移动自组网中一种基于分簇的信任评估方案*)

王寒凝　王亚弟　费晓飞　韩继红

(解放军信息工程大学电子技术学院　郑州 450004)

摘　要　移动自组网中信任评估方案主要用来防止网络中不良行为节点的安全威胁，本文提出一种基于分簇的信任评估方案。节点通过参考簇首发放的信任值证书可以对陌生节点进行准确有效的信任评估，并给出了该方案所涉及的信任评估公式以及簇的形成与管理的部分具体措施。它克服了移动自组网内传统信任评估方案中陌生节点间受限的信息交流的问题，减少了所需的存储空间，最后针对移动自组网部分安全问题给出了方案分析。

关键词　移动自组网，安全，信任评估，分簇

Cluster-Based Trust Evaluation Scheme in an Ad Hoc Network

WANG Han-Ning　WANG Ya-Di　FEI Xiao-Fei　HAN Ji-Hong

(Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou 450004)

Abstract　The important intent of the trust evaluation scheme is to resist the secure risk of misbehavior of node in an ad hoc network, and a cluster-based trust evaluation scheme is proposed in this thesis. The head issues a trust value certificate that can be referred to by its non-neighbor nodes. In this way, an evaluation of an unfamiliar node's trust can be done very efficiently and precisely. In this paper, we present a trust evaluation metric using this scheme and some operations for forming and managing a cluster. In contrast to the traditional schemes, it overcomes the limited information about unfamiliar nodes and reduces the required memory space. An analysis of the proposed scheme over some security problems is also presented.

Keywords　Ad hoc network, Security, Trust evaluation, Clustering

1　引言

移动自组网(MANET, mobile ad hoc networks)是由一组带有无线收发装置的移动节点组成的一个多跳的临时性自治网络。目前采用的主要安全策略可归为两类：基于预防技术的安全策略和基于侦测、反应技术的安全策略。属于后者的信任评估方案主要通过发现和排斥不可信节点来防止网络中不良行为节点的安全威胁，特别是对抗自私节点发出的攻击。在信任评估中，节点通过监测邻接节点间的通信行为以及与其它节点交换信息来动态获取其它节点的信任值，作为评价节点可信程度的指标，并维护一个全网的信任值表，表中为网络中的每个节点保留一个条目。工作过程中，节点将根据通信节点或协作节点的信任信息针对特定行为做出相应响应。

信任评估的主要目标包括：

- 提供用以判定节点是否可信的可靠信息；
- 鼓励节点的合作行为；
- 排斥不良节点，获取机制所保护的合作服务。

在 Z. Yan, Asad Amir Pirzada 提出的信任评估方案[2,3]中，每一个节点都需要评估网络中其它任何节点的信任度。若当前节点与其它节点的交互很少，则该节点的信任度将难以被准确评估。而且，此信任评估方案需要占用节点很大的存储空间用于存取网络中其它节点的信任值，造成了很大的资源开销。

MANET 中分簇的概念最早是在分组无线网络中提出的[4]。分簇算法的目标就是以较少的计算和通信开销来构造和维护一个簇集合，使其能够在覆盖整个网络的同时较好地支持资源管理和路由协议的相互连接。基于分簇的网络结构，减少了网络中路由算法和洪泛广播的开销，从使得管理移动节点和控制节点接入无线信道变得更加方便，并且提高了网络的可扩展性和 QoS 保障能力。

本文在分析已有信任评估安全性方案的基础上提出了一种基于分簇的信任评估方案，用于判断节点的好坏，并分析了移动自组网中基于该方案的安全应用。

2　基于分簇的信任评估方案

2.1　方案思想

本文提出的基于分簇网络结构的信任评估方案(CBTES: Cluster-Based Trust Evaluation Scheme)中，由邻居节点组成分簇结构，簇内节点选举出的一个簇首充当信任担保者 TG(Trust Guarantor)。节点的信任评估综合考虑了节点的经验值和节点所属簇的簇首出示的评价信息。因此，没有经验值的簇内节点也可以依据簇首出示的信任值对其它节点进行信任评估。另外，基于分簇结构的信任评估方案不需要存储和管理网络内其它所有节点的经验数据。

在本文方案中，MANET 网络中的节点根据自己的经验值评估其邻居节点的信任值；每个节点在计算其邻居节点的信任值完成后，选择一个持有最高信任值的节点作为 TG，被

*)基金项目：国防预研项目。王寒凝　工程师，硕士研究生，主研方向：信息安全、电子商务。王亚弟　教授，博导，主研方向：信息安全、密码协议分析。韩继红　副教授，硕导，主研方向：电子商务、信息安全。

选中的节点作为簇首，参选的节点作为簇成员，簇首持有最高的信任值，同时负责给簇内成员发放信任值证书。如果被选中的持有最高信任值的节点已经成为别的簇的成员，那么信任值排第二的节点被选为簇首。依据评估的信任值选择簇首形成的簇如图 1 所示。

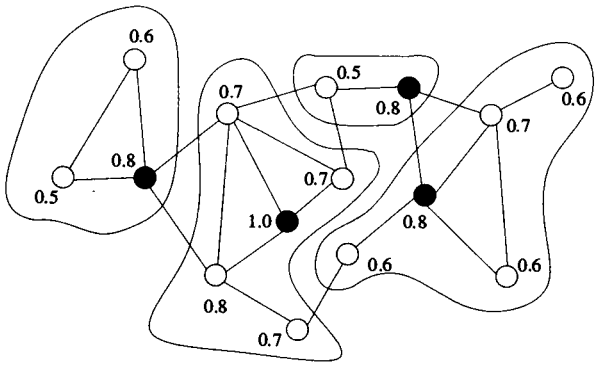

图 1　数值为每个节点的信任值，黑色节点为簇首

2.2　信任评估的相关概念

网络中某一节点对其它节点的信任评估要综合节点的经验值和被评估节点所属簇的簇首出示的信任值而定。在节点经验数值计算中所需参数定义如下：

通信数据比率(V_c)：被评估节点通信成功的比率。取值范围在[0,1]之间，初始值为 1。

数据分发比率(V_d)：被评估节点成功转发数据分组的比率。该比率评估一个节点作为中继转发从信息源到目的节点发送的数据包的成功率，取值范围在[0,1]之间，初始值为 1。

在早期的信任评估机制中，节点需要收集和存储移动自组网内其它所有节点的经验数据。然而，在 CBTES 中，节点可以将一个在一段时期内没有通信的节点的经验数据删除，因为对于拓扑结构高度变化的移动自组网来说，存储这些数据已经没有任何意义了。对于没有经验值的节点，其信任值依据簇首发放的信任证书来确定。同样，对于那些持有陈旧经验值的节点，综合考虑由簇首发放的证书可以使其信任值更加准确。但需要注意的是，由于分簇的需要，邻居节点的经验值数据不能删除。因此簇一旦存在，簇首将不能删除簇内成员的经验数据。

经验值的相关定义如下：

$$V_E(i,j)=\sum_{v\in V} v/|V| \tag{1}$$

是节点 i 对节点 j 的评估经验度量；

其中，$V=\{V_c,V_d\}$ 是经验因素的集合；

$$V_T(i,j)=(V_E(i,j)\cdot ew+V_T(H,j)\cdot(1-ew))\cdot V_B(j) \tag{2}$$

表示节点 i 对节点 j 评估的信任值，若 j 是簇首，则表示簇首对节点 j 的评估；

其中：$ew=ec/ec\_threshold$，表示经验权重，若其值超过 1，则取值为 1。ec 表示经验次数，$ec\_threshold$ 表示节点设置的经验次数的阈值。$V_B(j)$ 表示若 j 为恶意节点，则 $V_B(j)$ 取值为 0，否则为 1。

信任值的评估可以基于节点本身的经验值或基于簇首发放的证书，也可以两者兼顾。例如：对于没有被评估节点的经验数据或者已有的经验数据值由于超过有效期而被删除的评估者只能依据簇首发放的证书来进行信任值评估。从很多次经验中得出的节点的经验值是最准确的，因此对于那些经验次数超过阈值的被评估节点，最终的信任值仅取决于经验值。对于其它情况，经验值与来自簇首证书的比例与权重一致。

式(2)同样适用于簇首节点，但是 $V_T(H)$ 所表示的含义不同。$V_T(H)$ 表示被评估的节点原所属簇的簇首给出的信任值。这种情况的出现是由于节点的簇间移动。此时，簇首对新加入的节点没有足够的经验数据，信任值需要依据新加入节点上一所属簇给出。另一种情况是，新加入节点不是从别的簇移动过来的，同时簇首也没有关于它的足够经验数据，则其信任值设为 1。

式中 V_B 的值由各个簇的簇首节点广播的恶意节点或入侵节点信息决定。簇内节点收到广播信息后将这些节点加入自己的“黑名单”。文[3]中介绍了一些检测恶意节点的方法。

2.3　方案描述

在这一部分，将详细介绍簇的形成和认证。在这些具体措施中，信任值消息的完整性由步步为营安全模型(bootstrapping security model)[8]保护。

A　Hello 消息　处于未决定状态的节点将广播“Hello”探测消息，其中包括簇首的搜索信息。若节点的邻居节点中有若干个簇首，则选择簇成员最多的簇加入。若节点的邻居节点中没有簇首存在，则在它的邻居节点中推举一个新的簇首。这一过程如图 1 所示。

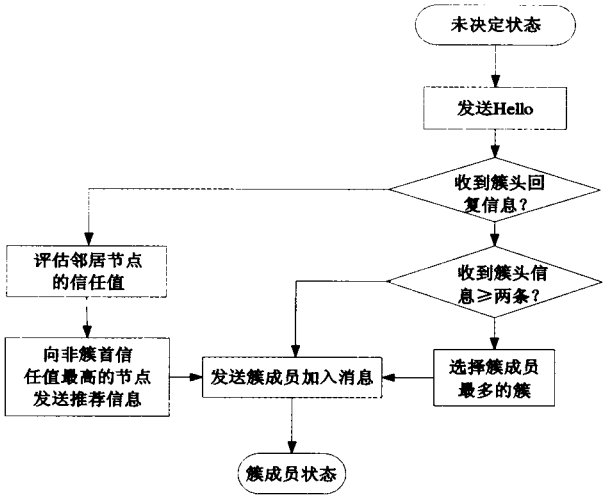

图 2　节点加入簇的状态图

推荐过程中涉及到的数据结构包括推荐消息和推荐证书，格式定义如下：

Recommend Message:
M(node1's id, node2' s id, node2' s trust value, R_Certificates, "recommend message");
Recommendation Certificate(R_Certificate):
{node1' s id, node2' id, create time, validation, "Recommend", node1's PUB_KEY, signature(node's id, node2's id, create time, validation, "Recommend")}

其中，node1 表示推举者，node2 表示被推举为簇首的节点。在推荐证书中，Validation 表示证书的有效期。当证书的有效期满，则簇首需要向簇成员申请新的证书。

B　信任证书　簇形成后，簇成员向簇首申请信任值证书。簇首在给簇成员发放信任值证书的同时发送自己的推荐证书用来证明自己的簇首身份是可信赖的。信任值证书定义如下：

Trust value certificate(T_Certificate):
{cluster head's id,node1'id, node1's trust value, cluster head's Pub key, create time, Validation, signature(cluster head's id, node1'id, node1'strust value, create time)}

(下转第 105 页)

Advances in Intrusion Detection(RAID 2003), Pittsburgh, PA, September 2003
17 Qin X, Lee W. Discovering novel attack strategies from INFOSEC alerts. In: Proceedings of the 9th European Symposium on Research in Computer Security, Sophia Antipolis, France, September 2004
18 Qin Xinzhou, Lee Wenke. Attack Plan Recognition and Prediction Using Causal Networks. ACSAC 2004: 370～379
19 Staniford S, Hoagland J, McAlerney J. Practical automated detection of stealthy portscans. Journal of Computer Security, 2002, 10(1-2): 105～136
20 Dain O, Cunningham R. Building scenarios from a heterogeneous alert stream. In: Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, June 2001. 231～235
21 Dain O, Cunningham R. Fusing a heterogeneous alert stream into scenarios. In: Proceedings of the 2001 ACM Workshop on Data Mining for Security Applications, Nov. 2001. 1～13
22 Schneier B. Attack Trees. Dr Dobb's Journal of Software Tools, 1999(12): 21～29
23 McDermott. Attack Net Penetration Testing. The 2000 New Security Paradigms Workshop(Ballycotton, County Cork, Ireland, Sept. 2000). In: ACM SIGSAC, ACM Press, 2000. 15～22
24 Helmer G, Wong J, Slagell M, et al. Software Fault Tree and Colored Petri Net Based Specification, Design and Implementation of Agent-Based Intrusion Detection Systems
25 Breiman L. Bagging Predictors. Machine Learning, 1996, 24(2): 123～140

(上接第 99 页)

C 节点加入 节点加入分两种情况：第一种情况是当一个节点第一次入网。第二种是一个节点脱离原簇加入另一个簇的情况。前者，由于节点没有信任值证书或者推荐证书，簇首不得不从头开始对该节点的信任值进行评估。在第二种情况，脱离原簇的节点向新簇首出示在原簇获得的信任值证书和推荐证书。依据这些证书，新簇簇首鉴别和设置新加入的节点的初始信任值而不需要其经验值。过程如下：首先，节点广播"Hello"探测消息，一些收到消息的簇首向该节点回复响应信息。响应信息中包括簇首所在簇的成员数量。其次，收到簇首响应信息的节点再向想要加入的簇的簇首发送加入消息，如下所示。

Joim Message:

M(node1's id, cluster head's id, previous cluster head's id, T_Certificate, R_Certificates, "join message")

若加入节点的邻居节点中簇首的数目超过两个，则选择簇成员最多的簇加入。第三，簇首收到请求加入的消息后，它根据请求加入节点原所在簇为其颁发的信任值证书评估该节点的信任值。如果申请加入的节点在一跳范围内没有找到可以申请的簇首就扩大范围搜索两跳的，若还没有找到，就只能和相邻的节点重建一个新簇。

D 节点离开 当一个节点离开原簇时向原簇首发送离开消息，原簇首收到后删除该节点的相关信息。

3 应用分析

此信任方案可应用于解决针对移动自组网的各种攻击引起的安全问题和安全路由的设计。

3.1 安全路由

应用 CBTES 方案，一个节点收到的路由请求的附加信息包括 T_Certificate, R_Certificates 和节点本身的地址。信息源在收到路由回复数据包后检查中间节点的信任值。如果中间有些节点的信任值较低，则信息源节点放弃这条路由，重新广播路由请求包来寻找别的路径。

3.2 其它安全问题

· 消息伪造攻击：本方案采用 Rakesh 不对称加密法[5]，同时在消息中绑定数字签名和发送者的公钥。这样接受者就可以检测公钥是否是发送者的，从而断定消息是否伪造。

· 黑洞攻击：攻击者在某节点的路由请求和路由回复过程中宣称自己拥有到目的节点的最短路由，这样该节点会选择其所宣称的路由，从而将数据包发向攻击节点，攻击节点截取数据包不再转发，在网络中形成一个吸收数据的"黑洞"。在本方案中，恶意节点的信任值会非常低，恶意节点宣称的路由将被放弃，从而保证数据的安全。

· 自私攻击：由于移动自组网的特殊性，网络中的部分节点可能会由于资源能量、计算能量等原因不愿意承担其它节点的转发任务而产生自私性攻击。在本方案中，自私节点由于数据转发率低导致其不可能有一个较高的信任值。通过不提供给低信任值节点数据包的方法，网络可以促进合作和减少自私节点。

结论 本文提出了一个针对移动自组网的新型信任评估方案，即基于分簇的信任评估方案。该方案可以解决移动自组网中现存的许多安全问题。依据该方案，移动自组网内任何一个节点都可以凭借簇首签发的信任值证明书对另一个陌生节点进行信任评估，从而使得每个节点均可以通过一种安全的方式和其它以前从未与之有过通信连接的节点进行通信。同时，由于网络节点不需要收集和存储移动自组网内所有其它节点的信任值的经验数据，大大减少了信任评估过程所需的资源开销。

参 考 文 献

1 Deng H, Li Wei. Agrawal D P. Routing Security in Wireless Ad Hoc Networks. IEEE Commun. Mag., 2002, 40(10): 70～75
2 Yan Z, Zhang P, Virtanen T. Trust Evaluation Based Security Solution in Ad Hoc Networks: [Technical Report]. Nokia Research Center, Helsinki, Finland, Oct. 2003
3 Pirzada A A, McDonald C. Establishing Trust In Pure Ad-hoc Networks. In: Proc. Australasian Computer Science Conf., Jan. 2004. 47～54
4 Gerla M, Tsai J T C. Multicluster, Mobile, Multimedia, Radio Network [J]. Wireless Networks, 1995, 1(3): 255～265
5 Sarela M, Hietalahti M. Security Topics and Mobility Management in Hierarchical Ad Hoc Networks: A Literature Survey: [Interim Report of Project Samoyed]. Helsinki Univ. of Technology, Apr. 2004
6 Bechler M, et al. A Cluster-Based Security Architecture for Ad Hoc Networks. In: Proc. IEEE INFOCOM, 2004, 4: 2393～2403
7 Park Chan-Il, Lee Y H, Yoon H, Choi D S, Jin S H. Cluster-Based Trust Evaluation in Ad Hoc Networks. In: Proc. Int'l Conf. Advanced Communication Technology, 4C-03, Feb. 2005
8 Basagni S. Distributed Clustering for Ad Hoc. Networks. In: Proc. Int'l Symp. Parallel Architectures, Algorithms, and Networks, 1999. 310～315
9 Bobba R B, et al. Bootstrapping Security Associations for Routing in Mobile Ad-Hoc Networks: [Technical Report, TR2002-44]. Univ. of Maryland, May 2002
10 Marsh S P. Formalizing Trust as a Computational Concept: [Ph. D. Thesis]. Dept. of Mathematics and Computer Science, Univ. of Stirling, 1994