Deconstructing Source Location Privacy-aware Routing Protocols

Arshad Jhumka
Department of Computer Science
University of Warwick, Coventry
United Kingdom, CV4 7AL
H.A.Jhumka@warwick.ac.uk

Matthew Bradbury
Department of Computer Science
University of Warwick, Coventry
United Kingdom, CV4 7AL
M.Bradbury@warwick.ac.uk

ABSTRACT

Source location privacy (SLP) is becoming an important property for a large class of security-critical wireless sensor network applications such as monitoring and tracking. Much of the previous work on SLP have focused on the development of various protocols to enhance the level of SLP imparted to the network, under various attacker models and other conditions. Others works have focused on analysing the level of SLP being imparted by a specific protocol.

In this paper, we focus on deconstructing routing-based SLP protocols to enable a better understanding of their structure. We argue that the SLP-aware routing protocols can be classified into two main categories, namely (i) spatial and (ii) temporal. Based on this, we show that there are three important components, namely (i) decoy selection, (ii) use and routing of control messages and (iii) use and routing of decoy messages. The decoy selection technique imparts the spatial or temporal property of SLP-aware routing. We show the viability of the framework through the construction of well-known SLP-aware routing protocols using the identified components.

CCS Concepts

•**Networks** → **Sensor networks; Network privacy and anonymity;** •**Security and privacy** → *Mobile and wireless security;*

Keywords

Source Location Privacy, Wireless Sensor Networks, Routing, Decomposition, Components, Spatial, Temporal.

1. INTRODUCTION

With the increasing popularity of wireless sensor networks (WSNs) to support novel monitoring and tracking applications, source location privacy (SLP) is becoming an important property that needs to be guaranteed by the WSN. However, providing SLP in wireless sensor networks presents a difficult challenge due to their potential to expose important information about the environment that they exist in, due to the broadcast nature of wireless communications. As messages are broadcasted, they can be eavesdropped by a malicious attacker. Even if encryption is used to protect the *content* of a message the *context* of the broadcast is still exposed for a malicious eavesdropper to take advantage of. In the case of SLP, the context that needs to be kept confidential is the location of the source node, which is closely related to the actual location of a physical asset. SLP is important in, for example, military applications, where locations of military personnel need to be kept secret.

SLP was initially introduced in terms of the panda-hunter game [16] where a WSN has been deployed across a large area to monitor pandas in their natural habitat. Using a directional antenna, it was shown that an attacker could identify the location of the immediate source of a message and, using this information, trace messages back through the system and find the ultimate source of the messages and thus the panda (or other asset). SLP protection schemes aim to protect against this scenario though various techniques. Many techniques centre around increasing the time an attacker would take to capture the source by *altering the routing protocol*.

There has been much work on routing-based SLP [3, 18], with many new techniques having been developed, and with the performance typically being evaluated through large-scale simulations. There are also several works that have developed models to analyse the privacy provided by their technique or protocol. However, these models tend to be specific to the type or nature of the technique. However, since most of the work on SLP have focused on altering the basic routing protocols to provide SLP, the focus of this paper is to identify whether there exists a basis set of components that support such protocol transformation. Such deconstruction will enable to (i) develop more efficient routing-based SLP protocols by refining specific components, (ii) create a formal model of each component and reason about the correctness of the overall protocol and (iii) provide a basis for comparing various SLP-aware routing protocols.

To this end, the contributions of this paper are:

- We argue that there exists two types of SLP-aware routing protocols for WSNs, namely (i) spatial and (ii) temporal.
- We provide *three* components, namely (i) decoy selection, (ii) use and routing of control messages and (iii)

SAC 2017, April 03 - 07, 2017, Marrakech, Morocco

ISBN 978-1-4503-4486-9/17/04…$15.00

DOI: http://dx.doi.org/10.1145/3019612.3019655

use and routing of decoy messages, that make the basis of an SLP-aware routing protocol, over the basic routing protocol for application messages.

- Through a series of examples of well-known SLP-aware routing protocols, we show how these protocols can be constructed using our proposed components, showing the viability of our framework.

The rest of the paper is structured as follows: in Section 2 we review some related work focusing on the relevant routing protocols. Section 3 contains the models we use and assume in this work. The deconstruction of the routing-based SLP algorithm is performed in Section 4 and examples are provided in Section 5. Finally, we conclude in Section 6.

2. RELATED WORK

Since the seminal work [16] there have been a variety of techniques developed to provide SLP in different situations against attackers of varying strengths [3, 9]. As this work focuses on exploring providing SLP at the routing layer, we will first provide a review of routing solutions before covering techniques that fall outside this area.

Phantom Routing, introduced in the seminal work, is a two-stage SLP protocol where (i) a directed random walk is performed away from the source to a *phantom* node and then, (ii) the phantom node routes the application message to the sink. The phantom node is the diversionary node an attacker should be lured to before the source, increasing the time-to-capture. It was initially defined with two variants, one where the second stage uses flooding [16] and another where the second stage uses single-path routing to reach the sink [8]. However, there have been many variations since such as GROW [24] which uses a bloom filter to prevent the walk doubling back on itself, techniques that allocate the phantom node in a specific area whilst avoiding direction information leakage [11] and angle-based techniques [21, 23] which calculate angles between certain nodes to influence the direction of the walk. Other techniques have adapted the random walk such that it forms a ring around the source and messages are routed through the ring before being forwarded onwards to the source [10, 25].

Another technique has been to use *fake sources*, which are nodes in the network that broadcast messages encrypted and padded to be indistinguishable from normal messages from the source. Fake source techniques aim to provide SLP by generating fake messages that lead to attackers being lured towards the fake source rather than the real source. There have been several implementations [6, 7, 8, 22] with the selection of the location of fake sources and the parametrisation having important impacts on the performance of the techniques. Recent work has focused on dynamically determine good parameters to use online [2]. A criticism of fake source is that they tend to be more energy intensive compared to other routing-based approaches.

Other techniques consist of a hybrid between generating fake messages and having messages modify their routing path. One example is tree-based diversionary routing [12] which imposes a tree structure on the network and then routes fake messages through the tree. The idea of fogs or clouds [4, 13] is also similar where a normal message is routed round a group of nodes called a fog and then onwards to other fogs. Fake messages are also used to provide additional privacy.

Other techniques to provide SLP against local attackers include using space in MAC beacon frames to disseminate messages from the source to other areas in the network before being routed to the sink [19].

Privacy against attackers with a global view of the network tends to be very different to defending against attackers with a local view. Periodic is one such algorithm that provides global SLP by having all nodes broadcast periodically, even if there is no protocol message to send [14]. Improvements have been made to this kind of technique by a variety of methods such as; sending messages according to a statistical model [20], optimisations based on clustering [15] and other traffic decorrelation techniques [17].

Of the most interesting to this work is the routing-based technique called Source Simulation [14], where optimal global SLP is traded in for improvements in energy efficiency. This is done by creating traces though the network that mimic the movement of real sources.

3. SYSTEM MODEL

In this section, we present the models we assume in this paper.

3.1 Network Model

A wireless sensor node is a device with a unique identifier that has limited computational capabilities and is equipped with a radio transmitter for communication. A WSN is a set of wireless sensor nodes with communication links between pairs of nodes. We consider a sensor network to be a graph $G = (V, E)$ where V represents the set of nodes and E the set of links between the nodes. When a link exists between two nodes m, n, then m and n can directly communicate with each other and are called neighbours.

There exists a distinguished node in the network called a *sink*, which is responsible for collecting data and which acts as a link between the WSN and the external world. Other nodes sense data and then route the data attached to protocol messages along a computed route to the sink for collection. We assume that any node can be a data source. We assume that the network is event-triggered, i.e., when a node senses an object, it starts sending messages periodically to the sink for a certain amount of time.

We assume the messages sent are encrypted and that the source node(s) includes its ID in the encrypted messages. Using the ID, the sink can infer an asset's location as we assume the network administrators will record where they put nodes. We do not assume that WSN nodes have access to GPS due to the resulting increase in energy cost. The type of encryption, be it end-to-end or pairwise is left undefined.

3.2 Privacy Model

The overall objective of any WSN-based SLP solution is to ensure that the asset (at a given location) is never captured through information leaked by the WSN. However, we make two observations:

1. If the asset is static, then the attacker can perform an exhaustive search of the network to find the asset. In this case, the SLP problem becomes irrelevant. Specifically, if there exists no time bound on the capture time, then an exhaustive search is a trivial solution, yet effective solution.

2. On the other hand, if the asset is mobile, then performing an exhaustive search of the network is unsuitable, as the attacker may hone in on a given location only to find out that the asset has moved. Thus, the SLP problem can only be considered when it is time-bounded, capturing the maximum amount of time there mobile asset will spend at a given location.

This notion of time bound has been termed as *safety period* in the literature. There are two alternative definitions of safety period: The first, used primarily by routing-based techniques, e.g. [8], is where the safety period is defined as the time required to capture the asset. The aim of these techniques is to maximise the safety period, i.e., the higher the time to capture, the higher the SLP level provided.

The second notion of safety period is used where it is desirable to bound the amount of time SLP is being considered for, i.e., if an attacker fails to capture a source within the specified safety period, then we say SLP has been provided. That notion of safety period intuitively captures the maximum time an asset will be at a given location before its next movement. Often, this can be obtained from previous data gathering to know more about such mobile assets.

This second notion of safety period is more generic that the first one in that, rather than attempting to maximise the amount of time an asset isn't captured (as under the first definition), the second definition captures the fact that the asset can't be reached before a certain time limit, i.e., setting the time limit to be ∞ in the second instance results in the first definition.

Thus, in this paper, we use the time bound model of safety period.

3.3 Attacker Model

It was shown in [1] that the strength of a WSN attacker can be factored along two dimensions, namely (i) presence and (ii) actions. Presence may, for example, be local while actions can be eavesdropping, crash or reprogramming among others. In this paper, we assume a *distributed eavesdropper* attacker. We chose a distributed attacker as the attacker can move around the network, gathering further information and the only action that he can perform is eavesdropping. Though being a weak attacker model, an attacker with a stronger set of actions will likely interfere with its stated objective of capturing the asset. For example, if the attacker attempts to jam signals at a given location, then the attacker cannot progress within the network to reach the asset within the specified safety period.

We assume the distributed eavesdropper to be initially located at the sink, since he is guaranteed to detect the arrival of a message at that location. Wherever the attacker is located, upon receiving (i.e., overhearing) the *first* new message at that location, the attacker moves to the neighbour who relayed the message. The reason to focus on the first new message is that the message has, with high probability, travelled along the shortest path from the source to the sink. To achieve this, we assume that the attacker has sufficient capabilities to determine the direction in which he receives the message, although the range of its detection is assumed to be limited and does not extend to the entire network. Thus, when the attacker hears a new message, it makes a step towards the source. This process can be repeated a number of times until the attacker reaches the source node, whereby it captures the asset. Such a routing protocol that provides little protection to the source location is called a *protectionless* routing protocol.

4. DECONSTRUCTING SLP-AWARE ROUTING PROTOCOLS

In this section, we explain the main components required in transforming a routing protocol for wireless sensor networks into one which is SLP-aware.

The problem of developing a SLP-aware routing protocol for WSN is that the routing protocol needs to satisfy two requirements: (i) data from sensor nodes need to be routed to the sink - this type of routing is called convergecast, and (ii) an eavesdropping attacker cannot trace the source within the safety period. The first requirement rules out trivial routing protocols that are not convergecast while the second one requires the routing protocol to enforce SLP. A typical approach has been to *transform* the original convergecast routing protocol, denoted by R, into an SLP-aware one, denoted by R^s. Invariably, to mask the actual location of the source at the routing level, the network traffic is re-engineered such that the attacker is delayed on its way to the source. The delay is proportional to the safety period.

There are two ways in which this delay can be imparted: (i) *spatially*, where the attacker takes a *longer* path to reach the source, or (ii) *temporally*, where the attacker is *slowed down* on his path. For the spatial delay, the attacker normally visits a higher number of nodes than what it would have under R, while under R^s, the attacker may visit the same number of nodes but the information required for the attacker to move is not made readily available. In either case, the attacker is made to "deterministically" follow a path that he believes will lead him to the asset within the safety period. In reality, the SLP-aware routing protocols lead the attacker down paths that will delay him. On such paths, one or more nodes with specific roles are known as *decoys*. Thus, the main transformation of a normal routing protocol into a corresponding SLP-aware one is through the use of decoys. However, several components are required to enable the WSN to properly use the decoys.

4.1 Component 1: Selection of Decoys

The selection of decoys is an ongoing process while application messages are being sent to the sink. These decoys have to be selected in such a way that there is little or no correlation between the decoys and the actual source, i.e., selecting a decoy should not indirectly leak the actual location of the source. To blur any possible relationship, some notion of probabilistic selection is performed.

Just as there are two ways the delay can be imparted, there are two ways in which decoys can be selected: (i) spatially and (ii) temporally. The *spatial* selection of decoys is performed in such a way that an attacker continuously receives messages but is made to go through a longer route. On the other hand, the *temporal* solution works in such a way that, at some point, the attacker does not overhear an application message over a certain amount of time, thereby being delayed.

4.2 Component 2: Use of and Routing of Control Messages

- *Spatial selection of decoys*: When this selection technique is chosen, decoys need to be chosen such that they

are adjacent to each other (and further away from the source) so that they can attempt to lure the attacker along longer paths in the network. To ensure this, control information need to be transmitted to enable nodes to randomly decide if and when to become a decoy. Also, this suggests that control information needs to be carefully routed so that decoys can be selected at every hop. With this technique, both the convergecast and the routing of control messages can be done using different protocols.

- *Temporal selection of decoys*: When this selection technique is chosen, the main aim is to deprive the attacker of application messages from time to time, so as to delay him. Thus, as opposed to the spatial case, where subsequent decoys need to be adjacent to each other, here decoys do not need to, and they can be selected at various locations. In such a situation, an attacker may be "deadlock" at a location and may have to wait a long time before getting the next message. Again, control messages will need to be routed in such a way that nodes can randomly decide if and when to become decoys.

4.3 Component 3: Use of and Routing of Decoy Messages

- *Spatial selection of decoys*: With the spatial selection of decoys, decoys are continuously selected further away from the source and the decoys need to continuously receive a send decoy messages so that they lure the attacker away. So, decoy messages need to be sent and routed in such a way that increases the chances of the decoy messages reach an attacker before it gets too close to the source and also the decoy routing strategy needs to be such that there is a high likelihood of the attacker receiving the decoy message. An example of such a routing protocol with higher reliability is flooding.
- *Temporal selection of decoys*: With the main aim of temporal selection of decoys being to deprive attackers of application messages, the need for decoy messages is very low. In fact, by starving the attacker of application messages that it can follow to backtrack to the source, no decoy messages need to be used (and no routing of decoy messages is needed).

5. EXAMPLE CASE STUDIES

In this section, we will showcase the generality of our framework by deconstructing three different SLP routing protocols. The first example will be based on the spatial selection of decoys while the second one will focus on the temporal selection strategy.

5.1 Spatial Selection

Dynamic Fake Sources (DFS) [2] is an SLP-aware routing protocol that uses a spatial selection of decoys. This selection is typically performed using control messages[1], which fall into two kinds: (i) network information dissemination and (ii) diversionary node allocation.

The first kind of message spreads network information to allow nodes to make decisions about whether they should be fake sources. For example, in the Dynamic Fake Source algorithm [2], an ⟨Away⟩ message is flooded from the sink node. This allows other nodes to determine their distance to the sink, who their neighbours are and also their neighbour's sink distance. The algorithm also places a header in the protocol messages to disseminate information such as the distance from the source. This information is then stored and updated to allow decisions to be made about fake source selection.

The second kind of control message is used to actually select a node as a fake source. In [2], when a ⟨Choose⟩ message is received a node becomes a fake source. The recipient of the ⟨Choose⟩ message is randomly selected, reducing the correlation between source and decoy. This selection process then allows the construction of a diversionary route, as decoy nodes are adjacent to each other. The type of fake source (temporary or permanent) is determined based on the information received in the information dissemination message, as are other fake source parameters; such as the fake message broadcast rate. Once a node has finished being a fake source the torch is passed to a subsequent node by sending a further ⟨Choose⟩ message.

Figure 1a shows an illustration of the working of the Dynamic Fake Source protocol. Decoys are created such that the attacker goes on a diversionary route, where the attacker initially moves towards the source but is then pulled back away from the source. Other techniques have a similar approach (i.e., using spatial selection), for example [12] first creates a tree structure in the network (using dissemination messages) and then sends requests to the leaves for nodes to generate and send dummy packets (using selection messages).

5.2 Temporal Selection

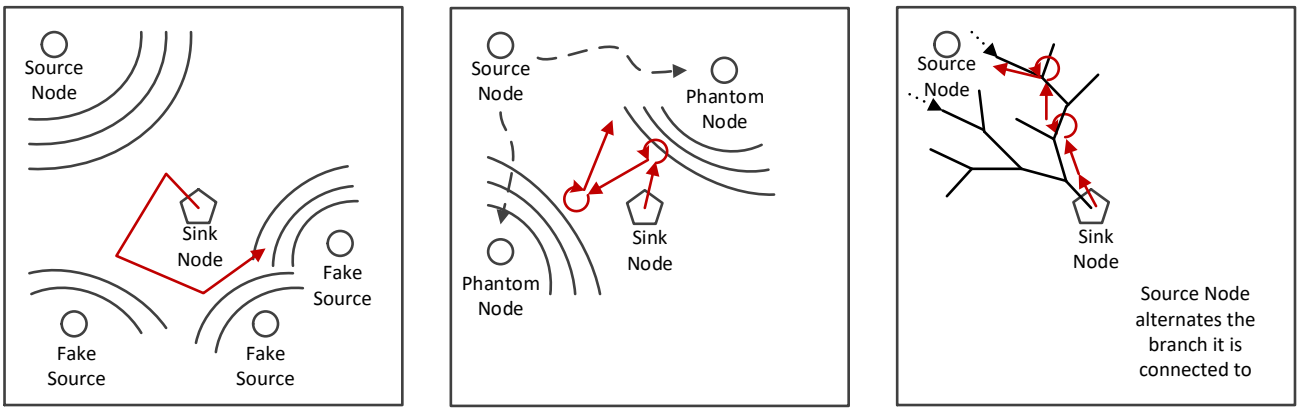
In this section, we will construct two SLP routing protocols that are based on temporal selection of decoys.

5.2.1 Phantom Routing

As mentioned previously, one important factor that needs to be satisfied for SLP routing is that there should be little or no correlation between the decoys and the actual source. For temporal selection, the source can send a control message prior to sending an application message in a random direction to a random node, informing it to become a decoy. Then, the source routes the application to the same node, which then act as a decoy by starting convergecast. This can be achieved through a similar route discovery technique, as in mobile ad hoc networks (MANET). Once a node has become a decoy, then it will route the application message using the convergecast routing strategy.

However, such a technique will induce a larger latency in the data delivery as the application message will incur the latency of the selection message to reach its destination. An optimisation of the above technique is, instead, to embed a "distance" value in the application message, which is subsequently sent on a directed random walk away from the source. At every hop, the distance value is decremented by one. The node that receives the message is distance 0 becomes a decoy. Such a routing protocol has been proposed in [8, 16] called Phantom Routing, which is illustrated in Figure 1b. The

[1]There have been examples of spatial section without control messages, e.g., in the Short-lived Fake Source strategy [8], a node chooses to become a fake source with a certain probability after receiving an application message. However, this technique performed poorly which gave rise to performing more intelligent diversionary allocation, that requires the two kinds of protocol messages.



(a) Dynamic Fake Sources: An example of spatial selection of decoys [2].

(b) Phantom routing: An example of temporal selection of decoys [8, 16].

(c) Tree routing: An example of temporal delay by alternating which branch the source node attaches to.

Figure 1: Three example techniques

figure shows the attacker waiting (i.e., looping on itself) for an application message to arrive before he can move. This delay prevents the attacker from reaching the source within the safety period.

So, in this case, component 1 is a temporal selection of decoys, component 2 being that control information (rather than control messages) need to be sent to select decoys[2]. Further, no routing strategy is needed to route the decoy messages as the decoys do not need to generate such decoy messages since the attacker is starved of application messages.

5.2.2 *A Tree-based Example*

Using the information gained by analysing Phantom Routing and understanding the protocols through the components, we can propose a novel temporal SLP-aware routing protocol that delays the attacker. This technique again attempts to delay the attacker by changing the path over which messages are routed. For example, when a spanning tree is overlaid on top of the network - such as the tree created by the Collection Tree Protocol (CTP) [5] - source nodes could alternate between the branches to which it is attached. This already occurs to some extent in CTP as routes are frequently changed to divert away from congested or unreliable areas. By having the node that generates application messages change between branches each time it sends a message, then the attacker may end up stuck along one branch for some time until the branch it is on is chosen again. It can be shown that this protocol will lead to higher levels of SLP.

So for this scheme, the decoy selection is the selection of which route to take to the sink, the control messages are used to setup and maintain the tree, and there are no decoy messages as the change in path of application messages leads to the delay. Typically, temporal SLP-aware protocols will not require decoy messages

6. CONCLUSION

In this paper, we have analysed SLP-aware routing protocols for WSNs and deconstructed these protocols to understand the main components of such SLP-aware routing protocols.

[2]Observe that piggybacking of control information is only an optimisation here.

We have firstly identified the nature of SLP-aware routing protocols and classified them as spatial or temporal. We then identified three main components, namely (i) decoy selection, (ii) use and routing of control messages and (iii) use and routing of decoy messages. We have subsequently shown how three protocols, one spatial and two temporal, can be constructed using the three above components, showing the viability of the framework.

As future work, we will formalise each component and then develop correctness proofs for the composition to yield SLP-aware routing protocols.

References

[1] Z. Benenson, P. M. Cholewinski, and F. C. Freiling. *Wireless Sensors Networks Security*, chapter Vulnerabilities and Attacks in Wireless Sensor Networks, pages 22–43. IOS Press, 2008.

[2] M. Bradbury, M. Leeke, and A. Jhumka. A dynamic fake source algorithm for source location privacy in wireless sensor networks. In *14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'15)*, pages 531–538, Aug. 2015.

[3] M. Conti, J. Willemsen, and B. Crispo. Providing source location privacy in wireless sensor networks: A survey. *IEEE Communications Surveys and Tutorials*, 15(3):1238–1280, 2013.

[4] M. Dong, K. Ota, and A. Liu. Preserving source-location privacy through redundant fog loop for wireless sensor networks. In *2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM)*, pages 1835–1842, Oct. 2015.

[5] O. Gnawali, R. Fonseca, K. Jamieson, M. Kazandjieva, D. Moss, and P. Levis. Ctp: An efficient, robust, and reliable collection tree protocol for wireless sensor networks. 10(1):161–1649, Dec. 2013.

[6] A. Jhumka, M. Bradbury, and M. Leeke. Towards understanding source location privacy in wireless sensor networks through fake sources. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom'12)*, pages 760–768, June 2012.

[7] A. Jhumka, M. Bradbury, and M. Leeke. Fake source-based source location privacy in wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 27(12):2999–3020, 2015.

[8] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk. Enhancing source-location privacy in sensor network routing. In *25th IEEE International Conference on Distributed Computing Systems, 2005. ICDCS 2005. Proceedings.*, pages 599–608, June 2005.

[9] N. Li, N. Zhang, S. K. Das, and B. Thuraisingham. Privacy preservation in wireless sensor networks: A state-of-the-art survey. *Ad Hoc Networks*, 7(8):1501–1514, 2009. Privacy and Security in Wireless Sensor and Ad Hoc Networks.

[10] S. Li, Y. Xiao, Q. Lin, and Z. Qi. A novel routing strategy to provide source location privacy in wireless sensor networks. *Wuhan University Journal of Natural Sciences*, 21(4):298–306, 2016.

[11] L. Lightfoot, Y. Li, and J. Ren. Star: design and quantitative measurement of source-location privacy for wireless sensor networks. *Security and Communication Networks*, pages n/a–n/a, 2012.

[12] J. Long, M. Dong, K. Ota, and A. Liu. Achieving source location privacy and network lifetime maximization through tree-based diversionary routing in wireless sensor networks. *Access, IEEE*, 2:633–651, 2014.

[13] M. Mahmoud and X. Shen. A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks. *Parallel and Distributed Systems, IEEE Transactions on*, 23(10):1805–1818, Oct. 2012.

[14] K. Mehta, D. Liu, and M. Wright. Location privacy in sensor networks against a global eavesdropper. In *IEEE International Conference on Network Protocols, 2007. ICNP 2007.*, pages 314–323, Oct. 2007.

[15] X. Niu, C. Wei, W. Feng, and Q. Chen. Osap: Optimal-cluster-based source anonymity protocol in delay-sensitive wireless sensor networks. In *2014 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 2880–2885, Apr. 2014.

[16] C. Ozturk, Y. Zhang, and W. Trappe. Source-location privacy in energy-constrained sensor network routing. In *Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks*, SASN '04, pages 88–93, New York, NY, USA, 2004. ACM.

[17] A. Proano, L. Lazos, and M. Krunz. Traffic decorrelation techniques for countering a global eavesdropper in WSNs. *IEEE Transactions on Mobile Computing*, PP(99):1–1, 2016.

[18] R. Rios, J. Lopez, and J. Cuellar. *Foundations of Security Analysis and Design VII: FOSAD 2012/2013 Tutorial Lectures*, chapter Location Privacy in WSNs: Solutions, Challenges, and Future Trends, pages 244–282. Springer International Publishing, Cham, 2014.

[19] M. Shao, W. Hu, S. Zhu, G. Cao, S. Krishnamurth, and T. La Porta. Cross-layer enhanced source location privacy in sensor networks. In *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09*, pages 1–9, 2009.

[20] M. Shao, Y. Yang, S. Zhu, and G. Cao. Towards statistically strong source anonymity for sensor networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pages –, Apr. 2008.

[21] P. Spachos, D. Toumpakaris, and D. Hatzinakos. Angle-based dynamic routing scheme for source location privacy in wireless sensor networks. In *Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th*, pages 1–5, May 2014.

[22] W. Tan, K. Xu, and D. Wang. An anti-tracking source-location privacy protection protocol in WSNs based on path extension. *Internet of Things Journal, IEEE*, 1(5):461–471, Oct. 2014.

[23] W. Wei-Ping, C. Liang, and W. Jian-xin. A source-location privacy protocol in WSN based on locational angle. In *Communications, 2008. ICC '08. IEEE International Conference on*, pages 1630–1634, May 2008.

[24] Y. Xi, L. Schwiebert, and W. Shi. Preserving source location privacy in monitoring-based wireless sensor networks. In *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International*, pages 8 pp.–, Apr. 2006.

[25] L. Yao, L. Kang, F. Deng, J. Deng, and G. Wu. Protecting source–location privacy based on multirings in wireless sensor networks. *Concurrency and Computation: Practice and Experience*, 27(15):3863–3876, 2015.