A New Secure Geographical Routing Protocol Based on Location Pairwise Keys in Wireless Sensor Networks

Haixia Zhao[1], Yaowei Li[2], Jincheng Shen[3], Mingchuan Zhang[1], Ruijuan Zheng[1], Qingtao Wu[1]

[1]Electronic & Information Engineering college, Henan University of Science and Technology, LuoYang, 471003, P.R. China

[2]LuoYang Electronic Information Equipment Testing Center. China, LuoYang, 471003, P.R. China

[3]Meteorological Bureau of Xinyang, Xinyang City, Henan Province, 464000, China

Abstract

Geographical and Energy Aware Routing (GEAR) is an efficient routing protocol in wireless sensor networks (WSN). It behaves well in the face of routing attacks, but it is incapable of defending bogus routing information, sybil attack and selective forwarding. Aimed at this problem, this paper present a location pairwise keys bootstrap scheme based secure geographical and energy aware routing protocol (SGEAR). SGEAR adapted to WSN very well. Then we give the performance analyses of SGEAR. Our performance analyses show that our scheme is efficient to defend above-mentioned attacks.

Keywords: *WSN; attack; secure bootstrap model; GEAR; SGEAR.*

1. Introduction

Wireless sensor networks (WSNs) are composed of a large number of densely deployed sensors. A key feature of such networks is that their nodes are unattended. Consequently, energy efficiency is an important design consideration for these networks. Routing technology is the core technology of the wireless sensor network communication layer. Geographic and Energy Aware Routing (GEAR)[1] algorithm uses energy aware and geographically informed neighbor selection heuristics to route a packet towards the target region. Within a region, it uses a recursive geographic forwarding technique to disseminate the packet. The simulation results show that GEAR exhibits noticeably longer network lifetime than non-energy-aware geographic routing algorithms.

In recent years, secure routing of WSNs has become popular research focuses. Since Perrig et al. presented the security routing problem of the wireless sensor networks [2], it has greatly interested the researchers, and large numbers of achievements have been attained, which greatly promoted the evolution of wireless sensor networks. Several techniques were proposed recently to address secure routing in wireless sensor networks, including the feedback information based secure routing protocol [10-11],the Location based secure routing protocol[12,13],the cryptographic algorithms based secure routing protocol[2,14,15,16] and other routing protocols. Those literatures accelerated the development of wireless sensor networks.

In order to improve the Security of GEAR, this paper presents a SGEAR(Secure Geographic and Energy Aware Routing) secure routing protocol, we adopt a novel pairwise key pre-distribution schemes to address the security for static sensor networks. These techniques are based on the observation that in static sensor networks, although it is difficult to precisely pinpoint sensors' positions, it is often possible to approximately determine their locations. For example, when we use trucks to deploy static sensors, we can usually keep sensors within a certain distance (e.g., 100yards) from their target locations, though it is difficult to place the sensors in their expected locations precisely. This paper focuses on the modeling and design of secure routing protocol to find a new research idea. By taking advantage of this observation, our techniques are efficient to defend bogus routing information, sybil attack and selective forwarding attacks.

2. GEAR Routing Protocol and Security Analysis of GEAR

Disseminating information to a geographic region is a very useful primitive in many location-aware systems, and especially sensor networks. An efficient way to disseminate the geographic query to a specified region is to leverage the location knowledge in the query and

to route the query directly to the region instead of flooding it everywhere. GEAR is an improved algorithm of Directed diffusion[3]. The latter is a data-centric protocol for sensor network applications. It achieves some level of energy savings by selecting empirically good paths, and by caching and processing data in-network. However, without proposed geographic routing support, there is initial and periodic interest and low rate data flooding throughout the network. GEAR protocol can compliment this work by efficiently route interest to the destination region, thus conserve more energy.

2.1 GEAR Routing Protocol Overview

GEAR algorithm uses energy aware and geographically informed neighbor selection heuristics to route a packet towards the target region. Within a region, it uses a recursive geographic forwarding technique to disseminate the packet.

The main idea of GEAR is using the location information. The process of forwarding a packet to all the nodes in the target region consists of two phases:

1. Forwarding the packets towards the target region:

GEAR uses a geographical and energy aware neighbor selection heuristic to route the packet towards the target region. There are two cases to consider:

(a) When a closer neighbor to the destination exists: GEAR picks a next-hop node among all neighbors that are closer to the destination.

(b) When all neighbors are further away: In this case, there is a hole. GEAR algorithm picks a next-hop node that minimizes some cost value of this neighbor.

2. Disseminating the packet within the region:

Under most conditions, GEAR algorithm uses a Recursive Geographic Forwarding algorithm to disseminate the packet within the region. However, under some low density conditions, recursive geographic forwarding sometimes does not terminate, routing uselessly around an empty target region before the packet's hop-count exceeds some bound. In these cases, GEAR algorithm proposes to use restricted flooding.

2.2 Security Analysis of GEAR

Chris Karlof al.[3] pointed out the security threats of sensor network routing protocol. These threats include bogus routing information, selective forwarding, Sinkhole attacks, Sybil attacks, Wormholes attacks, and HELLO flood attacks. The security defense capability of the GEAR routing protocol against the aboved attacks will discuss as below.

(1) bogus routing information. GEAR routing protocol can't resist this attack, because the path of the GEAR protocol establishing process from sink node use greedy algorithm, the attacker can forge their own positions and energy information, resulting in routing is not optimal.

(2) selective forwarding. Malicious nodes can be malicious discarded the received packets, most of the proposed routing protocol can not resist such attacks, GEAR routing is no exception, as long as malicious nodes exist, there may be selective forwarding.

(3) Sinkhole attacks. In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Because nodes on, or near, the path that packets follow have many opportunities to tamper with application data, sinkhole attacks can enable many other attacks (selective forwarding, for example). The GEAR routing protocol able to withstand such an attack, because routing selection relate to location information, the attacker need to declare that their own position.

(4) Sybil attacks. In a Sybil attack, a single node presents multiple identities to other nodes in the network. Sybil attacks also pose a significant threat to GEAR routing protocols. Location aware routing often requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. It is only reasonable to expect a node to accept but a single set of coordinates from each of its neighbors, but by using the Sybil attack an adversary can "be in more than one place at once".

(5) Wormholes attacks. Wormholes attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker. Two or more malicious nodes conspiracy through the encapsulation technology, compression the routing, reduce the path length between them, seems to be adjacent node. GEAR routing can resist the attack, because two nodes are neighbors can be through their position information to confirm.

(6) HELLO flood attacks. Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power

could convince every node in the network that the adversary is its direct neighbor. Node in the network will try to forward packets to the attacker, leading to network into confusion. This attack does not work for GEAR, each node in the GEAR know their location information, node neighbor relationship can be judged according to the location information.

The above analysis shows, GEAR protocol can resist Sinkhole attacks, Wormholes attacks, and HELLO flood attacks, but GEAR protocol almost had no effect on bogus routing information, selective forwarding, and Sybil attacks. And you can see, the important problem of the security in geographical routing is that neighbors advertising the position and residual energy information must be credible. In section 3 of the paper, we proposed a novel secure geographical and energy aware routing (SGEAR) algorithm, our goal is to ensure that the algorithm is efficient to defend above-mentioned attacks.

3. Secure Geographical and Energy Aware Routing protocol (SGEAR)

We now describe SGEAR algorithm. As mentioned in section 3, we are interested in ensure that the security of the sensor network.

3.1 Location Pairwise Keys Based Safety Bootstrap Scheme

The security bootstrap refers to the process for a sensor network to form a network with solid security outer protection gradually from a pile of scattered nodes without safe passages protection through some shared knowledge and agreement. The core issue of secure bootstrap is the establishment of security key process. Generally considered that the key pre-distribution model complete most of the establishment of the security infrastructure before deployment, just a very simple protocol for consultations after deployment process, and thus suitable for sensor network security guide.

A fundamental security service is the establishment of a symmetric, pairwise key shared between two sensors, which is the basis of other security services such as encryption and authentication. Several key pre-distribution techniques have been developed recently to address this problem. Key pre-distribution model mainly contains the pre-shared key model and the random key pre-distribution model. SPINS [2] uses a pre-shared key model, each ordinary node and the base station share a pair of master key. Its implementation is simple, guide the high success rate, drawback is that over-reliance on the base station, and can not resist the DoS attack in multi-hop network environment. Eschenauer and Gligor [6] proposed the basic probabilistic key pre-distribution, in which each sensor is assigned a random subset of keys from a key pool before the deployment of the network. Several techniques were proposed recently to address pairwise key establishments in wireless sensor networks [5,6], including the basic probabilistic key pre-distribution[6], the q-composite key predistribution [5] and the random pairwise keys scheme [5].Among them, the random pairwise keys model has good performance: (1) provide the best node restoring force of capture: each pairwise key is the only, Any node that is captured reveals no information about links that it is not directly involved in. (2) in the same memory capacity, random pairwise key can support more large-scale network.

Liu D G et al. [7] use the node position information to improve the performance of the pairwise key pre-distribution, and present several techniques for establishing pairwise keys in static sensor networks. Inspired by this idea, we propose the SGEAR security routing protocol.

3.2 Design of the SGEAR Security Routing Protocol

Use position information, node deployment requires a setup server. To pre-distribute pairwise keys, the setup server randomly generates a bivariate t-degree polynomial f(x,y)over a finite field Fq, where q is a prime number that is large enough to accommodate a cryptographic key, such that it has the property of f(x,y) = f(y,x). It is assumed that each sensor has a unique ID. For each sensor i, the setup server computes a polynomial share of f(x,y), f(i,y). For any two sensor nodes i and j, node i can compute the common key f(i,j) by evaluating f(i,y) at point j, and node j can compute the same key f(j,i) = f(i,j) by evaluating f(j,y) at point i. The security proof in [8] ensures that the collusion of no more than t compromised sensor nodes knows nothing about the direct key between any two non-compromised nodes.

In this approach, we partition the target field into small areas called cells, each of which is associated with a unique random bivariate polynomial. For simplicity, we assume the target field is a rectangle area that can be partitioned into equal-sized squares.

Partitions the target field into equal sized squares $\{C_{i_r,i_c}\}_{i_r=0,1,...,R-1,i_c=0,1,...,C-1}$, each of which is a cell with the coordinate (i_r,i_c) denoting row i_r and column i_c. For convenience, we use s = R ×C to denote the total number of cells. The setup server randomly generates s bivariate t-degree polynomials $\{f_{i_r,i_c}(x,y)\}_{i_r=0,1,...,R-1,i_c=0,1,...,C-1}$, and assigns

$f_{i_r,i_c}(x,y)$ to cell C_{i_r,i_c} . Figure 1 shows an example partition of a target field. For each sensor, the setup server first determines its home cell, in which the sensor is expected to locate. The setup server then discovers four cells adjacent to the sensor's home cell. Finally, the setup server distributes to the sensor its home cell coordinate and the polynomial shares of the polynomials for its home cell and the four selected cells. For example, in Figure 1, sensor u is expected to be deployed in cell $C_{2,2}$. Obviously, cell $C_{2,2}$ is its home cell, and cell $C_{1,2}$, $C_{2,1}$, $C_{2,3}$ and $C_{3,2}$ are the four cells adjacent to its home cell. Thus, the setup server gives this sensor the coordinate (2,2) and the polynomial shares $f_{2,2}(u,y)$, $f_{1,2}(u,y)$, $f_{2,1}(u,y)$, $f_{2,3}(u,y)$, and $f_{3,2}(u,y)$.

The main idea of the SGEAR secure routing protocol is a combination location-based pairwise keys bootstrap scheme and location-based routing protocol GEAR, and using the multi-path makes the protocol can resist more routing attack type.

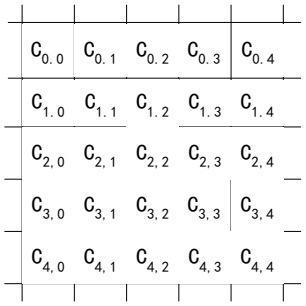

Fig. 1 Partition of a target field

3.2.1 Notation

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

A, B are principals, such as communicating nodes

pos_A denotes Position information of the node A

$M_1 | M_2$ denotes the concatenation of messages and maintain order

K_{AB} denotes the secret (symmetric) key which is shared between A and B

$\{M\}_{K_{AB}}$ is the encryption of message M with the symmetric key shared by A and B.

$\{M\}(K_{AB},IV)$ idenotes the encryption of message M, with key K_{AB}, and the initialization vector IV which is used in encryption modes such as cipher-block chaining (CBC), output feedback mode (OFB), or counter mode (CTR).

3.2.2 Adjacent Nodes Exchange Position and Energy Information

In GEAR routing protocol, each node knows their location and residual energy information. Node obtains location and energy information of neighbor node through a simple exchange mechanism. Nodes need share keys to ensure the security of the message. Below we give a detailed description of the establishment of pairwise key according to the method mentioned in section 3.2.

Direct Key Establishment. After deployment, if two sensors want to setup a pairwise key, they first need to identify a shared bivariate polynomial. If they can find at least one such polynomial, a common pairwise key can be established directly using the basic polynomial-based key pre-distribution presented in section 3.1 A simple way is to let one of them (called source node) disclose its home cell coordinate to the other node (called destination node). From the coordinate of the home cell of the source node, the destination node can immediately determine the set of polynomial shares the source node has. To protect this coordinate information, the source node may challenge the destination node to solve puzzles. For example, using the method in [6], the source node may send an encryption list, α,EKv(α), v = 1,...,5, where Kv is a potential pairwise key the other node may have. If the destination node can correctly decrypt one of them, it can establish a pairwise key with the the requesting node and thus send a short reply message to identify the common shared key.

Indirect Key Establishment. After deployment, if two neighbor sensors u and v do not share a pre-distributed pairwise key, they may find an intermediate neighbor sensor that shares pairwise keys with both of them to help establish a session key. Basically, either of these two sensors may broadcast a request message with their IDs. Without loss of generality, we assume u sends this request. Suppose sensor i receives this request, and i shares a pairwise key $f_1(i,u)$ with u, and a pairwise key $f_2(i,v)$ with v. Sensor i then generates a random session key k and sends a message back to u, which contains $E_{f_1(i,u)}(k)$ and $E_{f_2(v,i)}(k)$. These are the session key k encrypted with $f_1(i,u)$ and $f_2(i,v)$ respectively. Upon receiving this reply message, sensor u can get the session key by decrypting $E_{f_1(i,u)}(k)$,and inform sensor v by forwarding $E_{f_2(v,i)}(k)$ to v. Thus node u and v can establish a Shared key.

After established a pairwise key between adjacent nodes, we can get the location and energy information of the neighbor nodes through a simple exchange mechanism. Node u as an example, assuming that the position coordinate of node u is (i_r, i_c), residual energy information of node u is $e(u)$, Node u send an encrypted message to its neighbor node v, encryption formula is as follows:

$$E = \{u, (i_r, i_c), e(u)\}_{K_{enc}}$$

Where E represents the encrypted location and energy information, and u is the node ID, and k_{enc} is the encryption key, if node u and v has a direct key, k_{enc} can be $f_{i_r, i_c}(u, v)$, if node u and v are indirectly established key, k_{enc} is the key k, which get through the consultation of intermediate nodes. Neighbor node v receives the message, then use of a shared key to decrypt the message and reply to the above form of the same message to the node. Reply message format is as follows.

$$E_{reply} = \{v, (i_r', i_c'), e(v)\}_{K_{enc}}$$

Where E_{reply} is the encrypted location and energy information of the node v replies, and v is the node ID, (i_r', i_c') is the location coordinates of node v, $e(v)$ is the energy information of node v. In this way, node u gets location and residual energy information of its neighbors.

3.2.3 Query Message to the Target Area

Sink node sent a unicast packet to its nearest neighbor away from the target region, this packet is encrypted by the shared pairwise key and contains source location, the target region and message authentication code (MAC). Only the neighbor who has the same shared pairwise key with sink node can decrypt the message. The Sink node's neighbor decrypt the message, add their own location information, encrypt the message using the shared pairwise key, and sent to their neighbor close to the destination node, in turn, according to the greedy algorithm to proceed. The encrypted data has the following format: $E = \{D\}_{(K_{encr}, C)}$, where D is the data, the encryption key is K_{encr}, and the counter is C. The MAC is $M = MAC(K_{mac}, c \mid E)$. the complete message that A sends to B is:

$$A -> B: \{D\}_{(K_{encr}, C)}, MAC(K_{mac}, C \mid \{D\}_{(K_{encr}, C)})$$

Now we assume that the path is $S \to A \to B \to \ldots \to D$, we add the location information in the data, the complete message that S sends to D is:

$$S \to A: \{M \mid pos_S \mid pos_D\}_{(K_{SA}, C)}, \\ MAC(K_{SA}', C \mid \{M \mid pos_S \mid pos_D\}_{(K_{SA}, C)})$$

$$A \to B: \{M \mid pos_S \mid pos_D \mid pos_A\}_{(K_{AB}, C)}, \\ MAC(K_{AB}', c \mid \{M \mid pos_S \mid pos_D \mid pos_A\}_{(K_{AB}, C)}) \ldots\ldots$$

Now we analyze the communication process. Node A receiving the message from node S, decrypts the message with shared key K_{SA}, determines the location of next hop node; while node A calculates the authentication code with both shared another key K_{SA}' to certify the authenticity of the message originator. If two nodes only one shared key, K_{SA}' can be deduced from K_{SA} by the preset one-way hash function. Node B receiving the message from node A, decrypts the message with shared key K_{AB}, determines the location of next hop node, and certifies the authenticity of the message originator with key K_{AB}'. Continue until it reaches the destination node D. Node in the forward query message to add their own location information will help prevent malicious nodes giving the wrong location information, because the location information related to the pairwise keys, after decryption, if the location does not match with the pairwise keys, you know that is the behavior of malicious nodes.

3.2.4 Query Message Spread in Target Area

Under most conditions, GEAR algorithm uses a recursive geographic forwarding algorithm to disseminate the packet within the region. However, under some low density conditions, recursive geographic forwarding sometimes does not terminate, routing uselessly around an empty target region before the packet's hop-count exceeds some bound. In these cases, GEAR algorithm proposes to use restricted flooding.

In the case of large node density, GEAR algorithm uses a recursive geographic forwarding mechanism, many nodes in the same region often collect the similar data, we improved GEAR algorithm, our algorithm have the necessary data fusion, which can reduce the transmission of packets of the redundant data. Each recursive center node can be used as a data fusion node. After processed the data collected by the node in the subregion, data fusion node sends the fusion message to the reverse paths. The node which receives the query message first in the target region will send the fusion

data to the sink node along the reverse path. In the recursive geographic forwarding process, we choose unicast scheme to send query message to the center node of the subregion, where secure communication is similar to the above mentioned. If a node receives a message that can not be certified, and then discarded.

In the case of less node in the region, flooding protocol uses broadcast mode, our algorithm need to solve the problem of broadcast packets authentication. A better method is to adopt the μTESLA protocol[2]. We give a brief overview of μTESLA. is a protocol for efficient, authenticated broadcast and flooding that uses only symmetric key cryptography and requires minimal packet overhead. μTESLA achieves the asymmetry necessary for authenticated broadcast and flooding by using delayed key disclosure and one-way key chains constructed with a publicly computable cryptographically secure hash function. Replay is prevented because messages authenticated with previously disclosed keys are ignored. μTESLA also requires loose time synchronization. For simplicity, we consider only in the target region broadcast packets, and the deployment of the node key uses location based pairwise key. If the node and its neighbor have direct key, they will be sharing the polynomial share assigned by their main unit, so node can use this sharing key authentication of broadcast packets. If the node and its neighbor share indirect key, they can consultation main unit polynomial share for sharing key.

3.2.5 Multipath Establish

The reliability of the system can be increased by providing several paths from source to destination and sending the same packet through each of them through each of them. We adopt muiti-path to strengthen the routing security. In data forwarding stage, a query message will send to several paths, or use the method proposed by dulman S et al. [9], The data packet is split in k subpackets (k = number of disjoined paths from source to destination). If only Ek subpackets (Ek< k) are necessary to rebuild the original data packet (condition obtained by adding redundancy to each subpacket), then the trade-off between traffic and reliability can be controlled. The proposed scheme is useful for delivering data in unreliable environments. The advantage of this method is not to need to expand routing protocol, but the specific performance and implementation mechanism needs further research.

4. Performance Analysis of SGEAR Protocol

In this paper, we develop a new algorithm to address the security threats for static sensor networks. The goal of SGEAR is to ensure that the algorithm is efficient to defend bogus routing information, selective forwarding, and Sybil attacks in addition to Sinkhole attacks, Wormholes attacks, and HELLO flood attacks. In this subsection, we give a detailed analysis of the security and the overheads of SGEAR.

4.1 Security Analysis

(1) The Sybil attack

An effective method to resist sybil attack is location confirmation. SGEAR security routing uses a location pairwise keys bootstrap scheme based on the location and polynomial. Because the node authentication key is related to location, and the polynomial share in the node is related to node ID, a node which want to declare multiple identities must have polynomial share of the location, otherwise it can't through the authentication. As seen in Figure 1, assume that compromised node u at actual location (2,2) forges location advertisements for non-existent nodes V at location (1,2) as well as advertising her own location, it must have a polynomial share $f_{1,2}(v,y)$, but in fact it is stored $f_{2,2}(u,y)$, $f_{1,2}(u,y)$, $f_{2,1}(u,y)$, $f_{2,3}(u,y)$ and $f_{3,2}(u,y)$,pay attention to $f_{1,2}(v,y)$ and $f_{1,2}(u,y)$ is different. So SGEAR can effectively defense sybil attacks.

(2) bogus routing information

Node's location information is related to pairwise key, so that nodes can not arbitrarily declare a false location, otherwise it will not be certified and will to be discarded; in addition, we can effectively identify the malicious node by comparing two recent energy. Thus it is efficient to avoid the bogus location and energy information.

(3) selective forwarding

Multipath routing can be used to counter these types of selective forwarding attacks. Messages routed over n paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most n compromised nodes and still offer some probabilistic protection when over n nodes are compromised. The use of multiple braided paths may provide probabilistic protection against selective forwarding and use only localized information. Allowing nodes to dynamically choose a packet's next hop probabilistically from a set of possible candidates can further reduce the chances of an adversary gaining complete control of a data flow. We proposed a multipath structure method which is simple and easy to implement.

4.2 Overheads Analysis

Finally we examine the overheads of security mechanisms. Most of the overheads will come from extra transmissions required by the protocols. Key pre-distribution stage, each sensor needs to store the coordinate of its home cell and the polynomial shares of five cells. The storage overhead for the coordinate of its home cell is negligible. Thus, each sensor has to allocate 5(t + 1)logq memory space to store the secret. When there are compromised sensors, each non-compromised sensor also needs to store the IDs of the compromised sensors with which it shares at least one polynomial. However, for each of the 5 polynomials, a non-compromised sensor only needs to store up to t IDs; it can remove the corresponding polynomial share and all the related IDs if the number of compromised sensors with which it shares the polynomial exceeds t. To establish a common key between two neighbor nodes, the communication overhead includes sending a request message and a reply message. To compute the common key with a given sensor, each sensor node needs to evaluate a t-degree polynomial. Thus, the computational cost in each sensor mainly comes from the evaluation of this polynomial, which requires t modular multiplication and t modular addition.

5. Conclusion

The contribution of this paper is three-fold. First, we present the detailed security analysis of GEAR routing protocol for sensor networks. Then, we proposed a new secure geographical routing protocol based on a location pairwise keys bootstrap scheme. Finally, we present a analysis of the security and the overheads of SGEAR, which illustrates those novel designs can obtain a higher security in the smaller system overhead. SGEAR is suitable for wireless sensor network.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China (NSFC) under Grant No. U1204614, No. 61003035 and No. 61142002, and in part by the Plan for Scientific Innovation Talent of Henan Province under Grant No. 124100510006, and in part by the Science and Technology Development Programs of Henan Province under Grant No. 112102210187, and in part by the Youth Foundation of Henan University of Science and Technology under Grant No. 2011QN51.

References

[1] Yu Y, Govindan R, Estrin D. Geographical and Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks [R].UCLA Computer Science Department Technical Report, UCLA-CSD TR-01-0023, May 2001.

[2] Perrig A, Szewczyk R, Wen V,et al. Spins: Security protocols for sensor networks [C]. In: Proceedings of Seventh Annual International Conference on Mobile Computing and Networks, July 2001.

[3] Karlof C, Wagner D. Secure routing in wireless sensor networks: Attacks and countermeasures [J]. In First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[4] Intanagonwiwat C, Govindan R, Estrin D. Directed diffusion: a scalable and robust communication paradigm for sensor networks [A]. In: Proceedings of ACM MobiCom '00[C]. Boston: MA, 2000.56-67.

[5] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In IEEE Symposium on Research in Security and Privacy, 2003.

[6] Eschenauer L,Gligor V.D. A key-management scheme for distributed sensor networks [C]. In Proceedings of the 9th ACM Conference on Computer and Communications Security. November 2002. 41–47.

[7] Liu D G, Ning P. Location-based pairwise key establishments for static sensor networks[C].in Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (CCS'03), 2003.72 –82.

[8] Blundo C, et al. Perfectly-secure key distribution for dynamic conferences [J]. In Advances in Cryptology – CRYPTO '92, LNCS 740, 1993: 471–486.

[9] Dulman S, Nieberg T, Wu J. Trade-Off between Traffic Overhead and Reliability in Multipath Routing for Wireless Sensor Networks [C]. WCNC Workshop, New Orleans, Louisiana, USA, March 2003.

[10] CAO Zhen, HU Jian bin, CHEN Zhang, et al. FBSR: feedback basedSecure routing protocol for wireless sensor networks (C). Proc of the 20th IEEE International Conference of Advanced Networking and ApPlications. (S. L.): IEEE Press, 2006:160-164

[11] GALUBA W, PAPADIMITRATOS P, POTURALSKI M, et al. Castor:Scalable secure routing for Ad hoc networks (C) . Proc of IEEE IN FOCOM. Washington DC: IEEE Computer Society, 2010:1-9

[12] LI Yun, REN Jian. Source location privacy through dynamic routing in Wireless sensor networks (C). Proc of the 29th Conference on InforMation Communications. Piscataway: IEEE Press, 2010:1- 9

[13] DEFRAWY K E, TSUDIK G. Privacy preserving location based on Demand routing in MANETs (J). IEEE Journal on Selected Areas.In Communications, 2011, 29 (10):1926- 1934

[14] MISRA S, ROY S, OBAIDAT M D, et al. A fuzzy logic based energy Efficient packet loss preventive routing protocol (C).Proc of the 12th International Symposium on Performance Evaluation of Computer & elecommunication System. Piscataway: IEEE Press, 2009:185-92

[15] ANDEREGG L, EIDENBENZ S. Ad hoc VCG: a truthful and cost efficient routing protocol for mobile Ad hoc networks with selfish agents(C) .Proc of the 9th Annual International Conference on Mobile Computing and Networking. New York: ACM Press, 2003:245-259

[16] HU Y, PERRIG A, JOHNSON D B. Ariadne: a secure on demand Routing protocol for Ad hoc networks (J). Wireless Networks, 2005, 11(1 - 2):21-38

Haixia Zhao received her B.S. degree from South West Normal University in 1998 and M.S degree from National University of Defense Technology in 2005. She works as a Lecturer in Henan University of Science and Technology from 1998 to now. In particular, her research interests include wireless sensor networks, Internet of Things, cognitive network, database theory and technology etc.

Yaowei Li received his B.S. degree from National University of Defense Technology in 1998 and M.S degree from National University of Defense Technology in 2004. He works as a Engineer in LuoYang Electronic Information Equipment Testing Center from 1998 to now. In particular, his research interests include Information security, Internet of Things, cognitive network etc.

Mingchuan Zhang received his B.S. degree from Luoyang Institute of Technology in 2000 and M.S degree from Harbin Engineering University in 2005. He works as a Lecturer in Henan University of Science and Technology from 2005 to now. In particular, his research interests include ad hoc network, Internet of Things, cognitive network and future Internet technology.

Ruijuan Zheng received her B.S. degree from Henan University in 2003, studied in Harbin Engineering University from 2003 to 2008, and received Ph.D. degree. She works as an Associate Professor in Henan University of Science and Technology from 2008 to now. In particular, her research interests include bio-inspired networks, Internet of Things, future Internet and computer security.

Qingtao Wu received his Ph.D. degree from East China University of Science and Technology. He works as an Associate Professor in Henan University of Science and Technology from Mar 2006 to now. His research interests include component technology and future Internet security.