Middle-East Journal of Scientific Research 22 (1): 45-50, 2014
ISSN 1990-9233
© IDOSI Publications, 2014
DOI: 10.5829/idosi.mejsr.2014.22.01.21820

Localization Using Multilateration with RSS Based Random Transmission Directed Localization

[1]D. Sivakumar and [2]B. Sivakumar

[1]Easwari Engineering College, Chennai
[2]Adhipara Sakthi Engineering College, Melmaruvathur, India

Abstract: Wireless networks are rapidly spreading technology all around the world. The adaptability and openness of wireless networks empower an opponent to take on the appearance of different devices effortlessly. The Accurate positioning of nodes in wireless and sensor networks is vital since the location of sensors is critical information to various higher-level networking tasks. However, the localization infrastructure can be subjected to non-cryptographic attacks, such as signal attenuation and amplification that cannot be addressed by traditional security services. In this paper, present an attack detection schemes for wireless localization systems. Localization of node is performed using multi-lateration type of RSS measurement based random transmission directed localization (MRR) technique. Moreover, Ad hoc On Demand Distance Vector (AODV) routing is used to obtain the secure neighbors for transmission and communication forwarding in the process of routing. The error rate and accuracy factor are the performance metrics to determine the possible location of the receiver. Simulation shows our scheme evaluates the error rate and accuracy factor for each transmission and effectively revokes localization error.

Key words: A ODV · Wireless networks · Sensor networks · Received Signal Strength (RSS)

INTRODUCTION

Distributed localization or location discovery in wireless networks is the problem of determining the location (in a distributed fashion) devices in the system regarding some nearby or worldwide direction framework. Localization protocols in wireless networks can be categorized into two broad types: i) range-based and ii) range-free protocols [1]. Ranging-based localization is the task of identifying the positions of a network of nodes based on estimates of the distances between them, called range estimates. From numerous points of view, radio sign quality (RSS) is a perfect modality for reach estimation in remote systems in light of the fact that RSS data might be gotten at no extra cost with each one radio message sent and gained. The effortlessness of RSS is particularly engaging for the localization in wireless sensor networks because of the light of their expense, size and force imperatives, regardless of the way that RSS may yield exceptionally boisterous extent gauges.

A main challenge with RSS ranging is that the effect of reflecting and lessening protests in nature can have much bigger consequences for RSS than distance, making it troublesome to gather separation from RSS without a definite model of physical environment. This has given RSS the reputation of being too "unpredictable" for range estimation [2] [3]. As more location-dependent services are conveyed, they will progressively become tempting targets for malicious attacks. Unlike traditional systems, the restriction base is delicate to non-cryptographic attacks and these cannot be utilizing conventional security services. We have discovered that the execution of the localization algorithms degrades significantly physical ambushes, for instance, when signs are lessened, amplified, or reflected by an adversary [4].

Compromised localization results are a genuine danger due to their effect on applications and it is thus desirable to detect the presence of localization attacks.

The proposed MRR approach, examine the problem of detecting attacks on wireless localization. Obtaining transmission distance with an average RSS is concatenated with post antenna calibration such that the receiver is located at the antenna's degree in some 'x' units of distance. In particular, MRR utilize Ad hoc On

Corresponding Author: D. Sivakumar, Easwari Engineering College, Chennai, India.

Demand Distance Vector (AODV) routing protocol [5] on-demand methodology for discovering routes, that is, a route is built just when it is required by a source node for transmitting a packet [6, 7]. Based on this protocol, it is used to obtain the secure neighbors for transmission and communication forwarding in the process of routing.

The remainder of this paper is organized as follows. Section II discusses previous research in localization and attack detection. Section III presents preliminary work done. Section IV presents the proposed technique. Section V presents the simulation environment and Section VI provides results and discussion. Finally section VII concludes the paper [8].

Related Work: In particular, localizations techniques are categorized into range-based or range-free approach. The range-based approach involves distance estimation to nodes using the measurement of physical properties such as Time of Arrival [9], RSS and Time Difference of Arrival (TDOA) [10]. The existing systems that use RSS for localization employ a RF profiling technique, proposed by RADAR [11]. The RF profiling needs a pre-deployment stage where the RSS of each node is recorded at every position in the two dimensional space. The reading obtained at a particular position is the RF profile of that position. RADAR achieves approximately 4m localization indoor, a result that has been supported by several studied using VHF [12], 802.11 [13], cellular radios [14] and low power wireless sensor network [15].

Several studies that make use of RSS directly for range estimation obtained negative or inadequate results. The RF profiling technique was indeed motivated by the point that the RSS ranging indoor is ineffective [11]. A study explored outdoor RSS ranging in both open and heavily loaded environment utilizing two 802.11 nodes, but guaranteed only 50% standard error [16].

Another study showed that RSS ranging was effective for indoor localization within 1.8m and nodes having 2-3 meter spacing Berkeley Varitronix Fox receiver which is a high-fidelity Wi-Fi propagation analyzer is used for measuring RSS [17].

Numerous studies that categorized RSS measurement utilizing low power radios decided not to utilize these low power radios for multi-hop localization or rejected RSS in the support of other ranging techniques [18].

Recently it has been identified that there are various non-cryptographic attacks that affect the performance of the localization.[19]. For instance, wormhole attacks pass through a faster tunnel in order to shorten the distance between the nodes [19]. Physical barriers directly affect the physical property that is being used by the localization [20]. Secure localization techniques have been proposed for addressing these attacks. [21] detects attacks based on received beacon data inconsistency and uses a greedy search or voting algorithm for eliminating malicious beacon information. In [22] both directional antenna and distance bounding are used to achieve security. In hidden and mobile base stations are used to localize and verify the location estimation. Because such base station locations are hard to assume, it is difficult to introduce an attack, thereby providing additional security. In this paper RSS based ranging estimation and ADOV protocol is used for secured and effective localization of nodes.

Preliminarie:

Received Signal Strength (RSS) Based Ranging Technique: Received signal strength is the voltage measure at the receiver by the received signal strength indicator (RSSI) circuit. Then the power of the received signal is used to estimate the distance measure. The RSS based ranging technique is based on the standard that the signal strength decreases if distance between the nodes increases. This technique is widely used in wireless sensor networks. The receiving node estimates the distance from the source node by determining the RSS and then uses path-loss factor to convert RSS into distance measure.

The power received by the receiver is expressed as

$$P_{ij} = p_t - 10\alpha \log_{10} \frac{d}{d_0} + Y_\sigma \tag{1}$$

Where $p_{ij}$is the power of the received signal (dBm) from the transmitter i at the receiver j, p_t is the power transmitted is the true distance between the sender and the receiver, $Y_{ó}$ represents noise and á is the path loss factor.

Based on the above equation, the distance between node i and the node j is

$$d_{i,j} = d_0 10^{(p_t - p_{ij})/_{10\alpha}} \tag{2}$$

Position Estimation: The position of a node (x,y) can be determined by multilateration technique using the distance measurement obtained using equation 2. Multilateration is the most extensively used technique for positioning in wireless sensor network. Let us assume that there are three nodes with known positions $(x_{i,}y_i)$ where i=1,2,3 and a node with unknown position (x_n,y_n). From the Pythagoras, the set of equations can be written as

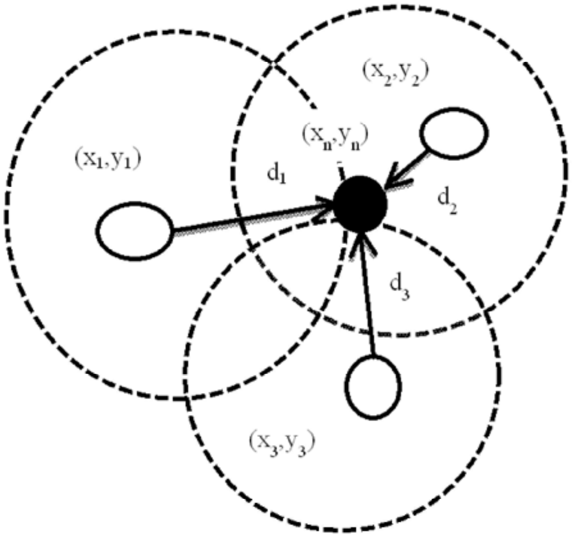

Fig. 1: Position Estimation

$$(x_i - x_n)^2 - (y_i - y_n)^2 = d_i^2 \tag{3}$$

Where d_i is the measured distance and i=1,2,3. To solve this, the equation can be written as a linear matrix equation.

$$2.\begin{bmatrix} x_3 - x_1 & y_3 - y_1 \\ x_3 - x_2 & y_3 - y_2 \end{bmatrix} \cdot \begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} (d_1^2 - d_3^2) - (x_1^2 - x_3^2) - (y_1^2 - y_3^2) \\ (d_2^2 - d_3^2) - (x_2^2 - x_3^2) - (y_2^2 - y_3^2) \end{bmatrix} \tag{4}$$

By solving the above linear equations the position of the unknown node (x_n, y_n) can be obtained.

Fig 1 shows the position estimation of an unknown node (x_n, y_n) using multilateration technique and RSS ranging measurement.

MRR Approach and AODV Protocol: A novel Multilateration with RSS based Random Transmission Directed Localization (MRR) has been proposed for identifying the location of unknown nodes. The error factor and accuracy factor for each transmission is computed for effective localization of nodes. In addition, the system uses an Ad hoc On Demand Distance Vector (AODV) for secure routing of packets from source to destination.

Multi-lateration with RSS based Random Transmission Directed Localization (MRR): Localization starts with initializing the data packet from the source. The frequency of the data packet at the sender is initially obtained. Then the received frequency at the receiver node is measured. The process is repeated for n number of packets. The RSS value is then computed by using equation 1. The error and the accuracy factor of each transmission are then computed using equation 5 and 6.

$$E = \sqrt{((RSS * data\ rate))/_{(ET - ST) \times SF}} \tag{5}$$

Where ET is the packet arrival time, ST is the packet departure time, starting frequency of the packet at the source, while E is the error rate. The accuracy factor is given by

$$AF = (AT_j \times AD_j) - (ST_j \times AD_j) \tag{6}$$

Where AD_j is the angular velocity at the destination during j^th^ data transfer cycle, AT_j is the packet arrival time during j^th^ round, ST_j is the packet departure time during j^th^ round while AF is the accuracy factor. If there occurs any packet delay during the transmission it then added to the error factor using $E = E + \left(pause\ time/_{data}\right)$. The RSS value for a particular data rate is noted after the first transmission. If the RSS value differs for the same data rate then the difference between the RSS value is obtained and the difference value is added and subtracted from error and accuracy factor. Based on the accuracy factor the antenna is post calibrated and the location of the unknown node is identified using equation 4.

Ad Hoc on Demand Distance Vector Routing (AODV): The proposed approach uses ad hoc on demand distance vector routing (ADOV) for effective and secured communication between the source and the destination. The security is enabled by using intrusion detection system. AODV enables dynamic and multi-hop routing. It establishes route to the destination only when the sender needs to communicate with the destination. The sender initiates a route request message (RREQ). The RREQ message contains the following fields

- {source address, source sequence num, broadcast id, destination addr, destination sequence num, hop-count}

The broadcast id is incremented each time the source broadcasts a new RREQ message. If the node contains the valid route to the destination it replies back with route reply (RREP) message, otherwise the it rebroadcasts the RREQ message to its neighbor and increases the hop-count. If the intermediate node receives a RREQ

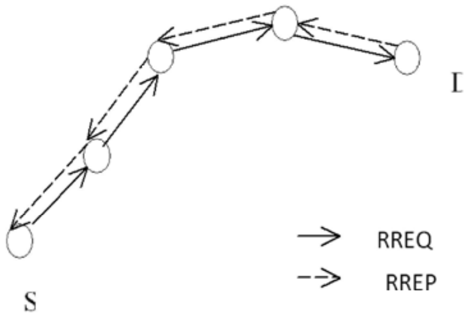

Fig. 2: Routing using AODV

with broadcast id, source address that has already been received, it simply drops the RREQ packet. The destination node upon receiving the RREQ, respond with a route reply message (RREP). The RREP message traverses back to the source utilizing the path established by the RREQ. The RREP message contains the following field:

- {source address, destination address, destination sequence num, hop count, lifetime}

As the RREP message traverses back to the source, a forward pointer is setup and updates the route entry in each node. Here security is ensured by employing a detection model in each node that uses the neighboring information for detecting misbehavior of the neighboring node. If a node receives more number of route requests than a predefined threshold from particular sources to a destination in specific time interval it is declared as a malicious node and propagates the information throughout the network and drops the route.

Simulation Model: This section describes the simulation tool and performance metrics used to evaluate the performance of the proposed approach.

Simulation Environment: The proposed technique is simulated using network simulator ns2. The simulation environment is 1630 × 100 m wide. The transmission range is 750m. Table 1 shows the parameters used for simulation.

Performance Metrics: The performance of the proposed approach is evaluated using the following metrics.

Error Factor: The error factor is computed using the following formula

Table 1: Simulation Parameters

Simulation and Network Parameters	
Network Area	1630 x 100
Protocol	AODV
No. of Mobile Nodes	40
Network Topology	Flat Grid
IEEE Standard	802.11
Frequency	2.472 hz
Carrier Sense Power	5.011872
Broadcasting Range	750mts
Application Type	Cbr
Application rate	1.0mb
No. of Packets	1500
Data Rate	I mbps
Delay	10ms
Simulation Time	10s

$$E = \sqrt{((RSS * data\ rate))\Big/(ET - ST) \times SF}$$

Where ET is the packet arrival time, ST is the packet departure time, starting frequency of the packet at the source, while E is the error rate.

Accuracy Factor: The accuracy is given by the following formula

$$AF = (AT_j \times AD_j) - (ST_j \times AD_j)$$

Where AD_j is the angular velocity at the destination during jth data transfer cycle, AT_j is the packet arrival time during jth round, ST_j is the packet departure time during jth round while AF is the accuracy factor.

Packet Delivery Ratio: It is the ratio of the number of packets received by the receiver to the number of packets delivered by the sender. This metric gives the intuition of how well the protocol is performing in terms of packet delivery.

RESULTS AND DISCUSSION

The error factor for both direct and n-hop neighbors is shown in Fig 3. In this case the error is computed for each transmission.

Fig 4 shows the accuracy factor in case of both direct and n hop neighbors. In this case the accuracy is computed for each transmission. The results show that the accuracy is maintained in case of the proposed approach.

Fig 5 shows the hit ratio results under various data. The packet delivery ratio and throughput of the protocol used is shown in Fig 6. The results show that the packets have been successfully delivered to the destination using the proposed protocol.

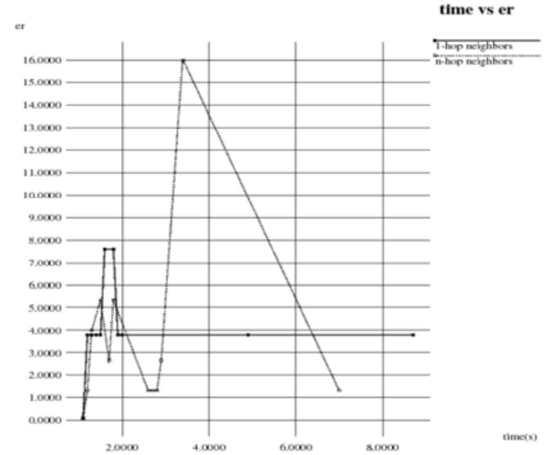

Fig. 3: Graphical Representation of the Error Rate for a Particular Time

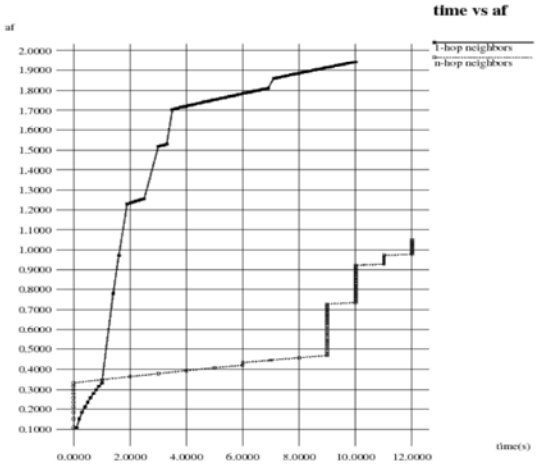

Fig. 4: Graphical Representation of the Accuracy Factor for a Particular Time

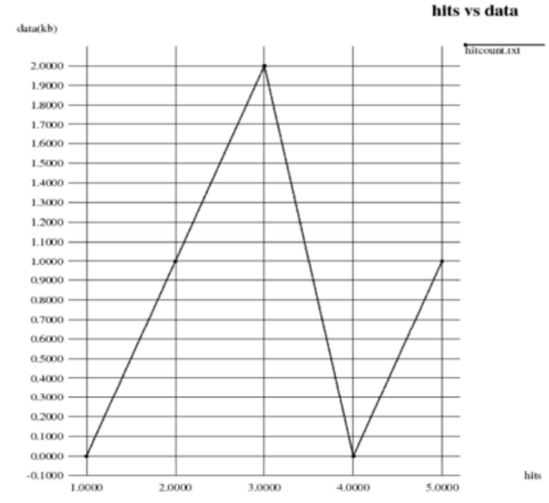

Fig. 5: Hit Ratio vs. Data

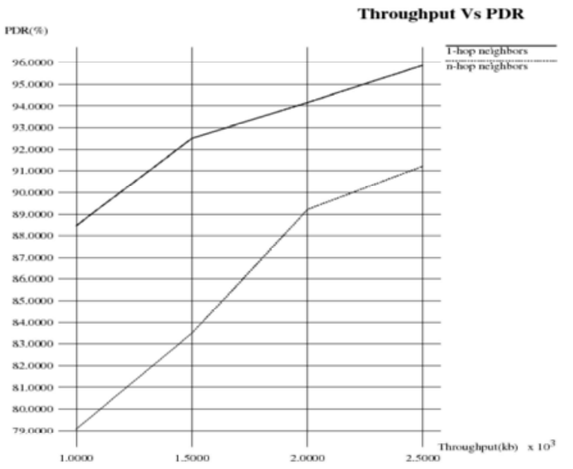

Fig. 6: Throughput vs. PDF

CONCLUSION

In this paper, a novel Multilateration type RSS based Random Transmission Directed Localization (MRR) has been proposed for effective localization of nodes. The technique utilizes RSS based ranging for distance measurement and a multilateration technique is used to obtain the coordinates of the node. Moreover, ADOV routing protocol is used for routing the data packets from source to destination. In addition the ADOV protocol provides secure neighbors.

REFERENCES

1. Hightower, J. and G. Borriello, 2001. Location Systems for Ubiquitous Computing, Computer, 34(8): 57-66.
2. Chen, Y., K. Kleisouris, X. Li, W. Trappe and R.P. Martin, 2006.The robustness of localization algorithms to signal strength attacks: a comparative study, in Proceedings of the International Conference on Distributed Computing in Sensor Systems (DCOSS).
3. He, T., C. Huang, B. Blum, J. Stankovic and T. Abdelzaher, 2003. Range-free localization schemes in large scale sensor networks.
4. Shang, Y., W. Ruml, Y. Zhang and M.P.J. Fromherz, 2003. Localization from mere connectivity, In Fourth ACM International Symposium on Mobile Ad-Hoc Networking and Computing (MobiHoc), June.
5. Perkins, C.E. and E.M. Royer, 1999. Ad-hoc On-Demand Distance Vector Routing, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp: 90-100.

6. Layuan, L., Y. Peiyan and L. Chunlin, 2007. Performance Evaluation and Simulations of Routing Protocols in Ad Hoc Networks, Computer Communications, 30: 1890-1998.
7. Perkin, C. and M. Royer Elizabeth, Ad hoc on demand Distance Vector Routing, RFC 3561, July 2003, http.//www.ietf.org/rfc/rfc3561.txt.
8. Enge, P. and P. Misra, 2001. Global Positioning System: Signals, Measurements and Performance, Ganga-Jamuna Pr.
9. Hightower, J., C. Vakili, G. Borriello and R. Want, Design and calibration of the spoton ad-hoc location sensing system.
10. Priyantha, N., A. Chakraborty and H. Balakrishnan, 2000. The cricket location-support system. In: Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom).
11. Bahl, P. and V.N. Padmanabhan, 2000. RADAR: An in-building RF-based user location and tracking system. In INFOCOM 2000, pp: 775-784.
12. Christ, T.W. and P.A. Godwin, 1993. A prison guard duress alarm location system. In IEEE International Carnahan Conference on Security Technology, October.
13. Add, A.M.L., K.E. Bekris, G. Marceau, A. Rudys, D.S. Wallach and L.E. Kavraki, 2002. Using wireless Ethernet for localization, In 2002 IEEE/RSJ International Conference on Intelligent Robots and Systems, September.
14. S.C.J.H.I.S.J.S.T.S.J.H.J.H.F.P.J.T.P.P.G.B. Anthony LaMarca, Yatin Chawathe and B. Schilit, 2005. Place lab: Device positioning using radio beacons in the wild. In Pervasive.
15. Lorincz, K. and M. Welsh, Mote Track: A Robust, Decentralized Approach to RF-Based Location Tracking. May.
16. Sichitiu, M.L., V. Ramadurai and P. Peddabachagari, 2003. Simple algorithm for outdoor localization of wireless sensor networks with inaccurate range measurements, In International Conference on Wireless Networks, pp: 300-305.
17. Patwari, N., A. Hero, M. Perkings, N. Correal and R. O'Dey, 2003.Relative location estimation in wireless sensor networks, IEEE Transactions on Signal Processing, Special Issue on Signal Processing in Networks, 51(8): 2137-2148.
18. Jeong, J. and S. Kim. Localization using dot3 wireless sensors. CS268 Class Project, UC Berkeley, 2003.
19. Hu, Y., A. Perrig and D. Johnson, Packet leashes: a defense against wormhole attacks in wireless networks, in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), 2003.
20. Li, Z., W. Trappe, Y. Zhang and B. Nath, Robust statistical methods for securing wireless localization in sensor networks, in Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005).
21. Liu, D., P. Ning and W. Du, 2005. Attack-resistant location estimation in sensor networks, in Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005).
22. Lazos, L., R. Poovendran and S. Capkun, 2005. Rope: robust position estimation in wireless sensor networks, in Proceedings of the Fourth International Symposium on Information Processing in Sensor Networks (IPSN 2005), 324-331.