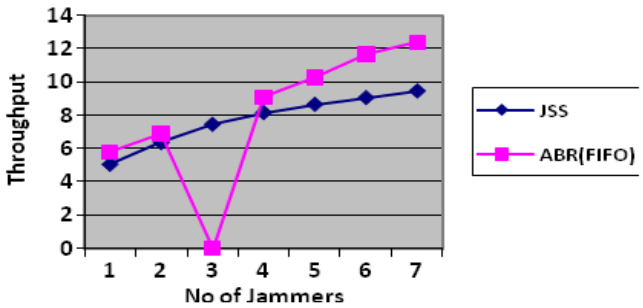

Figure 3: Show throughput against the number of nodes. It shows that when the number of nodes is 80 with up to seven jammers, the ABR with FIFO has higher throughputs than JSSS, respectively.

Table 5: End to End delay

Protocols	*jammers*						
	1	**2**	**3**	**4**	**5**	**6**	**7**
JSS	5.8	4.1	3.2	3.1	2.8	2.5	2.1
ABR(FIFO)	4.1	3.2	2.7	2.1	1.9	1.2	0.5

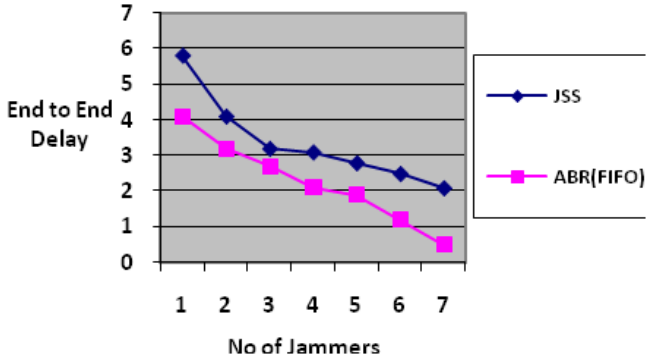

Figure 4: show delay against the number of nodes. It shows that when the number of jammer nodes high it take more delay time. The ABR with FIFO has lower delay value compared to existing JSSS.

6. Conclusion

We presented a new approach for efficient localization of jammer based on ABR with FIFO. The proposed approach implemented a request confusion strategy in order to an onymize localization requests and a reactive jamming strategy on the ABR response channel to actively disable malicious or cheating anchors. The jamming effects under multiple jammers and developed a framework that can perform critical tasks of automatic network topology. We have obtainable methods for each network node to probabilistically characterize the local impact of a dynamic jamming attack and for data sources to incorporate this information into the routing algorithm. This method does not depend on measuring signal strength inside the jammed area and also does not require delivering information out of the jammed area. Instead, proposed framework uses the disturbed network communication and derives node ABR for jammer localization grounded on network topology changes.

References

[1] R. Anderson, Security Engineering: A Guide to BuildingDependable Distributed Systems. John Wiley & Sons, Inc., 2001.
[2] J. Bellardo and S. Savage, “802.11 denial-of-service attacks:Real vulnerabilities and practical solutions,” in Proc. USENIXSecurity Symposium, Washington, DC, Aug. 2003, pp. 15–28.
[3] D. J. Thuente and M. Acharya, “Intelligent jamming in wirelessnetworks with applications to 802.11b and other networks,” inProc. 25th IEEE Communications Society MilitaryCommunications Conference (MILCOM’06), Washington, DC,Oct. 2006, pp. 1–7.
[4] G. Lin and G. Noubir, “On link layer denial of service in datawireless LANs,” Wireless Communications and MobileComputing, vol. 5, no. 3, pp. 273–284, May 2005.
[5] W. Xu, K. Ma, W. Trappe, and Y. Zhang, “Jamming sensornetworks: Attack and defense strategies,” IEEE Network, vol. 20,no. 3, pp. 41–47, May/Jun. 2006
[6] R. Leung, J. Liu, E. Poon, A.-L. C. Chan, and B. Li, “MP-DSR:A QoSaware multi-path dynamic source routing protocol forwireless ad-hoc networks,” in Proc. 26th Annual IEEE Conferenceon Local Computer Networks (LCN’01), Tampa, FL, USA, Nov.2001, pp. 132–141.