Detecting Sub-Marine Attack with Safe-triangle and GPS in Ad hoc Network

XiaoYang Zhang Yasushi Wakahara
Department of Frontier Informatics, Graduate School of Frontier Sciences, The University of Tokyo
zhang@cnl.k.u-tokyo.ac.jp, wakahara@nc.u-tokyo.ac.jp

1. Introduction

In this paper, we will be focusing on detecting a new attack which we named sub-marine attack, and which may result in black hole attack and DoS attack when previously proposed secure on demand routing protocols [1] are used in an ad hoc network. The sub-marine attack can occur when a malicious node receives a RREQ (Route Request) message. Generally, in the RREQ phase, the secure on demand routing protocols often use cryptography-based method such as digital signature to verify a node. However, in the sub-marine attack, the malicious node does nothing but just broadcasts the RREQ message to other nodes as soon as it receives a RREQ message and therefore, this malicious node joins the route path between a source node and a destination node. Moreover, in general terms, a malicious node can forward a message by using a higher gain antenna [2] or a larger power range. Even worse, a malicious node can send the RREQ message directly to the destination node. Then, the malicious node can do various attacks without being detected. In contrast to other malicious attacks in the ad hoc network, the sub-marine attack node changes nothing of the RREQ message and no node will know that there exists such a malicious node.

As we know, in order to limit the overhead of the flooding due to broadcast, each node typically forwards only one RREQ message for the same destination node and the destination node will also select one route path which contains the least hop counts. By playing the sub-marine attack, a node can not only forward a message in a fastest way (since malicious node just rebroadcasts the message without any processing of the message) but also join a route path which has less hop counts. Therefore, the route path which contains such a malicious node will be selected as the final route path with very high possibility.

To the best of our knowledge, we are the first who identified and defined the concept of sub-marine attack that cannot be defended by so far proposed secure routing methods effectively. Although some previous methods [3,4,5,6,7] which use the symmetric key scheme might give some help to avoid the sub-marine attack, they usually use some threshold that lead to some inaccuracy in the detection of attackers or has high overhead in terms of the computational cost.

In order to defend against this sub-marine attack, we propose a GPS based safe triangle method which can be easily deployed with a little modification to the various existing routing protocols.

2. A Proposed Method--GPS Based Safe Triangle Method

First of all, every node has a key pair of a public key and a private key and every node can get other nodes' public keys. When a node sends a message, it always signs the message with its own private key so that any other nodes can verify the sender of the message by the use of its public key. Second, all of the normal or legitimate nodes in the network have the same power range and the malicious node can have a different and larger power range. Third, neither source node nor destination node is malicious since a sub-marine attack must happen between two normal nodes. Finally, every node has a GPS which can derive its position coordinates values.

In the RREQ phase, if an intermediate node receives a RREQ message from one of its neighbors, it will first use the public key of the sender to verify the sender of this message and register this public key of the neighbor into its neighbor information table (NIT). NIT is defined as a table in each node to register its one-hop neighbor nodes' public keys that are obtained during the RREQ phase. However, if the intermediate node finds that after verifying the sender of this RREQ message, the public key already exists in the NIT, this intermediate node will judge that the RREQ message just arrived must have been relayed by a malicious node. When a sub-marine attacker receives a message, it will just rebroadcast it, and the signature of the message will not be changed. Our method takes advantage of this point of no change in order to detect the sub-marine attacker. On the other hand, if this intermediate node receives a normal RREQ message, after verifying the sender of this RREQ message, this intermediate node will encrypt this RREQ message by its own private key in order that the next node can verify the sender of the RREQ.

For an example network in Fig. 1, node B receives [(RREQ)a, IDa] from node A and a malicious node M also receives [(RREQ)a, IDa], where [(RREQ)x, IDx] in general denotes the RREQ message broadcasted and signed by node X and the ID of node X nodes and this ID is used by other nodes to identify node X and thus its correct public key, and [(RREQ)x, IDx] may be expressed with (RREQ)x for short hereinafter of this paper. Then, node M will just rebroadcast (RREQ)a. However, if node B is in the power range of node M, node B will receive the same (RREQ)a from node M and then node B can judge that this message must have been relayed by the malicious node M as shown in Fig.1.

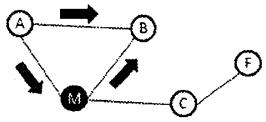

Fig.1 Example illustrating safe triangle

From above figure example, it is observed that nodes A, B and M form a triangle and it is concluded that if two normal nodes and one sub-marine attacker can communicate with one another, the sub-marine attacker can be detected in an ad hoc network. In more concrete, a sub-marine attacker receives a RREQ message from a normal node and if there is another normal node in addition to the malicious node in the power range of the first normal node at the same time, the second normal node will receive the same RREQ message twice. Thus, this second normal node can detect out the malicious node.

In the same example, once node B finds out that it has received (RREQ)a relayed by a malicious node, it will broadcast an alarm message (Aa)b which means there is a malicious node between nodes A and B, where an alarm message (Ay)x in general denotes a sub-marine attacker detection alarm message signed by node X and means that there is a malicious node between node X and node Y since one of the messages sent from node Y is relayed by a malicious node. (Aa)b will be relayed to the neighbor nodes of this malicious node. Since sub-marine attacker just rebroadcasts the alarm message, (Aa)b will be relayed to the nodes which are neighbors of this malicious node. These nodes will find a public key of node A but no public key of node B registered in their NITs and learn that this message was relayed by a malicious node.

However, when a malicious node plays a sub-marine attack, there might be no safe triangle formed. Therefore, we use GPS to help us to detect sub-marine attacker in such a case.

Suppose that there is a malicious node M between nodes A and B,

node M is not detected out in the RREQ phase and that a route containing A-M-B is selected by the destination node D. When each node including B relays the RREP message, it will add its own position coordinates such as (Xb,Yb) derived by GPS into the message. Node A receives this RREP and calculates the distance Dab between node B and itself based on their position information. Since nodes A, B and M do not form a triangle, Dab is larger than the power range of node A. Therefore, node A can detect out that there is a sub-marine attacker between node B and itself if node A receives some message that is considered to be directly transmitted by node B.

3. Evaluation

We first use the following metrics to evaluate our safe triangle method without using GPS:

- Recall=(the number of malicious node which are detected as malicious)/ (the whole number of malicious nodes)
- Precision=(the number of malicious nodes which are detected as malicious)/(the number of nodes which are detected as malicious)
- False Positive=the number of normal nodes which are detected as malicious
- False Negative=the number of malicious nodes which are not detected as malicious

From the definition of the false positive, we conclude that the false positive is 0 in our method and thus the precision is always 1.

Table 1 Simulation scenario 1:

Parameter	Value
Square size	1000m*1000m
Number of normal nodes	10
Number of malicious nodes	1
Power range of every node	100m--650m

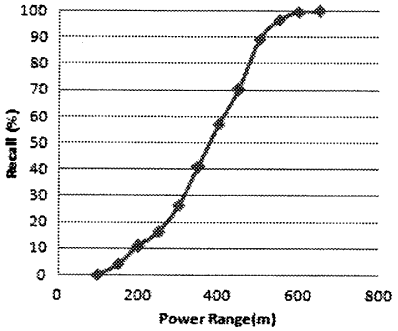

Fig.2 Results of simulation 1

Table 1 shows the scenario for evaluation by computer simulation 1 and Fig. 2 shows its results of the recall versus the power range. From the results, we could conclude that if every node including a malicious one uses a larger power range, the malicious node will be detected out with larger probability. This is because more nodes receive the broadcast message from a node when the node uses a larger power range to broadcast the message. Thus, with our method, the probability to form a safe triangle becomes larger.

Table 2 shows the scenario for simulation 2 and Fig.3 shows its results of the recall versus the number of normal nodes.

Table 2 Simulation scenario 2:

Parameter	Value
Square size	1000m*1000m
Number of normal nodes	5--45
Number of malicious nodes	1
Power range of every node	100m, 300m, 500m

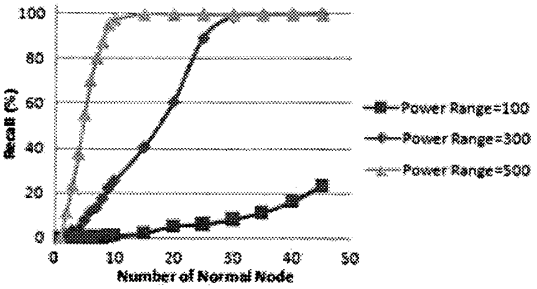

Fig.3 Results of simulation 2

The results in Fig. 3 show that if there are more normal nodes, the probability of detecting out a malicious node will be larger.

At the beginning of the paper, we mentioned that if a malicious node uses a larger power range or if there are more nodes in the network, the sub-marine attack will be much more harmful. However, with our safe triangle, we can detect a malicious node easier in such a much worse condition.

In order to improve the recall of safe triangle method, we combine GPS. In theory, by combining the triangle method with the GPS, we can detect the malicious node with 100 percent. However, in practice, we should consider the error of GPS. We assume GPS's error is from –e to +e. Here, we analyze the largest error in our method. Suppose the correct distance between two nodes is D, and that the largest error between these two nodes is 2*e. Then, there are some false negatives when (D-R)<2*e, where R is the power range and it is our future work to evaluate the recall when we use the GPS.

4. Conclusion and Future Work

In this paper, we proposed a GPS based safe triangle method to detect a newly defined routing attack—sub-marine attack. From some simulation results, we concluded that our proposed method can offer an effective way to detect and avoid the sub-marine attack.

In the future, we will make further related research as follows: we will clarify the proposed method in more details and make a study on how to detect and cope with the collusion of sub-marine attackers. We will also consider the model where every node moves frequently in the network so that we can evaluate the proposed method considering its overall function including the maintenance of NIT.

Reference

[1] Hongmei Deng, Wei Li, and Dharma P. Agarwal,"Routing Security in Wireless Ad Hoc Networks", University of Cincinnati, IEEE Communications magazine, October 2002.

[2] V. Karpijoki, "Security in Ad Hoc Networks", Seminar on Net Work Security, HUT TML 2000

[3] C.E. Perkins, S.R. Das, and E. Royer, "Ad-Hoc on Demand Distance Vector (AODV)", March2000, http://www.ietf.org/internet-drafts/

[4] Lidong zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE network, special issue, November/December 1999.

[5] Yi-Chun Hu, Adrian Perrig, "A Survey of Secure Wireless Ad Hoc Routing", IEEE Security and Privacy May/June 2004.

[6] Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" WiSe 2003, September 19, 2003, San Diego, California, USA.

[7] A.Heffernan, Protection of BGP via the TCP MD5 signature option, RFC 2385