Sybil Attack Detection Scheme Based on Data Flow Monitoring and RSSI ranging in WSN

Daiyu Xu[1, a], Yuanming Wu[1, b,*] and Yingzhe Duan[2, c]

[1]School of Optoelectronic Information, University of Electronic Science and Technology, Chengdu 610054, China;
[2] School of Optoelectronic Information, University of Electronic Science and Technology, Chengdu 610054, China;
[a]2014050206029@std.uestc.edu.cn, [b]ymwu@uestc.edu.cn, [c]yingzheduan@std.uestc.edu.cn

Keywords: WSN, Sybil attack, lifespan, RSSI ranging, Data flow monitoring.

Abstract: Sybil attack is a destructive attack in wireless sensor networks, where a node illegitimately takes on multiple identities. Some scholars focus on how to defense against Sybil attack if the attackers launch selective forwarding attack. However, threat of network lifespan caused by Sybil attack is ignored. In this paper, we demonstrate that network lifespan is possible to be shortened by Sybil attackers and then we put forward a countermeasure against Sybil attack based on RSSI ranging and data flows monitoring. First, we detect suspicious nodes (we call them as node M and node N) if all of their common neighbors find node M and N have the same distance to them. Second, a suspicious node will be marked as Sybil node if its data flow is abnormal according to criterion. Simulation results show that proposed secure mechanism can effectively detect Sybil nodes with a misdetection rate of 6.7% and a false alarm rate of 3.3%. Additionally, proposed security scheme extends the network lifespan by 26.3%.

1.Introduction

Sybil attack, first described by Douceur [1], refers to a kind of malicious behave undermining the network by steal or fabricate multiple identities by only a physical device. Sybil attack has two purposes. One is that it will damage the network by dropping or modifying data[2]. The other is that it will also narrow the lifespan of the network by transmitting data frequently in a certain area.

Many scholars have done research on Sybil attack. Karlof and Wagner[2] found that Sybil attack would pose a threat to routing mechanisms in sensor networks. James Newsome et al. pointed out that position verification was a promising approach[3] to defend against the Sybil attack, but it was difficult to verify a node’ s exact position. Demirbas M et al. gave a Sybil detection method based on the Received Signal Strength Indicator (RSSI[4]). Sharmila Sivaraj combined the transmission power with the distance detection between the nodes to detect the Sybil node [5]. Bin Tian argued that we can use three neighbor nodes which position have been known to detect Sybil node [6]. Udaya Suriya Raj Kumar Dhamodhar et al. proposed a positioning-related CAM-PAM (compare and match-position verification method) algorithm[7].

In this paper, a lightweight Sybil attack detection scheme based on data flow monitoring and RSSI ranging is put forward in this paper. The detection scheme considers the error of RSSI and remedies it by other approaches which exploit the characteristics of Sybil attack. Simulation results show that our scheme can detect the Sybil node effectively.

2.Proposed Security Scheme to Defense Sybil Attack

2.1 Shortening the network lifespan

Before the description of our scheme, we will make some assumptions. We assume that sink node is trustworthy and nodes in the network are immobile. Moreover, we assume that there is only a Sybil node with two identities in the network.

We can make a preliminary detection about which nodes may be Sybil nodes according to their position feature. If nodes locate in the network randomly and uniformly, once a node C scouts that it has the same distance to its two neighbors (node M and N), it will ask its other neighbors which are also the common neighbors of node M and node N for assistance to verify legitimacy of them. If one of the common neighbors (node C1) assures that the distance $|C_1M| \neq |C_1N|$, we can think of node M and node N as normal nodes. Conversely, if all of the common neighbors find node M and N have the same distance to them, they will be regard as suspicious nodes.

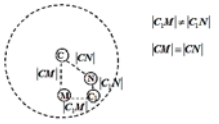

Fig. 1 The detection of normal node

RSSI [8] is applied to measure distance between two points. Unfortunately, the error of this method is above 10% due to environmental factors, the limit of hardware, etc. Therefore, we introduce confidence interval as the criterion to tell which node is impossible to be Sybil node. Result shows that with a confidence level 99%, if the difference between two measured distance $|OA|'$ and $|OB|'$ range from -10m to 10m, we will hold that the actual distance between O and A is the same as distance between O and B. However, this error range brings a certain misdetection rate and a false alarm, so we introduce data flow monitoring to distinguish Sybil nodes from suspicious nodes.

When the energy consumption of the network is balanced, the data flow transported by the same hop nodes should be approximately equal, while the data flow of Sybil nodes is larger than normal nodes'. Assume that the mean data flow of suspicious nodes is s and the range of data flow of the same hop node is (s_1, s_2), where $s_1 = \mu' - 3\sigma'$, $s_2 = \mu' + 3\sigma'$, μ' is the mean data for the same hop nodes and σ' is the standard deviation of data for the same hop nodes. The suspicious nodes will be regard as normal nodes if $s_1 \le s \le s_1$, otherwise, they are multiple identifies of Sybil node.

2.2 Selective forwarding

Position is a unique characteristic of Sybil attack. Therefore, the RSSI ranging described in section 'Shortening the network lifespan' is also use to detect suspicious nodes when Sybil attackers launch selective forwarding.

The adaptive threshold model [9] is introduced to determine suspicious nodes as Sybil nodes if the trust value T of a suspicious node is low than the trust threshold. The trust value T [10] of a node is shown in equation 1 and the threshold of trust value is defined as equation 2.

$$T = \frac{s+1}{s+f+2} \tag{1}$$

where s is the number of packets sent correctly and f is the number of packet dropped.

$$T(n) = t \times \{Pt + [1 - Pt] \times p(n)\} \tag{2}$$

where t is a variable($0 < t < 1$) used to ensure that the threshold is reasonable, Pt is the average forwarding rate of a certain monitor area and $p(n)$ is the forwarding rate of a sensor node in n^{th} turn .

2.3 Comprehensive security scheme

Based on two security schemes above, a comprehensive security scheme to defense against Sybil attack is put forward. It can be described as follows:

Step 1: Detect suspicious nodes based on RSSI ranging.

Step 2: Distinguish Sybil nodes from suspicious nodes if their data flow is abnormal or their trust value are lower than the threshold.

3 Simulation Analysis

3.1 Function of Detecting the Sybil Node

In this section, we use MATLAB to conduct simulations to evaluate the performance of proposed security scheme which aims at Sybil attack. The Sybil node's two identities are randomly generated by computer in the first turn. The forwarding rate of malicious nodes ranges from 30% to 50%. As it is shown in Figure 7, where horizontal axis represents the lifespan of the network while vertical axis represents the corresponding time when malicious nodes are detected (i.e. data collection turns in the network). Additionally, in trial 1, Sybil attackers undermine network with the purpose of shortening network lifespan. The 4 trials' results show that the malicious node is always detected and removed from the network before the sixth turn. That is to say our security scheme is able to detect the Sybil node rapidly.

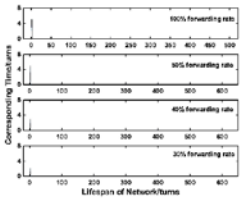

Fig. 2 The simulation results of security scheme

3.2 The Misdetection Rate and False Alarm Rate of Security Scheme

Some trials are carried out and they are divided into four groups according to the forwarding rate of malicious nodes. The experimental results of the first group (i.e. Sybil attackers undermine network with the purpose of shortening network lifespan.) are shown in Figure 3, where proposed security fails to work in experiment 3 and experiment 22. The misdetection of proposed security scheme is derived from the range error of RSSI. The misdetection rate of our security scheme (it means a Sybil node is mistaken for a normal node) can be described as equation 3.

$$\eta_1 = \frac{\text{misdetection amount}}{\text{experiment amount}} \tag{3}$$

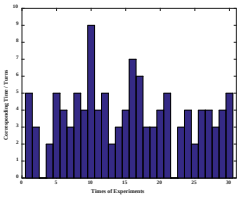

Fig.3 The simulation results of misdetection rate of the first group

At the same time, we can describe the false alarm rate of proposed security scheme (it means the normal nodes are mistaken for Sybil node) as follows.

$$\eta_2 = \frac{\text{false detection amount}}{\text{experiment amount}} \tag{4}$$

As it is shown in Table 1, the misdetection rate and the false alarm rate of proposed security scheme is reasonable. It is owing to further detection of suspicious nodes, which considers the data flow and trust value of Sybil nodes.

Table 1 Misdetection rate and false alarm rate of proposed security scheme

The forwarding rate of malicious nodes	Misdetection rate	False alarm rate
100%	6.7%	3.3%
50%	3.6%	4.5%
40%	3.4%	4.1%
30%	2.8%	3.7%

3.3 Simulation of the Network Lifespan.

The simulation results are shown in Figure 4. We can see that compared with the network without security scheme, the lifespan is prolonged by around 20% through using our security scheme. This result demonstrates that the security scheme proposed in this paper works effectively in defending Sybil attack.

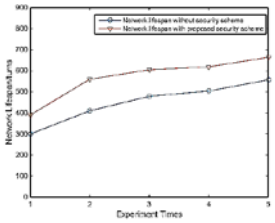

Fig.4 Simulation of the network lifespan

4. Conclusions

According to the characteristics of Sybil attack in wireless sensor network, a kind of security scheme based on RSSI and data transmission monitoring is put forward. It considers the range error of RSSI measurement and is modified by data transmission monitor and trust model. Besides, the EBRP[11] algorithm takes hops of node, the node residual energy and the density of the residual energy field into account. This is applied to MATLAB simulation. The simulation results indicate that the proposed security scheme can respond to Sybil attack rapidly with a misdetection rate of 6.7% and a false alarm rate of 3.3%. Additionally, the network lifespan is prolonged by 20% around using the proposed security scheme.

5. Acknowledgments

This research is based on Undergraduate Training Program for Innovation and Entrepreneurship -Secure Routing Techniques in Wireless Sensor Networks. It is also supported by the Fundamental Research Funds for the Central Universities (ZYGX2015J054). Finally, thanks Professor Yuanming Wu, who is the corresponding author of this paper.

References

[1] Douceur J R. The Sybil Attack, C. International Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, (2002) 251-260.

[2] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures, J. Ad Hoc Networks, (2003) 293-315.

[3] Newsome J et al. The sybil attack in sensor networks:analysis & defenses, C.International Symposium on Information Processing in Sensor Networks. IEEE,(2004) 259-268.

[4] Marian S, Mircea P. Sybil attack type detection in Wireless Sensor networks based on received signal strength indicator detection scheme, C. IEEE, Jubilee International Symposium on Applied Computational Intelligence and Informatics. (2015)121-124.

[5] Sivaraju S. Detection of Sybil attack in Mobile wireless sensor networks, J. Journal of Surface Engineered Materials & Advanced Technology. 2(2) (2012)256-262.

[6] Tian B et al. A novel sybil attack detection scheme for wireless sensor network, C. IEEE International Conference on Broadband Network & Multimedia Technology. (2013) 294-297.

[7] Dhamodharan et al. Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method, J. Scientific world journal, (2015)841267.

[8] Girod L et al. Locating Tiny Sensors in Time and Space: A Case Study, C. Werner B,ed. Proc. of the 2002 IEEE Int'l Conf. on Computer Design: VLSI in Computers and Processors. Freiburg: IEEE Computer Society. (2002)214-219.

[9] Hu Y, Wu Y, Wang H. Detection of Insider Selective Forwarding Attack Based on Monitor Node and Trust Mechanism in WSN, J. Wireless Sensor Network, 06(11) (2014)237-248.

[10] Jøsang A, et al. The beta reputation system, C. Bled Conference on Electronic Commerce. 2002.

[11] Wu Yuanming. An energy-balanced loop-free routing protocol for distributed wireless sensor networks, J. Sensor Networks.23(2) (2017) 123-131.