A Novel Bio-inspired Trusted Routing Protocol for Mobile Wireless Sensor Networks

Mingchuan Zhang[1,2], Changqiao Xu[1,3,4], Jianfeng Guan[1,4], Ruijuan Zheng[2], Qingtao wu[2], and Hongke Zhang[1,4]

[1] State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] Information Engineering College, Henan University of Science and Technology, Luoyang 471023, China
[3] Institute of Sensing Technology and Business, Beijing University of Posts and Telecommunications, Wuxi 214135, China
[4] National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University, Beijing 100876, China
[e-mail: {zmc, cqxu, jfguan, hkzhang}@bupt.edu.cn, rjwo@163.com, wqt8921@126.com]
*Corresponding author: Mingchuan Zhang

Received August 29, 2013; revised November 11, 2013; revised December 18, 2013; accepted December 22, 2013; published January 29, 2014

Abstract

Routing in mobile wireless sensor networks (MWSNs) is an extremely challenging issue due to the features of MWSNs. In this paper, we present a novel bio-inspired trusted routing protocol (B-iTRP) based on artificial immune system (AIS), ant colony optimization (ACO) and Physarum optimization (PO). For trust mechanism, B-iTRP monitors neighbors' behavior in real time and then assesses neighbors' trusts based on AIS. For routing strategy, each node proactively finds routes to the *Sink* based on ACO. When a backward ant is on the way to return source, it senses the energy residual and trust value of each node on the discovered route, and calculates the link trust and link energy of the route. Moreover, B-iTRP also assesses the availability of route based on PO to maintain the route table. Simulation results show how B-iTRP can achieve the effective performance compared to existing state-of-the-art algorithms.

Keywords: Bio-inspired, Trusted Routing, Artificial Immune System, MWSNs

http://dx.doi.org/10.3837/tiis.2014.01.005

1. Introduction

Mobile wireless sensor networks (MWSNs) are autonomous wireless communication networks and ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire [1]. Due to the features of MWSNs, e.g. sensor nodes' mobility and failures, limited bandwidth and power energy, routing algorithms need to handle dynamical changes of network topology, extra overhead, energy saving and other requirements. Therefore, routing in MWSNs is an extremely interesting and challenging issue, where two questions are needed to be considered mainly.

The first question is how to guarantee the trust of the multi-hop route. Traditional MWSNs routing protocols assume that all sensor nodes work in a benevolent manner which may render the MWSNs vulnerable to malicious attacks in case of the presence of selfish and malicious nodes. Routing protocols, data, battery power and bandwidth are the common targets of these attacks. Scientific researches prove that forward selfish behavior will affect seriously the network performance—just only a small number of ***selfish*** nodes (10%-40%) will lead to a significant decrease (16%-32%) of network performance [2]. Since the safety of multi-hop communication depends on the reliability of nodes on the route to destination primarily, it is important for routing protocols to know the reliability of the nodes forming the routes. The other question is how to guarantee the energy and efficiency of the multi-hop routes since both are important to prolong lifetime of MWSNs. Generally, there is a tradeoff between routing efficiency and energy equilibrium for MWSNs. The appropriate strategy for the tradeoff will prolong lifetime of MWSNs greatly. Therefore, trust, energy and efficiency are the significant features for routing in MWSNs.

Recently years, a great number of research results on the trust, energy and efficiency of routing protocols have been proposed. In order to solve the trust of routing protocol, many techniques (e.g. trust value, detection, cryptography and data hiding) are proposed based on different applications [1-7]. The measures of efficiency and energy are a pair of conflicting indexes and their tradeoff is needed in most cases, where some methods (e.g. location-aware, energy-aware, energy harvesting and their combination) are discussed [8-14]. In addition, bio-inspired methods [15, 17-23] have been shown to be a good technique for solving the problems regardless of trust, efficiency and energy of routing protocols.

In this paper, we propose a novel bio-inspired trusted routing protocol (B-iTRP) in comprehensive thought of trust, energy and efficiency. B-iTRP consists of trust mechanism and routing strategy. For trust mechanism, B-iTRP assesses nodes' trust value based on artificial immune system (AIS) through monitoring nodes' behavior in real time. For routing strategy, B-iTRP proactively finds routes to the *Sink* based on ant colony optimization (ACO) by introducing cross-layer [25], assesses the discovered routes based on Physarum optimization (PO), and optimizes the local routes during the course of communication session. The main contributions of our B-iTRP lie in:

- Introducing AIS into B-iTRP to assess the trust of neighbors which is an important parameter for trusted routing strategy.
- Improving ACO by introducing cross-layer to sense the link energy and link trust during the course of path-finding.
- Combing PO with MWSNs to assess the discovered route and optimize the local routing during the course of communication session.

In fact, B-iTRP is devoted to combing the advantages of AIS, ACO and PO (i.e. abnormal behavior recognition of AIS, path-finding of ACO and path-optimization of PO) to improve the routing performance, which is verified by simulation results. The rest of this paper is organized as follows. Section 2 gives a brief description of related work. Section 3 presents an overview for the B-iTRP system. Section 4 details the B-iTRP protocol. Section 5 evaluates our B-iTRP by simulations. Finally, the conclusion is presented in section 6.

2. Related Work

Trust is a significant index for WSNs' routing and has been considered by some researchers. Bao *et al.* [3] propose a highly scalable trust-based geographic routing protocol (TGRP) for WSNs to effectively deal with selfish or malicious nodes. Zhan *et al.* [1] design and implement the TARF, a robust trust-aware routing framework for dynamic WSNs, which provides trustworthy and energy-efficient routes. Xia *et al.* [4] present a dynamic trust prediction model to evaluate the trustworthiness of nodes based on the nodes' historical behaviors, as well as the future behaviors via extended fuzzy logic rules prediction. Some researchers use AIS to solve trust problem in wireless networks [5], where the researches are centered on four major AIS algorithms—negative selection algorithms, artificial immune networks, clonal selection algorithms, and danger theory and dendritic cell algorithms. Dal *et al.* [6] apply AIS along with genetic algorithm to develop an intrusion detection system, which can acquire reliable, robust and quick responding for intrusion attack. Yang *et al.* [7] propose a collaborative RFID intrusion detection method based on AIS, which can enhance the trust of RFID systems without need to amend the existing technical standards of RFID and achieve the detection rate 98% and 93% on known and unknown types of attacks, respectively. Based on those researches, it will become a new focus for assessing mobile nodes trust using AIS.

Energy and efficiency are two important parameters for routing protocol in MWSNs. Rao *et al.* [8] present a battery aware distributed clustering and routing protocol which incorporates the state of the battery's remaining charge and health parameters in computing the charge utility metric at each cluster formation round. By allowing the battery to rest for certain duration, without being subjected to heavy loads, Chau *et al.* [9] consider a portion of the lost charge can be recovered due to the battery's recovery effect and present a battery model. Yang *et al.* [10] propose sleeping multi-path routing, which selects the minimum number of disjoint paths to achieve the trade-off of given reliability requirement and energy efficiency. Kuhn *et al.* [11] utilize face (or perimeter) routing to go around voids in the topology. Trajcevski *et al.* [12] present heuristic approaches to relieve some of the routing load of the boundary nodes of energy holes in location-aware WSNs. The approaches propose some of the routes that would otherwise need to bypass the hole along the boundary, should start to deviate from their original path further from the hole instead. Chen *et al.* [13] present a method to enhance the efficiency of gathering sensor data based on a quadrotor-based mobile *Sink*. The method can get perfect transmission delay and packet loss rate by constraining the features of the mobile *Sink*, e.g. trajectory, velocity, and height. Therefore, the tradeoff of some features is researched by many researchers recently [10, 14], and how to balance the energy and efficiency for MWSNs routing should be considered further.

Bio-inspired methods have gained widely attentions by researchers for their advantages to solve path-finding, path-optimization and abnormal behavior recognition problems. Günes *et al.* [15] present an on-demand routing algorithm ARA based on ACO meta heuristic and AODV [16]. Caro *et al.* [17] propose a hybrid routing algorithm AntHocNet, where artificial ants reactively set up multiple routes on demand and proactively test existing paths and

explore new paths during the course of communication session. Wang *et al.* [18] present a hybrid routing algorithm HOPNET based on ACO, where each node sends out forward ants to proactively maintain its zone route table as well as reactively finding routes to destinations beyond its zone. Nakagaki *et al.* [19] build a maze, cover it with pieces of Physarum and then feed the Physarum with oatmeal at two locations. A few hours later, the Physarum retracts to a single tube that follows the shortest path connecting the food sources in the maze. Tero *et al.* [20] propose a mathematical model for the adaptive behavior of Physarum. Li *et al.* [21] present a routing protocol for wireless sensor networks based on PO. We study the foraging rule of Physarum and present a Physarum-inspired routing protocol for WSNs [22-23].

In this paper, we integrate the advantages of AIS, ACO and PO to design a trusted routing protocol based on our prior works [22-25], i.e. B-TRP recognizes neighbors' behavior based on AIS to assess their trusts, finds paths to the *Sink* based on ACO, assesses the discovered routes based on PO to maintain the route table.

3. B-iTRP System Design Overview

This paper considers large multi-hop MWSNs whose nodes are distributed randomly in a two-dimensional space. We assume that 1) each node has a single channel, 2) the interference range R is equal to the transmission range, 3) all communication links are bidirectional, and 4) each node is aware of its own energy residue. An example of MWSNs' topology is shown in Fig. 1.

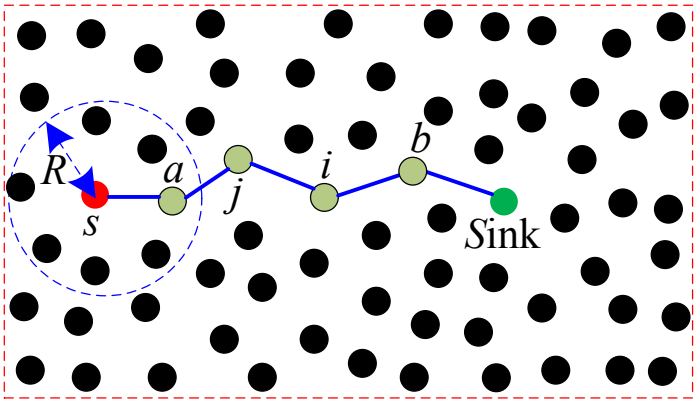


Fig. 1. An example of MWSNs' topology

Based on the assumptions, Fig. 2 illustrates the design of the proposed B-iTRP architecture which consists of trust assessment and routing strategy.

For trust assessment, each node monitors its neighbors' behavior in real time to get the behavior characterization (antigen gene) and the result (antigen assessment) caused by the behavior. Based on the behavior characterization and antibody base, B-iTRP assesses trusts of neighbors using AIS, i.e. the trust of corresponding neighbor is added by a different positive, negative or zero value according to the behavior's weight saved in antibody base. In addition, antibody achieves its own evolution according to the behavior result. What is more, the corresponding antibody generated by a new behavior will be inserted in antibody base. In most cases, the trust consists of two sections—direct trust and indirect trust. Because of considerable traffic load and computing cost, this paper only considers the direct trust.

For routing strategy, ACO and PO are used to find and assess routes, respectively. Each node s sends periodically forward ants to find routes to the *Sink*, where the cross-layer perception [25] is introduced to support route selection. When an ant hops from node i to node j on the way to source, it firstly senses its own energy residual and the trust value with respect to node i. Then, B-iTRP assesses the trust, energy and availability of route $j,i,\cdots$. If the availability value of the route is less than a specific threshold $TH_{A,Lower}$, B-iTRP kills the backward ant and discards the route. Otherwise, the route is inserted in the proper position of the route table of node j according to the availability value. If the availability value of the route is larger than a specific threshold $TH_{A,Upper}$, B-iTRP sets a flag at node j for a certain time to optimize local route when data packets are passing by node j. The process is repeated until the backward ant reaches source. When route failures happen, route maintenance is triggered to recover the route rapidly.

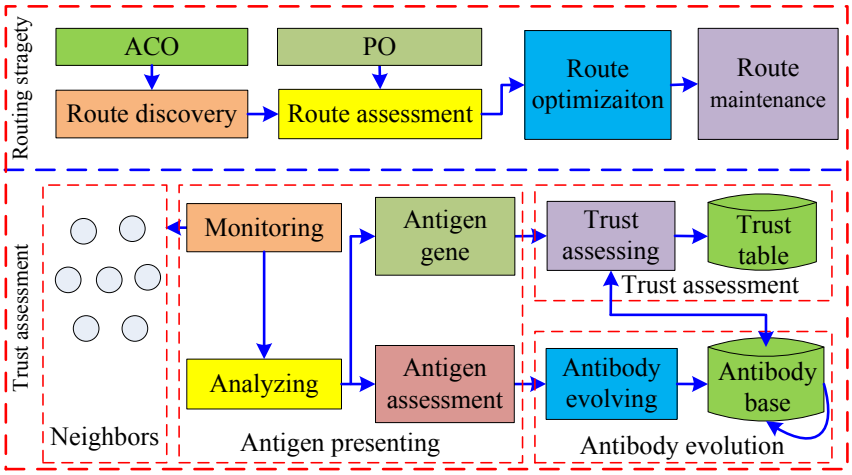


Fig. 2. B-iTRP architecture

4. B-iTRP Protocol

4.1 Trust in B-iTRP

In this section, we propose the trust assessment mechanism based on AIS, which is a very important part of B-iTRP.

4.1.1 Basic Description of AIS

In immunology, antigen is a material which can stimulate organism to produce immune response. In MWSNs, we define antigen is nodes' behaviors (e.g. forwarding, retransmitting and generating packets.), and antigen gene is nodes' behavior characterization. The set of antigens is $Ag = \{x \mid x \text{ is node's behavior in MWSNs}\}$, where antigen may be legal, illegal or uncertain behavior. The set of antigen genes is $AgG = \{y \mid y = \Phi(x), x \in Ag\}$, where $\Phi(\cdot)$ is a processes of antigen presenting (AgP).

In immunology, AgP is the core component of immune response. It processes antigens to make them can be recognized by immunocompetent cell. In MWSNs, we define AgP is two

processes $\Phi(\cdot)$ and $\Psi(\cdot)$ which can draw antigen gene (behavior characterization) and obtain antigen assessment (behavior result), respectively.

In immunology, antibody is a kind of protein which is used to recognize and neutralize foreign substance, e.g. bacteria and virus. In MWSNs, we define antibody is a kind of virtual substance which can recognize node's behaviors. The set of antibodies is expressed as $Ab = \{< gene, age, count, weight > | gene \in AgG, (age, count, weigh\ t) \in N\}$, where $gene$ is antigen gene, age is the age of antibody, $count$ is the times that the antibody has matched antigens, $weight$ is the weight of antibody. Particularly, we give a partition of set Ab is $\{Self, NonSelf, Doubt\}$, where the elements of $Self$ match legal behaviors, the elements of $NonSelf$ match illegal behaviors, and the elements of $Doubt$ match uncertain behaviors.

Finally, we define function $f(\cdot,\cdot)$ to match antibody $x \in Ab$ and antigen $y \in Ag$ as

$$f(x,y) = \begin{cases} x.weight, & \text{if } x.gene = \Phi(y) \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

where $.$ is an operator and $x.weight$ denotes the fourth element (i.e. $weight$) of x.

4.1.2 Antigen Presenting

In B-iTRP, each node monitors its neighbors' behaviors in real time to get corresponding information. Based on this, AgP is achieved through two processes $\Phi(\cdot)$ and $\Psi(\cdot)$.

$\Phi(\cdot)$ can draw antigen gene, which is easy to be achieved by normative description of antigen, e.g. $y = \Phi(x)$, where $x \in Ag, y \in AgG$. That is to say, $\Phi(\cdot)$ is used to recognize neighbors' behaviors. For giving a neighbor id and its behavior, $\Phi(\cdot)$ can output the characterization (also called $gene$) of the behavior. Thus, we can get a two-tuples $< id, gene >$ by $\Phi(\cdot)$, where id is the neighbor's address and $gene$ is the behavior characterization.

Analyzing node's behaviors can show whether the node is selfish, acting like a black hole, carrying out a modification or fabrication attack, inducing latency delays by delaying the retransmission of the packet, etc. Thus, once obtaining a group of complete statistical information by monitoring, $\Psi(\cdot)$ analyzes the obtained information to endow different behaviors with different weights. If the behavior is legal, the weight is positive, and the larger the weight is, the more trusted the behavior is. If the behavior is illegal, the weight is negative, and the larger the absolute value of the weight is, the more untrusted the behavior is. If the behavior is uncertain, the weight is zero.

Therefore, $\Psi(\cdot)$ can acquire the assessment of an antigen, e.g. $y = \Psi(x), x \in Ag, y \in N$. That is to say, $\Psi(\cdot)$ is used to assess neighbors' behaviors. For giving a $gene$, $\Psi(\cdot)$ can output the assessment $weight$ of the antigen. Thus, we can get a two-tuples $< gene, weight >$ by $\Psi(\cdot)$, where $gene$ is the gene of antigen and $weight$ is the evaluating value of the antigen.

4.1.3 Birth and Death Process of Antibody

B-iTRP deals with the variation of antibody set periodically. We assume that the period is 1 and the original status is $\{a_1, a_2, \cdots, a_i \in Ab, i = 1, 2, \cdots\}$.

From $t-1$ to t, the new increased antigen genes are shown as $AgG_{new} = \cup \{\Phi(y_k) | y_k \in Ag, \exists x \in Ab, f(x, y_k) = 0\}$, where y_k denotes the new antigens which

emerge at time k. Accordingly, $Ab_{new} = \{< g, 0, 1, w_{ini} > | g \in AgG_{new}, w_{ini} \in N\}$, where w_{ini} is a constant and denotes the initial weight of antibody genes.

At time t, B-iTRP will kill the antibodies which are shown as $Ab_{dead} = \{x \mid x.age \geq \text{lifecycle}, x.count < TH_{match}\}$, where TH_{match} is a constant. Then, B-iTRP adds 1 to field age for each element in Ab.

Thus, B-iTRP gets the new Ab as

$$Ab_t = \begin{cases} \{a_1, a_2, \cdots & t=0 \\ Ab_{t-1} \cup Ab_{new} - Ab_{dead}, & t \geq 1 \end{cases} \quad (2)$$

4.1.4 Antibody Evolution

A node monitors its neighbors' behavior in real time. Once the node captures a group of complete statistical information, the information is processed by $\Psi(\cdot)$ to output a two-tuples $< gene, weight >$. Then, B-iTRP will trigger an antibody evolution, where $gene$ is the gene of antigen and $weight$ is the assessment of the antigen. Taking node k for example, its antibody evolution is illustrated as follows.

Once the antibody evolution receives a message $< gene, weight >$ from $\Psi(\cdot)$, it will check each element in antibody set Ab of node k. If there is a element whose field $gene$ matches the field $gene$ of the message $< gene, weight >$, the algorithm updates the field $weight$ of the antibody and puts the antibody into different subsets according to its field $weight$. If there is no element whose field $gene$ matches the field $gene$ of the message $< gene, weight >$, the algorithm considers the antibody has not been added in antibody set Ab, and then does nothing. The pseudo code description of the process is shown as Algorithm 1, where w_0, $TH_{W,Lower}$, $TH_{W,Upper}$ are constants.

Algorithm 1: ***Antibody evolution***

```
receiving an item < gene, weight > from AgP;
for each i ∈ Ab do
    if ( i.gene == gene )
        if ( weight != 0 )
            i.weight = i.weight + weight ;
        else
            i.weight = i.weight + w0 ;
        find = TRUE ;
        break;
    end if
end for
if (find)
    if ( i.weight ∈ (−∞, TH_{W,Lower}) )
```

14: put i into *NonSelf* ;
15: **else if** ($i.weight \in (TH_{W,Upper}, +\infty)$)
16: put i into *Self* ;
17: **else**
18: put i into *Doubt* ;
19: **end if**

4.1.5 Trust Assessment

A node monitors its neighbors' behavior in real time. Once the node captures a behavior of one neighbor, the behavior is processed by $\Phi(\cdot)$ to output a two-tuples $< id, gene >$. Then, trust assessment will be triggered by B-iTRP to maintain the trust table, where id is the address of the assessed neighbor and $gene$ is the gene of the antigen. Taking node k for example, its trust assessment is illustrated as follows.

Once the trust assessment receives a message $< id, gene >$ from $\Phi(\cdot)$, firstly, it checks each element in antibody set Ab of node k. If there is a element j whose field $gene$ matches the field $gene$ of the message $< id, gene >$, the algorithm will get a value $weight$ and add 1 to the field $count$ of element j. If there is no element whose field $gene$ matches the field $gene$ of the message $< id, gene >$, the algorithm sets the value $weight$ a constant w_{ini}. Then, the algorithm checks each element in trust table of node k. If there is a element j whose field id matches the field id of the message $< id, gene >$, the algorithm will add the value $weight$ to the field $value$ of element j. If there is no element whose field id matches the field id of the message $< id, gene >$, the algorithm will add a new record $< id, Value_{ini} >$ to the trust table. The pseudo code description of the process is shown as Algorithm 2, where w_{ini} and $Value_{ini}$ are constants.

Algorithm 2: ***Trust assessment***

1: receiving an item $< id, gene >$ from AgP;
2: **for** each $i \in Ab$ **do**
3: **if** ($i.gene == gene$)
4: $weight = i.weight$
5: $i.count++$;
6: **else**
7: $weight = w_{ini}$;
8: **end for**
9: **for each** i in trust table **do**
10: **if** ($i.id == id$)
11: $i.value == i.value + weight$
12: $find = TRUE$;
13: **end if**

```
14:     end for
15:     if (!find)
16:         add < id, Value_ini > to trust table;
17:     end if
```

4.2 Routing in B-iTRP

The routing strategy of B-iTRP consists of route discovery, route assessment, route optimization and route maintenance. The route discovery is achieved based on ACO and route assessment is obtained based on PO.

4.2.1 Data Structures in B-iTRP

There are mainly three kinds of data structures in B-iTRP—ant structure, route table (RTab) and trust table. The ant structure is a seven-tuple $< Source, Sequence\_No, Type, Hops, Path, Link\_Trust, Link\_Energy >$. $Source$ field stores the source address. $Sequence\_No$ field stores the sequence number tagged to each ant. Source node generates incrementally a $Sequence\_No$ each time forward ant is sent out. $Type$ field indicates the ants' type. There are four types of ants: the first is lazy forward ant (LFA) which will get back when it reaches a node with a route to the *Sink*; the second is diligent forward ant (DFA) which will get back only when it reaches the *Sink*; the third is backward ant (BA) used for returning routes to source; the last is notification ant used for sending notification to other nodes. $Hops$ field indicates the number of hops that one ant can move for forward ants and stores the hops of a route for backward ants. $Path$ field stores the sequence of nodes from source to the *Sink*. $Link\_Trust$ and $Link\_Energy$ fields measure the link trust and link energy of the route, respectively.

RTab is a five-tuple $< Source, Hops, Link\_Availability, Path, Sequence\_No >$. $Hops$ field stores the hops from source to the *Sink*. $Link\_Availability$ denotes the availability of the route. Trust table is a two-tuples $< id, Value >$ which expresses the trust value of neighbor id is $Value$. In addition, each node i still needs to save its energy residual E_i and optimization flag OF_i.

4.2.2 Route Discovery

In this section, we illustrate the route discovery process referring to Fig. 1 based on ACO. In order to proactively maintain RTab, source node s sends periodically LFA or DFA to its trusted neighbors, where ant's $Hops$ field is set to allowable maximum value.

If a LFA reaches an intermediate node j, it checks whether there exists an unexpired route to the *Sink* in RTab of node j firstly. If there is an unexpired route, the first entity in RTab is selected and the LFA is transformed into a corresponding BA to return s. Otherwise, the LFA is sent to the trusted neighbors of node j. If a DFA reaches an intermediate node j, it is sent to the trusted neighbors of node j immediately. Once LFA or DFA reaches the *Sink*, it is transformed into a corresponding BA and sent back to s along the discovered route. When BA hops from node i to node j on the way to s, B-iTRP will perform two operations.

Firstly, B-iTRP senses E_i and T_{ji}, and then calculates the $Link\_Trust$ and $Link\_Energy$ as follows.

$$L\_T_{S,j} = \begin{cases} L\_T_{S,j} + T_{ji}, & \text{if } T_{ji} > T_0 \\ 0, & \text{if } T_{ji} \le T_0 \end{cases} \tag{3}$$

$$L\_E_{S,j} = \begin{cases} L\_E_{S,i} + E_j, & \text{if } E_j > E_0 \\ 0, & \text{if } E_j \le E_0 \end{cases} \tag{4}$$

where T_0 and E_0 are constants, T_{ji} is the trust of node j respect to node i, $L\_T_{S,j}$ and $L\_E_{S,j}$ denote the $Link\_Trust$ and $Link\_Energy$ from node j to $Sink$, respectively.

Secondly, B-iTRP assesses the availability of route $j, i, \cdots$ as narrated in section 4.2.3. If the availability value is larger than a specific threshold $TH_{A,Lower}$, the route will be inserted in the proper positions in RTab of node j. Otherwise, the BA will be killed and the route will be discarded. In addition, if the availability value is larger than a specific threshold $TH_{A,Upper}$, the optimization flag OF_j will be set to $TRUE$ for a period of time T_0.

This process will be repeated until the BA returns to s (i.e. the route discovery is over).

4.2.3 Route Assessment

In this section, we propose the route assessment based on PO. From paper [20], the flux through each plasmodial tube follows

$$Q_{ij} = \frac{\pi r_{ij}^4 (P_i - P_j)}{8\eta L_{ij}} = \frac{D_{ij}(P_i - P_j)}{L_{ij}} = \frac{D_{ij} \cdot \Delta P_{ij}}{L_{ij}} \tag{5}$$

where $\Delta P_{ij} = P_i - P_j$ is the pressure difference of two ends of the tube, η is the viscosity of the fluid, $D_{ij} = \pi r_{ij}^4 / 8\eta$ is a measure of the conductivity of the tube, and L_{ij} is the length of the tube.

Since PO comes from fluid dynamics and cannot be directly used in MWSNs, we should discuss how to migrate equations (5) to MWSNs. Because D_{ij} is an inherent physical characteristic of tubes, we replace D_{ij} with the $Link\_Trust_{ij}$ which is a measure of wireless link characteristic. Since we are apt to consider the hops of two nodes rather than their Euclidean distance in MWSNs, we use the hops H_{ij} from node i to node j to replace L_{ij}. If flux (fluid or data packet) wishes to migrate from source to destination passing by other two nodes, the fluid tends to flow through the node with lower pressure in fluid dynamics, while data packet wishes to be relayed by the node with enough energy. Thus, we replace ΔP_{ij} with $Link\_Energy_{ij}$. Using (5), we obtain

$$Q_{ij} = \frac{D_{ij} \cdot \Delta P_{ij}}{L_{ij}} = \frac{L\_T_{ij} \cdot L\_E_{ij}}{H_{ij}} \tag{6}$$

where Q_{ij} is the virtual flux of communication through the wireless link $e(i, j)$. We use equation (6) to calculate the availability value of the route, which is used for route decision in route discovery as narrated in section 4.2.2.

4.2.4 Route Optimization

If source node wishes to send data packet to the *Sink*, it will select the first entity in its RTab as the route. When data packet passes through an intermediate node j on the way to the *Sink*, it checks the optimization flag OF_j. If $OF_j = TRUE$ and the first entity in RTab of node j is not the same as the corresponding route in data packet, the data packet will be transmitted along the first route in RTab of node j. This optimization process will be iterated in each intermediate node until the data packet reaches the *Sink*.

4.2.5 Route Maintenance

Route maintenance handles routing failures especially caused by node mobility or breakdown which is very common in MWSNs. If the route failure happens, B-iTRP will check the RTab and delete the records relating to the failure nodes. If there are still one or more records in the RTab of damaged node, the first record will be chosen from the remaining records as the alternative route. Then, the transmission is going on and a notification ant is sent to source to update RTab of each node on the route. If there is no record in the RTab of damaged node, the route will recover after a period of time because proactive routing is adopted, and then the transmission is going on and a notification ant is sent to source. More complicated methods can be adopted to deal with route failure, such as sending source node a message to initiate a new procedure of route discovery. However, a simple waiting for next period of time is adopted in B-iTRP to alleviate the overhead.

4.3 Dicussion

In this section, we discuss two problems which affect B-iTRP's performance significantly. The first problem is why to set LFA and DFA? If all ants in B-iTRP are LFAs, the nodes far from the *Sink* always get the second-hand routes since LFA will return once it reaches a node with route to the *Sink*. Thus, the nodes far from the *Sink* may suffer from dilemma of expired routes. Therefore, B-iTRP sets LFA and DFA, and sends them in different periods, e.g. sending one time DFA every sending five times LFAs. The second problem is how to avoid resonance of ants, which will take place if adjacent nodes send forward ants simultaneously. B-iTRP deals with this problem in three conditions—1) in network initial stage, each node select a time T_p / τ to send ants after it starts; 2) if a new node joins in MWSNs, it select a time T_p / τ to send ants after receiving an ant from other nodes; 3) if a sending node is collided with other ants, it postpones its sending for T_p / τ, where T_p is sending period and $\tau \in \{2,3,4,5,6,7,8,9\}$.

5. Simulation Results and Analysis

We analyze B-iTRP in Network Simulator ns-2 (version 2.34) and compare its simulation results with those of AODV, AntHocNet and TGRP using IEEE 802.11a. In the base simulation scenario, the *Sink* node is placed in the center of a rectangular area of $1500\text{m} \times 300\text{m}$, and 100 nodes are uniformly placed in the area and move according to the random way mobility model (RWP) [26]. In the model, each node moves towards a random direction at a speed uniformly distributed [0, 20m/s]. Once a node reaches a target position, it pauses for resting 3s to send or transmit data packet, and then moves forward in the same way.

The simulation is run for 900s each time. The data traffic is generated by 20 constant bit rate (CBR) sources with sending rates of single 64-bytes every 3s. The radio propagation range and data rate are set to 250m and 2Mbit/s, respectively. We run each simulation scenario 10 times to acquire the average values of results and compare them.

First of all, we give brief descriptions of performance measurement metrics to understand the simulation results easily. Delay expresses the average time interval that data packets are successfully delivered to *Sink* under specific routing protocol and simulation scenario in a period of time. Delivery ratio denotes the ratio of the number of the successfully delivered data packets to the number of total data packets. Overhead denotes the ratio of the number of control data packets to the number of total data packets. Ratio of malicious nodes denotes the ratio of the number of malicious nodes to the number of total nodes. Dead nodes denote the number of nodes which cannot work.

Fig. 3 shows end-to-end delay vs. number of nodes when the ratio of malicious nodes is 10%. Since AODV is on-demand protocol, its end-to-end delay is the worst of the four protocols. Because AntHocNet can proactively test existing paths and explore new ones during the course of communication session, its end-to-end delay is better than that of AODV. Since both B-iTRP and TGRP can deal with malicious nodes, their end-to-end delays are much better than those of AODV and AntHocNet. In addition, the end-to-end delay of B-iTRP is better than that of TGRP because B-iTRP adopts proactive routing and local route optimization.

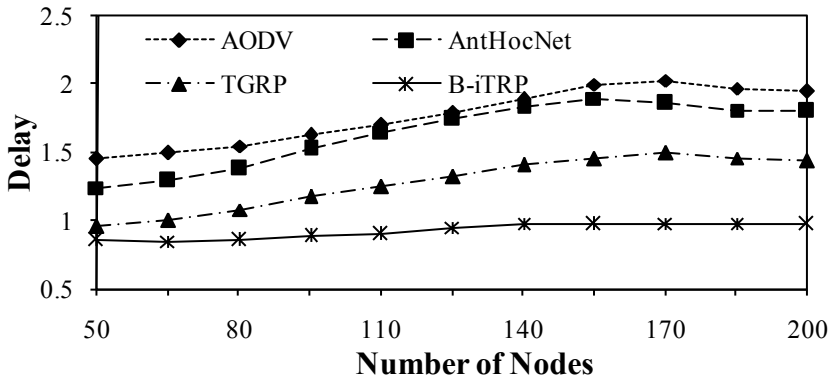


Fig. 3. Delay vs. number of nodes

Fig. 4 shows end-to-end delivery ratio vs. number of nodes when the ratio of malicious nodes is 10%. In the first stage, each delivery ratio increases rapidly with the increase of the number of nodes. After the number of nodes reaches a specific value, e.g. 100 for B-iTRP, the delivery ratio will keep a stable value approximately. Since B-iTRP and TGRP adopt trust mechanism, their delivery ratios are similar and greater than those of AODV and AntHocNet.

Fig. 5 shows overhead vs. number of nodes when the ratio of malicious nodes is 10%. Since AODV is a purely reactive and AntHocNet is hybrid, their control overheads are the least and the second least in the four protocols, respectively. However, their control overheads increase rapidly with the increase of the number of nodes. Since B-iTRP needs to periodically send out forward ants and deal with neighbors' trusts, its control overhead is greater than that of TGRP which only needs to deal with trust. However, the difference of control overhead is reduced with the increase of the number of nodes because B-iTRP adopts the mechanism of LFA and DFA.

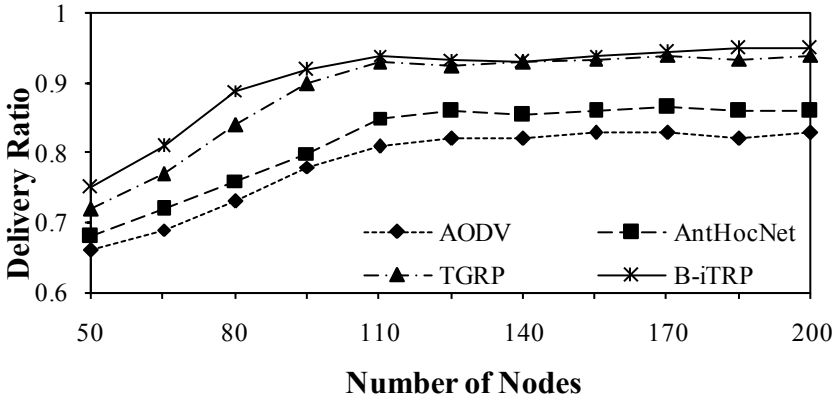


Fig. 4. Delivery ratio vs. number of nodes

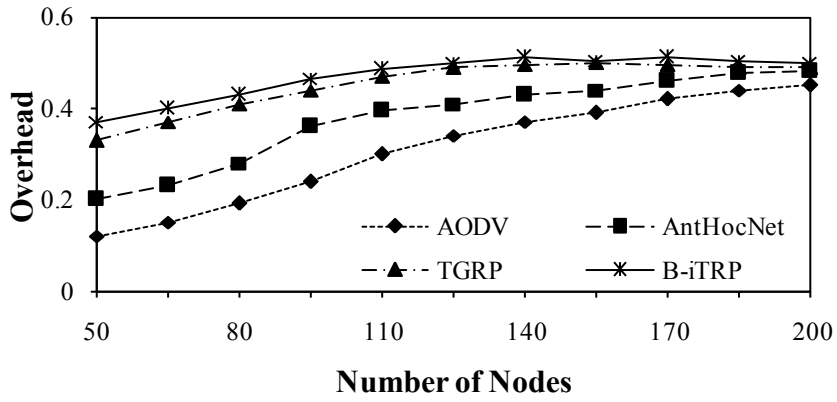


Fig. 5. Overhead vs. number of nodes

Fig. 6 shows end-to-end delay vs. ratio of malicious nodes. Since AODV and AntHocNet cannot deal with attacks from malicious nodes, their end-to-end delay increases with the increase of malicious nodes, and the increment is larger and larger. Since both B-iTRP and TGRP can deal with malicious nodes, their end-to-end delays are similar. What is more, the end-to-end delay of B-iTRP is better than that of TGRP since B-iTRP adopts proactive routing and local route optimization.

Fig. 7 shows delivery ratio vs. ratio of malicious nodes. Each delivery ratio decreases gradually with the increase of the ratio of malicious nodes, and the decrement is greater and greater. In the first stage, each delivery ratio decreases little with the increase of the ratio of malicious nodes. After the ratio of malicious nodes reaches a specific value, e.g. 30 for AODV and AntHocNet, the two delivery ratios will decrease rapidly. Since B-iTRP and TGRP adopt trust mechanism, their delivery ratios are similar and decrease slowly.

Fig. 8 shows dead nodes vs. simulation time when the ratio of malicious nodes is 10%. Once the simulation time is over 300s, dead nodes will emerge for AODV, AntHocNet and TGRP. Since the control overhead of AODV is the lowest in AODV, AntHocNet and TGRP, its dead nodes is the least in the three protocols. Similarly, the dead nodes of AntHocNet and TGRP are the second least and the most, respectively. Moreover, B-iTRP considers the energy of routes, thus its dead nodes is the least in the four protocols.

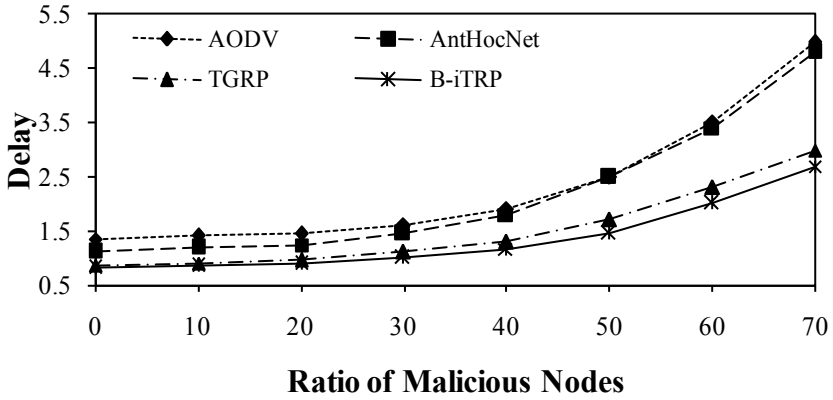


Fig. 6. Delay vs. ratio of malicious nodes

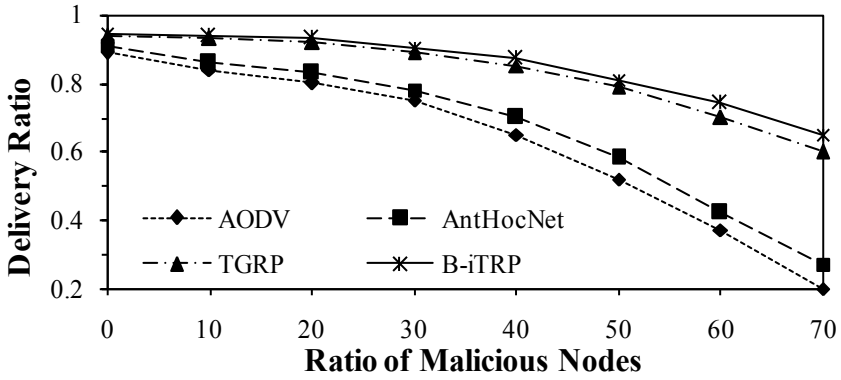


Fig. 7. Delivery ratio vs. ratio of malicious nodes

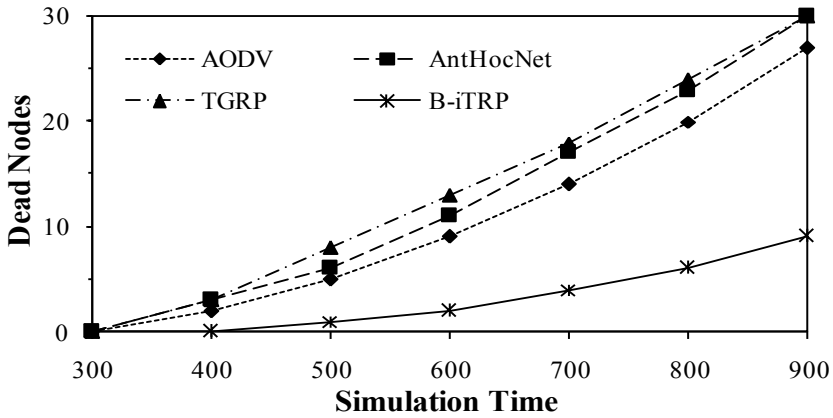


Fig. 8. Dead nodes vs. simulation time

6. Conclusion and Future Work

In this paper, we present B-iTRP, a trusted source routing protocol based on AIS, ACO and PO. On the one hand, B-iTRP uses AIS to assess neighbors' trusts in real time, where the original neighbor's behavior information is acquired by monitoring. On the other hand,

B-iTRP proactively finds routes to the *Sink* based on ACO firstly; then B-iTRP calculates the trust and energy of discovered route based on the information obtained by cross-layer perception; finally, B-iTRP assesses the availability of discovered route based on PO. In fact, B-iTRP is devoted to combing the advantages of AIS, ACO and PO to improve the routing performance.

In future work, we consider introducing actual mobility model into B-iTRP to make it further fit in with real MWSNs environment. Furthermore, we will realize the B-iTRP from the engineering and use it in some real-world experiments to further test the feasibility of B-iTRP.

Acknowledgment

This work was partially supported by the National Basic Research Program of China (973 Program) under Grant No. 2013CB329102, by the National Natural Science Foundation of China (NSFC) under Grant No. 61372112, 61232017, U1204614, 61142002 and 61370221, by the National High-Tech Research and Development Program of China (863 Program) under Grant No. 2011AA010701, and by the Natural Science Foundation of Jiangsu Province under Grant No. BK2011171, and by the key project of the Education Department Henan Province under Grant No. 14B520031, and by Key Project of Science and Technology Department of Henan Province under Grant No.112102210187, and by the Plan for Scientific Innovation Talent of Henan Province under Grant No. 124100510006.

References

[1] G. Zhan, W. Shi, and J. Deng, "Design and Implementation of TARF: A Trust-Aware Routing Framework for WSNs," *IEEE Trans. On Dependable and Secure Computing*, vol. 9, no. 2, pp. 184-197, March, 2012. Article (CrossRef Link)

[2] G. Wei, R. Xu, and B. Liu, "Research on Subjective Trust Routing Algorithm for Mobile Ad Hoc Networks," in *Proc. of WiCOM*, September, 2010. Article (CrossRef Link)

[3] F. Bao, I. Chen, M. Chang, and J. Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection," *IEEE Trans. On Network and Service Management*, vol. 9, no. 2, pp. 169-183, June, 2012. Article (CrossRef Link)

[4] H. Xia ,Z. Jia, X. Li, L. Jua, and E. Shab, "Trust prediction and trust-based source routing in mobile ad hoc networks," *Ad Hoc Networks*, vol. 11, no. 6, pp. 2096-2114, September, 2013. Article (CrossRef Link)

[5] D. Dasgupta, S. Yu, and F. Nino, "Recent Advances in Artificial Immune Systems: Models and Applications," *Applied Soft Computing*, vol. 11, no. 2, pp. 1574-1587, March, 2011. Article (CrossRef Link)

[6] D. Dal, S. Abraham, A. Abraham, S. Sanyal, and M. Sanglikar, "Evolution Induced Secondary Immunity: An Artificial Immune System based Intrusion Detection System," in *Proc. of Int. Conf. on Computer Information Systems and Industrial Management Applications*, pp. 65-70, June, 2008. Article (CrossRef Link)

[7] H. Yang, J. Guo, and F. Deng, "Collaborative RFID intrusion detection with an artificial immune system," *Journal of Intelligent Information Systems*, vol. 36, no. 1, pp. 1-26, February, 2011. Article (CrossRef Link)

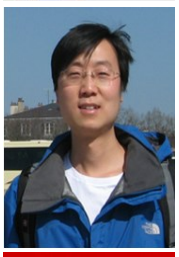
[8] J. Rao and A. O. Fapojuwo, "A Battery Aware Distributed Clustering and Routing Protocol for Wireless Sensor Networks," in *Proc. of WCNC*, pp.1538-1543, April, 2012. Article (CrossRef Link)

[9] C. Chau, Q. Fei, S. Sayed, M. Wahab, and Y. Yang, "Harnessing Battery Recovery Effect in Wireless Sensor Networks: Experiments and Analysis," *IEEE Journal on Selected Areas in*

Communications, vol. 28, no. 7, pp. 1222-1232, September, 2010. Article (CrossRef Link)
[10] O. Yang and W. Heinzelman, "Sleeping Multipath Routing: A Trade-off between Reliability and Lifetime in Wireless Sensor Networks," in *Proc. of Globecom*, December, 2011. Article (CrossRef Link)
[11] F. Kuhn, R. Wattenhofer, and A. Zollinger, "An algorithmic approach to geographic routing in ad hoc and sensor networks," *IEEE Transactions on Networking*, vol. 16, no. 1, pp. 51-62, February, 2008. Article (CrossRef Link)
[12] G. Trajcevski, F. Zhou, R. Tamassia, and B. Avii, "Bypassing Holes in Sensor Networks: Load-balance VS. Latency," in *Proc. of Globecom*, December, 2011. Article (CrossRef Link)
[13] J. Chen, Y. Chen, L. Zhou, and Y. Du, "A Data Gathering Approach for Wireless Sensor Network with Quadrotor-based Mobile Sink Node," *KSII Transactions on Internet and Information Systems*, vol. 6, no. 10, pp. 2529-2547, October , 2012. Article (CrossRef Link)
[14] L. Zhou, Q. Hu, Y. Qian, and H. Chen, "Energy-Spectrum Efficiency Tradeoff for Video Streaming over Mobile Ad Hoc Networks," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 5, pp. 981-991, May, 2013. Article (CrossRef Link)
[15] M. Günes, U. Sorges, and I. Bouazizi, "ARA – The Ant-Colony Based Routing Algorithm for MANETs," in *Proc. of Int. Conf. on Parallel Processing Workshops*, pp. 79-85, August, 2002. Article (CrossRef Link)
[16] C. Perkins and E. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. of 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pp. 90-100, Feburary, 1999. Article (CrossRef Link)
[17] G. Caro, F. Ducatelle, and L. Gambardella, "AntHocNet: an adaptive nature inspired algorithm for routing in mobile ad hoc networks," *European Transactions on Telecommunications*, vol. 16, no. 5, pp. 443-455, September, 2005. Article (CrossRef Link)
[18] J. Wang, E. Osagie, P. Thulasiraman, and R. Thulasiram, "HOPNET: A hybrid ant colony optimization routing algorithm for mobile ad hoc network," *Ad Hoc Networks*, vol. 7, no. 4, pp. 690-705, June, 2009. Article (CrossRef Link)
[19] T. Nakagaki, H. Yamada, and A. Toth, "Maze-solving by an amoeboid organism," *Nature*, vol. 407, p. 470, September, 2000. Article (CrossRef Link)
[20] A. Tero, R. Kobayashi, and T. Nakagaki, "A mathematical model for adaptive transport network in path finding by true slime mold," *Journal of Theoretical Biology*, vol. 244, no. 4, pp. 553-564, Feburary, 2007. Article (CrossRef Link)
[21] K. Li, C. Torres, and K. Thomas, "Slime mold inspired routing protocols for wireless sensor networks," *Swarm Intelligence*, vol. 5, no. 4, pp. 183-223, November, 2011. Article (CrossRef Link)
[22] M. Zhang, C. Xu, J. Guan, R. Zheng, Q. Wu, and H. Zhang, "P-iRP: Physarum-inspired Routing Protocol for Wireless Sensor Networks," in *Proc. of VTC*, September, 2013. Article (CrossRef Link)
[23] M. Zhang, C. Xu, J. Guan, R. Zheng, Q. Wu, and H. Zhang, "A Novel Physarum-Inspired Routing Protocol for Wireless Sensor Networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 483581, 12 pages, 2013. Article (CrossRef Link)
[24] C. Xu, T. Liu, J. Guan, H. Zhang, and G.-M. Muntean, "CMT-QA: Quality-aware Adaptive Concurrent Multipath Data Transfer in Heterogeneous Wireless Networks," *IEEE Transactions on Mobile Computing*, vol. pp, no. 99, August, 2012. Article (CrossRef Link)
[25] Y. Cao, C. Xu, J. Guan, J. Zhao, and H. Zhang, "Cross-layer Cognitive CMT for Efficient Multimedia Distribution over Multi-homed Wireless Networks," in *Proc. of IEEE WCNC*, April, 2013. Article (CrossRef Link)
[26] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, vol. 353, pp. 153-181. 1996. Article (CrossRef Link)

Mingchuan Zhang was born in Henan Province, PRC in May 1977. He studied in Harbin Engineering University (Harbin, Heilongjiang Province, PRC) from Sept. 2002 to Mar. 2005, majored in computer application and earned a Master of Engineering Degree. From 2011 to now, he is working toward his Ph.D degree in the State Key Laboratory of Networking and Switching Technology at Beijing University of Posts and Telecommunications. He works as a Lecturer in Henan University of Science and Technology from Mar.2005 to now. His research interests include ad hoc network, Internet of Things, cognitive network and future Internet technology.

Changqiao Xu is an Associate Professor in the Institute of Network Technology and vice Director of the Next Generation Internet Research Center at Beijing University of Posts and Telecommunications (BUPT), China. He received his Ph.D. in Computer Applied Technology from the Institute of Software Chinese Academy of Sciences (ISCAS), Beijing, China, in Jan 2009. He joined ISCAS in 2002 where he held roles as a research staff and project manager in the R&D area of communication networks. His research interests include computer networks, next generation Internet technology and wireless communications



Jianfeng Guan received his B.S. degree from Northeastern University of China in July 2004, and received the Ph.D. degrees in communications and information system from the Beijing Jiaotong University in Jan. 2010. He is a Lecturer in the Institute of Network Technology at Beijing University of Posts and Telecommunications (BUPT), Beijing, China. His main research interests focus around mobile IP, mobile multicast, IP security and next generation Internet.

Ruijuan Zheng was born in Henan Province, PRC in Mar 1980. She studied in Harbin Engineering University Technology (Harbin, PRC) from Mar 2005 to Mar 2008, majored in computer application and earned a Doctor of Engineering Degree in three year's time. She works as an Associate Professor in Henan University of Science and Technology from Mar 2008 to now. Her research interests include bio-inspired networks, Internet of Things, future Internet and computer security.

Qingtao Wu was born in Jiangsu Province, PRC in Mar 1975. He studied in East China University of Science and Technology (Shanghai, PRC) from Mar 2003 to Mar 2006, majored in computer application and earned a Doctor of Engineering Degree in three year's time. He works as a Professor in Henan University of Science and Technology from Mar 2006 to now. His research interests include component technology, computer security and future Internet security. Mr. Wu holds a membership of China Computer Federation (CCF).

Hongke Zhang received his Ph.D. degrees in electrical and communication systems from the University of Electronic Science and Technology of China in 1992. From 1992 to 1994, he was a postdoctoral research associate at Beijing Jiaotong University, and in July 1994, he became a professor there. He has published more than 150 research papers in the areas of communications, computer networks, and information theory. He is the author of eight books written in Chinese and the holder of more than 40 patents. He is now the director of National Engineering Lab for Next Generation Internet Interconnection Devices at Beijing Jiaotong University. He is also the head of the Institute of Network Technology at Beijing University of Posts and Telecommunications, and the chief scientist of a National Basic Research Program of China ("973 Program"). He is a member of the electronics and information science steering committee of the Ministry of Education, and a member of the expert committee of the Ministry of Information Industry.