延迟/中断容忍网络安全机制综述

胡乔林 苏金树 赵宝康 黄清元 孙一品

(国防科技大学计算机学院 长沙 410073)

摘 要 作为一种新型体系结构,延迟/中断容忍网络(DTN)近年来得到了广泛的研究与应用。由于其面临的应用环境极为特殊,DTN中存在着资源耗尽、数据安全、分片认证及隐私保护等诸多特有的安全问题。对上述安全问题进行了深入分析,并对解决这些问题的安全机制的最新研究成果进行了分类与评述,最后对DTN网络安全研究方向进行了展望。

关键词 延迟/中断容忍网络,安全机制,分片认证,隐私保护

中图法分类号 TP393 **文献标识码** A

Survey on Security Issues in Delay/Disruption Tolerant Networks

HU Qiao-lin SU Jin-shu ZHAO Bao-kang HUANG Qing-yuan SUN Yi-pin

(School of Computer Science, National University of Defense Technology, Changsha 410073)

Abstract As an emerging network architecture, Delay/Disruption tolerant networks (DTN) have been widely investigated in the last few years. Since the application scenarios of DTN is extremely different with existing networks, DTN should address several unique security issues, including resource exhaustion, data security, fragment authentication, privacy preservation, etc. We focused on these unique security issues in DTN, and provided a brief introduction for these issues. Further, we reviewed and performed detailed classification and analysis for existing research efforts and approaches in these issues. Finally, we also identified open research issues, and intend to motivate new research efforts.

Keywords Delay/disruption tolerant network, Security mechanisms, Fragment authentication, Privacy preservation

1 引言

随着微机电、通信与计算机等技术的不断进步和发展,推动了以Internet为代表的网络技术在社会生产、生活中的广泛应用。TCP/IP协议栈对Internet的巨大成功发挥了基础性的关键作用。它对于底层网络有如下假设:在收发节点之间的端到端通信路径持续稳定;任意收发节点对之间的RTT较小且相对一致;通信链路误码率及丢包率低;上下行数据率对称;应用程序无须考虑通信性能等。

然而,近年来稀疏Ad Hoc网络[1]、特殊介质数据传输[2-4]、车载通信[5]等新兴网络应用不断涌现,这些网络具备非常鲜明的特点:链路延迟大、频繁中断、不存在持续完整的端到端连接以及节点能量和存储资源有限等。由于上述绝大部分网络还存在Internet接入需求,因此对现有的基于TCP/IP协议栈的体系结构提出了巨大的挑战。Özgür B. Akan等人[6]的研究表明,TCP/IP协议在这种具有高延迟、中断频繁的网络中无法正常运行,即使采用Freeze-TCP[7]等机制对TCP/IP协议进行修补,也难以满足上述新型网络的需要。

为了解决这些问题,出现了以延迟/中断容忍网络(DTN)为代表的新型网络技术,并在此基础上开展了大量研究。DTN设计原则相对于TCP/IP协议栈放松了多个条件:允许使用可变长度消息、支持广泛命名和寻址机制、网内存储数据以支持多路径存储转发和保管传输、使用机会主义通信机制等。因此,DTN在军用移动Ad Hoc网络、普适计算、空间通信等方面获得了广泛应用。

DTN网络体系结构的主要创新在于在传输层之上叠加了一个新的Bundle协议层,从而构成了一种新型的重叠网体系结构[10-13]。Bundle通常建立在传输层之上,可兼容多种不同的传输协议;Bundle从体系结构上表现出汇聚层作用,其次Bundle的消息转发实际上是对多个报文存储聚合进行传输的,并逐跳保证可靠性与安全性。集成了Bundle层的DTN网络通常由DTN主机、DTN路由器、DTN网关等构成,其结构如图1所示。

DTN网络面临的环境以及面向的问题域,决定了其安全需求与传统Internet相比存在较大的差异。DTN网络安全的特殊性对其安全机制的设计提出了巨大的挑战[12,14,15]。本文主要针对DTN网络中面临的特殊安全问题进行深入分析;介绍了目前的研究现状与发展情况,并对相关研究进行了

到稿日期:2008-10-07 返修日期:2008-12-33 本文受国家973项目(2005CB321801),国家863项目(2006AA01Z401, 2008AA01A325),国家自然科学基金项目(90604006)资助。

胡乔林 男,博士生,研究方向为无线传感器网络与延迟容忍网络,E-mail:huqiaolin@nudt.edu.cn;**苏金树** 男,教授,博士生导师,研究方向为网络与信息安全;**赵宝康** 男,博士生,研究方向为无线网络安全与隐私保护机制;**黄清元** 男,博士生,研究方向为无线网络路由安全;**孙一品** 男,博士生,研究方向为无线网络安全与隐私保护机制。

深入述评；此外，对 DTN 网络的安全机制研究进行了展望。

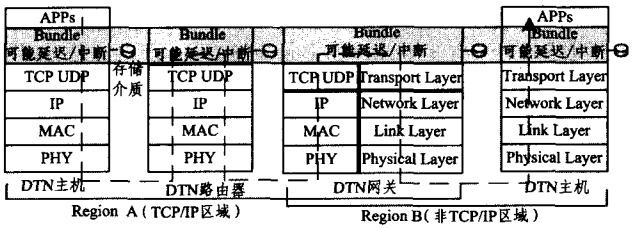


图 1　DTN 网络体系结构

本文第 2 节将对 DTN 面临的特殊安全问题进行详细分析与介绍；第 3 节将对现有的 DTN 安全机制进行全面的总结、分析与述评；最后是对全文的总结与展望。

2　DTN 网络安全面临的问题与挑战

与传统网络不同，传统基于主机的安全机制远不能满足 DTN 的安全需求。由于引入了 Bundle 这一独有的协议层，DTN 面临着资源安全、Bundle 安全及隐私保护等问题。

2.1　资源安全

DTN 网络中节点的存储、计算、通信资源缺乏，极易成为资源耗尽攻击的靶标。在这种情形下，如何保护有限资源，是 DTN 安全机制中面临的首要挑战之一。在以上资源中，通信连接会随时间而变，使通信资源显得更为重要。非授权实体访问、非授权应用控制 DTN 基础设施导致攻击路由平面、应用发送的 Bundle 超过比率限制或者服务等级、威胁网络基础等可能带来恶意或非授权的流量，加剧了对 DTN 资源的消耗，从而严重影响网络的可用性。为此，需要防御 DoS 类的攻击，对所有的用户、节点实施强认证，防止资源滥用。此外，DTN 网络中特有的 Bundle，LTP 等协议的漏洞防护对防范资源耗尽攻击也非常关键。

2.2　Bundle 安全

DTN 中独有的数据安全攻击集中在 Bundle 层，包括伪造 Bundle 源、篡改 Bundle 目的、篡改 Bundle 控制域、修改载荷内容、复制或者泄露 Bundle 数据等，这些也会消耗网络资源，同时威胁 Bundle 载荷数据的机密性、完整性、可用性。

解决 Bundle 安全问题通常需要采用加密机制。但由于 DTN 的特殊应用环境，使得现存的诸多需多次交互、资源消耗较大的安全协议无法适用，这造成 DTN 中密钥分发及管理困难。目前，在高延迟环境下密钥管理还没有较好的办法，因此难以实现端到端的安全机制，Bundle 安全还不能得到充分保证。

2.3　分片攻击

为了充分利用链路资源，消除链路易中断、长延迟等因素的影响，DTN 网络中采用了 Bundle 分片后进行机会路由通信的机制。这种独有的分片路由机制给消息签名、认证带来了巨大的挑战。与传统 Internet 中的消息分片不同[16]，Internet 网络中的分片一般能够在短时间内组装，从而顺利进行消息认证。而 DTN 中的消息组装耗时长，进程相对缓慢，这为攻击 DTN 网络提供了切入点。通过发送无意义的分片，由于接收者无法认证该消息，从而耗费了接收者资源，因此需要提供较好的分片报文认证支持。

2.4　隐私保护

DTN 网络中，消息采用“存储-携带-转发”机制进行传输，因此消息往往需要存储在中间节点上。中间节点具有信息传输路径上的上一跳及下一跳节点的信息。然而，在实际应用中并不能保证每个中间节点都是可信的，即使对消息进行了加密，中间节点也可能违反发送端的策略，获取通信双方身份等信息。但是，缺乏可控路由、信息反馈机制和全网拓扑知识等特点，使得传统的“洋葱路由”(Onion Routing)[17]等匿名通信机制无法满足 DTN 的需要。

3　DTN 网络安全机制

从 DTN 特有的安全问题出发，研究人员进行了大量的研究。总体说来，现有的 DTN 网络安全机制从安全体系结构、分片认证、协议、匿名性等方面致力于解决以上安全问题。本节将一一给予介绍。

3.1　DTN 安全体系结构设计

DTN 安全体系结构设计主要解决资源安全、Bundle 安全问题，其核心涉及到参与者的交互认证、密钥交换、消息完整性检查。目前，典型的方案包括早期使用 PKI 的设计，以及最近的基于 IBC、HIBC 等安全结构设计的方案。

为了对 DTN 网络的基础设施以及数据进行保护，DTN 工作组[12,18]提出了用于 DTN 网络的安全体系结构。出于对 DTN 设施的保护，需要对转发节点(DTN 路由器和 DTN 网关)认证，且发送者的消息也需要被转发节点认证，以防止未授权流量消耗资源。该安全体系结构的实现采用公钥加密机制，主要由 4 个部分组成：用户、DTN 路由器、DTN 网关、DTN 证书管理机构。路由器和用户各自具有公/私密钥对，用户在发送消息之前必须从证书管理机构取得其签名公钥和证书，“证书”以包含可验证的发送者的身份标识、服务请求类型以及其它用于消息内容认证的传统加密方法。当用户通过 DTN 路由器发送消息时，用户必须提交其签名公钥和证书。第一跳 DTN 路由器将使用从证书管理机构获得的公钥和证书，对该发送者、请求服务类型、访问控制等进行验证。消息被接受以后，该 DTN 路由器将使用自己的公钥对消息进行重新签名。通过使用这种方法，只有第一跳的接入路由器需要缓存每个用户的证书，非边缘的核心 DTN 路由器则通过上游的 DTN 路由器验证消息的合法性。

A. Seth 等[19]认为上述体系结构由于使用了 PKI 中心认证机构，不适用于 DTN 网络，因此提出了一种适用于 DTN 网络层次化的基于身份的加密方案 HIBC (Hierarchical Identity-based Cryptography)。基于身份的加密方法能够使用公用的标识符(比如 Email 地址等)对消息进行加密和签名验证。IBC 系统包含参与者(消息发送者和接收者)和一个公共第三方可信机构 PKG(Private Key Generator，PKG)。A. Seth 等提出的 HIBC 安全体系结构如图 2 所示。假设 HIBC 共有 t 个层次，其用户身份表示可以用 $username@ID_1 \cdots ID_{t-1}$ 表示。根据管理域或者策略，将 DTN 网络中的各个区域组织成类似的树结构。该域最高管理机构维护顶层的 PKG，而每个子域维护该域内的 PKG。用户可以从最近域的 PKG 请求公共 ID 和私钥，或者直接向顶层 PKG 请求。这个过程仅当新用户加入而需要 ID 的时候执行一次，同时每个 DTN 路由器也必须维护一个唯一的 ID。HIBC 允许用户创建一个端到端的安全通道，发送者通过使用接收者的身份作为公钥对消息进行加密，这将可以提供机密性、完整性以及授

权访问。除了提供端到端安全模型以外，HIBC 也可以对基础设施提供一定级别的保护。通过使用基于时间的证书回收机制实现证书的更新，防止其它恶意节点攻击。由于 HIBC 的优越性，实际开发使用的 DTN 网络也用此作为安全问题的解决方案[20]。

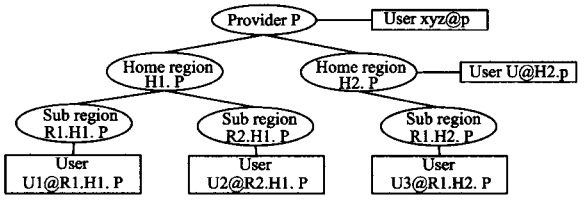


图 2　HIBC 模型

N. Asokan[21]对传统安全加密机制与基于身份的加密机制（IBC）进行了比较，认为 IBC 在认证方面并没有明显改进，但是其应用可以有效降低对网络连接和认证服务器的要求，并能够提供更好的机密性。他们同时提出了一种与通用授权结构（Generic Authentication Architecture，GAA）结合的安全初始化（Initializing security）方法，以解决用户与 PKG 进行安全关联的问题。

3.2　分片认证方案

分片认证是 DTN 网络中特有的一种现象。对 Bundle 进行完整性保护的最简单方法就是当整个 Bundle 传输完成后对其进行认证。然而这种方法持续时间较长，会消耗大量的 DTN 存储和通信资源。

早期，DTN 工作组提出了一种“一次性方法”（toilet paper approach），也即对 Bundle 每个分片独立地进行签名。这种方法计算开销较大，而且由于附加签名到数据上，带来了较大的流量负载。

C. Partridge[22]提出了“累积认证”（Cumulative Authentication）方法，该方法对 Bundle 的分片 $d_1, d_2, \cdots, d_m$，以及 Hash 函数 A，可以得到签名 $a_i = A(d_1, d_2, \cdots, d_i)$，而“一次性方法”采用的是 $a_i = A(d_i)$。使用这种“累积认证”方法可以在已经接收到 $(d_1, d_2, \cdots, d_{i-1})$ 的情况下认证 d_i。即如果 d_i 中的签名消息 $a_i = A(d_1, d_2, \cdots, d_{i-1}, d_i)$，可以认为 d_i 部分是完整的。与“一次性方法”相比较，接收端工作减少了，但是对于发送者的工作量并没有减少，而且由签名引起的流量开销也没有减少，同时这种方法需要假定每个分片需要顺序到达。

为了克服“累积认证”的缺点，C. Partridge 进一步提出采用“函数定义”（function definitions）方法认证分片，这种方法就是为认证函数 A 找到一个合适的初始化向量 iv，使得每一个分片 $d_1, \cdots d_i$ 在 A 和 iv 的映射下为其序列号，即服从 $A(iv, f_1)1, A(iv, f_2) = 2, \cdots, A(iv, f_m) = m$。如果能够找到一个较简单认证函数 A 和一个较小的初始向量 iv，这样就可以将 A 和 iv 发送给接收者进行认证，而不用对每个分片发送单独的 Hash 函数。目前已经证明，当使用的 iv 比较大的时候，普通 MD5 认证函数即可满足条件。不过，由于 iv 太大，降低了效率。如何找到一个更为高效的认证函数是一个未解决的问题。

N. Asokan[23]提出了一种基于构造二分 hash 树的方法，用于对分片进行认证。发送端将 n 个分片 d_i 采用“一次性方法”计算 $h_i = A(d_i)$，$i = 1, \cdots, n$，然后可以通过 $h_{h(i,i-1)} = h(h_i, h_{i+1})$，$i = 1, 3, \cdots, n-1$ 计算下一个 $n/2$ 集合的 Hash 值，一直迭代直到计算出了 $h_{(1,n)}$，最后的 hash 值作为顶层 Hash 值。比如，对于有 8 个分片的 Bundle，按照上面的方法，如图 3 所示，为了验证 d_3，需要已知 $h_4, h_{(1,2)}, h_{(5,8)}, h_{(1,8)}$ 即可，这种方法降低了发送端和接收端的计算开销，但是增加了存储开销。

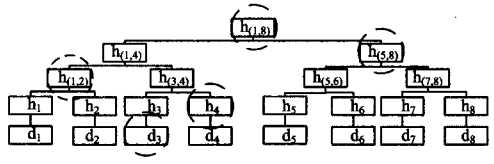


图 3　二分 hash 树

3.3　协议安全方案

DTN 网络中的协议安全主要是针对 Bundle 层及其相关的协议，包括 Bundle 层的路由以及建立在 Bundle 层上的应用协议等。

针对 Bundle 层，DTN 工作组提出在 Bundle 中添加 3 种形如 IPsec 风格的不同的安全首部，以提供不同的安全等服务[24]。其中 Bundle 认证块（Bundle Authentication Block，BAB）添加了消息认证码或签名，以保证每跳之间的完整性和认证；载荷完整性块（Payload Integrity Block，PIB）用以提供端到端的认证和完整性；载荷机密性块（Payload Confidentiality Block，PCB）用以对 Bundle 的加密载荷进行封装。对于以上的安全首部可以进行组合使用，以提供不同的安全性。

针对 Bundle 层的路由协议，DTN 网络中恶意节点可能会拒绝或者延时发送、泛洪无用数据、损坏路由表、伪造网络确认报文等。但是现有的安全路由协议通常需要认证机制的支持，这种认证机制通常难以部署和实现，并且 PKI 认证机制反而会对路由带来不利影响，减少宝贵的通信机会。John Burgess[25]对缺乏安全机制的路由协议的抗攻击进行了量化分析，其结果令人欣慰：对于移动模式未知、使用包复制的路由协议，DTN 网络具有很好的抗攻击能力。而对于复杂攻击，如果节点具有无中心认证机构，采用加密 Hash 认证，也能够取得较好的抗攻击能力。究其原因在于 DTN 环境中攻击传播速度相对较慢。

3.4　匿名性

A. Kate[26]在基于 IBC 的 DTN 安全网络体系结构上，提出了第一个匿名认证的协议。该匿名通信协议能够使得发送者和接收者都知道对方的身份，但是窃听者和网络实体不能确定发送者和接收者的身份。其匿名性主要是由该协议提供的“伪名称”机制保证的，且 DTN 路由器不用学习用户身份就能够确定合法用户的伪名称。

该匿名通信协议包括匿名认证、非交互式匿名传输、接收者匿名、密钥撤销多个阶段。在匿名认证阶段，匿名通信发起用户确认 DTN 路由器的身份，同样 DTN 路由器也能够确定使用伪名称的用户的合法性。具体的匿名认证功能通过修改 SOK 密钥协商框架，将原有 SOK 框架中的用户身份更换成为伪名称，从而定义了一个新的匿名密钥协商框架。

在非交互式传输阶段，匿名用户确保只有路由器才能对消息解密。在接收端匿名过程中，通过两次使用对称密钥加密密文来隐藏接收者的真实身份。在密钥撤回阶段，主要是 PKG 周期性地更换主密钥和撤销用户过期的私钥。该匿名

通信协议能够与多种路由策略结合，在多种 DTN 环境下获得匿名通信的效果。

结束语 DTN 网络具有广阔的应用前景，也得到了广泛的研究。本文对 DTN 网络特有的安全问题进行了深入分析，并总结了当前的已有研究成果。由于 DTN 网络仍然处于快速发展阶段，还有许多安全问题没有得到解决，尚有许多新的领域值得探索。密钥管理、路由安全、组播认证、任播认证、分片认证等领域将成为未来研究的热点问题。

在密钥管理中，虽然 IBC 方案相对于 PKI 更加适合于 DTN 网络，但是对于密钥的部署、更新等问题缺乏进一步的深入研究。

DTN 路由协议的安全性在多种移动模式、各类路由策略适应性方面的问题亟待解决。同时，还需要考虑到中间节点应能根据本地状态、发送者身份等信任条件实施存储、转发等决策，因此对于基于安全策略的路由协议尚需进一步研究。

参 考 文 献

[1] Zhao W, Ammar M, Zegura E. A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks[C]// Proc. of MobiHoc. Roppongi, Japan, 2004: 187-198

[2] Akyildiz I F, Akan O B, Chao Chen, et al. the state of the art in interplanetary Internet[J]. IEEE Communications Magazine, 2004: 108-118

[3] Kurose P J, Levine B N. A Survey of Practical Issues in Underwater Networks[C]// ACM WUWNet. Los Angeles. California, USA, Sept. 2006: 17-24

[4] Nichols R A, Hammons A R. Performance of DTN-based Free-space Optical Networks with Mobility[C]// IEEE MILCOM Conference, 2007

[5] Ott J, Kutscher D. A Disconnection - Tolerant Transport for Drive-thru Internet Environments[C]// IEEE INFOCOM. Miami, Mar. 2005: 1849-1862

[6] Akan Ö B, Fang Jian, Akyildiz I F. Performance of TCP Protocols in Deep Space Communication Networks[J]. IEEE Communications Letters, 2002, 6(11): 478-480

[7] Goff T, Moronski J, Phatak D S. Freeze-TCP: A True End-to-end TCP Enhancement Mechanism for Mobile Environments[C]// IEEE Infocom. Israel, 2000: 1537-1545

[8] http://www.dtnrg.org/

[9] Krishnan R, Basu P, et al. The SPINDLE Disruption - tolerant Networking System[C]// IEEE MILCOM. 2007

[10] Cerf V, Burleigh S, Hooke A, et al. Delay-Tolerant Networking Architecture[Z]. Internet RFC 4838, April 2007

[11] Scott K, Burleigh S. Bundle Protocol Specification[Z]. Internet RFC 5050, Nov. 2007

[12] Fall K. A Delay-tolerant Network Architecture for Challenged Internets[C]// ACM Sigcomm. Karlsruhe, Germany, 2003: 27-34

[13] Zhang Z. Routing in intermittently connected mobile ad hoc networks and delay tolerant networks: overview and challenges[J]. IEEE Communications Surveys and Tutorials, 2006, 8(1): 24-37

[14] Farrell S, Cahill V. Security considerations in space and delay tolerant networks[C]// IEEE International Conference on Space Mission Challenges for Information Technology (SMC-IT'06). July 2006: 29-38

[15] Farrell S, Symington S, et al, Delay-Tolerant Networking Security Overview[Z]. draft-irtf-dtnrg-sec-overview-04. txt February 24, 2008

[16] Kent C A, Mogul J C. Fragmentation Considered Harmful[C]// ACM SIGCOMM. New York, USA, 1995: 75-87

[17] Goldschlag D, Reed M, Syverson P. Onion routing for anonymous and private internet connections[J]. Communications of the ACM, 1999, 42(2): 39-41

[18] Durst B. A Infrastructure Security Model for Delay Tolerant Networks[OL]. http://www.dtnrg.org/

[19] Seth A, Hengartner U, Keshav S. Practical security for disconnected nodes[C]// First Workshop on Secure Network Protocols (NPSec). November 2005: 31-36

[20] Seth A, et al. Low-cost Communication for Rural Internet Kiosks Using Mechanical Backhauls[C]// ACM Mobicom. Los Angeles, CA, USA, 2006: 334-345

[21] Asokan N, Kostiainen K, et al, Applicability of Identity - based Cryptography for Disruption-tolerant Networking[C]// MobiSys Workshop on Mobile Opportunistic Networking (MobiOpp). San Juan, Puerto Rico, June 2007: 52-56

[22] Partridge C. Authentication for Fragments[C]// Fourth Workshop on Hot Topics in Networks (HotNets-IV). College Park, MD, November 2005

[23] Asokan N, Kostianinen K, et al, Towards securing disruption - tolerant networking[R]. NRC-TR-2007-007. Nokia Research Center

[24] Symington S, Farrell S, Weiss H. Bundle Security Protocol Specification[Z]. draft-irtf-dtnrg-bundle-security -05. txt, February 2008

[25] Burgess J, Bissias G, Corner M D, et al. Surviving Attacks on Disruption-Tolerant Networks without Authentication[C]// ACM Mobihoc. Montréal, Québec, Canada, 2007: 61-70

[26] Kate A, Zaverucha G, Hengartner U. Anonymity and security in delay tolerant networks[C]// 3rd International Conference on Security and Privacy in Communication Networks (SecureComm). 2007: 504-513

[27] Fall K, Farrell S. DTN: An Architectural Retrospective. Special issue on delay and disruption tolerant wireless communication [J]. IEEE JSAC, 2008, 26(5): 828-836