An Enhanced Security Measures of the source location among wireless sensor networks

[1]Dr. MD. Atheeq Sultan Ghori
Assistant Professor, CSE Dept., Telangana University, Nizamabad, India.

[2]P. Ila Chandana Kumari
Assoc. Professor, CSE Dept., Hyderabad Institute of Technology and Management, Hyderabad, India.

[3]Dr. M Naveen Kumar
System Administrator, Telangana University, Nizamabad, India.

[4]G. Chandra Sekhar
Asst.Professor, CSE Dept., Institute of Aeronautical Engineering, Hyderabad, India.

[5]Royyuru Srikanth
Assoc. Professor, CSE Dept., HMKS & MGS College of Engineering & Technology, Guntur, India.

Abstract— With the ongoing improvements of WSNs, computing and communication have encountered colossal headway. In the interim, security has not gotten a similar thoughtfulness regarding oblige such turns of events. In this paper, we center around the source location privacy issue in WSNs, a hot research theme in security, and propose probabilistic source location privacy (PSLP) insurance conspire for WSNs. An all the more impressive enemy, which can utilize hidden Markov model to assess the condition of the source, is considered in this investigation. To adapt to this sort of foe, apparition nodes and fake sources, which are mindful to mirror the conduct of the source, are used to expand the directing way. At that point, the heaviness of every hub is determined as a measure to choose the next-hop candidate. What's more, two transmission modes are intended to transmit genuine bundles. The reenactment results show that the proposed PSLP plot improves the wellbeing time without bargaining the vitality utilization.

Keyword: Wireless sensor networks, source location privacy, phantom node, fake source.

Introduction

WSNs comprise of various sensor nodes and conventions, which is the basis of administration like information authentication [1], event awareness [2], and hub charging [3]. These nodes play the job of microcomputer and are dispersed in various conditions. There are an ot of data transmissions and communication behaviors between nodes. Along these lines, it is essential to save the security [4].

Security of WSNs includes many aspects, for example, data privacy [5] and location privacy [6]. Data privacy can be ensured by encryption algorithms while location privacy cannot be secured to the outrageous. Because of the time correlation in data transmission between two nodes, the adversary can surmise location information through analysis. From a period correlation point of view, location privacy

comprises of the source location privacy and the sink location privacy. Given the importance of the source, in this paper, we center on the source location privacy, which is a developing research point in the field of security. There are many strategies, as secure routing [7], fake sources [8], phantom nodes [9], fake cloud [10], and group [11], that can be applied to ensure the source location privacy. We propose a probabilistic source location privacy insurance plot (PSLP), which adopts phantom nodes and fake sources for the reason that these two procedures can broaden the routing path. The means of PSLP are as per the following:

1) Phantom nodes are chosen around the source and the obvious area is taken into consideration.

2) A weight value, which is dynamically updated, is calculated in each hub to decide the next-hop candidate.

3) Fake sources are generated around the sink to send fake packets, all together confound the adversary.

In the above advances, the noticeable area is a special area. At the point when the adversary backtracks to this area, the source can be perceived immediately. Two sorts of packets exist in the transmission, which are the real packets and the fake packets. Real packets are generated by the source while fake packets are generated by fake sources. So as to shroud the source location, real packets sent by the source are first transmitted to a phantom hub through coordinated random walk. Here, thinking about the distance between the source and the sink, two transmission modes are taken into consideration and details will be given later. During the transmission of real packets, fake packets are also transmitted to the sink with a fixed period.

The proposed PSLP has shown a superior performance than two other ongoing plans in our simulations with regard to increasing the safety time while balancing the energy utilization.

The main commitments of this paper are:

1) Both phantom nodes and fake sources are integrated into the proposed PSLP, which enhance the source location privacy.

2) An all the more remarkable local adversary, which can utilize Hidden Markov Model to estimate the state of the source, is taken into consideration.

3) Two data transmission modes are structured based on the distance between the source and the sink, which further enhance the source location privacy.

Related Work

Many researchers have paid attention to the location privacy since Ozturk first proposed his idea [12]. As of late, location privacy has been generally researched in industrial wireless sensor networks [13], vehicular ad-hoc networks [14], cloud computing [15], and social network [16] and so on.

Location privacy covers the source location privacy and the sink location privacy. In this paper, we center on the source location privacy assurance. Manjula et al. utilized virtual sources to ensure the source location privacy [17]. In their plan, a routing procedure was proposed to maximize the safety time. By adding random walk into the routing procedure, nodes in non-hotspot areas participated in the establishment of multiple routing paths. Subsequently, the safety time increased without impacting the network lifetime.

Matthew et al. proposed two algorithms utilizing fake sources to ensure the source location privacy [8]. In the primary algorithm, fake sources were dynamically sent around the sink. At that point, the sink utilized flooding to choose fake sources. This algorithm can give a decent source location privacy to the detriment of the gigantic energy utilization. To adapt to this, another algorithm called dynamic single path routing algorithm (DynamicSPR) was proposed. By utilizing coordinated randomwalk, nodes away from the source were chosen as fake sources, which significantly diminished the energy utilization. Nonetheless, fake sources were related to the relative location of the source and the sink, sensor nodes in a particular area may exhaust energy.

Jing et al. considered an all the more impressive adversary and proposed a privacy enhancing routing algorithm to ensure location privacy [18]. In their research, a global adversary utilizing Bayesian maximum-a-posteriori (MAP) estimation strategy attempted to screen the communication between nodes. At that point, a dynamic framework was advanced to decrease the adversary's discovery probability. Finally, the problem was changed over into the adjustment of parameters.

Huang et al. concentrated on the energy utilization rate in WSNs while maintaining the source location privacy [19]. They proposed a redundancy branch-based source location privacy plot. In their plan, many redundancy branches were generated from the source to the sink. The quantity of branches was controlled by the energy gathered by nodes. In addition, these branches were combined into several routing paths later. Be that as it may, the quantity of joined routing paths was not clearly characterized and the energy gathered by nodes around the sink may be not exactly the energy cost by transmitting packets.

Chen et al. in [20] proposed a constrained randomwalk mechanism. In their mechanism, a next-hop candidate determination domain was generated based on the balance angle of current hub's neighbors and the danger distance, which made the choice domain resemble a circle. At that point, the heaviness of each hub in the domain was calculated by the ratio between a present hub's counterbalanced angle and the whole of total balance angle. The smaller the ratio, the higher the probability that this hub became the nexthop candidate. In any case, the balance angle of a nodewas fixed, and thereby the weight probably won't change. In this way, nodes which acted as the next-hop candidate would devour a lot of energy. Chen et al. used phantom nodes and proposed a constrained flooding algorithm to ensure the source location privacy [9].

Li et al. in proposed a plan utilizing random intermediate nodes and ring to secure the source location privacy. To start with, the authors acquainted the criteria with quantitatively measure the source location information leakage. At that point, to lessen the leakage probability, random intermediate nodes were added to make the routing path scatter. Packets were first transmitted to an intermediate hub and then forwarded to a hub in ring around the sink. Packets were directed on the ring for a random hop and then sent to the sink.

Mutalemwa et al. partitioned the entire network into areas and proposed a plan based on district transmission [22]. In this plan, the sink was located in the focal point of the network and locales were generated around the sink. The transmission between areas was actualized by a lot of relay nodes which were chosen strategically. These strategic relay nodes took up two districts and were liable for forwarding packets to the sink. Be that as it may, the dispersion of these nodes was near the sink. Relaying an excessive number of packets

would expend a great deal of energy. Thereby, the average energy proficiency was not high.

Wang et al. considered the source location privacy against another kind of adversary in [23]. The adversary model had two properties, global and local. Under normal circumstances, the adversary was a local adversary. At the point when a potential area where the source may stay was located, the adversary became a global adversary in this area. To adapt to it, a message mapping sharing strategy was introduced and a cloud containing many sham packets was created around the source to shroud the location. Each message duplicate was transmitted by random routing, which gave adequate source location privacy.

Problem Definition

Since the introduction of the source hub location in WSN inevitably threatens the security of the observed target, the source hub location privacy insurance turns into a critical issue to be understood. In any case, since the computational capability, storage capacity and energy resources of sensor nodes are constrained, the balance among security and network performance turns into an inevitable necessity.

The current researches on source hub location privacy insurance are mainly based on cyclic entrapment [11], sham data sources [6,7,12,13] and phantom routing [6,7,16]. Ouyang et al. [11] presented the cyclic entrapment idea as a special case of sham data source routing. In cyclic entrapment, multiple nodes act as sham data sources, and interconnect to frame a circle. The main aim of cyclic entrapment is to mistake adversary for these circles during a hop-by-hop-trace attack, thereby preventing the attacker from returning to the real source hub. Be that as it may, such a strategy needs to activate at least one circles to confine the attacker, and the nodes insider savvy which act as the fake data source need to generate sham data periodically, which causes a large amount of abnormal communication overhead, brings about energy opening [19] and damages the network performance genuinely.

Network Model

The network model in this investigation is based on the typical Panda-Hunter model [12]. As appeared in Fig. 1, a WSN which is made out of many sensor nodes is deployed to screen the activities of pandas. When a sensor hub distinguishes a panda, it turns into the source and sends packets to the sink through multiple hops. The pith of privacy security is diminishing the probability that the adversary finds the source location. In this manner, we make the accompanying assumptions:

1) Sensor nodes are randomly deployed. After being deployed, the location of each sensor hub remains unchanged. What's increasingly, all sensor nodes are homogenous, which means that they have the same initial energy, the same computing ability, and the same cache memory.

2) Routing is based on the weight. Each sensor hub is assigned a weight that is updated regularly. The weight here speaks to the probability that this hub is chosen as the next hop, or it very well may be comprehended as the inclination in choosing the next hop hub, which is related to the residual energy, the communication quality, and the hop count to the sink. Details of this weight will be given later.

3) Only one sink exists in the network. As in different plans or conventions [12], [15], the sink remains in the network community.

4) Each sensor hub has information on its own adjacent neighbors. Packets sent by each sensor hub are scrambled with an encryption algorithm. Notwithstanding, this part is past the extent of this examination.

Adversary Model

Because of the potential value of the source, the adversary starts from the sink and attempts his/her best to discover the source location. The observing range of the adversary equals to a sensor hub's radius, which means that the sort of the adversary is a local adversary. The local adversary has a restricted checking range, which is equal to or somewhat larger than the communication range of a typical hub. Accordingly, the local adversary can just screen parts of the network. Usually, the adversary performs passive attacks, for example, eavesdropping and backtracking, to avoid being found by the network administrator.

We think about an all the more impressive adversary in this paper. Apart from the passive attack, we assume that the adversary realizes the packet type by checking the header of each packet. At that point, the adversary can utilize the Hidden Markov Model (HMM) to induce the conceivable state of the source for a given time based on its observation. The goal of utilizing HMM to derive the conceivable state of the source is that, comparing with wandering in the network, it is increasingly viable for the adversary to discover the source location from the estimation consequence of HMM. This is because the estimation of HMM can enable the adversary to lessen the extent of finding the source.

Be that as it may, thusly the adversary just knows the source's state, not the source's location. What we consider here is that if the adversary has enough information about the network, he has a higher probability to discover the source from the estimated source state. In our proposed PSLP, the key idea is to make real packets and fake packets to be transmitted from various bearings with various states, which attracts the adversary's attention and lessens the accuracy of the estimate.

Implementation of PSLP

In this segment, a detailed depiction of PSLP is given. In the initialization procedure, the beacon message is periodically broadcasted by the sink to sensor nodes. At the point when a hub gets the message, it records the hop count put away in it, increases the hop count by one, repackages the packet, and sends to its neighbors. Each hub just records the base hop count. Therefore, all nodes realize their hop count to the sink and their neighbors. Since the adversary may know the state of the source at a given time while the location of the source is as yet obscure, we mean to increase the potential locations of the source. PSLP contains three stages: the initial step is the determination of phantom nodes; the subsequent advance is the determination of fake sources; the third step is the routing from the source to the sink. A diagram of PSLP is appeared in Figure.

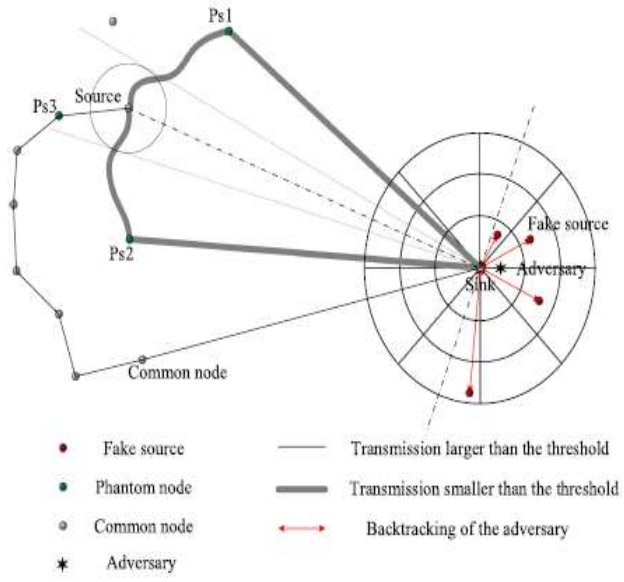

Fig: Proposed Implementation model

As referenced in the adversary model, the adversary can utilize HMM to estimate the state of the source and then perform targeted search. What we have to do is to increase increasingly potential states of the source. Phantom nodes and fake sources superbly match our

requirements. Although the capacity of the phantom hub and the fake source is similar, however the meaning of the two is extraordinary. The phantom hub alludes to nodes around or nearby the source, which simulate the capacity of the source. The fake source also alludes to nodes which simulate the capacity of the source. Be that as it may, the location of fake source is around the sink, which is far from the source. The motivation of consolidating the phantom hub and the fake source together is to create the diversification of the transmission headings. Both phantom nodes and fake sources are chosen in non-hotspot area, which has little effect on the network lifetime.

Determination of Phantom Nodes

As referenced previously, phantom nodes are nodes deployed around the source to simulate the capacity of the source. Thinking about the capacity of phantom nodes, we can see that the more extended the distance between a phantom hub and the source, the more grounded the privacy insurance is. The main reason for this arrangement is to coordinate the adversary away from the real source. Notwithstanding, authors in [17] have demonstrated the probability that a phantom hub stays inside 20% ofH hops from the source is 1−e−H/25. Therefore, we choose to utilize guided random walk to choose phantom nodes. In coordinated random walk, packets are transmitted a fixed way. Consequently, when coordinated random walk stops, the chose phantom hub stays away from the source.

For additional details, when the source appears, it sends packets to one of its neighbors inside H hops via coordinated random walk. At that point, the neighbor sends packets to a hub in its far neighbor rundown and decreases H by one. At the point when H gets zero, the present hub changes into a phantom hub and forwards packets sent by the source. The phantom hub changes during each data transmission.

In addition, the phantom hub must stay outside the obvious area (hover around the source). Because when the adversary backtracks to the obvious area, it perceives the source immediately. Besides, the source sends packets to the phantom hub once during the initialization. Thus, the transmission between the source and the phantom hub is assumed to be safe. Noticed that the determination of phantom nodes relates to the distance between the source and the sink, which will be introduced later.

Determination of Fake Sources

As portrayed in past definition, fake sources are generated around the sink to increase headings from where packets come. The sending range of a fake source is determined by angle θ2 in Fig. 3. Above all else, the sink separates the network into several rings. At that point, these rings are separated into n divisions. For separating fake sources and the source, fake sources are just chosen in the correct part of the line which is perpendicular to the line connecting the source and the sink. The quantity of fake sources is controlled by the actual application. At the initialization, the fake source arrangement is generated.

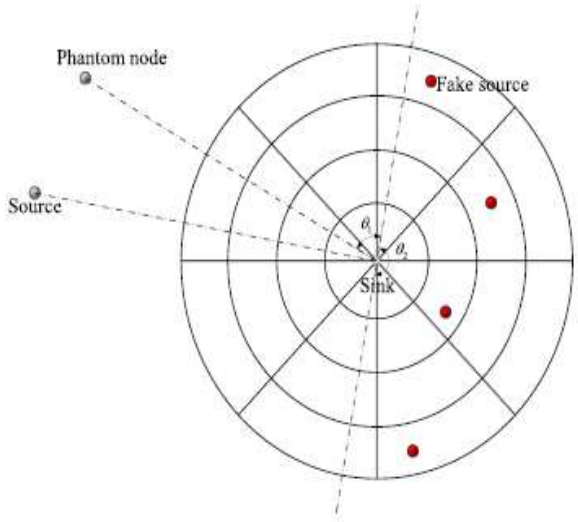

Fig3: Ring areas around the sink.

Each fake source is preferably to stay in various sectors, which guarantees that the heading of each fake packet is unique. Since the adversary realizes the source state in a particular time, it needs to analyze the packet stream to discover the source. Therefore, by adopting fake sources to enhance the source location, source location privacy is secured. A hub acts as a fake source for a fixed period. At the point when the timespan exhausts, another fake source appears. So as to alleviate the energy utilization of fake sources, we assume that there just exists one fake source for a certain timeframe.

The Routing From the Source to the Sink

After the determination of phantom nodes and fake sources, the next advance is the transmission between the real source and the sink. The source transmits a message to advise the sink when it appears. Then, the sink chooses a fake source immediately after getting this message. Taking into account that the source randomly appears, there exists a likelihood that distance between the source and the sink is small. In this way, in light of this situation, we set a limit between the source and the sink.

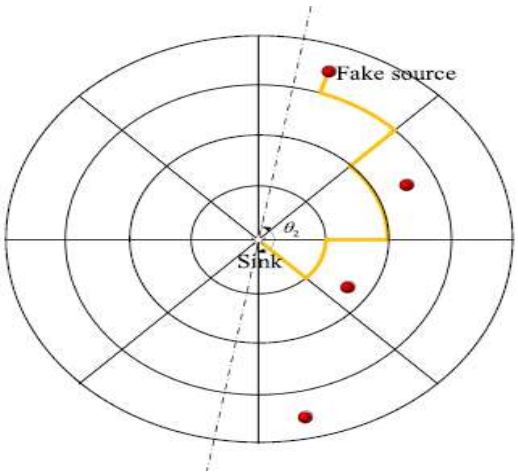

Fig4: Possible transmission of fake packets

Thereby, the routing procedure from the source to the sink contains two scenarios. The principal case is that the hop count between the source and the sink is larger than the edge. The subsequent case is that the hop count between the source and the sink is smaller than the edge. In general, as the source initially sends packets to a phantom hub, the main contrasts lie in the choice of phantom nodes and the transmission from the phantom hub to the sink.

Performance Evaluation

In this area, we evaluate the performance of PSLP. All the outcomes gave in this area are the average values of the experimental data.

In this area, four measurements are evaluated in the simulation, namely, the safety time, the energy utilization, the network lifetime, and the transmission delay. As a matter of first importance, we give the meaning of each measurement. The safety time is the distinction between when the source sends the primary packet and when the adversary finds the source's location. To be increasingly explicit, we utilize the hop count of backtracking taken by the adversary to speak to the safety time. The energy utilization speaks to the average energy cost per simulation run. As control

packets just take up next to no energy, so we disregard this part and mainly center on the energy utilization during packets transmission.

The network lifetime alludes to the time distinction between the network establishment and the death of the primary hub. The transmission delay means the average packet transmission and the data preparing time per simulation run.

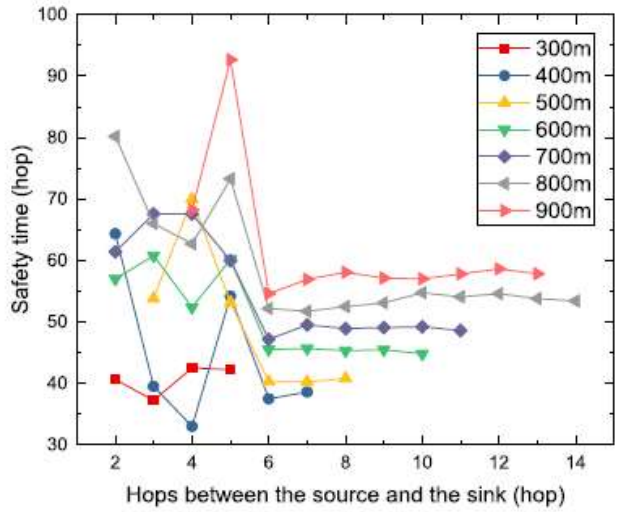

Fig5: Safety time versus various hops between the source and the sink.

PSLP is compared with two other schemes, which are the dynamic single path routing algorithm (DynamicSPR) [8] and the enhanced protocol for source location protection (SLP-E) [9]. DynamicSPR utilizes fake sources to secure the source location, while the SLP-E adopts phantom nodes to execute this. These two strategies are integrated in PSLP. Therefore, we pick DynamicSPR and SLP-E for the comparison.

Conclusion

Considering security in WSNs became increasingly important during the last decade. In this paper, we concentrated on the source location privacy, a research hotspot in security, and proposed a probabilistic source location privacy protection scheme (PSLP) based on WSNs. A ground-breaking adversary which use HMM is considered in this investigation. To adapt to it, phantom nodes, fake sources, and weight are adopted to change the packets' transmission headings. Thinking about the distance between the source and the sink, two sorts of routing modes are planned. Compared with DynamicSPR and SLPE, the simulation results demonstrate that the proposed PSLP achieves a high safety time and balances the energy utilization of each hub. Future examinations will concentrate on ensuring the source location by lessening the adversary's monitoring probability and secure communication among nodes.

References

[1] H. Lu and J. Li, “Privacy-preserving authentication schemes for vehicular ad hoc networks: A survey,” *Wireless Commun. Mobile Comput.*, vol. 16, no. 6, pp. 643–655, Apr. 2016.

[2] G. Han, X. Yang, L. Liu, S. Chan, and W. Zhang, “A coverage-aware hierarchical charging algorithm inwireless rechargeable sensor networks,” *IEEE Netw. Mag.*, to be published.

[3] G. Han, H. Guan, J. Wu, S. Chan, L. Shu, and W. Zhang, “An uneven cluster-based mobile charging algorithm for wireless rechargeable sensor networks,” *IEEE Syst. J.*, to be published.

[4] G. Han, H. Wang, J. Jiang, W. Zhang, and S. Chan, “CASLP: A confused arc-based source location privacy protection scheme in WSNs for IoT,” *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 42–47, Sep. 2018.

[5] H. Lu, J. Li, and M. Guizani, “Secure and efficient data transmission for cluster-based wireless sensor networks,” *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 750–761, Mar. 2014.

[6] G. Han, L. Zhou, H. Wang, W. Zhang, and S. Chan, “A source location protection protocol based on dynamic routing in WSNs for social

internet of things," *Future Gener. Comput. Syst.*, vol. 82, no. 5, pp. 689–697, Aug. 2018.
[7] H. Lu, J. Li, and H. Kameda, "A secure routing protocol for cluster-based wireless sensor networks using ID-based digital signature," in *Proc. IEEE Global Commun. Conf.*, Dec. 2010, pp. 1–5.
[8] M. Bradbury, A. Jhumka, and M. Leeke, "Hybrid online protocols for source location privacy in wireless sensor networks," *J. Parallel Distrib. Comput.*, vol. 115, pp. 67–81, May 2018.
[9] J. Chen, Z. Lin, Y. Hu, and B.Wang, "Hiding the source based on limited flooding for sensor networks," *Sensors*, vol. 15, no. 11, pp. 29129–29148, Nov. 2015.
[10] G. Han, X. Miao, H.Wang, M. Guizani, andW. Zhang, "CPSLP: A cloudbased scheme for protecting source-location privacy in wireless sensor networks using multi-sinks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2739–2750, Jan. 2019.
[11] G. Han, H.Wang, M. Guizani, S. Chan, andW. Zhang, "KCLP: Ak-means cluster-based location privacy protection scheme inWSNs for IoT," *IEEE Wireless Commun. Mag.*, vol. 25, no. 6, pp. 84–90, Dec. 2018.
[12] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energyconstrained sensor network routing," in *Proc. ACM Workshop Secur. Ad Hoc Sensor Netw.*, Jan. 2004, pp. 88–93.
[13] J. Wang, R. Zhu, S. Liu, and Z. Cai, "Node location privacy protection based on differentially private grids in industrial wireless sensor networks," *Sensors*, vol. 18, no. 2, pp. 410–425, Jan. 2018.
[14] A. Boualouache, S. Senouci, and S.Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Commun. Surv. Tut.*, vol. 20, no. 1, pp. 770–790, Jan.–Mar. 2018.
[15] Y. Gong, C. Zhang, Y. Fang, and J. Sun, "Protecting location privacy for task allocation in ad hoc mobile cloud computing," *IEEE Trans. Emerg. Topics Comput.*, vol. 6, no. 1, pp. 110–121, Mar. 2018.
[16] J. Du, C. Jiang, K. Chen, Y. Ren, and H. V. Poor, "Community-structured evolutionary game for privacy protection in social networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 3, pp. 574–589, Mar. 2018.
[17] R. Manjula and D. Raja, "A novel source location privacy preservation technique to achieve enhanced privacy and network lifetime in WSNs," *Pervasive Mobile Comput.*, vol. 44, pp. 58–73, Feb. 2018.
[18] J. Koh, D. Leong, G. Peters, I. Nevat, and W. Wong, "Optimal privacypreserving probabilistic routing for wireless network," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 9, pp. 2105–2114, Sep. 2017.
[19] C. Huang, M. Ma, Y. Liu, and A. Liu, "Preserving source location privacy for energy harvesting WSNs," *Sensors*, vol. 17, no. 4, pp. 724–755, Mar. 2017.
[20] W. Chen, M. Zhang, G. Hu, X. Tang, and A. Sangaiah, "Constrained random routing mechanism for source privacy protection in WSNs," *IEEE Access*, vol. 5, pp. 23171–23181, 2017.