Wireless Sensor Network, 2014, 6, 237-248
Published Online November 2014 in SciRes. http://www.scirp.org/journal/wsn
http://dx.doi.org/10.4236/wsn.611023

Scientific Research

Detection of Insider Selective Forwarding Attack Based on Monitor Node and Trust Mechanism in WSN

Yu Hu, Yuanming Wu, Hongshuai Wang

School of Optoelectronic Information, University of Electronic Science and Technology, Chengdu, China
Email: 903821402@qq.com, ymwu@uestc.edu.cn, 478284495@qq.com

Received 9 September 2014; revised 8 October 2014; accepted 7 November 2014

Abstract

The security problems of wireless sensor networks (WSN) have attracted people's wide attention. In this paper, after we have summarized the existing security problems and solutions in WSN, we find that the insider attack to WSN is hard to solve. Insider attack is different from outsider attack, because it can't be solved by the traditional encryption and message authentication. Therefore, a reliable secure routing protocol should be proposed in order to defense the insider attack. In this paper, we focus on insider selective forwarding attack. The existing detection mechanisms, such as watchdog, multipath retreat, neighbor-based monitoring and so on, have both advantages and disadvantages. According to their characteristics, we proposed a secure routing protocol based on monitor node and trust mechanism. The reputation value is made up with packet forwarding rate and node's residual energy. So this detection and routing mechanism is universal because it can take account of both the safety and lifetime of network. Finally, we use OPNET simulation to verify the performance of our algorithm.

Keywords

Insider Attack, Selective Forwarding, Trust Mechanism, Monitor Node, Secure Routing Protocol

1. Introduction

Wireless sensor network (WSN) is composed of a set of sensor nodes in the network. It has the features of self-organization, multiple-hop and limited energy resources, etc. In the WSN which is based on the center of data, because of jamming, collision and bad channel environment, the data packets which are far from the base station (BS) may lose or make mistakes in the route of being forwarded hop by hop. When the attacker intrudes the network, the forwarded data packets may be stolen, tampered, destroyed and discarded so that it makes more se-

How to cite this paper: Hu, Y., Wu, Y.M. and Wang, H.S. (2014) Detection of Insider Selective Forwarding Attack Based on Monitor Node and Trust Mechanism in WSN. *Wireless Sensor Network*, **6**, 237-248. http://dx.doi.org/10.4236/wsn.611023

rious damage to the network. The attack types to the network include insider attack and outsider attack, but insider attack [1] is hard to defense effectively.

The classic encryption [2] and authentication mechanism can only resist outsider attackers who steal the data or tamper the information and route. However, to the insider attack, after the attackers capture the normal nodes, they acquire the identity and encryption information and put the malicious nodes to destroy the network. The malicious nodes work in the network with the legal identity so that the method of encryption and authentication can't defense the insider attack. Therefore, an Intrusion Detection System (IDS) [3] should be injected in WSN as the second line of defense. Such a IDS works monitors the nodes which behave abnormally, then decides whether these nodes are malicious nodes according to their behaviors, and finally takes some measures to deal with these nodes.

Selective forwarding attack [4] is such a form of attack which is hardest to resist among various kinds of insider attacks. The malicious node drops all the forwarded packets to launch a black hole attack. This attack can be detected easily. However, the malicious node can launch the selective forwarding attack more intelligently and covertly, such as taking part of packet loss, periodic packet loss and intermittent packet loss in order to elude various detection mechanisms. If malicious nodes are more difficult to be detected or take us more time to find them, they will do more damage to the network. Thus, we have to find a more effective detection mechanism to remit the damage of the selective forwarding attack. This kind of security mechanism should have the following features:

1) During the lifetime of the network, it can detect the existence of the malicious nodes accurately and quickly as well as it can determine the type of attack. It should also indicate the location and ID of the malicious nodes.

2) After the security mechanism has inspected the malicious nodes, it should provide the feedback information to the network and update the routing, and reconsider the forwarding nodes and forward path.

3) In consideration of limited conditions of sensor nodes, the complexity of the design scheme should be lightweight. The scheme should try to reduce the communication cost and the node energy consumption in different working mode.

4) The proposed mechanism should try to solve the means of attack as more as possible not only a single type of attack. Otherwise, it is lack of value.

For selective forwarding attack, most of the existing solutions to them are based on monitoring mechanism and reputation value estimation. Different designing scheme has different idea and performance. The traditional watchdog [5] mechanism overhears the packets forwarded from node N to decide whether N is a malicious node. The system calculates the forwarding rate as reputation value to compare with an appropriate threshold. Ultimately, it can estimate whether node N has launched selective forwarding attack or not through the result of the comparison. Although the computation complexity of watchdog mechanism is ultra-lightweight and it meets the characteristics of WSN, it can resist very limited situations of attack. Only when a single malicious node intrudes in the network and the node launches a simple selective forwarding, watchdog can detect the malicious node successfully. However, if multiple nodes make collusion attack or one single node does other forms of attack, simple watchdog mechanism cannot defense effectively. Other methods are improved on the basis of the watchdog which can resist more forms of attack and all have their characteristics and advantages, but they also have some drawbacks.

In this paper, a scheme based on the monitor node managing the network and the watchdog mechanism is put forward referring to the characteristics of different defense mechanisms. Moreover, unlike general arithmetic based on static threshold, our algorithm is contained of dynamic threshold. The threshold is adjusted in real time according to the overall packet loss situation of the network so that the loss detection rate and false alarm rate can be decreased.

The paper's other paragraphs are as follows. Section II summarizes related work, elaborates and analyzes the advantages and disadvantages of some popular schemes against the attack. Our secure mechanism and network design is proposed in Section III. Section IV explains the ways of attack which can be solved by our secure scheme. Section V presents the simulation performance and interpretation of results. At last, we conclude the paper in Section VI.

2. Related Work

In this section, the related works against the insider selective forwarding attack are summarized specifically. Nowadays, to defense and reduce this kind of attack, the main solution includes watchdog, trust mechanism,

neighbor-based monitoring, multipath routing avoidance, multiple data flow scheme, etc. Such kinds of schemes show a good defending effect through continuous improvement. However, they are also hard to avoid exposing the defects of their own. So we should find a trade-off between their advantages and disadvantages in order to propose a more optimal scheme. We expound the characteristics of some mechanisms as following.

2.1. Watchdog

Watchdog monitoring mechanism was introduced by Marti *et al.* [5] to identify misbehaving nodes in wireless ad hoc networks. This scheme can be applied in WSN and it was the earliest trust mechanism which is the basis of many defense methods. In their approach, each sensor node has its own watchdog that monitors and records the behaviors of its one hop neighbors. The watchdog system of each node stores the routing table which is about the performance good or bad of the neighbor nodes. When the node M sends a packet to its neighbor node N, the watchdog of M verifies whether N forwards the packet toward the BS or not by using the sensor's overhearing ability.

The advantage of this kind of security mechanism is that the principle is simple, complexity is low and it adapts to the WSN completely. But this scheme can only solve limited conditions of malicious nodes packet dropping. It can just detect the behavior that a single node drops packet in the simple form, but it can't defend that more than two nodes collude to launch packet loss attack.

2.2. Trust Mechanism

On the basis of Watchdog scheme, Yu *et al.* [1] describe several representative approaches to build a trust model. In their paper, Bayesian approach, Entropy approach, Game-theoretic approach, and Fuzzy approach are proposed. Through the different algorithms, we convert the information which comes from the watchdog to statistical data in order to weigh the behavior of monitored node whether good or bad. The design of trust measurement is aimed at optimizing the condition of determining a forwarding node. We expect to choose the node whose all kinds of attributes are comprehensively perfect as the next-hop node.

Using different trust model, the reputation value of a node will be different. When the trust model is determined, we should set a reasonable threshold. If a node's reputation value below the threshold, it will be recorded as a malicious node. Moreover, depending on the WSN's trust mechanism, the detection of such malicious node will or will not be broadcast to the rest of the nodes and BS in the WSN.

2.3. Other Kinds of Defense Mechanism

1) Neighbor-based monitoring

Malicious node may be the intersection of several path, that is to say this kind of node may forward more than one source node's data. It can drop the data package of one or some node among those source nodes so that the estimation to this malicious node from each source node is different. Therefore, this kind of malicious node cannot be ruled out in time. Thus, a detection mechanism based on neighbor nodes monitoring was proposed. By listening to each other, each node takes statistics of the number of forwarded packets by neighbor nodes. Then, each node calculates the reputation values about its neighbor nodes. The information of all reputation values will be put together in order to compute each node's weighted credibility.

Several works [6] [7] that used neighbor-based approach have been introduced in order to mitigate selective forwarding attacks. Lu *et al*. [8] have proposed a neighbor-based monitoring mechanism. In their design, each node computes the trust value of its 1-hop neighbors based on their multiple behavior evaluation and builds a trust management so that it can confirm whether a node is a malicious node or not.

The benefit of this method is that we can find the captured node more accurately and faster through multiple nodes cooperation. However, there are some restrictions in these approaches. First, they do not describe how their approaches can counter a node's selective packet drops against source node. Secondly, because every node must overhear each other and calculate every neighbor node's trust value, it will need more communication overhead and computational cost. Thirdly, the conflict may take place when information is exchanged between each node.

2) Multipath-routing avoidance

No matter how optimizing the detection mechanism is, it always establishes on the situation that malicious nodes have already discarded a mass of data packets. Thus, if we want to make sure that the packets are for-

warded to the base station perfectly, we should let the packets avoid the malicious node. Karlof and Wagner [9] mentioned k disjoint multipath routing avoidance can completely defend against selective forwarding involving at most k compromised nodes. Several works illustrating that multipath routing defends against packet dropping attack can be found in [10] [11]. Although using this mechanism can make the information transmitted to BS more effectively, the communication cost is very high. Obviously, if there is k path, it will need k times communication overhead compared with a single path.

3) Multiple data flow

Similarly, Sun *et al.* [12] introduced multiple data flow scheme using multiple disjoint topologies. In this approach, a node sends its packets through one or more randomly chosen topologies among the pre-established multiple topologies to mitigate insider packet dropping. The theory of this scheme is similar to multipath routing avoidance, but there is some trade-off between communication consumption and the intension of avoidance function.

3. Network Design

In this section, combining with the advantages of watchdog algorithm and node monitoring mechanism in related work, we propose a new network scheme. We have designed a kind of local network security routing algorithm based on trust mechanism and monitor node. The monitor node overhears the forwarding rate and surplus energy of ordinary nodes, and weights the two factors as the composite reputation value of each node in order to determine the routing node.

3.1. Network Topology

1) In a certain range, a number of ordinary nodes which are used for gathering around data and forwarding information are sprinkled random and uniformly. 2) Then monitor nodes are sprinkled random and uniformly which are a certain percentage of ordinary nodes. For example, we set 10 monitor nodes for 100 ordinary nodes. That is to say, each monitoring node can regulate 10 common nodes. 3) Monitor nodes broadcast information around in turn with a settled communication radius, to attract the ordinary nodes nearby. Each monitor node owns its monitor area and member nodes. 4) According to the location to the sink node, monitor nodes acquire ID and allocate ID for each ordinary node in their area.

3.2. Monitoring Mechanism

In this mechanism, the head of forwarding packet should include the ID of source node, ID of forward node and ID of next-hop. When the packet is forwarded, the monitor node overhears the packet and just takes out the head information to achieve the ID information as the determination whether the monitored node's behavior is normal or not.

We mainly care about the design of local safety monitoring in network, and focus on the research about how to choose the node of the highest reputation value, how to detect and exclude the malicious node, how to set of threshold and other problems. The schematic diagram of local monitoring is in **Figure 1**.This picture shows the workflow of monitoring nodes which is like that, it overhears forwarding packets of ordinary nodes, then calculate the reputation value of all the monitored nodes in this area, and find the node with the highest reputation value. When the routing node is confirmed, if there is no collecting data task in this area, other nodes can move to hibernation mode in order to save some energy. The process of monitoring mechanism is in **Figure 2**. Monitoring nodes only read the data according to the structure of different packets, that is to say, they only read the information of packet's head. So it can reduce the resource consumption of monitoring nodes. And some security detection function can be carried out through testing the header information.

3.3. Setting of Reputation Value

The reputation value of each node is as follows:

$$\mathrm{Val}\left[\mathrm{node}_{\mathrm{id}}\right] = a * \mathrm{Pr}_{\mathrm{id}} + b * \mathrm{Power}_{\mathrm{id}} \tag{1}$$

Where $0 < a < 1$, $0 < b < 1$, $a + b = 1$.

The $\mathrm{Pr}_{\mathrm{id}}$ in Equation (1) is the trust value of this node. The trust value of a node may be different when we

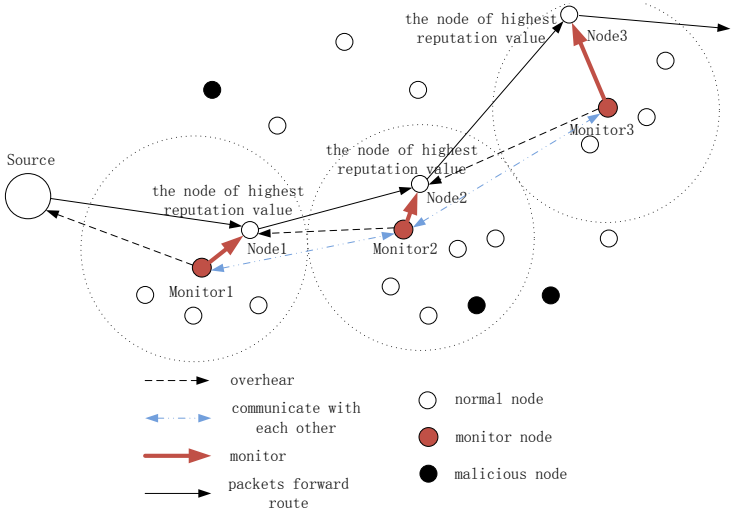


Figure 1. The local process of secure routing.

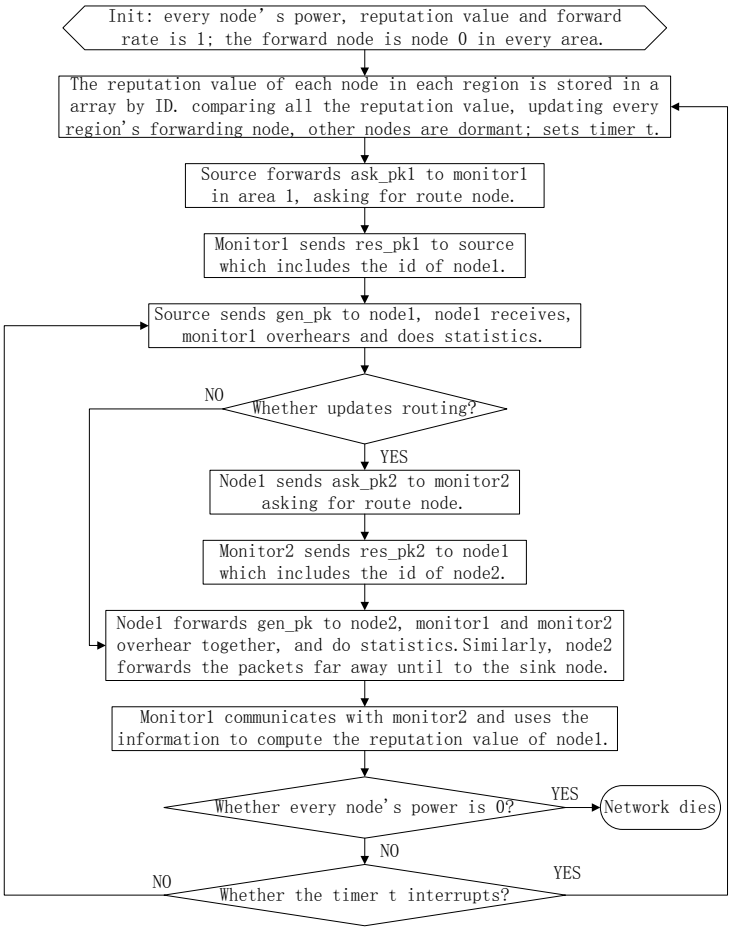


Figure 2. The process of monitoring mechanism.

use different trust models [12]. When a node is observed to forward the packet s times and drops the packet f times, the beta trust model will assign trust value Tr ($0 < Tr < 1$) to this node using the following formula:

$$Tr = (s+1)/(s+f+2) \tag{2}$$

Entropy trust model uses entropy function $H(p)$, whose input p is the trust value that can be obtained from beta trust model, to determine the trust value Tr. The entropy function:

$$H(p) = -p\log_2 p - (1-p)\log_2(1-p) \tag{3}$$

The trust value Tr ($-1 < \mathrm{Tr} < 1$) is defined by

$$\mathrm{Tr} = \begin{cases} 1 - H(p), \text{for } 0.5 \le p \le 1; \\ H(p) - 1, \text{for } 0 \le p < 0.5. \end{cases} \tag{4}$$

In our simulation, we use the beta trust model. In Equation (1), $\mathrm{Pr}_{id} = \mathrm{Forward\_pks}/\mathrm{Receive\_pks}$ is the forward rate of the node; Power_{id} is the node's residual energy; $\mathrm{Val}[\mathrm{node}_{id}]$ is composite reputation value of the node. Each monitor node calculates the reputation value of all nodes within its administering area and stores this information in an array. Then, the node of the highest value is selected as the routing node of this area. In order to ensure that monitoring node can listen to the general node, the radius of monitoring area should less than the quarter of normal node's forwarding radius.

- Routing node is updated periodically in order to prolong the network lifetime. Because the residual energy of nodes is taken into consideration, the node of high forward rate won't be overused. If some nodes of high credibility are overused, they will die prematurely so that the connectivity, cover degree and lifetime of network will decrease.

4. Function of Our Monitor Mechanism

According to the description of network in section Ⅲ, our secure routing protocol can not only accomplish the general sensor network' task about data collection and transmission, but also detect a variety of malicious nodes' internal selective forwarding in network. The secure mechanism can solve these ways of attack which are as the following conclusion.

4.1. Black Hole of One Node

When a normal node M is captured and becomes the malicious node, it can launch black hole attack. On the basis of Equation (1), due to the high node energy of black hole, M can achieve a high value, so that it will becomes the forwarding node. However, because M doesn't transmit packets, its forward rate will decline soon. After its forward rate is below the threshold T ($0 < T < 1$), it will be regarded as a malicious node by the monitor node. And the Val of M will be set at 0 so that M is excluded out of network.

4.2. Selective Forwarding Attack of One Node

Similar to the black hole attack, when the node N drops the received packets selectively, its general forward rate will decrease. If N's Val is below the threshold T ($0 < T < 1$), it will be regarded as a malicious node by the monitor node. This way of attack will need more time to be detected compared with black hole.

4.3. Colluding Attack of Multiple Nodes

As shown in **Figure 3**, the malicious node 1 forwards packets to malicious node 3 instead of normal node 2, and node 3 drops the packets. Because node 1 received m packets and sends m packets successfully, it attempts to deceive monitor node. However, according to the request of this routing algorithm, the packets must include the information about source ID, forward node ID and ID of next-hop. Whether node 2 receives packets is based on the head information from node 1's packet. If malicious node 1 changes the next-hop ID to node 3's ID, it will be caught by monitor node and be regarded as tampering the route.

This way of attack is similar to wormhole. With the control of monitor node, even though there is a high energy node attracting the packet stream, we don't change the route and follow the original route. Otherwise, if some node tampers the head information by itself, it will be regarded as malicious node.

4.4. Malicious Nodes Control the Transmitting Distance

As shown in **Figure 4**, malicious node 1 forward the received packets with small power, in order to control the

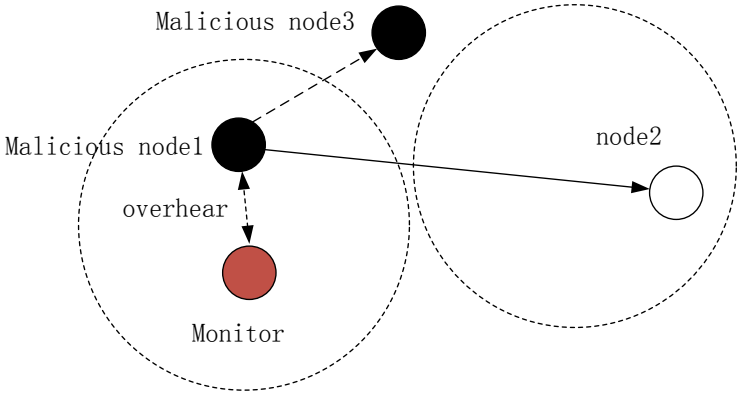


Figure 3. Colluding attack of multiple nodes.

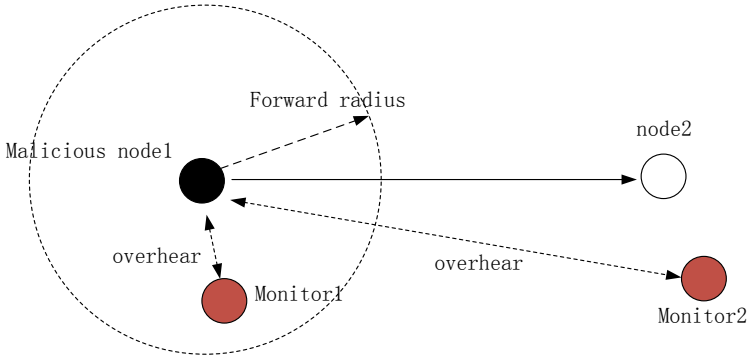


Figure 4. Malicious nodes control the transmitting distance to drop packets.

transmitting distance so that node 2 can't receive the packets. On the other hand, monitor 1 can hear the packets, so node 1 is aimed at cheat monitor 1 to achieve a high reputation value. However, both node 2 and monitor 2 can't receive the packets. After a period of time, monitor 2 will change some information with monitor 1. Monitor 1 hears m packets from node 1 and monitor 2 hears n packets from node 1. If the value of n/m is below a threshold t ($0 < t < 1$), node 1 will be regarded as a malicious node.

4.5. Trade-off of Energy Balance and High Forward Rate

In Equation (1) we can adjust the value a and b, in order to control the condition of becoming a high reputation node. So we can control the usage time of every node. That is to say, the characteristic of the network will be an energy balance one or the one of high forward rate according to the physical truth.

5. Simulation and Analysis

In this section, we use OPNET simulation to evaluate the performance of our trust monitor model and routing scheme. In our simulation, 100 sensor nodes and 10 monitor nodes are randomly distributed over a 100 m × 100 m area.

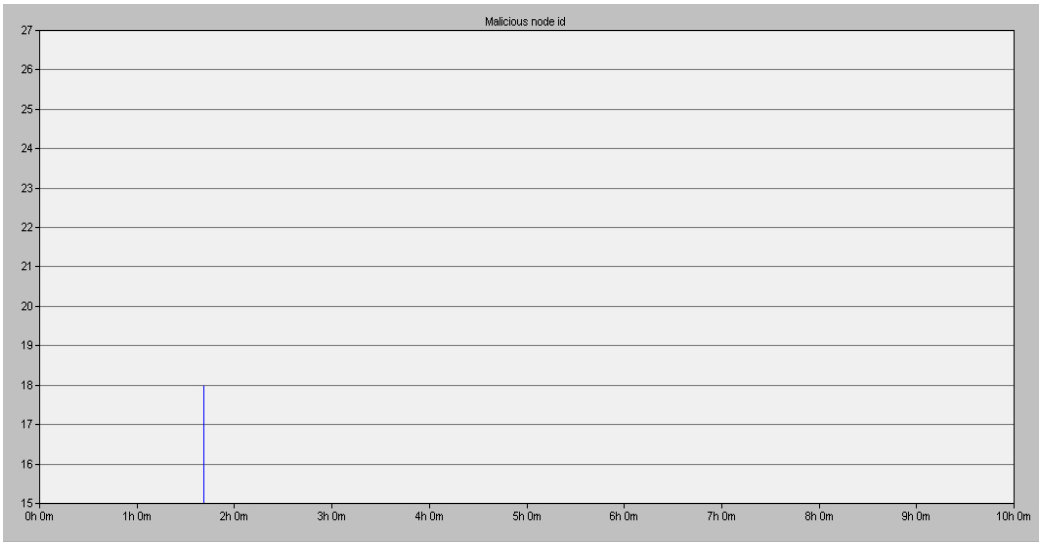
We only do the simulation of local network. A monitor node administrates 10 common nodes in each region. Firstly, the nodes will be numbered to meet the design requirements of the software. The size of node's ID is 1 byte (8 bits). The ID of source node is 00000000. The monitor node's ID in first region is 00000001. The ID of 10 common nodes within first region is from 00010000 to 00011001 (0001 indicates in region 1; 0000-1001 indicates 0-9). Therefore, the decimal ID of nodes in region 1 is from 16 to 25. Similarly, the ID of 10 nodes in region 2 is from 32 to 41. So every node in the network is numbered reasonably.

For each ordinary node in region 1, we set their forward rate respectively. The forward rate of node 16 and 24 is 70% - 90%; 20 and 25 is 80% - 90%; 19 and 21 is 80% - 100%; 22 is 65% - 85%. The node 18's init forward rate is 70% - 100%. After a certain number of turns, it will become a malicious node to launch selective forwarding attack with the forward rate of 30% - 50%.

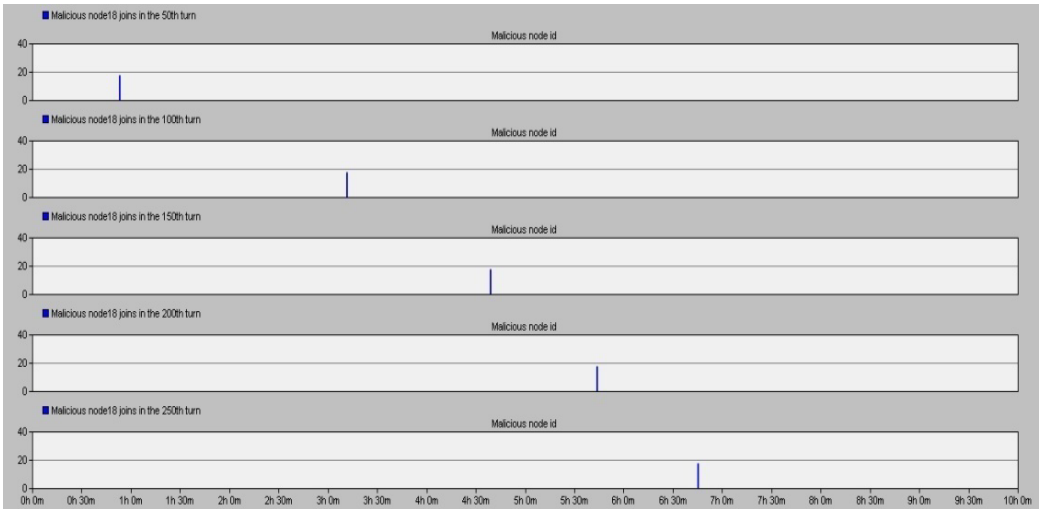
We assume that each node's initial energy is 1, and suppose that receiving a packet's energy consumption is 0.0001 and that sending a packet's energy consumption is 0.0003. It is 50 seconds each turn. That is to say, after requesting routing node, the source node sends packets at a speed of 2 packets per second for 20 seconds. At the same time, monitor node listens and forward node receives the packets. In the next 20 seconds, the forward node forwards the 40 packets random based on its forward rate; at the same time, the next-hop node receives the packets and monitor nodes listen and do some statistics and computation. There is 10s time for monitor node to calculate the reputation value of nodes and update the route node. Above is a turn of local data forwarding process and we cycle the process like that.

Suppose that node 18 turned to malicious node in 2000 s, its forward rate became 30% - 50%. As shown in **Figure 5(a)**, monitor node identified the malicious node, and showed the finding time and malicious node's ID. It's not hard to think of that if the normal node is captured later, it will cost more time to detect it out, because the node has performed well for a long time and established a relatively stable credibility. **Figure 5(b)** shows that the different finding time of node 18 which is captured in turn 50 (2500 s), turn 100 (5000 s), turn 150 (7500 s), turn 200 (10,000 s) and turn 250 (12,500 s). Therefore, the detection mechanism should be improved. If a node's forward rate is below the threshold three times continuously, it will be regarded as a malicious node.

In Equation (1), if value a is bigger enough than b, the nodes of high forward rate will always be selected



(a) Node 18 turned to malicious node in time 2000 s.

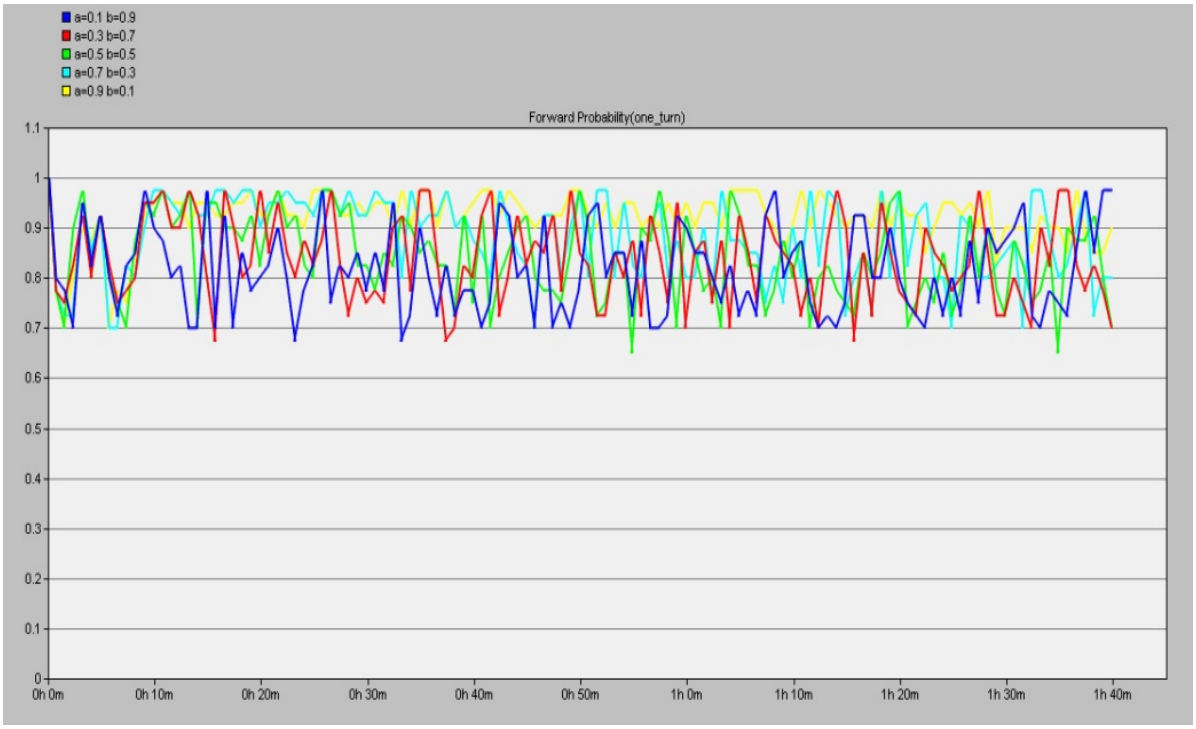


(b) Node 18 turned to malicious node in different time.

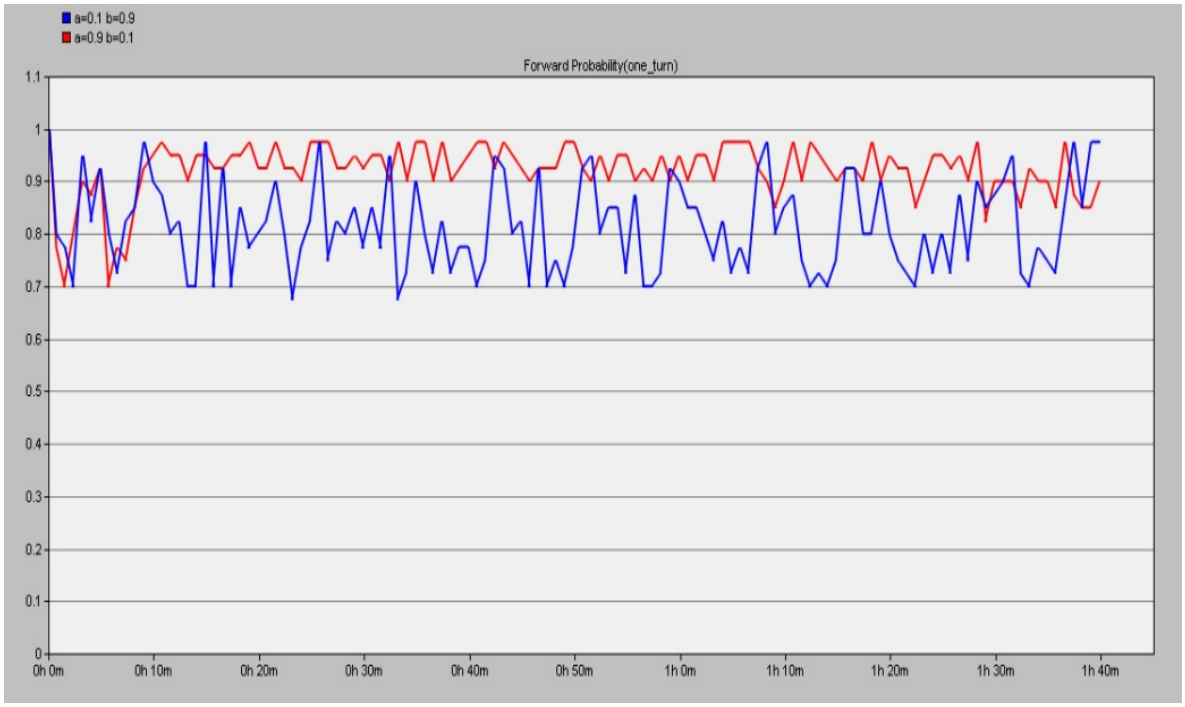
Figure 5. The time of detecting the malicious node 18.

as the forwarding nodes so that it will die soon. On the other hand, if a is bigger enough than b, the network will turn to an energy-balanced network. Every node will be used equally so that data forward rate of network is not stable. Thus, we should set a and b reasonably according to physical truth.

We don't put malicious nodes in the simulation. We get **Figure 6(a)** after the simulation of 6000 seconds



(a) Simulation with different value of a and b.



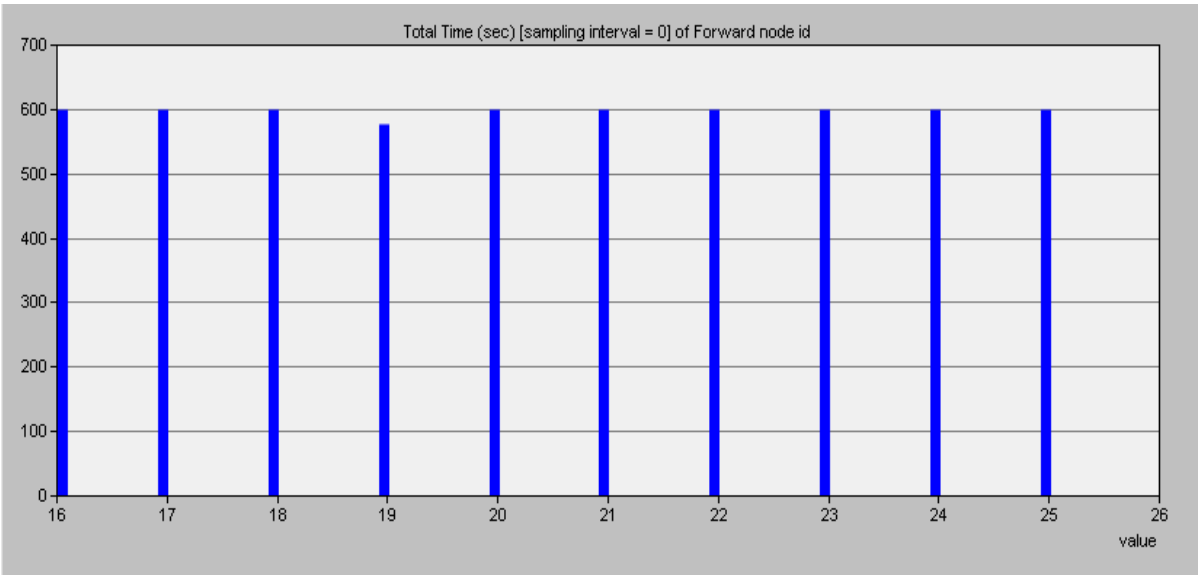
(b) Simulation when a = 0.1, b = 0.9 and a = 0.9, b = 0.1.

Figure 6. The changing of forward rate (one turn) over time.

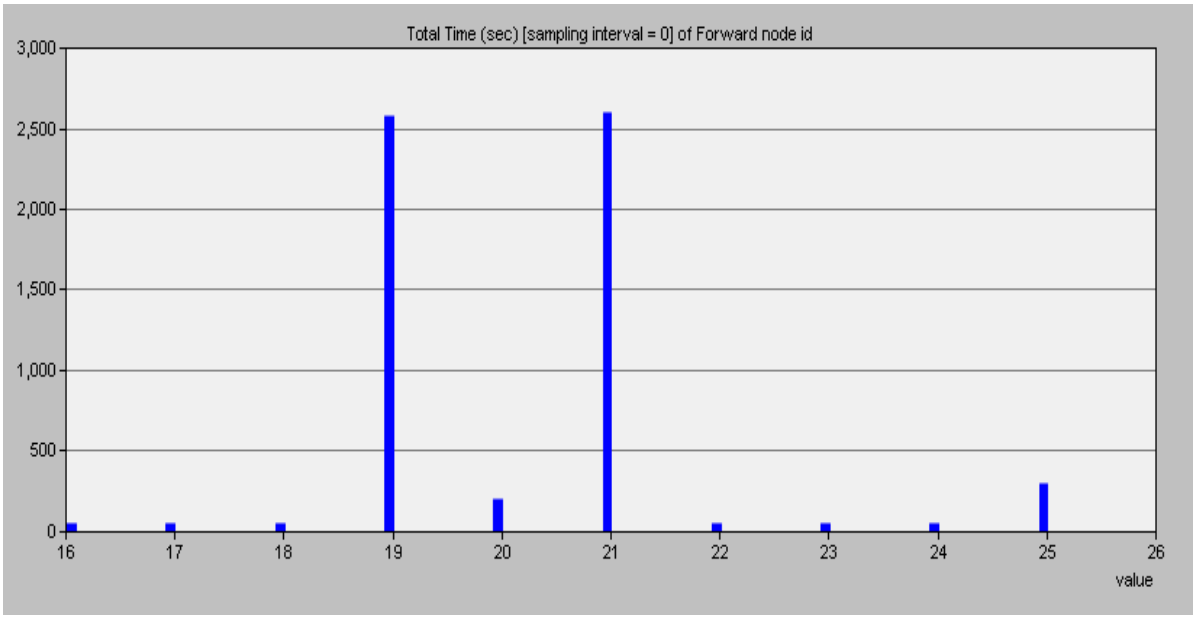
(120 turns). It shows that if a is big, nodes of high forward rate will be used more. So the whole forward rate of the network will be higher. When a = 0.1, b = 0.9 and a = 0.9, b = 0.1, the network's forward rate is as **Figure 6(b)**.

On the other hand, the nodes' use time is different because of different value of a and b. As shown in **Figure 7(a)** and **Figure 7(b)**, when a = 0.1, b = 0.9, the nodes were used equally. But when a = 0.9 and b = 0.1, the nodes were used not equally.

We define that the first node's death time is the network's lifetime. That is to say, although the early stage of forward rate in the network is very high, if the nodes of high forward rate are used excessively, the network's lifetime will decrease. We do a 40000 s simulation, until all the nodes die. In **Figure 8(a)** and **Figure 8(b)**, we can see when a = 0.9 and b = 0.1, the network has a high forward rate at first. But because of using the good nodes excessively, the best node dies so early. If we don't add new nodes instead of died nodes, the connectivity and

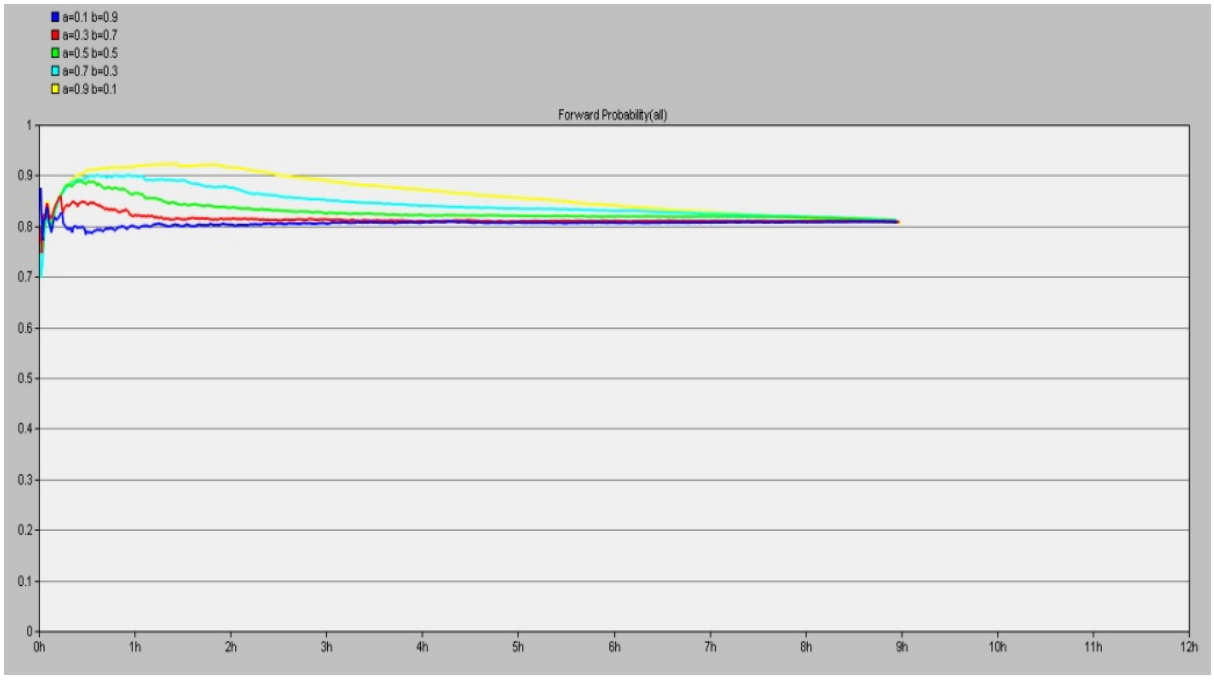


(a) When a = 0.1, b = 0.9.

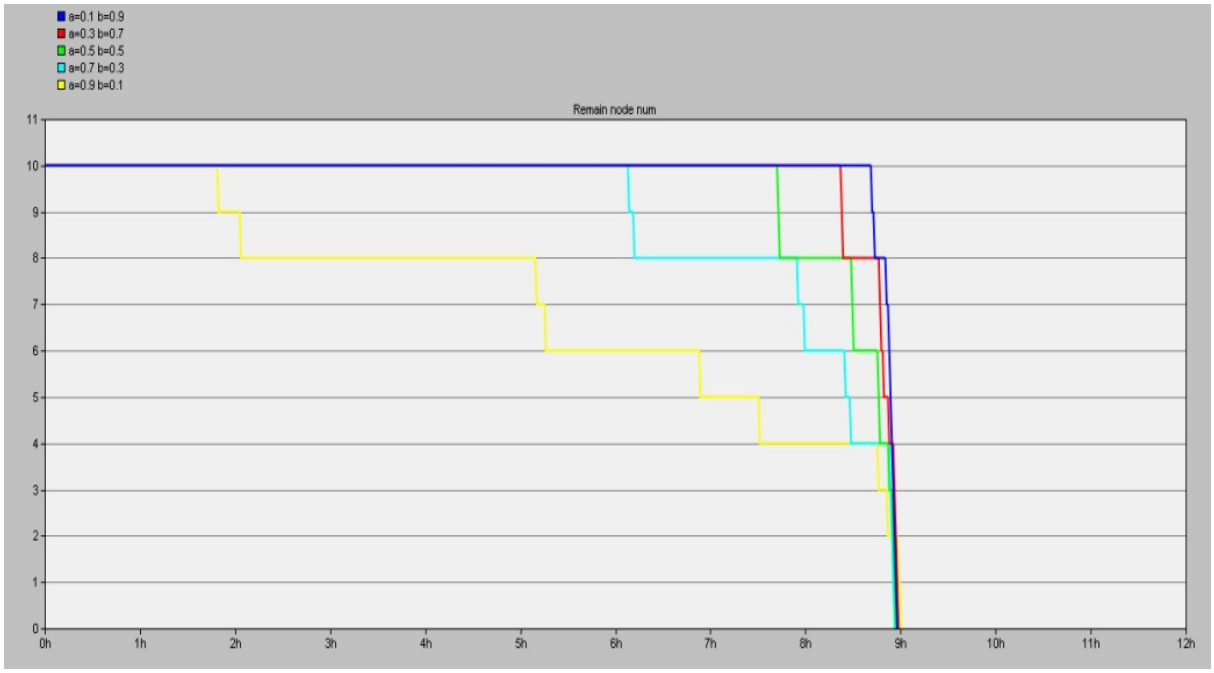


(b) When a = 0.9, b = 0.1.

Figure 7. Every node's using time.



(a) The forward rate (average) of the network.



(b) The remainder node of the local network.

Figure 8. The simulation until all the nodes' power using up with different value a and b.

cover degree of network will be destroyed.

Acknowledgements

The authors wish to acknowledge the anonymous reviewers for their valuable comments and suggestions. We also thank OPNET Technologies, Inc., for providing us with OPNET Wireless Modeler to validate our approaches.

References

[1] Yu, Y.L., Li, K.Q., Zhou, W.L. and Li, P. (2011) Trust Mechanisms in Wireless Sensor Networks: Attack Analysis and Countermeasures. *Journal of Network and Computer Applications*, **35**, 867-880.

[2] He, B., Joshi, S., Agrawal, D.P. and Sun, D. (2010) An Efficient Authenticated Key Establishment Scheme for Wireless Mesh Networks. 2010 *IEEE Global Telecommunications Conference*, Miami, 6-10 December 2010, 6-10.

[3] Butun, I., Morgera, S.D. and Sankar, R. (2013) A Survey of Intrusion Detection Systems in Wireless Sensor Networks. *IEEE Communications Surveys & Tutorials*, **16**, 266-282.

[4] Cho, Y. and Qu, G. (2013) Detection and Prevention of Selective Forwarding-Based Denial-of-Service Attacks in WSNs. *International Journal of Distributed Sensor Networks*, **2013**, Article ID: 205920, 16 p. http://dx.doi.org/10.1155/2013/205920

[5] Marti, S., Giuli, T.J., Lai, K. and Baker, M. (2000) Mitigating Routing Misbehavior in Mobile and Ad Hoc Networks. *Proceedings of International Conference on Mobile Computing and Networking*, Boston, 6-11 August 2000, 255-265.

[6] Hai, T.H. and Huh, E.-N. (2008) Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-Hops Neighbor Knowledge. 2013 *IEEE* 12*th International Symposium on Network Computing and Applications*, Cambridge, 10-12 July 2008, 325-331.

[7] Khalil, I., Bagchi, S., Rotaru, C.N. and Shroff, N.B. (2009) UnMask: Utilizing Neighbor Monitoring for Attack Mitigation in Multihop Wireless Sensor Networks. *Ad Hoc Networks*, **8**, 148-164. http://dx.doi.org/10.1016/j.adhoc.2009.06.002

[8] Lu, Y.F., Lin, K. and Li, K.Q. (2012) Trust Evaluation Model against Insider Attack in Wireless Sensor Networks. *International Conference on Cloud and Green Computing*, Xiangtan, 1-3 November 2012, 319-326.

[9] Karlof, C. and Wagner, D. (2003) Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. *Ad Hoc Networks*, **1**, 293-315. http://dx.doi.org/10.1016/S1570-8705(03)00008-8

[10] Challal, Y., Ouadjaout, A., Lasla, N., Bagaa, M. and Hadjidj, A. (2011) Secure and Efficient Disjoint Multipath Construction for Fault Tolerant Routing in Wireless Sensor Networks. *Journal of Network and Computer Applications*, **34**, 1380-1397. http://dx.doi.org/10.1016/j.jnca.2011.03.022

[11] Shu, T., Liu, S. and Krunz, M. (2009) Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes. *Proceedings of the IEEE INFOCOM Conference*, Rio de Janeiro, 19-25 April 2009, 2846-2850.

[12] Sun, H.-M., Che, C.-M. and Hsiao, Y.-C. (2007) An Efficient Countermeasure to the Selective Forwarding Attack in Wireless Sensor Network. *IEEE Region* 10 *Conference* (*TENCON*), Taipei, 30 October-2 November 2007, 1-4.

Scientific Research Publishing (SCIRP) is one of the largest Open Access journal publishers. It is currently publishing more than 200 open access, online, peer-reviewed journals covering a wide range of academic disciplines. SCIRP serves the worldwide academic communities and contributes to the progress and application of science with its publication.

Other selected journals from SCIRP are listed as below. Submit your manuscript to us via either submit@scirp.org or Online Submission Portal.