A Lightweight Detection Mechanism against Sybil Attack in Wireless Sensor Network

Wei Shi[1], **Sanyang Liu**[1] **and Zhaohui Zhang**[1]
[1] School of Mathematics and Statistics, Xidian University
Xi'an 710071, China
[e-mail: zhangzhaohui005@163.com]
*Corresponding author: Zhaohui Zhang

Received March 23, 2015; revised June 26, 2015; accepted July 27, 2015; published September 30, 2015

Abstract

Sybil attack is a special kind of attack which is difficult to be detected in Wireless Sensor Network (WSN). So a lightweight detection mechanism based on LEACH-RSSI-ID (LRD) is proposed in this paper. Due to the characteristic of Low-Energy Adaptive Clustering Hierarchy (LEACH) protocol, none of nodes can be the cluster head forever.

Meanwhile, in order to consume less energy, both factors which are called the remaining energy of nodes and relative density of nodes are taken into account. Therefore, Sybil attack can be found by analyzing the RSSI-ID tables. Different from the previous detection methods, even though Sybil attack occurs in the initialization phase, the malicious nodes can be detected by sink node. What's more, when each malicious node frequently changes identification, it will be detected in a short time. Through the simulations, it is revealed that the LRD mechanism can detect the Sybil attack with high detection rate and accuracy.

Keywords: Wireless Sensor Network, Sybil attack, LEACH protocol, RSSI-ID table

This work was supported by the National Natural Science Foundation of China (Grants No.61373174), and the Fundamental Research Funds for the Central Universities (Grants No. K5051270015 and No.K5051370026.).

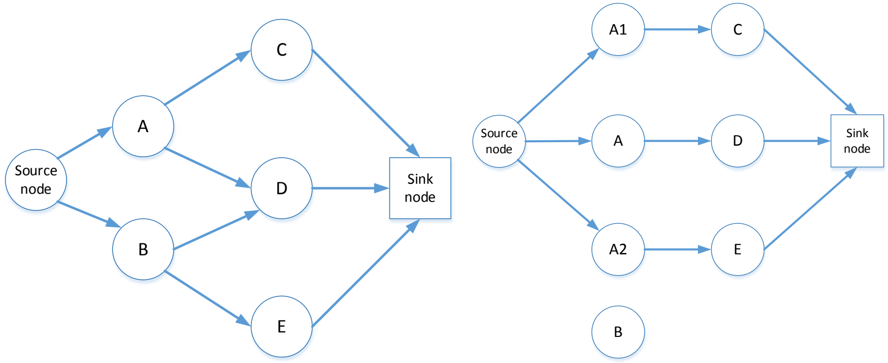
http://dx.doi.org/10.3837/tiis.2015.09.025 **ISSN : 1976-7277**

1. Introduction

Wireless Sensor Network (WSN), which is comprised of a large number of sensor nodes, is a self-organized network without any infrastructures. With the rapid development of wireless communication and sensor technique, WSN has been widely used in various fields, such as military, commercial and so on. Different from the traditional network, it is a large-scale, dynamic and integrated network. It is responsible for the sensor nodes in WSN to collect or monitor the surrounding information and convert it into forms of bytes so as to send to the user. WSN is usually deployed in adverse circumstances to monitor the temperature, air pressure, air humidity and other information. Therefore, the safety and stability of the network is very easily influenced by the surrounding environment. Due to the limitation of energy and the ability of data storage and data processing, when sensor nodes interact with each other, they are in a multi-hop fashion. Therefore, it is vulnerable to kinds of external attacks.

The attacks in WSN can be divided into three categories: (1) Attack based on confidentiality and authentication, such as channel monitoring, wormhole attack, tampering packet, and so on; (2) Attack aiming at the protocol layer, which is usually called the denial of service attack; (3) Attack based on the integrity of service where adversaries can mislead the base station through the injection of a large amount of false data.

Sybil attack [1] is a kind of malicious attack which is difficult to be detected against the protocol layer. Compared to other attacks, the hardware requirements of the malicious node in Sybil attack is not high. And Sybil attack does not require the cooperation of multiple nodes, so the implementation of the attack is easier. In such an attack, a malicious node has multiple identifications which are forged or impersonated according to the normal nodes. While normal nodes in the network can't distinguish the false nodes, therefore the normal nodes will be misled to communicate with malicious nodes directly. In this way, the malicious node attracts most of the data flow in the network. As shown in Fig. 1, when node A is captured to become the malicious node, it forges two legal identifications named A1 and A2. They will mislead source node to send data to the malicious node named A. And node B is ignored by source node. Therefore, Sybil attack can destroy the network by combining other attacks in this area. Moreover, once Sybil attack succeeding, adversaries will destroy the storage mechanism, data fusion mechanism, route mechanism and fair resource allocation mechanism in WSN. Therefore, under the condition of limited resources, how to detect Sybil attack quickly and accurately becomes the key issues of research in recent years.



a. Normal network b. Network under Sybil attack

Fig. 1. Data transmission under different network states in WSN

Applying cryptographic approaches are the traditional way to detect Sybil attack. Karlof et al. have claimed that we can defend Sybil attack by using symmetric encryption technology [2]. Then based on that, a method for detecting Sybil attack by using data encryption and node identification is proposed [3-5]. However, it requires much memory space to store identification information for the several methods above. And because of the limited energy and computing power of nodes, these methods are difficult to achieve in WSN. What's more, once capturing the normal nodes, adversaries will obtain the relevant information of shared encryption keys and then threat the security of entire network.

Therefore, most commonly schemes against Sybil attack is by measuring distance and using location. Then solutions based on RSSI (Received Signal Strength Indicator) are given. When collecting RSSI values, we do not need additional hardware devices to support. Demirbas et al. have proposed a detection mechanism based on RSSI [6]. They determine whether there are any malicious nodes by comparing the ratio of RSSI. But for this algorithm, it requires at least four testing nodes to achieve ideal effect and it is not high in detection rate. M. Li et al. put forward a regional statistics detection scheme against Sybil attack [7]. They assume that the network is static, that is, the location of each node in WSN keeps constant. Every node collects RSSI values around its neighbor nodes in its region. Then the RSSI-ID tables are established. By comparing the tables in several trusting nodes, Sink node will find the malicious nodes and isolate them from the network. However, for this scheme, it consumes so much energy that the network will run out in a short time.

A novel approach against Sybil attack is introduced in [8]. It is based on traffic monitoring and neighbor mechanism. Unlike most techniques, this method does not need location information of nodes and other special hardware. Malicious nodes can be detected by analyzing the traffic density around sensor nodes. It can detect Sybil attack with high detection rate and low misdetection rate. But this approach is a centralized method and costs too much energy. In [9], it proposes a lightweight Sybil attack detection framework (LSDF). This approach is based on evidence theory which includes evidence collection and validation. The LSDF works with information observed by each node. Through computing the relationship of distance, location and RSSI values of nodes, we can detect Sybil attack easily. The LSDF is robust for Sybil attack detection, but it will be greatly influenced by deviations when nodes collect information. Meanwhile, energy is consumed too much. A Security Mechanism called LEACH-S is proposed to detect Sybil attack in [10]. Once number of cluster heads exceeds the preset threshold, Sybil attack may happen. Only at this time it will start intrusion detection mechanism in WSN. Then base station will collect RSSI information of nodes and establish correlation matrix to find malicious nodes. However, the detection rate and accuracy of LEACH-S is not high.

In [11], it introduces a detection approach of selfish attack which is one of Sybil attack types by emulating legal node. In this paper, the authors identify a new selfish attack type in cognitive ratio ad-hoc networks and propose a detection method called COOPON which can detect this kind of selfish attack by neighboring nodes' cooperative information exchange. This technique is easy and efficient with better detection reliabilities, and it can be well useful in practice.

In this paper, taking advantage of the fact that every sensor node has its own unique identity, we put forward a novel method for detecting Sybil attack called LEACH-RSSI-ID (LRD). Without data encryption, our approach is based on the LEACH protocol and can detect attack with high efficiency.

The rest of this paper is organized as follows: Details of the LRD mechanism are brought in Section II. Section III introduces the results of system simulations. Finally, conclusions and prospect of this paper is proposed in Section IV.

1. Proposed Method

1.1 Preliminaries

2.1.1. LEACH: Low-Energy Adaptive Clustering Hierarchy

LEACH [12] is a self-organizing and adaptive clustering protocol that uses randomization to distribute the energy load evenly among the sensor nodes in the network. The operating process of LEACH protocol is the ongoing reconstruction process of clusters which is represented by "Round". Each round includes cluster building phase and data transmission phase. In the stage of establishing a cluster, cluster heads can be chosen as follows: Each sensor node randomly chooses a value between 0-1. If the selected value is less than a threshold value T, then this node becomes a cluster head node.

$$T = \begin{cases} \dfrac{p}{1-p[r \bmod (1/\mathrm{p})]} & , \quad if \quad n \in G \\ 0 & , \quad otherwise \end{cases} \tag{1}$$

Where T is the threshold value, r is the current round number, p is the percentage of the cluster head nodes in WSN. And G is the set of nodes that never act as a cluster head in recent 1/p round. Using this method, every node will be cluster head within 1/p round. During round 0 (r=0), each node has a probability p of becoming a cluster head. The nodes that are cluster heads in round 0 cannot be cluster heads for the next 1/p rounds. Thus the probability that the remaining nodes are cluster heads must be increased, since there are fewer nodes that are eligible to become cluster heads. And after 1/p rounds, all nodes are once again eligible to become cluster heads.

2.1.2.RSSI: Received Signal Strength Indicator

In the process of communication, RSSI received by the receiving node changes with the distance. Usually, the distance from the node to the node is greater, and the value of RSSI is lower. When the channel model is established, the formula of RSSI and distance can be obtained, so that the information of RSSI can be transformed into distance information. And then based on this model, nodes can be positioned in WSN.

1.2 The Modified LEACH protocol

After research, we found that LEACH protocol also had shortcomings. Firstly, the distribution of cluster head in the network has stochastic nature. Secondly, the density of the nodes in the actual network is not uniform. As a result, some nodes will run out of energy in advance due to the heavy burden. Therefore, in order to reduce energy consumption, we proposed the modified LEACH protocol. In this way, we will consider the relationship of node residual energy and the network average energy. What's more, the relative density of node is also an important parameter. Threshold is defined as follows:

$$T = \begin{cases} \dfrac{p}{1-p[r \bmod (1/\mathrm{p})]} \cdot \dfrac{E^{(n,r)}_{remain}}{E^{r}_{ave}} \cdot \rho^{r}_{n} & , \quad if \quad n \in G \\ 0 & , \quad otherwise \end{cases} \tag{2}$$

$E_{remain}^{(n,r)}$ represents the residual energy of node n at the r round while E_{ave}^{r} is the average energy of the whole network. ρ_{n}^{r} is the relative density of node n at the r round. First, the definition of neighbor nodes has been proposed as below.

$$Neighbor(n) = \{m \mid d_{mn} \le R, m \in N\} \tag{3}$$

The formula above is the set of neighbor nodes of node n. R is the communication radius and N represents the set of sensor nodes in the entire network. Next, we present a definition of density of sensor node.

$$\rho_{n}^{r} = \frac{Neighbor\_alive_{n}^{r}}{(1/p)-1} \tag{4}$$

Where $Neighbor\_alive_{n}^{r}$ is the number of neighbor nodes alive of node n at the r round. And (1/p)-1 represents the number of neighbor nodes in the standard cluster.

The selected cluster heads will broadcast in the entire network. Then other normal nodes decide to join which cluster according to the received signal strength information and notify the corresponding cluster head to complete the establishment of clusters.

1.3 Establishing RSSI-ID tables

Due to the fact that each node has its unique identity, cluster heads can communicate with intra-cluster nodes in order to record the RSSI values and then establish the table which reflecting the relation of RSSI value and identity. The model can be described as follows:

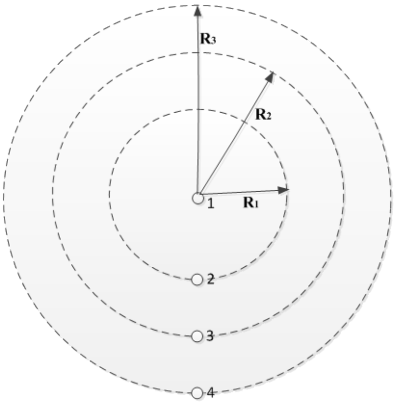


Fig. 2. The normal network without Sybil attack

As shown in **Fig. 2**, when there is no malicious nodes in WSN, node numbered 1 is a cluster head, and others are intra-cluster nodes. After communicating with intra-nodes, cluster head stores information such as identities and RSSI values, then find a RSSI-ID table, as shown in **Table 1.**

Table 1. The RSSI-ID table without Sybil attack

RSSI	R_1	R_2	R_3
ID	2	3	4

In every round, each cluster head should update its RSSI-ID table, then transmits it to sink node so as to detect Sybil attack immediately.

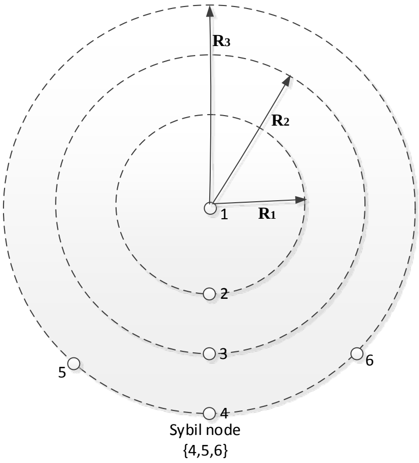


Fig. 3. The network existing Sybil attack

According to **Fig. 3**, when there is any malicious node deployed in WSN, node 1 is the normal cluster head while nodes numbered 4, 5, 6 are identities forged by a malicious node. The RSSI-ID table found by node 1 is shown in **Table 2**.

Table 2. The RSSI-ID table with a malicious node

RSSI	R_1	R_2	R_3	R_3	R_3
ID	2	3	4	5	6

From **Table 2**, we can take notice of that the RSSI values of node 4, 5, 6 are the same. So node 4, 5, 6 can be judged as a plurality of IDs of the same node. Then cluster head sends the corresponding information of node 4, 5, 6 to sink node. Finally sink node will broadcast in the whole network to make sure that other normal nodes do not send or receive information from these nodes, so as to isolate them from the network.

1.4 LRD mechanism against Sybil attack

As depicted in **Fig.4**, the detailed steps of LRD mechanism are given as follows:

Step1: After the network clustering based on modified LEACH protocol, every cluster head node exchanges information with intra-cluster nodes. Then cluster head collects RSSI values and IDs of intra-cluster nodes to establish RSSI-ID table**.**

Step2: Cluster heads send their own information and RSSI-ID tables to sink node.

Step3: Sink node fixes position on each cluster head through the related information of cluster head and intra-cluster nodes so as to detect whether cluster head is a malicious node. If it is a malicious node, switch to Step 4; otherwise, switch to Step 5.

Step4: Sink node communicates with intra-cluster nodes where cluster head is a malicious node, and establishes the RSSI-ID table. Then switch to Step 5.

Step5: Sink node detects whether there is a Sybil attack by analyzing the information stored in RSSI-ID tables. If multiple IDs have the same RSSI value, and number of these IDs exceeds the given threshold, nodes corresponding to these IDs are malicious nodes. Then sink node broadcasts to normal nodes in the entire network in order to isolate malicious nodes from the network. Otherwise, switch to Step 1.

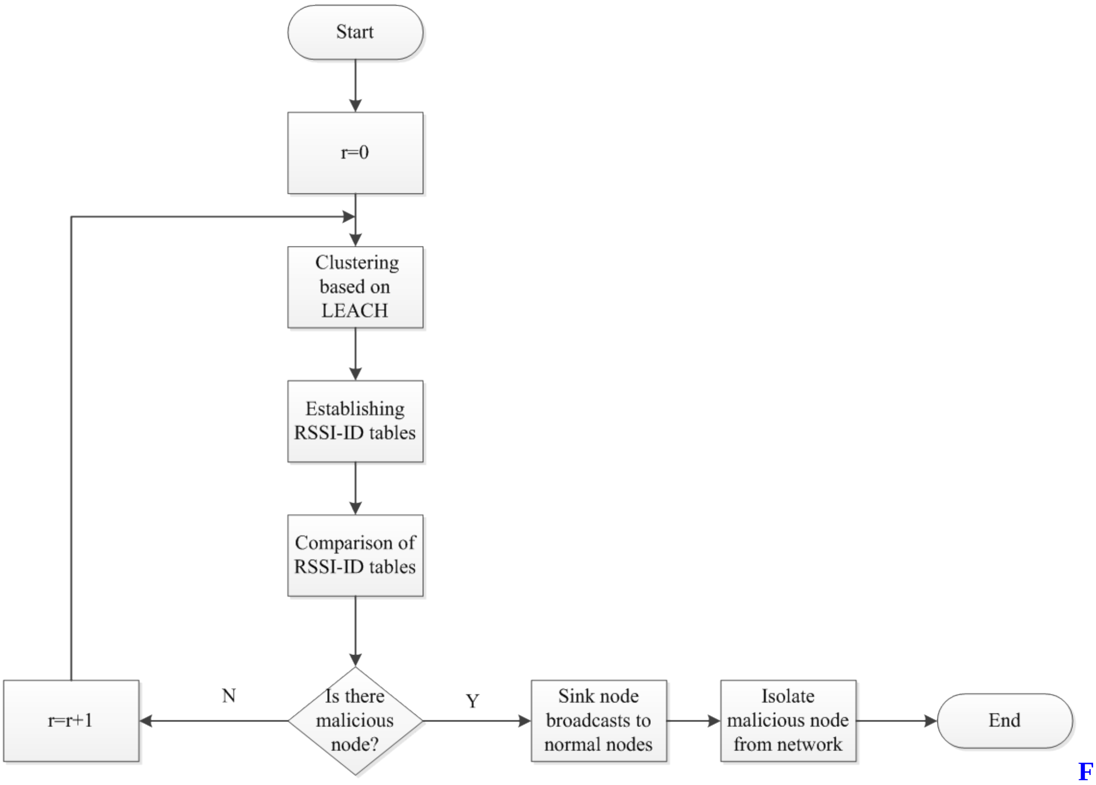

Start
r=0
Clustering based on LEACH
Establishing RSSI-ID tables
Comparison of RSSI-ID tables
Is there malicious node?
N
r=r+1
Y
Sink node broadcasts to normal nodes
Isolate malicious node from network
End
F

Fig. 4. Flowchart of LRD mechanism

1.5 Analysis of algorithm

In this paper, we assume that the network is static. Once Sybil attack happens, that means, a normal node has been captured and compromised by adversaries. Moreover, on the basis of this node, several identities are forged by adversaries. If node captured with normal ID becomes cluster head, it will falsify data to mislead sink node so as to avoid being detected. Therefore, we cannot detect Sybil attack in this situation. However, due to the characteristic of LEACH protocol, it cannot be always the cluster head. When node with forging ID becomes cluster head, it can be detected by sink node according to the relationship between RSSI value and distance.

Due to the fact that the magnitude of RSSI is influenced by temperature, humidity, topography and other factors, it requires relative ideal environment for this method. Therefore, in practice, we can set an error value while implementing LRD mechanism. If the difference of collecting RSSI values is within error, we believe that these RSSI values are the same. But if a great number of nodes are deployed in a small region, normal nodes may be detected as malicious nodes.

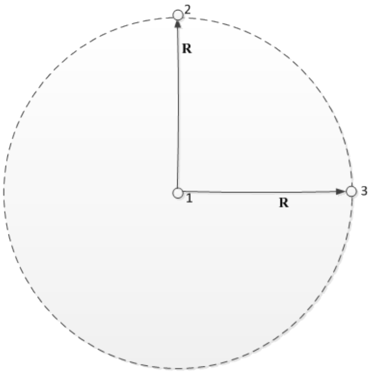


Fig. 5. Situation of false detection

As shown in **Fig. 5**, two normal nodes 2 and 3 are located on the circle with center point node 1, and a radius of R which represents the RSSI value. If we set the threshold as 2, node 2 and 3 are false detected as malicious nodes. But the probability of such a case in the network is very small. So the LRD mechanism can effectively detect Sybil attack and safeguard the security of network.

2. Simulation results

In order to test and evaluate the detection method proposed in this paper, we simulated a network with 100 normal nodes. And each node only communicates with other nodes which are within the communication radius. Once energy of node runs out, node will die and exit the network. Moreover, the lifetime of network comes to an end when all nodes have died. The simulation operates on MATLAB platform. And the simulation parameters for the network are illustrated in **Table 3**.

Fig. 6 shows the initial distribution of nodes in WSN.

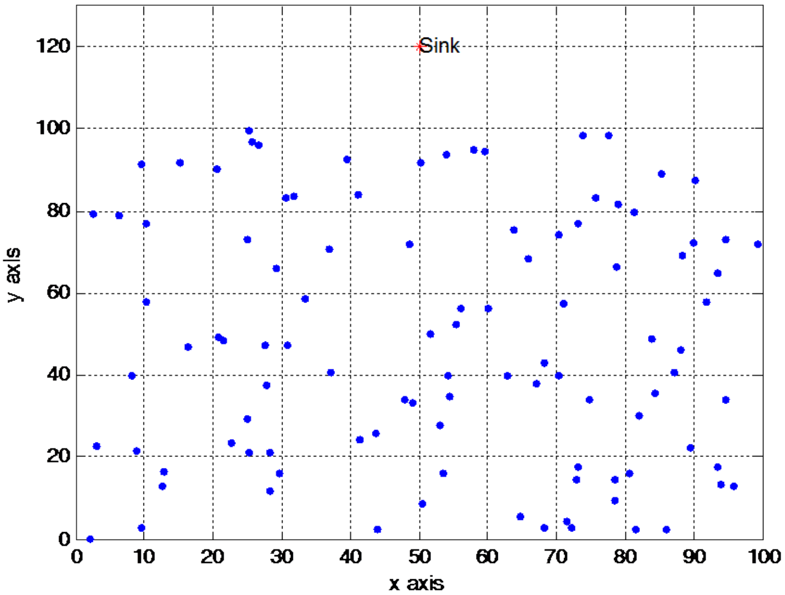


Fig. 6. Distribution of nodes

Table 3. Simulation Parameters in WSN

Parameter	Value
Distribution of nodes	Randomly
Number of nodes	100
Area	100*100
Coordinates of sink node	(50,120)
Communication radius	30
Initial energy/J	0.5J
Packet size	4000 bytes
Control packet size	100 bytes

2.1 Detection Rate

As shown in **Fig. 7**, the detection rate of LRD decreases along with the increase of the ratio of cluster heads in WSN. But LRD mechanism is much higher than LEACH-S scheme in detection rate. The RSSI-based scheme has nothing with the ratio of cluster heads.

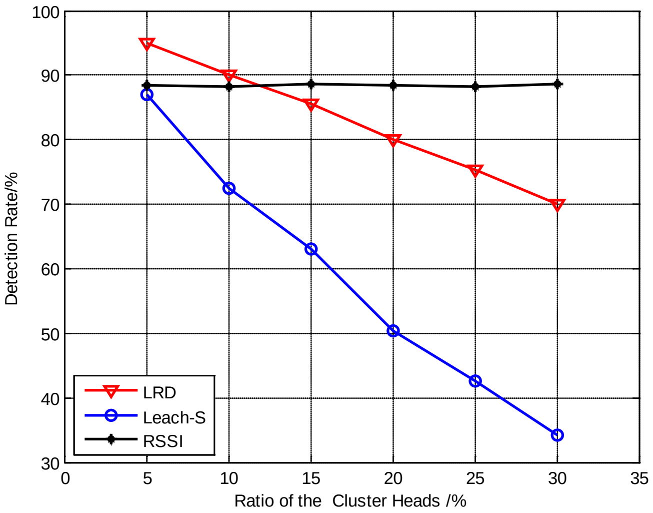


Fig. 7. The variation of detection rate with the ratio of CHs

We assume that there is only one Sybil node in WSN. **Fig. 8** shows that when the ratio of cluster heads keeps 5%, the detection rate of LRD is basically unchanged around 95%. The other two methods decline with the increase of number of forging identities in detection rate. That means, no matter how many identities forged by adversaries, the LRD can effectively detect the Sybil attack.

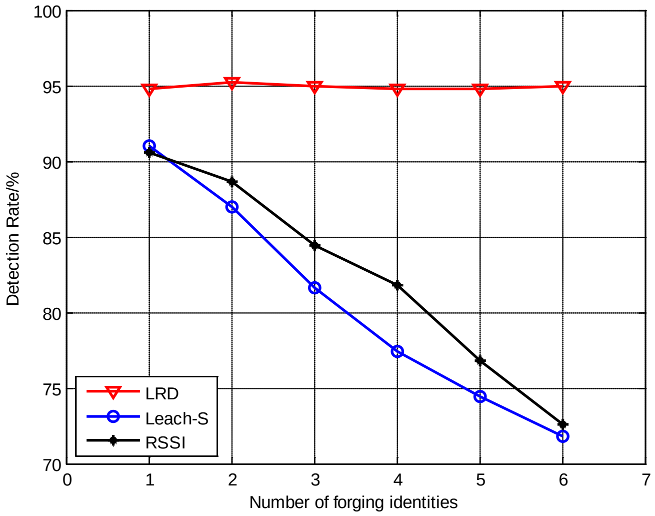


Fig. 8. The variation of detection rate with number of forging identities

Next simulation for the variation of detection rate with number of Sybil nodes is carried out under the premise of setting the ratio of cluster heads as 5%. Every Sybil node, that is each captured normal node, has two forging identities. From **Fig. 9**, we find that detection of rate decreases with the increase of number of Sybil nodes. But LRD is much higher than the other two methods in detection rate. Therefore we draw a conclusion that the LRD mechanism is robust.

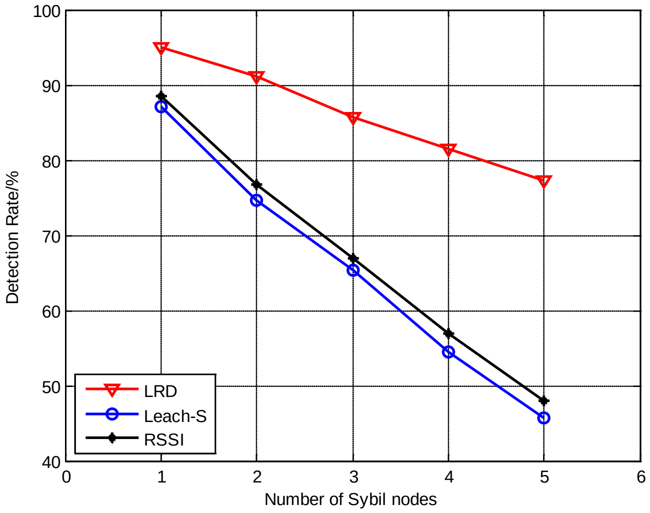


Fig. 9. The variation of detection rate with number of Sybil nodes

2.2 The Remaining Energy

As shown in **Fig. 10**, the remaining energy of LRD is slightly lower than LEACH-S algorithm. But there are much more remaining energy by using LRD scheme than by using the general RSSI-based scheme. In our simulation, there is no dead nodes in recent 500 rounds. Meanwhile, due to the fact that energy is almost consumed the same in each round of LEACH clustering, variation in **Fig. 9** is linear.

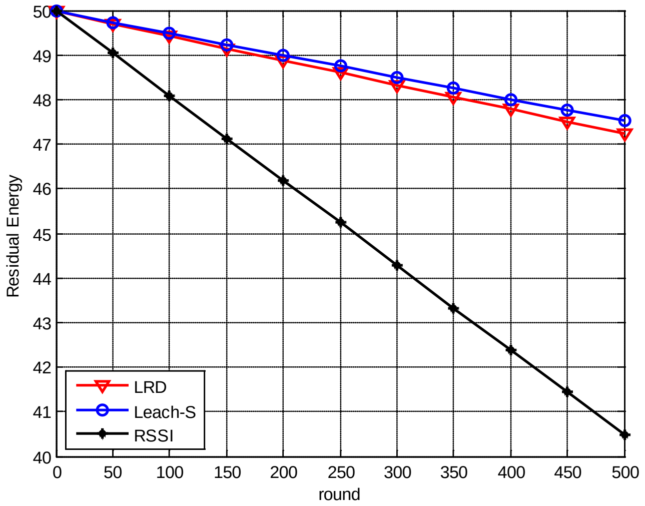


Fig. 10. The comparison of remaining energy

2.3 Lifetime of network

Fig. 11 shows the variation of lifetime in WSN along with time. We can know that even though it is a little shorter than LEACH-S scheme, lifetime of WSN based on LRD is much longer than which based on ordinary RSSI scheme.

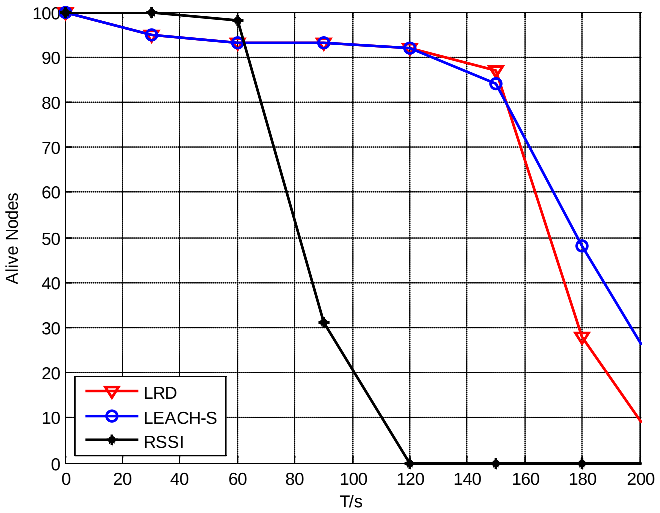


Fig. 11. The variation of the lifetime of network

As depicted above, we draw a conclusion that the LRD mechanism can prolong the lifetime of network while maintaining a high detection rate comparing with LEACH-S and RSSI-based schemes,

3. Summary and Future work

In this paper, a lightweight detection mechanism called LRD is proposed to detect Sybil attack. Even though Sybil attack exists in the network's initialization phase or Sybil node changes its identity, it can be detected by sink node in a short time.

The simulation results prove that the LRD mechanism detects Sybil attack with high accuracy and consumes less energy. However, Sybil attack often invades WSN accompanied by other attacks such as sinkhole attack, replication attack and so on. Therefore, how to design a kind of detection algorithm against a variety of attacks will be the direction of future research.

References

[1] Kai Xing, Shyaam Sundhar Rajamadam Srinivasan, Major Jose "Manny" Rivera, Jiang Li, Xiuzhen Cheng, "Attacks and countermeasures in sensor networks: A survey," *Network Security*, pp: 251–272, June 12, 2010. Article (CrossRef Link)

[2] Chris Karlof, David Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2–3, pp: 293-315, September, 2003. Article (CrossRef Link)

[3] Liang Xiao, Greenstein, L.J., Mandayam, Narayan B., Trappe, W., "Channel-based detection of Sybil attacks in wireless networks," *IEEE Transactions on Information Forensics and Security*, vol. 4, no. 3, pp: 492-503, July, 2009. Article (CrossRef Link)

[4] Qinghua Zhang, Wang, P., Reeves, D.S., Peng Ning, "Defending against Sybil attacks in sensor networks," *25th IEEE International Conference on Distributed Computing Systems Workshops*, pp: 185–191, June 6-10, 2005. Article (CrossRef Link)

[5] N. Tran, J. Li, L. Subramanian, S. S. M. Chow, "Brief announcement: improving social-network-based Sybil-resilient node admission control," in *Proc. of the 29th ACM SIGACT-SIGOPS symposium on Principles of distributed computing*, pp: 241-242, 2010. Article (CrossRef Link)

[6] M. Demirbas and Y. Song, "An RSSI-based Scheme for Sybil Attack Detection in Wireless Sensor Networks," in *Proc. of 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks(WoWMoM'06)*, pp: 564-570, 2006. Article (CrossRef Link)

[7] Mingxi Li, Yan Xiong, Xuangou Wu, Xiancun Zhou, Yuhui Sun, Shenpei Chen, and Xiaoya Zhu, "A regional statistics detection scheme against Sybil attacks in WSNs," in *Proc. of The 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom)*, pp: 285–291, July 16-18, 2013. Article (CrossRef Link)

[8] Golestani Najafabadi, S., Naji, H.R., and A. Mahani, "Sybil Attack Detection: Improving Security of WSNs for Smart Power Grid Application," in *Proc. of 2013 Smart Grid Conference (SGC)*, pp: 273-278, December 17-18, 2013. Article (CrossRef Link)

[9] P. R. Vamsi and K. Kant, "A Lightweight Sybil Attack Detection Framework for Wireless Sensor Networks," in *Proc. of Contemporary Computing (IC3), 2014 Seventh International Conference on*, pp: 387-393, August 7-9, 2014. Article (CrossRef Link)

[10] S.S. Chen, G. Yang, "A Security Routing Mechanism Against Sybil Attack for Wireless Sensor Networks," in *Proc. of Communications and Mobile Computing (CMC), 2010 International Conference on*, vol. 1, pp: 142-146, April 12-14, 2010. Article (CrossRef Link)

[11] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter In, "Selfish Attacks and Detection in Cognitive Radio Ad-hoc Networks," *IEEE Network*, vol.27, no. 3, pp. 46-50, June 2013. Article (CrossRef Link)

[12] Heinzelman, W.R., Chandrakasan, A., Balakrishnan, H., "Energy-Efficient Communication Protocol for Wireless Microsensor Networks," in *Proc. of the 33rd Annual Hawaii International Conference on System Sciences*, January 4-7, 2000. Article (CrossRef Link)

[13] Yide Liu. “Wireless Sensor Network Applications in Smart Grid: Recent Trends and Challenges,” *International Journal of Distributed Sensor Networks (IJDSN)*, pp: 1-8, July 16, 2012. Article (CrossRef Link)

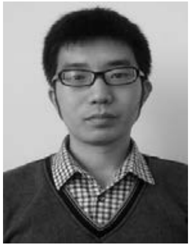
[14] Jiuqiang Xu, Wei Liu, Fenggao Lang, Yuanyuan Zhang, Chenglong Wang, “Distance measurement model based on RSSI in WSN,” *Wireless Sensor Network*, vol. 2, no. 8, pp: 606-611, 2010. Article (CrossRef Link)

[15] Jun-Won Ho, “Sequential hypothesis testing based approach for replica cluster detection in wireless sensor networks,” *Journal of Sensor and Actuator Networks*, vol. 1, no. 2, pp: 153–165, September 5, 2012. Article (CrossRef Link)

[16] Wei, Yawen and Guan, Yong, “Lightweight location verification algorithms for wireless sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 5, pp: 938–950, March, 2013. Article (CrossRef Link)

[17] Zied Trifa, Maher Khemakhem, “Sybil Nodes as a Mitigation Strategy against Sybil Attack,” *Procedia Computer Science*, vol. 32, pp: 1135 – 1140, June 5, 2014. Article (CrossRef Link)

[18] Jun-Won Ho, Wright, M., Das, S.K., “Zonetrust: fast zone-based node compromise detection and revocation in wireless sensor networks using sequential hypothesis testing,” *Dependable and Secure Computing, IEEE Transactions on*, vol. 9, no. 4, pp: 494-511, December 27, 2011. Article (CrossRef Link)



Wei Shi was born in 1990. He received his B.S. degrees from Xidian University in 2013. He is currently a postgraduate student and pursuing for master degree in School of Mathematics and Statistics from Xidian University. His research interests are Wireless Sensor Network and network optimization.
E-mail: 120168927@qq.com

Sanyang Liu received his M.S. degree at Xidian University in 1984, and received his Ph.D. degree in Xi’an Jiaotong University in 1989.Now he is a professor and Ph.D. supervisor of Xidian University. His research interest covers theory and application of optimization and network arithmetic.
Email: liusanyang@126.com

Zhaohui Zhang was born in Shaanxi, China. He received his M.S. degrees in School of Mathematics and Statistics from Xidian University, Xi'an, China in 2013. He is currently a postdoctoral researcher at Xidian University. His research interests include wireless sensor networks, network optimization and robust optimization.
E-mail: zhangzhaohui005@163.com