Hindawi Publishing Corporation
Journal of Sensors
Volume 2015, Article ID 156843, 8 pages
http://dx.doi.org/10.1155/2015/156843

Research Article

B-iTRS: A Bio-Inspired Trusted Routing Scheme for Wireless Sensor Networks

Mingchuan Zhang,[1,2] Ruijuan Zheng,[1] Qingtao Wu,[1] Wangyang Wei,[1] Xiuling Bai,[1] and Haixia Zhao[1]

[1]*Information Engineering College, Henan University of Science and Technology, Luoyang 471023, China*
[2]*National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University, Beijing 100044, China*

Correspondence should be addressed to Ruijuan Zheng; rjwo@163.com

Received 24 November 2014; Revised 11 March 2015; Accepted 20 March 2015

Academic Editor: Fei Yu

In WSNs, routing algorithms need to handle dynamical changes of network topology, extra overhead, energy saving, and other requirements. Therefore, routing in WSNs is an extremely interesting and challenging issue. In this paper, we present a novel bio-inspired trusted routing scheme (B-iTRS) based on ant colony optimization (ACO) and Physarum autonomic optimization (PAO). For trust assessment, B-iTRS monitors neighbors' behavior in real time, receives feedback from Sink, and then assesses neighbors' trusts based on the acquired information. For routing scheme, each node finds routes to the Sink based on ACO and PAO. In the process of path finding, B-iTRS senses the load and trust value of each node and then calculates the link load and link trust of the found routes to support the route selection. Moreover, B-iTRS also assesses the route based on PAO to maintain the route table. Simulation results show how B-iTRS can achieve the effective performance compared to existing state-of-the-art algorithms.

1. Introduction

Mobile wireless sensor networks (WSNs) are autonomous wireless communication networks and ideal candidates for applications to report detected events of interest, such as military surveillance and forest fire [1, 2]. Because of the 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 WSNs is an extremely interesting and challenging issue.

Traditional WSNs routing protocols assume that all sensor nodes work in a benevolent manner, which may render the WSNs 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 selfish behavior will seriously affect the network performance [3]. Since the safety of multihop 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 route. Moreover, how to guarantee the efficiency of the multihop route is important to prolong lifetime of WSNs. Therefore, security and efficiency are the significant features for routing in WSNs.

Recently, many research results on the trust and efficiency of routing have been proposed. In order to solve the security of routing protocol, some techniques (e.g., trust value, detection, cryptography, and data hiding) are proposed based on different applications [1–5]. Bao et al. [4] 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 TARF, a robust trust-aware routing framework for dynamic WSNs. Some methods (e.g., location-aware method, energy-aware method, energy harvesting method, and their combination) are discussed [6–9]. Yang and Heinzelman [7] propose sleeping multipath routing, which selects the minimum number of disjoint paths to achieve the trade-off of given reliability requirement and energy efficiency. Trajcevski et al. [8] present heuristic

approaches to relieve some of the routing load of the boundary nodes of energy holes in location-aware WSNs. Chen et al. [9] present a method to enhance the efficiency of gathering sensor data based on a quadrotor-based mobile Sink.

Bio-inspired methods [10–15] are advantageous for solving the problems regardless of security and efficiency of routing protocols. Gunes et al. [10] present an on-demand routing algorithm ARA based on ant colony optimization (ACO) and AODV [16]. Di Caro et al. [11] propose the 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. Tero et al. [12] propose a mathematical model for the Physarum autonomic optimization (PAO). Li et al. [13] present a routing protocol for wireless sensor networks based on PAO. We study the foraging rule of Physarum and present a Physarum-inspired routing protocol for WSNs [14, 15].

In addition, trust computation or management is important for assessing node's reliability. Ren et al. [17] propose a trust management scheme for UWSNs to provide efficient and robust trust data storage and trust generation, where a geographic hash table is employed. Chen et al. [18] design and validate a dynamic trust management protocol for secure routing optimization in DTN environments in the presence of well-behaved, selfish, and malicious nodes. Priyanka et al. [19] present a malicious node detection scheme for wireless sensor networks, where the malicious nodes are detected by computing the average number of event cycles. Indhu Lekha and Kathiroli [20] propose a vector based trust mechanism which nominates a cluster head based on the higher trust value computation with the earliest bit vectors and enhanced certificate revocation scheme for discarding the authorization of the misbehaving nodes. Wang et al. [21] propose the framework ARTSense to solve the problem of "trust without identity" in mobile sensing, where contextual factors are employed to dynamically affect the trustworthiness of the sensing data as well as the mutual support and conflict among data from different sources.

In this paper, we propose a novel bio-inspired trusted routing scheme (B-iTRS) in comprehensive thought of trust and load. B-iTRF consists of trust mechanism and routing scheme. For trust mechanism, B-iTRS assesses nodes' trust value through monitoring nodes' behavior in real time and receives feedback from Sink. For routing scheme, B-iTRS finds routes to the Sink based on ACO by introducing cross-layer [22] and assesses the discovered routes based on PAO.

The rest of this paper is organized as follows. Section 2 introduces the models used in B-iTRS. Section 3 details the proposed B-iTRS. Section 4 analyzes B-iTRS with mathematical method. Section 5 evaluates our models and algorithms with extensive simulations. Finally, the conclusion is presented in Section 6.

2. System Framework and Models

2.1. Typical WSNs Scenario. This paper considers large multihop WSNs 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, and (3) all communication links are bidirectional.

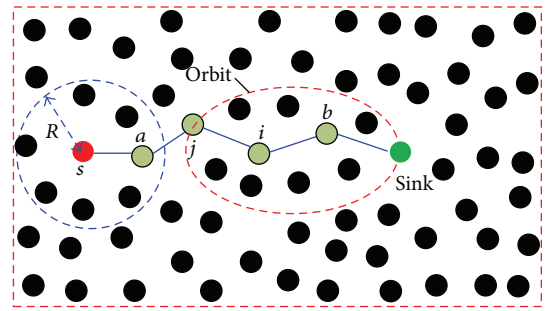

Figure 1: An example of MWSNs' topology.

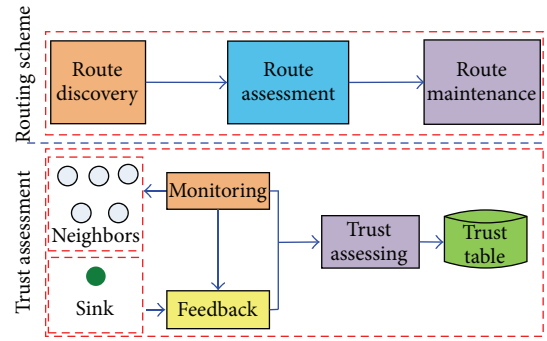

Figure 2: B-iTRS framework.

Based on the assumptions, WSNs can be abstracted as a graph $G = (V, E)$, where V is the set of all nodes and E is the set of all edges. Each edge $e(i, j) \in E$ denotes that the two nodes are located within each other's transmission range.

In some circumstances, the Sink node moves along a certain orbit in the field and broadcasts periodically its current positions to improve the efficiency of collected data. An example of such WSNs' topology is shown in Figure 1.

2.2. The Framework of B-iTRS. Based on the above discussion, Figure 2 illustrates the design of the proposed B-iTRS framework which consists of trust assessment and routing scheme.

For trust assessment, each node monitors its neighbors' behavior in real time and receives the feedback from the Sink node. Based on the neighbors' behavior and feedback information, B-iTRS assesses trusts of neighbors; that is, the trust of corresponding neighbor is added by a different positive, negative, or zero value according to the behavior's weight or Sink's feedback. 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 scheme, perceptive ACO is used to find and assess routes. Each node s sends perceptive forward-ants to find routes to the Sink, where the cross-layer perception [22] 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 load and the trust with respect to node i.

Then, B-iTRS assesses the trust, load, and availability of route $j, i, \ldots,$ Sink. If the availability value of the route is less than a specific threshold $\mathrm{TH}_{A,\mathrm{Lower}}$, B-iTRS 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. The process is repeated until the backward-ant reaches source. When route failures happen, route maintenance is triggered to recover the route rapidly.

2.3. Trust Assessment Model. In B-iTRS, each node monitors its neighbors' behaviors in real time and then analyzes them to get their trust weight, since analyzing node's behavior can show whether the node is selfish, is acting like a black hole, is carrying out a modification or fabrication attack, is inducing latency delays by delaying the retransmission of the packet [23], and so forth. In order to alleviate the calculating burden, we do not adjust the trust weight of behaviors automatically but adopt the prior trust weight which is determined by offline decision.

If a new neighbor j of node i arises, node i endows it with initial trust value $\mathrm{TRUST}_{i,j}$, which is determined by

$$\mathrm{TRUST}_{i,j} = \begin{cases} \dfrac{1}{n}\displaystyle\sum_{k=1}^{n} \mathrm{trust}_{i,k}, & \text{if } n \geq 1 \\ \mathrm{trust}_c, & \text{if } n = 0, \end{cases} \tag{1}$$

where $\mathrm{trust}_{i,k}$ is the trust value of node i with respect to the kth neighbor, n is the number of neighbors, and trust_c is a constant.

Once node i obtains a specific behavior about neighbor j by monitoring it, node i analyzes the behavior based on prior knowledge to identify the behavior of neighbor j and get the trust weight of the behavior and then updates the trust value of node i with respect to neighbor j by

$$\mathrm{trust}_{i,j}(t+1) = \begin{cases} \mathrm{TRUST}_{i,j} + \mathrm{weight}, & \text{if } t = 1 \\ \mathrm{trust}_{i,j}(t) + \mathrm{weight}, & \text{if } t > 1, \end{cases} \tag{2}$$

where weight is the trust weight of the behavior identified, $\mathrm{trust}_{i,j}(t)$ is the trust value after the tth updating, and $\mathrm{trust}_{i,j}(t+1)$ is the trust value after the $(t+1)$th updating.

Once node i receives the feedback about its neighbors from the Sink node, node i analyzes feedback information to modify the trusts of its neighbors by

$$\mathrm{trust}_{i,j}(\mathrm{new}) = \mathrm{trust}_{i,j}(\mathrm{old}) + \mathrm{weight}(j), \tag{3}$$

where $\mathrm{trust}_{i,j}(\mathrm{new})$ is the trust value after updating, $\mathrm{trust}_{i,j}(\mathrm{old})$ is the trust value before updating, and $\mathrm{weight}(j)$ is the trust weight of node j based on the feedback of Sink node, where $\mathrm{weight}(j)$ is standardized to the same range of $\mathrm{trust}_{i,j}$.

2.4. Perceptive ACO Path-Finding Model. We improve the traditional ants to perceptive ants based on ACO to obtain path-finding and path-assessment models by introducing cross-layer perception [22]. For MWSNs expressed by graph $G = (V, E)$, each edge $e(i, j) \in E$ has a variable artificial pheromone $\tau(i, j)$, which is an indication of usage of the edge and is modified by perceptive ants when they hop from node i to node j.

A perceptive ant located in node i uses $\tau(i, j)$ of node j to compute the probability of node j as next hop:

$$p_{ij} = \frac{\tau(i,j)}{\sum_{j \in N_i} \tau(i,j)}, \quad j \in N_i, \tag{4}$$

where p_{ij} satisfies $\sum_{j \in N_i} p_{ij} = 1$ and N_i is the set of one-hop neighbors of node i.

Once the perceptive ant moves from node i to node j, it senses two metrics L_j and $\mathrm{trust}_{i,j}$ to measure the link status, where L_j denotes the length of transmission waiting queue of node j and $\mathrm{trust}_{i,j}$ denotes the trust value of node i with respect to the j. If it is the $(t+1)$th time that perceptive ants pass by the edge $e(i, j)$, depositing pheromone on $e(i, j)$ and evaporating pheromone from $e(k, j)$, $k \neq i$, respectively, are followed by

$$\tau_{t+1}(i,j) = \begin{cases} \tau_t(i,j) + \dfrac{L_0 \cdot \mathrm{trust}_{i,j}}{L_j \cdot T_0} \cdot \Delta\tau, & \text{if } \dfrac{L_0 \cdot \mathrm{trust}_{i,j}}{L_j \cdot T_0} \leq K_0 \\ \tau_t(i,j) + K_0 \cdot \Delta\tau, & \text{otherwise,} \end{cases} \tag{5}$$

$$\tau_{t+1}(k,j) = \begin{cases} \left(1 - \dfrac{L_j \cdot T_0}{L_0 \cdot \mathrm{trust}_{i,j}}\right) \cdot \tau_t(k,j), & \dfrac{L_j \cdot T_0}{L_0 \cdot \mathrm{trust}_{i,j}} \in [0,1] \\ (1 - U_0) \cdot \tau_t(k,j), & \text{otherwise,} \end{cases} \tag{6}$$

where L_0, T_0, K_0, $\Delta\tau$, and U_0 are constants and $U_0 \in (0, 1)$. $\tau_t(i, j)$ denotes the pheromone on edge $e(i, j)$ after the tth depositing or evaporating. Equations (4), (5), and (6) are used to find routes in B-iTRS.

When a backward perceptive ant moves from node i to node j on the way to source, the link quality and link load are assessed with the metrics, respectively, following

$$L\_R_{dj} = \begin{cases} L\_R_{di} + T_0, & \text{if } \mathrm{trust}_{ij} > T_0 \\ L\_R_{di} + T_1, & \text{if } \mathrm{trust}_{ij} < T_1 \\ L\_R_{di} + \mathrm{trust}_{ij}, & \text{otherwise,} \end{cases} \tag{7}$$

$$L\_L_{dj} = \begin{cases} L\_L_{di} + L_0, & \text{if } L_j > L_0 \\ L\_L_{di} + L_j, & \text{if } L_j \leq L_0, \end{cases} \tag{8}$$

where T_0, T_1, and L_0 are constants and L_R_{dj} and L_L_{dj} denote the link reliability and link load from node d to node j, respectively. Equations (7) and (8) are used to assess the discovered routes in B-iTRS.

2.5. PAO Path-Assessment Model. In this section, we improve PAO to acquire PAO path-assessment model. From [12–15], the flux through each plasmodial tube follows

$$Q_{ij} = \frac{C_{ij}\left(P_i - P_j\right)}{D_{ij}} = \frac{C_{ij} \cdot \Delta P_{ij}}{D_{ij}}, \tag{9}$$

where $\Delta P_{ij} = P_i - P_j$ is the pressure difference of two ends of the tube, C_{ij} is a measure of the conductivity of the tube, and D_{ij} is the length of the tube. Physarum forages for distributed food sources through adapting its plasmodium to change the flux of each tube, which is described by

$$\frac{d}{dt}C_{ij} = \varphi\left(\left|Q_{ij}\right|\right) - \delta C_{ij}, \tag{10}$$

where δ is a decay rate of the tube and $\varphi(\cdot)$ is a monotonically increasing continuous function satisfying $\varphi(0) = 0$.

Since PAO comes from fluid dynamics and cannot be directly used in MANETs, we replace C_{ij} with the link trust trust_{ij}, D_{ij} with H_{ij} which denotes the hops from node i to node j, and ΔP_{ij} with $\Delta L_{ij} = L_i - L_j$. Thus, we obtain

$$Q_{ij} = \frac{C_{ij} \cdot \Delta P_{ij}}{D_{ij}} = \frac{\text{trust}_{ij} \cdot \Delta L_{ij}}{H_{ij}}, \tag{11}$$

$$\begin{aligned}\frac{d}{dt}\Delta\text{trust}_{ij} &= \varphi\left(|Q|\right) - \delta\Delta\text{trust}_{ij} \\ &= \left(\frac{\text{trust}_{ij} \cdot \Delta L_{ij}}{H_{ij}}\right)^{\mu} - \delta\Delta\text{trust}_{ij},\end{aligned} \tag{12}$$

where Q_{ij} is the virtual flux of communication through the wireless link $e(i, j)$, δ is the rate of trust changing, and μ is a constant satisfying $\mu > 0$. Equation (12) is used to select the optimal route in B-iTRS.

3. B-iTRS Protocol

The B-iTRS consists of trust assessment and routing scheme. The trust assessment is running in each node independently to acquire its neighbors' trusts. The route scheme works based on PACO and PAO. The module structure is shown in Figure 3.

3.1. Data Structures in B-iTRS. There are mainly three kinds of data structures in B-iTRS—perceptive ant structure, route table, and pheromone table. The structure of perceptive ant is seven-tuple ⟨Source, Sequence_No, Type, Hops, Path, Link_Reliability, Link_Load⟩. Source field stores the source node address. Sequence_No field stores the sequence number tagged to each ant. Source and destination nodes incrementally generate a Sequence_No each time forward- or backward-ants are sent out. The pair ⟨Source, Sequence_No⟩ can uniquely identify the ants' generation. Type field indicates the ants' type. There are four types of ants: the first is perceptive forward-ant used for finding routes; the second is perceptive backward-ant used for returning routes to source; the third is notification ant

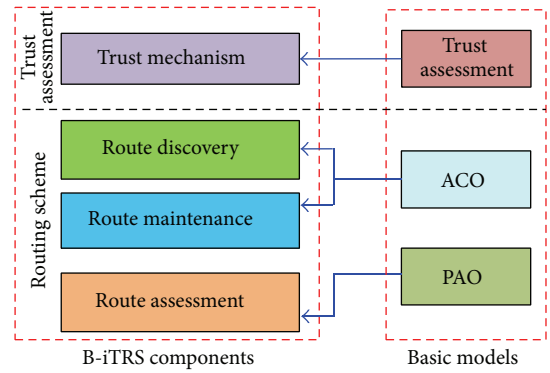

Figure 3: B-iTRS module structure.

used for sending notification to other nodes; and the last is error ant used for sending error to other nodes. For forward-ant, the Hops field indicates the maximum hops that one ant can move. For backward-ant, the Hops field stores the hops of a route. Path field stores the sequence of nodes from source to destination. Link_Reliability and Link_Load measure the link reliability and link load of the discovered routes, respectively.

Each node needs to maintain a route table whose structure is six-tuple ⟨Source, Hops, Link_Reliability, Link_Load, Path, Sequence_No⟩. Hops field stores the hops from source to destination. The structure of pheromone table is triple ⟨i, j, Value⟩ which expresses the pheromone of link $e(i, j)$ is Value.

3.2. Route Discovery. When a source s wishes to send data packet to Sink, it looks up its route table firstly. If only one route is found, the route discovery process is over. If multiple routes are found, the route selection is performed according to (12).

If there is no route from source s to Sink in route table, the route discovery will be triggered. The node s sets a timeout T_0 and sends perceptive forward-ants to find new routes, where Hops fields are set to the allowable maximum value, which means each perceptive forward-ant will die only to find Sink, a node with a route to Sink, or move limited maximum hops.

When a forward-ant reaches an intermediate node, it checks whether unexpired routes to destination Sink already exist in the route table firstly. If there are one or more unexpired routes, the optimal route to Sink is selected according to (9), and a corresponding perceptive backward-ant is generated and sent back to source along the discovered path. Otherwise, the transition probability, pheromone depositing, and evaporating are calculated following (4), (5), and (6), respectively. Once a perceptive forward-ant reaches Sink, a corresponding backward-ant is generated and sent back to source along the discovered path.

When the perceptive backward-ant reaches each intermediate node i on the way to source, B-iTRS will perform two operations. Firstly, the pheromone depositing, pheromone evaporating, link quality, and link load are calculated following (5), (6), (7), and (8), respectively. Secondly, the new route will be added to the route table of node i. After the perceptive

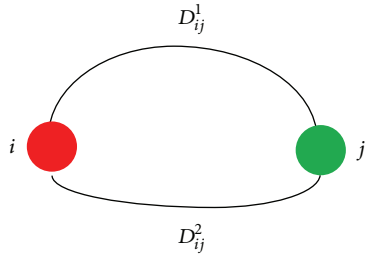

Figure 4: B-iTRS module structure.

backward-ant reaches source s, the new route will be added to route table.

If T_0 is time out and no route is found, the route discovery fails. If only one route is found, the route discovery process is over. If multiple routes are found, (9) is used to determine the optimal route.

3.3. Route Maintenance. Route maintenance handles routing failures especially caused by node mobility or breakdown which is very common in MWSNs. If the route failures happen, the upstream node of the broken link will trigger a repair procedure to find new routes to Sink, which is similar to the route discovery. If an alternative route is found, the transmission is going on and a notification ant is sent to source to update route table of each node on the path. If no route is found, an error ant will be sent to source as well as updating route table of each node on the path. After receiving an error ant, if the source still needs to transmit the data packet, it can select the backup route or other unexpired routes found in route table and even initiate a new procedure of route discovery among zones.

4. B-iTRS Analysis

In this section, we analyze the feasibility of B-iTRS by mathematical theoretical analysis. We study the cases in which two nodes connected to the same node compete to be the next hop, as shown in Figure 4.

There are two nodes i and j_1. For simplicity, we hereafter replace D_{ij_1}, D_{ij_2}, Q_{ij_1}, Q_{ij_2}, ΔP_{ij_1}, and ΔP_{ij_2} by D_1, D_2, Q_1, Q_2, ΔP_1, and ΔP_2, respectively. From (9) and (10), the virtual fluxes along each path are calculated as

$$Q_1 = \frac{\Delta P_1/D_1}{\Delta P_1/D_1 + \Delta P_2/D_2},$$
$$Q_2 = \frac{\Delta P_2/D_2}{\Delta P_1/D_1 + \Delta P_2/D_2}. \tag{13}$$

Since Q_1 and Q_2 are nonnegative, adaptation equation (9) becomes

$$\frac{d}{dt}(\Delta P_1) = \varphi(Q_1) - \delta \cdot \Delta P_1,$$
$$\frac{d}{dt}(\Delta P_2) = \varphi(Q_2) - \delta \cdot \Delta P_2. \tag{14}$$

Setting $\varphi(Q) = Q^\mu$, $(d/dt)(\Delta P_1) = 0$, and $(d/dt)(\Delta P_2) = 0$, we have

$$\left(\frac{\Delta P_1/D_1}{\Delta P_1/D_1 + \Delta P_2/D_2}\right)^\mu = \delta \cdot \Delta P_1,$$
$$\left(\frac{\Delta P_2/D_2}{\Delta P_1/D_1 + \Delta P_2/D_2}\right)^\mu = \delta \cdot \Delta P_2. \tag{15}$$

After some calculations, we obtain

$$\Delta P_1 = \frac{1}{\delta}\left[\frac{1}{\left(1 + (D_1/D_2)^{1/1-\mu}\right)}\right]^\mu,$$
$$\Delta P_2 = \frac{1}{\delta}\left[\frac{1}{\left(1 + (D_2/D_1)^{1/1-\mu}\right)}\right]^\mu. \tag{16}$$

From (10), if we suppose ΔL_{ij} is constant and use trust_{ij} replacing C_{ij}, H_{ij} replacing D_{ij}, and ΔL_{ij} replacing D_{ij}, we obtain

$$\Delta\text{trust}_1 = \frac{1}{\delta}\left[\frac{1}{\left(1 + (H_1/H_2)^{1/1-\mu}\right)}\right]^\mu,$$
$$\Delta\text{trust}_2 = \frac{1}{\delta}\left[\frac{1}{\left(1 + (H_2/H_1)^{1/1-\mu}\right)}\right]^\mu. \tag{17}$$

Namely, if we suppose ΔL_{ij} is constant, there is an equilibrium point given by $(\Delta\text{trust}_1, \Delta\text{trust}_2)$. If we suppose trust_{ij} is constant, there is an equilibrium point given by $(\Delta L_1, \Delta L_2)$. If both ΔL_{ij} and trust_{ij} are not constants, there is a more complicated equilibrium point. Therefore, the B-iTRS is always convergent, which is very important for a routing protocol.

5. Simulation Results and Analysis

We analyze B-iTRS in Network Simulator ns-2 (version 2.34) and compare its simulation results with those of AODV, AntHocNet, and TGRP. In the base simulation scenario, the Sink node is placed in the center of a rectangular area of 600 m × 600 m, and 100 nodes are uniformly placed in the area and move according to the random way mobility model (RWP) [24]. The Sink moves along an ellipse orbit in the center of the rectangular area. It broadcasts periodically its current positions, as shown in Figure 1. In the model, each node moves towards a random direction at a speed uniformly distributed [0, 10 m/s]. Once a node reaches a target position, it pauses for resting 2 s to send or transmit data packet and then moves forward in the same way. The data traffic is generated by 20 constant bit rate (CBR) sources with sending rates of single 64 bytes every 2 s. The radio propagation range and data rate are set to 50 m and 2 Mbit/s, respectively. The parameters are shown in Table 1.

The simulation is run for 600 s each time. We run each simulation scenario 10 times to acquire the average values of

Table 1: Simulation parameters.

Parameters	Value
Simulation range	600 m × 600 m
Node's number	100
Max speed	10 m/s
Min speed	0 m/s
Propagation range	50 m
Data rate	2 Mbit/s
Node moving time	3 s
Node rest time	2 s
Simulation time	600 s

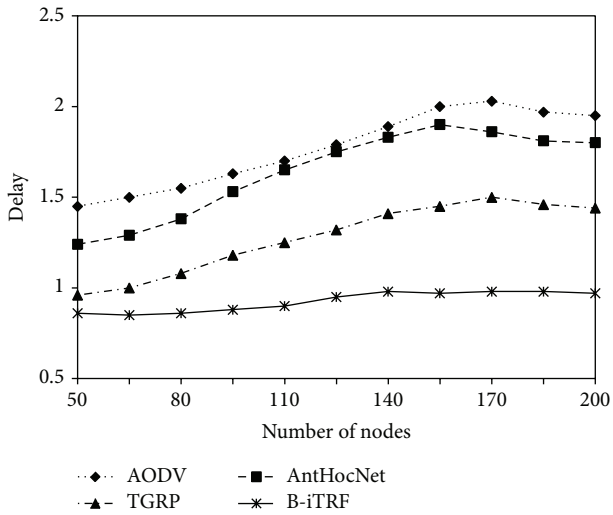

Figure 5: Delay versus number of nodes.

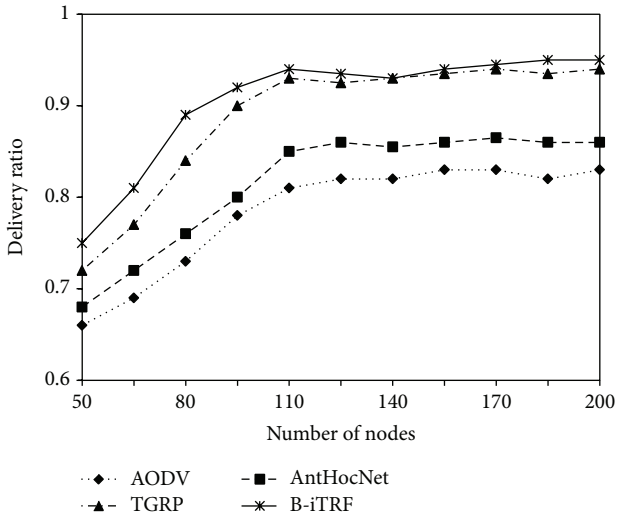

Figure 6: Delivery ratio versus number of nodes.

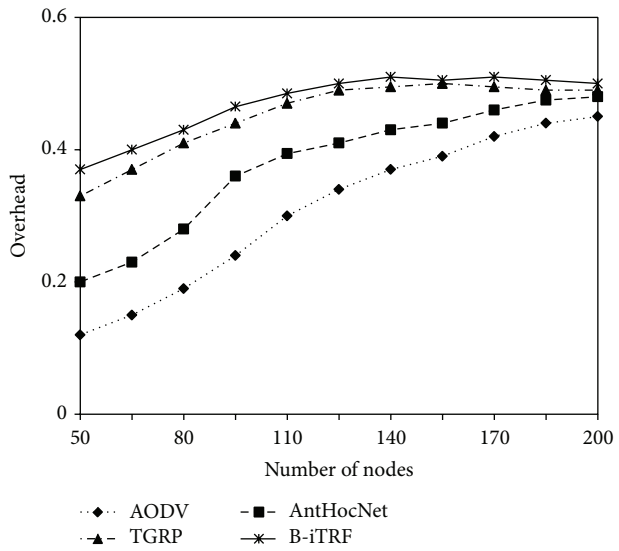

Figure 7: Overhead versus number of nodes.

results and compare them. The results and analysis are shown as follows.

Figure 5 shows end-to-end delay versus number of nodes when the ratio of malicious nodes is 8%. 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-iTRS and TGRP can deal with malicious nodes, their end-to-end delays are much better than those of AODV and AntHocNet.

Figure 6 shows end-to-end delivery ratio versus number of nodes when the ratio of malicious nodes is 8%. 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, the delivery ratio will keep a stable value approximately. Since B-iTRS and TGRP adopt security mechanism, their delivery ratios are similar and greater than those of AODV and AntHoc.

Figure 7 shows overhead versus number of nodes when the ratio of malicious nodes is 8%. 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-iTRS needs to deal with neighbors' trusts and Sink feedback, its control overhead is greater than that of TGRP which only needs to deal with trust.

Figure 8 shows end-to-end delay versus 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-iTRS and TGRP can deal with malicious nodes, their end-to-end delays are similar.

Figure 9 shows delivery ratio versus 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

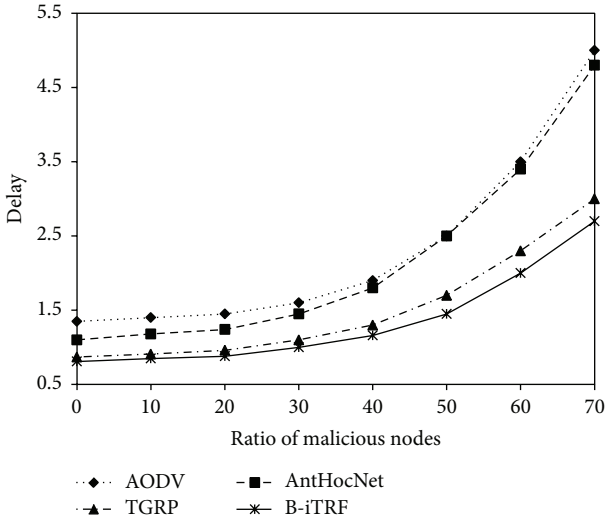

Figure 8: Delay versus ratio of malicious nodes.

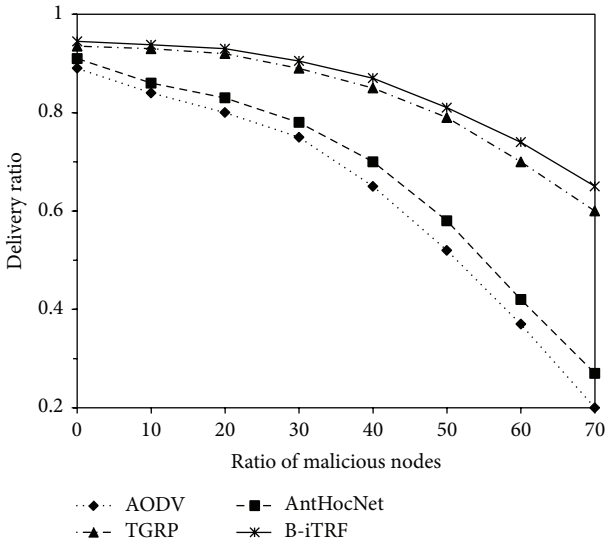

Figure 9: Delivery ratio versus ratio of malicious nodes.

value, the two delivery ratios will decrease rapidly. Since both B-iTRS and TGRP adopt security mechanism, their delivery ratios are similar and decrease slowly.

6. Conclusion and Future Work

In this paper, we present B-iTRS, a trusted routing scheme based on bio-inspired method. B-iTRS uses perceptive ants to reactively maintain the route table, where the link status metrics are sensed by perceptive ants to support path finding. Then, B-iTRS uses PAO to select the optimal route from multiple routes. In fact, B-iTRS is devoted to combining the advantages of both ACO and PAO to improve the effective performance, which is verified by simulation results. The proposed scheme can be used in both WSNs and MANETs scenario. In future work, we consider extending link status metrics (e.g., interference, energy) and introducing actual mobility model of nodes into B-iTRS to make it fit in with real WSNs environment.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work is partially supported by the National Natural Science Foundation of China (NSFC) under Grant no. U1404611, no. U1204614, and no. 61370221 and by the key project of the Education Department of Henan Province under Grant no. 14B520031, in part by Program for Science & Technology Innovative Research Team in University of Henan Province under Grant no. 14IRTSTHN021, and in part by the Program for Science & Technology Innovation Talents in the University of Henan Province under Grant no. 14HASTIT045.

References

[1] G. Zhan, W. Shi, and J. Deng, "Design and implementation of TARF: a trust-aware routing framework for WSNs," *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 2, pp. 184–197, 2012.

[2] X. Yin and J. Yang, "Shortest paths based web service selection in internet of things," *Journal of Sensors*, vol. 2014, Article ID 958350, 10 pages, 2014.

[3] W. Guo, R.-Z. Xu, and B. Liu, "Research on subjective trust routing algorithm for mobile ad hoc networks," in *Proceedings of the 6th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '10)*, September 2010.

[4] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 169–183, 2012.

[5] D. Dasgupta, S. Yu, and F. Nino, "Recent advances in artificial immune systems: models and applications," *Applied Soft Computing Journal*, vol. 11, no. 2, pp. 1574–1587, 2011.

[6] J. Rao and A. O. Fapojuwo, "A battery aware distributed clustering and routing protocol for wireless sensor networks," in *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '12)*, pp. 1538–1543, April 2012.

[7] O. Yang and W. Heinzelman, "Sleeping multipath routing: a trade-off between reliability and lifetime in wireless sensor networks," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '11)*, pp. 1–5, Houston, Tex, USA, December 2011.

[8] G. Trajcevski, F. Zhou, R. Tamassia, B. Avci, P. Scheuermann, and A. Khokhar, "Bypassing holes in sensor networks: load-balance vs. latency," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '11)*, December 2011.

[9] 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, 2012.

[10] M. Gunes, U. Sorges, and I. Bouazizi, "ARA—the ant-colony based routing algorithm for MANETs," in *Proceedings of the International Conference on Parallel Processing Workshops*, pp. 79–85, August 2002.

[11] G. Di Caro, F. Ducatelle, and L. M. 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, 2005.

[12] 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, 2007.

[13] K. Li, C. E. Torres, K. Thomas, L. F. Rossi, and C.-C. Shen, "Slime mold inspired routing protocols for wireless sensor networks," *Swarm Intelligence*, vol. 5, no. 3-4, pp. 183–223, 2011.

[14] M. Zhang, C. Xu, J. Guan, R. Zheng, Q. Wu, and H. Zhang, "P-iRP: physarum-inspired routing protocol for wireless sensor networks," in *Proceedings of the IEEE 78th Vehicular Technology Conference (VTC '13)*, September 2013.

[15] 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.

[16] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '99)*, pp. 90–100, IEEE, New Orleans, La, USA, February 1999.

[17] Y. Ren, V. I. Zadorozhny, V. A. Oleshchuk, and F. Y. Li, "A novel approach to trust management in unattended wireless sensor networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 7, pp. 1409–1423, 2014.

[18] I.-R. Chen, F. Bao, M. Chang, and J.-H. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 5, pp. 1200–1210, 2014.

[19] J. S. Priyanka, S. Tephillah, and A. Balamurugan, "Malicious node detection using minimal event cycle computation method in wireless sensor networks," in *Proceedings of the International Conference on Communications and Signal Processing (ICCSP '14)*, pp. 905–909, April 2014.

[20] S. Indhu Lekha and R. Kathiroli, "Trust based certificate revocation of malicious nodes in MANET," in *Proceedings of the IEEE International Conference on Advanced Communication Control and Computing Technologies*, pp. 1185–1189, May 2014.

[21] X. O. Wang, W. Cheng, P. Mohapatra, and T. Abdelzaher, "Enabling reputation and trust in privacy-preserving mobile sensing," *IEEE Transactions on Mobile Computing*, vol. 13, no. 12, pp. 2777–2790, 2014.

[22] 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 *Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC '13)*, pp. 4522–4527, April 2013.

[23] L. Abusalah, A. Khokhar, and M. Guizani, "A survey of secure mobile Ad hoc routing protocols," *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 78–93, 2008.

[24] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," *Mobile Computing*, vol. 353, pp. 153–181, 1996.