논문 18-43-09-05 The Journal of Korean Institute of Communications and Information Sciences '18-09 Vol.43 No.09
https://doi.org/10.7840/kics.2018.43.9.1429

# 무선 센서 네트워크에서 발생원 위치 프라이버시를 위한 라우팅 기법 연구

릴리안 찰스 무타람와◆, 신 석 주°

# Routing Schemes for Source Location Privacy in Wireless Sensor Networks: A Survey

Lilian Charles Mutalemwa◆, Seokjoo Shin°

ABSTRACT

Wireless Sensor Networks (WSNs) are used in sensitive applications such as monitoring of high value assets. One of the challenges facing these networks is preservation of source location privacy. In this work, a review of performance characteristics of some representative routing schemes is done. Performance analysis of the schemes shows that tree-based routing schemes can provide high privacy at a cost of high energy consumption while angle-based routing schemes provide a good balance between privacy and energy consumption. The work also highlights some challenges and open issues for the routing schemes.

**Key Words** : source location privacy, routing schemes, wireless sensor networks, back tracing, adversary

## Ⅰ. Introduction

A Wireless Sensor Network (WSN) is a network which consists of spatially distributed autonomous sensors with the aim of monitoring various physical and environmental conditions including asset monitoring and tracking[1,2]. A recent implementation of asset monitoring network is the Wildlife Crime Technology Report where a WSN is used to monitor a large area where animals roam[1,3]. In monitoring applications, nodes work by monitoring their surroundings to detect a presence of an asset. When the asset is detected, the node which detects the asset becomes a source node and transmits a packet to sink to report the presence of the asset in its surroundings[1,2]. The distance between source node and sink is often longer than the transmission range of sensor nodes making multi-hop communication a viable mode of transmission in WSNs[2,3].

One of the challenges that face multi-hop communication wireless networks is creating secure and private applications. This is due to their potential to expose important information as packets are broadcasted across the network. Security measures such as encryption are used to protect the content of a packet but the context of the broadcast remains exposed to adversaries[4]. Adversaries can monitor the pattern of broadcasts and back trace to the location of source node where the data packet originated[5-7]. This has motivated researchers to

◆ First Author : (ORCID:0000-0003-4342-5562)Chosun University Department of Computer Engineering, lilian.mutalemwa@gmail.com, 학생회원
° Corresponding Author : (ORCID:0000-0003-2092-1336)Chosun University Department of Computer Engineering, sjshin@chosun.ac.kr, 종신회원
논문번호 : 201806-B-150-RN, Received March 13, 2018; Revised July 12, 2018; Accepted July 24, 2018

propose schemes to preserve source location privacy. Privacy can be defined as the guarantee that information can only be observed or deciphered by those that it is intended for[2]. Source location privacy preservation is the process of keeping the location of a source node hidden from adversaries in an asset monitoring network[2]. Several privacy preserving techniques exist to ensure source location privacy. In this work, focus is given to routing based schemes for source location privacy. Routing schemes have proven to be promising for preserving source location privacy and this has motivated recent research to continue proposing new schemes. Energy consumption is an important parameter since energy is a limited resource in WSNs. For many schemes, providing efficient source location privacy requires a tradeoff with energy consumption. Designing of routing based techniques to preserve source location privacy must consider minimizing network energy consumption to improve network performance parameters such as network lifetime. Considering these features, this paper is motivated to do a review on the routing schemes and study their privacy preservation and energy consumption performance.

This paper classifies the routing schemes into phantom node routing, fake source routing, intermediate node routing, tree-based routing and angle-based routing. The paper reviews the performance features and characteristics of some representative routing schemes. These schemes are chosen for the study based on their popularity among routing based schemes for source location privacy preservation. The paper investigates the schemes performance features and provides performance analysis on the privacy preservation and energy consumption characteristics of the representative schemes. Furthermore, the paper explores some challenges and opportunities for routing based privacy preservation schemes.

The remainder of this paper is organized as follows: Section II discusses the concept of source location privacy in WSNs. Section III is a classification of routing schemes for source location privacy in WSNs. Section IV identifies adversary models of routing schemes for source location privacy in WSNs. Section V analyses the privacy preservation and energy consumption performance characteristics of some representative routing schemes. Section VI highlights some opportunities for future work. Finally, section VII concludes this paper.

## Ⅱ. Source Location Privacy in WSNs

Privacy attacks in WSNs can be classified in two categories: (1) data privacy attack and (2) context privacy attack[6,8,9]. Data privacy attacks relate to threats that are based on the contents of packets, including threats which are against the sensed data [6,10]. In such threats, attackers try to capture data to learn about the status of the network so that relevant attacks can be launched. Cryptographic techniques such as encryption and decryption are used to secure the integrity of data packet gathered and transmitted to the sink[9]. Context privacy attacks are based on the context associated with the measurement and transmission of the sensed data. Context is an attribute that captures several environmental aspects associated with network and sensed data, including aspects such as node location, node identity, packet route and packet generation time[4,6,9]. Location privacy is concerned with location of a node in the network. The work in this paper focuses on routing schemes for preserving source node location privacy.

Source location privacy requires more than just confidentiality of the packets exchanged between nodes. It requires that the flow of packets in network does not give away information about the location of a source node to the adversary[8,9]. The introduction of source location privacy problem in [11] used the Panda-Hunter Game network model. Using WSNs to monitor endangered giant pandas in a bamboo forest is a common example of WSN monitoring applications. Panda is a high value asset which needs protection. In 2003, a single piece of panda fur sold in Chongqing, China for $66,500[12]. In a forest, each panda will have an electronic tag that emits a signal to be detected by the sensor nodes in the network. The adversary is initially located in the vicinity of sink node, waiting to hear

packets sent from source nodes for back tracing attack. The near sink adversary initial location is assumed in many routing schemes including the schemes in [5], [8], [11], [13], [14] and [15]. Adversary starting at sink location guarantees it hears packets since sink node is the destination for all packets[11]. When a packet is received at the sink, adversary will overhear and start back tracing the packet route by moving 1 hop towards the source until it locates the source node. Routing schemes are used to obfuscate the back tracing process of an adversary.

There are different factors to consider when designing a routing scheme for preserving source location privacy in WSNs. These factors affect how effective a scheme is in its operation. These factors include energy consumption, mobility and adversary type[16]. Energy is a limited resource in WSNs and so it needs careful designing. Nodes that are mobile require different protocol solutions compared to scenarios in which nodes are static. Different adversary models and assumptions lead to different types of techniques for source location privacy preservation. Adversary that can compromise nodes poses different requirements than an adversary that cannot. The type of adversary that a source node is protected from can be passive or active adversary. A passive adversary does not interfere with the operation of network nodes but an active adversary does. An active adversary can perform serious attacks such as reprogramming of the sensor software while a passive adversary can simply eavesdrop on sensor communication[9]. A common adversary assumption in many routing schemes is a passive adversary called a distributed eavesdropping attacker. An example implementation of a distributed eavesdropping attacker can be a single mobile person equipped with a sensor node to allow eavesdropping on a network or, multiple persons each with a sensor node eavesdropping on a network [9].

Another factor, related to the adversary, is whether the adversary is global and has the capability to view all traffic within the WSN or local and can view only a part of network. A local adversary does not have instant access to global network information. It slowly accumulates knowledge to gain global network information. In some applications such as military or industrial spying, adversary can have big incentives to make it more powerful with a global view of the network. It is more difficult to provide source location privacy against global adversary[12]. A global adversary only needs to identify the sensor node which initiates communication with the sink. Instinctively, this sensor node will be close to location of the monitored asset.

In this work, a parameter called safety period is used to measure privacy. Two notions for the parameter safety period are given in [5] and [10]. The first notion is used mainly for routing schemes, it defines safety period as the time required for an adversary to back trace and capture the asset. The second notion is used when it is necessary to limit the amount of time source location privacy is being considered for, i.e., if an adversary fails to capture a source node within the specified safety period, then, it is considered that privacy has successfully been preserved. The notion defines safety period as the maximum time an asset will be at a given location before its next movement. This work assumes the first notion. Higher safety period provides higher privacy level. An objective of a source location privacy scheme is to maximize the safety period of a network.

## Ⅲ. Classification of Routing Schemes for Source Location Privacy in WSNs

Since the introduction of source location privacy problem in [11], the problem has been addressed with a variety of system models and schemes. Some of the schemes are routing based[7, 17]. Routing schemes work by preventing the adversaries from back tracing the source location through traffic monitoring and analysis. This section classifies the routing schemes into five categories: fake source routing, phantom node routing, intermediate node routing, tree-based routing and angle-based routing. The section reviews the literature on the

performance features of the routing schemes.

### 3.1 Fake Source Routing

The baseline Fake Source Routing (FSR) scheme was introduced in [11]. It is one of the pioneering schemes for source location privacy in WSNs. FSR scheme uses a set of fake source nodes to act as a decoy for the real sources. The fake source generates packets to engineer network traffic in a way that confuses an adversary by leading it away from the real source. Fake packets are of the same length as the real packets, and they are encrypted so as to make it difficult for adversary to tell the difference between a fake packet and a real packet. Fake sources are carefully positioned to avoid leading the adversary towards the real source. Two strategies exist for baseline fake source routing: (1) Short-lived fake source routing, and (2) Persistent fake source routing[8,18]. Short-lived fake source routing is a simple injection strategy that does not require additional overhead. It is easy to implement but provides poor privacy level, because the fake sources are short-lived. A fake packet can guide an adversary towards a fake location but there are no succeeding fake packets around that location to draw adversary even further away. This makes it easy for adversary to catch the next real packet. Persistent fake source routing functions similar to short-lived fake source routing but it takes into consideration that having one fake source at a time for only one fake packet is not enough to distract an adversary. In persistent fake source routing strategy, once a node decides to become a fake source, it keeps on generating fake packets regularly so that the adversary can be effectively deceived. A node continues to broadcast fake packets which are dropped instantly when neighbors receive the packets. The rate of fake packet injection is carefully controlled to maximize privacy. The use of shortest path routing scheme for source location privacy was also introduced in [11], [18]. In the shortest path routing, a node forms a single route between the source node and sink according to a gradient-based approach. During packet forwarding, a node which has the shortest hop distance to the sink is assigned the maximum gradient and packets are always forwarded to the next-hop node which has the maximum gradient. Since the shortest path routing scheme routes packets through the shortest path from source node to sink node, it has tradeoffs between privacy, energy consumption and packet delivery performance. The shortest routes provide short safety period and poor privacy while they consume very low energy and deliver packets with shortest delay and high delivery ratio.

A dynamic fake source routing scheme was proposed in [19] and a distributed solution that combines fake source routing and phantom source routing in [8]. The work in [19] points out that, earlier proposed fake source schemes provide suboptimal performance since they use network configurations which are not realistic in real world scenarios. It suggests that a scheme does not need to have prior network knowledge as network conditions may change in real world. It proposes a dynamic fake source routing scheme that does not require prior network knowledge. This is achieved through the use of online parameter estimation. It argues that the proposed dynamic fake source scheme provides state-of-the-art levels of privacy, making it a viable option for WSN deployment in contexts where less is known about the operational environment. In [10] it is shown that, for networks with multiple source nodes, in the worst case scenario, communicating with no source location privacy preserving scheme can yield better privacy than when fake source routing scheme is applied. Also observed in [10], [19], the variation in network traffic caused by multiple source nodes in a network can produce a push-pull effect on the adversary causing adversary to make a less informed decision. The push-pull effect can have better privacy effect than fake source routing scheme when there are more than two source nodes in the network.

Fake source routing schemes are often criticized for their high energy consumption. In [20], [21], it is highlighted that, the most significant limitation of fake source routing scheme is the high volume of packets required to broadcast in order to provide efficient source location privacy. The high volume

of packets in the network leads to increased energy consumption and increased number of collisions, both of which result in a reduced packet delivery ratio. Fake source routing schemes require tradeoffs between energy consumption and privacy. For this reason, these schemes are considered not appropriate for large-scale networks. In [22], evaluation of the impact of fake packet rates and collisions on fake source routing schemes is done. It confirms that, there exist practical rates at which fake packets should broadcast in order to be effective in providing source location privacy and energy efficiency. It is shown that, real and fake source packet rates are directly related to the number of collisions in the network. Higher packet rates increase the potential for collisions. Also, an increase in the proportion of collided packets on a WSN can reduce the source location privacy level. Reducing the packet rate of source nodes may increase energy efficiency but at a cost of reduced privacy level[22].

In [23], a formalization of the Fake Source Selection (FSS) problem is provided using two important parameters that affect the efficiency of fake source routing scheme. The FSS problem is defined in [23] as the process of selecting a set of permanent and temporary fake sources such that the adversary does not reach the source node within the safety period. The work points out that, the algorithm needed to select permanent and temporary fake sources is highly linked to the network configuration. Also, since the source node sends packets at a determined rate, it is important for fake sources to send packets at the right rates as well as over the duration of the fake sources. It then identifies the two parameters as fake packet rates and fake source duration. Investigations on the impact of temporary fake source duration on the level of source location privacy showed that, an increase in the duration during which a node acts as a fake source results in a higher level of source location privacy. Investigations on the impact of fake packet periods on the level of source location privacy showed that, a decrease in the fake packet period causes an increase in the level of source location privacy. It was also found that, a very high fake packet rate is likely to give rise to collision rates in the network, thus reducing the efficiency of the scheme. When the packet rate is very high, the proportion of packets received by the sink is significantly reduced. Energy consumption issues of fake source scheme were also studied in [23], it was found that, the two parameters, fake source packet period and fake source duration can be used to adjust the energy consumption of the scheme. A tradeoff can be made between higher fake source duration and lower fake packet periods to provide higher source location privacy level. A combination of values for fake source duration and fake packet periods may result in near optimal source location privacy level.

### 3.2 Phantom Node Routing

The baseline Phantom Routing Scheme (PRS) was introduced in [11] to improve the limitations of baseline FSR scheme. Baseline FSR scheme provides a fixed route for every packet making it easy for adversary to back trace the route. PRS uses the two most popular routing schemes in WSNs, flooding routing and single-path routing. Flooding routing works by making a node broadcast its packet to each of its neighbors, the neighbors then rebroadcast the packet to each of their neighbors. Flooding routing is easy to implement and allows easy modification. PRS involves two phases: (1) a walking phase using random walk, and (2) a succeeding flooding phase to deliver packets to the sink[17]. The phantom source is positioned far away from the real source which makes the real source node location difficult to trace back. Privacy protection improves as the network size and intensity increase because the path diversity between different packets increases with increase in network size.

Several versions of PRS exist to improve its performance[13,20,16]. PRS and Phantom Single-path Routing Scheme (PSRS) are among the most investigated versions. PSRS was introduced in [18]. It uses two phases: (1) random walk, and (2) single-path routing. Single-path routing allows nodes

to forward packets only to a subset of its neighbor nodes and save energy. An improved version of PSRS is directed walk PSRS, also proposed in [18]. Directed walk PSRS replaces the random walk phase with directed walk phase to ensure that the phantom source is far away from the real source. Directed walk is achieved either through sector-based or hop-based directed walk. Sector-based directed walk provides better privacy than hop-based directed walk. In terms of energy consumption, PSRS has better performance than PRS since it does not use flooding technique. A challenge in PSRS is, once the packet is captured on the directed walk path, the adversary is able to get the direction information stored in the header of the packet[21]. This is due to the re-usage of routing paths. This exposure of direction information reduces the privacy performance. Also, PSRS consumes slightly more memory than PRS. Both, PSRS and PRS preserve privacy against local adversary. It is argued in [24] that, PRS has been proven flexible and capable of protecting source node location, even when the source is mobile in the network. However, PRS is unable to preserve privacy against global adversary. In [25], it is argued that, the sector-based directed random walk provides higher privacy than the hop-based directed random walk but both schemes have limitations. The hop-based directed random walk becomes less random towards the sink, as there are fewer alternative paths around the sink. The sector-based directed random walk is sensitive to the source node position, if source node is close to a network border, the walk is directed towards the border closest to source node and the random walk cannot complete its walk.

There exist a few algorithms to improve performance of PSRS. Phantom Routing with Locational Angle (PRLA) is introduced in [14]. PRLA improves the performance of PSRS by using a random inclination angle for each packet routed from source node to the sink. PRLA deceives the adversary at the sink by choosing a random inclination angle for each packet routed from source node to the sink. PRLA has higher privacy period than PSRS and PRS. Analysis in [14] show that, on average, PRLA can improve the safety period by up to 50% compared to that of PRS, with a minor increase in energy consumption. The improvement is achieved by the use of nodes with larger inclination angle which guarantees more privacy effective routing paths for the packets.

An improved version of sector-based directed walk called Self-Adjusting Directed Random Walk (SADRW) is introduced in [25]. SADRW provides longer random walks than the sector-based directed walk. The random walk in SADRW proceeds past where a sector-based directed random walk ends. The Greedy Random Walk (GROW) was introduced in [26]. GROW considers the benefits of using random walk for privacy preservation. A random walk does not disclose direction information of source node as forwarding decision is made locally and independent of the source location. It uses two-way random walks, one from source node and another from sink node. The random walk starting from the sink forwards packets to a randomly selected phantom node (receptor – node). The other random walk starting from source node meets the first random walk at the phantom node. The phantom node then uses the path established by the random walk from the sink to the phantom node to route the packet from the source node to the sink. During forwarding, GROW covers unvisited areas by using greedy strategy which selects neighbor nodes that have not yet participated in the random walk. To achieve this, it uses Bloom filters in the packets. A node first adds its identity to the Bloom filter, before it forwards the packet.

Analysis in [26] show that, by relaxing the requirement for the delivery time, GROW is able to preserve source location privacy in large-scale networks with a much lower energy consumption as compared to flooding – based PRS. In some scenarios, GROW consumes less than half of the energy consumed by flooding-based PRS. Several works in the literature have reviewed the performance of GROW[16]. Some literature state that the random walk used in GROW is inefficient at creating a safe distance between the phantom node

and the source node. They point out that the latency is unstable due to the usage of two random walks. It is also pointed out that, finding a reliable phantom node is essential in the case of an internal adversary, but [26] does not give criteria for selecting the reliable phantom node[16]. Other review work of GROW highlights that, the phantom node can still be too close to the sink or source node. Also, packets leak too much information to adversary[16]. In [22], it is argued that GROW is not feasible for large scale networks. It argues that, the use of Bloom filters to store information of all the visited nodes in the network for each packet to prevent the packets from hopping back is not realistic. It is also argued in [13], [21] that, the design of GROW allows the adversary to recover significant routing information from the received packets and that, GROW is unrealistic for large scale networks. An observation is also given in [14], [24] that GROW can prevent the adversary from tracing back to the source node but with long delivery latency. A multi-phantom routing scheme was proposed in [15]. The scheme obscures the adversary by generating different paths for different packets for the same source node, creating multiple paths from source node to sink node. The scheme consists of two phases: (1) configuration phase which involves neighbor discovery, flooding, node reports its hop count from the sink and triplet selection, and (2) working phase which involves random walk and phantom selection based on given criteria. To minimize energy consumption and network congestion, the scheme in [15] avoids the use of fake packets and flooding in working phase. Analysis in [15] show that, the scheme achieves more privacy and greater safety period as compared to PSRS.

An analysis of PRS performance under various network configurations was done in [20]. The analysis argues that, results in [11] showed PRS provides a high level of source location privacy but these results were from simulations with restrictive network configurations. The analysis in [20] evaluated the ability of PRS to preserve source location privacy under different network configurations using three parameters: (1) packet rate, (2) number of source nodes, and (3) length of random walk. The parameters were varied to assess their impact. Results showed that, in PRS; a higher packet rate and higher number of source nodes reduce the source location privacy level while a longer random walk increases the source location privacy level.

### 3.3 Intermediate Node Routing

To prevent phantom routing scheme from exposing direction information to the adversaries while packets are forwarded to the phantom sources, Randomly Selected Intermediary Node (RRIN) scheme was introduced in [27]. In RRIN scheme, the source node first randomly selects an intermediate node at the sensor domain based on the relative location of the sensor nodes. The intermediate node is determined using two factors: (1) it must be outside the constrained region around the source, and (2) it is normally distributed outside the constrained region. The intermediate node then routes the received packet to the sink through a fixed route. The routing strategy of RRIN makes it difficult for adversary to trace back to the source node because the probability for packets from same source node to use the same routing path and intermediate node is very low for large networks. An analysis to find the effect of multiple routing paths originating from same source node was done in [28]. It found that, source location privacy increases with the increase in number of routing paths between a source node and sink. Also, privacy is increased with more paths of longer lengths. RRIN scheme has a limitation of high energy consumption but compared to PRS, RRIN has lower energy consumption.

There exist many other versions of RRIN including one where a source node forwards the packet to any intermediate node randomly. This version has a much improved safety period and privacy but with higher latency and energy consumption[16,29]. The work in [13] points out that, constrained RRIN can provide good level of source location privacy against local adversary, however, it

may not be able to provide adequate global source location privacy. To provide good level of source location privacy against global adversary, [13] proposes improvements by presenting two routing schemes. The proposed routing schemes provide routing through multiple randomly selected intermediate nodes based on angle and quadrant. It is argued in [13] that, the two proposed schemes can offer global source location privacy for WSNs. Other advantages of routing through multiple randomly selected intermediate nodes for large sensor networks as compared to the first version of RRIN are: (1) more reliability; since packets are routed by multi-intermediate nodes, the routing direction is changed every time the packet is forwarded by an intermediate node. So even if the packet is captured by an adversary, he is unable to get the direction of the source node, (2) energy-efficiency; using controlled multi-intermediate nodes, the average length of routing path can be decreased to save energy consumption, and (3) higher delivery ratio; as the length of routing path decreases through multiple intermediate nodes, reliability and delivery ratio can be improved simultaneously. A comparative analysis of the performances of quadrant-based multiple randomly selected intermediate nodes scheme and angle-based multiple randomly selected intermediate nodes scheme in [13] show that, the quadrant-based scheme can provide better performance than angle-based scheme. Both of these two schemes achieve global location privacy.

Intermediate node routing strategy is also used in combination with other routing strategies for source location privacy preservation. For example, a three-phase routing scheme was proposed in [30] where a packet is first routed to a randomly selected intermediate node, then, routed in a network mixing ring (NMR), and finally forwarded to the sink node. In [31], a two-phase routing scheme was proposed where a packet is first routed to a randomly selected intermediate node (RRIN) then through a NMR. The main shortcoming of NMR schemes is that, energy consumption in the network is unbalanced. Ring nodes are more likely to drain their batteries faster than other nodes. Moreover, sink node is surrounded by ring nodes which means if ring nodes die, sink node may become isolated from nodes outside the ring. Sink Toroidal Region (STaR) routing scheme was proposed in [21] to provide high source location privacy with low energy consumption as compared to RRIN. STaR scheme allows the source node to randomly select an intermediate node within a designed STaR region located neither too close, nor too far from the sink node. The intermediate nodes are evenly distributed in the STaR region to give an impression that the source node is forwarding packets to the sink node from all the possible directions. Analysis in [21] show that, from the probability point of view, for a large network, there is a very low probability that packets from same source node will be routed using the same path and the same intermediate nodes. This reduces the possibility for an adversary to intercept multiple packets from the same source node which in turn increases the source location privacy against a local adversary. The energy consumption of STaR is higher than that of constrained RRIN but much lower than that of totally random RRIN[29]. The delivery ratio for STaR is slightly lower than the two RRIN schemes due to the possible higher collision ratio. In [16], it is argued that, STaR scheme is more efficient than PRS and totally random RRIN. STaR has a similar latency to PRS, but also a higher packet drop rate than PRS.

An intermediate node based routing scheme was proposed in [32] to solve the limitations of traditional schemes such as shortest path routing scheme. In shortest path routing, selection of the next hop node always obey a constant rule, as a result, packets from same source node are routed through a set of similar routing paths to arrive at the sink node. Routing paths are strongly related to each other and get closer and closer to each other as they approach the sink node[32]. As routes become more similar and closer, it becomes easier for adversaries to back trace the source nodes. In [32], All-direction Random Routing (ARR) scheme was proposed. ARR selects the routing paths in a flexible way to ensure that the routing paths are totally dispersive

and even an accidental exposure of a part of a routing path does not lead the adversary to the source node. In ARR scheme, source nodes control the routing strategies and the routing process is done in three phases: (1) selecting a proper sink node and an agent node, (2) forwarding the packets to the agent node from the source node, and (3) forwarding the packet from the agent node to sink node. In this work, agent node in ARR is considered to function as an intermediate node. Performance analysis in [32] show that, ARR provides better privacy level than PRS and shortest path routing with a slight increase in the communication overhead and energy consumption. ARR consumes more energy because it has longer routing paths than shortest path routing and PRS. The delivery delay of ARR is higher than that of shortest path but lower than that of PRS. The analysis also shows that, privacy level of ARR, shortest path and PRS decreases with an increase of number of adversaries in the network.

### 3.4 Tree-Based Routing

Tree-based Diversionary Routing (TDR) scheme was proposed in [33]. The idea in the scheme is to use hide and seek strategy to create diversionary routes along the path to the sink from the real source. At end of each diversionary route, a fake source node is used to deceive the adversary by periodically sending fake packets. Each source node creates its own root path which goes to the end of the network boundary to divert the adversary from real path. The work of [33] agrees with [28] and points out that, the need for diversionary routes comes from the fact that, in PRS scheme, the phantom node is routed to the sink directly which to some degree allows the adversary to trace back along the route to phantom node and eventually to source node. It argues that, adding several diversionary routes between phantom node and sink node makes it more difficult for the adversary to determine in which route the real packet is. The scheme exploits the abundant energy in the region away from the sink to build redundant diversionary routes to make it difficult for the adversary to trace to phantom node.

Results in [33] show that, TDR has better privacy performance against direction-oriented attack as compared to PRS. The route length in TDR is more than 10 times of PRS leading to high level of privacy as the adversary has to spend more than 10 times of the time to achieve the same attack effect as with PRS. The energy consumption in TDR can be up to 22 times higher than the energy consumption in PRS, this is because TDR scheme creates many diversionary routes which increase the energy consumption. The energy consumption is increased in the non-hotspot region near network border, causing balanced energy consumption in different regions of the network and improved network lifetime. It is argued in [8], [3] that, TDR scheme consumes very high energy for each node to create their own root path that goes to the end of the network boundary. Although the path diverts the adversary from real path and increases privacy level, the energy consumption is too high.

The idea of tree routing for source location privacy preservation is also used in [34]. The proposed schemes in [34] are: Forward Random Walk (FRW), Bidirectional Tree (BT), Dynamic Bidirectional Tree (DBT) and Zigzag Bidirectional Tree (ZBT). The tree routing schemes provide end-to-end location privacy against local adversary with a low end-to-end latency. In BT scheme, a tree topology is employed at the two ends of the delivery path to enhance the location privacy of the source and sink nodes. Real packets are forwarded along the shortest path from source to sink. To protect the source location privacy, topological branches are designed along the shortest path at the source node, in which the fake packets are forwarded from the leaf nodes to the tree trunk nodes. If adversary back traces the source node, it will be deviated from the real packet path by the tree branches. In the DTB scheme, branches of the trees are generated dynamically to further improve the performance. The routing in BT scheme uses the shortest path, making it possible for the adversary to guess the location of the source node. ZBT is then used to solve the shortest path problem by adopting proxy source and a proxy sink techniques which prevents

the adversary from guessing the location of the source or sink easily. Analysis in [34] shows that, ZBT and DBT schemes can achieve high source location privacy against a patient adversary. ZBT, DBT and BT achieve higher privacy than the baseline shortest path scheme which delivers packets to sink through the shortest path. ZBT and BT can also provide high privacy level for sink.

### 3.5 Angle-Based Routing

The Angle-based Dynamic Routing (ADR) scheme was introduced in [29]. The scheme uses location information of the nodes and calculates two inclination angles formed between nodes: (1) inclination angle between a forwarding node and a receiving node, and (2) inclination angle between forwarding node and sink node. The angles are used to form a candidate set of neighbor nodes to forward the packet. One of the nodes in the candidate set is selected randomly and becomes the next forwarding node. The candidate set changes at every packet forwarding instance to form multiple paths towards the sink node. During packet forwarding, a source node floods a Request To Send (RTS) packet to all the neighboring nodes within its transmission range. Neighboring nodes then reply with a Clear To Send (CTS) packet. On reception of CTS packet, the source node or a forwarding node then calculates the distance to the neighboring node and the inclination angle between the source node and the neighboring node with respect to sink node. If the distance to the neighbor node is larger than a predefined distance and the inclination angle does not exceed a predefined angle, the neighboring node is added to the candidate node set. One node is then selected randomly to be the next forwarding node. Performance analysis in [39] show that, ADR scheme provides higher safety period and lower packet latency as compared to PSRS. The higher safety period is achieved by the random selection criterion of the next forwarding node. The lower packet latency is achieved by the use of inclination angle which ensures that nodes in the routing path do not deviate significantly from the shortest path. It is argues in [39] that, in comparison with PSRS, ADR scheme can provide better safety period of up to 70% and improve packet latency without increasing the complexity. A possible challenge with ADR scheme is packet collisions and reduced packet delivery ratio that could result from the RTS/CTS handshake process.

There exist a few other angle-based routing schemes for source location privacy in WSNs. 2-Phantom Angle-based Routing Scheme (2PARS) was proposed in [35]. The proposed scheme considers a triplet for selecting the phantom nodes. A triplet is a group of three nodes formed on the basis of three parameters: (1) their distance from the sink node, (2) their location information, and (3) the inclination angle between them. Phantom selection is performed for every packet forwarding instance, creating multiple paths for the packets. Routing path for the packets changes dynamically, increasing the safety period without significant increase in the packet delivery latency. The analysis in [35] shows that, 2PARS performs better in terms of safety period as compared to PSRS and multi-phantom routing schemes. A Constrained Random Routing (CRR) scheme was proposed in [24]. CRR scheme is based on the transmitting offset angles and constrained probability. To prevent adversary from tracing back to locate the source node, first, each forwarding node determines a specific selection domain for next-hop node according to the dangerous distance and the wireless communication range. Then, it analyzes the offset angles of the candidate nodes based on the direction of the nodes to the sink node. Lastly, the forwarding node calculates the selected weights of the candidate nodes according to their offset angles, and the selected weights are used to decide which node to become the next-hop node. Analysis in [24] show that, the packet routing paths in CRR are more random than ADRS giving it better privacy performance. However, CRR introduces a small amount of redundant paths which gives it a slight higher energy consumption and end-to-end delay than the shortest path routing. Phantom Routing with Locational Angle (PRLA) introduced in [14] is also an angle-based routing scheme. In [13], an

angle-based multiple randomly selected intermediate nodes scheme was proposed to improve the performance of RRIN.

## Ⅳ. Adversary Models in Routing Schemes for Source Location Privacy

As highlighted in section II, an important feature which affects the designing and privacy preservation performance of a routing scheme is the assumed adversary model. Most of the routing schemes assume a less powerful adversary which is passive, has a local view of the network, starts at sink and performs hop-by-hop back tracing attack to find location of the source node. Only tree-based diversionary routing scheme assumes a slightly powerful adversary called direction-oriented attacker. A direction-oriented attacker works by estimating the direction of the source node, and traces along the estimated direction rather than hop-by-hop back tracing attack. PSRS, BT, DBT and ZBT assume two types of adversary models, a patient adversary and a cautious adversary models. A cautious adversary is more powerful than a patient adversary. A patient adversary is simply a passive, local, back tracing adversary who uses the hop-by-hop tracing technique patiently until it finds the source node. In the cautious adversary model, the adversary uses a timer to limit its waiting time at a node and avoids revisiting nodes which have already been visited to escape from getting trapped in a loop. A cautious adversary will roll back to its previous node if its waiting timer expires without further eavesdropping on any packet. This work identifies four main adversary models assumed during the designing of the routing schemes for source location privacy. The four adversary models are: (1) a patient, local, passive, hop-by-hop back tracing adversary, (2) cautious, local, passive, hop-by-hop back tracing adversary, (3) a global, passive adversary, and (4) a direction-oriented adversary. Table 1 shows the adversary models assumed during designing of the routing schemes.

Table 1. Adversary models assumed for routing schemes

| Adversary Model | Routing Scheme |
|---|---|
| A patient, local, passive, hop-by-hop back tracing adversary | FSRP [8], FSR [11], SPR [11], MRRIN [13], PRLA [14], MPR [15], PSRS [18], DFSR [19], STaR [21], CRR [24], SADRW [25], GROW [26], RRIN [27], ADR [29], ARR [32], FRW [34], BT [34], DBT [34], ZBT [34], 2PARS [35]. |
| A cautious, local, passive, hop-by-hop back tracing adversary | PSRS [18], FRW [34], BT [34], DBT [34], ZBT [34]. |
| A global, passive adversary | MRRIN [13], RRIN [27], 3-NMR [30], 2-NMR [31]. |
| A direction-oriented adversary | TDR [33]. |

## Ⅴ. Performance Analysis of Routing Schemes for Source Location Privacy

A comparative analysis of privacy and energy consumption performance of five representative schemes was done using MATLAB simulation. The representative schemes are Phantom Routing Scheme [11], Shortest Path Routing[18], Randomly Selected Intermediate Node Routing[27], Tree-based Diversionary Routing[33], and Constrained Random Routing[24]. The network simulation parameters are summarized in table 2. Sink node is assumed to be located at the center of the sensor network domain so as to control the delivery latency in the network.

Table 2. Network simulation parameters

| Parameter | Value |
|---|---|
| Network size | 100 m x 100 m |
| Number of nodes | 400 |
| Target monitoring scheme | k-nearest neighbors tracking |
| Initial energy (J) | 0.5 |
| Threshold distance (do)(m) | 87 |
| Eelec(nJ/bit) | 50 |
| Eamp(pJ/bit/m4) | 0.0013 |
| Efs(pJ/bit/m2) | 10 |

A patient adversary who is local and performs only passive attack is assumed. Adversary is initially deployed near the sink node and performs a hop-by-hop back tracing attack to locate the source node. Sink area has the highest number of packet transmissions since sink is the destination node for all packets. This makes the area highly favorable for the adversary initial position.

For energy consumption analysis, the energy consumption model is adopted from [33]. For $l$-bit packet to transmit distance $d$, transmission energy, $E_t$ and receive energy $E_r$ follow equations (1) and (2) respectively.

$$\begin{cases} E_t = lE_{elec} + lE_{fs}d^2, & \text{if } d < d_0 \\ E_t = lE_{elec} + lE_{amp}d^4, & \text{if } d \geq d_0 \end{cases} \quad (1)$$

$$E_r = lE_{elec} \quad (2)$$

### 5.1 Privacy Analysis

Results of the comparative analysis on the privacy performance of the schemes are shown in Fig. 1. The figure shows that the tree-based diversionary routing scheme provides the highest safety period and privacy while shortest path routing scheme provides the lowest safety period. This is because, in tree-based diversionary routing scheme, each source node employs its own diversion path which goes to the end of the network boundary to divert the adversary from real path. The diversion paths are highly effective at confusing the adversary. Shortest path routing scheme provides the lowest privacy because packets are routed through the shortest path. It is easy for an adversary to back trace the shortest path to locate the source node. Constrained random routing scheme provides the second highest privacy level by randomly selecting next hops under constrained offset angles which are highly effective at confusing the adversary.

### 5.2 Energy Consumption Analysis

Sensor nodes are battery operated which means energy of a WSN is a limited resource. Energy consumption and network lifetime of a WSN have a strict inversely proportional relationship. Higher energy consumption means lower network lifetime. This makes energy consumption an important factor to consider during designing of a source location privacy scheme. Many routing schemes for source location privacy in WSNs have a limitation of high energy consumption. For example, in FSR schemes, high volume of packets is required to broadcast in order to provide efficient source location privacy. The high volume of packets in the network leads to increased energy consumption. Energy consumption performance of the routing schemes is shown in Fig. 2. The figure shows total energy consumption of the schemes for transmitting the same amount of packets from source node to sink node. It shows that tree-based diversionary routing scheme consumes relatively much higher energy to transmit same amount of packets. This is caused by the diversion paths which go to the end of the network boundary to divert the adversary from real path. The scheme also uses fake source nodes at the end of each diversion path to periodically send fake packets to confuse the adversary. Sending fake packets consumes a lot of energy. Comparing the results of Figs. 1 and 2, constrained random routing scheme appears to offer a good balance between safety period and energy consumption. Constrained random routing scheme offers safety period and privacy better than randomly selected intermediate node

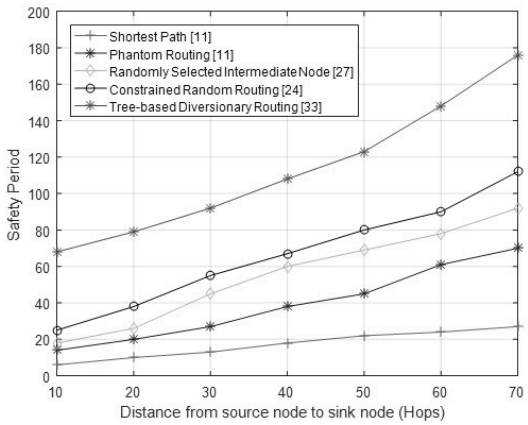


Fig. 1. Safety period for different distances from source node to sink node (Hops). Shortest path routing, Phantom routing, Randomly selected intermediate node, Constrained random routing, and Tree-based diversionary routing schemes.

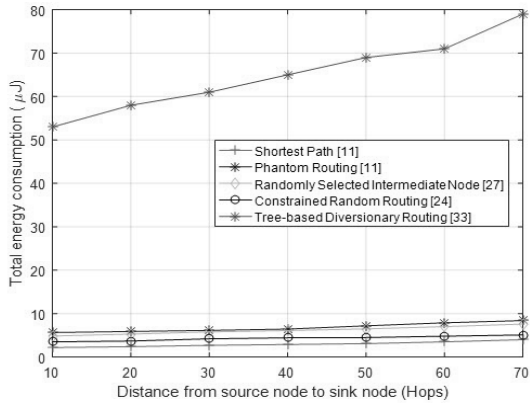


Fig. 2. Energy consumption at different distances from source node to sink node (Hops). Shortest path routing, Phantom routing, Randomly selected intermediate node, Constrained random routing, and Tree-based diversionary routing schemes.

routing scheme but at lower energy consumption. From the analysis results and discussions in section III, angle-based routing schemes such as constrained random routing scheme appear to offer high privacy level with low delivery costs including low energy consumption. One technique that enables constrained random routing scheme to minimize energy consumption is by randomly selecting next hop nodes under constrained offset angles and ensuring that relay nodes are relatively close to the sink node to guarantee the routing paths are relatively short.

## Ⅵ. Challenges and Opportunities

To preserve the source location privacy, the routing schemes employ packet transmission techniques that consume energy. In many routing schemes, privacy increases with the increase in number of packet forwarding instances. More packet transmissions are used to confuse the adversary. Fig. 1 also shows that, the longer the routing path from source node to sink node, the more energy is consumed. Routing schemes with stronger privacy such as tree-based diversionary routing have much higher energy consumption. Moreover, these schemes are incapable of completely securing the source node privacy but they only provide longer safety period. As energy is a limited resource in WSNs, it is necessary to devise new schemes that keep a reasonable energy budget without sacrificing the level of privacy preservation. Angle-based routing schemes such constrained random routing scheme are more energy efficient and they offer a good balance between safety period and energy consumption. Techniques used in angle-based routing schemes such as in the constrained random routing scheme can be applied to other routing schemes to minimize their energy consumptions while maintaining high source location privacy performance.

As shown in table 1, many routing schemes assume a less powerful patient, local, passive adversary starting at the sink node and performs hop-by-hop back tracing attack to find the location of source node. These adversaries perform only passive attacks and do not interfere with the normal operations of the network. This issue remains a challenge and open for future work. Future work should consider more powerful adversaries. Attention must be paid to active adversaries who are highly motivated and can interfere with the normal operation of nodes by injecting, modifying, or blocking packets from a portion of the network. Adversaries can be local with local hearing range or global with a global view of the network[36]. It is more difficult to prevent global adversaries and it remains an open issue for more work.

Many routing based schemes discussed in this work consider static networks where sensor nodes are static. When considering Internet of Things (IoT) applications, new scenarios where everyday objects are fitted with computational power and limited batteries must be considered[37]. Mobility of devices is an important parameter in IoT. Connectivity of the WSN nodes to Internet increases untrustworthy data transmissions in the network and reduces source location privacy. Also, IoT might introduce new types of adversaries. In some IoT scenarios such as smart cities, some applications allow remote control of devices through the Internet. In these applications, it is easier for adversary to eavesdrop on the communication and eventually locate the source node. Source location privacy schemes such as fake source routing and tree-based diversionary routing

schemes are not efficient for IoT scenarios where the number of devices in the network is high. These schemes will cause high energy consumption and reduce network lifetime. The use of fake sources will also introduce many packets which will result in increased packet collisions and reduced delivery ratio. Integrating WSNs and IoT will open doors for new findings in the area of routing schemes for source location privacy where new approaches are required to provide good privacy levels without incurring too much overhead. It is highlighted in [36] that cognitive radio network is one of the promising areas of research to address these challenges.

## Ⅶ. Conclusion

The topic of source location privacy in WSNs has received a lot of attention in recent years. Many routing schemes for source location privacy have been proposed. The routing schemes ensure that, traffic flow in the network does not expose important information about the location of a source node to the adversary. This work has provided a review of the literature and analysis of performance characteristics of some representative routing schemes for source location privacy in WSNs. The work has classified the routing schemes into fake source routing, phantom node routing, intermediate node routing, tree-based routing and angle-based routing schemes. A review on the key features of the schemes showed that each routing scheme has their unique features for preserving source location privacy against a back tracing adversary. These features provide different levels of privacy preservation for each scheme. Performance analysis on privacy and energy consumption characteristics of some representative schemes found that, tree-based diversionary routing scheme provides high privacy but at the expense of very high energy consumption. Constrained random routing scheme has the best performance with a good balance between privacy preservation and energy cost. Most routing schemes assume a less powerful adversary which is passive, has a local view of the network, starts at sink and performs hop-by-hop back tracing attack to find location of the source node. Only tree-based diversionary routing scheme assumes a slightly more powerful adversary. Energy consumption, consideration for more powerful adversaries and integration of WSN and Internet of Things technologies in the designing of routing schemes for source location privacy are among the issues that remain open for future work.

## References

[1] M. S. Bradbury and A. Jhumka, "A near-optimal source location privacy scheme for wireless sensor networks," in *Proc. 16th IEEE Int. Conf. Trust, Secur. And Privacy In Comput. And Commun.*, pp. 409-416, Sydney, Australia, Aug. 2017.

[2] J. Kirton, M. S. Bradbury, and A. Jhumka, "Source location privacy-aware data aggregation scheduling for wireless sensor networks," in *Proc. 37th IEEE Int. Conf. Distrib. Computing Syst.*, pp. 2200-2205, Atlanta, USA, Jun. 2017.

[3] L. C. Mutalemwa and S. Shin, "A new diversional routing scheme to preserve source location privacy in wireless sensor networks," in *Proc. 3rd ICNGC2017b*, pp. 260-262, Kaohsiung, Taiwan, Dec. 2017.

[4] A. Pudasaini and S. Shin, "A new routing strategy for enhancing source-location privacy in wsn," in *Proc. 2016 Symp. KICS*, pp. 172-173, 2016. Retrived June, 25, 2018, from https://www.kics.or.kr/storage/paper/event/20161119_workshop/publish/7B-1.pdf

[5] M. S. Bradbury and A. Jhumka, "Understanding source location privacy protocols in sensor networks via perturbation of time series," in *Proc. IEEE INFOCOM 2017*, pp. 1611-1619, Atlanta, USA, May 2017.

[6] A. Jhumka, M. Leeke, and S. Shrestha, "On the use of fake sources for source location privacy: Trade-offs between energy and privacy," *The Computer J.*, vol. 54, no. 6, pp. 860-874, Jun. 2011.

[7] J. Ren, Y. Li, and T. Li, "Routing-based source-location privacy in wireless sensor networks," in *Proc. 2009 IEEE ICC 2009*, pp. 1-5, 2009.

[8] P. K. Roy, J. P. Singh, P. Kumar, and M. Singh, "Source location privacy using fake source and phantom routing (fsapr) technique in wireless sensor networks," *Procedia Computer Sci.*, vol. 57, pp. 936-941, 2015.

[9] A. Jhumka, M. Bradbury, and M. Leeke, "Towards understanding source location privacy in wireless sensor networks through fake sources," in *Proc. 11th IEEE Int. Conf. Trust, Security, and Privacy in Comput. and Commun.*, pp. 760-768, Liverpool, UK, Jun. 2012.

[10] J. F. Laikin, M. S. Bradbury, C. Gu, and M. Leeke, "Towards fake sources for source location privacy in wireless sensor networks with multiple sources," in *Proc. 2016 IEEE Int. Conf. Commun. Syst.*, pp. 1-6, Shenzhen, China, Dec. 2016.

[11] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *Proc. 2nd ACM Workshop SASN'04*, pp. 88-93, Washington, USA, Oct. 2004.

[12] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in *Proc. 2007 IEEE Int. Conf. Network Protocols*, pp. 314-323, Beijing, China, Oct. 2007.

[13] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in *Proc. 2010 Proc. IEEE INFOCOM*, pp. 1-9, California, USA, Mar. 2010.

[14] W. Wang, L. Chen, and J. Wang, "A source-location privacy protocol in wsn based on locational angle," in *Proc. 2008 IEEE Int. Conf. Commun.*, pp. 1630-1634, Beijing, China, May 2008.

[15] P. Kumar, J. Singh, P. Vishnoi, and M. Singh, "Source location privacy using multiple-phantom nodes in wsn," in *Proc. TENCON 2015 - 2015 IEEE Region 10 Conf.*, pp. 1-6, Macao, China, Nov. 2015.

[16] M. Conti, J. Willemsen, and B. Crispo, "Providing source location privacy in wireless sensor networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1238-1280, Jan. 2013.

[17] I. Shaikh, H. Jameel, B. dAuriol, H. Lee, S. Lee, and Y.-J. Song, "Achieving network level privacy in wireless sensor networks," *Sensors*, vol. 10, no. 3, pp. 1447-1472, Feb. 2010.

[18] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proc. 25th ICDCS '05*, pp. 599-608, Ohio, USA, Jun. 2005.

[19] M. Bradbury, M. Leeke, and A. Jhumka, "A dynamic fake source algorithm for source location privacy in wireless sensor networks," in *Proc. 14th IEEE TrustCom*, pp. 531-538, Helsinki, Finland, Aug. 2015.

[20] C. Gu, M. S. Bradbury, S. Matthew, A. Jhumka, and M. Leeke, "Assessing the performance of phantom routing on source location privacy in wireless sensor networks," in *Proc. 2015 IEEE PRDC*, pp. 99-108, Zhangjiajie, China, Nov. 2015.

[21] L. Lightfoot, Y. Li, and J. Ren, "Preserving source-location privacy in wireless sensor network using star routing," in *Proc. 2010 IEEE GLOBECOM 2010*, pp. 1-5, Florida, USA, Dec. 2010.

[22] A. Thomason, M. Leeke, M. Bradbury, and A. Jhumka, "Evaluating the impact of broadcast rates and collisions on fake source protocols for source location privacy," in *Proc. 2013 12th IEEE Int. Conf. Trust, Secur. and Privacy in Comput. and Commun.*, pp. 667-674, Victoria, Australia, Jul. 2013.

[23] A. Jhumka, M. Bradbury, and M. Leeke, "Fake source-based source location privacy in wireless sensor networks," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 12, pp. 2999-3020, 2015.

[24] W. Chen, M. Zhang, G. Hu, X. Tang, and A. K. Sangaiah, "Constrained random routing

mechanism for source privacy protection in wsns," *Recent Advances on Radio Access and Security Methods in 5G Networks*, *IEEE Access*, vol. 5, pp. 23171-23181, Sept. 2017.

[25] L. Zhang, "A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing," in *Proc. 2006 Int. Conf. Wireless Commun. and Mob. Comput.*, pp. 33 - 38, British Columbia, Canada, Jul. 2006.

[26] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in *Proc. 20th Int. Parall. and Distrib. Process. Symp.*, pp. 1-8, Rhodes Island, Greece, Apr. 2006.

[27] Y. Li, L. Lightfoot, and J Ren, "Routing-based source-location privacy protection in wireless sensor networks," in *Proc. IEEE Int. Conf. Electro/Inf. Technol.*, pp. 29-34, Ontario, Canada, Jun. 2009.

[28] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," *IEEE Trans. Parall. and Distrib. Syst.*, vol. 23, no. 7, pp. 1302-1311, Jul. 2012.

[29] P. Spachos, D. Toumpakaris, and D. Hatzinakos, "Angle-based dynamic routing scheme for source location privacy in wireless sensor networks," in *Proc. 79th IEEE VTC Spring*, pp. 1-5, Seoul, South Korea, May 2014.

[30] Y. Li and J. Ren, "Mixing ring-based source-location privacy in wireless sensor networks," in *Proc. 18th Int. Conf. Comput. Commun. and Netw.*, pp. 1-6, California, USA, Aug. 2009.

[31] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh and Ad Hoc Commun. and Netw.*, pp. 1-9, Rome, Italy, Jun. 2009.

[32] N. Wang and J. Zeng, "All-direction random routing for source-location privacy protecting against parasitic sensor networks," *Sensors*, vol. 17, no. 3, pp. 1-18, Mar. 2017.

[33] 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," *IEEE Access*, vol. 2, pp. 633-651, Jun. 2014.

[34] H. Chen and W. Lou. "On protecting end-to-end location privacy against local eavesdropper in wireless sensor networks," *Pervasive and Mob. Comput.*, vol. 16, pp. 36-50, Jan. 2015.

[35] S. Gupta, P. Kumar, J. P. Singh, and M. P. Singh, "Privacy preservation of source location using phantom nodes," *Inf. Technol.: New Generations, Springer*, vol. 448, pp. 247-256, 2016.

[36] R. Rios, J. Lopez, and J. Cuellar, "Location privacy in wsns: solutions, challenges, and future trends," *Foundations of Secur. Anal. and Design, Springer*, vol. 8604, pp. 244-282, 2014.

[37] J. Lopez, R. Rios, F. Bao, and G. Wang, "Evolving privacy: from sensors to the internet of things," *Future Generation Comput. Syst.*, vol. 75, pp. 46-57, Oct. 2017.

**릴리안 찰스 무타람와** (Lilian Charles Mutalemwa)

2008년 7월 : University of Essex 통신 공학 학사

2010년 12월 : University of Surrey 모바일 및 위성 통신 석사

2012년 1월~현재 : The Open University of Tanzania 컴퓨터공학 보조 강사

2017년 1월~현재 : Chosun University 컴퓨터공학 석박사통합

<관심분야>통신 공학, 네트워크, WSN, 모바일 및 위성 통신

**신 석 주** (Seokjoo Shin)

1999년 : GIST 정보통신공학 석사
2002년 : GIST 정보통신공학 박사
2002년~2003년 : 한국전자통신연구원 이동통신연구단 선임연구원
2009년~2010년 : 미국 조지아공대 교환교수
2003~현재 : 조선대학교 컴퓨터공학교수
<관심분야> 이동통신 MAC, WSN, 스마트그리드, 네트워크 보안 등