2009 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications

Sink-Anonymity Mobility Control in Wireless Sensor Networks

Qijun Gu, Xiao Chen
Dept. of Computer Science
Texas State University
San Marcos, TX 78666
Email: {gq11, xc10}@txstate.edu

Zhen Jiang
Dept. of Computer Science
West Chester University
West Chester, PA 19383
Email: zjiang@wcupa.edu

Jie Wu
Dept. of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL 33431
Email: jie@cse.fau.edu

***Abstract*—As the technology of mobile sensors advances, mobility control becomes a viable option that can be utilized to minimize energy consumption in wireless sensor networks (WSNs). A mobility control protocol re-deploys mobile sensors to optimal positions to minimize energy consumption for communication. We identify a unique privacy issue in mobility control protocols that discloses the physical location of the sink node to intruders in WSNs. To protect the sink node, we propose a new privacy-preserving scheme to secure mobility control protocols against attacks that locate and sabotage the sink node. The privacy-preserving scheme obfuscates the sink location with dummy sink nodes. Analysis shows that the scheme can effectively hide the sink location via anonymity. The scheme can also be easily integrated into current mobility control protocols without raising much additional overhead. The performance simulation and analysis show that, with the sink node well-protected, mobility control protocols achieve similar performance as original protocols.**

I. Introduction

As mobility becomes readily available to wireless sensor networks (WSNs) [1], studies on using mobility as a control mechanism to minimize energy consumption [2]–[6] have been conducted. Several mobility control protocols have been developed, which move mobile sensors to the most power-efficient positions for communication. These studies show that the saved communication energy can compensate for the energy consumption in movement, thereby reducing the overall energy consumption of sensors.

In order for mobile sensors to find their most power-efficient locations, mobility control protocols yield the location information of the sink node to mobile sensors. The disclosure of such information endangers the sink node, because attackers can easily obtain the sink location information. Current mobility control protocols are risk free to attackers. Attackers can eavesdrop mobility control packets or compromise some nearby nodes to obtain the sink location. Such attacks can be accomplished by attackers anywhere far away from the sink node without exposing themselves.

The sink node in a WSN is crucial for gathering, aggregating, transferring and processing sensor information. If the sink node is located and destroyed, the network covered by the destroyed sink node will not function. Therefore, protecting the location of the sink node is one of the critical security issues to safeguard WSN operations.

Nevertheless, the sink location can be hardly protected using existing security mechanisms, such as packet encryption and key management. At the same time, a scheme for sink protection should not affect normal sensing, communication and mobility control tasks that require knowledge of the sink location. To address this privacy issue, we propose a novel privacy-preserving scheme, called *sink-anonymity*, which only discloses the location information of dummy sinks and hides the real sink in a Φ-anonymity area to deceive attackers.

The security achieved by the sink-anonymity scheme increases the cost of locating the sink node. By hiding the real sink location, attackers cannot directly obtain the sink location from mobility control packets or compromised nodes. Rather, attackers have to physically trace traffic flows hop-by-hop until reaching the sink node. Such tracing is demanding and possibly exposes and endangers the attackers themselves.

The contributions of the paper are threefold. (i) The privacy of the sink location is a unique issue in mobility control. It has not been given much attention in the sensor network research field. Most security and privacy related research focuses on secure routing, key management, source privacy and denial of service. (ii) The sink-anonymity scheme is the first work to address the sink location privacy issue in mobility control. The scheme does not disclose the sink location, nor any information to help attackers derive the sink location. We show that it has Φ-anonymity on the sink location. (iii) This scheme can be readily integrated into existing mobility control protocols to enhance their security. The simulation shows that the mobility control protocols with sink-anonymity have the similar performance as original protocols.

The rest of the paper is organized as follows. Section II introduces mobility control. Section III presents the privacy problem of sink location and the sink-anonymity scheme. Section IV proves its Φ-anonymity on the sink location. Section V evaluates the performance of sink-anonymity mobility control protocols. Section VI summarizes related privacy research in WSNs. Finally, Section VII concludes the paper.

II. Background on Mobility Control

Using mobility as a control primitive to minimize energy consumption in communication has been studied recently. As discussed in [2], there are many scenarios that mobility can be

978-0-7695-3841-9/09 $26.00 © 2009 IEEE
DOI 10.1109/WiMob.2009.16

IEEE computer society

Protocol MCM: **M**obility **C**ontrol with **M**inimum total moving distance

1: The source node s sends $L(s)$ and its label 0 to u_1. When each intermediate node u_i receives $L(s)$ and the label $i-1$, it will pass $L(s)$ and its own label i to the succeeding node along the path. Such a propagation will end at d.
2: Once the destination node d receives $L(s)$, it will send a message carrying $L(d)$ and n back to s along the path.
3: When each intermediate node u_i receives $L(d)$ and n, it will compute its optimal location $L^*(u_i) = L(s) + i \times \frac{L(d)-L(s)}{n}$ and move to $L^*(u_i)$.

Fig. 1.

used to improve network communications. In general, long-term deployments which exhibit persistent or habitual communication patterns are prime candidates for the application of mobility control to improve network performance. In such settings, the traffic is regular enough and has sufficient volume to warrant nodes expending energy on moving to save more energy on forwarding traffic in return.

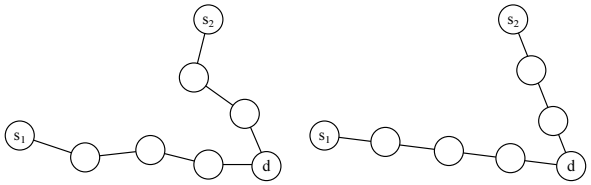
To discuss mobility control, we assume that neighboring nodes can share their location information by exchanging short messages. Location information can be provided by GPS or other positioning algorithms, such as the one in [7]. We assume that the paths from the sources to the sink d have already been discovered using a routing protocol, e.g., greedy routing or ad hoc routing.

Under a link cost model of $P(d) = a + bd^{\alpha}$, where d is distance, α a constant between 2 and 6, and a and b other constants, it is showed [8] that straight paths are most energy efficient and that there is a unique hop count for any distance that minimizes the cost of communications. Further, it is proved [2] that in a single flow between a source and a destination pair, if the energy cost function is a non-decreasing convex function, the optimal positions of the intermediate nodes shall lie entirely on the line between the source and the destination, and the intermediate nodes must be spaced evenly along the line.

Mobility control can be illustrated with a basic mobility control protocol MCM [9] as shown in Figure 1. For the communication between a sink d and a source s, we assume neither s nor d moves during mobility control. When s intends to optimize its path to d, it sends its location $L(s)$ to d. Then, d replies with its location $L(d)$ and the hop count n of the path back to s. An intermediate node u_i on the path, when forwarding the packets, obtains $L(s)$, $L(d)$, n and its own hop count i and then calculates its most power-efficient position $L^*(u_i)$ according to Equation (1) [2]. All intermediate nodes can thus move to their best positions and the best path between the source and the destination is established.

$$L^*(u_i) = L(s) + i \times \frac{L(d) - L(s)}{n} \quad (1)$$

In the paper, we consider the communication in multiple disjoint paths, since a sink normally takes information from multiple sources in a sensor network. Figure 2(a) shows a scenario where a sink d is communicating with two sources s_1 and s_2 through two disjoint paths. Then, each path is re-shaped using the location information of its source and destination according to mobility control as shown in Figure 2(b).



(a) Before mobility control (b) After mobility control

Fig. 2. Mobility Control

The MCM protocol has a nice property: the total moving distance of nodes in MCM is minimal. However, the communication among neighbors may be lost in movement. So it is not practical for a distributed environment like the WSNs. To overcome this drawback and speedup the process for nodes to move to their optimal locations (convergence process), two quick convergence mobility control protocols are proposed [6]: MCC (***M**obility **C**ontrol quick **C**onvergence*) and MCF (***M**obility **C**ontrol **F**ast convergence*) were proposed to speed up the convergence process without losing the connectivity between communicating neighbors. Both protocols use the optimal location information of the intermediate nodes calculated by MCM before the convergence process starts. MCC speeds up the convergence process by avoiding the overreaction of a node to the movement of its neighbors, while MCF reduces the convergence time by moving the nodes as close to their optimal positions as possible. In this paper, we will enhance MCM, MCC and MCF by the proposed privacy-preserving scheme to protect the sink location.

III. Sink-Anonymity Mobility Control

In this section, we present the sink-anonymity scheme to protect the sink location. We first describe a few unique attacks on sink location that motivate this study. Then, we describe the details of our solution. Finally, we show how to apply our solution into existing mobility control protocols.

A. Attacks on Sink Location

Mobility control protocols are susceptible to various attacks. For example, the location information could be modified for attacking purpose. However, many security schemes of authentication, encryption and key management were proposed in the past, which can be deployed in WSNs to protect mobility control. Hence, this paper will not address the traditional attacks. Rather, we show two attacks (*direct attack* and *intersection attack*) that are hardly defeated by current security countermeasures. The two attacks give attackers an easy access to sink location without exposing themselves. Using the two attacking approaches, attackers do not need to physically trace along a path hop by hop to the real sink node, but simply monitor nearby traffic or capture a few nearby nodes at any place far away from the real sink.

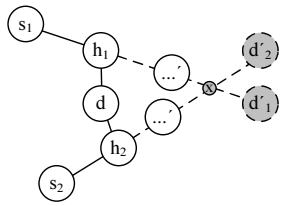


Fig. 3. Dummy Sinks

The direct attack exploits the fact that all mobility control protocols need to send the sink location information to nodes. Hence, attackers can directly obtain the sink location from the eavesdropped mobility control packets that carry the sink location information or the captured nodes that have the sink location information in memory.

The intersection attack exploits the geometric characteristic of paths formed in mobility control. Because the sink node places itself on the paths, attackers can infer the actual sink location by locating nearby nodes in two disjoint paths. This intersection attack is illustrated in Figure 2(b), in which the sink is communicating with two sources s_1 and s_2 via two disjoint paths. If an attacker can find any two nodes on each of the two disjoint paths, the attacker can obtain the two paths going through these nodes. Then, the intersection of the two paths discloses the location of the sink node. This attack allows attackers to obtain sink location without cracking any packet of mobility control protocols.

The challenge of defeating the two attacks and ensuring the privacy of sink location is that traditional security mechanisms cannot hide the sink location information. For example, encryption of the sink location cannot prevent a fully compromised node from disclosing the information because an attacker can easily obtain all credentials (such as keys) in the compromised node to decrypt any encrypted information.

Sink location anonymity is different from identity anonymity. Attackers can eavesdrop packets transmitted near them and find the identity information of the sink node (such as its IP address), but this kind of information cannot help the attackers locate the sink node. In this paper, we are concerned with the attacks that attempt to discover the location of the sink node and destroy it. Hence, the objective of our work is to hide the sink location.

B. Sink-Anonymity Scheme

We propose a sink-anonymity scheme (SAS) using dummy sink nodes instead of the real sink node in mobility control. Assume a sink node d is communicating with several sources through multiple disjoint paths. After d receives the source location $L(s)$ from each source, it does not reply with its real location $L(d)$. Instead, d picks a one-hop neighbor h and a dummy sink node d' for each path, and replies with the location $L(d')$ and the hop count $n_{d'}$ of the dummy sink node to each source s. Then, the intermediate nodes of each path use the location of the dummy sink to compute their best positions.

SAS selects h and d' for each path according to three conditions: (a) h satisfies Inequality (2), (b) d' satisfies Equation (3), and (c) all the disjoint paths satisfy Equation (4). In notation, n_i is the hop count of node u_i counted from the source s, and $|L(i) - L(j)|$ is the distance between nodes u_i and u_j.

Inequality (2) states that h's location is in the communication range R of d so that d is one-hop away from the path that goes through s and h. Equation (3) is a transformation of Equation (1) and states that d', h and s are on the same path and all intermediate nodes (including h) compute their optimal locations using the location of the dummy sink. Equation (4) states that all the disjoint paths intersect at an offset point x whose coordinate is (X_x, Y_x). Note that the offset point is neither a dummy node nor a real node.

$$|L^*(h) - L(d)| < R \tag{2}$$

$$\frac{L(d') - L(s)}{n_{d'}} = \frac{L^*(h) - L(s)}{n_h} = \frac{L^*(u_i) - L(s)}{n_i} \tag{3}$$

$$\frac{Y_x - Y_s}{X_x - X_s} = \frac{Y_h - Y_s}{X_h - X_s} \tag{4}$$

Figure 3 illustrates an example of the dummy sink nodes, the disjoint paths and the offset point x. For the two disjoint paths, d selects h_1 and d'_1 for s_1 and h_2 and d'_2 for s_2. d claims that it is the next hop to h_1 and h_2 on their paths pointing to the dummy sinks. Hence, when h_1 (or h_2) receives a packet from s_1 (or s_2), it will forward the packet to its next hop, which is d. That is, d can accept information delivered via both paths.

Because the real sink is not on any path, SAS addresses both direct and intersection attacks, even if any mobility control packet is eavesdropped, any sensor node on a path is compromised, or the intersection point of any disjoint paths is identified. When SAS is applied in mobility control, the direct attack only discloses the location of dummy sinks to attackers, and the intersection attack only discloses the location of the offset point to attackers.

Note that $L(d)$ and n are two private values kept in the sink node d in the dummy sink scheme. Hence, a security requirement in mobility control is that routing and data traffic shall not disclose the actual hop count of a path. We inspect several major routing protocols in WSNs [10], [11] and find that this security requirement can be satisfied. If sink nodes use dummy hops persistently in routing and forwarding, it will not affect the normal traffic.

C. Sink-Anonymity Mobility Control Protocols

SAS can be easily integrated into the existing mobility control protocols, MCM, MCC, and MCF, because SAS only substitutes the location information of a real sink with a dummy sink and does not change any control mechanism of any mobility control protocol. Since both MCC and MCF use MCM, the MCM part of these two protocols will be changed by adding SAS. The rest of the two protocols will remain the same. Due to space limitation, only the SAS embedded MCM is shown in Figure 4. The general idea is that (i) for each path, the sink node d picks a neighbor h and a dummy

Protocol SAMCM: **S**ink-**A**nonymity **MCM**

1: The sink node d obtains the source locations of all disjoint paths.
2: d picks a one-hop neighbor h and a dummy sink d' for each source s such that Inequality (2), Equation (3), and Equation (4) are satisfied.
3: For each path, d sends the dummy location $L(d')$ back via the selected neighbor h.
4: Intermediate nodes compute and move to their optimal locations according to Protocol MCM, MCC, or MCF.

Fig. 4.

sink d' according to SAS, and then (ii) intermediate nodes use the location of the dummy nodes to obtain their optimal positions and move to their optimal positions according to the mechanism in the original mobility control protocols.

IV. Anonymity Analysis

In this section, we propose Φ-anonymity to formalize the privacy problem and show that the sink is in fact hidden in a Φ-anonymity area of dummy nodes.

A. Φ-*anonymity*

Although SAS does not include the location of the real sink in mobility control, attackers can try to derive the sink location from the multiple paths. Hence, we propose a formal privacy model to analyze the privacy achieved by the proposed scheme. The model defines a *proximity area* surrounding the real sink node, which shows the range of the sink location that attackers can derive.

As shown in Figure 5, we place the sink node at the origin. Assume that attackers have found N disjoint paths. Each path p_i is a line $y = k_i x + c_i$, for $1 \leq i \leq N$. Because all these paths pass inside the communication range R of the sink node, the vertical distance from the sink to any path is less than R. Similarly, in order to determine whether the sink node is at the location (X, Y), attackers need to compute the vertical distance from the location (X, Y) to each path i using $d_i = \frac{|c_i + k_i X - Y|}{\sqrt{1+k_i^2}}$. If all d_i satisfy Inequality (5), i.e. the distance from the location (X, Y) to any of the disjoint paths is less than the communication range R, a sink node might be at the location (X, Y). The shadowed area in Figure 5 shows the proximity area in which any position (X, Y) satisfies Inequality (5).

$$\frac{|c_i + k_i X - Y|}{\sqrt{1+k_i^2}} < R \;\; for \;\; 1 \leq i \leq N \tag{5}$$

Since the proximity area covers the range of possible sink location, the size of the proximity area reflects the achieved privacy. Accordingly, we define Φ-anonymity below. The proximity area in Figure 5 is thus a Φ_P-anonymity, where P is the set of the two disjoint paths.

Definition 1: Let Φ be a proximity area and P be the set of all disjoint paths known to attackers. Φ is said to satisfy Φ_P-anonymity if and only if Φ is the maximum proximity area in which any location (X, Y) satisfies Inequality (5) for all paths in P.

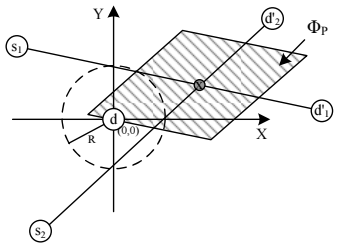
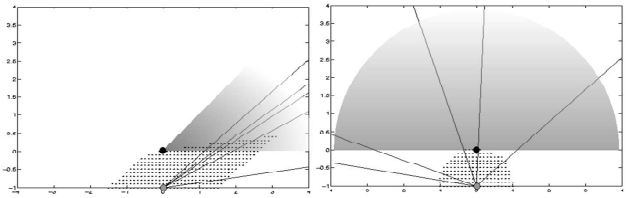


Fig. 5. Illustration of a Proximity Area



(a) θ=45° (b) θ=180°

Fig. 6. Illustration of Φ_P-anonymity

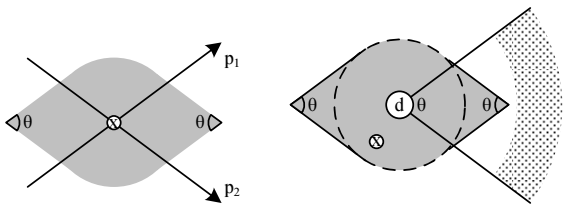
Definition 2: Let Φ be a proximity area and P^* be a set of disjoint paths known to the sink node. Φ is said to satisfy Φ-anonymity if and only if Φ is the maximum proximity area in which any location (X, Y) satisfies Inequality (5) for all paths in P^*.

The relation of Φ_P-anonymity and Φ-anonymity is shown by Theorem 1, which indicates that attackers can reduce the proximity area if more disjoint paths are known. The smaller the proximity area, the better estimation the attackers have on the real sink location. However, the minimum proximity area that attackers can achieve is the Φ-anonymity area.

Theorem 1: A Φ-anonymity area is the minimum in all Φ_P-anonymity areas, i.e. $\forall \Phi_P$, $\Phi \subseteq \Phi_P$. (Proof is omitted here.)

Figure 6 shows two examples of Φ_P-anonymity areas (the dotted areas) that attackers can estimate from five disjoint paths. In the figure, the black dots are real sink nodes, and the gray dots are the offset points where the disjoint paths intersect. The gray "fan" areas illustrate the areas in which sensors report data to the sink node. The angle of the fan is denoted as θ. When $\theta = 180^o$, paths to the sink node may come from all directions. Thereby, paths in a fan of $\theta > 180^o$ are the same as paths in a fan of $\theta = 180^o$. Note that the fan area of a sink node is normally determined by network deployment or task assignment. We assume the sink node has θ as a parameter in mobility control.

Because the Φ-anonymity area is what attackers can know best about the location of the real sink, the size of the Φ-anonymity area is the privacy achieved by SAS. We can identify the Φ-anonymity area using the approach stated in Theorem 2. The Φ-anonymity area is critical to the privacy of sink location. The larger the Φ-anonymity area is, the better the real sink node is protected. According to Definition 2, the shape and the size of the Φ-anonymity are determined by P^*. In other words, the disjoint paths selected by the sink node



(a) Φ-anonymity Area (b) Offset Area

Fig. 7.

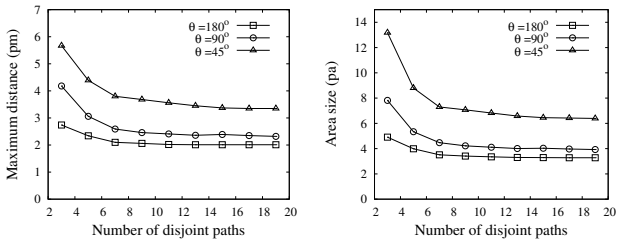


Fig. 8. Φ-anonymity of SAS

determine the privacy of the sink location.

Theorem 2: Let p_1 and p_2 be the two outmost paths such that all disjoint paths intersecting at the offset point x are bounded by the two paths (as shown in Figure 7(a)). The Φ-anonymity area is the gray area that does not reveal the real sink location. (Proof is omitted here.)

Actually, the sink node can select an offset point x in any place of the gray area shown in Figure 7(b) and achieve the same privacy. The dotted area in the figure is where sensors are deployed. The farthest distance between the offset point and the sink node is $\frac{R}{sin(\theta/2)}$. If $\theta \leq 60^o$, the offset point could be more than two hops away from the real sink node, while the closest point on any selected path passing the offset point is one-hop away from the real sink node.

B. Anonymity Measurement

We use two metrics to quantitatively measure the Φ-anonymity: maximum distance $pm = max_{(X,Y)\in\Phi}(D_{(X,Y)})$ and area $pa = \int_\Phi dXdY$, where $D_{(X,Y)}$ is the distance of the location (X, Y) to the real sink node. pm indicates the possible farthest location in the Φ-anonymity area to the sink node. pa shows the size of the Φ-anonymity area where the sink node is. Therefore, from a defender's perspective, the larger the pm and pa, the better the privacy.

Figure 8 summarizes the measurement of privacy in three metrics. We study three situations, setting θ to 45^o, 90^o or 180^o. We assume that the sink node has a few disjoint paths ranging from 3 to 19 in its covered area. The results are normalized as the communication range of the sink node is set to 1. All data points are averaged over 30 random scenarios generated in Matlab.

First, the results confirm the privacy analysis of SAS. As attackers obtain more disjoint paths, the inferred area size reaches a boundary and cannot be further reduced. In other words, if SAS is applied, attackers cannot obtain the exact sink location by trying more disjoint paths.

Second, we observe that smaller θ implies better privacy to the sink node. When the sink node collects information from a smaller fan area, disjoint paths lay more parallel to each other. Their one-hop surrounding areas thus have a larger overlap, which results in a larger Φ-anonymity area that makes attackers more difficult to infer. Thus, the sink node is better protected by a smaller θ.

V. Performance Analysis

In this section, we integrate SAS into existing mobility control protocols and show how the added SAS affects the performance of these protocols.

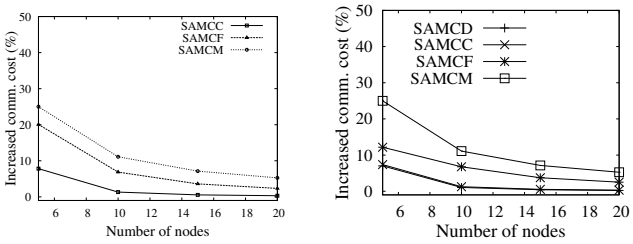
We implement three sink-anonymity mobility control protocols SAMCM, SAMCC and SAMCF by integrating SAS into MCM [2], MCC [6] and MCF [6] using self-implemented simulator written in C. The protocols work in a synchronous round-based system, where each mobility control message is sent and received in the same round. All the protocols presented in our paper can be extended to an asynchronous system.

The performance of these protocols is measured with three metrics: convergence speed, energy consumption in node movement, and the communication cost. The convergence speed is the number of rounds of node movement needed to achieve stabilization. The energy consumption in node movement is measured as the total moving distance of nodes. The communication cost of mobility control is calculated by the total number of messages exchanged between nodes in this paper.

We conduct experiments using various network settings with different parameters. The initial locations of nodes are randomly generated in a 100×100 area. The number of nodes is set to 5, 10, 15 or 20, including the source and the destination. The communication range (R) is 20 or 40 [12]. The performance measurements are averaged over $10,000$ experiments.

First, the convergence speed. When SAS is integrated into MCM, MCC and MCF, the resulting sink-anonymity mobility control protocols SAMCM, SAMCC and SAMCF will have the same convergence speed as the protocols they are built on. This is because after a dummy sink is selected according to SAS, the intermediate nodes between the source and the sink will try to align themselves based on the position of the dummy sink. This process is no different in terms of number of rounds of node movement than using the real sink. So adding security in these protocols does not affect the convergence property of them. Therefore, we still have the same results as in [6], SAMCM has the optimal convergence process, SAMCF and SAMCC are near optimal.

Second, the energy consumption. Similar to the convergence speed, built-in SAS has little impact on the total distance of node movement either. Therefore, same as in [6], SAMCM still achieves the minimal total movement, SAMCC is close



(a) Comparison when R=20 (b) Comparison when R=40

Fig. 9. Increased Communication Cost of Protocols with Embedded SAS

to SAMCM and SAMCF is very close to SAMCM.

Third, the communication cost. We show how the embedded sink-anonymity scheme affects the communication cost of the protocols. If SAS is integrated into MCM, MCF and MCC, the communication cost will increase as a result of extra message exchanges. We calculate the increased communication cost (in percentage) over each original protocol if security is embedded. From Figures 9(a) and 9(b), the communication cost increases for all four protocols if security is used. The communication cost of SAMCM increases the most: for example, 25% when the number of nodes is 5 and the communication range is 20; SAMCF is the next; SAMCC is the least. Since MCM and MCF are already low-cost protocols, anything added on to them will cause a greater increase in cost than those higher-cost protocols. As the number of nodes increases, the percentages fall sharply. Therefore, the built-in security will only bring trivial communication cost to the original protocols.

VI. Related Works

Privacy research has been primarily conducted in the context of information privacy and anonymous communication [13], [14]. A few schemes [15]–[18] have been proposed on *source location privacy* in WSNs. Their main ideas include using numerous paths to send packets to sinks, forming looping paths to forward packets, associating real sources with faked sources, and requiring real sources to send packets periodically. In this paper, we are interested in the problem of *sink location privacy* in mobility control. New schemes are needed to ensure the privacy of sinks in mobility control protocols.

The sink-anonymity problem in mobility control is also related to a formal privacy-preserving model named *K-anonymity* [19] in the data privacy research area. Using the model, the record of an individual is hidden in a group of at least k records with other individuals. In this paper, we propose the Φ-anonymity model for sink location privacy. Unlike the K-anonymity model, the Φ-anonymity scheme does not create a fixed number of nodes to disguise the real sink node. Instead, it finds a continuous area Φ such that the sink node could be hidden at any position inside Φ.

VII. Conclusion

In this paper, we identified a unique privacy issue in mobility control that discloses the physical location of the sink node to intruders in WSNs. To protect the sink node, we proposed a new privacy-preserving scheme to secure mobility control protocols against attacks that locate and sabotage the sink node. The privacy-preserving scheme can obfuscate the sink location with dummy sink nodes. The analysis showed that the scheme can effectively hide the sink location with Φ-anonymity. The scheme was also integrated into current mobility control protocols with trivial overhead. The performance simulation and analysis showed that the mobility control protocols with sink-anonymity still have similar performance as before, but keep the sink node well protected.

Acknowledgment

This research was supported in part by NSF grant CNS 0835834.

References

[1] V. Rodoplu and T. Meng, "Minimum energy mobile wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 17, no. 8, pp. 1333–1344, 1999.

[2] D. Goldenberg, J. Lin, A. Morse, B. Rosen, and Y. Yang, "Towards mobility as a network control primitive," in *Proc. of ACM MobiHoc*, 2004, pp. 163–174.

[3] L. Li and J. Halpern, "Minimum-energy mobile wireless networks revisited," in *Proc. of IEEE ICC*, vol. 1, 2001, pp. 11–14.

[4] W. Wang, V. Srinivasan, and K. Chua, "Using mobile relays to prolong the lifetime of wireless sensor networks," in *Proc. of ACM MobiCom*, 2005, pp. 270–283.

[5] Y. Wang, H. Wu, F. Li, and N. Tzeng, "Protocol design and optimization for delay/fault-tolerant mobile sensor networks," in *Proc. of IEEE ICDCS*, 2007, pp. 7–15.

[6] X. Chen, Z. Jiang, and J. Wu, "Quick convergence mobility control schemes in wireless sensor networks," in *Proc. of 10th Workshop on Advances in Parallel and Distributed Computational Models*, 2008.

[7] S. Capkun, M. Hamdi, and H. J., "GPS-free positioning in mobile ad hoc networks," in *Proc. of the 34th Annual Hawaii International Conference on System Sciences*, 2001, pp. 3481–3490.

[8] S. I. and L. X., "Power-aware localized routing in wireless networks," vol. 12, no. 11, 2001, pp. 1122–1133.

[9] Z. Jiang, J. Wu, and R. Kline, "Mobility control for achieving optimal configuration in mobile networks," *Proc. of IEEE International Workshop on Networking, Architecture, and Storages*, 2006.

[10] W. R. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive protocols for information dissemination in wireless sensor networks," in *Proc. of ACM MobiCom*, 1999, pp. 174–185.

[11] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," *IEEE/ACM Transactions on Networking*, vol. 11, no. 1, pp. 2–16, 2003.

[12] J. Wu, M. Cardei, F. Dai, and S. Yang, "Extended dominating set and its applications in ad hoc networks using cooperative communication," *IEEE Transactions on Parallel and Distributed Systems*, vol. 17, no. 8, pp. 851 – 864, 2006.

[13] M. Reed, P. Syverson, and D. Goldschlag, "Anonymous connections and onion routing," *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 482–494, 1998.

[14] B. Sheng and Q. Li, "Verifiable privacy-preserving range query in two-tiered sensor networks," in *Proc. of IEEE Infocom*, 2008, pp. 46–50.

[15] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," in *Proc. of IEEE IPDPS*, 2006.

[16] K. Mehta, D. Liu, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," in *Proc. of IEEE ICNP*, 2007.

[17] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," in *Proc. of IEEE ICDCS*, 2005, pp. 599–608.

[18] M. Shao, Y. Yang, S. Zhu, and G. Cao, "Towards statistically strong source anonymity for sensor networks," in *Proc. of IEEE Infocom*, 2008.

[19] L. Sweeney, "K-anonymity: a model for protecting privacy," *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, vol. 10, no. 5, pp. 557–570, 2002.