DOI 10.29042/2019-5042-5045

Helix Vol. 9 (3): 5042- 5045

Detection of Security Attack in IoT using Received Signal Strength Indicator

*[1]Snehal Deshmukh-Bhosale, [2]Dr. S. S. Sonavane

[1] Asst. Professor, RMD Sinhgad School of Engg, Warje, Pune & Research Scholar, Raisoni College of Engg and Management, Wagholi, Pune

[2] Professor, Dean Research, Indira College of Engineering & Management, Parandwadi, Pune,

*Email: sa_bhosale@yahoo.com

Received: 04th January 2019, Accepted: 13th February 2019, Published: 30th June 2019

Abstract

For Internet of Things (IoT) applications, the correct location of sensor node is a very important aspect. To achieve this the solution is quite expensive where it is needed to incorporate Global Positioning System (GPS) adapters in each sensor node. In IoT, majority sensors are small in size and constrained in terms of processing power, memory, battery life etc. So to add a GPS adapter into it is not a feasible solution. Also, GPS adapter cannot be used for indoor IoT applications. To achieve small-size and cost-effective solution, Received Signal Strength Indicator (RSSI) based localization technology is used for distance estimation. The correlation between distance and RSSI values are used to find ranging and localization in IoT. In the era of smart cities, localization is a key component for many applications like smart buildings, traffic management, parking etc. For indoor applications like home automation, GPS is not a practical solution hence RSSI technology is used to achieve correct localization of a sensor node. Many attacks like Wormhole attack, Sinkhole attack, Blackhole attack etc. which are taking place in IoT can be detected by finding the correct location of a sensor node. In this paper, we have used Contiki OS and its inbuilt Cooja simulator to find the expected result. We are using RSSI values to find the location of sensor nodes in given various topologies.

Keywords

Localization, Internet of Things, GPS, RSSI, Security, Attacks

Introduction

In IoT, all sensors used are constrained in many terms. A GPS is a good solution but it is not a practical application for IoT sensor nodes. It cannot be further burdened with extra hardware like GPS adapter for localization. There are many applications like traffic monitoring, object tracking, fire detection, home automation etc. where locating the sensor is a most important aspect. Even in rescue operations in case of earthquake, flood etc locating a person for survival is very important and challenging tasks. All these applications in IoT signifies the important role of correct localization. [1], [2],[3]

Over the past few years, many solutions have been proposed for localization in wireless ad-hoc and sensor networks which can be broadly classified into two main categories – *range based* and *range free*. Range based techniques estimate distances (range) from RSS measurements between the unknown node and the reference nodes and uses them to triangulate the location of the unknown node [4], [5], [6], [7], [8]. On the other hand, range free techniques estimate the location of the unknown node without determining the range like GPS, Cricket, and Ultrasonic sensor-based techniques. For our work, we have studied some range based localization techniques and previous analysis done on utilizing RSSI for localization.

For localization Received Signal Strength Indicator (RSSI) is a feasible solution for all IoT sensor nodes as it is inbuilt in almost all sensors. It does not require any added hardware. It indicates the strength in terms of power present in the received signal which comes under the IEEE 802.11 standard. There is no direct relation between RSSI value and power level in dBm defined by 802.11 standards. Vendors and manufacturers have defined the relationship between these two as per their products.

RSSI finds the distance between two sensors using power in the radio signal received by the receiver after the antenna and cable loss. RSSI values are measured in decibels (dB) hence it comes in negative terms (eg -120dB). Nearer the value of RSSI to zero, stronger is the signal. Till -40 dB signal is considered as a stronger signal and it is acceptable. Beyond -100 dB it is weak hence it is rejected by the sensor node.

Need of Security in IoT

Due to increased interest in IoT, many smart devices are connected to each other through the internet. IoT is grabbing space in professional as well as personal applications like a smart city to smart home. Many objects can be controlled remotely and connected to each other using various protocols like Zigbee, Z-wave or Bluetooth through the internet. As all these appliances used in IoT are prone to various security attacks, security is the most important concern in IoT. IoT network is vulnerable because of less lifespan of IoT devices, less cost and also because of no standardization as security is not thoroughly addressed while designing a smart network using IoT. Traditional security solutions cannot be used for IoT devices due to resource-constrained nature of these devices. Due to all these drawbacks many security attacks like wormhole attack, blackhole attack, a man in middle

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

attack etc. are present in IoT network. To detect these attacks, knowledge of attacker location is very important without which it is impossible to remove the attacker and so is the attack. To understand the location of attacker many localization techniques are used where many of which are straightway imported from Wireless Sensor Network (WSN). [9]

Related Work

Localization:

In IoT, locating sensor is the most important thing for communication as well as for detection of security attacks. Capturing the data from the appropriate sensor and forwarding it to next the sensor is a very challenging task. If the centralized server is unaware of the positions of IoT devices, then information generated by these devices are irrelevant and their limited resources are wasted by forwarding information blindly. To increase the efficiency of the IoT network, localization of sensors in real time with minimum knowledge of their surrounding is an essential aspect.

Different Wireless Technologies for Localization:

1. **WiFi-** A Wifi is the simplest option to implement due to the high availability of access points found in buildings. It also requires minimal additional hardware. But it utilizes a large amount of power which will not go well with IoT network which is having limited battery life. [10]
2. **Bluetooth-** BLE and their beacons are less expensive option which can be placed in the existing network of IoT to give better localization of IoT devices. The drawback of most of the beacon functions of BLE is batteries. Once the battery is depleted, it is no more useful. To replace the battery is going to be a very costly solution. [11], [12]
3. **LoRaWAN-** It has very good transmission range with low energy requirement. It is used for IoT localization in large areas. It gives good performance for outdoor localization but it is worst for indoor localization in terms of performance. [13]

Like these technologies, few more solutions are available eg. RFID, UWP, cellular etc. They are having their own pros and cons. As per requirement, we can use any of those accordingly.

Modes of Localization:

1. **Angle of Arrival (AoA):**
   In this method, the geometric principle of angles of triangles is used to determine the position of the receiver. But this method requires complex hardware and calibration to get an accurate location. [14], [15], [16]
2. **Time of Arrival (ToA):**
   In this method, synchronized clocks between transmitter and the receiver are used to determine signal propagation time from transmitter to receiver. The drawback of this method is that extra hardware is required to have synchronized clocks. [15], [16]
3. **Time Difference of Arrival (TDoA):**
   TDoA also uses the same principle as that of ToA, but it uses propagation time of the transmitted signal, received by multiple receivers. The distance between transmitter and receiver is calculated by difference different arrival time of receivers. [16]
4. **Received Signal Strength Indicator (RSSI):**
   Nowadays, RSSI is a very popular method for localization. It is one of the simplest and cheapest methods so far. It doesn't require any additional hardware and it is inbuilt in most of the wireless technology hardware. In this method, the distance between transmitter and receiver is measured using the strength of a signal of packets received by the receiver.[17],[18],[19].

   The RSSI values can be converted to a length, which can provide the estimated distance between the nodes. To relate the determined RSSI values to a distance, the path loss model [20] is used, which is seen in equation 1:

$$RSSI = -10n\log_{10}(d) + C \quad (1)$$

In this equation, n is the path loss exponent that varies depending on the environment, d is the distance between the transmitting and receiving devices, and C is a fixed constant that accounts for system losses.

Proposed System

The proposed system is used to find out RSSI values using Cooja simulator of Contiki Operating System. In the proposed system initially, it has been started with two nodes. With the RSSI program, which finds the strength of the signal, transmitted and received by both the nodes. It has been observed that as the distance between two nodes is varied the RSSI value changes. RSSI value is calculated in dBm. Experimentation result is shown in the following figure. The distance variation is shown in Fig 1. (a), (b), (c). In its write side window, the change in RSSI values is observed.

This experimentation is done for various topologies for N=8, 16, 24. The distance between all these nodes from each other is calculated using RSSI values. If there is a change in RSSI values between two nodes of given topology than already stored values then it is concluded that an attack has taken place. The delay of packet transmission occurs because of some attacks for eg. Wormhole attack. Because of this delay, the RSSI value of transmitted packet is decreased which could be further concluded as presence of attack. With the help of RSSI values, further a attacker is also detected.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

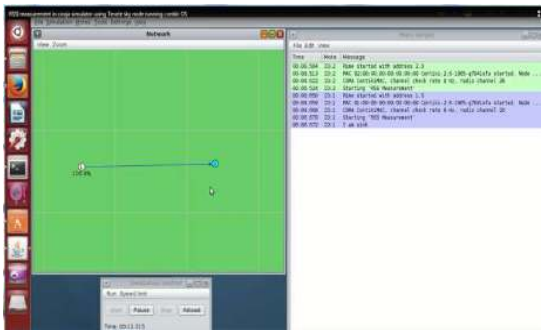

Figure 1(a): Simulation Setup

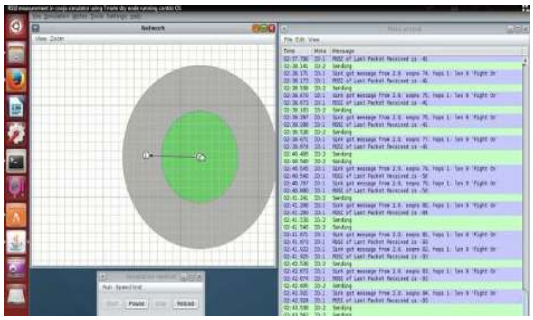

Figure 1(b): Simulation Setup

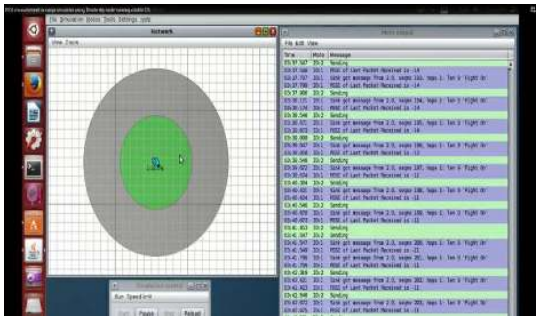

Figure 1(c): Simulation Setup

Results and Discussion

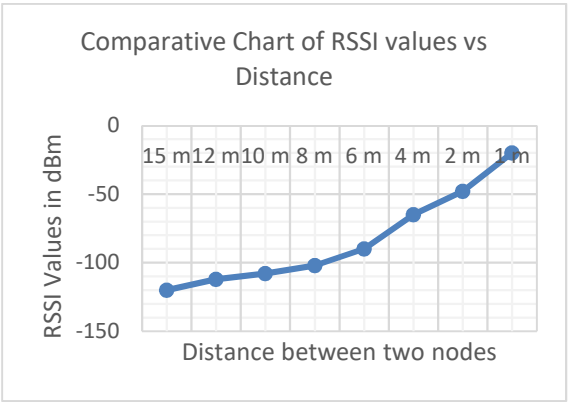

Figure 2: Simulation Reading of RSSI values

As shown in Fig 2, it is observed that, as distance varies between two nodes, RSSI values also vary. It shows the strength of received signal increases as a distance between two nodes is reduced. RSSI value is measured in dBm.

This graph is very important to observe how RSSI values vary with distance variation. These values further used to identify presence of security attack. While tracing any security attack, it is observed that RSSI values shown in Fig. 2, don't remain constant in presence of attack. In most of the cases eg. Wormhole attack, Blackhole attack, DoS attack, when any attack takes place, the transmission delay increases which affects the change in RSSI values.

 Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495

Conclusion

Localization is a very important aspect to detect the sensor node in the Internet of Things. There are many applications of localization which vary in many fields in today's era of smart city and smart home. To improve the security in IoT, it is very important to locate the security attacker node correctly. After finding the desired node, it could be removed from existing network permanently to remove the attack from the network. There are many methods to locate the node correctly. In our research work, we have used Received Signal Strength (RSS) localization method to locate the node position. Initially a experimentation is done to find the distance between every node with the help of RSSI values. After comparing the already stored RSSI values and the RSSI values received by the receiver after insertion of attack, it is noted that there is a large difference between those values. Hence it is concluded that the attack is present in the network

References

[1] N. A. Alrajeh, M. Bashir, and B. Shams, "Localization techniques in wireless sensor networks," Int. J. Distrib. Sensor Netw., vol. 9, no. 6, p. 304628, 2013.

[2] F. Zafari, I. Papapanagiotou, M. Devetsikiotis, and T. J. Hacker. (Mar. 2017). "An iBeacon based proximity and indoor localization system." [Online]. Available: https://arxiv.org/abs/1703.07876

[3] Sebastian Sadowski, Petros Spachos, "RSSI-Based Indoor Localization with the Internet of Things", IEEE Access, Digital Object Identifier 10.1109/ACCESS.2018.2843325, June 2018

[4] Ambili Thottam Parameswaran, Mohammad Iftekhar Husain, Shambhu Upadhyaya, "Is RSSI a Reliable Parameter in Sensor Localization Algorithms" – An Experimental Study, Field Failure Data Analysis Workshop September 27-30, 2009: Niagara Falls, New York, U.S.A.

[5] Kiran Yedavalli, Bhaskar Krishnamachari, Sharmila Ravula, Bhaskar Srinivasan, "Ecolocation: A Sequence Based Technique for RFLocalization in Wireless Sensor Networks", USC CENG TechnicalReport Number 2004- 16.

[6] Mohit Saxena, Puneet Gupta, BijendraNath Jain, "Experimental Analysis of RSSI-based Location Estimation in Wireless Sensor Networks", 3rd International ICST Conference on Communication, January 2008.

[7] Erin-Ee-Lin Lau, Boon-Giin Lee, Seung-Chul Lee, Wan-Young Chung, "Enhanced RSSI-based High Accuracy Real- Time User Location Tracking System for Indoor and Outdoor Environments", International Journal on Smart Sensing and Intelligent Systems, VOL. 1, NO. 2, JUNE 2008.

[8] R. Pahtma, J. Preden, R. Agar, P. Pikk, Utilization of Received Signal Strength Indication by Embedded nodes, ELECTRONICS AND ELECTRICAL ENGINEERING, 2009. No. 5(93), ISSN 1392 -1215.

[9] Ms. Snehal Deshmukh, Dr. S. S. Sonavane, "Security Protocols for Internet of Things: A Survey", ICNETS2, VIT University, Chennai, 2017, 978-1-5090-5913-3/17/$31.00_c 2017 IEEE.

[10] T. Pering, Y. Agarwal, R. Gupta, and R. Want, "Cool Spots: Reducing the power consumption of wireless mobile devices with multiple radio interfaces," in Proc. 4th Int. Conf. Mobile Syst., Appl. Services (MobiSys). New York, NY, USA: ACM, 2006, pp. 220_232. [Online]. Available: http://doi.acm.org/10.1145/1134680.1134704

[11] R. Faragher and R. Harle, "Location printing with Bluetooth low energy beacons," IEEE J. Sel. Areas Commun., vol. 33, no. 11,pp. 2418_2428, Nov. 2015.

[12] W. He, P.-H. Ho, and J. Tapolcai, "Beacon deployment for unambiguous positioning," IEEE Internet Things J., vol. 4, no. 5, pp. 1370_1379, Oct. 2017.

[13] LoRaWAN. LoRa Alliance Technology Online Available: https://www.bluetooth.com/speci_cations/ bluetooth-core- speci_cation

[14] H. Liu, H. Darabi, P. Banerjee, and J. Liu, "Survey of wireless indoor positioning techniques and systems," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev., vol. 37, no. 6, pp. 1067_1080, Nov. 2007.

[15] Z. Farid, R. Nordin, and M. Ismail, "Recent advances in wireless indoor localization techniques and system," J. Comput. Netw. Commun., vol. 2013, Aug. 2013, Art. no. 185138.

[16] F. Zafari, A. Gkelias, and K. Leung. (Sep. 2017). "A survey of indoor localization systems and technologies." Online. Available: https://arxiv.org/abs/1709.01015

[17] A. S. Paul and E. A. Wan, "RSSI-based indoor localization and tracking using sigma-point Kalman smoothers," IEEE J. Sel. Topics Signal Process., vol. 3, no. 5, pp. 860_873, Oct. 2009.

[18] K. Wu, J. Xiao, Y. Yi, D. Chen, X. Luo, and L. M. Ni, "CSI-based Indoor Localization," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 7, pp. 1300_1309, Jul. 2013.

[19] S. Mazuelaset al., "Robust indoor positioning provided by real-time RSSI values in unmodified WLAN networks," IEEE J. Sel. Topics Signal Process., vol. 3, no. 5, pp. 821_831, Oct. 2009.

[20] P. Kumar, L. Reddy, and S. Varma, "Distance measurement and error estimation scheme for RSSI based localization in Wireless sensor networks," in *Proc. 5th Int. Conf .Wireless Commun. Sensor Netw. (WCSN)*, Dec. 2009, pp. 14.

  Helix E-ISSN: 2319-5592; P-ISSN: 2277-3495