Computer Communications 34 (2011) 591–597

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Energy-efficient and high-accuracy secure data aggregation in wireless sensor networks ☆

Hongjuan Li, Kai Lin, Keqiu Li *

School of Computer Science and Technology, Dalian University of Technology, No. 2, Linggong Road, Dalian 116024, China

ARTICLE INFO

Article history:
Available online 1 March 2010

Keywords:
Wireless sensor works
Data aggregation
Security
Protocol

ABSTRACT

Due to the inherent characteristics of resource-constrained sensors, communication overhead is always a major concern in wireless sensor networks (WSNs). Data aggregation is an essential technique to reduce the communication overhead and prolong network lifetime. Since data aggregation results are usually used to make critical decisions, the accuracy of final aggregation results is very important. Furthermore, as wireless sensor networks are increasing being deployed in security-critical applications, we should take security into consideration as well. Therefore, for such applications, data aggregation protocols must be highly energy efficient and highly accurate while being able to prevent an adversary from stealing private data held by each sensor node. In this paper, we propose an energy-efficient and high-accuracy (EEHA) scheme for secure data aggregation. The main idea of our scheme is that accurate data aggregation is achieved without releasing private sensor readings and without introducing significant overhead on the battery-limited sensors. We conduct extensive simulations to evaluate the performance of EEHA. Our analysis and simulations show that EEHA is more efficient and accurate than the existing scheme.

1. Introduction

Wireless sensor networks are becoming increasingly popular in many applications [1–4] such as military surveillance and civilian usage. A wireless sensor network is composed of hundreds or thousands of tiny resource-constrained sensors, equipped with non-rechargeable batteries. For such sensors, transmission is much more energy consuming than computation. Therefore, the amount of communication overhead should be kept as low as possible, in order to extend the lifetime of wireless sensor networks (WSNs).

Large sensor networks usually generate substantial amounts of data, and as in many cases, there is high redundancy in their raw data. Hence, it is important to design efficient data processing technique to reduce redundant data and the amount of transmission. Data aggregation [6–10] is an essential paradigm to eliminate data redundancy and save energy. During a typical data aggregation process, sensor nodes are organized into a tree hierarchy rooted at the base station (BS). The non-leaf nodes act as aggregators, fusing data collected from their child nodes and forwarding the aggregated results towards the BS. In this way, only aggregated data are returned to the base station, rather than the summation of the data generated in each node. Compared with the centralized approach where all raw data are returned, data aggregation can reduce communication overhead significantly and hence increase the lifetime of WSNs.

Aggregation accuracy is desired for the final decision which is based on the aggregation result, especially for some sensitive applications where a small difference of result may lead to completely different decisions. In applications such as battlefield surveillance and forest fire monitoring, such variation deviating from the accurate result may lead to very severe consequences. Therefore, aggregation accuracy is an important criterion for data aggregation scheme.

Because of the low-cost and flexibility, the sensor network has the potential to change the way of people communicating with environment and the others. Wireless sensor networks have become a popular platform for pervasive computing. For example, sensor networks may be deployed in personal environment, such as houses and human body. People might not agree to participate in these applications without privacy protection. Therefore, data aggregations in such application should address privacy-preservation.

Therefore, such environments pose a particularly challenging set of constrains for the protocol design: data aggregation must be achieved with communication overhead as low as possible and aggregation accuracy as high as possible while without private data released. However, sensor networks have their inherent limitation: energy constraints, due to the small-size and low-cost sensor nodes; security vulnerability, due to the open nature of

☆ This work is supported by NSFC under Grant Nos. 90718030 and 60973117, and New Century Excellent Talents in University (NCET) of Ministry of Education of China.

* Corresponding author.
E-mail address: keqiu@dlut.edu.cn (K. Li).

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2010.02.026

wireless communication channels and the lack of physical protection of individual sensor nodes.

Extensive research has been conducted to overcome these limitations. He et al. [5] proposed the scheme of Slice-Mix-AggRegaTe (SMART) for additive aggregation functions, which guarantees data privacy through data "slicing and assembling" technique. In the SMART scheme, each sensor node needs to slice its sensor reading randomly into a certain number (say, n) of pieces, and one piece is kept on itself, the remaining $n-1$ pieces are securely distributed to $n-1$ neighbor sensor nodes, which results in high communication overhead and more message collisions. In this paper, we introduce an energy-efficient and high-accuracy scheme for secure data aggregation for WSNs, in which the "slicing and assembling" technique is only implemented to leaf nodes of the aggregation tree, and the other nodes just send one message for aggregation. Hence, the communication overhead is greatly reduced as the number of nodes which slice their primitive data are much less than that in SMART. Less communication overhead leads to less message collisions, sequentially achieving a higher level of aggregation accuracy. In this paper, we design the energy-efficient and high-accuracy (EEHA) scheme with comprehensive consideration of the three factors, which are communication overhead, aggregation accuracy and privacy protection, and try to explore the tradeoff among them.

Extensive simulations are conducted to compare our scheme with the existing SMART scheme. The results show that our scheme can reduce communication overhead and improve aggregation accuracy, while achieving the privacy-preservation.

Compared with SMART scheme, our energy-efficient and high-accuracy scheme has the following major advantages:

- *Efficiency*: Our proposed scheme EEHA can protect data privacy with moderate extra overhead, which is much lower than that of SMART, hence our scheme has less bandwidth and energy consumption.
- *Accuracy*: Experimental results show that our proposed scheme significantly improves the level of accuracy compared with SMART.

The rest of the paper is organized as follows: In Section 2, we overview some related works on secure data aggregation. Section 3 introduces the network model and design goals. In Section 4, we give a detailed description of our scheme EEHA. Theoretical analysis and performance evaluation of our scheme are presented in Section 5. Finally, we summarize our work and give the conclusions in Section 6.

2. Related work

There has been extensive research [11–14] on data aggregation schemes in different applications. However, these aggregation schemes have been designed without security in mind. In reality, the wireless sensor networks may be deployed in a hostile environment such as battlefield, where an adversary may launch a variety of attacks. Hence, the secure data aggregation is becoming a hot research problem in some specific applications.

Several secure aggregation algorithms have been proposed for the single-aggregator model. One early secure information aggregation (SIA) protocol for WSNs called aggregate-commit-prove is given by Przydatek et al. [15]. In their model, the BS is the only aggregator, which collects all the authenticated data and computes an aggregation result over the raw data together with a commitment to the data based on Merkle-hash tree then sends them to a trustable remote user, who later challenges the aggregator to verify the aggregation. This scheme provides resistance against adversaries who try to tamper with nodes. Also for this single-aggregator model, Du et al. [18] propose a scheme using multiple witness nodes as additional aggregators to verify the integrity of the aggregator's result.

For aggregation models that have more than one aggregator, Yang et al. [16] proposed SDAP which is a tree based protocol providing certain level of assurance on the trustworthiness of the aggregation result. The design of SDAP is based on the principle of divide-and-conquer and commitment-and-attest. First, SDAP uses a novel probabilistic grouping technique to dynamically partition the nodes in a tree topology into multiple logical groups (subtrees) of similar sizes. A commitment-based hop-by-hop aggregation is performed in each group to generate a group aggregate. The base station then identifies the suspicious groups based on the set of group aggregates. Finally, each group under suspect participates in an attestation process to prove the correctness of its group aggregate. Hu and Evans [20] present a secure aggregation protocol that is resilient to single device key compromise. The protocol is resilient to aggregator nodes compromising, as long as there is no two consecutive colluding compromised aggregator nodes in the tree.

Besides, there are some schemes for filtering of injected false data in sensor networks. In [19], Zhu et al. present an interleaved hop-by-hop authentication protocol, which guarantees that the base station will detect any injected false data packets when no more than a certain number t nodes are compromised, where t is a security threshold. Ye et al. [21] propose a detection scheme called SEF: a statistical en-route filtering of injected false data, which allows both the base station and en-route nodes to detect false data with a certain probability. SEF takes advantage of the large scale and dense deployment of sensor networks to determine the truthfulness of each report through collective decision-making by multiple detecting nodes and collective false-report-detection by multiple forwarding nodes.

In privacy-preservation domain, Castelluccia et al. [17] propose a new homomorphic encryption scheme where aggregation is carried out by aggregating the encrypted data at intermediate sensors without decrypting them, resulting in higher level privacy.

3. System model and design objectives

3.1. Network model

In this paper, we assume that a sensor network consists of a large number of resource-limited sensor nodes which cooperatively accomplish a task. Due to cost constraints these sensors are not equipped with tamper-resistant hardware. In addition, there exists a powerful BS that communicate with the querier which resides outside of the network. In EEHA, the aggregation is performed over an aggregation tree rooted at the BS. There are three types of nodes in the sensor network: base station, intermediate nodes, and leaf nodes. The base station is the node where aggregation result is destined. An intermediate node serves as an aggregator node, which is responsible for forwarding queries, aggregating the received data and its own sensor reading, then forwarding the new result to its parent. The leaf nodes adopt the "slicing and assembling" technique to protect privacy; thus, they are responsible for decomposing their primitive data into pieces, sending the pieces to different neighbors, then assembling the received slices to get new results, and sending the new results to their parents.

Typical aggregation functions include SUM, AVERAGE, COUNT, MAX, MIN. In this paper, we focus on additive aggregation functions. It is worth noting that using additive aggregation functions is not too restrictive, since all the typical aggregation functions and many other functions, including variance, standard deviation can be reduced to the additive aggregation function SUM.

3.2. Attack model

Security is becoming a more and more important concern with the extensive application of sensor networks. A malicious attacker can launch a variety of attacks to break the data security. And privacy concern is one of the major obstacles to apply the wireless sensor network to civilian applications. In this paper, we mainly focus on the defence of eavesdropping to protect data privacy in wireless sensor networks.

In an eavesdropping attack, an attacker tries to overhear the transmission over wireless links to obtain private information. We assume that the attacker may know the security mechanisms that are deployed in a sensor network; he may be able to compromise a node through the radio communication channel. Each node's data should be only known to itself. Such attacks make private data released to adversaries, threatening the privacy of data held by individual sensor nodes.

Security issues in mobile ad hoc networks are similar to those in sensor networks, but the defense mechanisms developed for ad hoc networks are not directly applicable to sensor networks. Ad hoc network security mechanisms are based on public key cryptography. Public key cryptography is too expensive for sensor nodes because they are extremely resource constrained.

3.3. Design objectives

The design objective of our scheme is to achieve accurate data aggregation with moderate extra communication overhead to preserve data privacy. Therefore, a desired data aggregation scheme should satisfy the following criteria:

Efficiency: Data aggregation is an important energy-efficient technique, which reduces the resource and power usage by using in-network processing to reduce the number of messages transmitted. To achieve the goal of protecting data privacy, additional overhead is unavoidable introduced in privacy-preservation scheme. However, we should keep that overhead as small as possible.

Accuracy: Since data aggregation results may be used to make critical decisions, the accuracy of final aggregation result at root is very important for data aggregation. Even with the constraint that data privacy is not released, the accuracy should also be assured. In this paper, we take accuracy as one of the criteria to estimate the performance of privacy-preserving data aggregation scheme.

Privacy-preservation: To broaden the area of WSNs' applications, the privacy of data must be guaranteed, which makes the application in civilian field more practical. Therefore, it is meaningful to develop privacy-preserving data aggregation schemes against eavesdropping. The private data aggregation scheme should be able to prevent the adversary from finding out the sensory data produced by any sensor node. Even though the wireless links are vulnerable to eavesdropping, a good private data aggregation scheme should be robust to such attack.

4. Energy-efficient and high-accuracy secure data aggregation

In this section, we present the details of our proposed scheme: Energy-Efficient and High-Accuracy (EEHA) Scheme for Secure Data Aggregation. There are four steps, i.e., aggregation tree construction, slicing, mixing and aggregation which are further described as follows.

Step 1. Aggregation tree construction

A common technique for data aggregation is to build an aggregation tree which is the directed tree formed by the union of all the paths from the sensor nodes to the base station. These paths may be arbitrarily chosen and are not necessarily shortest paths. The optimization of the aggregation tree structure is out of the scope of this paper. There are various methods for constructing the aggregation tree according to different application requirements. One method for constructing an aggregation tree is described in TAG [10]. First of all, the network is organized into a tree rooted at the base station. The leaves of the tree are denoted by green nodes in Fig. 1.

Step 2. Slicing

This step is similar to the step 2 of SMART [5]. We adopt the slicing technique proposed in [5]. First, each leaf i of the tree randomly selects a set of nodes S_i $(K = |S_i|)$ within h hops. For a dense sensor network, we can take $h = 1$. We define that the leaf itself is one element of S_i. The primitive data sensed by node i is denoted by v_i. Leaf i then slices its private data v_i randomly into K pieces, which means that the summation of K pieces is equal to v_i.

Fig. 2 describes the slicing step, where one of the K pieces is kept at node i itself, the remaining $K-1$ pieces are encrypted and sent to nodes in S_i, we take $h = 1$ here. We assume that the key used to encryption is only known to the two nodes who share the common key. We denote d_{ij} as a piece of data sent from node i to node j. For nodes to which node i does not send any slice, $d_{ij} = 0$. Thus, $v_i = \sum_{j=1}^{N} d_{ij}$, and the final aggregate result can be expressed as $R = \sum_{i=1}^{N}\sum_{j=1}^{N} d_{ij}$, where $d_{ij} = 0,\ \forall j \notin S_i$.

The notations we have introduced and will introduce later are summarized in Table 1.

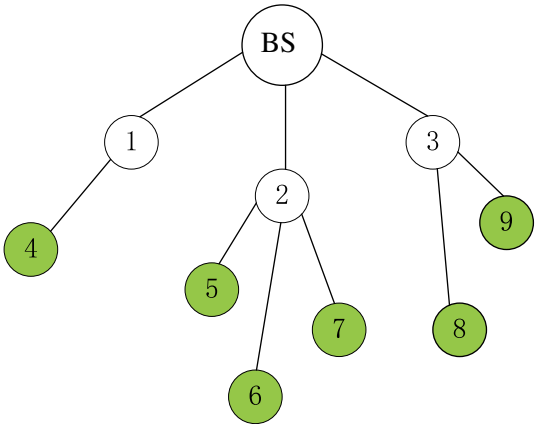


Fig. 1. Aggregation tree construction.

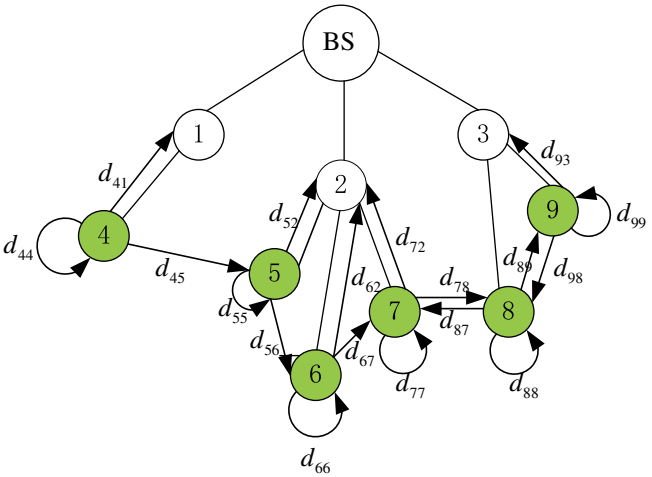


Fig. 2. Slicing.

Table 1
Summary of notations.

Notation	Definition
N	The number of sensor nodes in the network
v_i	Primitive data sensed by node i
d_{ij}	A piece of data sent from node i to node j
S_i	The set of neighbor nodes of node i within h hops
K	The number of pieces each leaf node slices its primitive data into
r_i	New result of node i after aggregation
t_i	The time interval node i wait for before sending new aggregation result
R	The final aggregation result, summation of all the sensor readings

Step 3. Mixing

First, all leaves of the aggregation tree wait for certain time, which guarantees that all slices are received. Then, each leaf decrypts the data using its shared key with the sender, sums up all the received slices and the slice left by itself to get a new result r_i. Fig. 3 shows the mixing step on leaf nodes.

Step 4. Aggregation

After a leaf sums up the received slices to get a new result, it encrypts the new result and sends it to its parent. And the intermediate nodes of the tree may receive slices d_{ij} sent by leaves, also may receive new results r_i sent by their children. Each intermediate sensor node in the aggregation tree performs an aggregation operation whenever it has heard from all its child nodes or leaf nodes. So parent nodes should wait for a longer time than child nodes, we denote the difference as time interval difference Δt, which is set in aggregation tree construction phase, then each node can compute its time-out t_i. Finally, each intermediate node sums up its own sensor reading and the received data, encrypts and sends the aggregation result to its parent when its t_i elapsed. The aggregation is performed along the aggregation tree constructed in step 1, partial results propagate level by level up the tree. Eventually the aggregation result reaches the root. The final data R at the root is the summation of all sensor data. Fig. 4 is the illustration of aggregation step.

The pseudo-code of EEHA for every node is described in Algorithm 1.

Algorithm 1. EEHA Algorithm

```
1: Construct an aggregation tree on top of TAG protocol;
2: Set time interval difference Δt and compute time-out t_i;
3: if IsLeafNode then
4:    perform slicing operation and wait;
5:    if t_i elapsed then
6:       perform mixing operation and send new result r_i to its parent
   node;
7:    end if
8: end if
9: if IsIntermediateNode then
10:   while t_i not elapsed and ReceiveMessage do
11:      sum up the received data;
12:   end while
13:   send aggregation result r_i to its parent node;
14: end if
```

5. Simulation study and performance analysis

5.1. Simulation setting

In this section, we evaluate the performance of EEHA and SMART through theoretical analysis and simulation study. For this purpose, we implemented these two schemes using ns-2 simulator. We did extensive simulations to compare these two schemes.

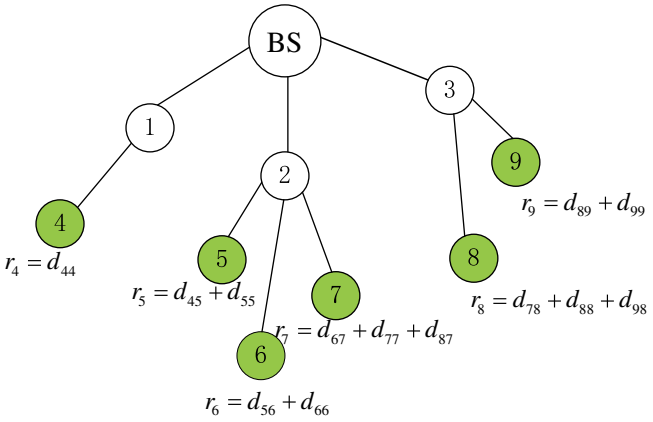


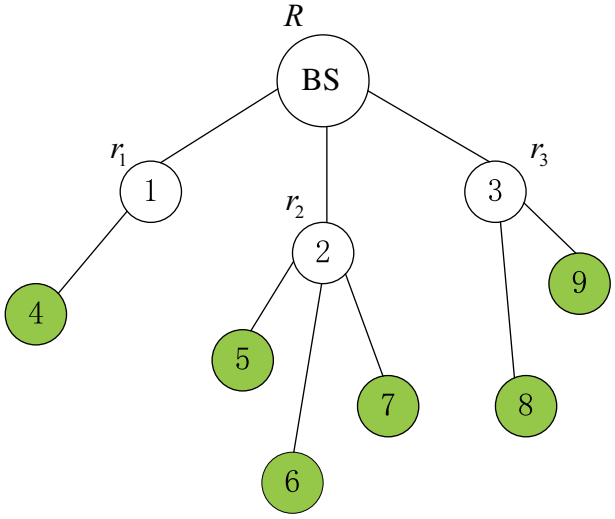
Fig. 3. Mixing.

In the following simulations, we considered the experiment model proposed in [5]. We also consider networks with 600 sensor nodes. These nodes are randomly deployed over a 400 m × 400 m area. The transmission range of a sensor node is 50 m and data rate is 1 Mbps. We evaluate EEHA in terms of communication overhead, aggregation accuracy, efficacy of privacy-preservation, and energy consumption, comparing with the SMART scheme.

5.2. Performance evaluation

5.2.1. Communication overhead

In our experiments, we implemented the two schemes on the same already constructed aggregation tree. The aggregation process is deployed repeatedly. During this phase, the network topology is fixed, and the aggregation tree is also fixed.



$$r_1 = v_1 + d_{41} + r_4$$
$$r_2 = v_2 + d_{52} + d_{62} + d_{72} + r_5 + r_6 + r_7$$
$$r_3 = v_3 + d_{93} + r_8 + r_9$$
$$R = r_1 + r_2 + r_3$$

Fig. 4. Aggregation.

Fig. 5 shows the communication overhead of EEHA and SMART with $K = 3$ under different time intervals. We use the total number of messages communicated during each aggregation round as the metric.

Simulation results show that the bandwidth consumption of SMART is higher than that of EEHA. This can be explained by analyzing the number of exchanged messages in each scheme. In SMART, with $K = 3$, each node needs to exchange three messages for private data aggregation: two messages during the slicing step and then one message for data aggregation. Hence, for the network with 600 nodes, the communication overhead is about 1800. In EEHA, only the leaf nodes of aggregation tree decompose their data into slices, and send the $K - 1$ slices to their selected neighbors. With $K = 3$, each leaf node needs to exchange three messages (the same as SMART) in each run. Each internal node needs to send only one message for data aggregation. The number of leaf nodes is much smaller than the number of sensor nodes in the whole network, therefore only a small part of network nodes need to send three messages, the other nodes send one message in EEHA. Comparing with SMART where all network nodes send three messages, EEHA introduces much less amount of transmission.

Consider a network with N sensor nodes, and the percentage of leaves of the aggregation tree is α in EEHA. Then it's obvious that the number of intermediate nodes is $(1 - \alpha) \cdot N$. We adopt the "slicing and assembling" technique to slice the private data into K pieces; thus, the communication overhead of the two schemes is simply

SMART:

$$N \cdot K \tag{1}$$

EEHA:

$$\alpha \cdot N \cdot K + (1 - \alpha) \cdot N \tag{2}$$

Therefore, the communication ratio between EEHA and SMART is given by

$$p = \frac{\alpha \cdot N \cdot K + (1 - \alpha) \cdot N}{N \cdot K} \tag{3}$$

A smaller p means that EEHA is more efficient relative to SMART.

$$p = \frac{\alpha \cdot N \cdot K + (1 - \alpha) \cdot N}{N \cdot K} = \alpha + \frac{1 - \alpha}{K} \tag{4}$$

From (4), we can see that if α is constant, the larger K is, the smaller p is, which means that when using the same aggregation tree, more slice pieces give better communication efficiency to EEHA relative to SMART. This is because the fact that more slice pieces make more messages in the whole network for SMART, make the aggregation of intermediate nodes more effective for EEHA.

$$p = \frac{\alpha \cdot N \cdot K + (1 - \alpha) \cdot N}{N \cdot K} = \left(1 - \frac{1}{K}\right) \cdot \alpha + \frac{1}{K} \tag{5}$$

From (5) we can see that if K is constant, the larger α is, the larger p is. This is because more leaves of the aggregation tree cause more communication for EEHA as the leaves adopt the "slicing and assembling" technique which induces K messages at each leaf, and the aggregation effect of the intermediate nodes is weakened as the number of intermediate nodes is reduced with a larger α.

5.2.2. Aggregation accuracy

The accuracy metric is defined as the ratio between the collected summation by the data aggregation scheme used and the real summation of all individual sensor nodes in [5]. Fig. 6 illustrates the accuracy of EEHA and SMART ($K = 3$) with respect to different time intervals from our simulations.

From Fig. 6 we can observe that the accuracy increases as the time interval increases. Two reasons contribute to this, which have already been analyzed in [5]. (1) With longer time interval, the data messages to be sent within this duration will have less chance to collide. (2) With longer time interval, the data messages will have a better chance of being delivered within the deadline.

Besides, we can also observe that EEHA has better accuracy than SMART. We have demonstrated that the communication overhead of EEHA is reduced significantly, the amount of transmission is much less than SMART, hence the chance of occurring collisions is also decreased, which causes an improvement of aggregation accuracy.

5.2.3. Privacy-preservation

The neighbor nodes or the attacker should not be able to read the data produced by any node. To address privacy, He et al. [5] adopt the "slicing and assembling" technique, where the sensor node hides its individual data by slicing the data and sending encrypted data slices to different neighboring aggregators, then the aggregators collect and route aggregated result back to the base station.

In EEHA, the schemes used to protect data privacy are different for leaf nodes and intermediate nodes. For leaf nodes, sensors need

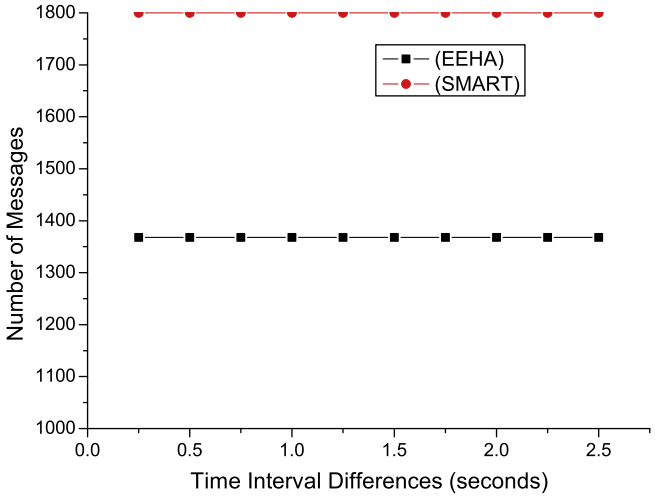


Fig. 5. Communication overhead of EEHA vs. SMART.

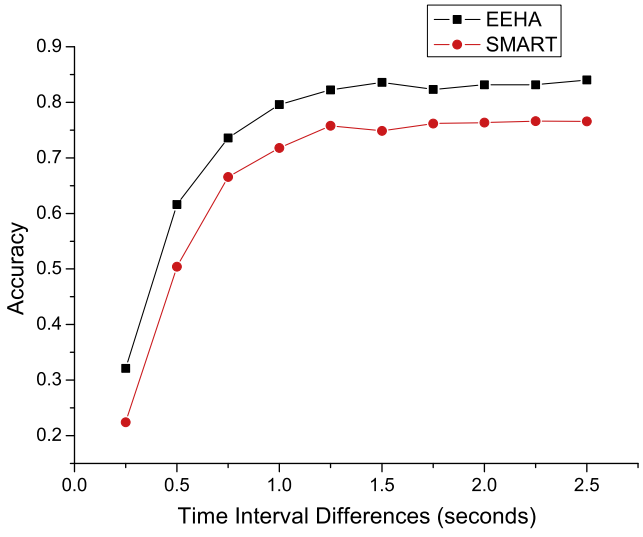


Fig. 6. Accuracy of EEHA vs. SMART.

to hide their original readings in the first hop data reporting. We adopt the "slicing and assembling" technique mentioned above. Because the primitive data of leaf nodes are separated into K pieces and sent to $K-1$ different neighbors, even if data are overheard and decrypted, it is still difficult for the adversary to recover sensitive information. However, for intermediate nodes, we take advantage of the aggregation function to hide the privacy. The privacy of intermediate nodes is guaranteed by replacing the primitive data with summation of the received data and its own data to conceal the original sensor reading. Even if data sent by intermediate nodes are overheard, they are not the primitive data, sensitive information is not released; thus, achieving privacy-preservation.

To strengthen the property of privacy-preserving, we can change the encryption key each time a massage is encrypted. In order to generate a different encryption key, the encryption key can be derived as a function of some nonpersistent quantity like a counter value which changes on every query. To lower the communication overhead, we can maintain a counter at both transmitting and receiving ends which is incremented each time the base station injected a query. The encryption key will be the function of counter value at that instant and the master secret shared between the transmitter and receiver.

5.2.4. Energy consumption

In our experiments, we considered the energy model as follows: a total available node battery of 100J; 0.660W for sending data; 0.395W for receiving data; 0.035W for idle state. In order to assess how the communication overhead impacts on energy consumption, Fig. 7 shows the percentage of left energy in the network with respect to execution time.

From Fig. 7, we can conclude that the SMART scheme consumes energy much faster. That is because there are more messages exchanges in SMART for each run. We know that the energy dissipation of communication plays an important role in the total energy consumption. Data transmitting and receiving is the major portion of power consumption for sensor nodes. So reducing the communication cost is an efficient way to save energy. As the communication overhead in our scheme is much less than SMART, the EEHA scheme is more energy efficient.

5.3. Discussions

In this paper, we design our scheme by comprehensively considering communication overhead, aggregation accuracy and privacy protection, and try to make an appropriate tradeoff among them.

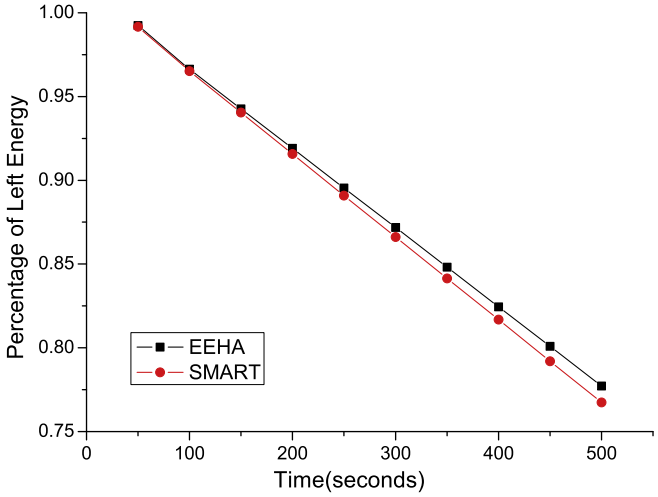


Fig. 7. Percentage of left energy of EEHA vs. SMART.

As mentioned in [5], only if an eavesdropper breaks all outgoing links and all incoming links of a node s, will it be able to crack the private data held by s. Therefore, the more the communication overhead, the better the privacy-preservation performance. Our proposed scheme EEHA has reduced communication overhead significantly which means that the level of privacy is lowed unavoidable compared with SMART [5]. But EEHA decreases communication overhead by 24% and improves accuracy level by 6–11% through simulation results.

Based on the analysis above, our scheme is more suitable for applications that have relative loose requirements of privacy-preservation, but place more emphasis on energy-efficiency and accuracy level.

6. Conclusions

In typical wireless sensor networks, sensor nodes are usually resource-constrained and battery-limited. And transmission is much more energy consuming than computation. Therefore, communication overhead is an important issue in wireless sensor networks. Data aggregation can reduce the communication overhead and energy consumption, thereby extending the lifetime of wireless sensor networks. And the aggregation accuracy is very necessary for sensitive applications such as battlefield surveillance and forrest fire monitoring. As sensor networks become more widely deployed, especially in military surveillance and civilian usage, how to protect the privacy of the sensed data are becoming a crucial concern.

We propose an energy-efficient and high-accuracy (EEHA) scheme for secure data aggregation in wireless sensor networks. The goal of EEHA is that the sensor network can obtain an accurate aggregation result while guaranteeing that no private sensor reading is released to other sensors and that no significant extra overhead is introduced. Extensive simulations are conducted to evaluate the proposed scheme. The results show that our scheme provides privacy protection for raw data and better aggregation accuracy with an overhead lower than the SMART scheme.

References

[1] D. Culler, D. Estrin, M. Srivastava, Overview of sensor networks, IEEE Computer (2004).
[2] N. Xu, S. Rangwala, K. Chintalapudi, D. Ganesan, A. Broad, R. Govindan, D. Estrin, A wireless sensor network for structural monitoring, in: Proceedings of the ACM Conference on Embedded Networked Sensor Systems, Baltimore, MD, November 2004.
[3] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler, J. Anderson, Wireless sensor networks for habitat monitoring. WSNA'02, Atlanta, Georgia, September 2002.
[4] Lewis, F.L. Wireless sensor networks. Smart Environments: Technologies, Protocol and Applications, 2004.
[5] W. He, X. Liu, H. Nguyen, K. Nahrstedt, T. Abdelzaher. PDA: privacy-preserving data aggregation in wireless sensor networks, in: IEEE INFOCOM, 2007.
[6] D. Estrin, R. Govindan, J. Heidemann, S. Kumar, Next century challenges: scalable coordination in sensor networks, in: Proceedings of ACM Mobicom, Seattle, Washington, USA, ACM, August 1999, pp. 263C270.
[7] J. Heidemann, F. Silva, C. Intanagonwiwat, R. Govindan, D. Estrin, D. Ganesan, Building efficient wireless sensor networks with low-level naming, in: Proceedings of the 18th ACM Symposium on Operating Systems Principles, 2001, pp. 146–159.
[8] B. Krishnamachari, D. Estrin, S. Wicker, The impact of data aggregation in wireless sensor networks, in: Proceedings of the ICDCS Workshops, 2002, pp. 575–578.
[9] Y. Yu, B. Krishnamachari, V.K. Prasanna, Energy-latency tradeoffs for data gathering in wireless sensor networks, in: Proceedings of the 23rd Conference of IEEE Communication Society (INFOCOM), Hong Kong, SAR China, March 2004.
[10] S. Madden, M.J. Franklin, J.M. Hellerstein, TAG: A Tiny AGgregation Service for Ad-Hoc Sensor Networks, OSDI, 2002.
[11] C. Itanagonwiwat, R. Govindan, D. Estrin, Directed diffusion: a scalable and robust communication paradigm for sensor networks, MobiCom, 2000.

[12] C. Intanagonwiwat, D. Estrin, R. Govindan, J. Heidemann, Impact of network density on data aggregation in wireless sensor networks, in: Proceedings of the 22nd International Conference on Distributed Computing Systems, 2002.
[13] I. Solis, K. Obraczka, The impact of timing in data aggregation for sensor networks, ICC, 2004.
[14] X. Tang, J. Xu, Extending network lifetime for precision constrained data aggregation in wireless sensor networks, INFOCOM, 2006.
[15] B. Przydatek, D. Song, A. Perrig, SIA: secure information aggregation in sensor networks, in: Proceedings of the First International Conference on Embedded Networked Sensor Systems, November 2003.
[16] Y. Yang, X. Wang, S. Zhu, G. Cao, SDAP: a secure hop-by-hop data aggregation protocol for sensor networks, ACM MobiHoc, 2006.
[17] C. Castelluccia, E. Mykletun, G. Tsudik, Efficient aggregation of encrypted data in wireless sensor networks, Mobiquitous, 2005.
[18] W. Du, J. Deng, Y. Han, P.K. Varshney, A witness-based approach for data fusion assurance in wireless sensor networks, in: Proceedings of the IEEE Global Telecommunications Conference, 2003.
[19] S. Zhu, S. Setia, S. Jajodia, P. Ning, An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks, in: Proceedings of the 2004 IEEE Symposium on Security and Privacy, May 9–12, 2004, pp. 259–271.
[20] L. Hu, D. Evans, Secure Aggregation for Wireless Networks, in: Proceedings of the 2003 Symposium on Applications and the Internet Workshops, 2003.
[21] F. Ye, H. Luo, S. Lu, L. Zhang, Statistical en-route detection and filtering of injected false data in sensor networks, in: Proceeding of IEEE INFOCOM, 2004.