On Sensor Network Routing for Cloaking Source Location Against Packet-Tracing

Yeonghwan Tscha*° *Lifelong Member*

ABSTRACT

Most of existing routing methods in wireless sensor networks to counter the local eavesdropping-based packet-tracing deal with a single asset and suffer from the packet-delivery latency as they prefer to take a separate path of many hops for each packet being sent. Recently, the author proposed a routing method, GSLP-w(GPSR-based Source-Location Privacy with crew size w), that enhances location privacy of the packet-originating node(i.e., active source) in the presence of multiple assets, yet taking a path of not too long. In this paper, we present a refined routing(i.e., next-hop selection) procedure of it and empirically study privacy strength and delivery latency with varying the crew size w(i.e., the number of packets being sent per path). It turns out that GSLP-w offers the best privacy strength when the number of packets being sent per path is randomly chosen from the range $[1,h_{s\text{-}b}/4]$ and that further improvements on the privacy are achieved by increasing the random walk length TTLrw or the probability prw that goes into random walk(where, $h_{s\text{-}b}$ is the number of hops of the shortest path between packet-originating node s and sink b).

Key Words : wireless sensor networks, routing for source-location privacy, packet-tracing, active/dormant source

Ⅰ. Introduction

Due to the open nature of wireless communication signals and wide-spread uses of standard communication interfaces, it may be easy for adversaries to eavesdrop or inject packets into the networks[1,2]. Many networks are often deployed in outdoor areas. This also comes with the security problem as attackers may break up or replace the nodes of the networks. Furthermore, there are applications that can not be successfully countered by the encryption-authentication mechanism alone. For instance, wireless sensor networks deployed in battlefields or natural habitats may strongly need to protect the locations of assets(i.e., soldiers or rare wildlives) against the adversaries(i.e., enemies or poachers). If exposed to the opponents, they would be in great danger[3].

The base station is a central part of the sensor network. Data traffics direct toward it and in turn control traffics go out from it. Adversaries can easily analyze the base station centric traffics by the rate-monitoring attacks and deduce the location of it[4]. Once the adversary stays round the base station, he/she may be able to *locally eavesdrop* the incoming packet and to take a movement to the immediate transmitter. By repeatedly taking such hop-by-hop tracing he can approach toward the packet-originating node.

The popular countermeasure on the routing level is to make it difficult for the adversary to trace his way back to the origin of communications(i.e., source)[3]-[6]. The preferred strategies usually adopt random walks to make the paths more irregular and longer, as opposed to the conventional routing that seeks the shortest or lowest-cost paths. Each packet is sent over a separate path for more path diversity. The goal is to send more packets before the source is located by the adversary, where the number of

※ This research was supported by Sangji University Research Fund in 2007.

* Department of Computer Engineering, Sangji University(yhtscha@sangji.ac.kr)(°: Corresponding author)

논문번호 : KICS2008-12-567, 접수일자 : 2008년 12월 26일, 최종논문접수일자 : 2009년 2월 17일

the packets delivered is known as *safety period*(SP)[3,5]. As a pair, there are studies[4,7] to protect the location of the sink but share a similar idea. Since the direction of the packet-forwarding is identical to that of the tracing by the opponent, fake-packet injections are usually deployed to entice the adversary on the wrong place.

The common problem to these studies[3]-[7] is that their schemes take long latencies in transferring packets, as they prefer to deliver more packets via long paths. Other flaw comes from the fact that they regard a single asset in the network. Many of their routing methods force to send each packet over a separate path.

In this paper, we consider a routing method GPSR-based Source-Location Privacy with crew size w(GSLP-w)[8,9], proposed recently by the author, that enhances location privacy of the packet-originating node in the presence of multiple assets, while taking a path of not too long. We give a refined and detailed routing procedure of it and study the performances of location privacy and delivery latency with varying the *crew size* w(i.e., the number of packets being sent per path). We also study how to increase the privacy and performance of GSLP-w by increasing the random walk length.

The rest of this paper is organized as follows. In the next section the related work is reviewed. The routing scheme GSLP-w is given in detail in Section III. The performance evaluation of GSLP-w through simulations is shown in Section IV. Comparisons with PR-SP are made in terms of the number of dormant sources. Further improvements of GSLP-w are also addressed. Our conclusions are drawn in Section V.

Ⅱ. Related Work

The most of studies on routing for source-location privacy in wireless sensor networks to counter the local eavesdropping-based packet-tracing assume a single asset and suffer from the relatively high packet-delivery latency as their routing methods prefer to develope a long route path for each packet being sent[3],[5]-[7].

Fortunately, a new routing method called GSLP(GPSR-based Source-Location Privacy) was introduced in order for taking care of multiple assets while reducing the delivery latency[8]. In it, four modes: **greedy**, **random**, **perimeter** and **retreat** are respectively committed with a certain probability or by default in choosing the next-hop node so that the path diversity(i.e., randomness) is increased while the path length be refrained from excessively lengthening. Particularly the perimeter routing function of GSLP makes detours to avoid the nodes near assets so that they can not be located by the adversary. The result shows that the source privacy measured as SP(Safety Period) becomes significant as the number of assets in the network increases, compared with PR-SP[3,5], a famous source-location privacy routing protocol. In the subsequent work[9], it is given that further improvement of the location privacy as well as reducing the path length is achievable when the number of packets being sent per path(defined as crew size w) is randomly chosen from the range $[(h_{s\text{-}b}/4)+1,(3h_{s\text{-}b})/4]$ where, $h_{s\text{-}b}$ is the number of hops of the shortest path between source s and sink b. In this regard, the revised one is called GSLP-w.

On the other hand, there are studies on destination-location privacy in wireless sensor networks[3,7] as the pair of the source-location privacy. But their results are not directly applicable for source-location privacy. The fake synchronization problem may arise and the path made by LPR[7] may occasionally bring many oscillations such as back-and-forth or zigzag movements during the packet-delivery. In [10], all nodes are independently asked to transmit packets at some frequency regardless of whether there is real data to send or not. Although the scheme may make it hard for the attacker to trace the real source, it is based on the global eavesdropper and introduces too many packet into the network.

Ⅲ. The extended GSLP-w

In this section we describe the details of GSLP-w and derives the expected length of the route path established by it.

3.1 Network and Adversary Model

There exist N sensor nodes and multiple assets in the network. Assets require their locations to be protected against the packet-tracing attack. Each node has the signal transmission(or sensing) range of $r(>0)$, two nodes longer than it away communicate via relay nodes in the multi-hop fashion. We do not consider any specific Medium Access Control(MAC) protocol for our study. The link-layer transmission of each node is based on the omni-directional local(i.e.,1-hop) broadcast. We assume that neither collisions nor errors arise in packet transmissions. This is because in this paper we are to concentrate on the source-location privacy issue like other related work[3],[5]-[7],[11]. All packets are assumed to be encrypted with appropriate secret keys, thus attackers can not interpret the contents of them even though they intercept or eavesdrop on communications.

The adversary can eavesdrop on the local traffic between nearby nodes to trace up the communication source. He/she is able to perform the hop-by-hop tracing toward the packet-originating node, but neither injects any packets into the network nor interferes with communications between nodes. He is also patient enough to wait at a location until he hears the new packet, i.e., the *patient model*[5]. We assume that the adversary always starts his tracing from the base station as other work[3],[5]-[7],[11].

Denote by $L(v)$ the coordinate of some object(for instance, sensor node, asset or adversary) v, i.e, $L(v)=(x_v,y_v)$. We say that the location of source s is captured by adversary χ if and only if $|L(s)-L(\chi)| \leq c$ where, c is a positive number called the *capture range*[3] or *disclosure distance*, and a disk of radius c is said to be *disclosure area*. Like other work[3],[5]-[7], we assume $c=r$, that is, the hearing radius of the adversary is equal to that of the sensor node.

3.2 Terminologies and Assumptions

A node that senses assets appearing within its signal range is called *source*. A source node usually gathers information from them and sends it by a series of packets to the base station. A source node is said to be *active* if it is now in the process of reporting gathered information to the sink, while *dormant* otherwise. The dormant source may be involved in local monitoring of the nearby assets or internal operations like compression of the gathered data[12]. In Fig. 1, for instance, source node m nearest to soldier_1 is active, and sources n and e, respectively, closest to soldier_2 and soldier_3 are dormant where, assets are soldiers: soldier_1, soldier_2 and soldier_3.

The active m makes use of a single path for the delivery of packets to the base station while the attacker tries to capture it by tracing up the path. Considering one-hop tracing per packet, it is seen that three packets have delivered to the base station(by assuming that the attack always begins at the base station). Thus, the adversary has moved three hops closer to m. Since asset soldier_3 is near node e that is two-hop away from the adversary, one more packet from m will cause soldier_3 to be put to battle(the assumption here is that the opponent can locate the asset within the capture distance $\alpha=r$). In the case, soldier_3 must be a victim of the *carelessly* routing method that takes the path passing by near the asset. The soldier would be protected by using a routing strategy that makes a detour around the assets in general.

Multiple nodes may simultaneously discover some assets in common, nonetheless we take it for granted

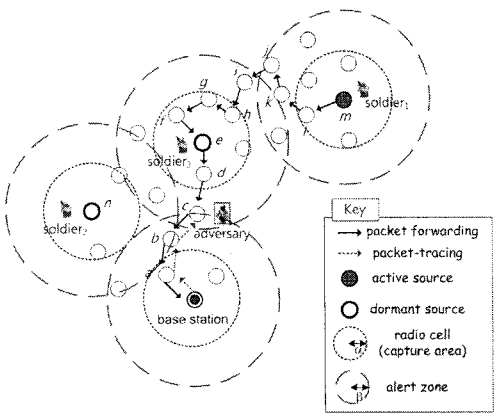


Fig. 1. Illustration of active/dormant source, capture area and alert zone in the presence of multiple assets

that the number of assets is quite small compared to the number of sensor nodes and that assets are sparsely scattered over the network. We assume that *there is a one-to-one relationship between asset and its corresponding source such that no two or more assets lie within the same radio cell.* Hence, to locate some specific source is equivalent to find the corresponding asset, and vice versa.

A simple procedure announcing a certain "be-aware-of" area is individually performed by a node that detects the asset appearing within the sensing range. As in Fig. 1, each source declares a circle of alert range $\beta(>\alpha)$ called *alert zone*, that is enough to protect itself and the corresponding asset against the attacker, and notifies the nodes within the zone of it. Packets announcing the alert zone setup can be diffused within the area by using geocasting[13] or scoped flooding[14]. Thus, every node within the zone is informed of the identity of the source node that declared the zone. And it is given that there exists some asset within β. In routing, the nodes in the alert zone are not allowed to be chosen as the next-hop nodes.

3.3 The Next-hop Selection

GSLP-*w* is a single phase protocol in the sense that every packet undergoes the same next-hop selection procedure shown in Fig. 2. Each time a packet is forwarded, one of four modes: **greedy**, **random**, **perimeter**, and **retreat**. We assume that each node x knows of the coordinate of its neighbor $y \in N(x)$ and whether $y \in AZ(z)$ or not for any z, where $N(x)$ is the set of neighbor nodes of x and $AZ(z)$ denotes the set of nodes within the alert zone set up by source node z.

3.3.1 Greedy Mode

As u receives packet **M** from some adjacent node t, it first checks if **M** is the first crew, i.e., the first packet that is to be sent. Then, the next-hop node is newly chosen and otherwise, **M** is forwarded to the next-hop node specified in the routing table. Denote by p_{rw} the probability that goes into **random** mode from **greedy**. First, generate a random number $p(0<p<1)$and make a transition to **random** mode if $p \le p_{rw}$ or remain. In **greedy** mode, current node u selects its adjacent node v that is the closest to sink b. And then, check whether $v \in AZ(z)$ or not for any z. If $v \in AZ(z)$, then v is ignored and the mode changes into **perimeter** mode. The greedy forwarding helps the path avoid from over-lengthening and converge to the destination.

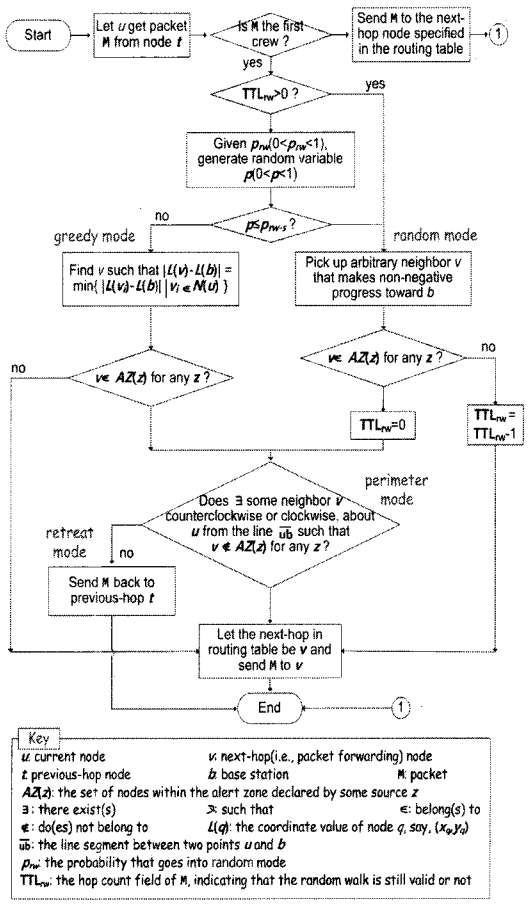


Fig. 2. The next-hop selection strategy GSLP-w

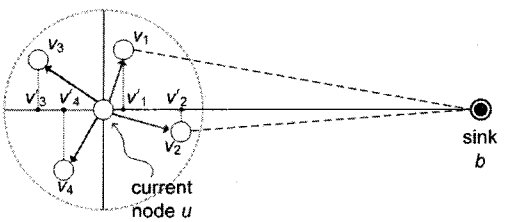


Fig. 3. Positive progress vs. negative progress

3.3.2 Random Mode

The mode **random** is devoted to make the path diversity enhanced, but it is not intended to take back-and-forth or zigzag movements. Progress is defined as the distance between the transmitting node and the receiving node, projected onto a straight-line drawn from the transmitter to the final destination as in Fig. 3. Four nodes v_1 thru v_4 are mapped on the x-axis, respectively, v'_1 thru v'_4. From u's point of view, both v_1 and v_2 yield the positive progress as their corresponding v'_1 and v'_2 are drawn on the positive side of the x-axis, while v_3 and v_4 make the negative progress. In **random** mode, *an arbitrary neighbor that makes non-negative progress is chosen*(this is known as *random progress*[17]), thus the path randomization may come with refraining from over-lengthening the path. It also may alleviate the suspicion that might be perceived by the attacker when he/she traces up the path. Once the mode **random** is committed, certain subsequent next-hop nodes are supposed to be chosen under the same mode for further randomization. The number of hops, defined as *random walk length*, is specified by field TTL_{rw} in the packet being sent. As in Fig. 2, the node u that receives packet **M** first checks the field. If $TTL_{rw}>0$, by default the mode goes into **random** mode, then the next-hop node v is chosen and TTL_{rw} is decremented by one. Otherwise, v is selected in the mode **greedy**. If $v \in AZ(z)$ for any z, then the mode switches into **perimeter** mode in order to newly choose v. In fact, field TTL_{rw} specifies an upper bound upon the random walk length because it is only valid as long as **perimeter** mode does not arise.

3.3.3 Perimeter Mode

Perimeter routing was originally introduced in GPSR[15] to avoid the routing hole that might arise due to the greedy forwarding. In GSLP-*w*, it is borrowed to exclude the nodes that reside within the alert zones from the next-hop selection and to direct the path under development not to come into the zones. This brings detouring of alert zones being encountered during the packet-delivery, and both each source node that has set up its alert zone and the asset within it are protected from the packet-tracing attack because the adversary can not sneak up on them within the alert range β.

In GSLP-*w*, two rules(clockwise and counterclockwise) are alternately designated by the packet-originating node(i.e., active source). If chosen, then it is specified within packet **M** being sent and the same rule is applied for every **perimeter** mode that encounters until the packet is delivered to the destination. Such alternating assignment brings the balanced distribution of paths from side to side in terms of the line segment from u to b[8].

3.3.4 Retreat Mode

This is backtracking to the previous-hop node as the path can not be developed any longer in three modes(**greedy**, **random**, and **perimeter**) at the current node.

Let $v_1, v_2, \ldots, v_m$ be the path from active source $s(=v_1)$ to sink $b(=v_m)$, which is established by the next-hop selection algorithm in Fig. 2. It is evident for the path that $v_i \notin AZ(z)$ for $2 \le i \le m-1$ and any z. Clearly, the following proposition holds.

Lemma 1: Suppose that active source s sends a series of packets to sink b by using the next-hop selection algorithm in Fig. 2, while the attack to capture s starts at b by tracing up the incoming packets. If there exists a path from s to b then, all dormant sources(and their corresponding assets) along the path are protected even though s is captured by the adversary.

3.4 Evaluation Criteria and Path Length

Two criteria: Safety Period(SP) and Delivery Latency(DL)[3], are used for the evaluation of the proposed routing method. Since this paper is concerned with the dormant sources regarding multiple assets, the original SP is re-defined as *the number of packets successfully delivered to the sink from the active source before the source is captured by the adversary, yet providing location-privacy of*

every dormant source along the path. DL is the length of the path in order for measuring the packet-delivery latency. It is well-known that the magnitudes of both SP and DL are directly proportional to the distance between the active source and the sink[3,4,7,11]. The metrics are measured under the condition that the attacker always begins his tracing at the sink. Hence, we use *Normalized Safety Period*(NSP) and *Normalized Delivery Latency*(NDL) for evaluation, which are respectively obtained by dividing SP and DL with the least number of hops between the active source and the sink.

Lemma 2: Let $p_g(0<p_g<1)$ be the probability that the greedy forwarding is committed in choosing the next-hop node as in Fig. 2. Then, the length of the path established by using GSLP-w is $1/(2p_g-1)$ times longer than that of the shortest path between active source s and sink b.

Proof: Denote by $E(k)$ the least number of hops remained toward b after $k(>0)$-consecutive movement from s. Let d be the number of hops of the shortest path between s and b. Initially, we have $E(0)=d$ at s, as there has been no movement yet. Then, 1-hop movement from s leads to the equality $E(1) = E(0)-p_g+(1-p_g) = E(0)+(1-2p_g)$, because *the new movement directs the path under development to be shortest toward b with probability p_g, yet to be non-shortest with probability $1-p_g$.* Thus, the recurrence relations for successive movements are given as follows.

$$\begin{aligned} E(0) &= d \\ E(1) &= E(0)+(1-2p_g) \\ E(2) &= E(1)+(1-2p_g) \\ &\cdots \\ E(k) &= E(k-1)+(1-2p_g) \text{ for } k>0 \end{aligned} \quad (1)$$

This yields to a general formular $E(k) = d+k(1-2p_g)$, where the inequality $p_g>1/2$ is constrained in any movement because the path should converge to the sink. Suppose that, after k-movement, the path converges to sink b. It implies that $E(k)=0$, i.e., $d+k(1-2p_g)=0$. Note here that k is the expected number of hops we want to get. Thus, it is given as follows.

$$\text{Expected length of the path(in hops)} = k = d/(2p_g-1) \quad (2)$$

The expected path length that is normalized by the least number of hops of the shortest path between s and b, i.e., d, is given as follows.

$$\text{Normalized delivery latency(NDL)} = 1/(2p_g-1) \quad (3)$$

Thus, the expected length of the path established by GSLP-w is $1/(2p_g-1)$ times longer than that of the shortest path d. □

Note that the equations above actually state the upper bounds on the path lengths since the possibility that the next-hop node chosen in **random** mode directs the path to be shortest to b is ignored.

Ⅳ. Performance Evaluation

In what follows, we present the performance evaluation results of the proposed GSLP-w through simulations with varying the crew size w.

4.1 Experiments Environment

As we are not aware of simulation tools, yet available in the public domain and dedicated to measuring the location privacy strength and related performances, we developed our own codes for simulations like other work[3,5,6,11]. Written in Java, codes are about 5,400 lines and 541Kbytes of executable files. It covers the routing algorithms of PR-SP and GSLP-w without including the physical and MAC layers. All sources are assumed to be stationary through simulations. Packets are sent according to the low-duty cycle model[3,5], i.e., the subsequent packet from the active source is not sent until its proceeding packet arrives at the destination.

Table 1 shows the simulation configurations. Each simulation uses 100 topologies of the network

Table 1. Simulation configurations

Parameter			Value or Range
Symbol	Meaning		
N	number of the nodes		22,500
average degree of the node			8
$h_{s\text{-}b}$	number of hops between active source s and sink(base station) b		30, 50, 70
N_s	number of dormant sources		0.2%, 0.4%, 0.8% of N
number of runs for each simulation			100
GSLP-w	w	crew size(number of packets being sent per path)	1, 1Q, 2Q, 3Q, 4Q, 2/3Q
	p_{rw}	probability that goes into **random** mode	0.05
	TTL_{rw}	random walk length(hops)	randomly chosen from [5%, 10%] of $h_{s\text{-}b}$(min.2)
	β	alert range	$2r$(r: transmission range)
	α	capture(disclosure) range	r
PR-SP	random walk length(hops)		randomly chosen from [25%, 50%] of $h_{s\text{-}b}$

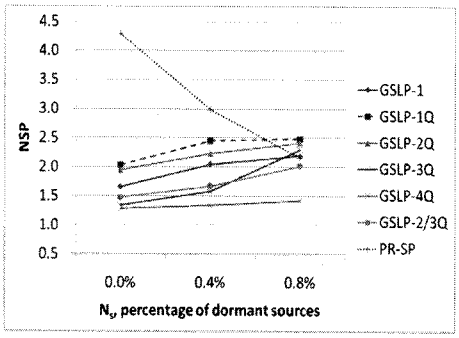
that is comprised of about 22,500 nodes with the average number of neighbors being 8, as other works[3],[5]-[7],[11], where the nodes are randomly placed. However, 80 out of 100 results except the least tens and the largest tens are averaged in order for excluding skewed values. The number of dormant sources N_s is restricted within 0.8% of N because the competitor, PR-SP, hardly develops its own path in case of beyond the bound. The distances(in hops) between the active source and the sink that we consider are 30, 50, and 70, taking account of respectively short-, middle-, and long-distance communications. The alert range β is assumed to be $2r$ for the sake of simplicity. Let us denote by $h_{s\text{-}b}$ the shortest distance between s and b, various fractions of it are considered for choosing w as follows(in the sequel, let us call all instances of GSLP-w as GSLP family).

- GSLP-1: w=1, one packet
- GSLP-1Q: $w \in$1Q, randomly chosen from $[1, h_{s\text{-}b}/4]$
- GSLP-2Q: $w \in$2Q, randomly chosen from $[(h_{s\text{-}b}/4)+1, h_{s\text{-}b}/2]$
- GSLP-3Q: $w \in$3Q, randomly chosen from $[(h_{s\text{-}b}/2)+1, (3h_{s\text{-}b})/4]$
- GSLP-4Q: $w \in$4Q, randomly chosen from $[((3h_{s\text{-}b})/4)+1, h_{s\text{-}b}]$
- GSLP-2/3Q: $w \in$2/3Q, randomly chosen from $[(h_{s\text{-}b}/4)+1, (3h_{s\text{-}b})/4]$

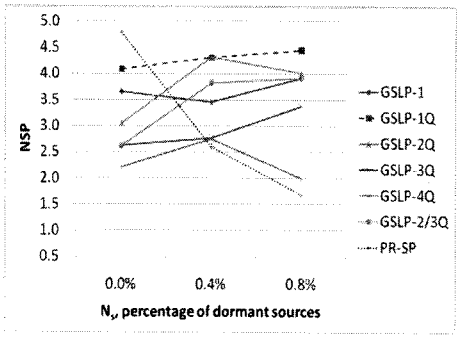
4.2 Normalized Safety Period(NSP)

The impact of the number of dormant sources N_s on NSPs is shown in Fig. 4. The key point is that, as it increases, NSPs of most of the GSLP family slightly grow, while those of PR-SP(shown in dotted lines) drop sharply. The trend stems from that the GSLP family all possess the perimeter routing capability that detours the alert zones(and nodes within them) encountering throughout the packet-delivery, but PR-SP has not. In PR-SP, as the distance between the active source and the sink increases, the possibility that the packet-forwarding confronts the alert zones also increases proportionally. Thus, the dormant sources within the encountered zones are highly vulnerable to the packet-tracing attack. That is, the packet-forwarding is prone to fail before the packet is delivered to the destination. This shortens the safety periods of PR-SP.

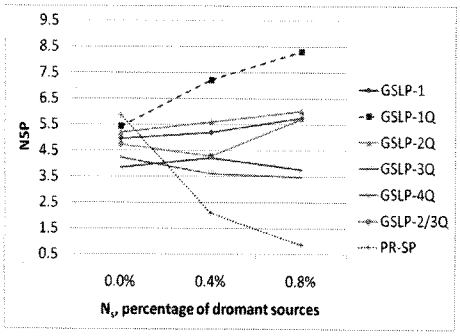
Among the GSLP family, GSLP-1Q(drawn in thick broken line) provides the highest NSPs for all cases. Concerning the crew size w, the more w, the less NSPs in general. But, it is worth noting that the story is peculiar for the case of one packet per path(i.e., w=1). Contrary to previous belief[3],[5]-[7], one packet for each path is not so good as much as GSLP-1Q, and it ranks roughly the middle among the GSLP family. Too large as $w \in$3Q or 4Q and too small as w=1, both are not good choices. On the other hand, GSLP-2/3Q yields NSPs, as expected, roughly between NSPs given by GSLP-2Q and GSLP-3Q.



(a) $h_{s\text{-}b}$=30



(b) $h_{s\text{-}b}$=50



(c) $h_{s\text{-}b}$=70

Fig. 4. Impact of N_s on NSP

Comparing with PR-SP, the longer $h_{s\text{-}b}$ and/or the higher N_s, the better NSPs the GSLP family provide as in Fig. 4(b) and (c). The GSLP family all surpass PR-SP for N_s>0.4% at $h_{s\text{-}b}$=50(Fig. 4(b)) and for N_s>0.2% at $h_{s\text{-}b}$=70(Fig. 4(c)). Interestingly, PR-SP is better than the GSLP family when either $h_{s\text{-}b}$ is relatively small as 30 or N_s is near zero(Fig. 4(a) and (b)). Since p_{rw} is 0.05 and TTL_{rw} is very small as 2 or 3 when $h_{s\text{-}b}$=30, neither the path diversity nor the path length is not achieved. On the contrary, the random walk length of PR-SP varies from 7 to 15, thus PR-SP yields relatively longer and more randomized paths and it provides more increased NSPs. In later, we address that how we can improve NSPs of the GSLP family further in such case.

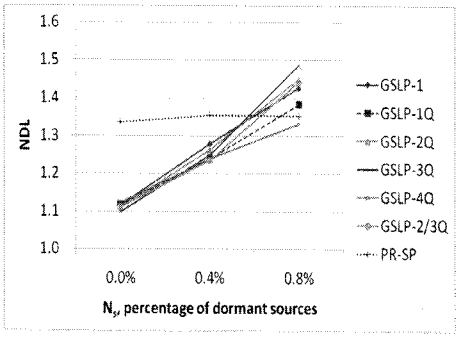
4.3 Normalized Delivery Latency(NDL)

Fig. 5 shows NDLs measured under the simulation configuration in Table 1. Since PR-SP does not take into account of the alert zones during the path development, it gives nearly invariant delivery latencies. NDLs of PR-SP remain below 1.4 for all cases. The GSLP family takes 1.53 on average and a maximum 1.85. Detouring of the alert zones in the GSLP family makes their paths longer than PR-SP. As N_s increases, the deviations among NDLs of the GSLP family slightly increase but still remain within 0.2. The GSLP family show longer NSPs with shorter NDLs when N_s=0.4 at $h_{s\text{-}b}$=50(Fig. 5 (b)) and when 0.0%<N_s<0.4% at $h_{s\text{-}b}$=70(Fig. 5 (c)). From the point of the ratio of NSP to NDL, the GSLP family also offers better results than PR-SP for $N_s \geq$0.4 at $h_{s\text{-}b}$=50 and $N_s \geq$0.2 at $h_{s\text{-}b}$=70.

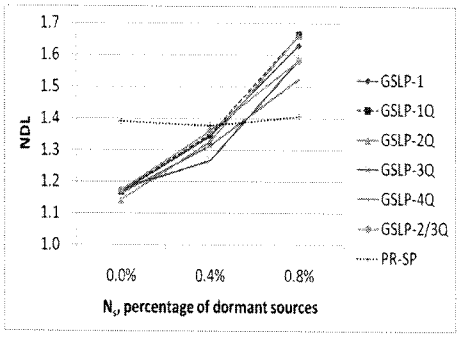
Remarks: Since one of four modes, **greedy**, **perimeter**, **random**, and **retreat** is committed at each next-hop node as in Fig. 2, let p_g, p_p, p_{rw}, and p_r denote respectively the probability that each mode is committed, where $p_g+p_p+p_{rw}+p_r=1$. It is shown that NDL can be obtained if p_g is known(see Equation (3)). However, finding p_g *in priori* is not so trivial in reality because we need to know other probabilities p_p, p_{rw}, p_r, as well. We now want to calculate approximately theoretical NDLs under the simulation configuration given for Fig. 5.

For the sake of simplicity we assume **retreat** mode never happens, i.e., p_r=0, because it very rarely occurs. The number of dormant sources N_s considered in Fig. 5 ranges from 0.0% to 0.8%(with the interval 0.4%) of the total number of nodes N in the network. Therefore, we would like to take it for granted that the probability p_p that **perimeter** mode is committed is proportional to the

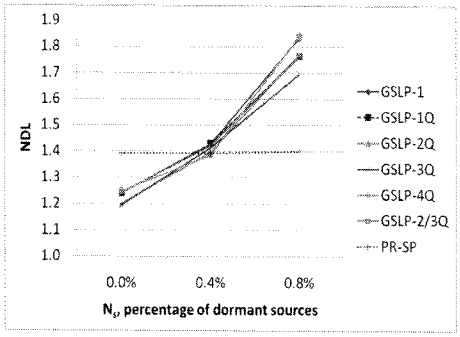
ratio of the areas occupied by alert zones to the radio areas induced by all nodes in the network. More specifically, we note that the area of each alert zone encompassing a dormant source is $\pi\beta^2=4\pi r^2$ while that of an ordinary radion cell is πr^2.



(a) $h_{s\text{-}b}$=30



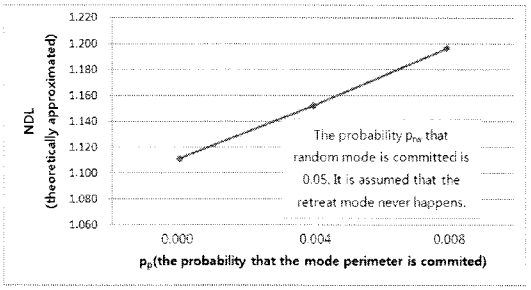
(b) $h_{s\text{-}b}$=50



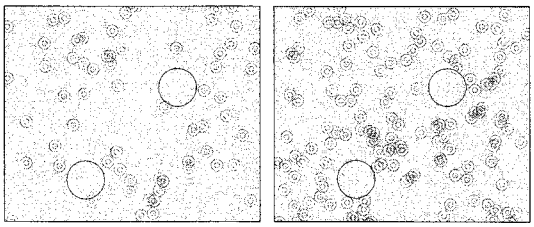
(c) $h_{s\text{-}b}$=70

Fig. 5. Impact of N_s on NDL

Thus, it follows that p_p=0.000, 0.016, 0.0032, respectively, as N_s=0.0%, 0.4%, 0.8% of N. In the meantime, it is seen that p_{rw}=0.05 from Table 1.



(a) Theoretical NDLs(p_{rw}=0.05)



(b) Random placements of nodes(left: N_s=0.4%, right: N_s=0.8%).

Fig. 6. Theoretical NDLs and placements of nodes.

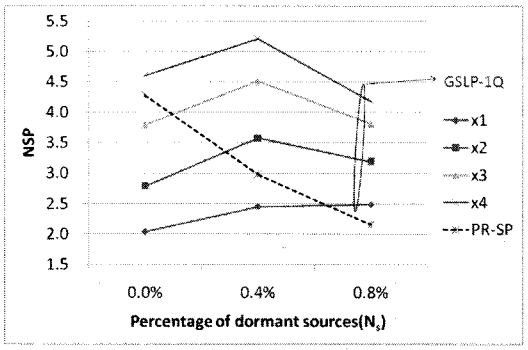
Noting $p_g=1-(p_p+p_{rw})$, we can find theoretical NDLs as depicted in Fig. 6 (a). Note that nodes are dotted while dormant sources are surrounded by double circles: the inner radio cell of radius r and the outer alert zone of range $\beta(=2r)$. Two big circles emphasize the locations where the active source and the sink reside, respectively. As expected, the simulation results are beyond the theoretical numerics. The gap gets larger as N_s and/or $h_{s\text{-}b}$ increases. This can be explained as follows. In simulations the placement of dormant sources are not *evenly* distributed as shown in Fig. 6 (b) and this becomes more outstanding as N_s increases. And the longer $h_{s\text{-}b}$, the larger p_p. These factors lengthen the path lengths and so NDLs in simulation. Besides, **retreat** mode does take place in simulations, even though it is very rare, and this further makes NDLs longer. In this sense the theoretical results can be regarded as baselines, and a more accurate equation should be studied further.

4.4 Further Improvements

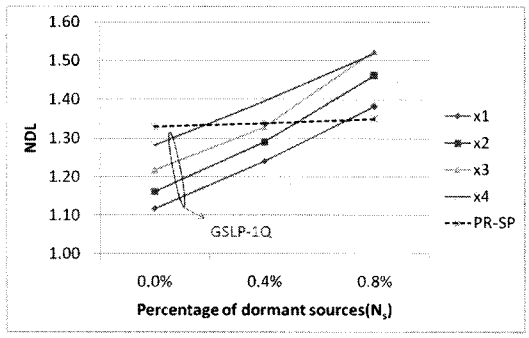
We intentionally consider the case of $h_{s\text{-}b}$=30 because, at this relatively small value, NSPs of the

GSLP family are lower than those of PR-SP as in Fig. 4 (a). We want to observe the impact of parameters p_{rw} and TTL_{rw} on NSPs. Our conclusion drawn by simulations is that increasing TTL_{rw} rather than p_{rw} is more effective.

First, the random walk length(TTL_{rw}) is increased, respectively, as one-folded(=×1), two-folded(=×2), three-folded(=×3) and four-folded(=×4). Thus, new TTL_{rw} ranges are [2,3], [4,6], [6,9], and [8,12], respectively, but still less than 15, the half of $h_{s\text{-}b}$. As shown in Fig. 7(a), NSPs of GSLP-1Q increases until $N_s \leq 0.4\%$, but decreases after that. The reason is as follows. During the first half, the effect of the path diversity by the extended random walk continues, because there exits still a few space to hold the paths that can make detours to avoid the alert zones. But for $N_s \geq 0.4\%$, the network is getting more overcrowded with many dormant sources. This implies that the mode **perimeter** is more frequently committed than **random** mode during the packet-delivery. So the path diversity effect gradually diminishes and it results in the decrease of NSPs. Nonetheless, in comparison with PR-SP, GSLP-1Q provides higher NSPs for $N_s \geq$ 0.3% at two-folded TTL_{rw} and for $N_s \geq 0.1\%$ at three-folded TTL_{rw}. And it offers always higher NSPs at four-folded TTL_{rw}.



(a) NSP



(b) NDL

Fig. 7. Impact of increased TTL_{rw}($h_{s\text{-}b}$=30)

NDLs under the same simulation settings are shown in Fig. 7 (b). As N_s increases, the number of alert zones also does so. Thus, the length of the path made by GSLP-1Q lengthens and NDLs of it, aswell. At N_s=0.4%, either two- or three-folded TTL_{rw} suffices to make GSLP-1Q offer higher NSPs with lower NDLs. From the point of the ratio of NSP to NDL, GSLP-1Q provides better results as long as N_s is greater than 0.2 and TTL_{rw} is doubled or more.

We further measured NSPs by increasing p_{rw} as one-folded, two-folded, three-folded, and four-folded, respectively(the figure of the results is not shown here). GSLP-1Q gives less NSPs than PR-SP at N_s=0.0%. As N_s grows, NSPs of PR-SP drop off quickly while GSLP-1Q begins to surpass PR-SP. As whole, the effect is not so much as that by increasing TTL_{rw}. For instance, the maximum NSP of GSLP-1Q remains 3.50, opposed to 5.21 by increasing TTL_{rw}. We expect that NSPs will further increase at the cost of lengthening NDLs if both TTL_{rw} and p_{rw} are increased.

V. Conclusions

In this paper we have done empirical simulations on the performance of GSLP-*w* that enhances location privacy of the packet-originating node in the presence of multiple assets. We found that GSLP-1Q among the GSLP family provides the best results regarding both the safety strength and the packet-delivery latency. In contrary to previous belief that one packet for each path provides better privacy, our routing method GSLP-*w* offers the best privacy strength when the number of packets being sent per path is randomly chosen from the range $[1, h_{s\text{-}b}/4]$, i.e., $w \in 1Q$. As N_s increases, improvements of NSPs compared to PR-SP become more apparent.

Higher NSPs can be achieved by increasing TTL_{rw} and/or p_{rw}.

As future work we look forward to extending our study to the networks with multiple active sources. Taking into account of the high-duty cycle model, the issue on location privacy in non delay-tolerant networks is also a challenging topic. A concrete equation to accurately calculate the path length made by GSLP-*w* also needs for further work.

References

[1] C. Karlof and D. Wagner ,"Secure routing in wireless sensor networks: attacks and countermeasures", *Ad Hoc Networks*, Vol.1, No.1, pp.293-315, 2003.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, Vol. 52, No.12, pp.2292-2330, 2008.

[3] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," *Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, pp.88-93, 2004.

[4] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," *Proc. of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp.113-126, 2005.

[5] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," *Proc. of the 25th IEEE International Conference on Distributed Computing Systems*, pp.599-608, 2005.

[6] L. Zhang, "A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing," *Proc. of the ACM International Wireless Communication and Mobile Computing Conference*, pp.33-38, 2006.

[7] Y. Jian, S. Chen, Z. Zhang, L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," *Proc. of the 26th IEEE Conference on Computer Communications*, pp.1955-1963, 2007.

[8] G.-W. Yang, H.-J. Lim, Y. Tscha, "Location privacy enhanced routing for sensor networks in the presence of dormant sources," *Journal of KIISE: Information Networking*, Vol.36, No.1, pp.12-23, 2008.

[9] Y. Tscha, "Routing for enhancing source-location privacy with low delivery latency in sensor networks," *The Journal of Korea Information and Communication Society*, Vol.33, No.8, pp.636-645, 2008.

[10] K. Mehta, D. Lie, and M. Wright, 2007, Location privacy in sensor networks against a global eavesdropper, Proc. of the 15th IEEE International Conference on Network Protocols: Session VIII, #4.

[11] Y. Ouyang, Z. Le, G. Chen, and J. Ford, "Entrapping adversaries for source protection in sensor networks," *Proc. of the 7th IEEE International Symposium on a Word of Wireless, Mobile and Multimedia Networks*, pp.23-32, 2006.

[12] S. Puthenpurayil, R. Gu, and S. S. Bhattacharyya, "Energy-aware data compression for wireless sensor networks," *Proc. of the International Conference on Acoustics, Speech, and Signal Processing*, Vol.2, pp.45-48, 2007.

[13] Y.-B. Ko and N. Vaidya, "Geocasting in mobile ad hoc networks: location-based multicast algorithms," *Proc. of 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp.101-110, 1999.

[14] K. Obraczka, K. Viswanath, and G. Tsudik, "Flooding for reliable multicast in multi-hop ad hoc networks," *Wireless Networks*, Vol.7, pp.627-634, 2001.

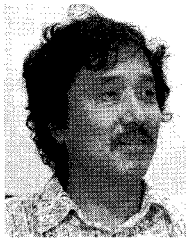
[15] B. Karp and H.-T. Kung, "Greedy perimeter stateless routing for wireless networks," *Proc. of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking*, pp.243-254, 2000.

[16] P. Bose, P. Morin, I. Stojmenovic and J. Urrutia, "Routing with guaranteed delivery in ad hoc wireless networks," *Proc. of the 3rd ACM International Workshop on Discrete Algorithms and Methods for Mobile Computing*

and Communications, pp.48-55, 1999.

[17] R, Nelson and L. Kleinrock, "The spatial capacity of a slotted aloha multihop packet radio network with capture," *IEEE Transaction on Communications*, Vol.32, No.6, pp.684-694, 1984.

Yeonghwan Tscha Lifelong Member



'83.2 Inha Univ., Computer Science(BS)

'85.2 KAIST, Computer Science(MS)

'93.2 Inha Univ., Computer Science(Ph.D)

'85.3~'90.2 ETRI, Senior Researcher

'86.3~'87.2 USA NIST(NBS), Guest Scientist

'93.3~'93.12 ETRI, Invited Researcher(WiBro)

'04.3~'05.2 Boğaziçi(Bosporus) University, Visiting Professor

'94.3~ Currently, Sangji Univ, Dep't of Computer Engineering, Professor

<Research Interests> Network Architectures, Communication Protocols, Network Security