An Overview of Wireless Indoor Positioning Systems: Techniques, Security, and Countermeasures

Mouna S. Chebli(✉), Heba Mohammad, and Khalifa Al Amer

Higher Colleges of Technology, Abu Dhabi, UAE
{mshebli,hmohammad,kal-amer}@hct.ac.ae

Abstract. The interest in Indoor position systems (IPSs) had been widely increased recently, due to technological advancement. IPSs provide users with location information of various objects inside big buildings, typically using a mobile device. Different wireless technologies are available to provide location service such RF, Wi-Fi, Bluetooth, Visible Light Communication (VLC), etc. IPSs mainly determine the position by analyzing sensory information which is collected by mobile device continuously on real time, unless the user turned off the service. Various services and security issues had been associated with IPSs. Secure positioning become more important and crucial to the success of the delivered service. Location service network that based on off-air signal measurement is susceptible to numerous attacks (e.g. wormhole, sinkhole and Sybil attacks). This paper aims to provide an integrated view of IPSs, technologies and associated security threats that face such positioning systems. The paper compares different wireless indoor position technologies, explore potential attacks, and evaluate IPS protection mechanism.

Keywords: Indoor positioning · Secure localization · WSN security

1 Introduction

Nowadays, the widespread of mobile devices allowed indoor positioning systems to receive greater attention [1]. IPSs have successfully integrated in different areas including health, assets tracking, child safety [2] and industry [3]. The systems detect the location of objects or humans in closed environment where satellite signals are unavailable or inaccurate. Moreover, GPS cannot be used for indoor positioning due to signal scattering, attenuation, and for the wide marginal error which can be bigger than the space itself. IPSs use two different nodes, the mobile-node and anchor-node. The anchor-nodes give reference points to detect location (e.g. Access Point) [4]. Implementing IPSs using RF can reduce the cost by reusing the existing network infrastructure. If the cost and deployment speed are the main consideration, then it is better to use the existing WLAN infrastructure. However, RFID and Bluetooth IPSs have better precision and accuracy [5]. Hybrid infrastructure can be used to improve the quality of the system [6].

R. Montella et al. (Eds.): IDCS 2019, LNCS 11874, pp. 223–233, 2019.
https://doi.org/10.1007/978-3-030-34914-1_22

Wireless signals weaken while traveling over space, IPSs use different methods to estimate nodes location. Received Signal Strengths (**RSS)** method determines distance between transmitter and receiver by evaluating signal strength at receiving point. RSS based localization is susceptible to localization error caused by low-cost antenna which is used by adversary [7], statistical-test of variance is proposed to overcome this issue. **Proximate** method uses grid of base stations with pre-defined location. When a mobile-node in range of known base-station, then the location will be approximated. If mobile-node is in range of multiple base-stations, then the strongest signal will be considered. **Time of arrival (TOA)** method calculates the propagation time of a radio waves from one transmitter to another receiver, it provides a circle of possible location in two-dimensional space. The center of the circle is the base station, and the radius is the calculated distance [8], as shown in (Fig. 1). This technique requires accurate knowledge of transmission time and confirm that all base stations and mobile nodes are accurately synchronized with precise timing source [9]. **Time Difference of Arrival (TDOA)** method measures the difference time of arrival of the signal emitted by multiple base stations [10] (see Fig. 2). Three base stations create two TDOAs (L1 and L2), the intersection points between L1 and L2 estimates the location of the mobile-node. TDOA needs correct time reference between the measuring units.

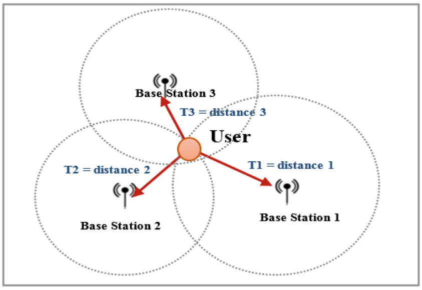

Fig. 1. Time of arrival concept (TOA)

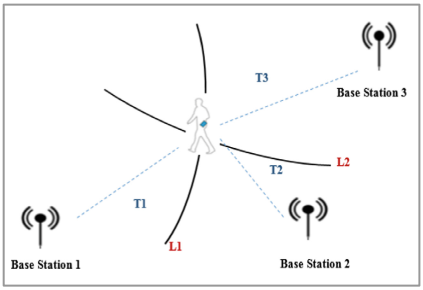

Fig. 2. Time difference of arrival concept

Angle of Arrival-AOA method determines the direction of RF signal when emitting from the antenna, this requires at least two angles to detect location. AOA is more complex and needs more expensive hardware. **Fingerprinting** technique determines the location by analyzing scene and compare it with the existing database. It consists of two stages: the first stage, offline stage, survey the area to collect location features and build the matching database. Location features include coordinates, and signals strength from adjacent base station. The second stage, online stage, will compare the current signal features with the database. There are several fingerprinting algorithms including: probabilistic methods, support vector machine (SVM), neural networks, k-nearest-neighbor (kNN), and smallest M-vertex polygon (SMP) [2].

IPS had been discussed by the research community from different perspectives. For instance, some researchers described the IPS in terms of implementation technologies and use, such as research paper [3, 16]. While [11] presented the IPSs from the performance perspective by comparing different performance measurements such as:

accuracy, electricity consumption and coverage range. Visible LED Lighting IPSs have great potential in future due to its low cost, security and high throughput. The research paper [12] surveyed VLC IPSs and discussed systems characteristics, positioning algorithms, and performance. However, few scholars highlighted the security threats and countermeasure aspects in indoor positing systems. Therefore, this paper aims to fill this gap by providing an integrated view of IPS from the security perspective.

2 IPS Network Infrastructure

This section will give a brief introduction of different IPS network infrastructures:

RFID IPS requires micro-circuit, antenna, and RFID reader, system can be passive or active [13]. Passive systems are reflectors. Therefore, it consumes less power than active, and does not require a power source in the mobile node. Active RFID tags are transceiver, it transmits its identification information and signal received from the reader [14]. RFID gives better accuracy and higher precision, it can be 50% precise in the distance of 1 m and accurate for a range less than 2 m. However, it is more complex and requires dense environment of RFID devices.

UWB uses sub-nanosecond radio pulses to send data in a wide range of bandwidth. It can use limited transmission power as restricted by FCC. This technology can be classified as: (1) Impulse Radio (IR-UWB) or (2) carrier-based UWB system. The first system sends narrow pulses with smooth transition (base-band). The second system, carrier based UWB is more complex design, although it is more flexible in selecting frequency [15]. UWB measures the node position using TDOA of the radio frequency signals [16].

Bluetooth IPSs can use two different approaches in defining the position. The first approach is based on proximity and RSS ranging techniques, the second approach is based on applying geometric calculation [5]. Although, geometric calculation is more accurate, it is considered more complex and prone to calculation errors. The low cost of Bluetooth chipset can reduce the price of positioning system implementation.

Visible Light Communication (VLC) is a LED-based IPSs that use visible light signals to transmit data, the installed LED-lamps on the ceiling will act as anchor nodes. VLC uses IEEE 802.15.7 standard and can give highly accurate location with a minimum calculation error [17]. This method found to be the most appropriate one [18]. In the system design, each LED-light will get unique address which represent its coordinate and the unique ID. The receiving nodes will forward the LED-ID to application service to determine location. VLC IPS can use proximate, triangulation or fingerprinting for positioning. The technology has several advantages: it is cost effective due to low energy consumption, longer life expectancy, and reusing the existing lighting system in the building. It does not produce electromagnetic interference, and therefore it is suitable where RF signal is prohibited, VLC is more secure as light cannot penetrate walls, and thus independent systems can be installed in different rooms smoothly. However, the technology is susceptible to different difficulties including: ambient Light, time measurement error, flickering and lens distortion [19]. Moreover, synchronization between LED-lights anchor nodes and mobile devices is very difficult to achieve [20].

WLAN IPSs which reuse the existing network infrastructure will reduce cost, however, WLAN IPS that is based on RSSI localization technique suffer from instability of the signal strength, therefore this system does not have high accuracy and precision. The accuracy of WLAN positioning system that utilizing RSS technique is approximately 1 to 5 m and the precision about 50% in 2 m [5]. Two approaches proposed to reduce errors: mono-objective and multi-objective approaches, both are based on variable neighbor search [6].

ZigBee defines higher level communication protocols that delivers network, security, and application support services operating on top of 802.15.4 standard for personal area network [21]. It is designed for small scale devices that require reliable wireless communication with low data transmission rate and low power consumption. ZigBee network consists of three types of devices coordinator, router, and end nodes [22]. ZigBee positioning systems are simple and operate using low power technology [23].

3 Secure Localization Services

Security is a crucial element when developing any information system, the next section discusses common attacks that would endanger IPSs, available countermeasures and the ability of localization algorithms to defeat the discussed threats.

3.1 Common Attacks

1. **False Node:** the insertion of additional node to the system. It can be used to propagate fake information or to prevent processing of legitimate signals.
2. **Spoofing:** a dishonest node impersonates the identity of legitimate base-station, this would persuade other nodes to believe that it is in a different location. Adversary can spoof management and control frame which can have huge impact on the network [24]. Spoofing can be the first step of DoS or injection attack.
3. **Sinkhole:** is an insider attack where malicious node tries to attract all neighboring node to establish connection with it, then it will attract all traffic from one area [25].
4. **Sybil:** attacker obtains several nodes identities, then use these identities to deceive other nodes. The compromised nodes identities can be replicated to several locations in the network and cause erroneous information [26].
5. **Replay:** involves storing the packets to re-sending then late, this cause the neighboring nodes to believe that the packet is authentic as it is a copy of the original. In this attack, the adversary first will jam the transmission between sender and receiver and will replay the packets in the future and claim that he is the sender [27].
6. **Wormholes:** malicious node records packet at one side of the network and re-transmit and replicate it by another malicious node on the side of the network, this can be done by adding virtual tunnel which has a low latency link [28].
7. **Hello flood:** the malicious node floods the network with hello message with increased power, and that will confuse the routine protocol and the victim node will try to refer to the adversary for localization service [28].

8. **Denial of Service:** DOS attack tries to stop the service by flooding the network with traffics that consume all available resources and deny legitimate nodes from benefit from the service. The attacker can inject bogus broadcast packet and force network nodes to complete expensive signature verification or packet forwarding broadcast authentication [29] which will result denying the service. DOS can occur at any layer of network model as illustrated in Table 1.

Table 1. Denial-of-Service attack at each layer of the network

Layer	Attack
Application	Reprogramming attack
Transport	Desynchronization attacks - Flooding Attacks
Network	Spoofing, routing-control traffic or clustering messages, replaying and homing
Datalink	Collision, exhaustion and unfairness attacks
Physical	Packet jamming and Anchor-Node tempering

3.2 Security Countermeasure

Security Through Cryptography: Malicious nodes can claim the identity of another legitimate entity and then alters the packet contents, this can be eliminated using cryptography and authentication. However, cryptography can only protect from external attacks and cannot defeat dishonest node that sends wrong positioning data. In addition, crypto-system requires additional resources, e.g. better processing speed and larger memory, and most of sensory devices has limited computational power. Therefore, most of secure localization algorithms use non-cryptographic security mechanism [30].

Misbehavior Detection and Blocking: This countermeasure technique involves monitoring nodes behavior over time to decide whether to trust them or not. Any information gathered from untrusted source will be ignored accordingly. To detect malicious node, Liu et al. [31] proposed two different methods. Method 1 compares the estimated distance of the beacon nodes with the average estimated distance of the signal (e.g., AoA, TDoA). If the distance between them is larger than the maximum distance error, then the received beacon is malicious. Method 2 can protect against replay attack and sinkhole, by introducing the idea that malicious beacon will need more time. Mainly, it examines the Round-Trip Time (RTT) between two neighbor nodes and try to detect if it differs significantly from the (RTT) range derived from monitoring network behavior. DRBT [32] proposed blocking untrusted nodes by allowing each base station to monitor the area and contribute in building trust table.

Detecting Location Using Statistical Method: Every anchor node has a specific location in the grid of cells. To determine the location of mobile-node, neighboring anchor-nodes can vote for the location, then the center of the most voted cell can be used as location. If malicious node sends a forgery data, it can be detected by comparing it with the context of the other cells. Another statistical method is using

Minimum Mean Squared Estimation (MMSE) [33]. This will verify if the estimated position is derived from consistent reference. If inconsistent sensor detected it will be revoked, and the node position will be calculated over again. This process will be repeated until all inconsistent nodes revoked. RRB-ScLoc proposed secure localization based on weighted square [34].

Counter Measure Hello-Flood Attack: Anchor nodes at wireless positioning networks are required to broadcast hello message to announce themselves to neighboring nodes. Attacker might inject the network with false hello packets, there are some methods to protect from hello flood attack including multi-path and multi based station data forwarding as described in [35], in this technique each node maintains a number of secret keys which can be used to transmit data to several routes. Another algorithm proposed an enhanced method to protect from Hello flood attack using client puzzle key. This will use a number that constitute a puzzle key, and it will be used to verify the validity of a node. The puzzle key difficulty will be increased when the node sends larger number of hello message (Puzzle difficulty $\propto$ Number of hello messages). Therefore, the node that send a fewer number of hello messages, will be processed first [36].

3.3 Secure Localization Algorithms

This section will discuss different secure localization algorithms.

SeRLoc [37]: Secure range independent localization for wireless sensor networks proposed by Lazos and Poovendran. SeRLoc uses two types of nodes mobile nodes (N) and Locators (L). Locators use omnidirectional antenna and mobile nodes can get location by analyzing signal emitted from locators. Locator propagates its coordinate and the angels of the antenna boundary line. Adversary needs to impersonate multiple beacons to compromise the system. SeRloc is range-free and distributer mechanism, it is robust against wormhole, impersonate and Sybil attacks. To improve localization accuracy, additional locator nodes must be installed or more directional antenna [38]. SeRLoc assumes that that no jamming of wireless medium will occur, and it cannot protect from attacks that target locator's information [27].

HiRLoc [39]: In this model, node detect its location passively without increasing the number of reference points. The node determines location by intersection beacon-frames in the coverage area with multiple reference points. HiRLoc is immune to Sybil attack, wormhole attack, false beaconing and impersonating. HiRLoc utilizes two properties: antenna orientation and communication range. This system uses cryptographic primitives to secure beaconing frames. GSK (Global symmetric key) is used to encrypt beacons frames. HiRLoc has better accuracy than SeRolc, whereas nodes receive multiple beaconing frames from different locators [38]. However, it causes more computation and communication overhead.

SPINE [40]: This system obtains location based on Verifiable Multilateration (VM), the system measures the propagation time of radio signal by examining at least three anchor nodes which provide a robust estimation. SPINE is immune to wormhole, jamming and spoofing attack. It also can prevent dishonest node from distribution fake location. Nodes in SPINE cannot produce wrong distance measurement. Although, SPINE requires a high number of reference points, and it can also cause a bottle-neck in the system [38].

ROPE [41]: This system uses location verification mechanism before the data collection phase which allow the nodes to detect their location without using centralized computation. The system defines two different types of nodes: sensors which equipped with omnidirectional antenna and locators which equipped with M-directional antenna. Every sensory node shares a pairwise key with every locator. To decrease storage size, pairwise keys are derived from master key. ROPE is a robust localization system, it is immune to traffic jamming, spoofing and Sybil attack. It is also resistant to wormhole attack.

DRBTS [32]: Distributed Reputation-based Beacon Trust System aims to exclude malicious beaconing nodes that propagate false location information to the network. The model assumes that every beaconing node monitor its first-hope neighbor to inspect any misbehaving beaconing frame, and then updates the reputation of the neighboring nodes to (NRT) neighbor's reputation table. This table will be used to either trust or reject broadcasted beacon frame based on the voting scheme. The robustness of the DRBTS system enhanced with increasing the number of beacon nodes. The system enables the network to find out which nodes can be trusted when determining the location. DRBTS can protect the network from impersonating, range changing and false beaconing frame.

The next Tables 2 and 3 will compare all the above localization algorithms using different factors such as behavior, robustness, disadvantages and the immunity to different threats.

Table 2. Secure Localization Algorithms overcoming security threats

System	Defeat region change	Defeat false-beacon	Defeat impersonating	Defeat wormhole	Defeat sybil
SeRLoc [37]	–	No	Yes	Yes	Yes
HiRLoc [39]	–	Yes	Yes	Yes	Yes
SPINE [40]	Yes	–	Yes	Yes	Yes
ROPE [41]	Yes	Yes	Yes	Yes	Yes
DRBTS [32]	Yes	Yes	Yes	No	No
Liu et al. [31]	Yes	Yes	Yes	Yes	No

Table 3. Secure localization systems comparison

System criteria	SeRLoc [37]	HiRLoc [39]	SPINE [40]	ROPE [41]	DRBTS [32]	Liu et al. [31]
Behavior	Prevention	Prevention Filtering	Prevention	Prevention Filtering	Detection	Detection
Cryptography	Encryption and authentication of beacon. Uses Global Symmetric Key	Encryption and authentication of beacon. Uses Global Symmetric key	Symmetric or public key encryption for authenticated distance estimator	Encryption and authentication of the beacon with pairwise keys, able to manage cryptographic primitives.	Encrypt using network wide group key. This allows network observation, and prevents outsiders from eavesdropping.	Beacon frames authenticated using pairwise key establishment
Misbehavior Detection	–	–	–	–	Yes, use reputation and trust base	Compare Distances and examine round trip time (RTT)
Robust	–	–	Verifiable Multination [present probabilistic notion of robust quadrilaterals]	–	Depends on the size of the common neighbor. Higher number of Beacon nodes the more robust DRBTS gets	Robust Statistical Method And voting method
Additional Hardware	Requires Additional Locator with directional antenna to improve accuracy	Requires extra hardware in a beacon node	Needs nanosecond clock, and radio frequency DB devices	Requires directional antenna in beacon nodes	–	Requires redundant beaconing nodes
Disadvantages	Additional locator information must be installed. Assume no jamming happens in wireless medium	Cause more computation and communication overhead	Requires a high number of reference points. Spine might cause a bottleneck in the system	Needs higher hardware requiremens	Dense Network	Needs higher number of anchor nodes
Simple	Yes	Yes	–	Yes	–	–

4 Conclusion

In this research paper, Indoor Positioning Systems had been presented from different security aspects and security countermeasures were discussed. The paper highlighted several security threats that would affect the success of the IPSs significantly.

It had been found that Cryptographic techniques are difficult to implement for real-time systems due to the high computational overhead and hardware requirements such as large primary memory. Therefore, it is important to find alternative methods that would provide secured IPS without relying on cryptography only. The paper compares various secure localization algorithms. The comparison integrated different criteria's such as cryptography, detection behavior, advantages, additional requirements, etc. Each presented threat had been mapped to secure localization algorithm, helping in defining the best algorithm that could be adopted in IPSs. For instance, the security algorithm which could be used to defeat most of the threats is ROPE. Despite the ability of Liu et al. to defeat most of the presented threats, it cannot defeat the Sybil threat.

Although, this paper is considered one of the few papers that described the IPSs in terms of security threats and prevention algorithms, more investigation could be done to evaluate Visible light localization service.

References

1. Li, T., Chen, Y., Zhang, R., Zhang, Y., Hedgpeth, T.: Secure crowdsourced indoor positioning systems. In: IEEE Conference on Computer Communications, Honolulu (2018)
2. Liu, H., Darabi, H., Banerjee, P., Liu, J.: Survey of wireless indoor positioning techniques and systems techniques and systems. IEEE Trans. Syst. Man Cybern. **37**(6), 1067–1080 (2007)
3. Mier, J., Jaramillo-Alcázar, A., Freire, J.J.: At a glance: indoor positioning systems technologies and their applications areas. In: Rocha, Á., Ferrás, C., Paredes, M. (eds.) Information Technology and Systems. ICITS 2019. Advances in Intelligent Systems and Computing, vol. 918, pp. 483–493. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-11890-7_47
4. Van Haute, T., et al.: Performance analysis of multiple Indoor Positioning Systems in a healthcare environment. Int. J. Health Geogr. **15**(1), 1–15 (2016)
5. Mišić, J., Milovanović, B., Vasić, N., Milovanović, I.: An overview of wireless indoor positioning systems. Infoteh-Jahorina **14**, 301–306 (2015)
6. Yassin, A., et al.: Recent advances in indoor localization: a survey on theoretical approaches and applications. IEEE Commun. Surv. Tutorials **19**, 1327–1346 (2017)
7. Zafari, F., Kin, L.K.: A survey of indoor localization systems and technologies. IEEE Commun. Surv. Tutorials **21**, 2568–2599 (2018)
8. Kim, S., Ha, S., Saad, A., Kim, J.: Indoor positioning system techniques and security. In: IEEE-Forth International Conference on e-Technologies and Networks for Development (ICeND), pp. 1–4 (2015). 10.1109(7328540)
9. Cisco, Wi-Fi Location-Based Services 4.1 Design Guide, Cisco Systems, Inc., San Jose (2008)
10. Disha, A.M.: A comparative analysis on indoor positioning techniques and systems. Int. J. Eng. Res. Appl. (IJERA) **3**(2), 1790–1796 (2013)
11. Malik, A., Zulfiqar, T., Javed, M.A., Nafi, N.S., Lodhi, H.: Performance evaluation of Wi-Fi finger printing based indoor positioning system. In: 2018 IEEE Conference on Wireless Sensors (ICWiSe), Langkawi (2018)
12. Zhuang, Y., et al.: A survey of positioning systems using visible LED lights. IEEE Commun. Surv. Tutorials **20**(3), 1963–1988 (2018)
13. Bouet, M., Dos Santos, A.L.: RFID tags: positioning principles and localization techniques. In: 1st IFIP Wireless Days, Dubai, pp. 1–5 (2008)
14. Gu, Y., Lo, A., Niemegeers, I.: A survey of indoor positioning systems for wireless personal networks. IEEE Commun. Surv. Tutorials **11**(1), 13–32 (2009)

15. García, E., Poudereux, P., Hernández, Á., García, J.J., Ureña, J.: DS-UWB indoor positioning system implementation based on FPGAs. Sens. Actuators A. Phys. **201**, 172–181 (2013)
16. Alarifi, A., et al.: Ultra-wideband indoor positioning technologies: analysis and recent advances. Sensors **16**, 707 (2016)
17. Mousa, F.I.K., Almaadeed, N., Busawon, K., Bouridane, A., Binns, R., Elliot, I.: Indoor visible light communication localization system utilizing received signal strength indication technique and trilateration method. Opt. Eng. Digit. Lib. **57**, 016107 (2018)
18. Brena, R.F.: Evolution of indoor positioning technologies: a survey. J. Sens. **2017**, 21 (2017)
19. Rajagopal, N., Lazik, P., Rowe, A.: Visual light landmarks for mobile devices. In: Proceedings of the 13th International Symposium on Information Processing in Sensor Networks, pp. 249–260. IEEE Press, April 2014
20. Do, T.-H., Yoo, M.: An in-depth survey of visible light communication based positioning systems. Sensors **16**(5), 678 (2016)
21. Hernandez, O., Jain, V., Chakravarty, S., Bhargava, P.: Position Location Monitoring Using IEEE 802.15.4 ZigBee technology. http://www.nxp.com/assets/documents/data/en/brochures/PositionLocationMonitoring.pdf. Accessed 5 Dec 2016
22. Kaushal, K., Kaur, T., Kaur, J.: ZigBee based wireless sensor networks. Int. J. Comput. Sci. Inf. Technol. (IJCSIT) **5**(6), 7752–7755 (2014)
23. Yick, J., Mukherjee, B., Ghosal, D.: Wireless sensor network survey. Comput. Netw. **52**, 2292–2330 (2008)
24. Yang, J., Chen, Y., Trappe, W., Chen, J.: Detection and localization of multiple spoofing attackers in wireless networks. IEEE Trans. Parallel Distrib. Syst. **24**(1), 44–58 (2013)
25. Kibirige, G.W., Sanga, C.: A survey on detection of sinkhole attack in wireless sensor network. arXiv preprint arXiv:1505.01941 (2015)
26. Yuan, Y., Huo, L., Wang, Z., Hogrefe, D.: Secure APIT localization scheme against sybil attacks in distributed wireless sensor networks. IEEE Access **6**(2018), 27629–27636 (2018)
27. Jiang, J., Han, G., Zhu, C., Dong, Y., Zhang, N.: Secure localization in wireless sensor networks: a survey. J. Commun. **6**(6), 460–470 (2011)
28. Singh, V.P., Anand Ukey, A.S., Jain, S.: Signal strength based hello flood attack detection and prevention in wireless sensor networks. Int. J. Comput. Appl. **62**(15), 1–6 (2013)
29. Ning, P., Liu, A.: Mitigating DoS attacks against broadcast authentication in wireless sensor networks. ACM Trans. Sens. Netw. **4**(1), 1–3 (2008)
30. Boukerche, A., Nakamura, E.F., Loureiro, A.A.F.: Secure localization algorithms for wireless sensor networks. IEEE Commun. Mag. **0163–6804**, 96–101 (2008)
31. Liu, D., Ning, P.: Detecting malicious beacon nodes for secure location discovery in wireless sensor network. In: 25th IEEE International Conference on Distributed Computing Systems, pp. 1063–6927 (2005)
32. Srinivasan, A., Teitelbaum, J., Wu, J.: DRBTS: distributed reputation-based beacon trust system. In: 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, pp. 277–283 (2006)
33. Liu, D., Ning, P., Du, W.K.: Attack-resistant location estimation in sensor networks. ACM Trans. Inf. Syst. Secur. (TISSEC) **11**(4), 22 (2008)
34. Mukhopadhyay, B., Srirangarajan, S., Kar, S.: Robust range-based secure localization in wireless sensor networks. In: IEEE Global Communications Conference (GLOBECOM), Abu Dhabi (2018)
35. Hamid, A., Rashid, M., Hong, C.S.: Defense against lap-top class attacker in wireless sensor network. In: 8th International Conference Advanced Communication Technology, pp. 318–323, February 2006

36. Singh, V.P., Jain, S., Singhai, J.: Hello flood attack and its countermeasures in wireless sensor network. IJCSI Int. J. Comput. Sci. Issues **7**(3), 23–26 (2010)
37. Lazos, L., Poovendran, R.: SeRLoc: secure range-independent localization for wireless sensor networks. In: 4th ACM Workshop on Wireless Security, Philadelphia, pp. 21–33, October 2004
38. Srinivasan, A., Wu, J.: A survey on secure localization in wireless sensor networks. In: Wireless and Mobile Communications. CRC Press/Taylor and Francis Group, London (2007)
39. Mohd, W.G., Sharma, S., Saklani, A., Singhal, A.: HiRLoc: high-resolution robust localization for wireless sensor networks. J. Comput. Eng. (IOSR-JCE) **16**(2), 112–115 (2014)
40. Capkun, S., Hubaux, J.-P.: Secure positioning of wireless devices with application to sensor networks. In: Proceedings of IEEE Computer and Communications Societies, vol. 3, pp. 1917–1928 (2005)
41. Lazos, L., Poovendran, R., Capkun, S.: Robust position estimation in wireless sensor networks. In: Proceedings of the 4th International Symposium on Information Processing in Sensor Networks, pp. 324–331 (2005)