2012 IACSIT Hong Kong Conferences
IPCSIT vol. 29 (2012) © (2012) IACSIT Press, Singapore

A Secure Clustering Algorithm in Mobile Ad Hoc Networks

Yao Yu[+], Lincong Zhang

College of Information Science and Engineering, Northeastern University

Abstract. Ad Hoc networks are much vulnerable to be attacked because of its characteristics. In this paper, we analyze the security problem in the hierarchical mobile Ad Hoc networks. And then we propose a secure clustering algorithm based on reputation in defense of threats in clustering. In the algorithm, the nodes' reputation is used to improve security, which is evaluated by combining the experience of the node in the routing process. In addition, we consider degree and relative mobility in the clustering to guarantee the stability of clusters. The weight of each node is computed through considering the above three factors simultaneously. It is used to elect the secure backbone nodes in the networks. Moreover, it is efficient in the cluster rebuilding and healing. The simulation results show that the proposed algorithm can effectively improve the security and stability of network.

Keywords: Hierarchical Ad Hoc Networks, Clustering, Threat Security, Reputation.

1. Introduction

A mobile ad hoc network (MANET) is the cooperative engagement of a collection of wireless mobile nodes without any predefined infrastructure relied on to keep the network connected. As ad hoc networks do not have any fixed infrastructure, all network functions can be performed by the mobile nodes themselves in a self-organizing manner. This gives rise to much vulnerability in ad hoc networks, making the issue of security very important and challenging [1].

With the growth of ad hoc networks, the hierarchical structure has been receiving a much attention due to its scalability in large-scale networks. In recent years, many kinds of clustering algorithms are proposed to elect the backbone nodes and build cluster [2-4]. According to the various objectives and requirements, clustering schemes focus on different metrics, such as the node's mobility, energy, connection and load balance. The lowest-ID cluster algorithm the highest-degree cluster algorithm and the weighted clustering algorithm are the typical clustering algorithms.

Currently, most clustering algorithms assume that the network environment is reliable and has no threats. In fact, ad hoc networks are easy to be wiretapped, intruded and attacked, because of the open distributed network structure. Clusterhead and gateway are the key nodes (i.e., backbone nodes) in hierarchical ad hoc networks. If they are intruded, the network performance must decrease seriously. Therefore, we need to promote an effective detection measure to the bone cluster structure for network security, such as clustering in hierarchical ad hoc networks. In this paper, we propose a secure clustering algorithm based on reputation (SCAR). The nodes' reputation is used to improve security, which is evaluated by combining the experience of the node in the routing process. In addition, we consider degree and relative mobility in the clustering to guarantee the stability of clusters. The weight of each node is computed through considering the above three factors simultaneously. It is used to elect the secure backbone nodes in the networks. Moreover, it is efficient in the cluster rebuilding and healing.

[+] Corresponding author. Tel.: + 86 24 83684219.
E-mail address: yuyao@ise.neu.edu.cn.

The rest of this paper is organized as follows. Section 2 describes attacks in clustering. Section 3 presents the reputation evaluation mechanism. Section 4 proposes SCAR in detail. Section 5 shows the simulation results and analysis of the proposed algorithm's performance. Section 6 concludes this paper.

2. Attack in clustering

According to the impact of the malicious nodes in clustering, we divide the attack into direct clustering attack and indirect clustering attack.

In the direct clustering attack, the malicious nodes discourage the clusterhead election procedure, which will make the network difficult to build the clusters. Moreover, it is unable to establish the routing in clusters. Thus, this kind of attack can further destroy the communication in the networks. Flooding [5] and rushing [6] are the typical direct clustering attack.

To complete the indirect clustering attack successfully, firstly malicious nodes should be chosen as clusterheads with the benefit of fake metrics (e.g., degree and mobility) in clusterhead election procedure. After that, these malicious clusterheads can carry out diverse attacks in the routing. Compared with the direct one, the indirect clustering attack is more difficult to be detected. Wormhole attack [7] is an example of this kind attack. In the clustering, the attackers are successful to be the gateway nodes, and then they attack the network as the role of the backbone nodes.

Figure 1 shows the wormhole attack in the process of clustering. Node A and B are the malicious nodes in the wormhole attack, and they are respectively in two widely separated clusters C and D. They associate with each other and send the cluster information to each other through the wormhole tunnel they build. And then, the malicious node can cheat the clusterhead and be elected as the gateway node. That is, the wormhole attackers build a backbone link C-A-B-D. They can carry out many kinds of attacks in this link, such as blackhole attack and resource consuming attack.

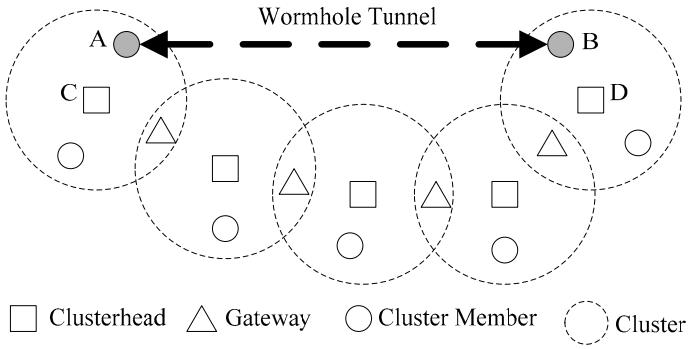

Fig. 1: Wormhole attack in the process of clustering

3. Reputation Evaluation

In our reputation evaluation mechanism, the reputation is evaluated by combining the experience of the node in the routing process. We can master the security situation of nodes through the reputation value to choose the nodes with higher value, thus ensuring communication reliability.

The reputation of the node is evaluated through the capability of the node in dealing with packets in the routing process. In ad hoc networks, the behaviours of the node involve processing routing control messages and data packets in the routing. Attack measures of these two kinds of packets include forging, deleting, and tampering. Considering these, attack actions can be divided into selfish and malicious attacks. In a selfish attack, the nodes may drop the data packets entirely or proportionally to save energy. In a malicious attack, the nodes may transact the routing control messages abnormally, which can result in increasing resource consumption and destroying the routing process. Therefore, we classify the reputation of the node into Selfish Reputation (SR) and Malicious Reputation (MR), which denote the different aspects of nodes in the routing process.

The manifestation of a selfish attack is that the attacker drops the data packets in proportion, and its damage potential changes from quantity to quality, which can indicate the risk intensity through the accumulation of dropped packets.

We assume that the activity of each node is random (i.e., the moving velocity of the node is uncertain.). Moreover, we evaluate the BR of each node by period and we assume that the numbers of positive and negative samples are S and F, respectively. Bayesian theory can be used to evaluate the quality of service. We have deduced the reputation value in our previous work [8].The selfish reputation value is written as

$$R_f = \frac{S+1}{S+F+2} \tag{1}$$

Compared with selfish attack, a malicious attack is sudden, and if the condition the attack needs to function is satisfied, it can destroy the network to a certain extent. Therefore, we set different values for the two kinds of reputation evaluation. In SR, we set the value to 1. In MR, the value of a will change with the degree of attack; that is, the more serious the attack, the higher the values are.

The reputation value can be calculated as follows.

$$R = \omega_f R_f + \omega_m R_m \quad (\omega_f + \omega_M = 1) \tag{2}$$

4. Clustering Algorithm

In this paper, we propose a secure clustering algorithm SCAR, which takes into account a combined weight metric, including the reputation value, the node' degree [9] and the relative mobility [10]. The weight is calculated as follow.

(1) Clusterhead election

In the initial of establishing cluster, the nodes are assigned as the role (i.e., clusterhead, gateway and cluster member) in the cluster through the clustering procedure.

Each node broadcasts Hello message to its neighbor nodes periodically for connectivity. In our algorithm, the weight information is carried in Hello message.

When the node receives its neighbor nodes' Hello messages, it updates the related nodes' reputation value. In addition, the node can update its degree and mobility, according to the number of Hello messages received and the transmission power, respectively.

After receiving Hello message in some period, the node gets its initial weight. Then the node sends its weight through the broadcasted Hello message. Compared with other nodes' weight, the node that has the highest weight is elected as clusterhead. If the node A receives the clusterhead message from its neighbor node B, and node B's reputation value is higher than A's, A will send the message to node B to join in its cluster. If node A hasn't received the clusterhead's message during a period, it becomes an isolate clusterhead which has no cluster member.

(2) Cluster update

Cluster update includes cluster rebuild and cluster healing.

Although the cluster is established, the topology of the network still may change due to the mobility of node, the descending of the energy and other factors. Thus, the node may leave the original cluster, or the node may join in the cluster. The original cluster will not be effective. This is cluster reestablishment.

In the cluster healing procedure, we set the related threshold according the node's role, i.e., T_{CH}, T_{GW} and T_{CM} (T_{CH}>T_{GW}>T_{CM}) are the thresholds of clusterhead, gateway and cluster member, respectively. When the node's reputation value is higher than its role's reputation threshold, it is suspicious. And then, if this node is clusterhead or gateway, search its neighbor's reputation value. If it is higher than this suspicious node's, cancel the suspicious node's role of clusterhead, and elect this node as clusterhead. Else, keep the suspicious node's role. If the suspicious node is cluster member, put it into the black list and isolate from the network.

5. Simulation

In this paper, we performed our experiment on an NS-2 simulator, and compare the performance of SCAR with WCA. WCA is a weighted clustering algorithm which considers the degree, transmission power, mobility and battery power of nodes in clusterhead election procedure [4]. We simulated a mobile hierarchical ad hoc network with 50 nodes. Each node can move in a square range of 1000 m by 1000 m. The initial positions of the nodes are random on the surface, and all nodes move arbitrarily with the maximum speed of 3 meters/sec. The simulation work considers the resisting performance of SCAR against both malicious and selfish attacks.

Figure 2 shows the variation of the overhead in clustering procedure under the rushing attack. From the figure, we can easily find that the overhead of WCA is more than SCAR's. This is due to the fact that when the malicious nodes send numerous clusterhead request messages, SCAR can find them rapidly under the support of the reputation scheme. And then, these malicious nodes will be isolated from the communication of network. Cluster recovery can maintain the normal correspond of the whole network, which makes the overhead descending.

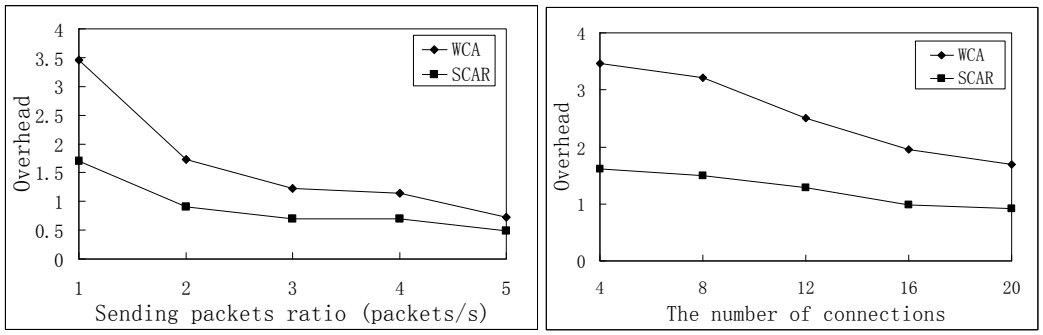

Fig. 2: The performance of routing overhead under rushing attack

Figure 3(a) shows the variation of packet delivery ratio under the wormhole attack. We observe that the packet delivery ratio of SCAR is 20% higher than WCA's. The packet delivery ratio is an important index in the evaluation of the performance of routing security. The packet delivery ratio is defined as the ratio of the number of data packets received by the destinations over the number of data packets sent by the sources. This is because that malicious nodes associate with each other and forge as gateway. Moreover, they destroy the routing through wormhole tunnel and cause the dropping of packets, which will disturb the correspondence of network and make the packet delivery ratio descending. In SCAR, the reputation scheme can find the malicious nodes from the reputation value. This kind of nodes will be not allowed to be the backbone nodes. This can effectively prevent the wormhole nodes' damage, and make the network the higher packet delivery ratio. Figure 3(b) shows the variation of the overhead under the wormhole attack. We can find that the overhead of SCAR is a little higher than that of WCA, and the growth rate is 5%. It is caused by the reputation update.

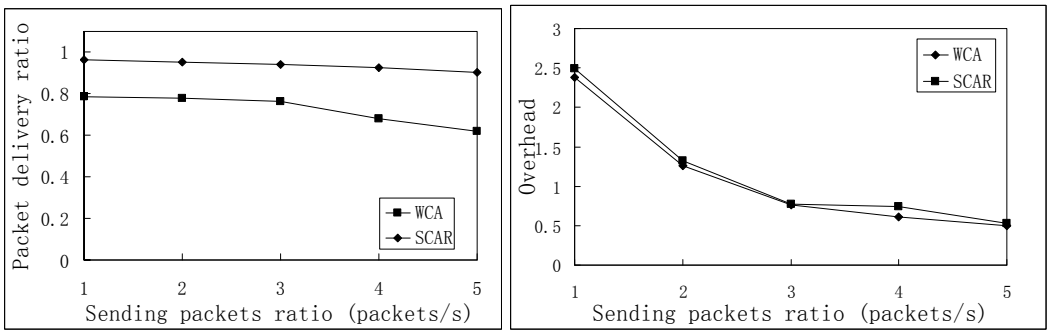

Fig. 3: The performance under wormhole attack

6. Conclusion

We research on the threat security in hierarchical ad hoc networks, and proposed a secure cluster algorithm based on reputation. In this algorithm, a reputation evaluation mechanism based on the behaviors of nodes is built to achieve accurate definition and precise quantization of reputation for nodes in the

network. To improve the reliability of a cluster structure, this algorithm considers the reputation, correlation and mobility of nodes in the process of electing cluster heads and gateways. Moreover, the rebuilding and recovering mechanism in the algorithm is able to resist attacks on the cluster structure. Simulation results show that the proposed algorithm can improve the security of clustering, and obtain good performance through rapid detecting, diagnosing and reacting to various invasions.

7. Acknowledgements

This work is supported by Specialized Research Fund for the Doctoral Program of Higher Education (20110042120035, 20110042110023), Fundamental Research Funds for the Central Universities (N100304009, N110204001), National Natural Science Foundation of China (61172051), and Fok Ying Tung Education Foundation (121065).

8. References

[1] J. Luo, D. Ye, L. Xue, and M. Fan. A survey of multicast routing protocols for mobile Ad-Hoc networks. *IEEE Communications Surveys & Tutorials*, 2009, **11** (1): 78-91.

[2] D. Wei and H. A. Chan. Clustering Ad Hoc Networks: Schemes and Classifications. *IEEE Communications Society on Sensor and Ad Hoc Communications and Networks*. 2006, pp. 920 – 926.

[3] A. Akbari, A. Khosrozadeh and N. Lasemi. Clustering Algorithm in Mobile Ad Hoc Networks. *Computer Sciences and Convergence Information Technology*. 2009, pp. 1509-1513.

[4] M. Chatterjee, S. K. Das and D. Turgut. WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks. *Cluster Computing*. 2002, **5** (2): 193–204.

[5] J. Kuo and W. Liao. Hop Count Distance in Flooding-Based Mobile Ad Hoc Networks with High Node Density. *IEEE Transaction on Vehicular Technology*. 2007, **56** (3): 1357-1365.

[6] G. Acs, L. Buttyan and I. Vajda. Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks. *IEEE Transaction on Mobile Computing*. 2006, **5** (11): 1533-1546.

[7] M. A. Azer, S. M. ElKAssas, A. W. F. Hassan and M.S. El-Soudani. Intrusion Detection for Wormhole Attacks in Ad hoc Networks a Survey and a Proposed Decentralized Scheme. *Availability, Reliability and Security*. 2008, pp. 636-641.

[8] Y. Yu, L. Guo, X. Wang and C. Liu. Routing security scheme based on reputation evaluation in hierarchical ad hoc networks. *Computer Networks.* 2010, **54** (9): 1460-1469.

[9] E. M. Royer, P. M. Melliar-Smith, and L. E. Moser. An Analysis of the Optimum Node Density for Ad hoc Mobile Networks. *IEEE International Conference on Communications.* 2001, pp. 857-861.

[10] K. Xu, X. Hong and M. Gerla. An Ad Hoc Network with Mobile Backbones. *International Conference on Communications.* 2002, pp. 3138-3143.