Credit Routing for Source-location Privacy Protection in Wireless Sensor Networks

Zongqing Lu and Yonggang Wen
Nanyang Technological University
{luzo0002, ygwen}@ntu.edu.sg

***Abstract*—Source-location privacy became one of major issues due to the open nature of wireless sensor networks. The adversary can eavesdrop and trace the message movements so as to capture the source. In the paper, first we propose Credit routing to provide the source-location privacy protection. Credit routing is able to route the message within the assigned credit at each message and randomize the routing path. Unlike other location privacy protection schemes in WSN, Credit routing not only can provide strong protection but also precisely control the transmission cost of each message. Then, we propose Hybrid credit routing, which routes the message to the receiver through three phases: totally random walk, forwarding random walk and credit random walk. These phases provide tri-fold protection to prevent the source from being captured by the adversary. We evaluate our proposed schemes based on several metrics including safe period, latency and protection efficiency. The simulation results show that Credit is able to provide the strong and efficient protection compared with other schemes including Phantom, LPR and RRIN. It is also shown Hybrid improves the protection strength and efficiency even further. The performance of Credit and Hybrid can be tuned by the assigned credit. For real application, the credit can be the real power consumption for forwarding the message from the source to the sink. So both Credit and Hybrid can be used to precisely control the power consumption for source-location protection.**

I. Introduction

Recent advances in wireless communication, micro-system techniques and sensing devices have resulted in significant developments of wireless sensor networks (WSNs) [1][2]. A WSN consists of a large number of low-power, cost-effective sensor nodes working together to monitor the physical environment. Each node collects the information from surrounding environment and transports data to a receiver in a multi-hop way. WSNs have a great potential to be widely deployed in near future.

As the increasing of wide deployment of sensor networks, privacy concerns have emerged as the main obstacle to success. Due to the open nature of wireless communication, it is easy for adversary to eavesdrop or inject data packet in WSN. Privacy in sensor networks can be classified into categories: content privacy and contextual privacy [3]. Content privacy refers to the confidentiality of the content of packets transmitted between the nodes in network, which can be threatened by the observation and manipulation of adversaries. This type of privacy can be guaranteed by encryption and authentication [4][5][6]. However, contextual privacy associated with communication has not been thoroughly addressed. In contrast to content privacy, the issue of contextual privacy is concerned about the confidentiality of information associated with the measurement and transmission of sensed data, for example, sender/receiver location information, which might be deduced by analyzing network traffic.

Location privacy is one kind of contextual privacy, which is an important security issue and must be protected in many scenarios. Lack of location privacy can expose significant information about the traffic carried on the networks and the physical world entities. This is particularly true when the sensor network monitors valuable assets since protecting the asset's location becomes critical. For example, on a battlefield sensors can detect the movements of soldiers and report them to the headquarters; an attacker may then be able to use intercepted sensor network communications to determine the exact location of opposing soldiers through traffic analysis. In panda-hunter scenarios [3], the sensor attached at panda sends the information to research center; the hunter may trace the message movements to capture the panda. Unlike the confidentiality of content privacy can be ensured through encryption, it is much more complicated and difficult to adequately address the location privacy issue in senor networks, as sensor networks consist of only low-cost and low-power radio devices [1][2]. WSNs are designed to operate unattended for long periods of time. Battery recharging or replacement may be infeasible or impossible. These characteristics of sensor networks make location privacy protection an extremely challenging research task [7].

In the paper, we focus on source-location privacy protection. We design two credit based routing schemes to provide the protection. Before a message is transmitted to the destination by source node, an amount of credit is assigned to the packet, which can be consumed during the transmission of the message from the source to the destination by network nodes. For Credit routing, the sender first generates a forwarding list according to the remaining credit. The forwarding list includes its neighbors satisfying the condition that the forwarding cost through that neighbor is less than or equal to the remaining credit. Then the sender randomly selects one receiver from the forwarding list. Eventually, the packet will be forward to sink within the assigned credit. Our analysis show that how our credit routing can guarantee the delivery of the packet within the assigned credit and provide the strong and efficient source-location privacy. To further improve the performance, we propose Hybrid credit routing that provides the protection by three different routing schemes. Our simulation results

978-1-4673-2433-5/12/$31.00 ©2012 IEEE

demonstrate that these two routing schemes not only can provide the strong and power efficient source-location privacy protection for two adversary models compared with other existing research work. It is also shown how the credit value can effectively tune the balance between energy cost and provided privacy protection.

The major contributions of this work can be summarized as following:

- Credit routing without the assumption of location information is proposed, which not only can provide strong and efficient source-location protection but also precisely control the transmission cost of each message.
- Hybrid credit routing-three-phase routing scheme is designed to improve the protection performance.
- The extensive simulations, compared with Phantom, LPR and RRIN, show that our schemes have better performance in several metrics including safe period, latency and protection efficiency.

The rest of the paper is structured as follows. Section II discusses the related work. Section III defines network and adversary models. Section IV and V describes our proposed credit and hybrid credit routing schemes for source-location privacy protection. Section VI presents the simulation-based evaluation compared with other research works and we conclude this paper in Section VII.

II. Related Work

During last decade, location privacy in sensor networks has gained more and more attention. Different schemes have been proposed to address this issue. [8] and [9] address traffic-analysis attack that an adversary can deduce the location information by traffic-analysis (or global eavesdropper). The basic idea is that the sensors near the sender (or receiver) have much denser traffic pattern than the sensors further away from the sender (receiver). By collecting the traffic information at various locations in a sensor network, an adversary can compute the traffic densities at these locations, based on which it can deduce the location of the source or sink. However, to perform the traffic-rate analysis, an adversary has to stay at each location long enough so that sufficient data can be gathered for computing the traffic pattern. Since this process takes very long time as the adversary moves from location to location, the adversary prefers another attack scheme, packet-tracing attack.

Phantom is proposed in [10][3] against packet-tracing attack, which provides source-location privacy for panda-hunter application scenario. In phantom routing scheme, the message from source node will be routed to a phantom node along a directed walk based on hop-based approach. Firstly, the source randomly choose a direction, forward or backward to sink, that the message will be sent to. The direction information is stored in the header of the message. Within the assigned random walk distance, every forwarder on the random walk path will forward this message to a random neighbor in the same direction. In this way, the phantom source can be away from the actual source. However, once the message is captured on the random walk path, the adversaries will be able to get the direction information stored in the header of the message. Therefore, the exposure of direction information decreases the complexity for adversaries to trace back to the actual message source.

In order to preserve the performance advantage of shortest path routing while protecting source-location privacy, cyclic entrapment is proposed in [11]. Cyclic entrapment creates looping paths at various places in sensor network. When a message is being routed from the source to the destination along shortest path, the encountered pre-created loop will be activated and will begin cycling fake messages around the loop. This is supposed to cause an adversary to follow these loops repeatedly and thereby enhance the source-location privacy. Both energy consumption and privacy provided by this method will increase as the length of the loops increase. However, as the messages are always forwarded along shortest path, it will be still easy for the adversary with loop detection to capture the source node by following the shortest path.

The broadcasting that mixes valid messages with dummy messages is used to provide source-location privacy in [12][13]. The basic idea is that each node needs to transmit messages continuously. Whenever there is no valid message to transmit, the node will transmit dummy messages. The transmission of dummy messages not only cost a large amount of energy, but also increases the networks collisions and decreases the packet delivery ratio. Therefore, these schemes are not quite suitable for large scale sensor networks.

In [14] and [8], base station location privacy based on multi-path routing and fake messages injection was proposed. In this scheme, every node in the networks has to transmit messages at a constant rate. LPR is another scheme for providing receiver-location privacy, which is proposed in [15][16]. LPR involves location privacy routing and fake message injection. In LPR scheme, the neighbors of the message forwarders are categorized into closer list, consisting of neighbors that are closer to the destination, and a further list, consisting of neighbors that are farther from the receiver. The sender randomly chooses one list, and also randomly select one node from the list as next hop of the message. Fake message is randomly injected into network and forwarded to opposite direction of real message by the nodes along the forwarding path. LPR is supposed to make the adversary harder to trace the movement of the real message. However, even with fake message injection, LPR cannot protect the source-location privacy well. The way of fake message injection actually cannot enhance the source-location privacy for the sophisticated adversary.

In [7], RRIN is proposed to provide source-location privacy in sensor network. In RRIN, the message is routed to a randomly selected intermediate node before the message is transmitted to sink along shortest path. Actually, the idea is similar with Phantom. However, as RRIN might not be able to provide the global source-location privacy, Li et al. present other two routing schemes that provide routing through multiple randomly selected intermediate nodes based on angle

and quadrant to improve the performance. Unfortunately, these two schemes are based on the assumption that source node knows the locations of the intermediate nodes and the receiver. This assumption makes these two schemes unapplicable to real application scenarios, becauase in most case of wireless sensor networks, sensor nodes only know the local location information (only its neighbors).

All the existing schemes, which are proposed to protect location privacy either by random walk, or random fake message injection, or both, never consider about the exact energy cost for forwarding a message to the destination. The cost can be extremely high if the random walk goes through the entire network. However, as sensor networks only have constrained energy resource, it is very important to exactly know how much energy will be spent on source-location privacy protection. Moreover, previous works also fall or ignore to evaluate the metric-protection efficiency (safety strength/energy cost) of their proposed schemes. In this paper, we propose two credit based routing schemes for providing source-location privacy protection. The credit can be used to accurately control the energy cost of the message transmission and tune the tradeoff between power consumption and protection strength.

III. Network, Adversary and Simulation Models

A. Network Model

In the paper, we use the sensor network that consists of a sink node and a number of sensors, deployed in a certain region. The information of the sink is public. It is the destination that all data messages will be transmitted to through multi-hop routing. Each node has a transmission range of r. If the distance between two sensors is no more than r, they can directly communicate with each other. Source nodes are those sensors that report data to the sink. Any sensor can become a source node as long as it has something to report to the sink. We assume that, after a sensor becomes a source node, it periodically sends packets to the sink in a certain period of time. During the setup of sensor network, minimum-cost forwarding solution [17] is used to set up the minimum cost path to the receiver and gain the information of its neighbors for each sensor. The process is started by sink which broadcasts a beacon message into network. When a sensor received this message, it will compute the minimum energy costs to reach the sender and sink according to the information included the message. Then it will include its minimum cost to the sink in beacon message and broadcast it. Eventually, every sensor node will acknowledge the information including its minimum cost to reach the sink, next hop on the minimum-cost path to sink, its neighbors, the cost to reach each neighbors and the minimum cost to the sink of its neighbors. Notice that we use the distance between two nodes as the transmission cost in simulation. However, the transmission cost can be any other metric, such as hop count. For real application, the minimum energy cost to reach the sender can be calculated by including the transceiver information, transmission power and so on into beacon message. The node can adjust the transmission power and use the minimum transmission power to reach the specific neighbor.

B. Adversary Model

We assume that the content of each message will be encrypted. The adversary can only overhear the transmission of message. We define the characteristics of an adversary as follows, some of which are borrowed from the "panda-hunter" model in [3]:

- The adversary has unbounded energy resource, adequate computation capability and sufficient memory for data storage.
- The adversary will not interfere with the proper functioning of the networks, such as modifying packets, altering the routing path, or destroying sensor devices, since such activities can be easily identified.
- The adversary is equipped with powerful devices, such as antenna and spectrum analyzer, which can be used to measure the arriving angle and the received signal strength of a message. Based on the above two measurements, the adversary can identify the location of the immediate sender. However, we assume that the adversaries are unable to monitor the traffic of the entire network.
- The adversary is able to visually find the source when it is close enough.
- The movement of the adversary is far slower than the transmitting speed of a message in the network. The adversary can only trace the flow by one hop for one message transmission.

As the information of sink is public, an adversary initially waits for eavesdropping a message at the sink. As soon as it detects a new packet, it can determine the location of the immediate sender for tracing the source. Then it moves to that location and waits there for the next packet.

In the paper, we assume there are two adversary models: patient adversary model and cautious adversary model.

The adversary behaves differently according to the chosen model. In patient adversary model, whenever the adversary eavesdrops a packet transmission, it will move the immediate sender and wait there until it detects another message. The adversary patiently behaves in this way until it captures the source node.

In cautious adversary model, the adversary will return back to previous visited node if it waits for a given period at some location and does not detect any valid packet transmission. We borrow the definition of this behavior from [18]. The path that the adversary visited is defined as $V = n_1, n_2, ..., n_{c-1}, n_c$, where n_c is the current location of the adversary. When the adversary has not detect any new message transmission within a certain interval at n_c, it will move back along V to n_{c-1}, delete n_c in V and then wait there for new packet. We define F as the set of locations that the adversary has visited and moved back. To avoid invalid tracing, when the adversary traces back from n_c to n_{c-1}, it will add n_c into F, and ignore packets coming from any location in F. To avoid the interference of

fake messages injected in network, the message sent by the sensor that is nearer to the sink than the current location of the adversary will not be considered as valid message, and the message sent by the sensor that the adversary has visited more than specific times will also not be seen as valid message. Furthermore, the adversary can avoid getting lost in a loop with loop detection techniques.

C. Simulation Model

In the paper, we do the simulation in Qualnet and use the network with 1000 nodes distributed in a square area of size 750×750 meter. We evaluate our credit routing schemes with other three methods for location privacy protection-Phantom [3], LPR [15] and RRIN [7]. We compare with those schemes in several metrics including safe period, latency and protection efficiency for both patient adversary and cautious adversary. We define safe period as the messages sent by the source continuously before the adversary captures the source (the source transmits the message in certain frequency). Safe period stands for protection strength. We also introduce protection efficiency as the ratio between safe period and average power consumption per message, to evaluate the efficiency of different privacy schemes.

IV. Credit Routing for Source-Location Privacy Protection

A. Credit Routing

The minimum-cost path from each sensor to the sink is established before any message transmission from source as discussed in network model. Although this path can be used to route message to the sink, as the path is fixed, it is very easy for the adversary to trace back to the source hop by hop. Like other routing schemes for location privacy, we also choose to randomize the path from the source to sink, which the message actually goes through. However, unlike other schemes that cannot control the energy cost spent on the random path, our routing scheme can accurately regulate the cost spent on providing location privacy.

Credit routing works as follows. When a sensor forwards a packet, the sensor needs to decide how much extra cost will be spent for location privacy, defined as δ. The network is supposed to spend less than or equal to $\alpha = c_s + \delta$ credit to forward the packet to the receiver. We denote the source node as s, the minimum cost to the sink as c_s, and its neighbors as s_n. Then the sensor sorts its neighbors into the forwarding list, which includes the neighbors that have less or equal cost than the assigned credit to route the packet to the sink. The cost of the neighbor to route the packet is defined as the sum of c_{s_i} and d_{ss_i}, where d_{ss_i} is the cost to reach its neighbor s_i. Then, it selects one neighbor randomly from its forwarding list as the next hop. Because the next hop is randomly chosen, the routing path for packets from the source node to the destination is not fixed. Besides the information acquired by the sink, the packet also carries the remaining credit. Before transmitting the packet to the chosen next hop, the sender will update the remaining credit α, $\alpha = \alpha - d_{ss_i}$.

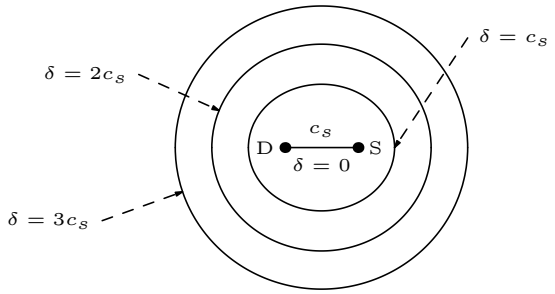


Fig. 1: Credit Routing Area

As α is no less than the minimum cost to the receiver at each sender, the packet will be transmitted to the receiver eventually. When there is no extra credit assigned to the packet transmission, the packet will be forwarded from the source to the sink along minimum-cost path. For each transmission, only the neighbor that is next hop of minimum-cost path will be included in the forwarding list according to the condition. When there is extra credit attached to the packet, the transmission path will deviate from minimum-cost path. The more credit assigned, the more deviation from minimum-cost path the transmission path will make. That is because the more neighbors will be included into forwarding list when there is more credit assigned at the packet.

B. Security and Mathematical Analysis

In Credit routing, on one hand, the next hop is randomly selected from the forwarding list by the sender, where all the nodes satisfy the routing requirement; on the other hand, the forwarding list of each node varies according to the remaining credit. This makes it extremely hard for the adversary to trace the message on randomly selected routing path. So Credit routing provide strong source-location privacy protection. As the packet must be delivered within the assigned credit, the packet is constrained in certain area according to the credit assigned. As shown in Fig. 1, S and D are the source and the destination respectively, and the minimum routing cost between them is c_s. When $\delta = 0$, the routing area is just the minimum-cost path from the source to the receiver. When the credit δ is increased, the routing area is also increased as shown in Fig. 1, which details the routing areas for $\delta = c_s$, $\delta = 2c_s$ and $\delta = 3c_s$.

Assuming the receiver is at coordinate $(0, 0)$ and the source is at coordinate $(c_s, 0)$, the credit routing area includes all the points that satisfy the condition:

$$\sqrt{x^2 + y^2} + \sqrt{(x - c_s)^2 + y^2} \leq c_s + \delta \qquad (1)$$

In credit routing, the real routing path can go through any node in the routing area from the probability perspective. If there is sufficient credit given to the message, the message can be sent out from any direction of the source, the message goes through path randomly chosen between the source and the sink, and the message can also be received from any direction of the sink. So, it is extremely difficult for the adversary to trace back or capture the source node based on an individual

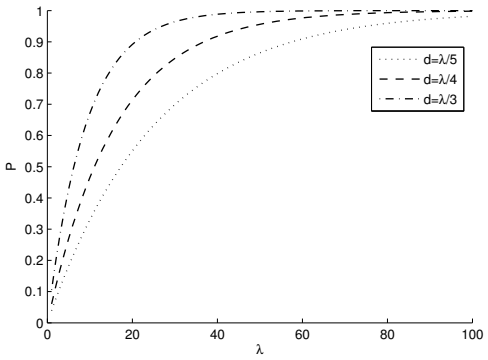


Fig. 2: Asymptotic Probability

traffic monitoring. This is because the probability that the message use the repeated routing path is very low for large scale sensor networks.

To our best knowledge, all the existing work for location privacy in sensor network does not take the management of transmission cost of message into consideration. For example, in RRIN, the intermediate node is randomly selected in the entire network, so the power consumption is naturally out of control. In Phantom, although the random walk distance can be used to control the power consumption of transmissions between the real source and the phantom source, the cost from phantom source to the sink is undetermined and variant. In LPR, the message lingers on the path from the source to the sink either forward or backward. In CEM [11], the fake message is cycled in pre-created loop. Without the control of power consumption for providing location privacy, the energy source of node will be depleted rapidly, and it is especially true in sensor networks. However, Credit routing is the first work that provides the control of power consumption of message transmission in terms of location privacy in sensor networks. As discussed above, δ is designed to exactly control how much energy will be spent on providing location privacy.

Unlike RRIN, where an intermediate node is selected based on the node location information to route the message to the sink, our credit routing does not assume any location information knowledgeable by the nodes, since the message is routed to the sink only based on remaining credit. Also, unlike the directed walk used in Phantom, our scheme does not leak any direction information to the adversaries, even if the message content is captured by the adversary. Since the only information carried in the message is the remaining credit, the adversary cannot infer the distance to the source from the remaining credit, since the source can assign the different credit for each message. Therefore, besides our credit routing can accurately control the power consumption for source-location privacy routing, it can also protect source-location privacy without any other assumption.

As analyzed in [3], the asymptotic probability of the location of packet being within the distance d hops to the source, after λ random walk steps from the source, is given by

$$P = 1 - e^{-d^2/\lambda} \tag{2}$$

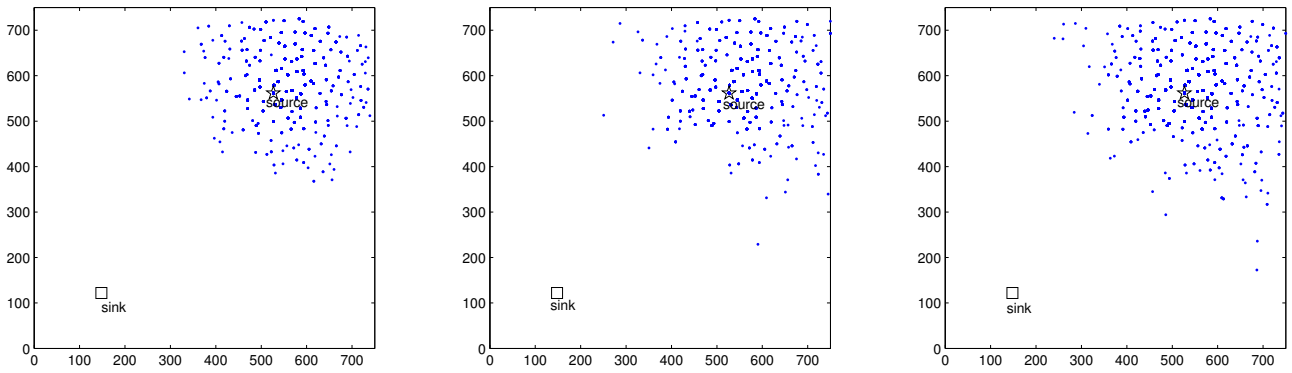
As shown in Fig. 2, when $\lambda > 40$, the probability of being within the distance $\lambda/3$, $\lambda/4$, and $\lambda/5$ tends to 1 , when $\lambda > 40$, $\lambda > 60$ and $\lambda > 100$, respectively. Although we can assign more credit to the packet for random walk and it will still take the packet far from the source, the efficiency is decreased significantly, as in Fig. 2, from $1/3$, $1/4$, to $1/5$. Thus, most of the credit consumed near the source is certainly inefficient. From above analysis, we can see the packets cluster around the location of the source before transmitted to the sink. This can make the real routing paths of the packets overlapped more frequently.

We carry out a small simulation to show the distribution of nodes that begin to route the message along minimum-cost path to sink. The sink and source are at the locations as shown in Fig. 3. We send 500 messages from the source to the sink by Credit routing with $\delta = c_s$, $\delta = 2c_s$, $\delta = 3c_s$. As shown in Fig. 3, the nodes scatter around the source node and the scattering area increases with δ. However, as discussed above, the more credit could not make the message all over the routing area as theoretically analysis in Fig. 1. So the adversary will probably trace the overlapped minimum-cost paths to the locations near the source and it will eventually capture the source.

V. Hybrid Credit Routing for Source-Location Privacy Protection

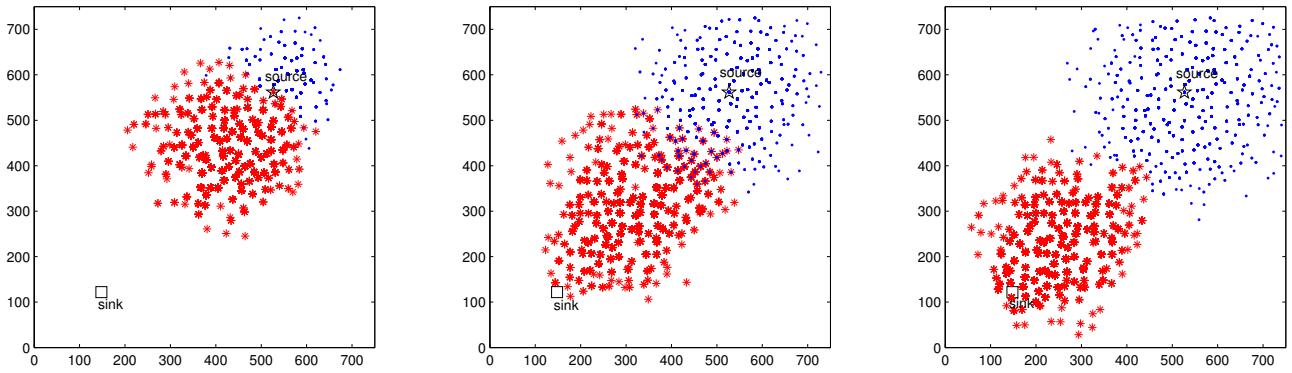
As discussed above, although the more credit will make the message go farther from the source before the message is transmitted along minimum-cost path to the sink, the more credit makes the inefficiency of spending and the safe period is not significantly increased with the increased credit as before when δ is small. To tackle this issue of inefficient random walk, in Phantom the directed random walk is proposed, which routes the message from the source either to the direction towards the sink or backwards the sink. However, the phantom source towards to the sink will expose the sink more quickly and the phantom source backwards to the sink will consume much more energy. In RRIN, one or multi total random selected nodes are used as the intermediate nodes to route the message to the sink. However, RRIN assumes the nodes know the location information of the entire network, which makes RRIN not widely applicable, only for special networks. LPR provides the location privacy by randomizing every forwarding step either towards the sink or backwards the sink and by injection of fake message. However, as we will shown in evaluation, the injection of fake message cannot enhance the protection strength under cautious adversary.

In this section, we propose Hybrid credit routing. Unlike Credit routing that just spends all the extra credit near the source, the idea of Hybrid credit routing is to redistribute the expense of credit so as to resolve the inefficiency of random walk from the source. We divide the extra credit δ into three parts, which will be spent on three different routing phases. The first phase is totally random walk initialized by the source,



(a) (b) (c)

Fig. 3: Distribution of the nodes that start minimum-cost path routing in credit routing, when δ is c_s (a), $2c_s$ (b) and $3c_s$ (c), respectively.



(a) (b) (c)

Fig. 4: Distribution of the nodes that initiate forwarding random walk (in blue dot) and the node that start credit random walk (in red star), when p_r is 0.3 and δ is c_s (a), $2c_s$ (b) and $3c_s$ (c), respectively.

where the sender will randomly choose any neighbor as next hop. This process will continue until all the credit at this phase is fully consumed. Then the second phase will begin, which is called forwarding random walk. During forwarding random walk, the sender will randomly take one node of forwarding list as next hop, which consists of the neighbors that has less cost (or equal) to the sink than the sender. After forwarding random walk, the routing process enters the last phase-credit random walk. Credit random walk works in the same way as Credit routing as discussed in Section IV.

Hybrid credit routing spends the credit more efficiently than credit routing and provides tri-fold protection for source-location. First, totally random walk phase can diversify the paths and the directions the messages go along from the source. This makes the adversary difficult to trace back to the source even if the adversary is near the source. Then, forwarding random walk randomizes the forwarding path from the end point of totally random walk to the start of credit random walk. The phase enhances the tracing complexity from the location near the sink to the location near the source. Finally and most importantly, credit random walk phase will provide the variety of paths and directions in the way the messages arrive at the sink. As the message has been already forwarded near the sink by forwarding random walk phase, more credit can be used to broaden the input ways of message at the sink. Unlike in other source-location privacy schemes, where the traffic at the sink exposes the direction towards the source, the traffic in hybrid credit routing can come from any direction. So, credit random walk phase makes the adversary much more difficult to trace the direction of the source even if at the beginning of the tracing process when the adversary is waiting at the sink.

In order to successfully deliver the message and maximally provide location privacy, the credit must be distributed properly. From the probability aspect, by considering an extreme case that the message is always forwarded in the direction opposite the sink during totally random walk, to guarantee the delivery of the message, the percentage of total extra

credit δ given to totally random walk phase, p_r, cannot be more than 50%, and for credit random phase, the extra credit assigned, p_c, could not be less than p_r, where p_r and p_c are system parameter to adjust the extra credit distribution. To make it easier, we use $p_r = p_c$, so the share of the credit is δp_r, $\delta(1 - 2p_r)$, $\delta p_r + c_s$ for totally random walk, forwarding random walk and credit random walk, respectively. By adjusting the value of p_r , one can get the best location privacy for different network scenarios.

We also make a simulation to show the distribution of the nodes (FORWARDER) that initiate the forwarding random walk phase and the nodes (WALKER) that start the credit random walk. We use the same sink and source node, which sends 500 messages to sink using Hybrid credit routing. As shown in Fig. 4, FORWARDERs are clustered around the source node just like the initiator node of minimum-cost path routing in Credit routing. And the clustered area increases when δ is increased. These nodes provide the protection for source location, when the adversary is near the source node. When δ is small, WALKERs scatter near the source in Fig. 4a. However, they are located far away from the source and scattered around the sink when δ is increased. As discussed above, these scattered nodes near the sink will delude the adversary into different directions, thus provide the protection at the beginning of the tracing process.

VI. Performance Evaluation

We evaluate the performance of our Credit routing and Hybrid credit routing based on three criteria: safe period, delivery latency, and protection efficiency. We do the simulations in the network described in Section III-C. We compare our schemes with Phantom in [3], LPR in [15] and RRIN in [7] for both patient and cautious adversary models. Although LPR is originally designed to receiver location privacy protection, it can also be adapted to protect source-location. For Phantom, we assign the random walk distance of directed random walk phase to 25 hops. And in LPR, we set the probability of backward transmission to 0.35, which is the value with the best protection performance in [15]. For RRIN, we set the minimum distance of between source node and intermediate node to be 100 meters. In simulation, the source continuously transmits message to sink node in certain frequency. The adversary is waiting for the message at the sink, when the simulation starts.

A. Safe Period

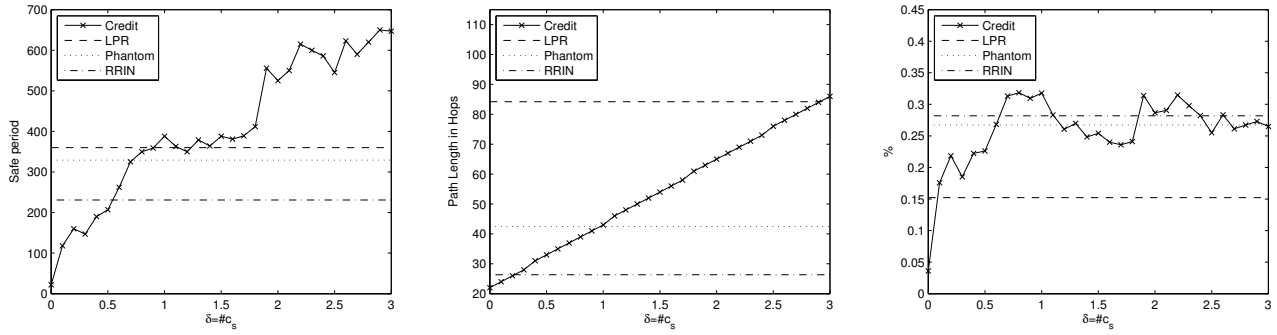
Fig. 5a shows the simulation results on safe period by RRIN, Phantom, LPR and Credit routing with varying δ. For RRIN, the source is captured after 230 messages delivered. LPR and Phantom provide the comparable protection and improve the safe period to more than 300. Credit routing provides different safe period with varying δ. When δ is 0 (no extra credit assigned), the message just follows the constant minimum-cost path between the source and sink, which does not provide any privacy protection. But this has the the lowest delivery latency and energy cost. The safe period increases rapidly when δ varies from 0 to c_s. When δ is from c_s to $1.6c_s$, the safe period is relatively stable and just more than LPR. When δ is more than $1.6c_s$, again, the safe period augments quickly. Since $\delta = 1.6c_s$, Credit routing provides the strongest protection among all the compared schemes and the safe period continuously increases with δ. In real application, as the credit is total energy cost of transmitting a message from the source to the sink, the protection strength is enhanced with more energy spent in Credit routing. However, the spending is under precise control.

Fig. 6a shows the protection strength comparison between Credit and Hybrid routing with varying p_r, when $\delta = 2c_s$. When p_r is small, most credit is consumed during forwarding random walk phase. Very little credit are distributed on totally random walk and credit random walk. So, FORWARDER and WALKER are near the source and the sink, respectively. Thus Hybrid cannot provide the strong protection only by forwarding random walk phase. When p_r increases, FORWARDER and WALKER are scattered at large area around the source and sink, respectively, as discussed in Section V, which enhances the protection strength. When $p_r = 0.3$, we get the peak value around 800. However, when p_r is further increased, less credit is assigned to forwarding random walk, which makes the scattered areas of FORWARDER and WALKER are both around the source. The diversity of direction that the message arrive at the sink is merely provided. That is the reason why the safe period of Hybrid falls bellow that of Credit routing when p_r is more than 0.4.

Table I presents the safe period comparison of all the schemes under cautious adversary. For LPR+fake, we use the parameter setting from its original paper. The probability of generating the fake message at each forwarder is 0.4, the backward probability is 0, and the maximum number of hops the fake message will be forwarded away from the receiver is 7. The credit assigned at Hybrid and Credit routing is both $\delta = 2c_s$, and for Hybrid $p_r = 0.3$. As shown below, Phantom and RRIN provide similar safe period as in patient adversary. LPR+fake cannot provide strong source-location protection under our cautious adversary model. As the backward probability is set to 0, the safe period of LPR+fake is even worse than LPR. Although the safe period of Credit and Hybrid is not strong as in patient adversary model, both of they are still more secure than other schemes.

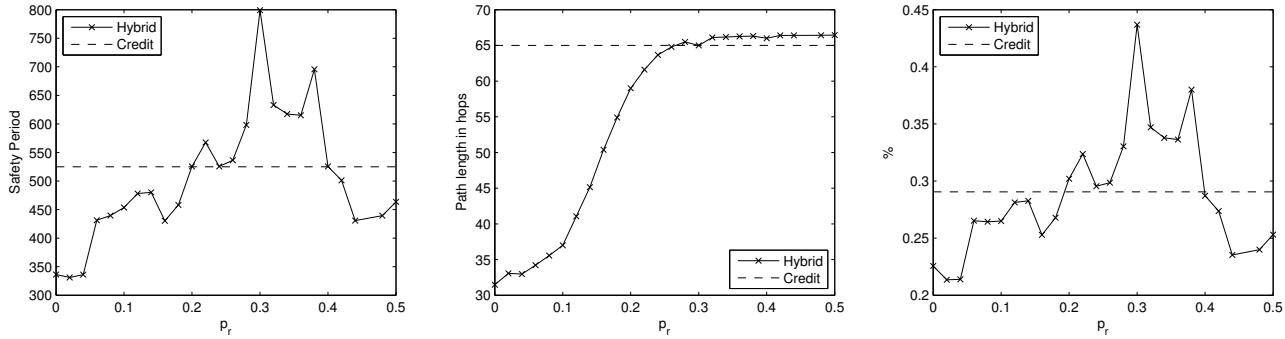
	Safe Period
LPR+fake	250
Phantom	272
RRIN	283
Credit	364
Hybrid	477

TABLE I: Safe period under cautious adversary model



(a) Safe Period (b) Latency (c) Protection Efficiency

Fig. 5: Performance Comparison among Credit Routing, LPR, Phantom and RRIN in safe period, latency and energy efficiency with varying δ under patient adversary model



(a) Safe Period (b) Latency (c) Protection Efficiency

Fig. 6: Performance Comparison between Hybrid and Credit Routing in safe period, latency and energy efficiency with varying p_r under cautious adversary model. $\delta = 2c_s$

B. Latency

Delivery latency is the time a message takes to move from its source to the destination under a certain routing protocol. In our simulations, it is measured as the average number of hops that the messages from source node traverse before reaching the sink. As shown in Fig. 5b, RRIN has the smallest delivery latency compared with LPR and Phantom, because the messages in RRIN always follow the shortest path to reach both intermediate node and the receiver. For other schemes, the messages may follow longer paths due to path randomization introduced by the routing process. For LPR, as the message goes back and forth on the path from the source to the sink according to the backward probability, the latency of LPR is long than others.

For credit routing, when δ is 0, there is no extra credit assigned to the message transmission. So the message will follow minimum-cost path to reach the sink. This gives the shortest message latency. When δ is increased, the deviation from minimum-cost path raises, thus the message latency increases. As shown in Fig. 5b, the relation between δ and message latency is linear, because the messages always consume all the credit assigned to reach the sink in credit random walk. More credit leads to more transmission hops before the message arrives at the receiver.

In Hybrid credit routing, when p_r is small, most of the credit is assigned to forwarding random walk. As next hop is chosen from the neighbors that have less cost to reach the receiver in forwarding random walk, when most credit is assigned to forwarding random walk, the message trends to reach at receiver without spending all the credit. That is the reason why the latency is short when p_r is small. As shown in Fig. 6b, the latency increases quickly with p_r varied from 0 to 0.3. After $p_r = 0.3$, it trends to be smooth that means all the credit assigned are totally consumed during the message transmission. Meanwhile, in Credit routing, all the credit is assigned to credit random walk, which always spends all the credit during message transmission.

C. Efficiency

For most applications in wireless sensor networks, the energy is a constraint. So the protection efficiency is another important metric to be evaluated. We define the protection efficiency as the ratio between protection strength (safe period) and average energy cost per message. For the applications

where safe period and energy cost are both important, they should choose the most efficient protection scheme. As shown in Fig. 5c, among LPR, Phantom and RRIN, LPR is the worst case, because the message lingers on the path from source to receiver. RRIN and Phantom are similar as they both includes shortest path transmission, which includes the transmission from source to intermediate node and from intermediate node to sink in RRIN, and from phantom node to receiver in Phantom.

In Credit routing, protection efficiency varies with δ. There are two interesting ranges, one is around $\delta = c_s$, another one is around $\delta = 2c_s$. The efficiency of these two ranges is higher than all other schemes, because the protection strength raises dramatically during these two ranges. Although the protection strength still increases when $\delta > 2.4c_s$, the efficiency goes down. As discussed in Section IV-B, this is because of the inefficiency of credit spending.

For Hybrid credit routing, as shown in Fig. 6c, the efficiency varies with p_r just like that in safe period. The range, from $p_r = 0.3$ to $p_r = 0.4$, is our interested. In this range, Hybrid credit routing not only provides strong privacy protection, but also gives high protection efficiency.

VII. Conclusion

In the paper, first we propose Credit routing for source-location privacy protection. An amount of credit is assigned to the message when it is transmitted to the sink from the source. The message is routed to the sink by randomly choosing routing path based on the remaining credit restriction. The randomized routing paths make it very hard for an adversary to trace back to the location of the source. Unlike other location privacy protection schemes in WSN that do not take energy cost into consideration, Credit routing not only can provide strong protection but also precisely control the transmission cost of each message. Then, Hybrid routing is proposed to improve the protection strength and efficiency of Credit routing, which has three routing phases. By adjusting the distribution of credit at each routing phase, Hybrid can achieve much better performance than Credit routing. We perform extensive simulations to evaluate Hybrid and Credit routing with other three schemes, Phantom, LPR and RRIN based on the metrics: safe period, latency, and protection efficiency. The results show that, comparing with other methods, Credit and Hybrid routing provides strong and efficient source-location privacy protection.

References

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer networks*, vol. 38, no. 4, pp. 393–422, 2002.

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

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

[4] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler, "Spins: Security protocols for sensor networks," *Wireless networks*, vol. 8, no. 5, pp. 521–534, 2002.

[5] L. Eschenauer and V. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*. ACM, 2002, pp. 41–47.

[6] S. Zhu, S. Setia, and S. Jajodia, "Leap+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Transactions on Sensor Networks (TOSN)*, vol. 2, no. 4, pp. 500–528, 2006.

[7] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in *INFOCOM, 2010 Proceedings IEEE*. IEEE, 2010, pp. 1–9.

[8] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," in *Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on*. IEEE, 2005, pp. 113–126.

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

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

[11] Y. Ouyang, Z. Le, G. Chen, J. Ford, and F. Makedon, "Entrapping adversaries for source protection in sensor networks," in *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks*. IEEE Computer Society, 2006, pp. 23–34.

[12] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE, 2008, pp. 51–55.

[13] Y. Yang, M. Shao, S. Zhu, B. Urgaonkar, and G. Cao, "Towards event source unobservability with minimum network traffic in sensor networks," in *Proceedings of the first ACM conference on Wireless network security*, ser. WiSec '08. New York, NY, USA: ACM, 2008, pp. 77–88.

[14] J. Deng, R. Han, and S. Mishra, "Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks," in *Dependable Systems and Networks, 2004 International Conference on*. IEEE, 2004, pp. 637–646.

[15] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*. IEEE, 2007, pp. 1955–1963.

[16] ——, "A novel scheme for protecting receiver's location privacy in wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 10, pp. 3769 –3779, october 2008.

[17] F. Ye, A. Chen, S. Lu, and L. Zhang, "A scalable solution to minimum cost forwarding in large sensor networks," in *Computer Communications and Networks, 2001. Proceedings. Tenth International Conference on*. IEEE, 2001, pp. 304–309.

[18] H. Chen and W. Lou, "From nowhere to somewhere: Protecting end-to-end location privacy in wireless sensor networks," in *Performance Computing and Communications Conference (IPCCC), 2010 IEEE 29th International*, dec. 2010, pp. 1 –8.