

Secure Routing for Wireless Mesh Sensor Networks in Pervasive Environments

Feilong TANG, Minyi GUO, Minglu LI, Cho-Li WANG and Mianxiong Dong

Abstract- Wireless mesh sensor network (WMSN) is a new architecture that merges advantages of wireless mesh networks and wireless sensor networks, especially on scalability, robustness and balanced energy dissipation. Secure routing in WMSNs faces with more challenges than that in traditional sensor networks by reason of multiple sink nodes and the mobility of nodes. In this paper, we propose a scalable architecture of WMSNs, discuss and analyze key research issues under the proposed architecture, and then design two routing protocols aiming at minimizing the number of hops between a source node and a destination node and maximizing the lifetime of sensor networks. Considering new challenges to security in WMSNs, this paper also presents a secure routing protocol SecMLR, which can resist most of attacks against routing in WMSNs and work in energy-efficient way.

Index Terms—Wireless mesh sensor network, wireless sensor network, security, routing protocol, architecture.

1. INTRODUCTION

The goal of pervasive computing is to create ambient intelligence, reliable connectivity, and secure and ubiquitous services in order to adapt to the associated context and activity. To make this envision a reality, various interconnected sensor networks have to be set up to collect context information, providing context-aware pervasive computing with adaptive capacity to dynamically changing environment.

Wireless sensor networks (WSN) can help people to be aware of a lot of particular and reliable information anytime anywhere by monitoring, sensing, collecting and processing the information of various environments and scattered objects. The flexibility, fault tolerance, high sensing, self-organization, fidelity, low-cost and rapid deployment characteristics of sensor networks are ideal to many new and exciting application areas such as military, environment monitoring, intelligent control, traffic management, medical treatment, manufacture industry, antiterrorism and so on [1, 2]. Therefore, recent years have witnessed the rapid development of WSNs. Routing for WSNs is one of the most active research areas. However, existing routing protocols for WSNs are built on the network architecture (called flat architecture) such that all sensor nodes are homogeneous and send their data to a single sink node by multiple hops [3-5]. Such a flat

architecture is inapplicable to many real applications with large-scale and heterogeneous sensor nodes. Summarily, on account of limited power, computing and memory of sensor nodes, the flat architectural model inherently has the following problems:

- *Unbalance on energy consumption among nodes.* Energy consumption on sensor nodes is a focus in design of WSNs because of restricted and usually unchargeable batteries in sensor nodes. Many energy-centralized routing protocols for WSNs were investigated and reported [6-8]. In those proposals, all the sensed data is routed to the single sink node so that sensor nodes near the sink inevitably drain their energy ahead of other nodes far from the sink because the former forwards data for the entire sensor network. Such a limitation is unavoidable even if maximizing network lifetime based routing protocols[9-10] are used in the flat architecture of WSNs. To alleviate this limitation, some researchers proposed the concept of mobile base stations [11], however, sensor nodes located in the edge of sensor networks still drain their energy prior to others.

- *Poor scalability.* Wireless transmission in the flat architecture makes use of short-distance communication protocols (e.g., 802.15.4). With the expansion of sensor networks, the average number of hops between a source sensor node to the single sink become more and more, resulting in more energy consumption and transmission delay, which restricts deployment of sensor networks in more scale, thus limits its application areas.

- *Poor robustness.* Some sensor nodes potentially cannot send their data back to the sink node if their neighbor nodes do not work because of exhausted battery, bad environment and others.

- *Single point of failure.* WSNs cannot work completely if the single sink node fails. Further, there is potential communication traffic congestion around the sink.

Owing to above limitations of traditional architecture of WSNs, wireless mesh sensor network (WMSN) is attracting more and more attentions from industry and academic communities as a possible way to improve the scalability, reliability and throughput of sensor networks and support the node mobility [12, 13]. Sereiko [14] firstly proposed to introduce technologies of wires mesh networks into wireless sensor networks, namely deploying wireless mesh nodes as gateways in wireless networks to form a new network architecture. By deploying some super mesh nodes with capacities to transmit data in a long-distance way and self-organize reliably, WMSN merges the advantages of mesh networks and wireless sensor networks, providing the capacities to interconnect multiple

Manuscript received May, 2007.

Feilong Tang and Minyi Guo are with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (email: {tang-fl, guo-my}@cs.sjtu.edu.cn), and the School of Computer Science and Engineering, the University of Aizu, Japan (email: {fltang, minyi}@u-aizu.ac.jp). Minglu Li is with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China. Cho-Li Wang is with the Department of Computer Science, The University of Hong Kong. Mianxiong Dong is with the School of Computer Science and Engineering, the University of Aizu, Japan.

homogeneous/heterogeneous sensor networks, improve the scalability, robustness and data throughput of sensor networks, and support the mobility of nodes.

Routing is highly related to the network architecture. Further, it should be carefully considered how to keep forwarded data safe for extremely open pervasive environments, however, little results have been reported. For WMSNs, there has not yet a well-defined architectural model with scalability and robustness. Also, there is a lack of secure and energy-efficient routing protocols for WMSNs at this time, considering multiple mobile sink nodes as well as information assurance. Neither of existing Internet and wireless mobile network routing protocols sufficiently address new requirements and issues of communications in WMSNs.

This paper is set to address the above challenging issues, focusing on two major parts: (1) the architectural model of WMSNs that greatly extend the functionalities of traditional sensor networks to suit for pervasive computing, and (2) secure and energy-efficient routing protocols under the proposed architecture. Our architectural model and routing protocols are based on guaranteeing routing security as well as minimizing energy consumption to adapt the characteristics of sensor networks.

The remainder of this paper is organized as follows. In the next section, we review related work. In Section 3, we propose a scalable architecture for WMSNs. In Section 4, we discuss key issues under the proposed architecture. Section 5 presents two routing protocols aiming at minimizing the number of hops and maximizing the lifetime of sensor networks respectively. In Section 6, we investigate secure routing in WMSNs. The implementation considerations are reported in Section 7. Finally, Section 8 concludes the paper.

2. RELATED WORK

There have been many research efforts on WSNs [15]. In this Section, we will review the background and work related to our research issues, with the focuses on architecture, routing protocols and proposals on security routing in WSNs.

2.1 Architectural Model of Wireless Sensor Networks

Existing researches on WSNs generally are built on flat architecture mentioned above, where hundreds of even thousands of sensors (randomly) distributed in a monitoring area self-organize into a sensor network with a single sink node for connecting to wired or wireless networks. Sensor nodes communicate with each other using wireless broadcast. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink and further to the end users. For saving power, each node can receive only its neighbor nodes by adjusting its radio power. Sensed data is sent back to the

sink node step by step by multiple hops [3, 16]. Such a flat architecture inherently is poorly scalable and robust, and unbalanced to use energy.

To improve the routing efficiency and scalability, some researchers proposed cluster-based hierarchical routing protocols such as *LEACH* (low energy adaptive clustering hierarchy)[17] and *TEEN* (threshold sensitive energy efficient sensor network protocol)[18]. In *LEACH*, A head randomly elected relays sensing data for all sensor nodes in its cluster. We found that such protocols are not able to overcome the poor robustness problem even if the hierarchical routing protocols are used. For example, if a head goes wrong in the *LEACH* routing, all nodes in the same cluster with the head cannot send back their data. In summary, the existing flat architecture cannot reliably work for large-scale pervasive application, using whether flat routing protocols or hierarchical ones.

Wireless mesh network [13] is a type of mobile wireless network that does not have a wired infrastructure to support communication among the mobile nodes. This type of infrastructure is decentralized (with no central service provider), relatively inexpensive, and very reliable and resilient. The most important feature that distinguishes wireless mesh networks from other wireless networks is high robustness, which means that if one node drops out of the network, due to hardware failure or any other reasons, its neighbors simply find another route. More, extra capacity can be installed by simply adding more nodes. P.Sereiko [14] firstly proposed the concept of wireless mesh sensor network (WMSN) through deploying wireless routers to connect sensor networks.

2.2 Routing Protocols for Wireless Sensor Networks

Many routing protocols have been specifically designed for WSNs. From the perspective of network architecture, these routing protocols can generally be divided into flat-based routing, hierarchical-based routing and location-based routing [19].

2.2.1 Flat-based routing

In flat-based routing, all nodes are typically assigned equal roles or functionality.

Flooding is a classical mechanism to relay data in sensor networks without the need for topology maintenance, but with several serious deficiencies such as implosion, overlap and resource blindness[3, 20]. In flooding, each node receiving a data or management packet broadcasts the packet to all of its neighbors, unless a maximum number of hops for the packet is reached or the destination of the packet is the node itself. *Gossiping*, a derivation of flooding, sends data to one randomly selected neighbor, which avoids implosion problem. However, message propagation takes longer time[3].

SPIN (Sensor Protocols for Information via Negotiation) is a family of adaptive protocols and addresses the deficiencies of classic flooding by considering resource adaptation and data negotiation between nodes. In *SPIN*,

whenever a node has available data, it broadcasts a description of the data instead of all the data and sends it only to the sensor nodes that express interest to save energy [20, 21].

Directed Diffusion [22] is a data-centric and application-aware paradigm in the sense that all data generated by sensor nodes is named by attribute-value pairs. The main idea is to combine the data coming from different sources (in-network aggregation) by eliminating redundancy, minimizing the number of transmissions; thus saving network energy and prolonging its lifetime. *Rumor* routing [23] is a variation of directed diffusion. It routes the queries to the nodes that have observed a particular event rather than flooding the entire network to retrieve information about the occurring events. *CADR* (Constrained anisotropic diffusion routing) aims to be a general form of directed diffusion. The key idea is to query sensors and route data in the network such that the information gain is maximized while latency and bandwidth are minimized.

MCFA (Minimum Cost Forwarding Algorithm) [24] exploits the fact that the direction of routing is always known, that is, towards the fixed external base-station. Hence, a sensor node need not have a unique ID nor maintain a routing table. Instead, each node maintains the least cost estimate from itself to the base-station.

2.2.2 Hierarchical-based routing

In hierarchical routing, sensor nodes play different roles in the network, where higher energy nodes can be used to process and send the information while low energy nodes can be used to perform the sensing in the proximity of the target. Hierarchical routing is an efficient way to lower energy consumption within a cluster by performing data aggregation and fusion in order to decrease the number of transmitted messages to the sink node.

LEACH (low energy adaptive clustering hierarchy)[17] is a 2-level hierarchical routing protocol which attempts to minimize global energy dissipation and 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. However, *LEACH* uses single-hop routing where each node can transmit directly to the cluster-head. Therefore, it is not applicable to networks deployed in large regions. *PEGASIS*[25] (Power-Efficient Gathering in Sensor Information Systems) is an enhancement over the *LEACH* protocol. The basic idea of the protocol is that in order to extend network lifetime, nodes need only communicate with their closest neighbors and they take turns in communicating with the sink.

In *TEEN* (Threshold-sensitive Energy Efficient sensor Network protocol)[18], a cluster node send a hard threshold and a soft threshold to its members to meet time-critical sensing applications. As sensed data exceeds the hard threshold, the node set the new threshold as the hard

threshold and send the data in next slot. Thus, the user can control the trade-off between energy efficiency and data accuracy.

2.2.3 Location-based routing

In this kind of routing protocols, sensor nodes are addressed by means of their locations, and route data using node positions. The distance between neighboring nodes can be estimated by means of incoming signal strengths or GPS (Global Positioning System). Relative coordinates of neighboring nodes can be obtained by exchanging such information between neighbors. Representative protocols include *GAF*(Geographic Adaptive Fidelity)[26] and *SPAN* [27].

2.3 Security Solutions to Routing Protocols for Wireless Sensor Networks

Applications of wireless sensor networks often include sensitive information such as enemy movement on the battlefield or the location of personnel in a building. Lacking security services in the routing protocols, WSNs are vulnerable to many kinds of attacks.

A secure routing in WSNs must address several challenges: vulnerable wireless communication, highly resource-constrained sensor nodes in terms of processing power, storage, and especially battery life, and the risk physically captured. However, few of existing routing protocols for WSNs have been designed with security as a goal [28].

Wang et al. [28] surveyed security issues, summarized the constraints, security requirements, and attacks with their corresponding countermeasures in WSNs, and discussed five kinds of security issues: cryptography, key management, secure routing, secure data aggregation, and intrusion detection. Especially, this research pointed out main network layer attacks against sensor networks: spoofed, altered, or replayed routing information, selective forwarding, sinkhole, sybil, wormholes, hello flood attacks, acknowledgment spoofing. In [29], Karlof et al. proposed threat models and security goals for secure routing in WSNs, introduced two novel classes of attacks against sensor networks-sinkhole attacks and HELLO floods. In particular, this paper analyzed all the major routing protocols and energy conserving topology maintenance algorithms for sensor networks, demonstrating that currently proposed routing protocols for these networks are insecure, and finally discussed countermeasures and design considerations for secure routing protocols in sensor networks.

INSENS [30] is an intrusion-tolerant routing protocol for WSNs. This protocol comprises of route discovery and data forwarding phases. Route discovery phase ascertains the topology of the sensor network and builds appropriate forwarding tables at each node to facilitate communication between sensor nodes and a base station. Data forwarding phase deals with forwarding data from sensor nodes to the

base station, and from base station to the sensor nodes. INSENS does not rely on detecting intrusions, 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 damage in the network. However, INSENS is built on a table based routing protocol, and as such depends on the base stations to collect all needed topology information to calculate the forwarding table for each individual sensor. Thus, INSENS is not scalable in large sensor networks.

SPINS[31] is a suite of security protocols optimized for sensor networks, including two secure building blocks: SNEP and μ TESLA. SNEP provides data confidentiality, two-party data authentication, and data freshness. μ TESLA provides authenticated broadcast for severely resource-constrained environments.

Zhu et al. proposed the *LEAP* (Localized Encryption and Authentication Protocol)[32], a key management protocol for sensor networks that is designed to support in-network processing, while at the same time restricting the security impact of a node compromise to the immediate network neighborhood 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.

The currently proposed secure routing protocols for WSNs focus on static sensor networks only, ignoring mobility. Thus, secure routing protocols for mobile sensor networks need to be investigated.

3. AN ARCHITECTURE OF WIRELESS MESH SENSOR NETWORKS

In this Section, we briefly introduce wireless mesh networks and then propose a scalable architecture of wireless mesh sensor networks. Different from traditional WSNs, each sensor network in our architecture includes more than one wireless mesh nodes as gateways (i.e., sink nodes). The model can easily connect multiple homogeneous or heterogeneous sensor networks, thus significantly improves the scalability, robustness and throughput of sensor networks, and supports node' mobility.

3.1 Wireless Mesh Network

Wireless mesh network (WMN) is a kind of new wireless network architecture paid more and more attention recently. There are different definitions about WMNs, however, their essences are identical: WMN is a self-organized, self-configured, and decentralized wireless network[13]. There are two kinds of nodes in WMNs: mesh router and mobile client. Mesh routers with powerful capacities and lower mobility automatically set up and maintain wireless connection, forming the backbone of WMNs. If routers are equipped with the function of

gateways/bridges, they can interconnect with other kinds of networks (e.g., Internet). Mobile clients also forward data for their neighbor nodes, but they usually provide simple functionalities and a single interface.

One of the most significant characteristics of WMNs is that it provides interconnections among all networked nodes, where each node can send and receive data. Wireless devices in traditional wireless networks have to firstly connect with AP(Access Point) to communicate with other devices, even if they locate within the radio range of each other. Instead, each node in WMNs may directly communicate with more neighboring nodes.

Compared with traditional wireless networks, WMNs have many attractive features such as self-organization, self-healing, little investment, convenient maintenance, high reliability and scalability [13]. For example, when devices are added to or moved from networks, WMNs are able to automatically discover topology change and self-adaptively modify routing for more efficient data transmission. Moreover, WMNs are easy to achieve load balance by rerouting parts of data to neighbor nodes with lower load.

3.2 Architectural Model of Wireless Mesh Sensor Network

Combining wireless mesh networks and wireless sensor networks, we propose an architecture of wireless mesh sensor network (WMSN) by deploying multiple wireless mesh routers equipped with gateways in each sensor network, as shown in Fig.1. The mesh routers deployed in different sensor networks automatically interconnect to form a mesh network while are connected with Internet through powerful base stations. In the proposed architecture, there are three kinds of networks on three logical layers respectively:

- Wireless sensor network for monitoring objects and reporting the objects' information (e.g., temperature and humidity)
- Wireless mesh network for transmitting sensed data in long-distance and reliable way, and
- Internet for users to remotely access sensed data.

Accordingly, a WMSN is composed of three kinds nodes: sensor node, wireless mesh gateway(WMG¹) and wireless mesh router(WMR). In particular, base stations are used to support the mobility of WMGs andWMRs, and connect wireless mesh network with Internet. Sensor nodes continuously or intermittently detect objects and then send data to the most appropriate WMG based on specific routing policies, which will be discussed in details in next Section. WMGs work as sink nodes and gateways of low-level wireless sensor networks, as well as routers of middle-level wireless mesh network. By comparison, WMRs only serve as routers of wireless mesh network. WMGs and WMRs self-organize as the middle-level

¹ We use WMG and gateway interchangeably in this paper.

wireless mesh network for long-distance transmission and interconnect of sensor networks.

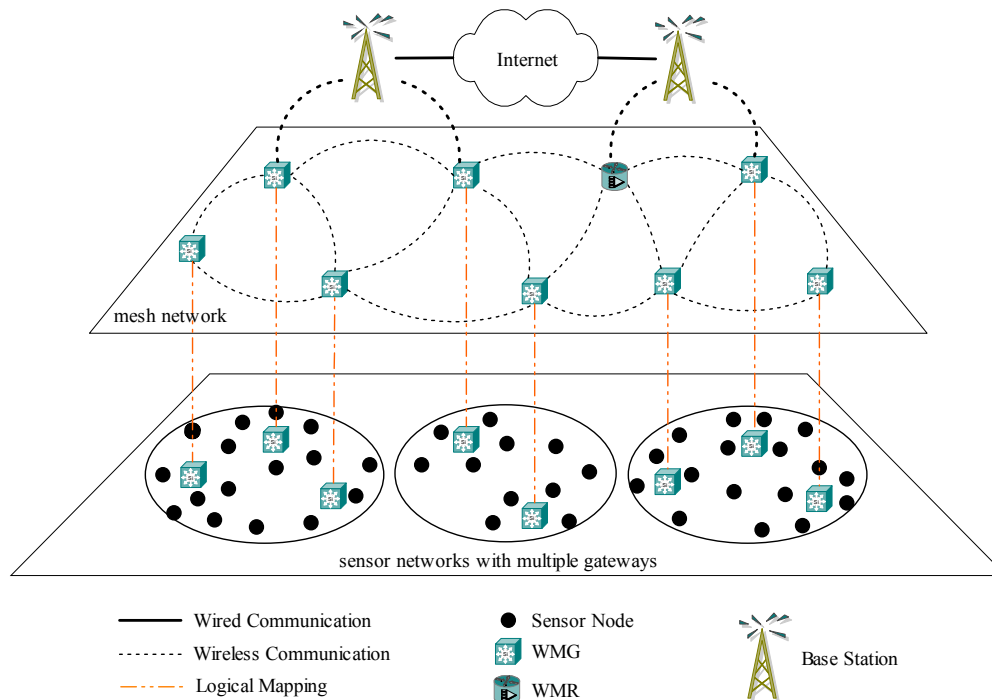


Fig. 1. A scalable wireless mesh sensor network architecture.

Different networks in the architecture use different medium access control (MAC) and routing protocols. In general, wireless sensor networks use short-distance communication protocol (e.g., 802.15.4) while wireless mesh network uses long-distance transmission protocol (e.g., 802.11). More specifically, three kinds of nodes respectively support different MAC protocols: sensor nodes only support 802.15.4; WMRs only support 802.11; WMGs support both.

By merging the advantages of wireless mesh networks and wireless sensor networks, the proposed architecture is self-organized and self-configured, highly scalable and reliable, easy to deploy and interconnect.

4. KEY ISSUES IN WMSNS

To make proposed architecture work more efficiently, the following challenging issues have to be researched, including multiple-gateway deployment, secure routing protocol, multiple gateways based fault-tolerance, load balance and QoS, and topology control. We discuss these issues in the following subsections. This paper focuses on the secure routing, which will be investigated in Section 5 and Section 6.

4.1 Multiple-Gateway Deployment

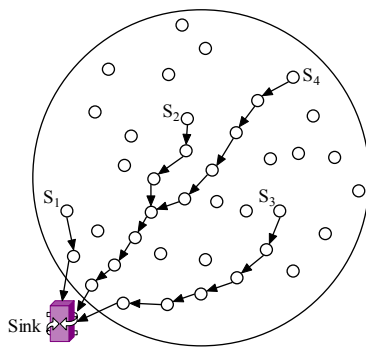
In traditional architecture of sensor networks with a single sink, sensor nodes around the sink inevitably drain

their energy ahead of other nodes because of more heavy data forwarding, whether using flat[21], hierarchical[17] or other routing protocols (e.g., QoS routing[33]). Deploying multiple gateways in a sensor network aims at overcoming this problem, as well as improving network performance and lengthening network lifetime. Two issues have to be researched. One is how many gateways should be deployed for a specific sensor network; another is where the gateways should be deployed. More specifically, we discuss these two issues as follows.

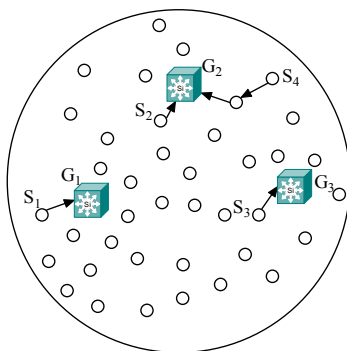
Gateway number model. Multiple gateways avoid the single failure, as well as significantly reduce the average number of hops of data transmission, saving energy consumption and accordingly lengthening network lifetime. We demonstrate this by an example. Let there be an sensor network shown in Fig.2(a), sensor nodes S_1 , S_2 , S_3 and S_4 send data to the single sink by 2,7,6 and 9 hops respectively. By comparison, if three gateways are deployed in the same sensor network, as shown in Fig. 2(b), nodes S_1 , S_2 (S_4) and S_3 send data to gateways G_1 , G_2 and G_3 , respectively by 1, 1(2) and 1 hop(s).

How many gateways are the best for a specified sensor network? Gateway number model is used to formally describe the relationship between the number of gateways and the size of a sensor network, the density and distribution of sensor nodes as well as cost and even other factors. Further, how to divide a large-scale sensor network into a set of subnets? Existing multiple base stations' schemes[10,34] can be helpful to model gateway number.

For example, literature [34] formally described the best number of base stations in a specified sensor network using integer linear programming, and tested by experiments base station number K_{max} when each sensor node is one hop away from the nearest base station. Experiment results demonstrated that increasing the number of base stations (k) cannot improve the network lifetime when k is more than K_{max} . But this proposal did not consider the distribution of sensor nodes and cost and energy restriction of base stations. In some applications of sensor networks, e.g., forest monitoring, mesh gateways are also energy-restricted. Also, mesh gateways are more expensive than sensor nodes. Gateway number model should incorporate these restricted conditions and thus becomes more complex.



2(a). a single sink



2(b). three gateways

Fig. 2. Routing in sensor networks with one sink and three gateways.

Gateway deployment model. Multiple gateways reduce average transmission hops. However, the sensor nodes around gateways still consume more energy to forward packets for other nodes. Gateway deployment model describes how to distribute MGRs in a specified sensor network, including how to select locations and how to schedule gateways in these locations, to maximize the lifetime of the sensor network. The basic principle is minimizing the total energy consumption of the sensor network while balancing the energy consumption of individual sensor nodes.

4.2 Secure Routing Protocol

Routing is a fundamental problem in any type of networks. Compared with existing routing protocols, secure routing for WMSNs is more challenging because WMSNs have the following features:

- multiple gateways. Different sensor nodes select different gateways (i.e., WMGs) as routing destinations, based on specified optimization policy.
- load balance and fault-tolerance. When data transmission from partial monitoring area is too heavy (e.g., a forest fire occurs) during a period of time, some gateways in that area possibly become over loading. Routing protocols should provide the capacity to automatically dispatch parts of traffic to other gateways with low load. Similarly, when a gateway fails, data destined to that gateway should be redirected to its neighboring gateway(s).
- mobility of gateways. To balance energy consumption of all sensor nodes, gateways should keep mobile because sensor nodes around gateways consume more energy to forward data for other nodes. Routing protocols have to self-adapt the mobility of gateways.

4.3 Multiple-Gateway Based Fault Tolerance, Load Balance and QoS

Load balance and traffic congestion control are very important in WMSNs. If too traffic is forwarded to a overloaded gateway based on given routing mechanism (e.g., the least hops), the gateway and its neighboring sensor nodes cannot correctly forward data, increasing transmission delay and losing ratio of packets, while at the same time, other gateways are under starvation state. Therefore, it is necessary to set up QoS control mechanism to redirect parts of network traffic to the starved gateways to balance network load and alleviate network congestion. It is a trade-off how to optimize multiple QoS metrics. QoS based multiple-path routing is one of promising approaches.

4.4 Topology Control

The topology of a WMSN is highly dynamic owing to node (sensor node and/or WMG) mobility or failure. Topology control targets for maximizing network lifetime by optimizing network topology on condition that main network performances, such as connectivity, coverage, traffic delay, load balance, reliability and scalability, are satisfied. It is a challenging problem to develop an energy-efficient topology control mechanism to configure a logical topology that is efficient in energy consumption and stable in topology changes, while at the same time meeting the QoS requirements. Current topology control technologies fall into two categories: power control and sleep scheduling. Power control adjusts sensors' transmission power and /or angle to save energy, lengthen network lifetime, avoid or reduce radio conflict and enhance

network throughput. Sleep scheduling controls sensors between work and sleep states, i.e., schedules sensor nodes to work in turn.

5. ROUTING PROTOCOLS FOR WMSNS

A routing protocol mainly involves finding a route from a source node to a destination node, forwarding data in terms of the established route while maintaining the route in accordance with up-to-date network topology. Routing protocols highly depend on network architecture [5]. In the architecture discussed above, mesh network routing in middle layer has been well researched. In this Section, we focus on routing in low-level sensor networks in the proposed architecture and propose two routing mechanism based on the shortest path and maximal network lifetime.

5.1 Network Model

Let a set of gateways be distributed randomly in a sensor network, forming a mixed sensor network as shown in Fig.3. We model such a sensor network as a graph $G(V,E)$, where

$V=V_S \cup V_G$: V_S is the set of sensor nodes; V_G is the set of gateways;

$E \subseteq (V_S \times V_S) \cup (V_S \times V_G)$: $(V_S \times V_S)$ is the set of one hop links between sensor nodes; $(V_S \times V_G)$ is the set of one hop links between sensor nodes and gateways. By *one hop link*, we mean two nodes can immediately communicate with each other.

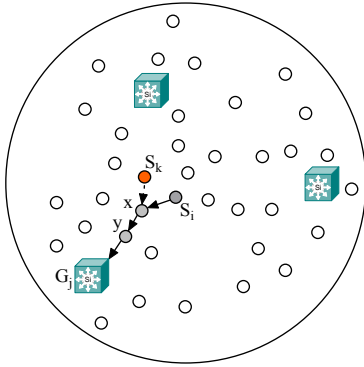


Fig. 3. A wireless sensor network with three mesh gateways.

Let there be two kinds of data transmissions: from sensor nodes to gateways and on the contrary. The radio range of a sensor node only covers its immediate neighboring nodes. Moreover, we model gateways as $MG=\{(G_i, (x_i, y_i)) : 1 \leq i \leq m, (x_i, y_i) \text{ represents any point located in the sensor network}\}$, where m is the number of gateways. In our model, any sensor node $S_i (1 \leq i \leq n)$ keep on static while gateway(s) $G_j (1 \leq j \leq m)$ discretely move(s) within the range of its 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*. As a result, during a round, the sensor network topology keeps fixed.

5.2 Shortest Path Routing (SPR)

Our shortest path routing (SPR) minimizes the number of hops of data transmission between each sensor node and a gateway, thus minimizing total hops of a sensor network. Let all sensor nodes transmit data in identical power so that transmitting 1 bit data consumes the same energy to all of them. Therefore, the less hops, the less energy consumption. So we firstly present the routing protocol SPR which selects the route with the least hops as the best routing. SPR protocol has good performance for sensor networks with nodes distributed evenly. By observation, we find the following property in sensor networks (see Fig. 3).

Property 1. Let exist a path from sensor node x to gateway G_j such that $Path_x = \langle x, y, \dots, G_j \rangle$. If $Path_x$ is the shortest path from x to G_j , its sub-path $Path_y = \langle y, \dots, G_j \rangle$ is also the shortest path from y to the G_j .

Proof: let $Path_x = \langle x, y, \dots, G_j \rangle$ be the shortest path from x to G_j . If a sub-path $Path_y = \langle y, \dots, G_j \rangle$ is not the shortest path from y to the G_j , i.e., there at least exists another path $Path'_y (Path'_y \neq Path_y)$ that has less hops from y to the G_j . If so, there exists another path $Path'_x = \langle x, Path'_y \rangle$ with less hops than $Path_x$. As a result, the $Path_x$ is not the shortest path from x to the G_j , which conflicts with given condition. Therefore, property is correct.

According property 1, we simplify routing discovery and maintenance by the following ways.

- (1) Sensor nodes that locate at an established route do not need to discover routing during the current round. As shown in Fig.3, if there is the shortest path $\langle S_i, x, y, G_j \rangle$ from S_i to G_j , the best routes of nodes x and y are contained in $\langle S_i, x, y, G_j \rangle$. More specifically, x and y all select G_j as the best gateway, and further the shortest paths of x and y are $\langle x, y, G_j \rangle$ and $\langle y, G_j \rangle$ respectively.
- (2) Sensor nodes that have set up routing tables directly return path information rather than further flood. For example, if node S_k in Fig.3 needs to send data, it floods routing request packet RREQ. When x receives the RREQ message with destination G_j , it directly appends sub-path from x to G_j by querying routing table after (S_k, x) and returns the path $\langle S_k, x, y, G_j \rangle$ to S_k .

The shortest paths of sensor nodes change with the movement of gateway(s). 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. Our SPR merges the advantages of table-driven and on-demand routing mechanisms. During a round not all sensor nodes need to set up routing tables; and in next round nodes that need to send data reset up routing table, which not only reduces network traffic and energy consumption

for routing establishment but also can adapt dynamic network topology.

SPR protocol is described as follows, where $\langle S_i, S_j \rangle$ represents a path from sensor node S_i to S_j .

Step 1. If S_i needs to transmit data, it check local routing table. If there is an entry destined to a gateway G_j , which means G_j is the best gateway of S_i , S_i directly broadcast a packet DATA. Otherwise, go to step 2.

Step 2. Routing query. S_i floods a query packet RREQ with m destinations $G_j(j=1,2,\dots,m)$ to find the best gateway and the corresponding shortest path. Go to step 3.

Step 3. Routing response.

Step 3.1 Other sensor others $S_k(k=1,2,\dots,n; k \neq i)$ check their local routing tables. If S_k finds a entry containing a routing information to a gateway G_j , it appends the shortest path $\langle S_k, G_j \rangle$ from S_k to G_j after the path $\langle S_i, S_k \rangle$ that RREQ has passed such that $\langle S_i, G_j \rangle = \langle S_i, S_k \rangle + \langle S_k, G_j \rangle$, and returns path $\langle S_i, G_j \rangle$ to S_i . Otherwise, it floods RREQ packet.

Step 3.2 If a gateway G_j receives the RREQ packet, it responds the path $\langle S_i, G_j \rangle$ to S_i .

Step 4. Source node S_i ascertains the best gateway and the corresponding shortest path. After receiving multiple routing information to multiple gateways, S_i draws a conclusion on the best gateway and the corresponding shortest path.

Step 5. Setting up routing table and transmitting data.

Step 5.1 S_i encapsulates a data packet DATA, attaching the short path $\langle S_i, G_j \rangle$ in the head of the first data packet.

Step 5.2 Sensor nodes located in the path $\langle S_i, G_j \rangle$ forward in turn the data packet until G_j hop by hop according to the routing information $\langle S_i, G_j \rangle$. At the same time, these nodes set up their local routing tables, each of them takes G_j as its best gateway.

Step 5.3 Following data packets generated from 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.

5.3 Maximal Network Lifetime Routing (MLR)

Network lifetime is the most important performance of sensor networks [35]. Above SPR protocol aims at minimizing the number of hops, which minimizes energy consumption but does not consider energy balance among sensor nodes. If sensor nodes are unevenly distributed, some nodes are possibly located on the shortest paths of multiple nodes so that they take charge of too heavy forwarding tasks and die before others.

In this paper, we define network lifetime as the time when the first sensor node drains its energy. We formally describe the routing protocol MLR with the goal of maximizing network lifetime. Let gateways have unrestricted energy. Ideally, maximizing lifetime of sensor networks needs to simultaneously satisfy the following two conditions: (1) total energy consumption of all sensors in a network $\sum E_i$ is minimal, where E_i is energy consumption of node S_i ; (2) differences between individual node' energy consumption $E_i(1 \leq i \leq n)$ and average energy consumption

\bar{E} is minimal, i.e., variance $D^2 = \sum_{i=1}^n (E_i - \bar{E})^2$ gets

minimal, where \bar{E} is the average of energy consumption of all sensor nodes in a network such that $\bar{E} = \sum_{i=1}^n E_i$.

Therefore, above problem becomes how to solve minimal D^2 under minimal $\sum E_i$, namely

Goal: Minimize $D^2 = \sum_{i=1}^n (E_i - \bar{E})^2$

$$\text{Minimize } \bar{E} = \sum_{i=1}^n E_i \quad (1)$$

$$E_t \sum_{j \in N(i)} x_{ij} + E_r \sum_{k \in N(i)} x_{ki} = E_i \quad (2)$$

$$\sum_{j \in N(i)} x_{ij} - \sum_{k \in N(i)} x_{ki} = T \quad (3)$$

$$\sum_{l \in V_g} x_{il} = T g_{il} \quad (4)$$

$$g_{il} = \begin{cases} 1, & S_i \text{ sends data to } G_l \\ 0, & \text{otherwise} \end{cases} \quad (5)$$

$$x_{ij} \geq 0, i \in V_s, k \in V_s, j \in V, l \in V_G \quad (6)$$

where

E_r and E_t : energy consumption for receiving and sending a packet respectively(here we do not consider energy consumption for data processing);

x_{ij} : the number of packets sent from S_i to S_j ; and

$N(i)$: the set of neighboring nodes of S_i .

E_i in equation (2) is S_i ' energy consumption for receiving and sending data during a round; T in equation (3) represents the number of packets generated by S_i during a round. Equation (4) restricts S_i sends data packets to the same gateway G_l during a round.

Accurately resolving above goal is rather complex because it probably is a NP problem. In this Section, we propose a heuristic routing protocol, providing results approximate to above design goal. Similar to existing related work [34,36], we let m gateways only be deploy in a set of feasible places such that $P = \{P_i; P_i \text{ is a feasible place in the network area}\}$, m of them are deployed

gateways during a round. Unlike those work which resets up routing tables at the beginning of each round, our principle is to accumulate routing tables round by round. After all places are deployed gateways, all sensor nodes keep a routing table that contains the best gateway and corresponding path, without demand to set up new routing any more. If a gateway changes place in a new round, it only notifies all sensor nodes its new place. This approach significantly reduces delay and saves energy for routing discovery. Using this approach, each node keeps a routing table containing $|P|$ (the number of feasible places) entries, with an extra storage overhead ($|P|-m$), which is acceptable under limited feasible places $|P|$. We describe the basic idea of the algorithm as follows.

- (1) Set up routing table. There are $|P|$ feasible places to deploy gateways. We locate gateways at m feasible place in terms of energy-efficient criteria during a round. Each sensor first discovers the best path to each gateway using above SPR protocol, then stores them in local routing table, finally takes the path with minimal hops as actual forwarding path.
- (2) Update routing table by adding entries. At the beginning of a new round, moved gateways notify all sensor nodes in local network of their new places. Each node checks its own routing table. If there does not exist an entry destined to the new places, the sensor node sets up new routing and selects the best path using the method described in step 1. Note that unmoved gateways do not need to issue such a notification.
- (3) After each feasible place has been deployed a gateway, routing table of each sensor node contains $|P|$ entries. From then on, each sensor node only needs to select the best path from m entries which respond to m deployed places during the current round based on notifications from moved gateways. In our current consideration, we define the shortest path with the least hops as the best path.

To explain above procedure more clearly, we illustrate a process of routing setting and maintenance by an example with five feasible places and three gateways such that $|P|=5$ and $m=3$. Five places are represented by A,B,C,D and E respectively, by which we also denote gateways deployed at corresponding places. In routing table shown in Table 1, *route* means the shortest path from S_i to corresponding gateway, *hops* represents the number of hops on the corresponding shortest path.

(1) In the first round, let gateways are deployed at places A, B and C. Node S_i finds routing information (see Table 1(a)) using our SPR protocol, then selects “-----,B” that is a route as the shortest path, i.e., sends data packets to the gateway B along the specified path.

(2) In the next round, let the gateway deployed previously at place B be moved to place D while gateways at places A and C are not moved, shown in Table 1(b). The shortest paths from S_i to gateways A and C are unchanged because these gateways and all sensor nodes are located at the same places as those in last round. However, routing

destined to gateway D will be added to its routing table. After comparing, S_i selects “-----,D” with 5 hops as the short path.

(3) In the third round, let gateway A be moved to place E while gateways C and D keep unmoved. By similar procedure, S_i sets up incremental routing table shown in Table 1(c). By comparison, S_i still selects “-----,D” with 5 hops as the short path.

(4) After each feasible place has been deployed a gateway, S_i completes its routing setting. Form then on, S_i only needs to select the path with the least hops as its forwarding path from current m places during current round.

Other sensor nodes similarly set up routing tables.

Table 1: Routing table generation and maintenance of node S_i

(a) S_i routing table during the first round

P_i	hops	route
A	8	-----
B	6	-----,B
C	7	-----

(b) S_i routing table during the second round

P_i	hops	route
A	8	-----
B	6	-----
C	7	-----
D	5	-----,D

(c) S_i routing table during the third round

P_i	hops	route
A	8	-----
B	6	-----
C	7	-----
D	5	-----,D
E	6	-----

6. SECURE ROUTING FOR WMSNs

Many applications of WMSNs have mission-critical tasks, dependent on the correctness of sensed data obtained from dispersed sensor nodes, however, sensor networks are susceptible to a variety of attacks, including node capture, physical tampering, and denial of service. Thus, security has to be considered for WMSNs.

Because sensor networks pose unique challenges, traditional security techniques used in wired and wireless networks cannot be applied directly. First, sensors 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 (e.g., captured) attack. And third, sensor networks interact closely with their physical

environments and with people, posing new security problems[37].

6.1 Overview of Secure Routing for Wireless Sensor Networks

For multiple hops WSNs, sensed data needs to be forwarded to its destination by multiple sensor nodes that potentially are attacked. As a result, secure routing is at the center for ensuring the security of WSNs. The goal of security services in WSNs is to protect the information and resources from attacks and misbehavior, including *availability*(ensuring the desired network services available even in the presence of denial-of-service attacks), *authorization*(ensuring that only authorized sensors can be involved in providing information to network services), *authentication* (allowing a receiver to verify that the data really was sent by the claimed sender), *confidentiality* (a given message cannot be understood by anyone other than the desired recipients), *integrity* (a message is not modified by malicious intermediate nodes), *nonrepudiation*(a node cannot deny sending a message it has previously sent) and *freshness* (no adversary can replay old messages) [28].

Compared with traditional networks, WSNs have many characteristics that make them more vulnerable to attacks. Hence, when designing or proposing security mechanisms against routing attacks, besides the basic requirement, e.g., data availability, confidentiality, authenticity and integrity, for any security mechanism, the following peculiarities should be carefully considered:

- *lightweight computations*. In generally, WSN nodes are equipped with battery power, which means these 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 have been proposed to achieve the goals of data secrecy and integrity [38].

- *fault-tolerance*. A distinguishing feature of WSNs is that attackers can capture a sensor and acquire all the information stored within it[39]. The security routing should automatically recover from potential attacks. More specifically, secure routing should be able to function correctly at a cost of graceful performance degradation even if some of the nodes participating in routing are intentionally disrupting its operation.

6.2 Secure Maximal Network Lifetime Routing (SecMLR)

Most of the current protocols assume that the sensor nodes and the base station are stationary. However, there may be situations, such as battlefield environments, where the base station and possibly the sensors need to be mobile. The mobility of nodes has a great influence on sensor

network topology and thus raises many issues about secure routing protocols [28]. Generally, the sensor networks may be deployed in unprotected areas so that individual sensor nodes are untrusted. Similar to existing secure routing schemes that regard base stations trustworthy [28], we assume that gateways are trustable and there are only two kinds of communications: one is from sensor nodes to gateways and another is on the contrary. Further, let each sensor node be pre-distributed secret keys, each shared with a gateway.

We use the following notation to describe security protocols and cryptographic operations in this paper.

S_i : one of n sensor nodes in a sensor network ($1 \leq i \leq n$)

G_j : one of m gateways in the sensor network ($1 \leq j \leq m$)

x, y : intermediate sensor nodes located in a path between a source node and a destination node

REQ, RES, DATA: the type of packets, representing routing query, routing response and data packets respectively

K_{ij} : a symmetric secret key shared between a specified sensor node S_i and a specified gateway G_j .

$M_1|M_2$: the concatenation of messages M_1 and M_2

$\{M\}_{<K_{ij}, C>}$: the encryption of message M , with key K_{ij}

and the incremental counter C [31]

$MAC(K_{ij}, M)$: the message authentication code (MAC) of message M , with the symmetric secret key K_{ij}

$path_{ij}(k)$: a path between a sensor node S_i and a gateway G_j

We present a secure routing protocol SecMLR that ensures the security of our MLR protocol by the following measures.

6.2.1 Routing query

In this phase, sensor nodes that need to send data but has not set up a routing table query routing information by flooding a query packet with m destinations, i.e., all m gateways, using the following message:

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

where *req* denotes the routing query information between S_i and G_j , as shown in Fig. 4(a).

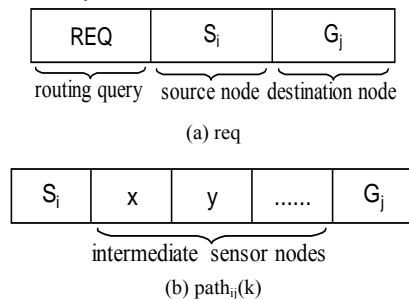


Fig.4. path query information *req* for node pair (S_i, G_j).

A request message broadcasted by a node x includes a path from the source node S_i to x . When a node receives the request message for the first time, it in turn forwards (broadcasts) this message after appending itself in the

$path_{ij}(k)$ field. If the node receives duplicate request message, the duplicate request is not rebroadcasted. For example, if node y receives a query packet sent from x and originated by S_i with a head REQ, it adds itself to existing " $S_i \rightarrow x$ ", forming an added path such that " $S_i \rightarrow x \rightarrow y$ ".

6.2.2 Response to routing query

Whenever a gateway G_j receives a routing query packet, it verifies (1) whether the req 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 by G_j .

For each pair nodes (S_i, G_j), there in general are multiple different paths $path_{ij}(k)$. Thus, when G_j receives the first query packet from S_i , it waits a given timeout to collect multiple path information. After the timeout, G_j calculates the shortest path between S_i and G_j by the following formula:

$$path_{ij} = \text{Min} (|path_{ij}(k)|) \text{ for all } k$$

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 $\text{Min}()$ is a function to solve the path with the least hops among all $path_{ij}(k)$.

After getting $path_{ij}$, G_j encapsulates a routing response packet RRES in the following format:

$$G_j \rightarrow S_i: \{res\}_{<K_{ij}, C>}, path_{ij}, MAC \{K_{ij}, C | \{res\}_{<K_{ij}, C>}\}$$

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

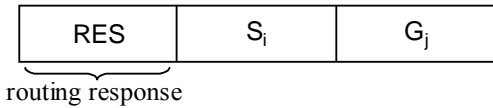


Fig. 5. path response information res for node pair (S_i, G_j)

Finally, G_j sends the RRES packet to S_i . Sensor nodes located in $path_{ij}$ forwards in turn the RRES packet in terms of the information in $path_{ij}$ field while simultaneously records the corresponding path information in local routing tables. For example, if $path_{ij}$ is $S_1 \rightarrow x \rightarrow y \rightarrow G_1$, nodes S_1, x and y parse individual shortest path to G_1 , specifically $S_1 \rightarrow x \rightarrow y \rightarrow G_1$, $x \rightarrow y \rightarrow G_1$ and $y \rightarrow G_1$ respectively, in corresponding local routing tables.

6.2.3 Routing updating

At the beginning of a round, gateways that move broadcast their new places, using μ TESLA protocol [31] to achieve authenticated broadcast.

6.2.4 Data forwarding

Data forwarding means to route data from sensor nodes to gateways, or from gateways to sensor nodes. After a sensor node successfully discovered the shortest path to a specified destination (gateway) node, all sensor nodes located in the path record corresponding shortest path to

the specified gateway in 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 is constructed as follows:

$$S_i \rightarrow G_j: \{data\}_{<K_{ij}, C>}, RI, MAC \{K_{ij}, C | K_{ij}\}$$

where $data$ means forwarded data from S_i to G_j , and RI is routing information (see Fig.6).

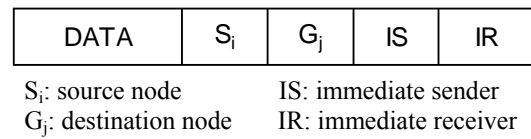


Fig.6. packet format of RI

With routing tables constructed previously, forwarding data packets is quite simple. On receiving a data packet, a node searches for a matching entry in its routing table. If it finds a match, it respectively changes the IS and IR fields into itself and next hop node, and then forwards (broadcasts) the data packet. Otherwise, it drops the data packet. For the discovered shortest path $S_1 \rightarrow x \rightarrow y \rightarrow G_1$ between S_1 and G_1 , for example, each node keeps the routing entry to G_1 such that

$$S_1: (S_1, G_1, \emptyset, x)$$

$$x: (S_1, G_1, S_1, y)$$

$$y: (S_1, G_1, x, G_1)$$

If node x receives a matching data packet with $IS=S_1$ and $IR=x$, x modifies IS and IR into x and y respectively, then forwards this packet.

Our SecMLP can resist most of attacks against routing in sensor networks. In addition, it performs main computing tasks on *resource-rich gateways* during routing establishment, which significantly lengthens the lifetime of sensor networks as well as improves to some extent the network performance.

7. IMPLEMENTATION CONSIDERATIONS

Pervasive applications need sensor networks and other infrastructures to sense and transmit context information. In this Section, we discuss implementation considerations.

7.1 Design of a Scalable WMSN Architecture

The proposed architecture should be able to self-organize (as nodes are powered on, they automatically enter the network), self-heal (as a node leaves the network, the remaining nodes automatically re-route their data around the out-of-network node) and *interconnect heterogeneous sensor networks*. The topology of a WMSN

is highly dynamic owing to node (sensor and/or gateway) mobility or failure. An energy-efficient topology control mechanism is needed to configure a logical topology that is efficient in energy consumption and stable in topology changes, while at the same time meeting the routing requirements.

7.2 Implementation of Routing Protocols SPR and MLR

To design efficient routing protocols for WMSNs, the following considerations need to be taken into account.

Developing an analytical model

Since the network parameters such as WMG distribution, node mobility, and node status changes (e.g., failure) differ dramatically from application to application, it is necessary to have an analytical model to quantitatively analyze the performance of routing methods under various network situations and determine the best method for a particular application. We will first develop an analytical performance model for evaluating different routing strategies in wireless mesh sensor networks, so that the developed routing methods can be highly adaptive to specific application requirements and the network environments. We will take the following three steps: (1) developing an analytical model to describe the relationship among the number of WMGs, the number and distribution of sensor nodes in a sensor network. (2) developing a model to solve how to move WMGs. (3) developing a model for analysis of routing protocols.

Design self-adaptive routing protocols

Routing protocols for WMSNs must consider not only to minimize the energy consumption of networks but also to use the energy in a balanced way because sensor nodes are energy-restricted. In WMSNs proposed above, multiple (mobile) gateways (i.e., routing target nodes for a sensor network) are deployed in a sensor network, making secure routing protocols more complex. We will seek efficient solutions to secure routing for WMSNs, and develop routing algorithms that satisfy the following requirements:

- The routing algorithm should be highly self-adaptive. On the one hand, different sensor nodes route their data to different WMGs. On the other hand, the same node possibly routes the sensed data through a different path and to different WMGs at different time because of energy restrictions, node mobility and sudden changes in node status (e.g., failure).
- The routing algorithm should be fully distributed. Highly distributed sensor nodes are limited in energy, computing and storage capability so that it is impossible for a central node to keep this information.
- The routing algorithm should be efficient in terms of both the number of messages and the time required for finding a route.

8. CONCLUSIONS

We have proposed an architecture for WMSNs, designed a set of routing protocols focusing on maximizing lifetime of sensor networks, and finally presented a security solution to routing protocols of WMSNs. The proposed three-layer architecture is self-organized, self-healing, and thus reliable. The distinguishing feature of the architecture is that it significantly improves the scalability of sensor networks by introducing mesh nodes for long-distance transmission. Our routing protocols are designed for multiple-gateway sensor networks, each gateway as a sink node. Routing protocol MLR, which aims at maximizing network lifetime, merges the advantages of table-driven and demand-driven routing protocols. Secure solution to routing protocols can prevent or increase the difficulty of launching many security attacks against sensor networks. In SecMLR protocol, any sensor node that has sent data sets up a routing table with multiple entries, each of them routes data from the sensor node to a specified gateway. If the best route fails to transmit data correctly, sensor nodes may redirect data transmission using other routes, which providing fault-tolerance ability to malicious intrusion to some extent.

ACKNOWLEDGEMENT

This work was supported by National Natural Science Foundation of China (Grant Nos. 60773089, 60533040, and 60725208), 863 Program of China (Grant Nos. 2006AA01Z199 and 2006AA01Z172), Natural Science Foundation of Shanghai Municipality of China (Grant No. 05ZR14081) and Shanghai Pujiang Program (Grant No. 07pj14049).

REFERENCES

- [1] Ming Y.U., Aniket M. and Wei S.U., "An Environment Monitoring System Architecture Based on Sensor Networks", *International Journal of Intelligent Control and Systems*, VOL. 10, No. 3, 2005, pp. 201-209.
- [2] Chao H.Y., Chen Y.Q. and Ren W., "A study of grouping effect on mobile actuator sensor networks for distributed feedback control of diffusion process using central voronoi tessellations", *International Journal of Intelligent Control and Systems*, Vol.11, No.2, 2006, pp. 185-190.
- [3] Akyildiz I.F., Su W., Sankarasubramaniam Y and Cayirci E. "A survey on sensor networks", *IEEE Communications Magazine*, Vol.40, No.8, 2002, pp. 102-114.
- [4] Boukerchea A., Pazzia R. N. and Araujob R. B., "Fault-tolerant wireless sensor network routing protocols for the supervision of context-aware physical environments", *J. Parallel Distrib. Comput.*, Vol. 66, 2006, pp. 586-599.
- [5] Akkaya K. and Younis M., "A survey on routing protocols for wireless sensor networks", *Ad Hoc Networks*, Vol. 3, 2005, pp.325-349.
- [6] Kwon H., Kim TH., Choi S.Y. and Lee B.G., "A Cross-Layer Strategy for Energy-Efficient Reliable Delivery in Wireless Sensor Networks", *IEEE Transactions on Wireless Communications*, Vol.5, No.12, 2006, pp.3689 - 3699.

- [7] Hayoung O., Bahn H. and Chae K.J., "An energy-efficient sensor routing scheme for home automation network", *IEEE Transactions on Consumer Electronics*, Vol.51, No.3, 2005, pp. 836-839.
- [8] Lukachan G., Labrador M.A. and Moreno W., "Scalable and Energy-efficient Routing for Large-scale Wireless Sensor Networks", *Proceedings of the 6th International Caribbean Conference on Devices, Circuits and Systems*, Mexico, Apr. 26-28, 2006, pp.267-272.
- [9] Park, J. and Sahni S., "An online heuristic for maximum lifetime routing in wireless sensor networks", *IEEE Transactions on Computers*, Vol. 55, No. 8, 2006, pp. 1048-1056.
- [10] Madan R. and Lall S., "Distributed algorithms for maximum lifetime routing in wireless sensor networks", *IEEE Transactions on Wireless Communications*, Vol. 5, No. 8, 2006, pp. 2185-2193.
- [11] Ammari H.M. and Das S.K., "Data dissemination to mobile sinks in wireless sensor networks: an information theoretic approach", *Proceedings of IEEE International Conference on Mobile Adhoc and Sensor Systems Conference*, 2005.
- [12] Bruno R., Conti M. and Gregori E., "Mesh Networks: Commodity Multihop Ad Hoc Networks", *IEEE Communications Magazine*, vol. 43, 2005, pp. 123-131.
- [13] Akyildiz I.F., Wang X.D. and Wang W.L., "Wireless mesh networks: a survey", *Computer Networks* 47, 2005, pp. 445 - 487.
- [14] Sereiko P., "Wireless Mesh Sensor Networks Enable Building Owners, Managers, and Contractors to Easily Monitor HVAC Performance Issues", <http://www.automatedbuildings.com/news/jun04/articles/sensicast/Sereiko.htm>.
- [15] Younis O., "HEED: A Hybrid, Energy-Efficient, Distributed Clustering Approach for Ad Hoc Sensor Networks", *IEEE Transactions on Mobile Computing*, vol. 1.3, 2004, pp. 660-669.
- [16] Karlof, C. Li, Y. and J. Polastre, "ARRIVE: An Architecture for Robust Routing in Volatile Environments", University of California at Berkeley, Technical report UCB-CSD-03-1233, 2003.
- [17] Heinzelman R., Chandrakasan A. and Balakrishnan H., "LEACH: Energy-efficient Communication protocol for wireless microsensor networks", *Proceedings of Hawaii International Conference on System sciences*, 2000, pp. 3005-3014.
- [18] Manjeshwar A. and Agrawal D.P., "TEEN: A routing protocol for enhanced efficiency in wireless sensor networks", *Proceedings of the 15th Parallel and Distributed Processing Symposium*, San Francisco: IEEE Computer Society, 2001, pp. 2009-2015.
- [19] Al-Karaki J. N. and Kamal A. E., "Routing Techniques in Wireless Sensor Networks: A Survey," *IEEE Wireless Commun.*, vol. 11, no. 6, Dec. 2004, pp. 6-28.
- [20] Heinzelman W. R., Kulik J. and Balakrishnan H., "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks", *Proc. of ACM MobiCom 99*, Seattle, WA, 1999, pp. 174-185.
- [21] Kulik J., Heinzelman W.R. and Balakrishnan H., "Negotiation-based protocols for disseminating information in wireless sensor networks", *Wireless Networks*, Vol. 8, 2002, pp. 169-185.
- [22] Intanagonwiwat C., Govindan R. and Estrin D., "Directed Diffusion: A scalable and robust communication paradigm for sensor networks", *Proceedings of ACM MobiCom*, 2000, pp. 56-67.
- [23] Braginsky D. and Estrin D., "Rumor Routing Algorithm For Sensor Networks", *Proceedings of ACM MobiCom*, 2002.
- [24] Ye F., Chen A., Liu S., Zhang L., "A scalable solution to minimum cost forwarding in large sensor networks", *Proceedings of the tenth International Conference on Computer Communications and Networks (ICCCN)*, , 2001, pp. 304-309.
- [25] Lindsey S., Raghavendra C., "PEGASIS: Power-Efficient Gathering in Sensor Information Systems", *IEEE Aerospace Conference Proceedings*, Vol. 3, 2002, pp. 1125-1130.
- [26] Xu Y., Heidemann J. and Estrin D., "Geography-informed Energy Conservation for Ad-hoc Routing", *Proceedings of the Seventh Annual ACM/IEEE International Conference on Mobile Computing and Networking*, 2001, pp. 70-84.
- [27] Chen B., Jamieson K., Balakrishnan, H. and Morris R., "SPAN: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks", *Wireless Networks*, Vol. 8, No. 5, Page(s): 481-494, September 2002.
- [28] Wang Y., Attebury G. and Ramamurthy B. "A survey of security issues in wireless sensor networks", *IEEE Communications Surveys & Tutorials*, Vol. 8, No. 2, 2006, pp. 2-23.
- [29] Karlof C. and Wagner D., "Secure routing in wireless sensor networks: attacks and countermeasures", *Ad Hoc Networks* 1, 2003, pp. 293 - 315.
- [30] Deng J., Han R., and Mishra S., "INSENS: Intrusion-Tolerant Routing Wireless Sensor Networks," Department of Computer Science, University of Colorado, Tech. Report CU CS-939-02, Nov. 2002.
- [31] Perrig A., Szewczyk R., Tygar J.D. et al., "SPINS: Security Protocols for Sensor Networks," *Wireless Networks*, vol. 8, no. 5, Sept. 2002, pp.521-34.
- [32] Zhu S., Setia S., Jajodia S., "LEAP: Efficient security mechanisms for large-scale distributed sensor networks", *Proc. of the 10th ACM Conf. on Computer and Communications Security*. New York: ACM Press, 2003, pp. 62-72.
- [33] Sohrabi K., Pottie J., "Protocols for self-organization of a wireless sensor network", *IEEE Personal Communications*, Vol. 7, No.5, 2000, pp. 16-27.
- [34] Gandham S.R., Dawande M., Prakash R. and Venkatesan S., "Energy efficient schemes for wireless sensor networks with multiple mobile base stations", *Proceedings of IEEE GLOBECOM 2003*, December 2003, pp. 377-381.
- [35] Hou Y.T., Shi Y., Pan J.P. and Midkiff S.F., "Maximizing the Lifetime of Wireless Sensor Networks through Optimal Single-Session Flow Routing", *IEEE Transactions on mobile computing*, Vol.5, No.9, 2006, pp. 1255-1266.
- [36] Azad A.P., "Mobile Base Stations Placement and Energy Aware Routing in Wireless Sensor Networks", *Proceedings of IEEE WCNC 2006*, pp. 264-269.
- [37] Perrig A., Stankovic J. and Wagner D., "Security in wireless sensor networks", *Communications of the ACM*, Vol. 47, No. 6, 2004, pp. 53-57.
- [38] Traynor P., Kumar R., Choi H. et al., "Efficient Hybrid Security Mechanisms for Heterogeneous Sensor Networks", *IEEE Transactions on Mobile Computing*, Vol.6, No.6, 2007, pp. 663-677.
- [39] Pietro R.D., Mancini L.V. and Mei A., "Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks", *Wireless Networks*, Vol.12, No.6, 2006, pp. 709 - 721.



Feilong Tang received his Ph.D degree in Computer Science and Technology from Shanghai Jiao Tong University, China. Currently, he works with the Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His research interests focus on Grid and pervasive computing, wireless sensor network, computer network and distributed transaction processing.



Minyi Guo received his Ph.D. degree in computer science from University of Tsukuba, Japan. Before 2000, Dr. Guo had been a research scientist of NEC Corp., Japan. He is now a full professor at the Department of Computer Software, The University of Aizu, Japan. His research interests include parallel and distributed processing, parallelizing compilers, pervasive computing and software engineering. He is a member of the ACM, IEEE, IEEE Computer Society, and IEICE.



Cho-Li Wang received his Ph.D. degrees in Computer Engineering from University of Southern California in 1995. He is currently an associate professor with the Department of Computer Science at The University of Hong Kong. Wang's research mainly focuses on the system software for Pervasive Computing, Cluster/Grid Computing and Wireless Sensor Networks. Dr. Wang serves as an editorial board member of IEEE Transactions on Computers, International Journal of Pervasive Computing and Communications, and Multiagent and Grid Systems.



Minglu Li is a full professor and associate director in Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. Now he also is a director of Grid computing center and Web Services research center of Shanghai Jiao Tong University, Grid expert of Ministry of Education, P.R.China, and expert-in-chief of ShanghaiGrid project. His research interests mainly include Grid computing, Web Services and multimedia computing.



Mianxiong Dong received his B.S. in computer science and engineering from the University of Aizu, Japan, in 2006. He is currently a graduate student at school of Computer and Engineering, the University of Aizu, Japan. His research interests include pervasive computing, sensor network and e-learning.