群组密钥协商协议的安全性分析方法研究

赵秀凤[1,2] 徐秋亮[2] 韦大伟[1]
(信息工程大学电子技术学院 郑州 450004)[1] (山东大学计算机科学与技术学院 济南 250101)[2]

摘 要 群组密钥协商允许多个用户通过不安全的信道建立一个共享的会话密钥,设计安全的群组密钥协商协议是最基本的密码学任务之一。介绍了群组密钥协商协议的两类安全性分析方法:计算复杂性方法和形式化分析方法,详细讨论了计算复杂性方法中的关键技术,包括基于规约的证明技术及基于模拟的证明技术、基于规约的安全模型和基于模拟的安全模型,探讨了安全性分析方法的发展趋势。

关键词 密钥协商,可证明安全,安全模型,规约,模拟,UC框架
中图法分类号 TP309 **文献标识码** A

Security Analysis Approaches for Group Key Agreement Protocols

ZHAO Xiu-feng[1,2] XU Qiu-liang[2] WEI Da-wei[1]
(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)[1]
(School of Computer Science and Technology, Shandong University, Jinan 250101, China)[2]

Abstract Group Key agreement allows multi users to establish a common session key though insecure channels. Designing secure group key agreement protocols is one of the most fundamental cryptographic tasks. This paper introduced two approaches developed for analyzing security group key agreement protocols: computational complexity approach and formal analysis approach. The key technologies of computational complexity approach were discussed, including the proof technology based on reduction and simulatability, and security models based on reduction and simulatability. The trends in this field were presented.

Keywords Key agreement, Provably secure, Security model, Reduction, Simulatablility, UC framework

密钥协商是信息安全中的基础问题,是建立信息系统安全机制的关键。由于网络中群组活动的增多,比如远程会议、多方协作、网络资源服务等,使用群组密钥协商(Group Key Agreement,GKA)协议来保护通信的安全性的需求越来越广泛,群组密钥协商协议的研究因而成为近来非常活跃的研究领域。研究群组密钥协议对电子政务、电子商务日常生活等诸方面都有重要的理论意义和应用价值。

1 安全性分析方法概述

早期的密码协议设计和分析方法是启发式方法。由于新的密码分析技术的出现是不确定的,而任何新的分析技术都可能使得密码协议被破解,因此启发式方法很难确保一个密码协议的安全性。在这种情况下,密码协议的形式化分析成为研究热点。所谓形式化方法,指的是分析者通过建立安全模型,该模型用基于计算复杂性,或者逻辑推理的形式化方法来分析协议的安全性。

密钥协商协议的安全性分析方法主要有两种:计算复杂性方法(Computational complexity approach)和形式化方法(Formal analysis approach),所对应的模型分别称为计算性模型和形式化模型。在计算复杂性方法中,消息表示为比特串,敌手是概率多项式时间的图灵机。这种模型和协议的现实执行比较接近,但是证明往往是手工的和非形式的。相比之下,在形式化方法中,各种密码学操作被认为是完美的黑盒,描述为符号化的函数或方程,敌手通过黑盒进行计算。采用这种抽象的符号逻辑方法可以建立自动化的验证工具,但是安全证明在计算模型中不一定可靠(sound)。

1.1 计算复杂性方法

密码学界对计算复杂性理论的研究始于20世纪80年代,发展于90年代。1984年,Goldwasser和Micali[1]首次将计算复杂性理论引入密码学领域,提出了可证明安全的思想。90年代,Bellare等人[2]将计算复杂性方法用于两方的密钥协议,提出了著名的BR模型,充分体现了可证明安全理论的应用前景。追求密码协议或密码算法的可证明安全依然是目前的研究热点,并且可证明安全理论仍将是密码协议研究的主流方向。

可证明安全建立在计算复杂性理论的框架内,它通过评估敌手攻击协议的成功概率和计算复杂度来衡量协议的安全性。在可证明安全方法中,主要包括3个部分:困难问题、安全模型(即安全性定义)和证明方法。其中,困难问题是指人们普遍相信在多项式时间内解决该问题的概率是可以忽略的

到稿日期:2010-07-07 返修日期:2010-09-30 本文受国家自然科学基金(60873232)资助。
赵秀凤(1977—),女,博士生,讲师,主要研究方向为信息安全与密码学;徐秋亮(1960—),男,教授,博士生导师,主要研究方向为信息安全与密码学,E-mail:xuqiuliang@sdu.edu.cn(通讯作者);韦大伟(1962—),男,副教授。

问题。

1.2 形式化分析方法

对密码学协议进行形式化分析可以追溯到 Dolev-Yao 模型。1983 年 Dolev 和 Yao[3]最早提出了协议安全性分析的符号模型，称为 Dolev-Yao 模型。20 世纪 90 年代，形式化方法开始成为协议分析领域的研究热点。

形式化分析方法是指用数学方法描述形式规则和推理的证明系统。通常将安全协议形式化分析方法分成两类：自动化证明和半自动化证明。模型检测方法借助于自动化分析工具，从协议的初始状态开始，对合法主体和攻击者的所有可能执行路径进行穷尽搜索，以期找到可能的错误状态。另外一类是定理证明方法和信念逻辑方法，从用户接收和发送的消息出发，通过一系列的推理证明协议是否满足目标安全属性，需要协议分析人员辅助执行，属于半自动化证明技术。

使用形式化分析方法时需要注意两点：第一，对于分析得到的一个值，必须保证所断言的抽象安全特性可以转化为具体协议的具体安全特性。第二，自动化分析的复杂性随着系统中消息和会话数量的增加而增长得特别快。因此，一个可行的方法是把协议分解为简单的子协议，然后独立地分析子协议的安全特性，再通过组合定理得到协议的安全特性[4]。

形式化分析方法已成功用于两方密钥协商协议的安全性分析[5]，但是目前还没有成果显示用形式化的方法来分析群组密钥协商协议的安全性。所以，这里不再详细介绍形式化分析方法及形式化模型。

2 计算复杂性方法中的证明技术

在计算性安全模型中，计算复杂性方法又分为两种证明技术，即规约证明（proof based on reduction）和模拟证明（proof based on simulatability/indistinguishability）。

2.1 规约证明

所谓规约证明，就是在一定的安全目标下，为待设计的密码协议建立严格的安全模型，并在计算复杂性理论的框架下，利用“归约”的方法把已经得到深入研究的计算问题或者基本密码模块的安全性归约到对密码协议的攻击[5]。密码协议的安全性一般借助于由敌手和挑战者组成的攻击游戏（attack game）来定义。因此，规约证明有时也称为基于游戏的证明方法（game-based approach）。

2.1.1 直接规约

敌手定义为试图赢得游戏的多项式时间的图灵机，游戏描述了密码学协议和假设以及应该满足安全特性。协议的可证明安全性通过反证法得到：如果敌手可以以不可忽略的概率赢得这样一个攻击游戏，那么一个良定义（well defined）的计算假设是无效的（如求解离散对数、大整数分解的困难性等），即可以利用敌手的能力构造一个解决困难问题的模拟器[6]。例如，文献[7]中将两方密钥协商协议的安全性直接规约到求解一个判定的扩增双线性 Diffie-Hellman 指数（decisional ABDHE）问题。

2.1.2 游戏序列法（Sequence of Games）

2004 年，Shoup[8]提出了一种密码协议的安全性规约证明技术，称为“游戏序列”法。“游戏序列”法的证明框架描述为：首先构造一系列的游戏 $G_0, G_1, \cdots, G_n$。其中 G_0 是敌手与密码学任务之间原始定义的攻击游戏。在安全性证明中，对于每个游戏定义一个事件 $Win_i, i=0,1,\cdots,n$，事件 Win_0 表示对原始游戏成功的攻击。而事件 $Win_i, i=1,2,\cdots,n$ 表示与 Win_0 相关的事件。然后证明 $\Pr[Win_i]$ 和 $\Pr[Win_{i+1}]$“非常近似”（$i=0,1,\cdots,n-1$）。而 $\Pr[Win_n]$ 和目标概率相等（或近似相等）（or negligibly close）。由于 n 是常数，就可以得出 $\Pr[Win_n]$ 与目标概率“非常近似”，安全性得证。文献[9,10]分别利用“游戏序列”法证明了群组密钥协商协议的安全性。

2.1.3 混合证明技术（Hybrid Technique）

“混合证明”技术[11]是一种特殊类型的规约技术，通过构造计算不可区分的混合采样序列来证明两个分布的计算不可区分性。令 D_A 和 D_B 为两个分布，为了证明它们计算不可区分，定义一系列混合采样序列 D_i（前 i 个变量从分布 D_A 上采样，其余变量从另一个分布 D_B 采样），$i=0,1,2,\cdots,n$，这样 $D_0=D_B, D_n=D_A$。如果存在一个区分器 D 可以区分两个分布上单个的采样（single sample），则区分器 D 可以区分任何两个相邻的混合采样 D_i 和 D_{i+1}，而区分器 D 可以通过困难问题利用直接规约法得到。假设区分器 D 的优势为 Adv_D，则利用区分器 D 可以构造 D_A 和 D_B 的区分器 D'，其优势为 $(n-1)Adv_D$。文献[12]利用“混合证明”技术证明了基于身份的群组密钥协商协议 ID-GKA 的会话密钥安全和前向安全。

2.2 模拟证明

所谓模拟证明，即首先在理想模型中定义密钥协商协议和敌手，然后利用计算不可区分性来定义理想模型中的安全性。如果能够证明现实世界的协议和敌手可以模拟理想协议和敌手，则证明了现实世界的协议至少具有和理想协议同样的安全属性。模拟证明的难点在于定义理想模型中的安全性和构造模拟器（simulator）。理想模型中的安全性定义应该可以让敌手充分发挥其攻击能力，而在模拟证明过程中，模拟器往往不知道群组密钥协商协议使用的私钥。为了模拟真实环境，算法需要借助某些基本方法论。文献[13]通过构造模拟器，利用模拟的方法，证明了群组密钥协商协议 LTDH 的 UC 安全性。

3 计算性安全模型

安全模型是可证明安全方法的关键部分，在安全模型中需要定义敌手行为和敌手目的。敌手行为是对敌手可能采取攻击方法的形式化描述，敌手目的定义了敌手攻击协议成功所需要达到的目标。一般而言，敌手具有最强的攻击行为，而敌手目的最简单，这样的安全定义提供最好的安全性。

3.1 安全属性

群密钥协商协议最基本的安全性需求是保证会话密钥的机密性，称为认证的密钥交换（Authenticated Key Exchange，AKE）安全，目标在于保证外部敌手不能区分真实协议的会话密钥和一个随机数。第二个安全性需求称为相互认证（Mutual Authentication，MA）安全，目标在于保证所有合法用户并且只有合法用户才可以计算出相同会话密钥。

AKE 安全是针对新鲜会话定义的，即敌手不允许代表合法用户，也不允许获得会话的中间状态，也就是说在会话期间用户必须是诚实的。相对于 AKE 安全，MA 安全则没有这样的限制。由于 MA 安全考虑了恶意参与者的内部攻击，因此

MA 安全是群密钥协商协议的一个重要的安全属性。

考虑到在会话结束之后用户可能遭受到威胁，引入了前向安全(Forward Secrecy，FS)的概念。前向安全指当协议的某个参与者的长期私钥泄露，攻击者仍然不能由此求出在私钥泄露之前所协商的会话密钥，若所有协议参与者的长期私钥都泄露，攻击者不能由此求出他们在私钥泄露之前协商获得的会话密钥，则称为完美前向安全(Perfect Forward Secrecy，PFS)。

群密钥协商协议中另外一个非常重要的安全属性称为抗密钥泄露伪装攻击安全(Key Compromise Imprersonation Resilience，KCI)。我们可以非形式地描述为：假设实体 A 和 B 是两个协议参与者，则当实体 A 的长期私钥泄漏之后，很显然，一个获得该私钥的攻击者能够向其他用户(例如 B)来冒充 A。然而，我们还希望这一密钥泄漏不会使攻击者反过来向实体 A 冒充为其他用户(例如 C)。

考虑恶意参与者的情况下，群密钥协商协议的一个重要安全属性为无密钥控制或贡献性，保证会话密钥必须由所有参与者共同合作产生，即无论是协议参与者，还是攻击者，都不能将群用户正在协商的会话密钥的全部或部分设置成某个其预先选定的值，以保证会话密钥的贡献性、新鲜性和不可预知性。

3.2 基于规约证明的计算性安全模型

自 1993 年 Bellare & Rogaway[2] 提出 BR 模型以来，出现了许多 BR 模型的扩展，如用于分析基于口令认证的三方密钥协商协议的 BPR 模型[14]。2001 年，Bresson，Chevassut 和 Pointcheval[15] 等人首次将 BR 模型扩展到面向群组的应用环境，提出了群组密钥协商协议的计算性安全模型，即 BCPQ 模型。Bresson 等人在随后的工作中仍然致力于群组密钥协商协议的计算安全模型研究，提出了动态 GKA 协议的安全模型[16]和基于口令认证的 GKA 协议安全模型[17]，并且提出了考虑恶意参与者的内部攻击模型：BMS 模型[18]、BM 模型[19]和优化的 BM 模型[20]。PKC 2009，Choudary Gorantla 等人[9]研究了抵抗 KCI 攻击的群组密钥协商协议的计算性安全模型，称之为 CBN 模型。

3.2.1 BCPQ 模型

BCPQ 模型是第一个群组密钥协商协议的计算安全模型，对于群组密钥协商协议的可证安全性研究具有十分重要的理论意义。

(1)协议参与者(protocol participants)

非空集合 $ID=\{U_1,U_2,\cdots,U_n\}$ 是由 n 个群组密钥协商协议 P 参与者的身份标识构成，用户数 n 是安全参数 k 的多项式。模型用大量的实例来表示协议的参与者 $U_i\in ID$，每个用户可以有多个不同的实例同时运行群组密钥协商协议。用 $\prod_i^{si}$ 表示用户 U_i 的第 si 个实例，这些实例主要用来模拟协议的并发执行。

(2)长期密钥(long-lived keys)

在协议运行之前，假设每个用户 U_i(ID 都有一个长期私钥 LL_i(对称的或非对称的)。

(3)会话标识(session IDS：SIDS)

在协议的一次运行中，定义预言机 $\prod_i^{si}$ 的会话标识为 $SIDS(\prod_i^{si})=\{SID_{ij}:U_j\in ID\}$，其中 SID_{ij} 是预言机 $\prod_i^{si}$ 和预言机 $\prod_j^{sj}$(也可能是攻击者 $\mathcal{A}$)之间在协议的一次运行中交换全部信息的级联。攻击者 $\mathcal{A}$ 仅需窃听就可以把 $SIDS$ 恢复出来。

(4)接受(accepting)

若预言机 $\prod_i^{si}$ 有足够的信息可以计算出会话密钥 SK，则称 $\prod_i^{si}$ 接受。$\prod_i^{si}$ 接受意味着会话密钥 SK 和会话标识 $SIDS$ 变成确定的值。

(5)预言机查询(oracle queries)

敌手 $\mathcal{A}$ 可以对无数个 oracle 进行以下查询，每一种查询都模拟了敌手的攻击能力。

Send($\prod_U^s$，m)：敌手 $\mathcal{A}$ 向用户 U 的实例发送消息 m，并获得用户 U 出来消息 m 的响应。查询 Send($\prod_U^s$，"*start*")表示对协议 P 的初始化。

Reveal($\prod_U^s$)：这个查询无条件地返回会话密钥 SK 给敌手 $\mathcal{A}$。只有在用户实例 $\prod_U^s$ 已经接受的情况下，敌手才可以进行 Reveal 查询。Reveal 查询刻画了已知会话密钥安全。

Corrupt(U)：这个查询返回用户 U 的长期私钥 LL_i，但是并不返回用户实例 $\prod_U^s$ 在协议 P 运行过程中的任何内部数据。

Test($\prod_U^s$)：这个查询模拟了会话密钥的语义安全性，并且在协议运行中，敌手只能进行一次 Test 查询，且被查询的用户实例是新鲜的(fresh)。用户实例 $\prod_U^s$ 随机抛币 b，如果 $b=1$，则将会话密钥 SK 返回为敌手 $\mathcal{A}$，否则将一个随机数返回给敌手 $\mathcal{A}$。

(6)伙伴关系(partnering)

如果两个实例 $\prod_i^s$ 和 $\prod_j^t$ 接受了它们计算的会话密钥，且 $SIDS(\prod_i^{si})\cap SIDS(\prod_j^{tj})\neq\varnothing$，则称 $\prod_i^{si}$ 和 $\prod_j^{tj}$ 是直接伙伴，表示为 $\prod_i^s\leftrightarrow\prod_j^t$。如果存在图 $G_{SIDS}:=(V,E)$，其中 $V:=\{\prod_i^s|U_l\in ID,l=1,2,\cdots,n\}$，$E:=\{(\prod_i^s,\prod_j^t)|\prod_i^s\leftrightarrow\prod_j^t\}$，对协议中的所有实例($\prod_i^s$)有如下式子成立：$\exists k>1$，$\langle\prod_1^{s_1},\prod_2^{s_2},\cdots,\prod_k^{s_k}\rangle$ 使得 $\prod_1^{s_1}=\prod_i^s$，$\prod_k^{s_k}=\prod_j^t$，$\prod_{l-1}^{s_{l-1}}\leftrightarrow\prod_l^{s_l}$，则称实例 $\prod_i^s$ 和 $\prod_j^t$ 是间接伙伴关系，记为 $\prod_i^s\leftarrow\sim\sim\rightarrow\prod_j^t$。

(7)新鲜性(freshness)

如果一个实例 $\prod_U^s$ 是新鲜的(或实例 $\prod_U^s$ 有一个新鲜会话密钥 SK)，则必须满足下面 4 个条件同时成立：(1) $\prod_U^s$ 已经接受一个会话密钥；(2)在 $\prod_U^s$ 接受之前没有对它进行 Corrupt 查询；(3)在 $\prod_U^s$ 接受之后，没有对它进行 Reveal 查询；(4)没有对 $\prod_U^s$ 的伙伴 PID($\prod_U^s$)进行 Reveal 查询。

(8)AKE 安全

通过攻击者 $\mathcal{A}$ 和用户实例 $\prod_U^s$ 之间的游戏 $Game^{AKE}(\mathcal{A},P)$ 来定义协议的安全性：首先，敌手可以查询上述任意 oracle，在协议运行的某一阶段，攻击者 $\mathcal{A}$ 向新鲜的用户实例 $\prod_U^s$ 发送

Test 询问，然后 $\mathcal{A}$ 可继续作其它询问，最后 $\mathcal{A}$ 输出 Test 询问中 b 的猜测值 b'。如果 $Adv^{AKE}(\mathcal{A})$ 是可忽略的，则称协议 $\mathcal{A}$ 是 AKE 安全的，其中 $Adv^{AKE}(\mathcal{A},P)$ 表示敌手成功猜测 b 的优势。

(9)MA 安全

MA 安全用来描述一个计算有限的敌手无法成功伪装一个合法的用户 U。通过攻击者 $\mathcal{A}$ 和用户实例 $\prod_U^s$ 之间的游戏 $Game^{MA}(\mathcal{A},P)$ 来定义 MA 安全性：敌手可以查询上述任意 oracle。对于协议 P 执行过程中，称敌手破坏了 MA(mutual authentication)，如果至少存在一个协议实例 $\prod_U^s$ 使得该实例以 $SIDS(\prod_U^s)$ 为会话标识，以 $PIDS(\prod_U^s)$ 为伙伴标识接受，但是 $|PIDS(\prod_U^s)|\neq n-1$。记 $Adv^{MA}(\mathcal{A},P)$ 为敌手成功破坏 MA 安全的优势。如果 $Adv^{MA}(\mathcal{A},P)$ 是可忽略的，则称协议 P 是 MA 安全的。

3.3 基于模拟证明的计算性安全模型

1998 年，Bellare，Canetti 和 Krawczyk 提出了两方的认证密钥协商协议的可计算性安全模型，称为 BCK 模型[21]。BCK 安全模型提出了一种“模块化”的设计原则，并采用了“模拟”的证明方法。Shoup[22] 借鉴了 BCK 模型的模块化设计思想，提出了基于模拟证明的两方密钥协商协议的计算性安全模型，即 Shoup 模型。2001 年，Canetti 和 Krawczyk[23] 提出了著名的 CK 模型，用于分析两方的认证密钥协商协议，该模型也是基于模块化思想。

在复杂网络环境中，密码学协议并不是单独运行的(stand-alone)，而是与其它协议同时运行或者同一协议的多个副本同时运行，协议之间存在调用关系或消息的收发关系，协议可以以多种方式进行组合和互相影响。单个协议的基本安全性不能保证多协议组成的系统的安全性。

2001 年，Canetti[24] 首次明确提出 UC 框架(Universally Composible Framework)。UC 框架为密码协议任务的安全定义提供了精确方法，符合 UC 框架安全定义的协议称为 UC 安全的。在 UC 安全框架中，密码协议的安全性不是一一列出，而是通过理想函数准确地表达安全协议要达到的目标。UC 安全的一个显著特点是当一个安全协议和任意其他协议组合，或作为任意一个系统的组件时，这种安全性依然保持。特别地，在任意数目的协议实例并发运行并由敌手控制的条件下 UC 安全性仍然可以保持。

3.3.1 UC-KS 模型

2005 年，Katz 和 Shin[25] 在 UC 框架下给出了 GKA 的理想函数 $\mathcal{F}_{GKE}$，并证明了任何实现理想函数 $\mathcal{F}_{GKE}$ 的群组密钥协商协议可以保证 AKE 安全和抵抗内部攻击安全，我们称为 UC-KS 模型。群组密钥交换理想函数 $\mathcal{F}_{GKE}$ 描述如下：

k 为安全参数，$(U_1,U_2,\cdots,U_n)$ 为 n 个协议参与方，$\mathcal{S}$ 代表理想世界中的模拟器。$\mathcal{F}_{GKE}$ 运行如下：

(1)协议初始化阶段

当从参与方只收到 $(sid,pid,NewSession)$ 消息后，如果是第 1 次，则记录消息 (sid,pid,U_i)，同时把它转发给 $\mathcal{S}$。如果此时理想函数已经收到了 $|pid|-1$ 条这样的消息，就存储消息 $(sid,pid,Ready)$，并把这条消息转发给 $\mathcal{S}$。

(2)群组密钥生成阶段

当理想函数从 $\mathcal{S}$ 收到消息(OK)后，检查是否存在消息 $(sid,pid,Ready)$。如果有，则进行如下操作：

· 如果所有协议的参与方 $U\in pid$ 都没有被敌手攻陷，那么就由理想函数 $\mathcal{F}_{GKE}$ 生成群组会话密钥 $SK\leftarrow\{0,1\}^k$ 并存储消息 (sid,pid,SK)。

· 如果有某一个协议参与方被敌手攻陷，那么理想函数就等待模拟器 $\mathcal{S}$ 发送消息 (Key,SK)，收到后保存为 (sid,pid,SK)。

(3)密钥的发送

当收到模拟器 $\mathcal{S}$ 发送的消息 $(deliver,U_i)$ 时，理想函数检查是否存在消息 (sid,pid,SK) 并且是否属于 $U_i\in pid$。如果都符合，则向 U_i 发送消息 (sid,pid,SK)。否则，忽略掉这条消息。

(四)参与者腐败

如果模拟器 $\mathcal{S}$ 腐化了某参与者 $U_i\in pid$，而且存在这样一条消息记录 (sid,pid,SK)，并且理想函数还没有发送给 U_i，则理想函数将 SK 发送给模拟器 $\mathcal{S}$。否则，理想函数不发送任何消息给模拟器 $\mathcal{S}$。

正如文献[26]中所评论的，Katz 和 Shin 形式化了存在内部攻击者的认证群组密钥协商协议的安全模型与定义，但 Katz 和 Shin 并没有给出达到此种安全性的协议，也没有证明现有协议在他们的模型下是安全的。

UC 安全是较高级别的安全性，难以在现实环境下得以实现。一种可行的方法是假设参与方可以访问某些可信机构(trusted set-up)。基本思想是假设参与方可以访问由“可信方式”生成的初始信息，即提出了理想化的模型来辅助实现。这些模型中分别定义了某种信任假设，现有的假设模型主要有公共参考串(CRS)模型、密钥注册(KR)模型、硬件模型、时间假设(Timing)模型等。

最近，我国学者贾洪勇[13] 参考 UC-KS 模型中群组密钥交换的理想函数，在防篡改硬件令牌的基础上，利用部分隔离状态下证据不可区分知识证明，设计了一个群组密钥交换协议，安全地实现了这个理想函数。提出的群组密钥交换协议经过证明具有 AKE 安全，并且能够抵抗适应性敌手攻击和恶意参与者攻击。

结束语 随着群组密钥协商协议的广泛应用，对安全性分析方法的研究也越来越深入。首先，研究具有密码可靠性形式化分析方法是未来的发展方向之一。其次，由于群组密钥协商的安全属性比较复杂，所以如何为新的安全属性进行定义并建立合理的安全模型，仍是可证安全领域需要解决的问题。另外，从实用的角度来说，研究单个协议的安全性并不保证协议在并发网络环境中的安全性，而且形式化的分析工具无法避免状态爆炸，也试图将协议分成若干子协议来进行分析，因此研究 UC 框架及组合定理也将成为未来的研究方向之一。

参 考 文 献

[1] Goldwasser S, Micali S. Probabilistic encryption [J]. Journal of Computer and System Science, 1984, 28: 270-299

[2] Bellare M, Rogaway P. Entity authentication and key exchange [C]// Stinson D R, ed. Proc. of the Advances in Cryptology—Crypto' 93. LNCS 773. Berlin, Heidelberg: Springer-Verlag, 1993: 232-249

(下转第 156 页)

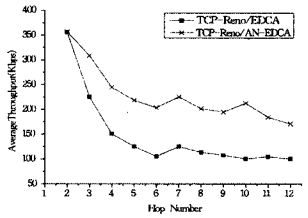

图 7　相对静止、链式拓扑数据业务吞吐量

结束语　车用自组网的固有特点严重影响了网络中数据业务的服务质量。仿真实验表明，AN-EDCA 跨层数据传输控制机制对各种应用环境中车用自组网数据业务性能均有较大提升。继续优化和改进 AN-EDCA 机制，进一步提升高速移动和多跳环境下车用自组网数据业务性能，是今后研究的重点方向。

参 考 文 献

[1] 陈立家，江昊，吴静，等. 车用自组织网络传输控制研究[J]. 软件学报，2007，18 (6)：147-149

[2] Hayashi M，Fukuzawa S，et al. Development of Vehicular Communication (WAVE) System for Safety Applications[C]// 7th International Conference on ITS. June 2007：1-5

[3] IEEE802. 11 WG，PartII：Wireless LAN Medium Access Control (MAC) and Physical (PHY) Layer Specification，Amendment 8：Medium Access Control(MAC) Quality of Service Enhancements[S]. 2005

[4] 宋军，金艳华，李媛源，等. 无线局域网 MAC 机制对 TCP 性能影响分析[J]. 计算机科学，2009，36(5)：111-114

[5] 宋军，李浩，李媛源，等. Ad-hoc 中的 TCP 改进方案—Adaptive ADTCP [J]. 计算机应用，2010，30(7)：1750-1753

[6] Fu Zheng-hua，Zerfos P，Luo Hai-yun，et al. The Impact of Multihop Wireless Channel on TCP Throughput and Loss[C]// Proc. of IEEE INFOCOM'03. April 2003

[7] 陈林，赵莉，唐亮. 网络数据传输的实现[J]. 重庆工学院学报：自然科学版，2007，21(11)：123-126

(上接第 148 页)

[3] Dolev D，Yao A C-C. On the security of public key protocols[J]. IEEE Transactions on Information Theory，1983，29 (2)：198-207

[4] Canetti R，Herzog J. Universallly composable symbolic analysis of mutual authentication and key-exchange[C]// Proc of Theory of Cryptography. LNCS 3876，2006. Berlin，Heidelberg：Springer-Verlag，2006：380-403

[5] 中国密码学会. 密码协议发展研究[R]. 2009-2010 密码学学科发展报告[D]. 北京：中国科学技术出版社，2010-04

[6] 冯登国. 可证明安全性理论与方法研究[J]. 软件学报，2005，16 (10)：1743-1756

[7] 王圣宝，曹珍富，董晓磊. 标准模型下可证安全的身份基认证密钥协商协议[J]. 计算机学报，2007，30(10)：1842-1852

[8] Shoup V. Sequences of Games：A Tool for Taming Complexity in Security Proofs[EB/OL]. Cryptology ePrint Archive，Report 2004/332，http：//eprint. iacr. org/2004/332. pdf，2004

[9] Choudary G M，Boyd C，González N J M. Modeling key compromise impersonation attacks on group key exchange protocols[C]// Jarecki S，Tsudik G. eds. Proc. of PKC 2009. LNCS 5443，Berlin，Heidelberg：Springer-Verlag，2009：105-123

[10] 李国民，何大可. 基于身份的群密钥协商协议[J]. 计算机科学，2009，36(1)：60-64

[11] Goldreich O. Foundations of Cryptography-Basic Tools[M]. volume 1. Cambridge University Press，2001

[12] Choi K Y，Hwang J Y，Lee D H. Efficient id-based group key establishment with bilinear maps[C]// Proc. of PKC 2004，LNCS vol. 2947. Berlin：Springer-Verlag，2004：130-144

[13] 贾洪勇，卿斯汉，谷利泽，等. 通用可组合的组密钥交换协议[J]. 电子与信息学报，2009，31(7)：1571-1575

[14] Bellare M，Pointcheval D，Rogaway P. Authenticated Key Exchange Secure Against Dictionary Attacks[C]// Proc. of the Advances in Cryptology-EUROCRYPT'00. LNCS 1807. Berlin，Heidelberg：Springer-Verlag，2000：139-155

[15] Bresson E，Chevassut O，Pointcheval D，et al. Provably Authenticated Group Diffie-Hellman Key Exchange[C]// Proc. of 8th ACM CCS. New York：ACM Press，2001：255-264

[16] Bresson E，Chevassut O，Pointcheval D. Provably authenticated group Diffie-Hellman key exchange-the dynamic case[C]// Boyd C. ed. Proc. of the advance in cryptology-Asiacrypt'2001. LNCS 2248. Berlin，Heidelberg：Springer-Verlag，2001：290-309

[17] Bresson E，Chevassut O，Pointcheval D. Group Diffie-Hellman Key Exchange Secure against Dictionary Attacks[C]// Proc. of the Advances in Cryptology -ASIACRYPT'02. LNCS 2501. Heidelberg：Springer-Verlag，2002：497-514

[18] Bresson E，Manulis M，and Schwenk J. On security models and compilers for group key exchange protocols[C]// Proc. of the 2nd International Workshop on Security (IWSEC 2007). LNCS 4752. Heidelberg：Springer-Verlag，2007：292-307

[19] Bresson E，Manulis M. Malicious Participants in Group Key Exchange：Key Control and Contributiveness in the Shadow of Trust[C]// Proc. of the 4th Autonomic and Trusted Computing Conference (ATC 2007). LNCS 4610. Heidelberg：Springer-Verlag，2007：395-409

[20] Bresson E，Manulis M. Securing group key exchange against strong corruptions[C]// Proc. of ACM Symposium on Information，Computer and Communications Security (ASIACCS 2008). New York：ACM Press，2008：249-260

[21] Bellare M，Canetti R，Krawczyk H. A modular approach to the design and analysis of authentication and key exchange protocols (extended abstract)[C]// Proc. of the Thirtieth Annual ACM Symposium on the Theory of Computing (STOC'98). New York：ACM Press，1998：419-428

[22] Shoup V. On formal models for secure key exchange (Version 4)[EB/OL]. RZ 3120，IBM Research，available at http：// shoup. net/，November 1999

[23] Canetti R，Krawczyk H. Analysis of key-exchange protocols and their use for building secure channels[C]// Proc. of Advances in Cryptology-EUROCRYPT'01. LNCS 2045. Heidelberg：Springer-Verlag，2001：453-474

[24] Canetti R. Universally composable security：A new paradigm for cryptographic protocols[C]// Proc. of 42nd Annual Symposium on Foundations of Computer Science (FOCS 2001). 2001：136-145

[25] Katz J，Shin J S. Modeling insider attacks on group key-exchange protocols[C]// Proc. of the 12th ACM Conference on Computer and Communications Security (CCS'05). New York：ACM Press，2005：180-189

[26] 秦波，伍前红，王育民，等. 密钥协商协议进展[J]. 计算机科学，2008，35(9)：9-12