维普资讯 http://www.cqvip.com

移动 Ad hoc 网络中节点合作性研究综述*)

谭长庚　罗文燕　陈松乔　王建新
(中南大学信息科学与工程学院　长沙 410083)

摘　要　移动 Ad hoc 网络的动态性和暂时性导致节点间的信任关系不断变化,这给密钥管理带来困难;对于网络内部恶意节点和自私性节点的攻击,传统的安全方案不再有效。在缺少预先约定的信任关系时,合作性安全机制是解决网络内部恶意节点和自私性节点不合作行为的有效方法。本文首先分析了移动 Ad hoc 网络中所面临的各种安全弱点,指出节点相互合作的重要性,然后综述了现有典型的合作性方案,指出了各种方案的优缺点,提出了进一步的研究方向。

关键词　移动 Ad hoc 网络,网络安全,虚拟货币的合作性方案,声誉值系统

A Survey of Cooperation of Nodes in Mobile Ad Hoc Networks

TAN Chang-Geng　LUO Wen-Yan　CHEN Song-Qiao　WANG Jian-Xin
(College of Information Science and Engineering, Central South University, Changsha 410083)

Abstract　It is difficult to manage the secret key in mobile Ad hoc network, because the trust relationship between nodes is change incessantly due to the dynamic and temporarily of network. To the attack which launched by the malicious and selfish nodes in the inner mobile Ad hoc networks, the traditional security mechanism isn't efficacious anymore. With lack of a prior trust relationship, the cooperative security schemes offer the reasonable effective solution to resolve the uncooprative behavior which launched by the malicious and selfish nodes in the inner mobile Ad hoc networks. This paper analyses the vulnerability of mobile Ad hoc network at first, points out the importance of cooperation between nodes, and then surveys the typical cooperation schemes, makes a comparison and discussion of their respective merits and faults. Finally, we outline future research directions.

Keywords　Mobile Ad hoc network, Network security, Virtual currency-based schemes, Reputation-based schemes

1　引言

移动 Ad hoc 网络(Mobile Ad Hoc Networks)由许多可以自由移动的节点组成,每一个节点既是主机,又是路由器,节点间的通信通过无线信道、由多个节点转发来共同完成[1]。移动 Ad hoc 网络不依赖于任何固定的网络,无中心控制,是完全自组织的,因此它与传统的无线网络有着很大的区别。由于移动 Ad hoc 网络本身独特的结构,从而产生了一些很突出的特点:网络的自组性、拓扑结构的动态变化、传输带宽和能源的有限性、移动终端的局限性和网络的分布式控制等。

移动 Ad hoc 网络最近得到了很大的发展。但是,目前有许多技术问题尚未解决,这给它的普及和推广带来一定的障碍。安全性是其中的核心技术和热点问题。本文首先分析了移动 Ad hoc 网络中所面临的各种安全弱点,指出节点相互合作的重要性,然后综述了现有的各种典型的合作性方案,指出了各种方案的优点和缺点,最后对全文进行了总结,提出了进一步的研究方向。

2　移动自组网安全研究、弱点及节点合作的重要性

移动 Ad hoc 网络具有拓扑结构动态变化、传输范围与带宽有限、能源受限和分布式控制等特点,这些特点使其具有诸多系统脆弱性,比固定网络更容易遭受各种安全的威胁,加之没有基础设施的支持、没有可信任的认证中心来提供密钥管理和身份认证等服务,传统的安全机制在移动 Ad hoc 网络中难以实现。

2.1　移动 Ad hoc 网络具有的系统脆弱性

从安全角度看,与传统网络相比,移动 Ad hoc 网络本身具有如下系统脆弱性:

(1)采用无线信道。

移动 Ad hoc 网络采用无线信号作为传输媒介,具有广播特性,因此很容易受到被动窃听、主动干扰、数据篡改、假冒、消息重放、拒绝服务以及通信量分析等攻击。

(2)无基础设施的分布式网络。

移动 Ad hoc 网络中节点大都是对等的,没有中心控制,采用分布式管理,这样避免了单点失效,却让网络变得更加脆弱。由于没有基础设施的支持、没有可信任的认证中心来提供密钥管理和身份认证等服务,传统的安全机制,如密码体制、目录服务等,在移动 Ad hoc 网络中难以实现。

(3)动态变化的拓扑结构。

移动 Ad hoc 网络中节点的位置是不固定的,可随时移动,造成网络的拓扑结构不断变化。移动 Ad hoc 网络的动态性和暂时性导致节点间的信任关系不断变化,这给密钥管理

*)国家自然科学基金(90304010,60403032)。**谭长庚**　副教授,博士研究生,主要研究移动自组网的路由协议和性能评价;**罗文燕**　硕士研究生,主要研究移动自组网络安全;**陈松乔**　教授,博导,主要研究领域为软件工程与计算机网络;**王建新**　教授,博导,主要研究领域为路由算法及网络性能评价。

维普资讯 http://www.cqvip.com

带来困难，为静态配置系统而设计的标准安全方案不再适用。

(4)节点行为的不可控性。

节点可以自由漫游并与邻居节点通信，在加入或离开一个子网时无需任何声明，因此无法保证两个节点间路径上经过的中间节点都按协议操作，不能排除其中存在想要破坏网络的恶意节点。节点在移动过程中可能被敌方俘获而泄露重要信息，还可能叛变后以正常面目重新加入网络，以此来获取秘密信息和破坏网络的正常运行。节点靠电池供电，给拒绝服务攻击提供了新的机会。节点还有可能为了节省自己的资源只使用网络而不转发报文，发起自私性攻击。文[2]的研究表明，自私行为对整个网络性能有着很大的影响。因此，移动 Ad hoc 网络不仅要防范外部节点的入侵，而且要对付内部叛变节点、恶意节点和自私性节点的攻击。

2.2 移动 Ad hoc 网络安全研究

移动 Ad hoc 网络安全研究主要有 4 个方面：(1)密钥的管理与认证[9,10]。研究在移动 Ad hoc 网络中无中心自组织的情况下，如何实现密钥的分配与相互认证，主要采用基于门限密钥的管理方案[11]和基于 PGP 的自组织的认证方案[12]两种方式。(2)路由安全方案。研究如何对路由协议提供安全保障，通过对路由协议中的报文提供完整性校验、身份认证等安全措施，防止报文篡改[13,14]。(3)入侵检测。研究如何在网络运行中及时发现恶意节点的入侵，通常采用邻居监视、合作检测的方法[15]。(4)增强合作性。研究内容是如何鼓励节点参与网络转发，防止节点为了节省自己的能源，不参与网络交换，主要采用两种方法：①基于惩罚的方法[16]，利用邻居监视，不参与网络交换将被排除出网络；②基于奖励的方法[17]，节点转发报文就给与虚拟货币作为奖励，只有持有货币才能发送自己的报文。

2.3 移动 Ad hoc 网络的合作性

网络中节点的合作性是一个很重要的问题，对移动 Ad hoc 网络来说更是如此。一方面，移动 Ad hoc 网络中节点间是通过无线信道来发送信息的，由于节点的发射距离有限，不在彼此信号覆盖范围内的两个节点之间要通信，只能通过中间节点的共同合作来完成。如果没有节点间的相互合作，路由就不能够建立，数据包就不能够发送，更不用说网络基本功能的实现了。而移动 Ad hoc 网络的分布式管理、动态的拓扑结构使密钥管理变得更加困难，从而不能够通过有效的实体认证来确保网络关键功能的正确运行。另一方面，在固定网络中，通过信任中心可以对节点进行身份认证，从而可以有效地区分可信节点与不可信节点。但移动 Ad hoc 网络没有基础设施和授权机构，也就无法区分节点是否可信任。在移动 Ad hoc 网络中，所有节点都要参与支持网络的运转，无法事先为所有节点建立安全关联，也就失去了对节点进行分类的基础。因此，在缺少预先约定的信任关系的情况下，合作性的安全机制是解决网络内部恶意节点和自私性节点不合作行为的有效方法。在合作性的安全机制中，通过对节点行为予以适当的评价和标记，找出不合作节点，并给予相应的惩罚，以激励节点相互合作，共同完成网络的基本功能。节点间的相互合作不仅有利于整个网络，而且有利于节点本身。

3 移动自组网络中的合作性方案

目前，增强节点间合作性的方案大体上可以分为两大类：基于虚拟货币的合作性方案和基于声誉值的合作性方案。下面分别就这两大类方案中的典型协议进行介绍与分析。

3.1 基于虚拟货币的合作性方案

3.1.1 Nuglets

为了激励节点的合作性，Levente Buttyan 和 Jean-Pierre Hubaux 提出了虚拟货币的合作性方案 Nuglets[3~5]。在文[3]中，作者提出了两种虚拟货币的合作性方案：钱包方式(费用由发送方支付)和购买方式(费用由接收方支付)。在钱包方式中，当有报文发送时，源节点估计报文所经过的节点与需要的花费，将计算所得的虚拟货币数放入钱包内，钱包随报文一起发送，中间节点从钱包中取出其所得后将剩余的货币与报文转发给下一个节点。每个节点只有尽力转发其他节点的报文才能获得足够的货币，以发送自己的报文。在购买方式中，中间节点从其上游节点购买下该报文，然后加上本节点的转发费用再卖给下游节点，直到目的节点。在这种方式中，中间节点转发数据包的费用最后由目的节点支付。这两种方式都有优缺点：对于前者，优点是费用由发送者支付，可以防止节点滥发报文、发动拒绝服务攻击；缺点是源节点难以精确计算报文转发的费用，有可能源节点所放的筹码数少于转发报文所需的筹码数，最终使报文不能到达目的节点。对于后者，优点是费用由接收者支付，免除了事先估算费用的麻烦；缺点是因为发送者无需支付发送费用，可能会滥发报文，造成网络负载过重，最终使得网络不可用。这两种方式的每个报文都要携带货币，增加了报文的长度，也就增加了开销。还有，难以防止中间恶意节点私自侵吞所有货币。

在文[5]中，作者提出了改进方案。在此方案中，每个节点都安装有一个防止用户修改的安全卡，卡内为筹码累加器。当源节点要发送报文时，筹码累加器减去 n 个筹码，即报文要通过 n 个节点转发才能到达目的节点。节点每转发一个报文，该节点的筹码累加器加 1。该方案算法简单，但需要硬件的支持。

3.1.2 Sprite

Sprite[6]也是用虚拟货币作为奖励节点转发报文的报酬，所不同的是 Sprite 用清算中心 CCS(Credit Clearance Service)替代了安全卡。清算中心存储每个节点的筹码数，计算每个节点的开销(发送报文数)和收入(转发报文数)。当节点转发一个报文时，该节点保留着票据，然后与清算中心联系，上传该票据。清算中心根据报文转发情况付给参与转发节点相应的筹码数，同时减去发送节点总筹码数。此方案的优点是不需要硬件支持，同时由于是发送方支付费用，可以防止拒绝服务攻击；缺点是由于清算中心的存在，容易引起单点失败。

虚拟货币的合作性方案的特点是依赖于额外硬件或清算中心来增加或减少节点的筹码，节点只有尽力转发报文，获得筹码，以发送自己的报文，这样可以激励节点参与合作，但可扩展性不强，不适用于大型的和对实时性要求比较高的移动 Ad hoc 网络。此外，由于节点处在网络中的位置不同，因而会导致位置特权问题[7]，即处于网络中心的节点由于周围邻居比较多。有较多的机会转发报文，所得的筹码就比较多。而处于网络边沿的节点，转发报文的机会较少，所得的筹码也就较少，可能所得筹码数还远远小于发送报文所需要的筹码数，引起不必要的时延，甚至不能发送报文，带来不公平性。

3.2 基于声誉值的合作性方案

3.2.1 Watchdog and pathrater

Watchdog and pathrater[8]最初用来解决移动 Ad hoc 网络中如何减轻路由错误的问题。由两部分组成：Watchdog 和 pathrater。Watchdog 用来检测具有不良行为的节点，path-

维普资讯 http://www.cqvip.com

rater 则负责在路由选择时避免将这些节点包含在路径中。Watchdog 的工作原理是：节点把刚发送给下游节点的数据包放在缓冲区中，侦听其下游节点是否转发该数据包。若在规定的时间内下游节点转发了该数据包，且与缓冲区中的数据包相匹配，则证明已成功转发，释放缓冲区中的数据包；若不匹配，则说明下游节点修改了该数据包，为不良节点。如果在规定时间内节点都没有侦听到下游节点转发该数据包，则说明有错误发生。当错误发生的次数超过某一阈值时，则证明该节点为不良节点。Watchdog 把这些信息反馈给 pathrater，pathrater 根据不同的行为来更改相应节点的声誉值。声誉值的计算方法如下：每个节点记其他节点的初始声誉值为 0.5，自己则记为 1.0。在活动路径中，每隔 200ms，正常节点的声誉值加 0.01。当检测到有链路断裂或节点不可达时，节点的声誉值减少 0.05。不改变不在活动路径的节点的声誉值。Pathrater 根据路径中节点的平均声誉值水平来选择路由，避免声誉值为负的节点，即不良节点。

该文首次提出了 Watchdog 这个概念，以后的声誉系统均沿用这种方法来检测节点行为。Watchdog 尽管本身并不完美，但在一定程度上可以检测节点的不良行为。Pathrater 只是简单标记了节点的声誉值，负责在路由选择时绕过不良节点，并没有惩罚不良节点，在一定程度上还减轻了不良节点的负担。

3.2.2 CONFIDANT

CONFIDANT[9,10]是按需路由协议的扩展，其目标是检测并孤立不合作节点，以此来促使节点的相互合作。每个节点都包含有如下 4 个模块：监测器、声誉值系统、信任管理和路径管理。这 4 个模块相互合作，共同提供和处理路由信息。监测器用于监测节点的不良行为，一旦有可疑行为，它就将此信息上报给声誉值系统。声誉值系统是一个表，包含节点 ID 及其声誉水平。声誉水平只有在有足够证据证明节点有恶意行为时才会改变。信任管理负责报警信息的发送和接收，根据报警信息发起节点的信任水平来处理收到的 incoming ALARM messages，只给友好列表中的节点发送 outgoing ALARM messages。路径管理根据其路径中节点的声誉水平选择路由。包括以下几个功能：根据安全度量如节点的声誉值来标记路径等级；删除包含有恶意节点的路径；处理恶意节点发起的路由请求；处理收的含恶意节点的路由应答包。

CONFIDANT 使用全局声誉值，节点保存有网络中每一个节点的声誉值。声誉值的改变只依赖于自己的直接观察，不直接发送声誉值，而是通过发送报警信息来达到共享信息的目的。这样可以充分学习别人的经验，快速地惩罚不合作节点。但报警信息在传输过程中有可能被篡改。另外，还存在错误控告等问题。

3.2.3 CORE

CORE[11]通过使用联合监测技术和声誉值机制来激励节点合作。在这个方案中，声誉值是用来衡量节点对网络运行所作的贡献。具有良好声誉的节点，可以使用网络资源；而具有不良声誉的节点，因为它们拒绝合作，最终被排除出网络中。CORE 由两部分组成：看门狗机制和声誉值表。看门狗用来检测节点的不良行为。通过侦听下一跳节点的传输情况来判断该节点是否发送了数据包。如果下一跳节点没有发送数据包，则它就被认为是不良节点。声誉值表是一个数据结构，用来存储节点的声誉值。表中每一行由 4 部分组成：唯一的节点 ID、自己观察所得的自主声誉值、由其他节点所提供的间接声誉值和功能性声誉值。节点通过一个综合公式将这 3 种类型的声誉值计算为总的声誉值。当某节点的总声誉值低于阈值时，其他节点拒绝为其提供服务，那样就会将不合作节点排除出网络中。

CORE 对不同的信息发送赋予不同的权值，注意到了网络中不同功能的重要性不同，但增加了声誉值系统的复杂性。另外，声誉值在传输过程中有可能被篡改，节点有可能发送不真实的声誉值。

3.2.4 OCEAN

与前 3 种方案不同，OCEAN[12]避免间接声誉值而只使用自己观察得来的第一手资料，每个节点只根据自己观察的结果来选择路由。节点只保存有一跳邻居节点的声誉值，声誉值都初始化为 0，如果是良好行为则加 1，不良行为则减 2。当某一节点其声誉值低于 −40 时，就将其加到错误列表中，错误列表代表有不良行为的节点。该方案由 5 部分组成：①邻居监控用来检测邻居节点行为。当错误行为被检测到时，邻居监控就会将此信息报告到路由级别表，路由级别表用来存储每一个邻居节点的声誉值。②路由选择根据节点的声誉值来选择，避免选择包含有错误列表中节点的路由。③恶意流拒绝器用来拒绝从恶意节点发出的信息，所有从不良节点发出的信息流均被拒绝掉，从而使得恶意节点不能发送数据包。④二次机会机制让错误节点有机会再参与网络运行。⑤当一个节点被加到错误列表后，经过一段时间后将从错误列表中移除。尽管节点从错误列表移除了，但它的声誉值还是没有增加。如果节点继续有不良行为，它很快又会被加到错误列表中。

OCEAN 不允许声誉值的交换，仅根据自己观测所得的声誉值来进行路由选择，减少了协议的复杂性，但用于判断节点行为的信息减少了。仿真结果表明，在达到同样性能的情况下，该方案比使用间接声誉值的方案更简单，并且避免了错误控告的风险，但是对某些参数比较敏感。由于使用二次机会机制，不像全局声誉值系统那样严厉地惩罚不良节点，还会带来恶意节点的重复攻击。

3.2.5 LARS

与 OCEAN 一样，LARS[13]（Locally Aware Reputation System）也是采用本地声誉值，每个节点都只保留到它一跳邻居的声誉值，声誉值的更新只依赖自己直接观察所得，不存在声誉值的交换。为了减轻自私节点和恶意节点的负面影响，当一个不合作节点被辨别出来后，它的 k 跳邻居都会接到警告信息，被告知该节点为不良节点，从而拒绝为不合作节点服务。为了防止错误控告和声誉值不一致问题，警告信息在广播前，必须得到 m 个一跳邻居节点的签名。在此方案中，节点的信任度与它的声誉值联系在一起。信任度用 T 来标记，共分为 3 个水平：可信、不可信和不确定。可信节点是指行为良好的节点，不可信节点是指不合作的节点。信任关系不确定的节点通常是一个新加入到网络中的节点或是从一个地方移动到另一个地方的节点，其信任水平根据其后面的行为来判定。声誉值用 R 来表示，节点的声誉值在最大值和最小值之间，即 $R_{min}<R<R_{max}$。用两个阈值 R_u、R_t 来判断节点的信任度，即当节点的声誉值小于 R_u 时，该节点为不可信节点；当节点的声誉值大于 R_t 时，该节点为可信节点；而节点声誉值处于这两个阈值之间时，为信任关系不确定的节点。对不合作节点，LARS 同样采用了二次机会制。

LARS 不允许声誉值的交换，避免了复杂的计算。通过

维普资讯 http://www.cqvip.com

发送警告信息来学习别人的经验，并采取了一定的措施来解决错误控告和声誉值不一致问题，但增加了协议的复杂性。另外，LARS中引入了信任水平，但在协议中并没有具体的运用。

基于声誉值的合作性方案，其特点是通过邻居监测节点行为，并对不同的行为予以一定的评价，用声誉值来标记节点的声誉情况，并根据不同的声誉水平而采取不同的应对措施。以上5种方案存在一些共同点，如节点都工作在混杂侦听模式下，都用声誉值来标记、区分节点，都在DSR协议上进行扩展与仿真。但它们之间又存在许多不同之处，如表1所示。

表1 各种基于声誉值合作性方案的比较

声誉值系统	Watchdog and pathrater	CONFIDANT	CORE	OCEAN	LARS
声誉值类型	自主声誉值	自主声誉值	自主声誉值、间接声誉值、功能性声誉值	自主声誉值	自主声誉值
声誉值的作用范围	整个网络	整个网络	整个网络	本地一跳邻居内	本地一跳邻居内
声誉值更新	周期更新	事件触发更新	事件触发更新	事件触发更新	事件触发更新
交换信息	无	报警信息	正的声誉值	无	警告信息
惩罚手段	绕过不良节点	排除出网络	排除出网络	二次机会制	二次机会制

根据声誉值的作用范围，这5种方案又可以分为两大类：全局声誉值和本地声誉值。全局声誉值是指节点保存有网络中所有节点的声誉值，并且其声誉值在整个网络范围内都有效；而本地声誉值是指节点只保存其一跳邻居节点的声誉值，其声誉值只在邻居范围内有效。全局声誉值由于节点间通过交换信息（黑名单、声誉值或报警信息）来共享经验，能比较快速地检测出不合作节点，但交换声誉信息增加了开销，存在声誉信息可能遭受篡改等不安全因素及错误控告问题。而本地声誉值方案只保存一跳内邻居节点的声誉值，节省了存储空间。由于不存在声誉值的交换，避免了复杂的计算，但不能充分学习别人的经验来提高自己的判断能力，效率相对比较低。

对不合作节点的惩罚上，Watchdog and pathrater只是简单地绕开不良节点，并没有采取相应的惩罚措施；CONFIDANT和CORE采取了只罚不奖，不合作节点永久排除出网络，不能容忍节点无意错误；OCEAN和LARS都采用了二次机会机制，可容忍节点无意错误，但带来节点重复攻击。

3.3 两类合作性方案的比较

对于增强网络节点的合作性，防止节点自私性行为，目前主要有两种方案：基于虚拟货币的合作性方案和基于声誉值的合作性方案。这两种方案各有优缺点，如表2所示。

总结与展望 由于移动Ad hoc网络本身的特点，使其比固定网络更容易遭受各种安全攻击，在移动Ad hoc网络中实现安全方案更加困难。本文首先分析了移动Ad hoc网络中所面临的各种安全弱点，指出节点相互合作的重要性：在缺少预先约定的信任关系的情况下，合作性的安全机制是解决网络内部恶意节点和自私性节点不合作行为的有效方法。然后综述了现有的各种典型合作性方案，指出了各种方案的优点和缺点。

表2 合作性方案比较

合作性方案	基于虚拟货币的合作性方案	基于声誉值的合作性方案
激励手段	虚拟货币	声誉值
主要思想	以虚拟货币作为节点合作的奖励，鼓励节点转发报文	通过监测，对节点行为进行评价，并用声誉值来标记，根据节点的声誉值的不同而区别对待，以此来鞭策节点参与网络功能
工作模式	正常	混杂侦听
网络开销	低	较低
节点开销	较低	较高
优点	算法简单	纯软件实现，无需硬件支持
缺点	需要额外的硬件或清算中心支持，可扩展性不大；存在位置特权问题	算法比较复杂；节点负担比较重

由于移动Ad hoc网络节点具有移动性、网络拓扑变化快、节点能源有限等特点，在Ad hoc网络中加强节点的合作性具有很大的挑战。我们认为，在设计合作性方案时，可以从以下几个方面考虑：

(1)加强合作的安全机制必须是分布式的和自组织的。由于移动Ad hoc网络是自组织、动态的，因此任何中心认证或集中管理都是不适合的。移动Ad hoc网络中，节点可以随时加入或离开，节点的信任关系也在不断的变化中。因此，合作性的安全方案必须能够动态地衡量节点的信任值，并能及时地反映节点信任值的变化情况。

(2)合作性的安全机制不能过多消耗网络资源，从而降低网络性能。目前，许多合作性的安全机制都需要节点工作在混杂侦听模式下，消耗的能量比较多。而有的方案需要节点具有较强的计算能力或存储能力，这对于带宽、计算能力和能源都有限的移动Ad hoc网络来说是不太现实的。因此，我们在考虑安全的同时，也可以考虑将能源、QoS等问题结合起来，设计出一种既能节省能源又可以保证一定安全的合作性方案。

(3)移动Ad hoc网络动态的拓扑要求合作性的安全机制是可扩展的和可靠的，能够适应不同的网络规模。

参 考 文 献

1 Macker J P, Corson M S. Mobile Ad Hoc Networking and the IETF. Mobile Computing and Communications Review, 1999, 3(1): 11～13

2 Michiardi P, Molva R. Simulation-based analysis of security exposures in mobile Ad hoc networks [A]. In: Proc. of European Wireless Conference [C]. Firenze, Italy, 2002

3 Buttyan L, Hubaux J-P. Enforcing service availability in mobile Ad-Hoc WANs [A]. In: Proc. of the IEEE/ ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC) [C]. Boston, MA, USA, August 2000. 87～96

4 Hubaux J P, Buttyan L. Toward Mobile Ad-Hoc Wans: Terminodes: [Technical Report]. No. DSC/2000/006. Swiss Federal Institute of Technology, Lausanne, July 2000

(下转第62页)

维普资讯 http://www.cqvip.com

到 Init 状态。

(2)向 DUT 发送 2-way Hello 消息,BDR 设为测试仪端口,DR 为被测端口。

(3)接收 DUT 发送的 DD(数据库描述包),将其存入数组 buffrece[ ]中。这样就可以将 buffrece 中的数据与 ExpectReceive 中的进行对比。如果相同,则为 PASS,否则为 FAIL。经过验证,这个测试例能够在 Linux 环境下正确执行,执行结果与预期结果相符。

6 测试例分析

根据 OSPFv3 协议模块,我们抽象出一个测试套,即 TestSuit_OSPFv3;8 个测试组分别是:(1) 接口状态机部分的测试;(2)Hello 消息的测试组;(3)数据库交换协议测试组;(4)扩散协议测试组;(5)OSPF 头部处理测试组;(6)IPv6 头部处理测试组数据包格式;(7)数据包格式测试组;(8)路由计算测试组。每个测试组中又抽象出不同数目的测试例。

使用这些测试例,我们对 Linux RedHat 9.0 中的路由协议软件包 Zebra 进行了一致性测试。在这里我们以扩散协议为例,给出部分测试例列表及其结果。扩散协议主要利用洪泛机制,建立邻接关系的路由器之间的数据库同步,部分测试例列表如表 3。

表 3 OSPFv3 扩散协议测试例及其测试结果

测试例编号	测试项目	测试结果
Testcase4-1	当 DUT 收到一个包含比 DUT 数据库更新的实例的路由器 LSA 时,并且接收端口是 DR 而 LSA 的发送方不是 BDR 时,洪泛该 LSA	PASS
Testcase4-2	DUT 在 FULL 状态下收到它自己生成的 LSA 的更新的实例时,DUT 应将收到的 LSA 序列号加 1 后,发还给发送方。	PASS
Testcase4-3	DUT 对收到的自己洪泛出去的 LSA 时,不进行确认	PASS
Testcase4-4	当 DUT 收到一个更新的 LSA 并且该 LSA 没有从接收端口洪泛出去时,如果 DUT 是 BDR 并且 LSA 来自 DR,那么 DUT 应发送一个延迟的确认。	PASS
Testcase4-5	DUT 在进入 Exchange 状态之前应丢弃收到的 LSA。	PASS
Testcase4-6	当作为 DR 时,DUT 应对来自于 BDR 的新的 LSA 发送延迟的确认。	PASS
Testcase4-7	DUT 收到自己生成的序号为 0x7FFFFFFF 的 LSA 时,应冲掉该 LSA 的现有实例。	FAIL

我们发现 Testcase3～7 的测试结果与协议不符。在该测试例中,在把 LSA 的 Sequence Number 置为=0x7fffffff 时,即置为最大,按照 RFC2328 及 RFC2740 所述,被测应该向测试仪发送 LSA,其中的序列号设为 0x7FFFFFFF,Age 设为 MaxAge。但实际测试过程中,我们发现被测会认为这是一个无符号数,而给它增加序列号,再返回到测试仪,导致测试结果与协议说明不符。

结论 随着下一代互联网技术的部署,支持 IPv6 的不同路由设备的研发和需求也越来越多。本文对于下一代域内路由协议 OSPFv3 进行了一致性测试研究,分析了 OSPFv2 与 OSPFv3 的异同点,并根据需要选定了远程测试方法作为 OSPFv3 的测试方法。文中使用 XML 定义了协议测试套的描述模板,并用该模板实现了对 OSPFv3 测试套的描述。通过对 Linux 下的 OSPFv3 的协议实现进行一致性测试,发现了被测实现上的一些不一致问题。进一步的工作包括继续完善 OSPFv3 的协议一致性测试工作,建立完整的 OSPFv3 协议测试系统,同时将针对测试中发现的不一致的地方对被测实现进行分析。

参 考 文 献

1 Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. RFC2460, December 1998 (Status: DRAFT STANDARD)

2 Moy J. RFC 2328 OSPF Version 2[S]. April 1998

3 Coltun R, Ferguson D, Moy J. RFC 2740 OSPF for IPv6[S]. December 1999

4 赵邑新,吴建平,韩博. 路由协议测试研究——边界网关路由协议 BGP-4 测试. 通信学报,2001, 22(9):91～98

5 吴建平,陈修环,郝瑞兵,等. 基于形式化技术的协议集成测试系统—PITS. 清华大学学报,1998,38(S1): 26～29

6 李建,周颢,赵保华. 路由协议一致性测试系统研究及实现. 计算机工程与应用,2005,16:119～123

7 Wu Jianping, Li Zhongjie, Yin Xia. Towards Modeling and Testing of IP Routing Protocols. TestCom, 2003. 49～62

8 杨建华,王俊峰,谢高岗. OSPFv3 协议一致性测试系统设计与实现. 计算机应用, 2003,23 (7)

9 ISO/IEC 9646-2. Information Processing Systems, Open System Interconnection, OSI Conformance Testing Methodology and Framework. Part 2: Abstract test suite specification. 1991

(上接第 27 页)

5 Buttyán L, Hubaux J P. Stimulating cooperation in self-organizing mobile Ad Hoc networks [J]. Mobile Networks and Applications, 2003, 8 (5): 579～592

6 Zhong Sheng, Chen Jiang, Yang Y R. Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In: The 22nd Annual Joint Conf. IEEE Computer and Communications Societies (INFOCOM 2003), San Francisco, CA, 2003

7 Wang Yongwei, Giruka V C, Singhal M. A Fair Distributed Solution for Selfish Nodes Problem in Wireless Ad Hoc Networks. In: Ad-Hoc Mobile, and Wireless Networks: Third International Conference, ADHOCNOW 2004, Vancouver, Canada, July 22-24, 2004. 211～224

8 Marti S, Giuli T J, Lai Kevin, et al. Mitigating routing misbehavior in mobile Ad hoc networks [A]. In: Proc of the Sixth International Conference on Mobile Computing and Networking (Mobicom2000)[C]. Boston, August, 2000. 255～265

9 Buchegger S, Le Boudec J Y. Performance analysis of the CONFIDANT protocol: Cooperation of nodes2fairness in distributed Ad-hoc networks [A]. In: Proc of IEEE/ ACM Workshop on Mobile Ad hoc Networking and Computing (MobiHOC2002)[C]. EPFL Lausanne, Switzerland, 2002. 226～236

10 Buchegger S, Le Boudec J Y. Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks. In: 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing. Canary Islands, Spain, January 2002. 403～410

11 Michiardi P, Molva R. Core: A collaborative reputation mechanismto enforce node cooperation in Mobile Ad Hoc Networks [A]. In: Sixth IFIP conference on security communications and multimedia (CMS2002)[C]. Portoroz, Slovenia, 2002. 107～121

12 Bansal S, Baker M. Observation-based Cooperation Enforcement in Ad hoc Networks: [Research Report]. cs. NI/0307012. Stanford University, 2003

13 Hu Jiangyi. Cooperation in Mobile Ad Hoc Networks. http://www.cs.fsu.edu/research/reports/TR-050111.pdf. January 11, 2005