Chapter 21
Security Model Based on Cluster Formation in Ad Hoc Network

Shuyu Hu

Abstract We apply the idea of systems analysis and integration to constructing the AD hoc network security model based on cluster formation in this paper. In this security model for ad hoc networks, the initial nodes are authorized by the user, or validated by the cluster headers in other clusters when the cluster is created. The cluster header is elected by all nodes in the cluster, and there is a temporary cluster header in charge of the cluster header elections.

Keywords Ad hoc networks · Cluster formation · Security

21.1 Introduction

Mobile Ad Hoc networks are dynamic self-organizing networks, which are built by some mobile nodes. Those mobile nodes are capable of wireless communication. Mobile Ad Hoc networks have the arbitrary and temporary topology [1]. In the networks, each node can be used as a host or router. Mobile terminal has a routing function, and can make up arbitrary topology by wireless network connection [2, 3, 4]. This kind of network can not only work independently but also connect with the Internet or a cellular wireless network [5, 6, 7]. Compared with the usual networks, the mobile Ad Hoc network has some special features: self-organization, dynamic network topology, multi-hop communication route, limited wireless communication bandwidth, limited host energy, distributed network, and so on [8, 9, 10].

S. Hu (✉)
Liaoning Medical University, Jinzhou 121001, Liaoning, China
e-mail: hushuyu@hrsk.net

Z. Zhong (ed.), *Proceedings of the International Conference on Information Engineering and Applications (IEA) 2012*, Lecture Notes in Electrical Engineering 219,
DOI: 10.1007/978-1-4471-4853-1_21, © Springer-Verlag London 2013

The security of mobile ad hoc network has been the hotspot of current research. Compared with the fixed wired networks, mobile Ad Hoc networks face more security threats [11, 12, 13]. In the fixed network, the enemy needs to lap cable to wiretap, and to find loopholes of the firewall or gateway to access internal resources. But for mobile Ad Hoc networks, wireless channel make wiretap become probable anywhere, with the mobility of nodes making the networks without border and the firewall unable to play a role [14, 15]. Mobile Ad Hoc networks face more threats than fixed networks, such as wiretap, falsification of identity, replay, message tampering and refuse services, and so on, and therefore need security protection [16, 17].

At present, researches on cluster technology of mobile Ad Hoc network are still at the initial stages. There are still many unresolved issues in modeling of mobile Ad Hoc Networks, such as what is the appropriate architecture? What is the best framework model? How to authorize nodes to create networks? How to validate the security of mobile Ad Hoc network? And so on.

21.2 A Wireless a Hoc Network Ids Model Based on the Cluster

21.2.1 Assumptions

We proposed a mobile IDS model based on the cluster. As its structure shows in Fig. 21.1, the assumptions are as follows:

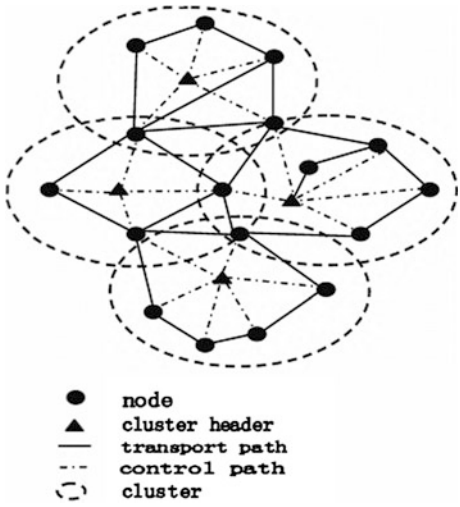

Fig. 21.1 Cluster formation

(1) Each node is inserted a GPS positioning system. And by doing so, the cluster header can get each node's moving speed, direction and orientation in the cluster.
(2) Wireless signal propagations are in accordace with fee space propagation model [2], and use the prediction method proposed in literature [3]. This method assumed that the strength of the received signal of the model are mainly decided by the distance between receiver and the sender.
(3) Each node's effective radiate distance are equal: specifically, if one node is in the other node's radiate rage, then they are adjacent nodes and have a line between them.

21.2.2 Cluster Formation

There are many conditions of formatting a cluster, as shown in Fig. 21.1.

The initial nodes must be authorized by the user or validated by the cluster headers in other clusters if they what create a cluster.

(1) Each discrete node indicates itself by sending a HLLO message and authentication handshake.
(2) There is only one hop distance between each the node in a cluster.
(3) The number of nodes in a cluster is limited. If there are too many nodes in one hop distance, some nodes will create a new cluster.
(4) The created new cluster must be able to maintain the channel with the cluster header validating it. If the channel is brea, the initial node needs to be re-authorized or re-validated and cluster re-created.

The process of Initial nodes' cluster formation:

If the initial node X is authorized by the user, then the user input the initial key to generate the key pair for the initial node.

If the initial node X is authorized by the cluster head of other cluster, firstly, this node will generate the key parr $M_x\{SK_x, PK_x\}$ by assembling the public key of the cluster head and the random number generated by itself. Secondly, PK_x will be encrypted by SK_x and distributed to the cluster head for certification.

SK_x is the secret key of this. There is no node in the network knows its contents. PK_x is the initial node's public key and known by all nodes in the network. Set the number of cluster nodes is m, the initial node broadcast it's PK_x to m neighbors node in its one hop.

The nodes which receive packets will generate the key pair $M_x\{SK_x, PK_x\}$ by assembling its public key of the cluster head and the random number generated by itself. PK_x will be encrypted by PK_x and distributed to the initial node X.

While X receive this package, it will decrypt it will decrypt it SK_x, and obtain public keys of each nodes.

X issue Certificate $CT < V_i, PK_i, N_i, t, T >$ for each node, it meas that: in the time interval $[t,t + T]$, persona public key is PK_t elective.

21.2.3 Election of the Cluster Header

Cluster headers are elected by nodes in the cluster; the following factors need to be considered in election:

(1) The security of nodes: whether the initial nodes are authorized by users or validated by the cluster headers in other clusters.
(2) The residual energy: Mobile Ad Hoc network nodes' battery power is limited, the residual energy is very important.
(3) The configuration parameters of the performance: to choose good performance, high efficiency, high hardware parameters as the cluster header as much as possible.
(4) Dynamic parameter: the node's mobility speed, moving direction, and the distance between nodes are the most important data; we can calculate the dynamic parameter of the node by using them.
(5) The cluster header control and manage the entire cluster and it does not participate in the cluster Routing Forwarding when the cluster header is not as sender or receiver in the cluster.

The election procedures of the Cluster header are as follows:

If the initial node was not validated by the cluster header in other clusters, then the initial node works as a temporary cluster header, and it also can be elected as the official cluster header in the following creation process. If the initial node has been validated by the cluster header in other clusters, then the cluster header in other clusters works as a temporary cluster header, and it cannot be elected as the official cluster header in the following creation process.

At first, each node sends its vote to the temporary cluster header, then the temporary cluster header calculates and compares the votes, and then select the official cluster header.

Assuming the nodes amount in a cluster as m, the nodes respectively are decrypted as: $X_1, X_2, X_3, \ldots\ldots X_m$ the remaining energy of the node X, is A_i, the configuration parameter of the performance is B_i; the dynamic parameter is C_i, the cluster header election function is:

$$W(X_i) = eA_i + fB_i + gC_i \tag{21.1}$$

where e, *f*, *g* are weights;

Node X_i sends its parameters of speed, coordinates, id, and direction of movement to its adjacent X_k.

X_k receive the information of X_i, then calculate the predicted connection time using the method proposed in the literature [4]:

Assuming the speed of node X_i is V_i, the adjacent nodes X_k's speed is V_k, node X_i's position coordinates is (x_i, y_i), the adjacent nodes X_k's position coordinates is (x_k, y_k), the node X_i's mobile direction is θ_i $(0 < \theta_i < 2\pi)$, the adjacent nodes X_k's mobile direction is θ_k $(0 < \theta_k < 2\pi)$, the distance between two nodes is S:.

$$C_i = \frac{(a(x_i - x_k) + c(y_i - y_k)) + \sqrt{(a^2 + c^2)s^2 - (a(y_i - y_k) - (x_i - x_k)c)^2}}{a^2 + c^2} \tag{21.2}$$

in the formula:

$$a = v_i \cos\theta_i - v_k \cos\theta_k \tag{21.3}$$

$$c = v_i \sin\theta_i - v_k \sin\theta_k \tag{21.4}$$

$$S = \sqrt{(x_i - x_k)^2 + (y_i - y_k)^2} \tag{21.5}$$

Assuming the shortest maintain time of the links (x_i to x_k) is $T_{\min}$, compared $C_i < T_{\min}$, if $C_i < T_{\min}$, then calculate the following associated values:

Which E_i is the node's residual energy, $E_{\max}$ is maximum energy capacity of the node;

$$Bi = kM_i + fN_i + hP_i \tag{21.6}$$

Where, k, f, h as the wrights, M_i is the parameter of the CPU's operation rate, N_i is the memory parameter, P_i is parameter of the network throughput;

$$F(X_i) = eA_i + fB_i \tag{21.7}$$

Where, e, f is the wright?

Then, send the value of $F(X_i)$, C_i to the cluster header;

Compare the values of $W(X_1)$, $W(X_2) \cdots\cdots W(X_m)$, the largest one is the cluster header;

21.2.4 To Add and Remove Nodes in Cluster

Each node in cluster can be added or removed from the cluster, as shown in Fig. 21.2:

Each node can change their places in AD HOC network. So when a node X moves outside the scope of the cluster W, the cluster header Wm will send transfer messages including authentication information to the cluster header Mm of the cluster M base on the mobile path of the node X. While node X is nearing Mm, X will send a join request including its authentication information to m. M receives

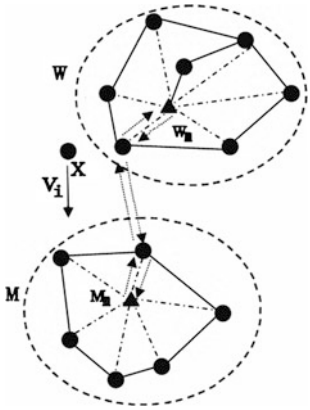

Fig. 21.2 Nodes in cluster to join and remove

the request and checks it with messages. If consistent, Mm will agree X to become the member of cluster M, and W will send a conf message to Wm.

Wm will record the event into log when it receive message from Mm, then update the cluster information, and delete the relevant information of node X in the W.

If the node X moves outside the cluster W, and not near any cluster (it is judged by the direction of node X's movement). The cluster header Wm will send transfer packets to all the cluster headers in the Ad Hoc network until receiving the message that this node had been attended any cluster. Then, it records this event into its log, updates the cluster's information, and deletes the relevant information of node X in the W.

21.3 Conclusion

If the cluster heads do not play any role as a sender or receiver, they also need not participate in the route exchanging and data forwarding. They are in charge of resource scheduling and intrusion detection control of this cluster. Although a cluster model of the Ad Hoc network is given in this article, its algorithm still needs more in-depth study, and also intrusion detection of cluster.

References

1. Goldsmith A, Wicker SB (2002) Design challenges for energy constrained Ad hoc wireless networks. IEEE Wireless Commun 9(4):8–27
2. Kachirski O, Guha R (2002) Intrusion detection using mobile agents in wireless Ad Hoc networks. IEEE workshop on knowledge media networking (KMN'02), Tokyo, Japan vol 15, issue no 12, pp 153–158
3. Tseng C-Y, Balasubramanyam P (2003) Based intrusion Detection system for AODV on Security of Ad Hoc and Sensor Networks (SA VA), USA 10(9):135–139

4. Royer E, Toh CK (1999) A review of current routing protocols for ad hoc mobile wireless network. IEEE Pers Commun 6(2):46–55
5. Capkun S, Hubaux J-P, Buttyan L (2003) Mobility helps security in Ad hoc networks. The fourth ACM interational symposium on mobile Ad hoc networking and computing. Annapolis, vol 6, issue no 4, Maryland, pp 46–56
6. Zhou L, Hass ZJ (1999) Securing ad hoc networks. IEEE Netw 13(6):24–30
7. Johnson DB, Waltz DA (1996) Dynamic source routing in ad hoc wireless, TImielinski. HK 4th. Mobile computing, vol 6, issue no 3, Kluwer Academic Publisher, Dordrecht, pp 153–181
8. Zhang Y, Lee W (2007) Intrusion detection in wireless Ad2Hoc networks, Proceedings of the sixth international conference on mobile computing and networking (MobiCom 2000), Boston, vol 7, issue no 3, pp 275–283
9. Ping Y, Jiag Y-C, Zhang S-yY, Zhong Y-P (2005) A survey of security for mobile ad hoc networks. Acta Electronica Sinica 31(2):161–165
10. Proctor PE (2002) The practical intrusion detection Handbook. vol 34, issue no 27, Prentice Hall, New York, pp 627–634
11. Ghosh AK, Schwartzbard A (2009) A study in using neural network for anomaly and misuse detection. In: Proceedings of the 8th USENIX security symposium, vol 14, issue no 9, pp 74–82
12. Zhag Y, Lee W (2000) Intrusion detection in wireless ad hoc networks. The 6th Annual It conference on mobile computing and networking, Boston, vol 12, issue no 8, pp 275–283
13. Montenegro G, Castelluccia C (2002) Statistically unique and cryptographically verifable (SUCV) identifers and addresses. Netw Sec Conf 18(9):76–85
14. Zhou H, Li J, Zhao N, Dai F, Jiang R (2008) An intrusion detection system model for Ad Hoc networks based on the adjacent agent. In: Proceedings of 2008 international conference on multimedia and information technology (MMT 2008), IEEE Computer Society, vol 12, issue no 9, Three Gorges, China, pp 598–601, Dec 30–31
15. Zhao N, Dai F, Yu Y, Li T (2008) An extended process model supporting software evolution. In: Proceedings of 2008 International symposium on intelligent information technology application (IITA 2008), vol 12, issue no 9, IEEE Computer Society, Shanghai, China, pp 1013–1016
16. Zhao N, Yang Z, Li T (2005) A method of modelling and performance analysis for concurrent development process of software. In: Proceedings of the 11th joint international computer conference, vol 24, issue no 11, World Scientific, New Jersey, pp 803–809
17. Zhao N, Li T, Yang LL, Yu Y, Dai F, Zhang W (2009) The resource optimization of software evolution processes. In: Proceedings of 2009 international conference on advanced computer control (ICACC 2009), vol 12, issue no 8, Singapore, pp 332–336