Int. J. Communications, Network and System Sciences, **2010, 3, 689-696**
doi:10.4236/ijcns.2010.38092 Published Online August 2010 (http://www.SciRP.org/journal/ijcns)

MRBCH: A Multi-Path Routing Protocol Based on Credible Cluster Heads for Wireless Sensor Networks

Yang Yang, Enjian Bai, Jia Hu, Wenqiang Wu
College of Information Science & Technology, Donghua University, Shanghai, China
E-mail: baiej@dhu.edu.cn

Received April 26, 2010; *revised June* 3, 2010; *accepted July* 7, 2010

Abstract

Wireless sensor networks are widely used for its flexibility, but they also suffer from problems like limited capacity, large node number and vulnerability to security threats. In this paper, we propose a multi-path routing protocol based on the credible cluster heads. The protocol chooses nodes with more energy remained as cluster heads at the cluster head choosing phase, and then authenticates them by the neighbor cluster heads. Using trust mechanisms it creates the credit value, and based on the credit value the multi-path cluster head routing can finally be found. The credit value is created and exchanged among the cluster heads only. Theoretical analysis combined with simulation results demonstrate that this protocol can save the resource, prolong the lifetime, and ensure the security and performance of the network.

Keywords: Wireless Sensor Network, Clustering, Multi-Path Routing, Credit Value

1. Introduction

Wireless sensor networks (WSNs) develop rapidly in recent years. As an intelligent and private network, WSNs consist of a large number of specific sensor nodes which cooperatively realize desired functions through self-organized wireless communication. Because of the flexibility in arrangement as well as the less effort demanded for maintenance, WSNs have exhibited promising applications in many fields like military, healthcare, environmental applications, etc [1,2].

In spite of the great application potential, there also exist some problems concerning WSNs [3]. For example, most of the traditional routing protocol, with minimum hop number as the goal in routing optimization, would give malicious nodes chances to distort the number of hops. Besides, the nodes in WSNs are thought to be confined by available energy, computational effort, memory, and communication range. To assure the security, we must design an efficient routing protocol algorithm to defend the network against attack.

The elements and protocols of a well designed WSN must be prepared to cope with problems from faulty nodes and malicious entities. Most of the routing protocols presently used in WNSs, however, cannot fulfill this requirement. The problem originates from the use of single-path routing in these protocols. In single-path routing, if authentication between two communicating nodes cannot be established or verified due to malicious activity or network problems, then the utilized path cannot be used to route packets from source to destination. The route maintenance phase must be initialized in order to establish a new route and support packet exchange. Such detriments can be eliminated by using multi-path routing, which enhances the security of WSNs with respect to single-path routing.

WSNs usually consist of a large number of nodes. Because of the greater node number and distribution density of WSNs than that of Ad-hoc networks, clustering is of much importance in the WSNs. LEACH [4] is a commonly referenced clustering algorithm. In each round, cluster head nodes (CHs) are randomly selected according to the CHs selection algorithm, and the remaining nodes, belonging to certain clusters, are able to route sensed data back to the base station through CHs. While many routing protocols especially the multi-path ones often overlook the importance of clustering. Generally, WSNs can be attacked by selective forwarding, Sybil attacks, Sinkhole attacks and Wormhole attacks. All of these attacks threaten the net by means of malicious nodes.

In [5], N. Nasser and Y.F. Chen propose a secure and energy-efficient multi-path routing protocol called SEEM. In SEEM the routing path is selected by the base station instead of the source or sink node. Therefore, whatever the adversity advertises, it has no impact on routing path selection and cannot attract traffic through itself.

The protocol considers the base station definitely safe and reliable, while it is not true for WSNs. Once the base station is invaded, the entire network will be affected. In [6], I. Khalil and S. Bagchi propose a secure routing protocol, achieving routing security by detecting the malicious node and isolating them from the network. In [7], Suk-Bok Lee and Yoon-Hwa Choi present a secure alternate path routing. These two methods use the detect system for each node, and malicious nodes account a small percent, but they also make calculations a heavy burden for WSNs. In [8], S. Madria and J. Yin propose a mechanism to defend the network against wormholes. The neighboring nodes exchange their neighbor lists for detecting wormhole connection. This method achieves a safe routing to a certain extent, but it is only effective against wormhole attacks. In [9], R. Mavropodi and P. Kotzanikolaou propose a protocol that hides the address of nodes in the routing and authenticates nodes with the single hash function. The algorithm transfers data as soon as the first route is established, and then keeps looking for other alternative paths. By such means, this algorithm saves time, but may not be a good choice when a securer path is wanted.

In this paper, inspired by the above related work, we propose a multi-path routing protocol based on the credible cluster heads which we call MRBCH. The MRBCH is based on a clustered WSN with reputation of the CHs, it introduces a trust setup strategy running on the nodes which are selected as the CHs. If the CHs are credible or not is important, CHs are responsible for relaying and aggregating local data sent by cluster members back to the base station. Once some CHs are malicious or are detected as malicious, the entire WSN is endangered. By evaluating and storing the reputation of the CHs, it is possible to calculate the degree by which those nodes can be trusted. After clustering, the CHs will be evaluated by its neighboring CHs, and create trust value in terms of the delay factor and packet loss rate. At last routing path is selected periodically from multi-path based on the trust value of CHs. This protocol ensures security by combining the multi-path and CHs certification. And only cluster head nodes are planned to be authenticated in each round.

The remaining part of this paper is organized as follows. Section 2 describes the trust management system which is used to evaluate the CHs. The MRBCH protocol is introduced in Section 3, and detailed analysis on this protocol is given in Section 4. Section 5 describes the simulation model and provides the performance evaluation results on the protocol. Section 6 gives the conclusion.

2. Trust Management System

In WSN data transmission security relies on the safety of communication link and the credibility of nodes. When the available data are traveling to destination, we need to assure that the received data have been sent by a reliable node. In this phase, trust management system for CHs is adopted to assess the trust level from one CH to another.

2.1. Evaluation of Trust Degree

CHs start a trust mechanism right after clustering in each round. We don't evaluate every sensor nodes but the CHs, and describe how much CHs i trust on its neighbor CH j by the trust degree T_{ij}. T_{ij} is managed in terms of two parameters: the delay factor τ and packet loss rate l_p, which are defined as the following.

Delay factor τ is denoted by $\imath$-queue, the length of queue we get from the queue monitor. Here, the queue members are the forwarding packets waiting to be transferred to the CH. The bigger the number of the waiting packets is, the bigger the delay factor τ is. Considering that malicious CH nodes cheat for forwarding packets as much as possible by scattering false routing information and forging identity, even a normal CH with large τ is not a good choice for routing. Thus delay factor τ is taken into consideration.

The packet loss rate is defined as

$$l_p = \frac{N_f - N_r}{N_f} \tag{1}$$

where N_f is the number of packets sent to node, N_r is the number of the packets actually received by the node. The packet loss rate tells that the CH may attack the net by dropping packets.

Utilizing the parameters above, T_{ij} is defined as

$$T_{ij} = \alpha * (1 - l_p) + \beta *(1/\imath - \text{queue}) \tag{2}$$

where the weight factors α and β is positive, with $\alpha + \beta = 1$. In this paper, we consider the two parameters effect the network at the same level. So both of α and β are taken to be 0.5. T_{ij} is in the range [0, 1], with 0.5 as the initial value.

2.2. Mergence of Trust Degree

When the trustee CH wants to evaluate the neighbor CH, it can not only rely on its own trust on the nodes. The trust evaluation for a CH comprises a direct trust degree and an indirect trust degree. The direct trust degree is calculated by the trustee CH. The indirect trust degree is derived from the direct trust degree calculated by the common neighbor CH of the trustee CH and the node under evaluation. The relationship between these nodes is shown in **Figure 1**. The trustee node gets the trust degree, both direct and indirect, from its neighbor nodes, and integrates them to get a trust value for the node under evaluation.

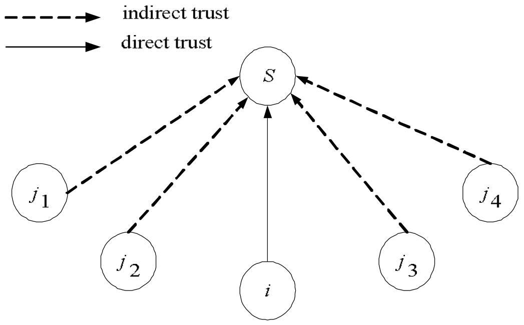


Figure 1. The relationship among nodes for evaluating the trust degree.

In **Figure 1**, *S* is the trustee CH, *i* is the CH under evaluation, j_1, j_2, j_3,…, j_n, as recommenders that provide trust degree about *i* to *S*, are common neighbor CHs of *S* and *i*. After getting all the trust degrees about *i* from its neighbor nodes, *S* evaluates the trust value for *i* by giving a global reputation value from the local reputation value using the weighted average method [10]. The trust value of *i* on *S* is

$$V_{si} = \frac{\sum_j w_j \times t_{ji}}{\sum_j w_j} \tag{3}$$

where t_{ji} is the trust degree, *j* is the common neighbor CH of *S* and *i*, and w_j is a positive weight factor. In this paper the weight factor w_j is equal to the trust degree of *i* calculated by *S*

$$w_j = t_{sj} . \tag{4}$$

Now that the trust value is derived according to the trust degrees from more than one CH, if the malicious node wants to forge or alter the trust degree, they can not change the trust value much.

3. MRBCH: The Proposed Protocol

3.1. The Network Model

If we suppose sensor nodes are thrown by an aircraft to the target area, their positions would be random in the network area. We make the following assumptions.

1) All the sensor nodes are static. Mobility is not supported in MRBCH. In many applications of WSN, the mobility is not mandatory. Thus this assumption is feasible to these applications and the communication range of these nodes is a circular area with radius *R*.

2) All sensor nodes are identical, with the same initial energy. And each node consumes the same level of energy for transmitting and receiving one packet.

3) The link is symmetric. It mainly involves bidirectional communication between the nodes.

3.2. Cluster Formation

The algorithm divides all nodes in the region into several clusters.

1) Firstly, choose the nodes near BS to be CHs to balance the network loading. Base station selects a communication radius R_{bs}, within which range the nodes can receive the information. These nodes automatically upgrade to be CHs. Because CHs have the responsibility of sending data to BS, the CHs near the BS have much more transmitting tasks than those far away from the BS. Disposing more CHs near BS is helpful in balancing the network loading.

2) Secondly, choose the rest CHs according to the LEACH clustering algorithm. As some nodes are selected in step (1) as CHs, the other ones become candidates. In order to give priority to the nodes with higher remaining energy, current energy of the node is involved in the LEACH method. The probability for a node to be chosen as CH in the current round is described by a quantity *T*, which satisfies

$$T(n) = \begin{cases} \dfrac{p}{1-\left(r \bmod \dfrac{1}{p}\right)} \cdot \dfrac{E_{n-current}}{E_{n-\max}}, & n \in G, \\ 0, & otherwise. \end{cases} \tag{5}$$

where *p* is the percentage of CHs in all nodes, *r* is the current round, $E_{n\text{-}current}$ is the current energy of the node, $E_{n\text{-}\max}$ is the initial energy of the node, and *G* is the group of nodes not chosen as CHs. Once a node is selected as CH, its *T*(*n*) is reset to 0, so that this node will not be reselected.

3) After that, the CHs broadcast ADV message (advertisement message) within a communication radius *R*. The nodes which receive such message become the cluster members of the corresponding CH. Once a node have received ADV message and chosen its cluster, it will refuse to receive other ADV message again. When cluster formation is done, the CHs start the credit evaluation on each other by detecting the neighbor CHs' acts. Credit value will be recorded on the list of the neighbor CHs. The net topology is shown in **Figure 2**.

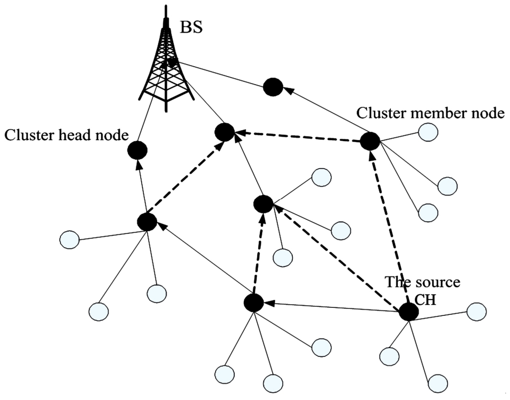


Figure 2. The net topology.

3.3. Trust Value Establishment

Trust value establishment takes place right after the clustering. At this stage, we present a CHs neighbor discovery process, then compute the trust value of CHs' neighbor according to the trust management system described in Section 2, and finally construct neighbor trust value list for each CH.

1) To start the neighbor discovery process, each CH in the network broadcasts a ND (Neighbors Discovery) message. Each CH receiving this message stores in the neighbor-list the ID, in ascending message-received-time order, of the current CH that sends the message. Once a message is received, this ND is dropped and not re-broadcast.

2) After neighbor discovery is completed, trust degree evaluation starts according to the procedure given in Subsection 2.1. Then each CH broadcasts another message NTC (Neighbor Trust value Collection), with its neighbor CHs' list included. CHs that receive NTC would compare the list of the source CH's neighbor CHs with their own list, thus common neighbor CHs are found. After that, they send a NTCR (Neighbor Trust value Collection Reply) with the ID and trust degree of their common neighbor CHs.

3) When the source CH receives the NTCR from its neighbors, it gets the trust degree about them at the same time. With this information CH can generate a matrix about trust degree. Using the Formula (3), the source CH computes the trust value about its neighbors, arranges them in the list in ascending order, and finally reserves the top 3 in the list. **Figure 3** gives an overview of the trust value establishment.

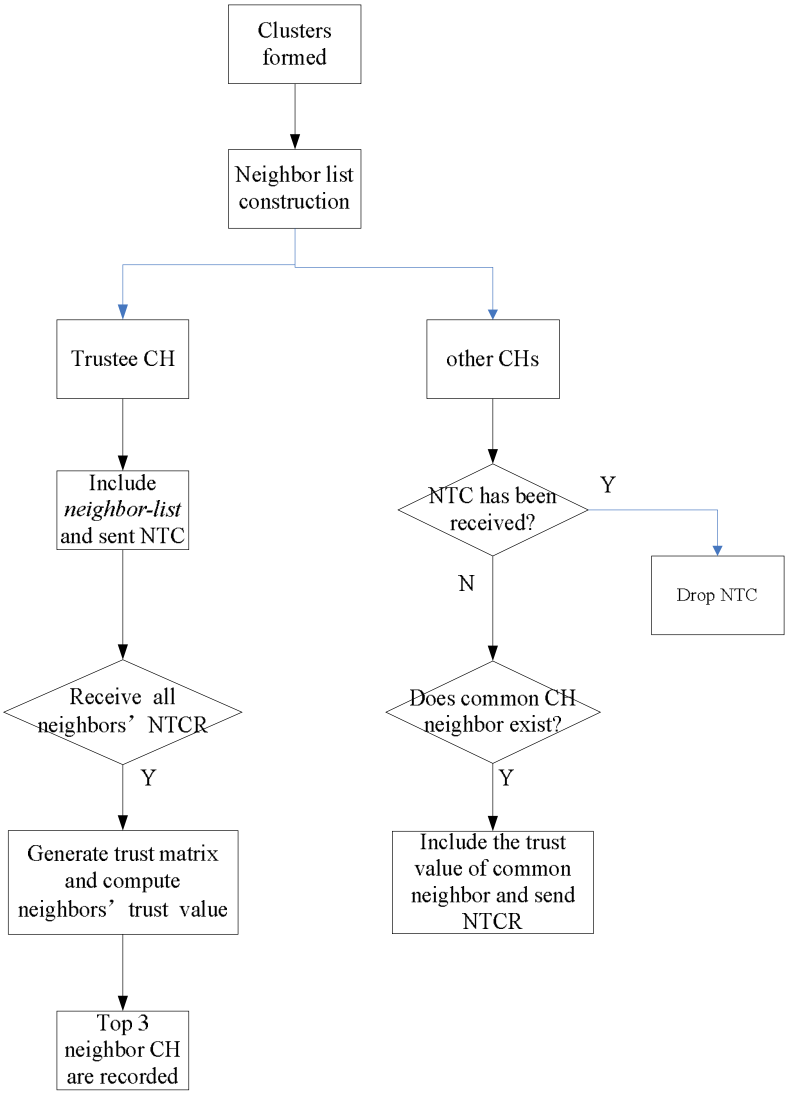

Clusters formed
Neighbor list construction
Trustee CH
other CHs
Include *neighbor-list* and sent NTC
NTC has been received?
Y
Drop NTC
N
Receive all neighbors' NTCR
Does common CH neighbor exist?
Y
Y
Generate trust matrix and compute neighbors' trust value
Include the trust value of common neighbor and send NTCR
Top 3 neighbor CH are recorded

Figure 3. Establishment of trust value.

3.4. Route Setup

When the source CHs *S* have data to transfer, *S* sends a route request RREQ (route request) around the neighbor CHs by broadcasting. Route setup follows three steps:

Step 1 The source CH *S* sends its neighbor CHs list in RREQ. If the CH that receives the RREQ is in the list, which means this CH is among the top 3 trusted neighbor CHs of *S*, it would send a RREP (route reply) and update the reverse route. Otherwise, it would drop the RREQ.

Step 2 Once *S* receives RREP from the top 3 nodes in the list, it sends the confirmation message. CH that receives the confirmation message goes to step 1 to reselect the next hop node. Steps 1 and 2 are repeated until the RREQ reaches the BS.

Step 3 The CHs which get the RREP from the BS go back to *S* with the intermediate node information. Because there are more than one safe path from the source node to the BS, *S* chooses the first arrived routing path for data transmission. **Figure 4** gives an overview of the route discovery process of MRBCH.

3.5. Route Maintenance

During the route setup, if the trust value of some CH is lower than threshold *Trust-lim*, the node is taken as malicious. The trustee node requests the BS to cancel its cluster head status, and select other to take place. When trust values of two nodes are found equal, the node with bigger ID will be chosen into the next hop.

After the data transmission phase, a round is done. When a new round starts, CHs are reselected. So the trust values update dynamically in each round. Even if malicious nodes are involved in data transmission, it only affects one round.

4. Security and Performance Analysis

1) *Energy Conservation.* First of all, we improve the cluster head election algorithm based on the classical algorithm LEACH. The remaining energy of nodes is taken into consideration. Optimal clustering prolongs lifetime of the network. Secondly, we evaluate the CHs. Usually the CHs account for 5%~10% of the nodes. Compared with the previous method, computational costs are largely decreased in the present treatment.

2) *Defending Wormhole and Sinkhole.* Both Wormhole and Sinkhole attacks try to lure traffic from sensor nodes to BS through the attacker or compromised nodes, essentially. If CHs are disguised by malicious nodes, or

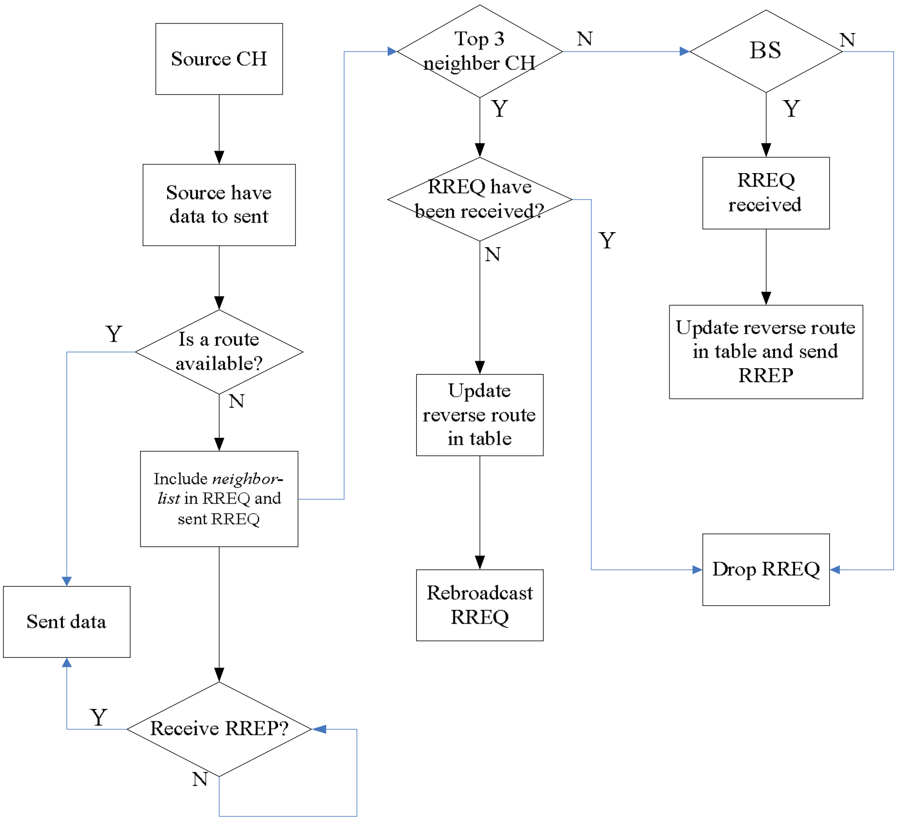


Figure 4. Route discovery process of MRBCH.

captured to be malicious nodes, they are more damageable than the normal ones. Therefore, trust mechanism is introduced to evaluate the CHs, according to delay factor. The length of the queue of the waiting nodes is taken into consideration to balance the network load. The trust mechanism make sure sinkhole and wormhole created by luring messages don't exist.

3) *Defending Selective Forwarding Attacks.* In Selective forwarding attacks, malicious nodes reuse to forward all or part of the messages and simply drop them so they are not propagated any further. Selective Forwarding attacks threaten the net also through the malicious nodes. Trust mechanism is jointly used to evaluate the CHs by packet loss rate. The value of packet loss rate tells whether the node attacks the net by dropping messages. One route request leads to more than one routing paths for data transfer. For any reason if the path is down, we can always fix it. Even if malicious nodes happen in the routing path, the attack will only lasts a limited time.

5. Simulations

We simulate the proposed routing protocol on OMNeT++ platform and the environment settings are shown in **Table 1**.

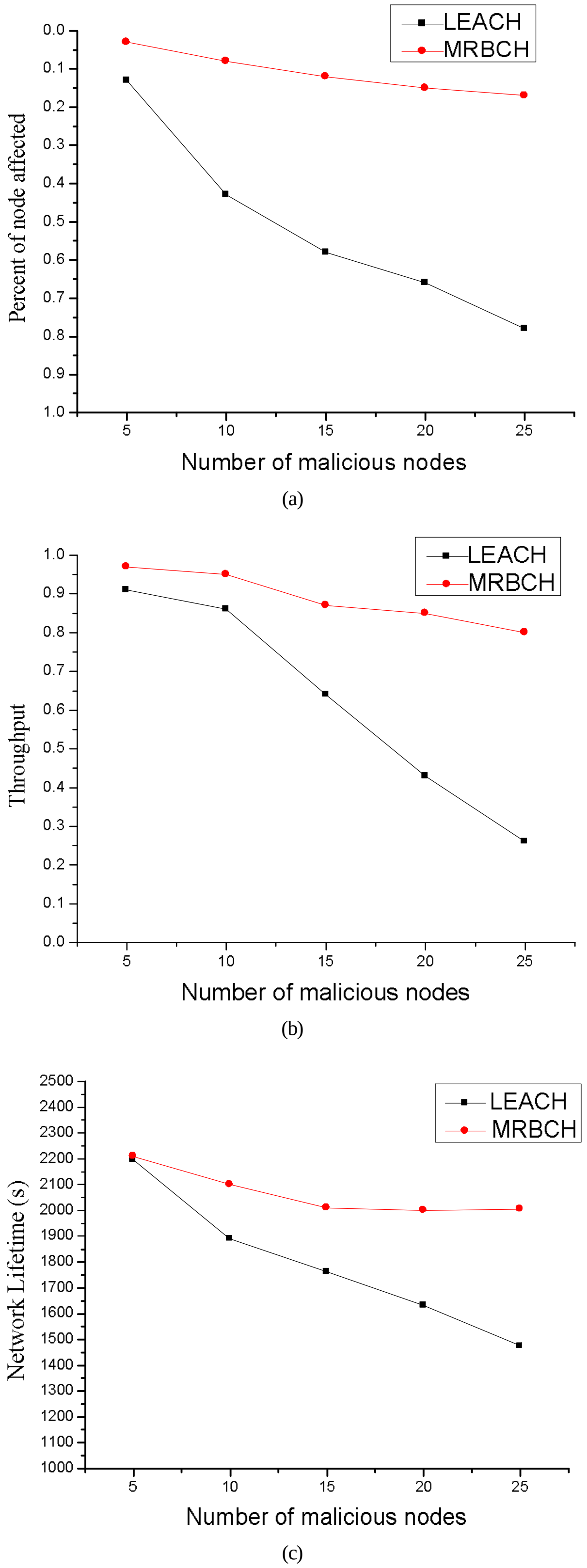
The experiment consists of 100 wireless nodes. We compare the performance of our protocol MRBCH with that of the LEACH protocol [4]. In each of our tests, we study five conditions with the number of malicious nodes ranging from 5 to 25 increased by 5. Network lifetime and Throughput are used as evaluation measures. The former is defined as the time required before half of the nodes in the network fail, and the latter is the percentage of successfully received data packets by the BS.

From **Figure 5(a)** we can observe that MRBCH performs better than LEACH. In LEACH, once a malicious node is selected to be the CH, all the cluster nodes are affected. But in MRBCH, the CHs are identified by trust value. Those with the low values are kept out of the routing path. So the number of the affected nodes is controlled around the number of malicious nodes. From **Figure 5(b)** we can see that MRBCH has a high data delivery ratio and ratio decreases slightly as the number of malicious nodes increases. While the throughput for

Table 1. Simulation parameters.

Parameters	Value
WSN area ($L \times L/\mathrm{m}^2$)	100 × 100
Number of nodes (N)	100
Transmission power consumption	0.002*dist J
Reception power consumption	0.02 J
Data integration power consumption	0.005*clnr J
Initial energy	5 J

*dist is transmission distance, clnr is number of cluster nodes.



(a)

(b)

(c)

Figure 5. Comparing network performance between MRBCH and LEACH. (a) Average affected nodes; (b) Average network throughput; (c) Average network lifetime.

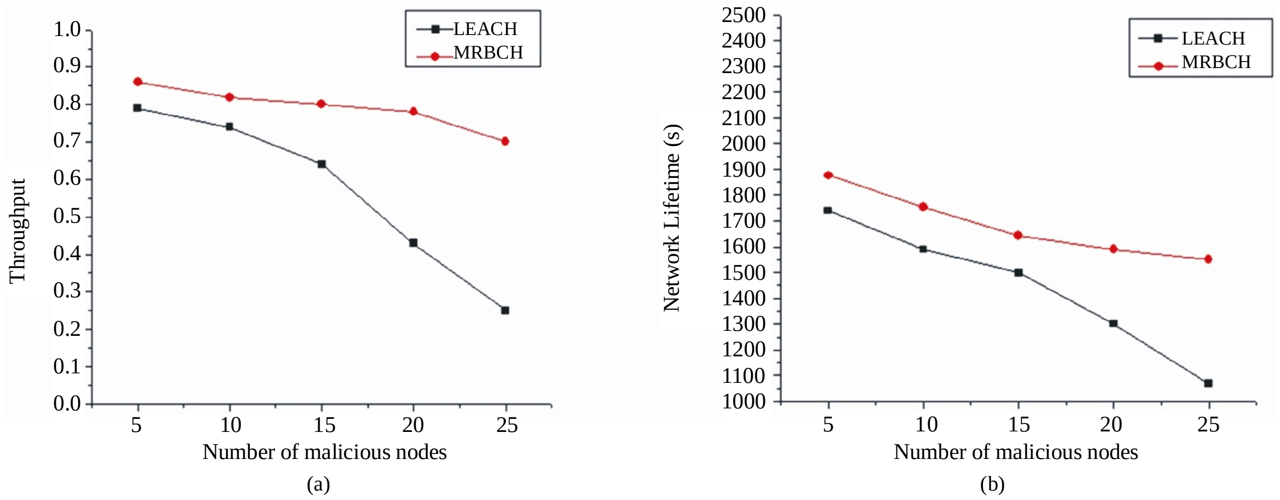


Figure 6. Comparing network performance between MRBCH and LEACH when 20% of the nodes misbehaving. (a) Average network throughput (20% of the nodes misbehaving); (b) Average network lifetime (20% of the nodes misbehaving).

LEACH decreases from 91% to 26%. In LEACH, if CHs are disguised by malicious nodes, or captured to be malicious nodes, they forward all or part of the messages even simply drop them. And MRBCH can detect this behavior and selects another path. The communication goes well and the throughput didn't affect too much.

Figure 5(c) shows network lifetime. For the 5 malicious-node case, no clear difference can be observed between MRBCH and LEACH. This is because MRBCH has to consume energy in calculation and transmit trust value. For the cases with more malicious nodes, LEACH has to spend a lot of energy on message retransmission. However, with trust mechanism and multi-path which defends the malicious nodes, in MRBCH the malicious nodes can be well distinguished and excluded out of network by other nodes. Further increasing the malicious nodes would induce little decreasing of the network lifetime.

Figure 6 is the simulation results when 20% of the nodes misbehave. From this figure we can see that performance of two metrics decrease more or less. The network throughput, as shown in **Figure 6(a)**, does not experience an obvious decrease in both protocols. For the network lifetime, both protocols suffer a decrease, while the lifetime of MRBCH is still 7~30% longer than LEACH because of the trust mechanism and multi-path routing.

6. Conclusions

Based on the credible cluster heads, we propose a multi-path routing protocol, which we call MRBCH, for WSNs. Unlike other routing protocols, MRBCH takes both energy-efficiency and security into consideration. MRBCH has the following advantages over other current routing protocols: 1) prolonged lifetime of the whole network by using multi-path route for data transfer, 2) the credit value is created and exchanged among the cluster heads exclusively, thus energy can be saved, 3) taking use of the multi-path cluster-head routing based on the credit value ensures a high-quality route. Simulation results and comparisons demonstrate that this protocol can save the network resources, increase the network lifetime, and ensure the network safety as well.

7. Acknowledgements

The authors would like to thank the anonymous reviewers and the work was supported by Shanghai Municipal Natural Science Fund under grant 10ZR1401400.

8. References

[1] K. Romer and F. Mattern, "The Design Space of Wireless Sensor Networks," *IEEE Wireless Communications*, Vol. 11, No. 6, 2004, pp. 54-61.

[2] C. F. Garcia-Hernandez, P. H. Ibarguengoytia-Gonzalez, J. Garcia-Hernandez and J. A. Perez-Diaz, "Wireless Sensor Networks and Application: A Survey," *International Journal of Computer Science and Network Security*, Vol. 7, No. 3, 2007, pp. 264-273.

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," *Proceedings of IEEE International Workshop on Sensor Network Protocols and Applications*, Alaska, 11-13 May 2003, pp. 113-127.

[4] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy Efficient Communication Protocol for Wireless Sensor Networks," *Proceedings of the Hawaii International Conference on System Sciences*, Maui, 4-7 January 2000, pp. 3005-3014.

[5] N. Nasser and Y. F. Chen, "Secure and Energy-Efficient

Multi-Path Routing Protocol for Wireless Sensor Networks," *Computer Communications*, Vol. 30, No. 11-12, 2007, pp. 2401-2412.

[6] I. Khalil, S. Bagchi, C. N. Rotaru and N. B. Shroff, "UNMASK: Utilizing Neighbor Monitoring for Attack Mitigation in Multi-Hop Wireless Sensor Networks," *Ad Hoc Networks*, Vol. 8, No. 1, 2010, pp. 148-164.

[7] S.-B. Lee and Y.-H. Choi, "A Secure Alternate Path Routing in Sensor Networks," *Computer Communications*, Vol. 30, No. 1, 2006, pp. 153-165.

[8] S. Madria and J. Yin, "SeRWA: A Secure Routing Protocol against Wormhole Attacks in Sensor Networks," *Ad Hoc Networks*, Vol. 7, No. 6, 2009, pp. 1051-1063.

[9] R. Mavropodi and P. Kotzanikolaou, "SecMR: A Secure Multi-Path Routing Protocol for Ad Hoc Networks," *Ad Hoc Networks*, Vol. 5, No. 1, 2007, pp. 87-99.

[10] S. Song, K. Hwang, R. Zhou and Y. K. Kwok, "Trusted P2P Transactions with Fuzzy Reputation Aggregation," *IEEE Internet Computing*, Vol. 9, No. 6, 2005, pp. 24-34.