A Secure Routing Protocol and its Application in Multi-sink Wireless Sensor Networks

Nike Gui, Jianbin Hu, Zhong Chen
Institute of Software, School of Electronics Engineering and Computer Science, Peking University, China
Key Laboratory of High Confidence Software Technologies (Peking University), Ministry of Education, China
Email: gnnike@gmail.com, hjbin @infosec.pku.edu.cn, chen @infosec.pku.edu.cn

***Abstract*—Wireless sensor networks are increasingly deployed in security-critical areas, such as battle field. However, general sensor nodes are manufactured with inexpensive components, and they are short of security enhancement. Therefore, an adversary could capture and compromise sensor nodes easily, then launch some malicious attacks (including tampering or discarding useful data collected from source nodes). In this paper, we propose a secure routing and aggregation protocol with low energy cost for sensor networks (named STAPLE), which utilizes one-way hash chain and multi-path mechanism to achieve security of wireless sensor networks, and develop a network expanding model to control communication cost incurred by multi-path routing. Then we discuss the protocol application in multi-sink wireless sensor networks. Finally, we perform the simulation of STAPLE in comparison with INSENS, the results demonstrate that STAPLE achieves a higher level security with considerably low communication overhead.**

***Index Terms*—Wireless sensor networks, Security, Low energy cost, Multi-sink**

I. INTRODUCTION

Recent advances in wireless communications and electronics have enabled the development of low cost, multifunctional sensor nodes that are small in size and communicate wirelessly in short distances. Wireless sensor networks offer economically solutions for various applications (e.g., health, military, home), and they are increasingly deployed in security-critical areas [1], such as battle field. In battle field, for example, the rapid deployment, self-organization, and fault tolerance characteristics of sensor networks make them a very promising sensing technique for military command, control, communications, computing, intelligence, surveillance, reconnaissance, and targeting systems.

Because sensor networks pose unique challenges, traditional security techniques used in traditional networks cannot be applied directly. First, to make sensor networks economically viable, sensor devices are limited in their energy, computation, and communication capabilities. Second, unlike traditional networks, sensor nodes are often deployed in accessible areas, presenting the added risk of physical attack. And third, sensor networks interact closely with their physical environments and with people, posing new security problems. Therefore, sensor nodes containing the keys or communication protocols, could be captured and analyzed easily [2] [3] [4] after deployment. Then they may be forged and put back into sensor networks without being noticed. Finally, the adversary may launch a variety of attacks [5] [6], such as selective forward data and tamper data. Furthermore, wireless sensor nodes are powered by batteries, so they only have limited energy capacity [7], and the computation and communication cost should be strictly controlled. These circumstances pose critical challenges to protocol designers.

In some applications, several thousands of sensor nodes might be deployed over the monitored region, such large-scale sensor networks would be necessary. Moreover, the diameter of the region might easily be several kilometers. In this case, scalability of the network is a very important design issue. In order to obtain a scalable network, the sensor nodes should be divided into clusters. The nodes within a cluster will then be connected to the sink nodes dedicated for that cluster. During the design phase of a large-scale sensor network, the designer should decide on the number of clusters, and more important than that, the optimum locations of the sink nodes. We call this problem as the "multiple sink sensor network design problem" and try to provide some solutions.

Various mechanisms and protocols have been proposed with emphasis on secure aggregation [8] ,multi-path routing [9] and multi-sink sensor networks [19]. However, our key observation is that communication cost is not directly taken into account in the previous work, and how many sink nodes should be deployed to achieve cost-effective goal is not theoretically analyzed. So we develop a Secure rouTing and Aggregation Protocol with Low Energy cost for sensor networks, named STAPLE. We design it to achieve a tradeoff between security and communication cost: on one hand, we combine one-way hash chain and multi-path routing to achieve security in sensor network; on the other hand, we develop a network expanding model and utilize a limit to control communication cost. Finally, we utilize this model to analyze the cost-effective number of sink nodes.

We compare performance of STAPLE with that of INSENS, the results of which show that STAPLE makes better use of network redundancy, and it can tolerate larger node failure ratios of sensor networks. In large scale sensor networks, performance of STAPLE is similar with that of INSENS. The rest of this paper is organized as follows. Section 2 will present related work in wireless

doi:10.4304/jnw.5.5.535-542

networks. Section 3 gives assumptions and terminologies. Details of STAPLE are proposed in section 4. Simulation and evaluation are given in section 5. The last section is our conclusion and future work.

II. RELATED WORK

A. One-way Hash Chain

Using message authentication code (MAC), Zhu et al. presented an interleaved hop-by-hop authentication scheme [10], which guarantees the base station detects injected false data packets, when no more than a certain number nodes are compromised. But this scheme requires each cluster has fixed nodes, such as 3, 4, or 5. Yang et al. proposed SDAP [11], based on the principles of divide-and-conquer and commit-and-attest, is a general-purpose secure aggregation protocol applicable to multiple aggregation functions. The spirit of SDAP is similar to Merkle hash tree [12]. Nevertheless, communication cost of SDAP is fairly high. Ye et al. presented a statistical en-route filtering (SEF) mechanism [13] that can detect and drop false reports injected by compromised nodes. Each sensing data should be validated by MAC, which is generated by a node that detects the same event. But SEF needs a global key pool and key distribution before sensor deployment. Chan et al. presented an algorithm for provably secure hierarchical in-network data aggregation [14]. It is guaranteed to detect any manipulation of aggregation by adversary beyond what is achievable through direct injection of data values at compromised nodes.

B. Multi-path Routing

Deng et al. provided two secure strategies [15]. First, secure multi-path routing to multiple destination base stations is designed to provide intrusion tolerance against isolation of a base station. Second, anti-traffic analysis strategies are proposed to help disguise the location of base station from eavesdroppers. Then Deng et al. described an INtrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS) [9], the key object is to tolerate damage caused by an intruder, who has compromised deployed sensor nodes and is intent on injecting, modifying, or blocking packets. INSENS is an important multi-path routing protocol for wireless sensor networks, but the routing tables of sensor nodes are computed in sink node, this may cause a high computation cost in sink node and a high communication cost to distribute the routing tables, especially in large scale sensor networks. Other researchers are also productive in this area. Lee et al. proposed a distributed secure multi-path solution [16] to route data across multiple paths so that intruders require much more resources to mount successful attacks. Nassr et al. addressed the problems of scalability and reliability in sensor network routing through a simple but powerful scheme [17] implemented on Mica2 motes, which significantly improves upon results from standard TinyOS [18] routing implementation of MINTRoute. Multi-path routing is efficient in false node tolerance, however, it causes fairly high communication cost, which is a critical problem in wireless sensor networks.

C. Multi-sink

In [19], Oyman et al. proposed a multiple sinks WSN architecture where the network is partitioned into clusters. All the sources in a cluster were assigned to send the data to the sink designated to that particular cluster. In [20], Thulasiraman et al. considered a multi-drain sensor network. Data from each source is logged into two distinct drains for data collection to be resilient to any single drain failure. In [21], the upper and lower bounds for the optimal solution of the multiple sink problem are obtained. It is shown that the bounds are tight for networks with a large number of nodes. As stated in [22]. While incrementing the number of sink nodes by one, the network lifetime is evaluated. The search will stop, whenever the desired lifetime is reached.

III. ASSUMPTIONS AND TERMINOLOGIES

We assume that a large number of sensor nodes and several sink nodes are contained in a sensor network. Sensor nodes have limited memory, energy capacity, computation and communication capabilities, consequently, they are easy to be compromised. While sink nodes are security-enhanced and difficult to be compromised. Each sensor node contains several items of information, shown in Table I.

TABLE I.
PARAMETERS OF SENSOR NODES

Information of Node	Description
ID	The unique integer in network allocated to a sensor node.
level	The minimum number of hops away from the sink node.
key	A node has one or more keys, generated by its parents' keys with HMAC function. They are utilized to encrypt data and authenticate children's identity.
MAC	A node has only one MAC, generated by its own ID with HMAC function. It is utilized to authenticate source node's identity.
parents	A node's neighboring nodes in the previous level.
brothers	A node's neighboring nodes in the same level.
children	A node's neighboring nodes in the next level.

TABLE II.
PARAMETERS OF NETWORK

Parameter of Network	Description
m	The number of sink nodes contained in a network.
n	The number of sensor nodes contained in a network.
a	The price or financial cost of a sink node.
b	The price or financial cost of a sensor node.
r	The communication radius of sensor nodes.
d	The average distance between sensor nodes.
e	The energy capacity of a sensor node.
t	The energy consumption in a wireless communication session, e.g. sending and receiving a data packet.

There are *m* sink nodes and *n* sensor nodes deployed in sensor network. These nodes are divided into *m* clusters, each of which contains one sink node and $\frac{n}{m}$ sensor nodes. The price of a sink node is *a* and the price of a sensor node is *b*, usually *a* is much higher than *b*. Communication area of a sensor node is round, the radius of which is *r*, and the average distance between them is *d*. To guarantee all the nodes could communicate, the length of r must be larger than that of *d*. A sensor node has energy capacity of *e*, and the energy consumption in each communication session is *t*, that means a sensor node can send and receive $\frac{e}{t}$ data packets. The parameters of network are shown in Table II.

An adversary could capture a small ratio of sensor nodes, then he can fetch the keys and the MACs, and analyze protocols or algorithms exactly. We assume the adversary could control the compromised nodes to launch a variety of attacks. However, no sensor node has been compromised before deployment.

The following notations are used in the description of our protocol:

- *m1|m2* denotes the concatenation of two messages *m1* and *m2*.
- *E(k, m)* refers to the encryption of message *m* using key *k*.

HMAC(k, m) is the message authentication code (MAC) of message *m* with key *k*.

IV. THE DETAIL OF STAPLE

A. Network Initialization

After deployment of sensor network, STAPLE is launched by sink node. It organizes sensor nodes in different levels according to the minimum hops away from sink node, then generates keys and MACs and builds hash chains for sensor nodes. STAPLE achieves three goals during this phase: First, find all the sensor nodes hop by hop; Second, organize sensor nodes into different levels, and build parent-brother-child relationships between them; Third, generate key(s) and a MAC for each sensor node.

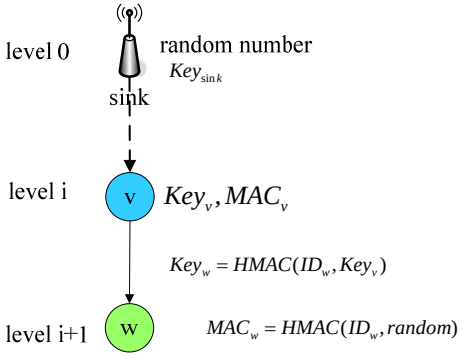

Figure 1. Network Initialization

At the beginning, sink node generates $key_{\sin k}$ and a *random* number, then broadcasts a HELLO packet to find its neighbors (the nodes located in one communication hop of the sink). Sink node computes neighbors' keys, and sends them to its neighbors, including the random number. Neighboring nodes utilize the random number to compute their own MACs. As shown in Figure 1, node *v* in level *i* finds node *w* in level *i*+1.

The discovering and computation steps are as follows:

1) v broadcasts HELLO packet.

2) w sends ACK packet to v, containing ID_w.

3) v computes $key_w = HMAC(ID_w, key_v)$.

4) v sends key_w *and the random number (generated by sink node) to w.*

5) v deletes the random number from memory.

6) w computes $MAC_w = HMAC(ID_w, random)$.

After all nodes are discovered, the initialization phase ends up. If a node has *n* parents, it has *n* keys. However, each sensor node has only one MAC.

B. Data Transmission and Filtering

After initialization phase, source node generates data, sending it to its parents. Then parents transmit data packets to grandparents. Hop by hop, the packet is authenticated or filtered by the intermediate nodes. During this phase, STAPLE achieves the following three goals: First, authenticate child node's identity; second, authenticate data integrity; Third, filter out false data packet. As shown in Figure 2, node w generates data, and sends a packet to parent v with the following format:

$$w \to v : ID_w \mid E(key_w, Data \mid HMAC(key_w, Data) \mid HMAC(MAC_w, Data))$$

In this packet, *w* encapsulates ID_w, utilizes key_w to encrypt data and two message digests: $HMAC(key_w, Data)$ and $HMAC(MAC_w, Data)$. On receiving this packet, *v* executes the following steps for authentications:

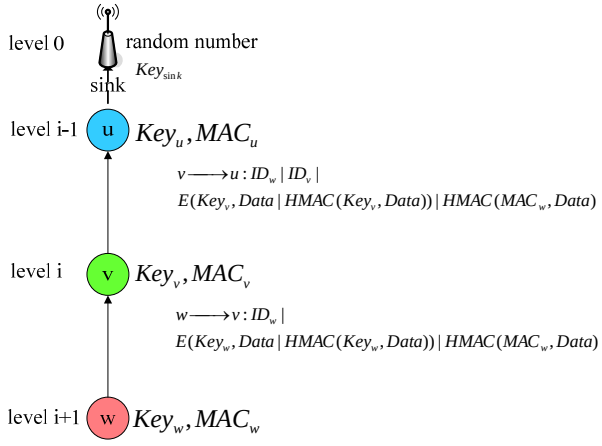

Figure 2. Data Transmission and Filtering

7) v first gets ID_w.

8) v re-computes key_w *with HMAC function:* $key_w = HMAC(ID_w, key_v)$.

9) v decrypts data packet with key_w.

10) v re-computes value of $HMAC(key_w, Data)$ *, compares it with the message digest* $HMAC(key_w, Data)$ *contained in data packet.*

11) If the two values are identical, v transmits data to its parent u; otherwise, v discards the packet.

If the packet is not discarded, it will be transmitted to *v*'s parent *u* with the following format:

$$w \to v : ID_w \mid ID_v \mid E(key_v, Data \mid HMAC(key_v, Data) \mid HMAC(MAC_w, Data))$$

On receiving the new data packet, *u* executes similar steps with *v*.

C. Source Authentication in Sink

When sink node receives data packets, it will authenticate their sources. In this phase, STAPLE achieves the following two goals: First, authenticate the identity of source node; Second, authenticate the integrity of data. Sink node does the following steps to achieve these two goals:

12) Decrypt the packet, get data and message digest from source node w.

13) Get ID_w *from the packet.*

14) Compute MAC_w *with:*

$$MAC_w = HMAC(ID_w, random).$$

15) Computes the message digest with MAC_w*:*

$$HMAC(MAC_w, Data).$$

16) Compares these two message digests: one is decrypted from the packet, the other is computed in the previous step.

17) If they are identical, data is accepted; otherwise, data has been tampered.

To prevent intermediate nodes' malicious behaviors, sink node utilizes the random number, remaining only in sink node, to compute source node's MAC for authentication. We can guarantee that no intermediate node can compute the source node's MAC, because it does not have the random number. However, if the source node's MAC has been leaked, an adversary may forge a compromised source node and generate false data. This problem is described in the last section.

D. Network Expanding Model in one cluster

First we analyze one cluster, which contains one sink node and $\frac{n}{m}$ sensor nodes. Since multi-path mechanism is used in STAPLE to tolerate false nodes and it may cause high communication cost, we develop a mathematical model to evaluate the effect. In this section, we focus on the network expanding model, and find the factors influencing node's number of parents ss(Multi-path mechanism is built by transmitting data to multiple parents.), then we give some effective mechanisms to limit communication cost.

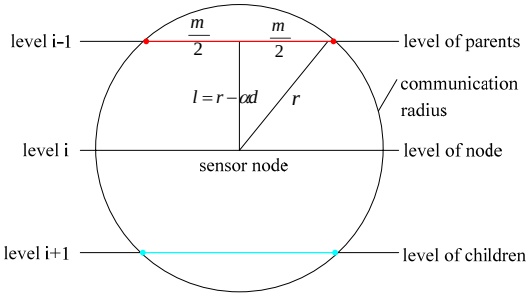

Figure 3. Number of a Node's Parent

Lemma 1. *The number of parents is shown as following:*

$$\sqrt{\frac{8\alpha r}{d} - 4\alpha^2} \quad (0 < \alpha < 1)$$

r is the communication cost, d is the average distance between sensor nodes.

Proof: The distance between two adjacent levels of sensor nodes is *l*. The distance between a sensor node and its neighbors in adjacent level must be shorter than communication radius *r*; but on average there must be a sensor node in the distance of *r-d*, because the average distance between sensor nodes is *d*. We can get the relationship: $r - d < l < r$, and we get the following assumption:

$$l = r - \alpha d \quad (0 < \alpha < 1)$$

As shown in Figure 3, a node is located in level *i*, and its parents are located in level *i−1*, while its children are located in level *i+1*. Parents should also be covered by communication radius, so we assume the length of level *i* remaining in the circle is *m*. Based on theory of trigonometry, we have the following equation:

$$m = 2\sqrt{r^2 - l^2} = 2\sqrt{r^2 - (r - \alpha d)^2}$$
$$= 2\sqrt{2\alpha r d - \alpha^2 d^2} \quad (0 < \alpha < 1)$$

A sensor nodes' number of parent P_{parent} is as following:

$$P_{parent} = \frac{m}{d} = \frac{2\sqrt{2\alpha r d - \alpha^2 d^2}}{d} = \sqrt{\frac{8\alpha r}{d} - 4\alpha^2} \quad (0 < \alpha < 1) \quad (1)$$

Lemma 1 indicates that number of parents has a direct relationship with the ratio of *r* and *d*. If sensor nodes need more parents, we should increase *d*, or decrease *r*. With the same computation process, we can get the number of children:

$$P_{child} = \sqrt{\frac{8\alpha r}{d} - 4\alpha^2} \quad (0 < \alpha < 1)$$

Without loss of generality, we let α = 0.5, then we can get some useful examples, then adjust *r* or *d* to keep a suitable number of parents:

- when $r = \frac{5d}{4}, P_{parent} = 2;$
- when $r = \frac{5d}{2}, P_{parent} = 3;$

Lemma 2. *The number of levels is shown as following:*

$$\frac{\sqrt{\frac{4nd}{\pi m(r-\alpha d)}+1}-1}{2} \quad (0<\alpha<1)$$

Proof: There are $\frac{n}{m}$ sensor nodes deployed in a cluster, which are organized on x levels. These levels could be considered as a series of concentric circles, expanding from the sink to the edge of network, so their radiuses range from l to $x \times l$. The total girth of these circles are $\sum_{i=1}^{x} 2\pi l i$. Then we can get the following equation:

$$\frac{n}{m} = \frac{\sum_{i=1}^{x} 2\pi l i}{d} = 2\pi l \frac{x(x+1)}{2d}$$

$$x = \frac{\sqrt{\frac{4nd}{m\pi l}+1}-1}{2} = \frac{\sqrt{\frac{4nd}{\pi m(r-\alpha d)}+1}-1}{2} (0<\alpha<1)$$

Lemma 2 indicates that number of levels scales as $O(\sqrt{\frac{n}{m}})$. If r becomes larger, the number will be smaller. However, the influence of d is more complex.

Lemma 3. *The communication cost in one cluster could be controlled under a constant:* e^c.

Proof: If a packet is sent by a source node, and it is not discarded by intermediate nodes, the number of packets arriving at the sink node is shown as follows:

$$N_{packet} = (P_{parent})^x = \sqrt{\frac{8\alpha r}{d} - 4\alpha^2}^{\frac{\sqrt{\frac{4nd}{\pi m(r-\alpha d)}}+1-1}{2}} \quad (2)$$

We could see it scales as $O(a^{\sqrt{\frac{n}{m}}})$. To control the communication cost, we modify P_{parent}:

$$P_{parent} = 1 + \frac{c}{x}$$

c is a constant, x is the number of levels. Then number of packets becomes:

$$N_{packet} = P_{parent}^x = (1+\frac{c}{x})^x$$

Using the limit: $\lim_{r->\infty}(1+\frac{1}{r})^r = e$, We order $r = \frac{x}{c}$, and get the following equation:

$$\lim_{x->\infty}(1+\frac{c}{x})^x = \lim_{rc->\infty}(1+\frac{c}{rc})^{rc} = \lim_{r->\infty}(1+\frac{1}{r})^{rc} = e^c \quad (3)$$

So the number of packets could be controlled under the constant: e^c, c is used to control number of packets in detail. This process could be executed in distributed manner without the participation of sink node.

E. Application in multi-sink sensor networks

In large-scale networks with a large number of sensor nodes, multiple sink nodes should be deployed, not only to increase the manageability of the network, but also to reduce the energy dissipation at each node. Therefore, for an economically feasible investment, the designer should focus on correct placement and optimal number of the sink nodes. In [19], several approaches have been discussed for the correct placement, while in this paper so we focus optimal number of sink nodes. Deploying multiple sink nodes is necessary in large-scale sensor networks, but sink node is much more expansive than sensor node, so deploying too many sink nodes might be not economical.

Then we define a concept: *round*, in a round, each sensor node sends one data packet to its sink node through single path. As the total energy of sensor network is limited, the number of rounds is also limited.

Lemma 4. *The number of sensor network rounds is as following:*

$$\frac{ne}{\frac{ntl}{3(r-\alpha d)}\sqrt{\frac{4nd}{\pi m(r-\alpha d)}}}$$

Proof: In one round of a cluster, the consumed communication energy is as following:

$$t\sum_{i=1}^{x} i \times \frac{2\pi i \times l}{d} = \frac{2\pi l}{d}\sum_{i=1}^{x} i^2 = \frac{\pi t l}{3d} x(x+1)(2x+1) \approx \frac{2\pi l}{3d} x^3$$

$$= \frac{2\pi t l}{3d}(\frac{\sqrt{\frac{4nd}{\pi m(r-\alpha d)}+1}-1}{2})^3$$

Then considering all the sensor nodes, the total consumed communication energy is as following:

$$m \times consumed\ energy\ in\ one\ cluster = m \times \frac{2\pi t l}{3d}(\frac{\sqrt{\frac{4nd}{\pi m(r-\alpha d)}+1}-1}{2})^3$$

$$\approx m \times \frac{2\pi t l}{3d}(\frac{\sqrt{\frac{4nd}{\pi m(r-\alpha d)}}}{2})^3 = \frac{ntl}{3(r-\alpha d)}\sqrt{\frac{4nd}{\pi m(r-\alpha d)}}$$

But the total energy of sensor nodes is limited: ne, so we could get the number of sensor network rounds as follows:

$$\frac{totoal\ energy}{energy\ cost\ in\ one\ round} = \frac{ne}{\frac{ntl}{3(r-\alpha d)}\sqrt{\frac{4nd}{\pi m(r-\alpha d)}}}$$

Lemma 5. *The economical cost in a sensor network round is as following:*

$$\frac{lt}{3e(r-\alpha d)}\sqrt{\frac{4nd}{\pi(r-\alpha d)}}(a\sqrt{m}+b\frac{n}{\sqrt{m}})$$

Proof: Based on assumptions, the total economical cost of a sensor network is $ma + nb$, so the economical cost in a sensor network round is as following:

$$\frac{total\ economical\ cost}{number\ of\ rounds} = \frac{ma+nb}{\frac{ne}{\frac{ntl}{3(r-\alpha d)}\sqrt{\frac{4nd}{\pi m(r-\alpha d)}}}}$$

$$= \frac{lt}{3e(r-\alpha d)}\sqrt{\frac{4nd}{\pi(r-\alpha d)}}(a\sqrt{m}+b\frac{n}{\sqrt{m}})$$

Based on Lemma 5, when $a\sqrt{m} = b\frac{n}{\sqrt{m}}$, the economical cost in a sensor network round is minimal. That means when there are $\sqrt{\frac{nb}{a}}$ sink nodes deployed in a sensor network, we can get the minimal economical cost, so the optimal number of sink nodes is $\sqrt{\frac{nb}{a}}$.

V. SIMULATION AND EVALUATION

In this section, we compare the performance of STAPLE with a classic secure routing protocol (INSENS). Performance under different numbers of parents are shown in Figure 5, Figure 6, Figure 7 and Figure 8. From these four figures, we can get the following results:

- Compared with INSENS, STAPLE transmits data packet to sink node with higher possibilities.
- As false node ratio increases, the possibility of successfully transmitting data to sink decreases.
- As number of parents increases, the possibility of successfully transmitting data to sink increases both in STAPLE and INSENS.

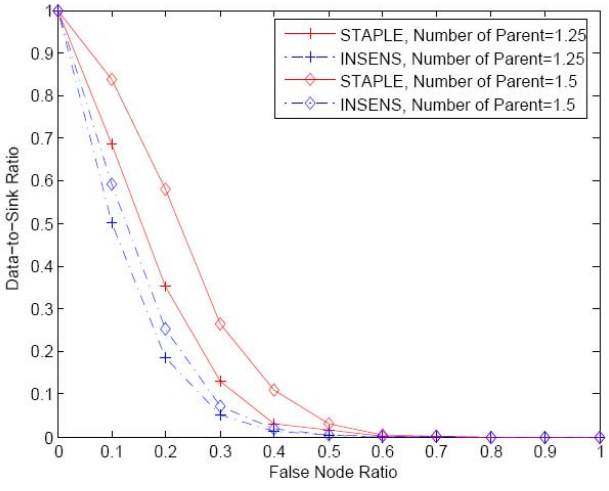

Figure 4. Number of parents = 1.25 and 1.5

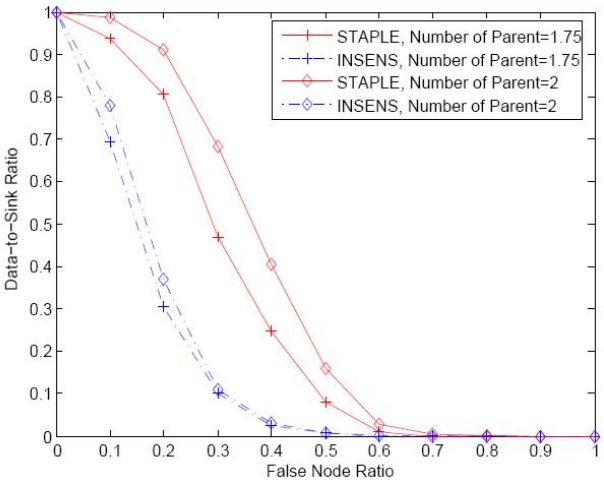

Figure 5. Number of parents = 1.75 and 2

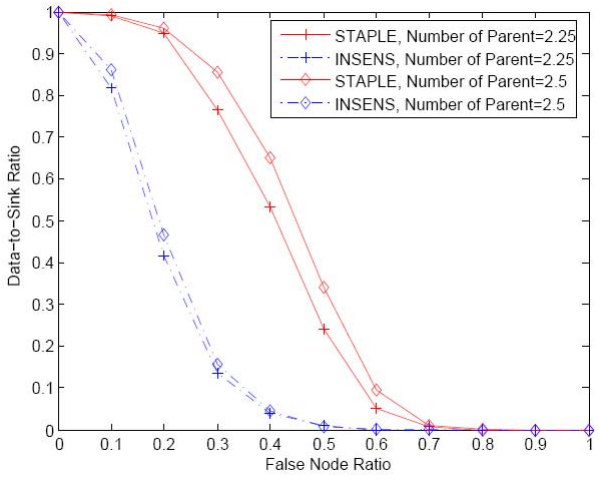

Figure 6. Number of parents = 2.25 and 2.5

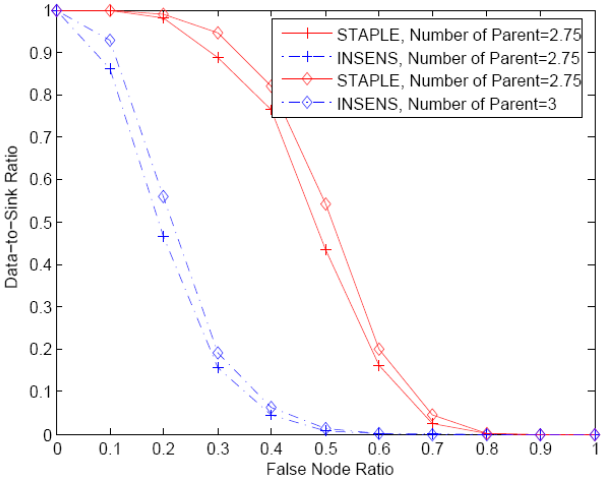

Figure 7. Number of parents = 2.75 and 3

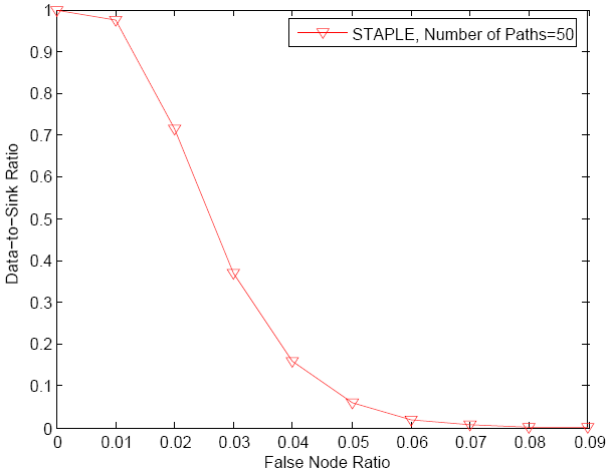

Figure 8. STAPLE in Large-scale networks

The performance of STAPLE in large scale sensor networks is evaluated in Figure 8, and the data transmission policy is modified based on equation 2 and equation 3: the packet number incurred by multi-path routing is limited into a constant, such as 50 in our simulation. When false node ratio increases, the possibility of successfully transmitting data to sink node decreases.

VI. CONCLUSION AND FUTURE WORKS

This paper proposes the notion of a tradeoff between security and communication cost. The security is achieved via one-way hash chain and multi-path routing mechanism; and control of communication cost is based on the network expanding model and a mathematical limit. Then we discussed the optimal number of sink nodes in multi-sink sensor networks. Finally, from the performance evaluation, our scheme achieves a significant improvement under node failure or selective forwarding attack, compared with INSENS. Our future work includes the follows:

- Evaluate our scheme in realistic applications of wireless sensor networks.
- Consider maintenance of STAPLE, e.g. the key resetting and topology repair caused by network dynamics.

ACKNOWLEDGMENT

The authors wish to thank Ruichuan Chen, Zhuhua Cai. This work was supported in part by a grant from the National Natural Science Foundation of China under No.60873239.

REFERENCES

[1] A. Perrig, J. A. Stankovic, and D. Wagner, “Security in wireless sensor networks,” Commun. ACM, vol. 47, no. 6, pp. 53–57, 2004.
[2] H. Chan and A. Perrig, “Security and privacy in sensor networks,” IEEE Computer, vol. 36, no. 10, pp. 103–105, 2003.
[3] X. Chen, K. Makki, K. Yen, and N. Pissinou, “Node compromise modeling and its applications in sensor networks,” in ISCC, 2007, pp. 575–582.
[4] Q. Zhang, T. Yu, and P. Ning, “A framework for identifying compromised nodes in wireless sensor networks,” ACM Trans. Inf. Syst. Secur., vol. 11, no. 3, 2008.
[5] J. Newsome, E. Shi, D. X. Song, and A. Perrig, “The sybil attack in sensor networks: analysis & defenses,” in IPSN, 2004, pp. 259–268.
[6] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks,” IEEE Computer, vol. 35, no. 10, pp. 54–62, 2002.
[7] Y. S. Ian F. Akyildiz, Weilian Su and E. Cayirci, “A survey on sensor networks,” IEEE Communications Magazine, 2002.
[8] B. Przydatek, D. X. Song, and A. Perrig, “Sia: secure information aggregation in sensor networks,” in SenSys, 2003, pp. 255–265.
[9] J. Deng, R. Han, and S. Mishra, “Insens: Intrusion-tolerant routing for wireless sensor networks,” Computer Communications, vol. 29, no. 2, pp. 216–230, 2006.
[10] S. Zhu, S. Setia, S. Jajodia, and P. Ning, “An interleaved hop-byhop authentication scheme for filtering of injected false data in sensor networks,” in IEEE Symposium on Security and Privacy, 2004, pp. 259– 271.
[11] Y. Yang, X. Wang, S. Zhu, and G. Cao, “Sdap: a secure hop-by-hop data aggregation protocol for sensor networks,” in MobiHoc, 2006, pp. 356–367.
[12] R. C. Merkle, “A certified digital signature,” in CRYPTO, 1989, pp. 218–238.
[13] F. Ye, H. Luo, S. Lu, and L. Zhang, “Statistical en-route filtering of injected false data in sensor networks,” in INFOCOM, 2004.
[14] H. Chan, A. Perrig, and D. X. Song, “Secure hierarchical in-network aggregation in sensor networks,” in ACM Conference on Computer and Communications Security, 2006, pp. 278–287.
[15] J. Deng, R. Han, and S. Mishra, “Intrusion tolerance and anti-traffic analysis strategies for wireless sensor networks,” in DSN, 2004, pp. 637– .
[16] P. P. C. Lee, V. Misra, and D. Rubenstein, “Distributed algorithms for secure multipath routing in attack-resistant networks,” IEEE/ACM Trans. Netw., vol. 15, no. 6, pp. 1490–1501, 2007.
[17] M. S. Nassr, J. Jun, S. Eidenbenz, A. A. Hansson, and A. M. Mielke, “Scalable and reliable sensor network routing: Performance study from field deployment,” in INFOCOM, 2007, pp. 670–678.
[18] “Tiny operating system. uc berkeley.” http://tinyos.net/.
[19] E. I. Oyman and C. Ersoy, “Multiple sink network design problem in large scale wireless sensor networks,” in Proc. of IEEE ICC, Paris, France, June 2004.
[20] P. Thulasiraman, S. Ramasubramanian, and M. Krunz, “Disjoint multipath routing to two distinct drains in a multi-drain sensor network,” in Proc. of IEEE INFOCOM, Anchorage, Alaska, May 2007.
[21] V. Shah-Mansouri and V. W. S. Wong, “Bounds for lifetime maximization with multiple sinks in wireless sensor networks,” in Proc. of IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, Victoria, Canada, Aug. 2007.
[22] J. J. F. Hair, R. E. Anderson, R. L. Tatham and W. C. Black, Multivariate Data Analysis with Readings, Prentice-Hall, Inc., 1995.

Nike Gui received B.S. degree in computer science and technology from University of Electronic Science and Technology of China in 2005. He is currently a Ph.D. candidate advised by Prof. Zhong Chen in the School of Electronics Engineering and Computer Science at Peking University. His technical interest includes wireless sensor network protocols, security and software engineering and he has published two papers in such areas. His current work is supported by the National Natural Science Foundation of China under Grant No.60873239.

Jianbin Hu is an associate professor of the Network and Information Security Research Group of the Software Institute, Peking University. He received his PhD in Computer Science from Peking University. His technical interest includes network security and embedded systems. He has published five papers in his interested areas. He is currently the leader of many projects, which contain the project of the National Natural Science Foundation of China under Grant No.60873239.

Zhong Chen is a professor of the Software College of Peking University and director of the Network and Information Security Research Group of the Software Institute, Peking University. He is engaged in research on System-on-chip and SW/HW co-design tools and methodology in the ICCAD Research Lab of the Department of Computer Sciences of UCLA from April 2001 to December 2002. He is also an -
IEEE and Computer Society Member
- Senior Member of Chinese Institute of Electronics since 1996
- Managing Director of Directorate of China Software Industry Association since 1998
- Co-chair of professional committee of Information Security and Privacy of China Computer Federation since 2002
- Expert of Technical Auditing Committee of securities online trading, China Securities Regulatory Commission
- Vice-chairman of Editorial Committee of the Journal of Network Security Technologies and Application since 2001