SDN-Based Secure Localization in Heterogeneous WSN

Meigen Huang(✉) and Bin Yu

Zhengzhou Information Science and Technology Institute,
Zhengzhou 450001, China
huang_meigen@163.com, byu2009@163.com

Abstract. There is a big security risk in traditional distributed localization without protecting the location and identity privacy of anchor nodes. Thus, based on software-defined networking (SDN), we propose a security localization mechanism for heterogeneous wireless sensor networks (WSN). After obtaining the state of sensor nodes in data plane, SDN controller runs the complementary range-based and range-free positional algorithms in a centralized way. At the same time, the difference of transmission power of heterogeneous sensor nodes is taken into account. The security analysis and experimental results show that the mechanism can reduce the positioning error while ensuring the privacy of anchor nodes.

Keywords: Wireless Sensor Networks (WSN)
Software-Defined Networking (SDN) · Secure localization · RSSI
DV-Hop

1 Introduction

The rapid development of Internet of Things (IoT) [1,2] makes wireless sensor networks (WSN) [3] face great challenges in heterogeneous interconnection and network management. The introduction of software-defined networking (SDN) has brought the dawn to solve this problem [4,5]. Centralized control is one of the core feature of SDN. Constructing network global view is the basis task of control plane [6], where the sensor node location information is the priority among priorities. On the one hand, the valuable sensing information must be associated with the location, and which is an important guarantee of quality of service (QoS). On the other hand, with the paradigm of "sensing as a service", location information is a significant foundation for the distribution and deployment of sensing services [7].

In distributed WSN, the sensor nodes localization method is usually divided into two kinds of range-based and range-free technologies [8]. Note that the

M. Huang—This work is supported by Key Laboratory of Information Assurance Technology Open Fund under granted no. KJ-15-104.

S. Qing et al. (Eds.): ICICS 2017, LNCS 10631, pp. 276–287, 2018.
https://doi.org/10.1007/978-3-319-89500-0_25

localization in this paper refers to the planar positioning of sensor node itself. The range-based localization refers to achieve location by using certain means to measure the distance between nodes, which including received signal strength indicator (RSSI), signal transmission time or angle [9–11]. With ease of implementation and no additional hardware, the RSSI-based method becomes the preferred localization technology in WSN. The range-free positioning indicates some properties of sensor nodes are used to obtain location, such as neighbors or hops [12,13]. This approach reduces the localization cost by sacrificing positioning accuracy, and is generally applicable to large-scale networks. Among them, the most classic one is hop-based DV-Hop algorithm [14].

Although there are large divergences in the above two methods, the basic process is essentially the same. First, the blind node (the sensor node to be positioned) acquires the distance (expressed as RSSI or hops, etc.) with the anchor node (the reference node with known location) through the range-based or range-free methods. Then, the anchor node publishes its own location information as a reference to blind node. Finally, the blind node calculates the position through plane geometry relation.

However, the above procedure does not take into account the anchor node location and identity privacy, and it is a big security threaten. The malicious node can pretend to be the blind node to eavesdrop the location information of anchor node. As the next step, it can destroy the network positioning capabilities by targeted physical destruction or signal interference. In turn, the malicious node can affect the positioning accuracy and QoS by impersonating anchor node to publish the fictitious location information [15]. In addition, the transmission power and radius of sensor nodes are different in heterogeneous WSN, and the RSSI- or hop-based distance may have notable errors, so the node localization accuracy is confronted with great challenges [16].

As far as the authors know, there is no related research using SDN to solve the security location problem in WSN, and only [17,18] using SDN method to program the activation state of anchor nodes. Although the node localization accuracy and network energy consumption are well balanced, it is still belonging to distributed positioning with the privacy leak problem. In view of this, we propose a centralized security localization mechanism based on SDN for heterogeneous WSN. In which, the localization algorithm is run on the SDN controller, thus ensuring the security of sensitive information such as anchor node location and identity. In addition, in the distance calculation process, the positioning accuracy is greatly enhanced by considering the transmission power of heterogeneous sensor nodes. Relative to sensor nodes, many capabilities of SDN controller like energy, computing, storage, communication, etc., are generally considered unrestricted. Therefore, the mechanism can effectively reduce the sensor node positioning load.

The outline of the rest of this paper is organized as follows: Sect. 2 gives a general introduction to the secure localization model. And the corresponding algorithm is detailedly described in Sect. 3. Section 4 analyzes the security and performance of the mechanism. Experimental design and results analysis is elaborated in Sect. 5 and summed up in Sect. 6.

2 Secure Localization Model

According to SDN paradigm, a security localization model is designed for heterogeneous WSN, as shown in Fig. 1. The model is mainly divided into control plane and data plane, in which SDN controller realizes the logical control of sensor nodes through the control link (essentially belongs to southbound interface protocol, such as Sensor OpenFlow [4], etc.).

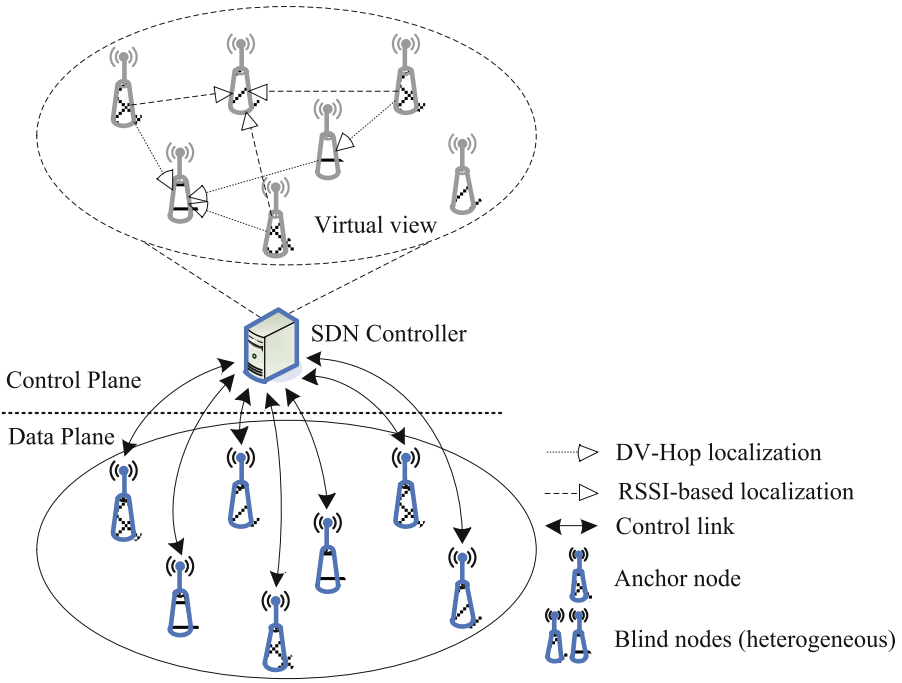


Fig. 1. Secure localization model

The data plane includes anchor and blind nodes. The anchor nodes can obtain its own position information by coordinates presetting or GPS positioning, so as to provide reference for the blind nodes. Considering heterogeneous factor, we design two classes of blind nodes. The same point is that they are sensor nodes to be located and can communicate with each other. And the difference between them is in the level of residual energy, communication radius and transmission power [19].

Limitations of space, we only designed a single controller, but can be extended to a logic unified control plane with multi-controllers. SDN controller is the key of security localization mechanism, the ultimate goal is to achieve the virtual view (part of the network global view) which all the sensor nodes are accurately positioned. It is necessary to illustrate that the position similarity between virtual view and data plane reflects the mechanism performance. At the same time,

the security embodied in the virtual view too. By using centralized localization instead of traditional distributed one, SDN controller can protect the sensitive information in positional process, thus effectively resisting multiple attacks from malicious node for location based services. In the choice of centralized positioning algorithm, considering the diversity of traditional location technology, we only select two popular algorithms from range-based and range-free classes respectively, namely RSSI-based and DV-Hop algorithms.

3 Secure Localization Algorithm

According to the above model, the secure location algorithm includes state acquisition and centralized positioning. Among them, the former is the basis of mechanism security, and the latter is the key to algorithm efficiency.

3.1 State Acquisition

After the network is deployed, SDN controller first constructs the quaternion $LT = \langle ID, GP, SP, NT \rangle$ with the status information related to the sensor node location in data plane through control link. Where ID stands for the sensor node identity, GP represents the node location information (the blind node is empty) in the form of plane coordinates, and SP indicates the node transmission power (dBm). In the end, $NT = (\langle ID, LS \rangle, \langle ID, LS \rangle, \cdots)$ is the node neighbor table as linked list, where LS means the link quality with neighbor node in the form of RSSI.

In order to facilitate the calculation, the LSs of heterogeneous sensor nodes are preprocessed. The wireless signal propagation model commonly used in WSN is log-normal distribution model [20]. In the model, SP has the positive correlation with LS, as shown in Eq. (1), where $P_L(d)$ is the path loss when distance is d.

$$P_L(d) = SP - LS \tag{1}$$

It can be seen that SDN controller can normalize all the LSs by the minimum transmit power (SP_{min}) among all the sensor nodes, as shown in Eq. (2), and the amended LS denoted as LS'.

$$LS' = LS - (SP - SP_{min}) \tag{2}$$

Therefore, the preprocessing process is as follows: SDN controller traverses the NT in LT, then fixes the LS using formula (2) and rewrites the LS' to the corresponding $\langle ID, LS \rangle$ in each loop.

3.2 Centralized Positioning

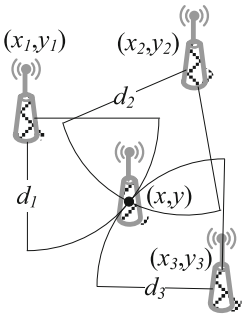
After completing the state acquisition phase, SDN controller begins to perform centralized positioning to build a virtual view that actually reflects the data plane location information. In general, the node communication radius is not

the same in heterogeneous WSN. In addition, there is a certain randomness with the node position by throwing deployment. Therefore, two types of positioning algorithm, namely RSSI-based and DV-Hop, shown in Fig. 2, with a view to the joint application to improve the positioning accuracy.

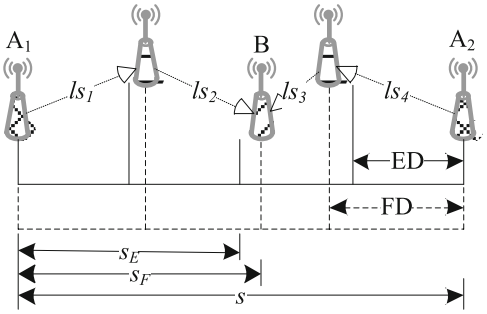
In Fig. 2, (a) is the RSSI-based localization algorithm, and three-or more anchor nodes can be used to calculate the location of blind nodes in the form of trajectory intersection, as shown in Eq. (3). Where the distance d is calculated using the log-normal distribution model [20]. Note that if the intersection located a small area, then the center of mass can be regarded as the final result. In general, this algorithm has high positioning accuracy and is well suited for dense areas of anchor nodes deployment (the more concentrated the anchor nodes, the higher the positioning accuracy).

$$\begin{cases} (x-x_1)^2+(y-y_1)^2=d_1^2 \\ (x-x_2)^2+(y-y_2)^2=d_2^2 \\ (x-x_3)^2+(y-y_3)^2=d_3^2 \end{cases} \tag{3}$$

(b) is the DV-Hop localization algorithm in the range-free class. Its main idea is taking the product of average estimated distance (ED) per hop and the number of hops as the final estimation distance between blind and anchor nodes. Thus,



(a) RSSI-based localization



(b) DV-Hop localization

Fig. 2. Localization algorithms

it can be used as a supplement to RSSI-based algorithm for the areas where the anchor nodes are sparser. In order to improve the positioning accuracy of DV-Hop, this paper adopts the fixed distance (FD) by RSSI replace of ED per hop. As shown in Fig. 2(b), the number of hops between the anchor nodes A_1 and A_2 is 4, the distance is s, and the number of hops between blind node B and A_1 or A_2 are 2, so the traditional DV-Hop algorithm estimates the distance from B to A_1 or A_2 are $s_E = s \times 2/4$. Obviously, the positioning error arises. Therefore, we use the ratio relation between LSs to correct each hop distance, and the distance between B and A_1 (S_F) is shown in Eq. (4). Similarly, the distance between B and A_2 can be calculated.

$$s_F = \frac{ls_1 + ls_2}{ls_1 + ls_2 + ls_3 + ls_4} \times s \tag{4}$$

The algorithm flow chart is shown in Fig. 3. Among them, "Build LT" and "Amend LS" belong to the state acquisition phase, "RSSI-based Localization" and "DV-Hop Localization" are implemented in the centralized positioning stage, and "Complete Virtual View" is the final result of the algorithm.

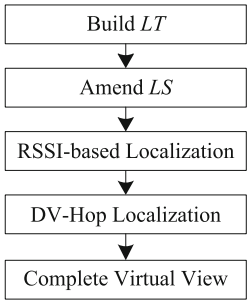


Fig. 3. Algorithm flow chart

4 Security and Performance Analysis

This section mainly analyzes the security and performance of the proposed algorithm. To our mind, the high security is the advantage, and the high performance is the prerequisite for our scheme.

4.1 Security Analysis

The design motivation of the security localization mechanism is to protect the anchor node location and identity privacy. Note that we assume that SDN controller with its control links is secure and sensor nodes can be effectively authenticated. On the basis of this, the algorithm adopts centralized positioning method. In the state acquisition stage, SDN controller treats all the nodes equally, avoiding the need for anchor nodes to broadcast their own location and identity in

the distributed positioning technology. Thus, the attacker cannot get through eavesdropping to obtain the anchor node location, but also difficult to locate the anchor node through traffic analysis attack, and then capture or tamper is not feasible too. In other words, the probability of discovery anchor node through eavesdropping or traffic analysis attacks is equal to the one that the random selection node among all the sensor nodes is an anchor node. In addition, the attacker disguised as an anchor node is bound to be recognized by SDN controller.

Obviously, due to the openness of WSN deployment with its wireless channel, the attackers can physically capture all the sensor nodes, but the attack cost is huge, the actual feasibility is not high. It is worth mentioning that this mechanism cannot resist certain attacks aimed at the transmission signal to increase the positioning error, such as the installation of obstacles to reduce the LS between the neighbors. Such attacks in the distributed positioning method is also difficult to withstand.

4.2 Performance Analysis

The algorithm performance mainly includes three aspects: storage, calculation and communication. However, there is very little demand for storage resources in the positioning process, so it is not to be considered.

Towards calculation overhead, distributed positioning mechanism (including RSSI-based and DV-Hop algorithms), the blind nodes are required to perform certain operations to calculate their own location information. In our algorithm, the anchor and blind nodes do not need to run any action, all the computational overhead are concentrated in the SDN controller. Typically, SDN controller runs on the resourceful server, and the computing power can be considered infinity. Therefore, the computational cost of secure localization mechanism is better than that of distributed positioning method.

Wireless communication is the largest energy source of sensor nodes [21], which has a large impact on the lifetime of WSN. Figure 2 is used as a reference to compare the communication overhead, as shown in Table 1.

Obviously, the centralized localization advantage is very obvious in the communication overhead. For (a) and (b), the security localization mechanism can save 25% and 40% of communication cost than distributed positioning method respectively. Note that this is an analysis within five or less nodes. Typically, the number of nodes in WSN is very large, for example, ZigBee network can

Table 1. Comparison of communication overhead

		(a) RSSI-based	(b) DV-Hop
Centralization	Anchor node	12 bits	8 bits
	Blind node	6 bits	4 bits
Distributed	Anchor node	6 bits	8 bits
	Blind node	18 bits	12 bits

accommodate up to 65535 nodes [22]. Therefore, the communication cost of distributed positioning method may have a great impact on the network energy consumption in a large-scaled network.

5 Experiments and Results

The experiment is based on SDN-WISE architecture [23] and COOJA simulator [24]. During the construction of network global view, SDN-WISE only considers the connection relation of sensor nodes, but doesn't take the location information into account. Therefore, this paper builds the virtual view by adding new security module in SDN controller.

5.1 Experimental Deployment

The experimental network is randomly deployed in the planar area of $200 \times 200\,\mathrm{m}^2$, and the node transmission radius is set to 50 m. The number of nodes is regard as independent variables, from 30 to 110 with increment is 20, to analyze the effect of network size on the performance of the localization algorithm. In addition, the ratio of anchor nodes is also as a variable, taking 10%, 30% and 50% respectively, to analyze the influence of the number of anchor nodes on the network positioning accuracy. Considering the difference of transmission power between heterogeneous sensor nodes, 60% node is set to 1.0 dBm, and the remaining 40% nodes is randomly set to −1.5 dBm or 4.5 dBm. To simplify the analysis, we assume the transmit power has no effect on the transmission distance (there are quadratic curve relationship in theory). In addition, the node initial power is set to 9×10^6 mC (approximately equal to the power of 2 AAA batteries). The parameter settings are shown in Table 2.

Table 2. Parameter settings

Parameters	Value
Deployment area	$200 \times 200\,\mathrm{m}^2$
Transmission radius	50 m
Initial power	9×10^6 mC
Number of nodes	From 30 to 110 with increment is 20
Anchor node ratio	10%, 30% and 50%
Transmission power	1.0 dBm (60%), −1.5 dBm (20%) and 4.5 dBm (20%)

5.2 Experimental Results

(1) Energy Consumption

The comparison of energy consumption in centralization and distributed positioning methods is shown in Fig. 4. In which, the X- and Y-axes are the number of

sensor nodes and network average residual energy respectively, the black polygonal line represents the proposed centralized positioning algorithm, and the blue one stand for the distributed positioning using DV-Hop Algorithm. In addition, the percentage data in explanatory text means the anchor node ratio.

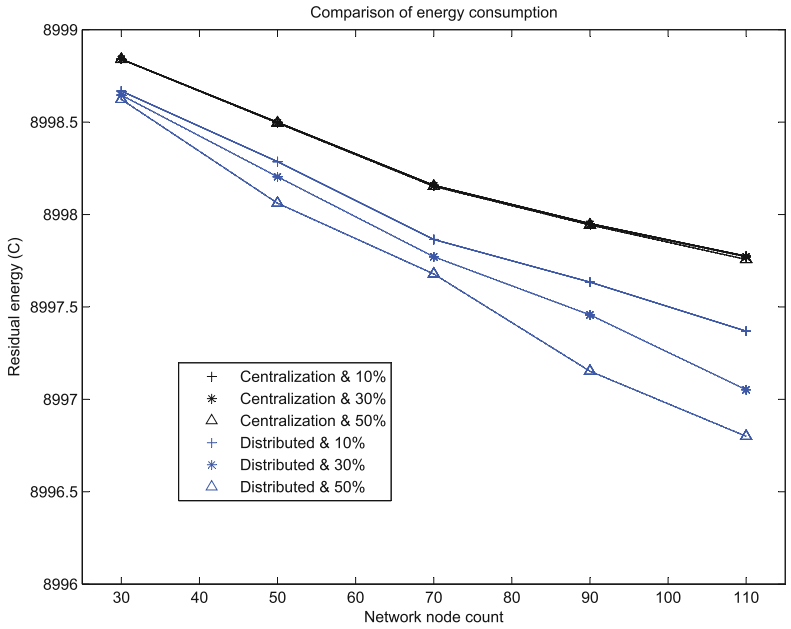


Fig. 4. Comparison of energy consumption (Color figure online)

It can be seen from Fig. 4 that the centralized localization algorithm is superior to the distributed one in energy consumption. With the increase in the number of network nodes, it is natural that the time and energy required for network positioning are correspondingly raised. However, the dissipation energy in the distributed method is relatively fast. In addition, with the increase in the proportion of anchor nodes, the energy consumption in centralized localization is only slightly increased, while the raise in distributed positioning is very obvious. The fundamental reason is that the energy consumption of our mechanism is mainly reflected in the state acquisition phase. At the same time, for all the nodes are treated equally by SDN controller, thus it is only need to transfer the location data of additional anchor nodes. On the contrary, DV-Hop algorithm will in the full use of the anchor nodes to improve the positioning accuracy, naturally wasting more network energy.

(2) Positioning Accuracy

In this paper, we take the concept of overall positioning accuracy, that is, the sum of all the location deviation distance divided by the product of network

node count and communication radius, recorded as P_a, as shown in Eq. (5). Note that the deviation distance of unsuccessful positioning node is the same as node transmission radius.

$$P_a = \frac{\sum |p, \tilde{p}|}{NR} \tag{5}$$

Where p and $\tilde{p}$ are the true and calculated node locations respectively, $|\bullet|$ denotes as the Euclidean distance, N represents the number of blind nodes, and R is the node transmission radius.

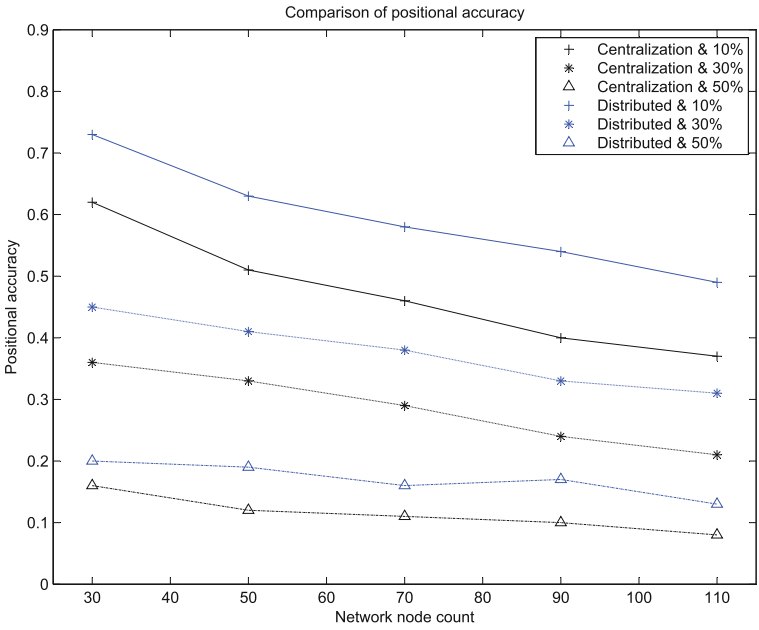


Fig. 5. Comparison of positioning accuracy

The positioning accuracy is shown in Fig. 5, and the drawing notes are the same as those shown in Fig. 4, which are no longer explained. Obviously, the security localization mechanism is better than the distributed positioning scheme, and the advantages are more prominent when the anchor nodes are deployed sparse. The reason is that this mechanism joint uses a variety of positioning algorithms (This paper enumerates only RSSI-based and DV-Hop methods). In the meantime, the transmission power is adopted to amend the link quality, and further applied to reduce the DV-Hop positioning error. In addition, as a whole, the more anchor node deployment, the higher the positioning accuracy, and when the proportion reaches 50%, the positioning error can be less than 0.1. Therefore, this scheme can effectively improve the positioning performance of heterogeneous WSN.

6 Summary

In the traditional distributed positioning method, the anchor node must broadcast its own location and identity information to assist the blind node positioning process. However, this approach makes the anchor node easily become the attack target, such as malicious nodes launching eavesdropping attacks to obtain anchor node location, and then can be implemented targeted manual capture or signal interference. To change this situation, we adopt SDN paradigm to transfer the distributed positioning process to SDN controller, so as to effectively protect the privacy information such as location and identity of anchor nodes. The above conclusions are verified by security analysis. In addition, after modifying the link quality of heterogeneous sensor nodes, SDN controller can improve the positioning accuracy of blind nodes by running the complementary range-based and range-free localization algorithms. Finally, based on the open source architecture SDN-WISE and COOJA simulation platform, we designed and implemented the verification experiment. The results show that the scheme has better energy efficiency and higher positioning accuracy than the traditional method.

References

1. Miorandi, D., Sicari, S., Pellegrini, F.D., Chlamtac, I.: Internet of things. Ad Hoc Netw. **10**, 1497–1516 (2012)
2. Capella, J.V., Campelo, J.C., Bonastre, A., Ors, R.: A reference model for monitoring IoT WSN-based applications. Sensors **16**, 1816–1836 (2016)
3. Ovsthus, K., Kristensen, L.M.: An industrial perspective on wireless sensor networks—a survey of requirements, protocols, and challenges. IEEE Commun. Surv. Tutor. **16**, 1391–1412 (2014)
4. Luo, T., Tan, H.P., Quek, T.Q.S.: Sensor OpenFlow: enabling software-defined wireless sensor networks. IEEE Commun. Lett. **16**, 1896–1899 (2012)
5. Caraguay, Á.L.V., Peral, A.B., López, L.I.B., Villalba, L.J.G.: SDN: evolution and opportunities in the development IoT applications. Int. J. Distrib. Sens. Netw. **2014**, 1–10 (2014)
6. Kreutz, D., Ramos, F.M.V., Verissimo, P.E., Rothenberg, C.E., Azodolmolky, S., Uhlig, S.: Software-defined networking: a comprehensive survey. Proc. IEEE **103**, 14–76 (2015)
7. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Sensing as a service model for smart cities supported by Internet of Things. Trans. ETT **25**, 81–93 (2014)
8. Han, G., Xu, H., Duong, T.Q., Jiang, J., Hara, T.: Localization algorithms of wireless sensor networks: a survey. Telecommun. Syst. **52**, 2419–2436 (2013)
9. Shao, J.F., Tian, W.Z.: Energy-efficient RSSI-based localization for wireless sensor networks. IEEE Commun. Lett. **18**, 973–976 (2014)
10. Shao, H.J., Zhang, X.P., Wang, Z.: Efficient closed-form algorithms for AOA based self-localization of sensor nodes using auxiliary variables. IEEE Trans. Signal Process. **62**, 2580–2594 (2014)
11. Go, S., Chong, J.: Improved TOA-based localization method with BS selection scheme for wireless sensor networks. ETRI J. **37**, 707–716 (2015)

12. Ma, D., Meng, J.E., Wang, B.: Analysis of hop-count-based source-to-destination distance estimation in wireless sensor networks with applications in localization. IEEE Trans. Veh. Technol. **59**, 2998–3011 (2010)
13. García-Otero, M., Población-Hernández, A.: Secure neighbor discovery in wireless sensor networks using range-free localization techniques. Int. J. Distrib. Sens. Netw. **2012**, 178–193 (2012)
14. Gui, L., Val, T., Wei, A., Dalce, R.: Improvement of range-free localization technology by a novel DV-Hop protocol in wireless sensor networks. Ad Hoc Netw. **24**, 55–73 (2015)
15. Li, P., Yu, X., Xu, H., Qian, J., Dong, L., Nie, H.: Research on secure localization model based on trust valuation in wireless sensor networks. Secur. Commun. Netw. **2017**, 1–12 (2017)
16. Assaf, A.E., Zaidi, S., Affes, S., Kandil, N.: Low-cost localization for multihop heterogeneous wireless sensor networks. IEEE Trans. Wirel. Commun. **15**, 472–484 (2016)
17. Zhu, Y., Zhang, Y., Xia, W., Shen, L.: A software-defined network based node selection algorithm in WSN localization. In: IEEE Vehicular Technology Conference, pp. 1–5. IEEE Press, New York (2016)
18. Zhu, Y., Yan, F., Zhang, Y., Zhang, R., Shen, L.: SDN-based anchor scheduling scheme for localization in heterogeneous WSNs. IEEE Commun. Lett. **21**, 1127–1130 (2017)
19. Liu, X., Evans, B.G., Moessner, K.: Energy-efficient sensor scheduling algorithm in cognitive radio networks employing heterogeneous sensors. IEEE Trans. Veh. Technol. **64**, 1243–1249 (2015)
20. Peng, R., Sichitiu, M.L.: Probabilistic localization for outdoor wireless sensor networks. ACM SIGMOBILE Mob. Comput. Commun. Rev. **11**, 53–64 (2007)
21. Anastasi, G., Conti, M., Francesco, M.D., Passarella, A.: Energy conservation in wireless sensor networks: a survey. Ad Hoc Netw. **7**, 537–568 (2009)
22. Gill, K., Yang, S.H., Yao, F., Lu, X.: A ZigBee-based home automation system. IEEE Trans. Consum. Electron. **55**, 422–430 (2009)
23. Galluccio, L., Milardo, S., Morabito, G., Palazzo, S.: SDN-WISE: design, prototyping and experimentation of a stateful SDN solution for WIreless SEnsor networks. In: 2015 IEEE Conference on Computer Communications, INFOCOM, pp. 513–521. IEEE Press, New York (2015)
24. Osterlind, F., Dunkels, A., Eriksson, J., Finne, N., Voigt, T.: Cross-level sensor network simulation with COOJA. In: 2006 IEEE Conference on Local Computer Networks, pp. 641–648. IEEE Press, New York (2006)