Quantitative Security and Efficiency Analysis of SEAR in Wireless Sensor Networks

Di Tang, Tongtong Li and Jian Ren
Department of Electrical and Computer Engineering, Michigan State University, East Lansing, MI 48824
Email: {ditony, tongli, renjian}@egr.msu.edu

***Abstract*—SEAR is a novel secure and energy aware routing protocol proposed to address the energy balance and routing security through a balanced energy consumption and probabilistic random walking. Recently, a quantitative security measurement scheme for source-location privacy based on source-location disclosure index (SDI) and source-location space index (SSI) has been proposed. In this paper, we first derive a numerical formula to quantitatively estimate the routing efficiency through the number of routing hops for a given routing security level. We then consider the reverse problem: For a given routing *cost factor*, how to determine the maximum security level for a message to be transmitted. Our simulation results demonstrate that the theoretical results provide a very tight estimation of the actual routing hops for various security parameters. Finally, we prove that the SEAR scheme can provide provable security under the quantitative security measurement criteria.**

I. Introduction

The technological advances of the recent years have made wireless sensor networks (WSNs) to be envisioned as a ideal technology many military and civilian applications like monitoring of environmental ambient conditions, climate measurements, wildlife habitat and critical infrastructures. WSNs consist of a large number of untethered and unattended autonomous sensor nodes. WSNs offer a lower-cost method for information gathering. However, these nodes often have very limited and non-replenishable energy resources, which makes energy efficiency an essential issue for these networks. In addition, WSNs rely on wireless communications, which is by nature a broadcast medium, anybody with an appropriate wireless receiver can monitor and intercept the sensor network communications. It is possible for the adversaries to perform routing traceback attacks.

Based on the aforementioned issues, a properly designed routing protocol should not only ensure a high message delivery ratio and low energy consumption for packet delivery, but should also be able to balance energy consumption through the entire networks to extend the sensor network lifetime while providing the corresponding security to protect the networks from adversarial attacks.

Motivated by the fact that sensor networks routing may often be geographically based, we proposed a geographical-based secure and energy aware routing (SEAR) protocol for WSNs in [1]. It has been demonstrated that SEAR routing protocol can significantly extend the sensor network lifetime while providing routing security concurrently through a balanced energy consumption and probabilistic random walking to preventing routing traceback attacks. We also analyzed the routing performance for various security levels in [1].

In this paper, we first derive a numerical formula to quantitatively estimate the routing efficiency through the number of routing hops for a given routing security level. We then consider the reverse problem: For a given routing *cost factor*, how to determine the maximum security level for a message to be transmitted. Our simulation results demonstrate that the theoretical results can provide a very tight estimation of the actual routing hops for various security parameters. We also give quantitative security analysis of the SEAR protocol in this paper based on the criteria proposed in [2].

The rest of this paper is organized as follows. The system model is presented in Section II. The preliminaries are described in Section III. Routing overhead analysis is performed in Section IV. In Section V, quantitative security analysis is presented. In Section VI, the related work is reviewed. We conclude in Section VII.

II. Models and Assumptions

A. The System Model

We assume that the WSNs are composed of a large number of sensor nodes and a sink node. The sensor nodes are randomly deployed throughout the sensor domain. Each sensor node will have a very limited and non-replenishable energy resource. The sink node is the only destination that every sensor node will send message packets to through a multi-hop routing strategy. The information of the sink node is made public. For security management purpose, each sensor node may also be assigned a node ID corresponding to the location where this message is generated. To prevent adversaries from recovering the source location from the node ID, *dynamic ID*s [3] can be used. In addition, the content of each message can also be encrypted using the secret key shared between the node/grid and the sink node.

We also assume that each sensor node knows its relative location in the sensor domain and has knowledge of its immediate adjacent neighboring grids and their energy levels. The information about the relative location of the sensor domain may be broadcasted in the network for routing information update.

The key management, including key generation, key distribution and key update, is beyond the scope of this paper. However, the interested readers are referred to reference, such as [4], for more information.

978-1-4577-2053-6/12/$31.00 ©2012 IEEE

B. The Adversarial Model

In WSNs, the adversary may try to recover the message source node or jam the packet from being delivered to the sink node. The adversaries would try their best to equip themselves with advanced equipments, which means they would have some technical advantages over the sensor nodes. In this paper, the adversaries are assumed to have the following characteristics:

- The adversaries will have sufficient energy resources, adequate computation capability and enough memory for data storage. On detecting an event, they could determine the immediate sender by analyzing the strength and direction of the signal they received. They can move to this sender's location without too much delay. The adversaries may also compromise some sensor nodes in the network. We assume that the adversaries will never miss any event close to them.
- The adversaries will not interfere with the proper functioning of the network, such as modifying packets, altering the routing path, or destroying sensor devices, since such activities can be easily identified. However, the adversaries may carry out passive attacks, such as eavesdropping of the communications.
- The adversaries are able to monitor the traffic in an area that is important to them and get all of the transmitted messages. However, we assume that the adversaries are unable to monitor the entire network. In fact, if the adversaries could monitor the entire wireless sensor networks, then they can monitor the events directly without relying on the sensor network.

C. Design Goals

Our design goal can be summarized as follows:

- To maximize the sensor network lifetime, we will ensure that the energy consumption of all sensor grids are balanced.
- To achieve a high packet delivery ratio, our routing protocol should try to avoid packet dropping when alternative paths exist.
- The adversaries should not be able to get the source location information by analyzing the traffic pattern.
- The adversary should not be able to get the source location information if he is only able to monitor certain area of the WSNs and compromise a few sensor nodes.
- Only the sink node is able to identify the source location through the messages received. The recovery of the source location from the received message should be very efficient.
- The routing protocol should maximize the probability that the packet is being delivered to the sink node when adversaries are only able to jam a few sensor nodes.

III. Preliminaries

In this section, we will describe some preliminaries that will be used in this paper.

A. SEAR Scheme

In [1], we have proposed the SEAR algorithm. The algorithm consists of two strategies for a message forwarding: the shortest path forwarding based on the geographical information, and the random walking message forwarding, which is used to create routing unpredictability for source-location privacy and jamming prevention.

In the SEAR algorithm, we assume that each node A maintains its relative location and the remaining energy levels of its immediate adjacent neighboring grids. The set of node A's immediate adjacent neighboring grids is denoted as $\mathcal{N}_A$, and the remaining energy of grid i, $i \in \mathcal{N}_A$, is denoted as $\mathcal{E}r_i$. The average remaining energy of grids in $\mathcal{N}_A$ can be computed as $\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|}\sum_{i\in\mathcal{N}_A}\mathcal{E}r_i$.

In the multi-hop routing, node A selects its next hop grid from the set $\mathcal{N}_A^\alpha = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha\mathcal{E}_a(A)\}$ as its next routing hop, where α is the *energy balance control (EBC)*. Obviously, all the nodes in this set have energy level above $\alpha\mathcal{E}_a(A)$. α also provides a tradeoff between energy balance and routing security.

SEAR algorithm contains two routing algorithms in message forwarding, one is a deterministic shortest path routing grid selection, and the other is a secure routing grid selection through random walking. In the deterministic routing algorithm, the next hop grid will be selected from $\mathcal{N}_A^\alpha$ based on the relative locations of the grids. The grid that is closet to the sink node will be selected for packet forwarding. In the secure routing algorithm, the next hop grid will be randomly selected from $\mathcal{N}_A^\alpha$ for message forwarding. The distribution of these two algorithms is controlled by a *security level* $\beta \in [0, 1]$ carried in each packet.

The SEAR routing algorithm[1] is described in Algorithm 1.

Algorithm 1 Node A find the next hop routing grid based on the given parameters $\alpha, \beta \in [0, 1]$

1: Compute the average remaining energy of the adjacent neighboring grids: $\mathcal{E}_a(A) = \frac{1}{|\mathcal{N}_A|}\sum_{i\in\mathcal{N}_A}\mathcal{E}r_i$.
2: Determine the candidate grids for the next routing hop: $\mathcal{N}_A^\alpha = \{i \in \mathcal{N}_A \,|\, \mathcal{E}r_i \geq \alpha\mathcal{E}_a(A)\}$.
3: Select a random number $\gamma \in [0, 1]$.
4: **if** $\gamma \geq \beta$ **then**
5: Send the packet to the grid in the $\mathcal{N}_A^\alpha$ that is closet to the sink node based on its relative location.
6: **else**
7: Route the packet to a randomly selected grid in the set $\mathcal{N}_A^\alpha$.
8: **end if**

B. Quantitative Source Location Privacy Measurement

In [2], we introduced two criteria to quantitatively measure the source-location privacy for WSNs.

Definition 1 ([2] Source-location Disclosure Index (SDI))**.** SDI *measures, from an information entropy point of view, the*

[1]The algorithm presented here is slightly different in expression from the original algorithm.

amount of source-location information that one message can leak to the adversaries.

For a routing scheme, to achieve good source-location privacy, *SDI* value for the scheme should be as close to zero possible.

Definition 2 ([2] Source-location Space Index (SSI))**.** SSI *is defined as the set of possible network nodes, or area of the possible network domain, that a message can be transmitted from.*

For a source-location privacy scheme, *SSI* should be as large as possible so that the complexity for an adversary to perform an exhaustive search of the message source is maximized.

Definition 3 ([2] Normalized Source-location Space Index (NSSI))**.** NSSI *is defined as the ratio of the* SSI *area over the total area of the network domain. Therefore,* $NSSI \in [0,1]$*, and we always have* $NSSI = 1-\delta$ *for some* $\delta \in [0,1]$*. The* δ *is called the local degree.*

IV. Routing Overhead and Routing Security

In this section, we further study the relationship between routing efficiency and security. We provide a numerical method to estimate the number of routing hops based on the routing security level. We also consider the reverse problem, that is the determination of the appropriate security level for a given routing cost factor.

Theorem 1. *Suppose that the sensor nodes have a balanced energy distribution, then the average number of hops that a message needs to be routed in the sensor domain to reach the sink node can be estimated as follows:*

$$\frac{h\sqrt{1+\left(\frac{\beta}{2(1-\beta)}\right)^2}}{1-\beta},$$

where h *is the required number of hops for security level* $\beta = 0$ *(i.e., when no security is enforced).*

Proof: For a security level β, the probability that the message is routed forward using the deterministic shortest path routing strategy is $1-\beta$. For probability β, the message is forwarded using random walking. At each source, we can roughly divide the entire domain into four $\frac{\pi}{2}$ sections, each with probability $\frac{\beta}{4}$: (i) the section faces the sink node, (ii) the section opposite to the sink node, and (iii) the two sections perpendicular to the direction of the sink node.

Since the probability that the message will be routed to these four section is equal, the effect of (i) and (ii) cancels each other. Therefore, the routing that contributes to forwarding has probability $1-\beta$ for each hop, while the routing that contributes to the perpendicular direction is $\frac{\beta}{2}$. Since a successful delivered message needs to transmit h hops in the direction of the forward direction. Therefore, we have

$$(1-\beta) : \frac{\beta}{2} = h : x,$$

TABLE I
Routing hops for different security parameters. The simulation was performed using OPNET.

Security parameter β	Average hops in simulations	Estimated SEAR hops
0	10.00	10.00
0.125	11.97	11.46
0.25	14.51	13.52
0.375	17.98	16.70
0.5	23.34	22.36

where x is the routing hops that the message will be routed in the perpendicular direction, which is

$$x = \frac{\frac{\beta}{2}}{1-\beta}h = \frac{\beta}{2(1-\beta)}h.$$

This makes the entire routing path length to be

$$h\sqrt{1+\left(\frac{\beta}{2(1-\beta)}\right)^2},$$

and the total routing hops to be

$$\frac{h\sqrt{1+\left(\frac{\beta}{2(1-\beta)}\right)^2}}{1-\beta},$$

since each hop, the message will only be routed forward $1-\beta$ hop toward the sink direction. ■

Theorem 1 shows that $C(\beta) = \frac{\sqrt{1+\left(\frac{\beta}{2(1-\beta)}\right)^2}}{1-\beta}$ is the *cost function* for a message delivery with security parameter β. We always have $C(\beta) \geq 1$ and $C(\beta) = 1$ if and only if $\beta = 0$. In other words, when the security level $\beta \neq 0$, there will be some routing overhead.

Table 1 compared the number of routing hops derived according to Theorem 1 with the simulation results using OPNET for the SEAR protocol for multiple security levels. It can be seen that Theorem 1 provides a very tight estimation of the number of routing hops, especially when for small β values.

Based on Theorem 1, for a given routing budget, we can also find the maximum routing security level. This result is given in the following theorem.

Theorem 2. *For a given routing cost factor* f*. The optimal security level can be estimated from the following quartic equation:*

$$4fx^4 - 5x^2 + 2x - 1 = 0,$$

where $x = 1-\beta$*.*

Proof: According to Theorem 1, we have

$$\frac{\sqrt{1+\left(\frac{\beta}{2(1-\beta)}\right)^2}}{1-\beta} = f.$$

Multiply both side with $1-\beta$, we have

$$\sqrt{1+\left(\frac{\beta}{2(1-\beta)}\right)^2} = f(1-\beta).$$

Square of both side, we get

$$1+\left(\frac{\beta}{2(1-\beta)}\right)^2 = f^2(1-\beta)^2.$$

Equivalently, we have

$$4(1-\beta)^2+\beta^2 = 4f^2(1-\beta)^4.$$

Let $1-\beta = x$, we can derive

$$\beta^2 = (1-x)^2 = x^2-2x+1,$$

and the above equation can be changed to

$$4f^2x^4-5x^2+2x-1=0. \quad (1)$$

■

Algorithm 2 Solve equation $4f^2x^4-5x^2+2x-1=0$.

1: $a \leftarrow 4f^2; c \leftarrow -5; d \leftarrow 2; e \leftarrow -1;$
2: $\alpha \leftarrow \frac{c}{a}; \beta \leftarrow \frac{d}{a}; \gamma \leftarrow \frac{e}{a};$
3: $p \leftarrow -\frac{1}{12}\alpha^2-\gamma; q \leftarrow -\frac{\alpha^3}{108}+\frac{\alpha\gamma}{3}-\frac{\beta^2}{8};$
4: $r \leftarrow -\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}};$
5: $u \leftarrow \sqrt[3]{r};$
6: $y \leftarrow -\frac{5}{6}\alpha+u-\frac{p}{3u}; w \leftarrow \sqrt{\alpha+2y};$
7: $s \leftarrow \frac{-w+\sqrt{-3\alpha-2y+2\beta/w}}{2}.$

Equation (1) can be solved using Ferrari's method [5] following Algorithm 2 to recover $s = 1-\beta$. The security level β can be recovered as: $\beta = 1-s$.

Example 1. *Suppose we want to deliver a message with cost factor $f = 1.5$. To find the maximum routing security level, we need to find the security parameter β. We can compute $s = 1-\beta$ as follows:*

1: $a \leftarrow 9; c \leftarrow -5; d \leftarrow 2; e \leftarrow -1;$
2: $\alpha \leftarrow -0.556; \beta \leftarrow 0.222; \gamma \leftarrow -0.111;$
3: $p \leftarrow 0.0854; q \leftarrow 0.016;$
4: $r \leftarrow 0.001;$
5: $u \leftarrow 0.110;$
6: $y \leftarrow 0.314; w \leftarrow 0.270;$
7: $s \leftarrow 0.684.$

Therefore, we have $\beta = 1-s = 0.316$, which means 31.6% random walking can be used for message forwarding.

V. Quantitative Security Analysis of SEAR

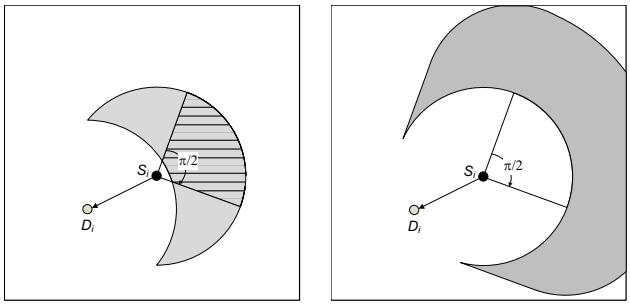
In this section, we provide quantitative security analysis of the SEAR protocol based on the criteria proposed in [2].

A. SDI in SEAR Routing Protocol

Theorem 3. *SEAR routing protocol can achieve perfect source node location information protection, that is*

$$SDI \simeq 0.$$

Proof: First, in SEAR, we assume that a dynamic ID will be used for each message, which prevents the adversary from linking multiple messages from the same source or linking the message to the source direction using correlation based techniques.



(a) (b)

Fig. 1. Routing source traceback analysis.

Second, due to probabilistic distribution of random walking and deterministic routing, the number of total routing paths can be infinite since, in theory, the packet can be transmitted back and forth continuously. And the routing paths can intercept at any node. When an adversary intercepts a message, it is infeasible for the adversary to determine the previous hop source node through a routing traceback. The probability that the adversaries will receive the messages from one source node continuously is negligible. Therefore, we have

$$SDI \simeq 0.$$

■

Theorem 4. *The source location that can be provided by the SEAR routing protocol is probabilistically proportional to the distribution of the random walking. That is*

$$NSSI \simeq 1.$$

Proof: When an adversary intercepts a message m while the message is being transmitted from node A to node B, there are two possible scenarios: (i) the message A transmits the message m using random walking routing strategy, and (ii) the message is transmitted from node A to node B using deterministic routing.

For scenario (i), based on the routing criteria, the previous source node will be located in shaded area, as shown in Fig. 1(a), based on the routing scheme and routing hop distance, where the angle of the shaded circular sector with horizontal lines is $\frac{\pi}{2}$ and symmetric to the S_iD_i.

Since each node will route the message forward with probability $1-\beta$ directly to the node A, and with probability β to all possible directions, where β is the probabilistic distribution for random walking to be used in SEAR routing protocol. It can be derived that the probability for the immediate previous hop node to be located in the shaded sector is $1-\beta+\frac{\beta}{4} = 1-\frac{3}{4}\beta$, and to be located in the rest of the shaded area is $\frac{3}{4}\beta$.

The probability advantage for the immediate previous hop node to be in the shared sector area with horizontal lines is,

$$1-\frac{3}{4}\beta-\frac{1}{4} = \frac{3}{4}(1-\beta).$$

However, when the traceback analysis continues, we will not be able to get any probability advantages for the next previous hop routing source node, except that the node will

be located in the shaded area, given in Fig. 1(b), based on the hop distance.

Since the hop distance between the actual source node and the current intercepted node is unknown, this makes it impossible for the actual source node to be located in the sensor domain, with an negligible exception of a small area around the node D_i. Therefore, we have

$$NSSI \simeq 1.$$

■

From the proof of the above theorem, we can see that the adversary can only get probability advantage $\frac{3}{4}(1-\beta)$ of one hop source node. In particular, when $\beta = 1$, that is the case of random walking, the adversary will not be able to get any probability advantage.

VI. Related Work

Routing is a challenging task in WSNs due to the high dynamic nature and limited resources. Geographic routing algorithms offer the advantages that the nodes only need to maintain neighboring information and while providing higher efficiency and better scalability for large scale WSNs. However, these algorithms may reach their local minimum, which will create routing dead end or loops. In geographic routing, the source will choose the immediate neighboring node to forward the message hop by hop from the source to the destination.

However, the existing research on geographic routing focuses largely on routing efficiency and routing dead end and loop issues through combined greedy and facing routing protocols [6], [7] and local broadcast [8]. Although there have been many research papers dealing with the lifetime of wireless sensor networks, only a few of them are related to energy aware geographic routing [9]–[11]. How to balance the energy consumption and thereby increase the network lifetime remains a problem for geographic routing protocols.

In addition, exposure of routing information presents significant security threats to WSNs. By acquisition with the location and routing information, the adversaries may be able to traceback the source node easily. To solve this problem, several schemes have been proposed to provide source-location privacy through secure routing protocol design [3], [12]–[14]. However, to the best of our knowledge, none of these schemes have considered energy balance and provide quantitative source-location information leakage and security analysis.

In [2], we developed criteria to quantitatively measure source-location information leakage and security of routing-based schemes through source-location disclosure index (SDI) and source-location space index (SSI).

The SEAR protocol was proposed to address routing security and energy balance through a quantitative control of routing security and energy balance. We have demonstrated through extensive OPNET simulations that SEAR can provide an excellent energy balance and a high message delivery ratio with only a very moderate routing overhead. In this paper, we further analyze the relationship between the routing overhead and the security levels quantitatively. For a given routing cost factor, we also derive a numerical method to determine the corresponding security parameter. The numerical results provide a tight approximation of the actual results. We also perform quantitative security analysis of the SEAR protocol based on the criteria proposed in [2].

VII. Conclusions

In this paper, we first performed a theoretical analysis for the relationship between routing security and energy efficiency in SEAR routing protocol. We derived a numerical formula to estimate the number of routing hops based on the routing security level. The numerical method provides a very tight estimation on the number of the actual routing hops. We also provided an algorithm to determine the security parameter for a given energy consumption. Finally, we performed quantitative security analysis based on the criteria proposed in [2]. The security analysis also demonstrates that the SEAR routing protocol can provide an excellent source-location privacy.

Acknowledgements

This research was supported in part by the NSF under grants CNS-0845812 and CNS-1050326, and CNS-1117831.

References

[1] D. Tang, T. Jiang, and J. Ren, "Secure and energy aware routing (sear) in wireless sensor networks," in *Proceedings of IEEE Globecom 2010*, (Miami, FL), December 6-10, 2010.

[2] Y. Li, J. Ren, and J. Wu, "Quantitative measurement and design of source-location privacy schemes for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, accepted, to appear.

[3] Y. Li and J. Ren, "Preserving source-location privacy in wireless sensor networks," in *Proceedings of IEEE SECON 2009*, (Rome, Italy.), June 22-26, 2009.

[4] H. Chan and A. Perrig, "Pike: peer intermediaries for key establishment in sensor networks," *Proceedings of IEEE INFOCOM*, vol. 1, pp. 524–535 vol. 1, March 2005.

[5] WikipediA, "Quartic function." http://en.wikipedia.org/wiki/Quartic_function.

[6] B. Karp and H. T. Kung, "GPSR: Greedy perimeter stateless routing for wireless networks," in *MobiCom'2000*, (New York, NY, USA), pp. 243 – 254, 2000.

[7] T. Melodia, D. Pompili, and I. Akyildiz, "Optimal local topology knowledge for energy efficient geographical routing in sensor networks," in *Proc. IEEE INFOCOM*, vol. 3, pp. 1705 –1716 vol.3, March 2004.

[8] Q. Fang, J. Gao, and L. Guibas, "Locating and bypassing routing holes in sensor networks," in *Proc. IEEE INFOCOM*, vol. 4, pp. 2458 – 2468, march 2004.

[9] G. Zhao, J. Li, X. Liu, and A. Kumar, "Lifetime-aware geographic routing in wireless sensor networks," in *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery 2009*, pp. 355 –362, Oct. 2009.

[10] I. Stojmenovic and X. Lin, "Power-aware localized routing in wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 12, pp. 1122 –1133, Nov. 2001.

[11] J. Kuruvila, A. Nayak, and I. Stojmenovic, "Hop count optimal position-based packet routing algorithms for ad hoc wireless networks with a realistic physical layer," *IEEE Journal on Selected Areas in Communications*, vol. 23, pp. 1267 – 1275, june 2005.

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

[13] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," in *SASN*, pp. 88–93, ACM, 2004.

[14] Y. Li and J. Ren, "Source-location privacy through dynamic routing in wireless sensor networks," in *Proceedings of IEEE INFOCOM 2010*, (San Diego, USA.), March 15-19, 2010.