PAPER *Special Section on Trust, Security and Privacy for Pervasive Applications*

Tier-Based Scalable and Secure Routing for Wireless Sensor Networks with Mobile Sinks

Feilong TANG[†,††*a)], ***Nonmember***, **Minyi GUO**[†,††], ***Member***, ***and*** **Song GUO**[††], ***Nonmember***

SUMMARY Multiple hop based routing in homogeneous sensor networks with a single sink suffers performance degradation and severe security threats with the increase of the size of sensor networks. Large-scale sensor networks need to be deployed with multiple powerful nodes as sinks and they should be scheduled to move to different places during the lifetime of the networks. Existing routing mechanisms lack of such supports for large-scale sensor networks. In this paper, we propose a heterogeneous network model where multiple mesh nodes are deployed in a sensor network, and sensed data are collected through two tiers: firstly from a source sensor node to the closest mesh node in a multiple-hop fashion (called sensor routing), and then from the mesh node to the base station through long-distance mesh routing (called mesh routing). Based on this network model, we propose an energy-efficient and secure protocol for the sensor routing that can work well in large-scale sensor networks and resist most of attacks. Experiments demonstrate that our routing protocol significantly reduces average hops for data transmission. Our lightweight security mechanism enables the routing protocol to defend most attacks against sensor networks.

key words: *routing protocol, sensor network, mesh network, secure routing*

1. Introduction

The flexibility, self-organization, low-cost and rapid deployment characteristics of sensor networks create many new and exciting application scenarios for which traditional wired and wireless networks are not suitable, such as road traffic management, medical treatment, battleground and environment monitoring [1]. As a result, recent years have witnessed the rapid development of wireless sensor technologies. Routing is at the center of sensor networks; however, existing routing protocols are inapplicable to large-scale applications. On one hand, existing efforts are built on a flat network architecture, where all homogeneous sensor nodes route data to a single sink by multiple hops [3]. With the increase of sensor nodes, the average number of hops between a sensor node and the single sink grows rapidly, resulting in more energy consumption, packet loss and transmission delay. Meanwhile, energy-limited sensor nodes near the single sink in a flat architecture inevitably drain their energy ahead of other nodes, no matter whether the energy-centric or lifetime-centric routing protocols [18] are used. On the other hand, existing routing protocols suffer from the single point of failure as well as potential traffic congestion, especially around the sink. A sensor network crashes if the single sink fails.

Wireless mesh sensor network (WMSN) is currently one of the most astounding trends in network computing from industry and academic communities as a promising solution to solve the above problems [8]. However, very few results have been reported in this area so far. There has not been yet a well-defined architecture model for the new hybrid network environment. The existing routing protocols do not consider the multiple mobile sinks for large-scale applications. Finally, there is a lack of the secure routing that supports for multiple-sink WMSNs at this time. In this paper, we will propose an adaptive routing protocol based on mesh sensor network architecture, which is applicable to many large-scale applications by reducing the average number of transmission hops. Further, we also present mechanisms to guarantee routing security. The results will be useful to the development and deployment of wireless sensor networks in many applications.

The remainder of this paper is organized as follows. In the next Section, we review related work. Section 3 proposes a tiered network model for large-scale sensor networks and presents an energy-efficient routing protocol under the proposed network model. In Sect. 4, we investigate the security mechanism for our routing protocol. Experiments and evaluations on our routing protocol are reported in Sect. 5. Finally, Sect. 6 concludes this paper with a discussion on future work.

2. Related Work

Routing is a fundamental problem in any type of networks and has been studied comprehensively in sensor networks. Routing protocols in wireless sensor networks can be broadly classified as flat-based and hierarchical-based. In flat-based routing, e.g., flooding, Gossiping, SPIN, Directed Diffusion, Rumor, and MCFA [3], all nodes are typically assigned equal roles or functionality. In hierarchical-based routing, e.g., LEACH, PEGASIS and TEEN, sensor nodes play different roles in networks, where nodes with higher energy can be used to process and send the information while nodes with low energy are used to perform the sensing in the proximity of targets.

Clustering is an important method for hierarchical routing. LEACH (low energy adaptive clustering hierarchy) [11]

Manuscript received July 1, 2009.
Manuscript revised September 22, 2009.

[†] The authors are with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China.

[††] The authors are with the School of Computer Science and Engineering, The University of Aizu, Aizu-Wakamatsu-shi, 965–8580 Japan.

[*] Corresponding author.

a) E-mail: tang-fl@cs.sjtu.edu.cn

DOI: 10.1587/transinf.E93.D.458

is a 2-level clustering-based routing protocol which attempts to minimize global energy dissipation and to distribute energy consumption evenly across all nodes. The nodes self-organize into local clusters with one node in each cluster acting as a cluster head. Energy dissipation is evenly spread by dissolving clusters at regular intervals and randomly choosing the cluster heads. Hausdorff clustering algorithm [12] sets up static clusters based on node locations, communication efficiency, and network connectivity. Selected cluster heads form a backbone network to periodically collect, aggregate, and forward data to the base station using minimum energy (cost) routing so that the lifetime of sensor networks is lengthened. Moreover, an energy-efficient dynamic clustering technique [13] was presented for large-scale sensor networks. By monitoring the received signal power from its neighboring nodes, each node estimates the number of active nodes in real-time and computes its optimal probability of becoming a cluster head.

An important observation is that these routing protocols are based on the homogeneous flat network architecture, without powerful nodes for long-distance data transmission. Neighboring sensors of the sink suffer much heavier forwarding tasks in networks with a single static sink so that as the size of WSNs increases, they become inefficient. The bigger the network size is, the more serious the non-balance of energy consumption will be and the more average hops the data transmission will take. So, existing routing protocols cannot effectively support large-scale sensor networks. To tackle this problem, to increase the number of sinks may be a solution [14]–[16].

Applications of sensor networks often involve sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Secure routing is a prerequisite to such sensor applications. Wang et al. [7] surveyed security issues and summarized the constraints, security requirements, and attacks with their corresponding countermeasures in sensor networks. Especially, this research pointed out the main network layer attacks against sensor networks: spoofed, altered, or replayed routing information, selective forwarding, sinkhole, sybil, wormholes, hello flood attacks, acknowledgment spoofing, etc. In [5], Karlof et al. proposed threat models and security goals for secure routing in sensor networks, introduced two novel classes of attacks against sensor networks–sinkhole attacks and HELLO floods, and finally discussed countermeasures and design considerations for secure routing protocols in sensor networks. INSENS [6] is an intrusion-tolerant routing protocol, which does not rely on intrusion detections, but rather tolerates intrusions by bypassing the malicious nodes. An important property of INSENS is that while a malicious node may be able to compromise a small number of nodes in its vicinity, it cannot cause widespread damages in the network. SPINS [4] is a suite of security protocols optimized for sensor networks, including two secure building blocks: SNEP and μTESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness. μTESLA provides authenticated broadcast for severely resource-constrained environments.

Zhu et al. proposed the LEAP [2], a key management protocol for sensor networks that is designed to support in-network processing, while at the same time restricting the security impact only to the immediate neighbors of the compromised node. LEAP supports the establishment of four types of keys for each sensor node: an individual key shared with the base station, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network.

3. An Energy-Efficient Routing Protocol for Large-Scale Sensor Networks

Routing protocol mainly involves finding a route from a source node to a destination node, forwarding data over the established route, and maintaining the route in accordance with the up-to-date network topology. Routing protocols in sensor networks differ depending on the network architecture, where energy awareness is always an essential design issue [5], [17]. In this Section, we firstly propose a reference model of WMSNs, and then present an energy-efficient routing protocol for WMSNs with multiple mobile sinks.

3.1 Network Model

By analysis of existing researches on sensor networks, we found that the poor scalability of the flat architecture mainly results from a lack of long-distance transmission nodes. A wireless mesh network is able to provide interconnections among all networked nodes, where each node can send and receive data. By deploying multiple wireless mesh nodes equipped with gateway functionalities in a sensor network, we propose a kind of tiered network architecture, i.e., WMSN (see Fig. 1), where sensor nodes detect objects and send data to the most appropriate mesh nodes, while mesh nodes are specifically responsible for collecting sensed data as well as long-distance data transmission.

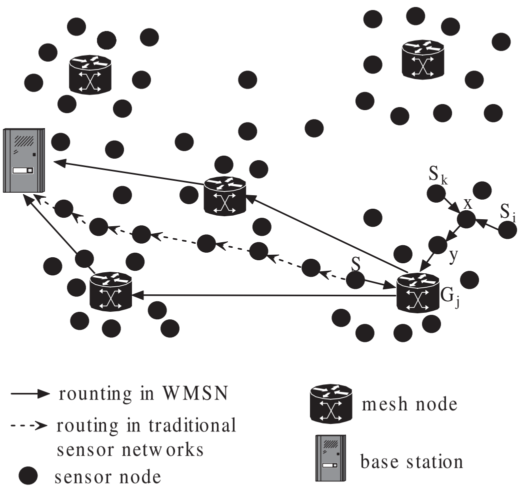

Fig. 1 A network model of WMSNs.

In WMSNs, sensor nodes use short-distance medium access control (MAC) protocol (e.g., 802.15.4) while mesh nodes use long-distance MAC protocol (e.g., 802.11).

Multiple mesh nodes in a sensor network can significantly reduce the average number of hops of data transmission, and thus can save energy consumption and accordingly lengthen network lifetime. For example, a source node S in Fig. 1 routes data to the base station via 7 hops in a traditional sensor network while 3 hops in a WMSN (1 hop to gateway G_j and 2 hops to the base station).

3.2 Energy-Efficient Routing (EER)

Routing in a WMSN involves two tiers: routing among sensor nodes and mesh nodes, and routing among mesh nodes and the base station. This paper investigates the first one because it is more challenging. Let a set of gateways (i.e., mesh nodes) be distributed randomly in a sensor network. We model such a WMSN as a graph G (V,E), where V is the combination of the set of sensor nodes (V_S) and the set of gateways (V_G); and E is the combination of the set of one-hop links between sensor nodes ($V_S \times V_S$) and the set of one-hop links between sensor nodes and gateways ($V_S \times V_G$). By one-hop link, we mean two nodes can directly communicate with each other.

3.2.1 Overview of Energy-Efficient Routing

In a WMSN, there are two kinds of data transmissions: from sensor nodes to gateways and on the reverse direction. In our model, each sensor node S_i ($1 \leq i \leq n$) keep static while each gateway G_j ($1 \leq j \leq m$) performs discrete movements within the sensor network. The sensor network topology changes if any gateway moves to a different place. We define the period during which all gateways are static as a *round*, i.e., the sensor network topology stays unchanged during a round.

Our routing protocol EER includes the following phases: *routing query*, *routing response*, *data transmission* and *routing table updating*. In the routing query phase, the sensor node that needs to transmit data floods a query packet to all gateways. Next, gateways or intermediate sensor nodes, which keep the corresponding routing information, respond to the routing query with the path information in the routing response phase. From then on, the sensor node decides the best gateway and the best path based on the responded path information in the data transmission phase. Finally, in the case that any gateway moves to a new location, our routing protocol keeps routing tables set up in sensor nodes in the last round, however, the routing to the moved gateway will be updated.

Our routing protocol has the following two characteristics distinguishing from existing ones. On the one hand, EER discovers the best gateway from a set of sinks for a sensor node. Accordingly, the sensed data is transmitted to the gateway by the least number of hops. Let all sensor nodes transmit data at identical power levels so that transmitting 1 bit data consumes the same energy to all sensor nodes. Therefore, the less hops, the less energy consumption. On the other hand, our EER merges the advantages of table-driven and on-demand routing mechanisms. Traditional table-driven routing protocols need to update frequently routing tables of all sensor nodes, arising too heavy traffic overhead and energy consumption in dynamically changing networks. In our protocol, however, the routing information generated previously is still kept and only nodes, whicht need to send data and cannot find routing information in their local routing tables, update their routing table. Such a mechanism not only reduces network traffic and energy consumption for routing establishment but also can adapt dynamic network topology.

```
RoutingQuery
{
    $S_i$ floods a query packet RREQ with
    m destinations (i.e., m gateways);
    repeat
        $S_i$ waits for response messages;
    until (t<=timeout) or ($S_i$ receives m responses);
    $S_i$ selects the path with the least hops as p($S_i$,$G_j$)
    from response messages;
    $S_i$ adds a routing entry in its local routing table;
}
```

Fig. 2 Query a routing p(S_i,G_j).

3.2.2 Energy-Efficient Routing Protocol

Before presenting our routing protocol EER, we define some terms used in EER.

- Source node S_i: the sensor node that needs to transmit data to the best gateway.
- Intermediate node: the sensor node in the routing path between a source node and the best gateway.
- p(x,y): the shortest path between node x and node y.

Routing query. Whenever a source node S_i needs to transmit data, it firstly checks its local routing table. If there is an entry destined to a gateway G_j in the routing table, which means G_j is the best gateway, S_i directly broadcasts a DATA packet. Otherwise, S_i initiates a routing query to set up a routing p(S_i,G_j), using the algorithm RoutingQuery as shown in Fig. 2.

Routing response. On receiving the request packet, any intermediate node S_k(k=1,2,. . . ,n; k≠i) responds to the routing query using the algorithm RoutingResponse (see Fig. 3). On the other hand, if a gateway G_j receives the request packet, it responds the path p(S_i,G_j) to source node S_i.

In a sensor network with multiple sinks, if there exists the shortest path from a sensor node x to a gateway G_j such that Path_x=<x,y,. . . ,G_j >, its sub-path Pathy=<y,. . . , G_j > is also the shortest path from y to the G_j. Based on this property, our RoutingResponse algorithm responds routing using the following mechanism.

```
RoutingResponse
{
   $S_k$ checks its local routing tables;
   If ($S_k$ finds a routing entry $p(S_k, G_j)$)
   {
      $S_k$ returns $p(S_i,G_j)=p(S_i,S_k)+p(S_k, G_j)$ to $S_i$;
   }
   else
   {
      $S_k$ floods request packet to neighbors after
      appending its address to the route list;
   }
}
```

Fig. 3 Routing response.

- Sensor nodes that have established routing do not need to forward routing query messages during the current round. As shown in Fig. 1, if there is a shortest path $<S_i,x,y,G_j>$ from S_i to G_j, the best routes of nodes x and y are included in $<S_i,x,y,G_j>$. More specifically, both x and y select G_j as the best gateway, and the shortest paths of x and y are $<x,y,G_j>$ and $<y,G_j>$, respectively.
- Sensor nodes that have set up their routing tables directly return path information instead of further flooding. For example, if node S_k in Fig. 1 needs to send data, it floods routing request packet. When node x that has established the route $<x,y,G_j>$ receives the request message with destination G_j, it directly appends sub-path $<x,y,G_j>$ after (S_k,x) by querying its routing table and returns the path $<S_k,x,y,G_j>$ to S_k.

Data transmission. On selecting the shortest path $p(S_i,G_j)$, the source node S_i encapsulates a data packet DATA. S_i attaches the short path $p(S_i,G_j)$ in the head of the first data packet. Intermediate nodes located in the path $p(S_i,G_j)$ forward the data packet in turn until reaching G_j hop by hop according to the attached routing information $p(S_i,G_j)$. At the same time, these nodes add an entry in their local routing tables, each of them taking G_j as its best gateway. Subsequent data packets generated by S_i do not need to carry routing information any more. Each sensor node can forward data packets to G_j by checking its local routing table.

Routing table updating. The ideal goal of routing for sensor networks is to lengthen the network lifetime as long as possible. But the problem of routing messages in a wireless sensor network so as to maximize network lifetime is NP-hard [19]. To balance the energy consumption of sensor nodes, we schedule the gateway(s) in a set of candidate positions in turn. The moved gateway G_j notifies sensor nodes in the network of its movement. A sensor node S_i queries the path $p(S_i, G_j)$ to the moved gateway G_j only before it transmits the date. The sensor node and the intermediate nodes in the selected routing add the corresponding shortest routing information in their local routing tables.

4. Secure Routing

Many sensor network based applications are mission-critical so that security mechanism is indispensable to the data transmission from dispersed sensor nodes.

4.1 Requirements for Secure Routing in Wireless Mesh Sensor Networks

The goal of security services in multiple-hop sensor networks is to protect the information and resources from attacks and misbehavior, including availability, authorization, authentication, confidentiality, integrity, nonrepudiation and freshness [7]. Compared with traditional networks, sensor networks have many characteristics that make them more vulnerable to attacks. Hence, when designing or proposing security mechanisms against routing attacks, besides the basic requirements for any security mechanism, the following peculiarities should be carefully considered:

Lightweight computations. Sensor nodes have limited computational abilities and cannot be expected to be able to carry out expensive computations. For WMSNs proposed above, heavyweight computations should be performed by gateways. Furthermore, asymmetric-key solutions are difficult to implement in such a resource-constrained environment, and symmetric-key methods coupled with a priori key distribution schemes would be more appropriate to achieve goals of data secrecy and integrity [10].

Attack-tolerance. A distinguishing feature of sensor networks is that attackers can capture a sensor and acquire all the information stored within it. The security routing should automatically recover from potential attacks.

Multiple mobile gateways. To balance energy consumption of all sensor nodes, gateways should keep mobile. As a result, sensor nodes select different gateways as routing destinations at different time. Routing protocols have to self-adapt the mobility of gateways.

4.2 Secure Mechanisms for Routing

Similar to existing secure routing schemes that regard base stations trustworthy [7], we assume that gateways are trustable. Further, we let each sensor node be preloaded secret keys, each shared with a gateway. We use the notations in Table 1 to describe security protocols and cryptographic operations in this paper.

4.2.1 Secure Routing Query

When a sensor node queries the best routing using our protocol EER described in Sect. 3, it uses the following request packet RREQ(i,j).

$\{req\}_{<K_{ij},C>}$, $path_{ij}(k)$,MAC$\{K_{ij}, C|\{req\}_{<K_{ij},C>}\}$

RREQ(i,j) is sent from the sensor node S_i to the gateway G_j ($1 \leq i \leq m$), where *req* denotes the routing query information between S_i and G_j, and m is the number of gateways,

Table 1 Notations for secure routing.

Symbol	Description
S_i	one of n sensor nodes (1 ≤ i ≤ n)
G_j	one of m gateways (1≤ j ≤ m)
x,y	intermediate nodes in a path
RREQ	routing query packet
RRES	routing response packet
DATA	data packet
K_{ij}	symmetric secret key shared by S_i and G_j
M_1 |M_2	concatenation of messages M_1 and M_2
$M_{<Kij,C>}$	encryption of message M, with key K_{ij} and the incremental counter C [9]
MAC(K_{ij},M)	message authentication code (MAC) of M, with symmetric secret key K_{ij}
path_{ij}(k)	the k^{th} path between S_i and G_j
A→B	a message transmission from node A to node B

RREQ	S_i	G_j

(a) req

S_i	x	y	......	G_j

(b) path_{ij}(k)

Fig. 4 Path query information req for node pair (S_i, G_j).

as shown in Fig. 4 (a).

When an intermediate node receives the RREQ message for the first time, it in turn forwards (broadcasts) this message after appending itself in the path_{ij}(k) field (see Fig. 4 (b)). If the intermediate node receives the same RREQ message more than one times, the duplicate RREQ message is dropped directly. If node y receives a request packet transmitted from x and originated by S_i with a packet head RREQ, for example, it adds itself to the existing path p(S_i,x)=S_i →x, and forms a new path p(S_i,y)=S_i →x→y.

4.2.2 Secure Routing Response

Whenever a gateway G_j receives a routing query packet, it verifies (1) whether the *req* message is originated from the claimed sender S_i by checking MAC and K_{ij}, and (2) whether the message is replayed by a malicious node by checking counter value C in the MAC. If any verification is not correct, the message is dropped. For each node pair (S_i, G_j), in general there are multiple different paths path_{ij}(k). Thus, after G_j receives the first query packet from S_i and gets the path_{ij}(1), it waits a given timeout to collect multiple path information and then calculates the shortest path between S_i and G_j by the following formula:

$$\text{path}_{ij}= \min_{k} (|\text{path}_{ij}(k)|)$$

where path_{ij} denotes the shortest path between S_i and G_j; |path_{ij}(k)| is the number of hops in path_{ij}(k), and min() is a function to solve the path with the least hops among all path_{ij}(k). By the path_{ij}, G_j encapsulates a routing response packet RRES(j,i):

$$\{\text{res}\}_{<K_{ij},C>}, \text{path}_{ij}, \text{MAC}\{K_{ij}, C|\{\text{res}\}_{<K_{ij},C>}\}$$

where *res* represents the routing response information between G_j and S_i, as shown in Fig. 5.

RRES	S_i	G_j

Fig. 5 Path response message res for node pair (S_i, G_j).

DATA	S_i	G_j	IS	IR

Fig. 6 Packet format of routing information (RI).

From then on, G_j sends the response packet RRES(j,i) to the source node S_i. Intermediate sensor nodes located in path_{ij} forward in turn the packet RRES(j,i) according to the information in path_{ij} field while simultaneously record the corresponding path information in their local routing tables. If path_{ij} is S_1 →x→y→G_1, for example, nodes S_1, x and y then parse individual shortest path to G_1 as p(S_1,G_1)=S_1 →x→y→G_1, p(x,G_1)=x→y→G_1 and p(y,G_1)=y→G_1 respectively, in their corresponding local routing tables.

Gateways that are moved need to broadcast their new places to all sensor nodes. So, the moved gateways use μTESLA protocol [9] to achieve authenticated broadcast at the beginning of each round.

4.2.3 Secure Data Forwarding

After a sensor node successfully discovered the shortest path as well as the best gateway, all intermediate sensor nodes located in the path record the corresponding shortest path to the specified gateway in their local routing tables. A routing table has several entries, one for each route to a gateway. Each entry is a 4-tuple: *source*, *destination*, *immediate sender* and *immediate receiver*. Destination is the gateway to which a data packet is sent; source is the sensor node that created this data packet; immediate sender is the node that just forwarded this packet; and immediate receiver is the node that will receive this packet in next hop. Data packet DATA(i,j) is constructed as follows.

$$\{\text{data}\}_{<K_{ij},C>}, \text{RI}, \text{MAC}\{K_{ij}, C|K_{ij}\}$$

where data means the forwarded data from S_i to G_j, RI is the routing information, IS means an immediate sender, and IR means an immediate receiver, as shown in Fig. 6.

Data packets are forwarded based on the routing tables constructed previously. On receiving a data packet, a node searches for a matching entry in its routing table. If there is a match, it changes the IS and IR fields into itself and the next hop node respectively, and then forwards (broadcasts) the data packet. Otherwise, it drops the data packet. For the discovered shortest path S_1 →x→y→G_1 between S_1 and G_1, for example, each node keeps the routing entry to G_1 as S_1: (S_1, G_1,ϕ, x), x: (S_1, G_1, S_1, y), and y: (S_1, G_1, x, G_1), respectively. If node x receives a matched data packet with IS=S_1 and IR=x, x modifies IS and IR into x and y respectively, then forwards this packet.

5. Experiments and Evaluation

In this Section, we present the performance evaluation of our routing protocol, focusing on the scalability. We implemented our routing protocol EER in WMSNs, with a simplified notation as WMSNRouting, and the shortest path routing in single-sink-based flat sensor networks, simplified as SSRouting, respectively. We tested and compared these two routing protocols. As described previously, our WMSNRouting protocol only routes the sensed data from a source sensor node to the closest mesh gateway.

For the SSRouting, the single sink (only one mesh gateway) was always placed at the center of the networks, while as for the WMSNRouting, we symmetrically deployed four powerful mesh gateways, each as a sink, in the sensor network. Sensor nodes were randomly deployed in the network. The size of the packets sent out by sensor nodes was set up as 64 bytes. Each result was averaged over 10 random network topologies.

We kept approximately equal density of sensor nodes, around 0.01 nodes per square meter, in the two groups of experiments. The more sensor nodes, the bigger size of the sensor network, as shown in Table 2. Therefore, the number of sensor nodes may demonstrate the size of the sensor network.

We tested how the average number of hops and the average energy consumption for each packet routing change with the number of sensor nodes using SSRouting and our WMSNRouting, respectively. Finally, we tested how the node failure affects the delivery ratio on the two routing protocols.

Number of hops. The average number of routing hops in a sensor network reveals the energy efficiency of the routing protocol because each hop involves a packet sending and a packet receiving. Fig. 7 illustrates the average hops of two routing protocols under different network sizes, where we varied the number of sensor nodes from 100 to 1000 with an increment of 100. The result shows our protocol WMSNRouting has less hops than SSRouting under different number of sensor nodes. In particular, WMSNRouting increases slowly with the increase of network size. The reason is that each sensor node in WMSNRouting routed data to the closest mesh gateway so that the number of hops in a data transmission increased more slightly than that in SSRouting.

Table 2 Sensor number and network size.

Sensor number	Network size	Node density
100	100*100	0.01
200	140*140	0.0102
300	170*170	0.0102
400	200*200	0.0102
500	220*220	0.0102
600	240*240	0.0102
700	260*260	0.0102
800	280*280	0.0102
900	300*300	0.0102
1000	320*320	0.0102

Energy consumption. Energy consumption is the most important performance metrics for sensor networks. We set up the transmitting and receiving power consumption rates as 0.66 W and 0.395 W, respectively. In our experiments, we ignore the idling power consumption because it does not affect the relative performance comparison. Parameters in this experiment is listed in Table 3. We have the following formula:

$$\overline{E} = \overline{E}_T + \overline{E}_R \tag{1}$$

where

$$\overline{E}_R = \overline{N}_R * P_R * t_R, \qquad \overline{E}_T = \overline{N}_T * P_T * t_T \tag{2}$$

Furthermore, we have $\overline{N}_T$=$\overline{N}_R$=$\overline{N}_{hop}$ and
t_R=t_T=t=S_{packet}/μ=64*8/(1.6*10^6)=3.2*10^{-4}(sec)
From the above, there is a formula:

$$\overline{E} = \overline{N}_{hops}(P_T + P_R)t = 3.376\overline{N}_{hops} \tag{3}$$

The average energy consumptions per delivered packet in the two protocols are reported in Fig. 8. The energy consumptions of both protocols grow with the increase of the number of sensor nodes. By comparison, the energy consumption of SSRouting increases much faster than that in WMSNRouting, and it becomes very high when the size of the network grows. In particular, the energy consumption of WMSNRouting only increases a little bit when the number of sensor nodes grows. The main reason is that longer distance was covered by powerful mesh nodes. Consequently,

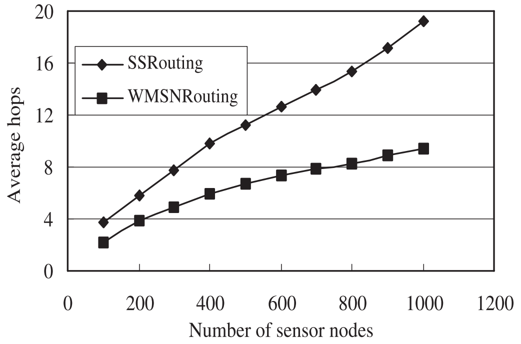

Fig. 7 Average hops vs the size of sensor networks.

Table 3 Notations for routing performance testing.

Symbol	Description
P_T(0.66 W)	transmitting power consumption
P_R(0.395 W)	receiving power consumption
t_T	transmitting time for a packet
t_R	receiving time for a packet
$\overline{E}_T$	transmitting energy consumption for a packet
$\overline{E}_R$	receiving energy consumption for a packet
$\overline{E}$	average energy consumption per packet
$\overline{N}_T$	average transmitting times per packet
$\overline{N}_R$	average receiving times per packet
$\overline{N}_{hops}$	average hops per a packet
μ(1.6*10^6 Mbps)	transmitting / receiving speed
S_{packet}	size of a packet

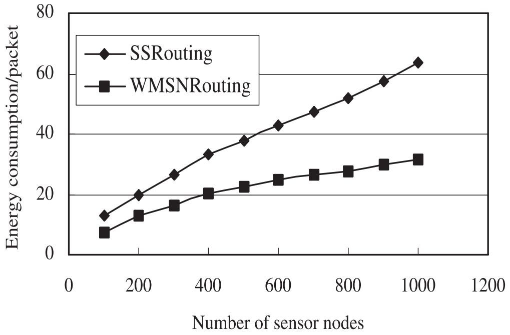

Fig. 8 Average energy consumption per packet vs the size of sensor networks.

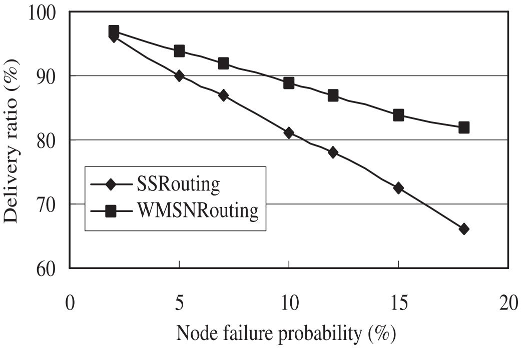

Fig. 9 Average delivery ratio under different failure probability of sensor nodes.

our routing protocol is more energy-efficient than SSRouting, especially for large-scale sensor networks.

Packet delivery ratio. Data packets may be lost because of the failure of sensor nodes. Packet delivery ratio is a performance metrics that measures the ratio of packets received by the sink to that generated by the sensor nodes. In this experiment, the number of sensor nodes was 100; and the area of the network was 100 m×100 m. Figure 9 demonstrates that the delivery ratios of both protocols decrease as sensor failure probability increases. However WMSNRouting always has higher delivery ratio than SSRouting.

In WMSNRouting, a sensor node only sends data packets to the closest mesh gateway, and the rest transmissions to the base station are finished by the mesh transmission backbone. A data packet routing in WMSNRouting involves fewer hops than that in SSRouting. As a result, node failure affects WMSNRouting on the packet delivery ratio much less than SSRouting. On the other hand, mesh nodes are more reliable than sensors. Thus, the delivery ratio of WMSNRouting is higher than that of SSRouting.

6. Conclusions and Future Work

We have proposed a scalable routing protocol designed for tier-based large-scale sensor networks, and presented a security mechanism for our routing protocol. Our routing protocol aims at multiple-gateway sensor networks with high scalability. Secure solution can resist most of attacks against routing in sensor networks. Simulations show that our WMSNRouting protocol has lower average hops, less energy consumption, and higher delivery ratio than SSRouting for single-sink-based sensor networks. Better routing performance is achieved by utilizing powerful multiple mesh nodes, which forward data over the long-distance and in a more reliable way.

We are going to investigate how to schedule mesh nodes to the best locations to maximize the lifetime of sensor networks. The mobility of sensor nodes also will be considered to support many mobile applications such as traffic management and antiterrorism activities.

Acknowledgements

Feilong Tang would like to thank The Japan Society for the Promotion of Science (JSPS) and The University of Aizu (UoA), Japan for providing the excellent research environment during his JSPS Postdoctoral Fellow Program (ID No. P 09059) in UoA, Japan.

This work was supported by the National Natural Science Foundation of China under grants 60773089, 60533040 and 60725208, and the 863 Program of China under grants 2006AA01Z172 and 2008AA01Z106.

References

[1] E. Biagioni and K. Bridges, "The application of remote sensor technology to assist the recovery of rare and endangered species," Distributed Sensor Networks for the International Journal of High Performance Computing Applications, vol.16, no.3, pp.112–121, 2002.

[2] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient security mechanisms for large-scale distributed sensor networks," Proc. 10th ACM Conf. Computer and Communications Security, pp.62–72, New York, 2003.

[3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Commun. Mag., vol.40, no.8, pp.102–114, 2002.

[4] A. Perrig, R. Szewczyk, J.D. Tygar, et al., "SPINS: Security protocols for sensor networks," Wirel. Netw., vol.8, no.5, pp.521–534, 2002.

[5] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Networks, vol.1, pp.293–315, 2003.

[6] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing wireless sensor networks," Department of Computer Science, University of Colorado, Technical Report CU CS-939-02, 2002.

[7] Y. Wang, Attebury G. and B. Ramamurthy, "A survey of security issues in wireless sensor networks," IEEE Communications Surveys & Tutorials, vol.8, no.2, pp.2–23, 2006.

[8] I.F. Akyildiz, X.D. Wang, et al., "Wireless mesh networks: A survey," Comput. Netw., vol.47, pp.445–487, 2005.

[9] A. Perrig, R. Canetti, D. Song, and J.D. Tygar, "Efficient and secure source authentication for multicast," Proc. Symposium on Network and Distributed Systems Security (NDSS 2001), pp.35–46, 2001.

[10] P. Traynor, R. Kumar, H. Choi, et al., "Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks," IEEE Trans. Mobile Comput., vol.6, no.6, pp.663–677, 2007.

[11] R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "LE ACH: Energy-efficient communication protocol for wireless microsensor networks," Proc. Hawaii International Conference on System Sciences, pp.3005–3014, 2000.

[12] X. Zhu, L. Shen, and T.-S.P. Yum, "Hausdorff clustering and minimum energy routing for wireless sensor networks," IEEE Trans. Veh. Technol., vol.58, no.2, pp.990–997, 2009.

[13] M. Yu, K.K. Leung, and A. Malvankar, "Dynamic clustering and energy efficient routing technique for sensor networks," IEEE Trans. Wireless Commun., vol.6, no.8, pp.3069–3079, 2007.

[14] J.H. Chang and L. Tassiulas, "Maximum lifetime routing in wireless sensor networks," IEEE/ACM Trans. Netw., vol.12, no.4, pp.609–619, 2004.

[15] A.P. Azad and A. Chockalingam, "Mobile base stations placement and energy aware routing in wireless sensor networks," Proc. WCNC 2006, pp.264–269, 2006.

[16] V. Shah-Mansouri, A.H. Mohsenian-Rad, and V.W.S. Wong, "Lexicographically optimal routing for wireless sensor networks with multiple sinks," IEEE Trans. Veh. Technol., vol.58, no.3, pp.1490–1500, 2009.

[17] J.N. Al-Karaki and A.E. Kamal, "Routing techniques in wireless sensor networks: A survey," IEEE Wireless Commun., vol.11, no.6, pp.6–28, 2004.

[18] R. Madan and S. Lall, "Distributed algorithms for maximum lifetime routing in wireless sensor networks," IEEE Trans. Wireless Commun., vol.5, no.8, pp.2185–2193, 2006.

[19] J. Park and S. Sahni, "An online heuristic for maximum lifetime routing in wireless sensor networks," IEEE Trans. Comput., vol.55, no.8, pp.1048–1056, 2006.

Feilong Tang received his Ph.D. degree in Computer Science and Technology from Shanghai Jiao Tong University (SJTU), China in 2005. From September 2007 to October 2008, Dr.Tang was a visiting researcher in the University of Aizu, Japan. Currently, he works with the Department of Computer Science and Engineering at SJTU, China. His research interests include wireless sensor networks, grid and pervasive computing, reliability computing, and distributed systems.

Minyi Guo received his Ph.D. degree in computer science from University of Tsukuba, Japan. He is now a full professor at the Department of Computer Software, The University of Aizu, Japan. His research interests include pervasive computing, parallel and distributed processing and parallelizing compilers. He is a member of ACM, IEEE, and IEEE Computer Society.

Song Guo received the Ph.D. degree in computer science from the University of Ottawa, Canada in 2005. From 2006 to 2007, he was an Assistant Professor at the University of Northern British Columbia, Canada. He is currently an Assistant Professor at School of Computer Science and Engineering, the University of Aizu, Japan. His research interests are in the areas of protocol design and performance analysis for communication networks, with a special emphasis on wireless ad hoc and sensor networks.