ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.9, September 2008, pp.2403−2412
DOI: 10.3724/SP.J.1001.2008.02403
© 2008 by *Journal of Software*. All rights reserved.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种 UC 匿名的移动自组网概率组播策略*

章 洋+

(中国科学院 软件研究所 综合信息系统技术国家重点实验室,北京 100190)

A Probabilistic Multicast with Universally Composable Anonymity in MANETs

ZHANG Yang+

(National Key Laboratory of Integrated Information Systerm Technology, Institute of Software, The Chinese Academy of Sciences, Beijing 100190, China)

+ Corresponding author: E-mail: zhang_yang_own@yahoo.com.cn

Zhang Y. A probabilistic multicast with universally composable anonymity in MANETs. *Journal of Software*, 2008,19(9):2403−2412. http://www.jos.org.cn/1000-9825/19/2403.htm

Abstract: Current anonymous routing protocols do not provide anonymous mechanism for multicast in MANETs and have only had ad-hoc anonymity analysis. This paper proposes a new scheme called probabilistic multicast with universally composable anonymity. One-Time key pair is used to keep a route record in privacy during route discovery processes. Gossip-Scheme, secret DH path and Bloom Filter are adopted to realize anonymous source multicast during transmission of data packets. Finally, the protocol is analyzed based on the UC (universally composable) framework and its performance is evaluated by simulation. The analysis and simulation results show that the proposed scheme provides both anonymity and reliability for multicast in MANETs.
Key words: multicast; universal composition framework; hybrid encryption; anonymity; MANET

摘 要: 鉴于现有移动自组网匿名路由协议不能为组播提供匿名通信支持,而只能提供特定非形式化的匿名性分析,提出了一种 UC(universally composable)匿名的移动自组网概率组播策略.在路由发现阶段,采用一次性密钥对保持路径记录私密.在数据分组传输阶段,采用 Gossip 机制、DH 秘密路径及 Bloom Filter 编码实现匿名源路由组播.最后,采用 UC 框架分析了协议的匿名性,并对协议的性能进行了仿真.分析与仿真结果表明,该策略在实现匿名性的同时还提供了较好的可靠性.
关键词: 组播;UC 框架;混合加密;匿名性;移动自组网
中图法分类号: TP393 **文献标识码**: A

在典型的移动自组网(MANET)应用中,主机通常按组共同完成一个特定的任务,例如在军事上对人员、装备的指挥与控制.因此,组播在移动自组网中扮演着重要的角色.实施匿名组播机制对保护指挥机构与关键节点至关重要.

文献[1−4]在 MANET 匿名通信领域作了开创性的研究,从不同的角度提出了适用于移动自组网的匿名路由协议,并对协议的匿名性进行了分析.但是,已有的分析都是针对具体攻击类型逐条进行的,由于攻击类型很

* Supported by the National Basic Research Program of China under Grant No.2007CB307103 (国家重点基础研究发展计划(973))
Received 2006-11-06; Accepted 2007-04-06

© 中国科学院软件研究所 http://www.jos.org.cn

难穷尽列举,其分析结果不能充分说明协议满足匿名性要求.另外,这些方案都是针对单播而非组播的匿名解决方案.匿名 Gossip 协议[5]使组成员节点无需知晓与它会话的对象(其他组成员),而通过邻居节点成功传输数据,但不保证源节点身份匿名与路径私密.因特网中匿名组播协议一般使用代理服务器完成匿名收发[6],但 MANET 中拓扑的频繁变化使得直接指定代理服务器变得困难.因此,如何实现 MANET 匿名组播是一个难题,本文对此将进行研究.至于非移动自组网匿名通信技术的进展可见文献[7].

虽然在移动自组网的研究方面尚未出现经严格证明的匿名路由协议,但基于因特网的匿名信道的形式化分析逐渐被重视.文献[8]基于 UC(universally composable)[9]框架对混淆网络进行了建模、分析与构造.文献[10]同样使用 UC 框架对洋葱路由协议进行了构造与证明.不过,两者都未对路由发现过程进行分析,也不是针对移动自组网进行建模.利用 UC 框架除了可以对匿名信道进行分析,也可用于分析其他类型协议的匿名性,例如文献[11]对其提出的无线设备认证协议的 UC 匿名性与安全性进行了证明.UC 安全模型的核心思想是,首先给出理想的安全协议,其次,证明实际协议与理想协议在各自敌手攻击下其执行结果不可被环境区分,最后由合成理论保证复合后协议的安全性[9].其本质是假设在理想情况下存在可信第三方,如果实际协议达到了理想情况下的同样效果,则认为协议是安全的,这也是协议安全性证明的通用方法,例如文献[12].

移动自组网中的组播协议一般不提供可靠性机制,例如 ODMRP[13],DDM[14]等,但可靠组播在关键命令的发布、复制数据的管理、故障检测等需要保证服务可靠性的应用领域非常关键.可靠组播可粗略地分为 3 类:一类是提供“要么都交付要么都不交付”语义的组播;另一类是提供实用可靠性的组播;最后一类为基于 Gossip 的概率型组播,丢失的数据通过 Gossip 过程恢复.第 1 类由于其高负荷使其不适用于 MANET;第 2 类的例子如文献[15],但其确认机制限制了网络规模;第 3 类的例子如文献[16,17],它们通过分布负载在扩展性与可靠性方面提供了较好的均衡.本文采取的组播策略属于最后一种类型.

文中,匿名是指在数据传输过程中敌手不能确定数据分组的源节点与目的节点.按照匿名的含义,对按需源路由组播进行了定义,即定义了理想的路由发现与数据交换过程.在路由发现阶段,使用基于一次性密钥对 CPA (chosen plaintext attack)安全的混合加密方案[18,19]加密路径链表,使路径保密与完整.在数据传输阶段,基于 UC 安全信道[20]采用 Gossip,DH 秘密路径及 Bloom Filter 编码实现源路由组播.最后对协议进行了分析与仿真,得出结论.

1 模型与定义

1.1 网络与敌手假设

假设网络中有 n 个节点 $P_i(i=1,\ldots,n)$,节点间的无线信道是对称与双向的,节点具有相同的传输能力与较强的计算能力;其次,每个节点 P_i 接入网络时需要与周围节点进行认证,认证后与邻居节点 P_j 共享对称密钥 k_{ij},且拥有节点名称 N_i,N_i 用来替代节点的永久身份 P_i 作为通信时的标识,有时也称 N_i 为 P_i 的假名.发送数据的端节点 N_s 称为发送节点(或源节点),接收数据的端节点 N_d 称为接收节点(或目的节点).

假设敌手具有静态局部的窃听与入侵能力.静态是指在会话开始前,被攻陷与被窃听的节点就已被确定.局部是指敌手只能监视与控制网络中部分节点.认为组成员节点间是互信的,如果成员节点被攻陷,则协议的匿名性不再被保证;因为组成员节点间共享组密钥,成员节点被攻陷后,敌手可以获取组密钥,依赖于组密钥实施的匿名机制将不再有效.局部性隐含地假设存在独立的信道图灵机完成消息递交的功能.

1.2 混合加密与DDH假设

定义 1. 明文标记的混合加密方案Π[19,21]包含如下 3 种算法:

Gen:输入安全参数$\kappa\in Z^+$,输出公开密钥 PK 和私有密钥 SK.

Enc:输入消息 m、两个满足密码学要求的散列函数 H_1 与 H_2,选择随机数 R,输出 $E_{H_2(R)}(m)\,\|\,E_{PK}(R;H_1(R,m))$, E_{PK} 表示用公钥加密, $E_{H_2(R)}$ 表示用 $H_2(R)$作为对称密钥加密.

Dec:输入 $C_1\|C_2$,计算 $(R';H')=D_{SK}(C_2), m'=D_{H_2(R')}(C_1)$,D_{SK} 为用私有密钥 SK 解密, $D_{H_2(R')}$ 为用对称密钥

© 中国科学院软件研究所 http://www.jos.org.cn

$H_2(R')$解密;若 $H'\neq H_1(R',m')$,则拒绝 m',输出“⊥”而终止,否则正常输出 m'.

其中,$H_1(R,m)$作为消息 m 的明文标记,以验证消息 m 未被篡改.要求混合加密方案Π及原公钥加密方案至少是 IND-CPA 安全的,含义如下:

定义 2(公钥加密方案的 IND-CPA 安全性). 敌手可看作 $A=(A_1,A_2)$,其中,A_1 与 A_2 都是概率多项式时间算法.计算.

$$Adv_{A,\Pi}^{IND-CPA}=|P[(PK,SK)\leftarrow Gen(1^k);(x_0,x_1,s)\leftarrow A_1^{Enc}(PK);b\leftarrow(0,1);y\leftarrow Enc(x_b);A_2^{Enc}(x_0,x_1,s,y)=b]-1/2|.$$

x_0 与 x_1 长度相等.若对任意的概率多项式时间敌手 A, $Adv_{A,\Pi}^{IND-CPA}$ 可以忽略,则该方案就是 IND-CPA 安全的.一个概率函数 $F(x)$其概率可忽略是指对固定的正数 $l>0$,充分大的正整数 x,其值小于 $1/x^l$.

定义 3. DDH(decisional Diffie-Hellman)假设. 素数 p 阶的乘法群 G 上离散对数难解,g 为 G 的生成元;若 $Q_0=\{(p,g,g^x,g^y,g^{xy}):x,y\xleftarrow{R}Z_p\}$, $Q_1=\{(p,g,g^x,g^y,g^z):x,y,z\xleftarrow{R}Z_p\}$,$Q_0$ 与 Q_1 计算不可区分.

DDH 假设隐含 CDH 假设,即已知定义中的 g^x 与 g^y,计算 g^{xy} 困难.不失一般性,可设节点名称 N_i 为 G 中元素,$N_i=g^{x_i}$,$x_i\in_R Z_p$ 由节点 P_i 秘密保存,作为节点名称秘密数(可将(x_i,N_i)看成一对密钥).另外,可设在群 G 上存在选择消息攻击下不可伪造的数字签名方案Π_{sig}[22],据文献[9]中 Claim 14 的结论,此方案可用来实现理想的数字签名协议 F_{sig}.对于群组通信,设其成员节点共享会话密钥 k_{grp},k_{grp} 的管理超出本文范围,只假定它是 UC 安全的组密钥[23](是文献[20]中两方密钥交换概念的扩展).基于 k_{grp} 的 UC 安全信道记为 F_{SC}(相应的实现方案记为 Π_{sc})[20],Π_{sc} 在发送端的加密等操作记为$\varepsilon_{sc}(\cdot)$,接收端解密等操作记为 $D_{sc}(\cdot)$.记 F_{RKR} 为一个理想的公钥生成发布函数.本文涉及到的对称加密方案都假设满足 CPA 安全要求.

1.3 Bloom filter

Bloom Filter 作为一个 l 比特位的向量 BF,是对集合中 n 个元素的编码.选择 J 个独立的散列函数,每个都将集合中的元素映射为$\{1,2,\ldots,l\}$中的数.开始时将 BF 置 0,然后对集合中每个元素用 J 个函数散列,得到 J 个位置值,将 BF 中这些位置上的比特值置 1.

要检验一个元素是否属于集合,将其经过 J 个散列函数散列,得到 J 个值,若 BF 中相应位置都是 1,则认为其属于集合.此方法会把非集合中的元素错判为集合中元素,其概率为$(1-(1-1/l)^{nJ})^J$.给定 l 与 n,最优 J 值为 $\ln 2\times l/n$.应用时需权衡 l,n,J,可见文献[24].在设计的协议中,用此方法来形成与压缩匿名源路由组播的头地址域,以显著节省带宽,在报文重复性检验中减少存储空间并提高查询效率.向量 BF 本身不用来提供任何安全与匿名性质,在进行匿名性分析时,将向量 BF 看作一个集合.

2 匿名组播设计

移动自组网匿名概率组播(anonymous probabilistic multicast,简称 APM)是一种按需源路由组播,它包含加入通告与数据交换两个过程.组成员节点广播加入通告,其他节点收到加入通告后,以一定的概率对其优先进行 Gossip,并捎带可达路径,Gossip 方式借鉴文献[17]中的策略.当源节点与若干目的点进行 Gossip 时,它读取路径,对每个路径节点计算源与该节点的 Diffie-Hellman 秘密数(DH 数),将此 DH 数与该节点下一跳邻居的名称连接计算散列值.路径节点遍历计算 DH 数与邻居名称连接的散列值,并与源节点的散列值比较来发现下一跳节点.散列是一种高效算法,因此遍历计算可行.组播时,源节点将路径散列值 Bloom Filter 编码到数据分组的头部,路径点查询该 Bloom Filter 向量确定自己是否在路径上,从而实现匿名源路由组播.

2.1 加入通告

成员节点 N_s 在需要数据交互时广播自己的加入通告,通告报文格式如下:

$$[JOIN,seq,PK_t,\varepsilon_{sc}(x_{seq},SK_t,N_s),RList],$$

其中,$x_{seq}\in_R Z_p$,$seq=g^{x_{seq}}\in G$,seq 为全局唯一的序号,即不同节点间 seq 冲突的概率可以忽略[2];(PK_t,SK_t)为 N_s 生成的一次性非对称密钥对;$RList$ 为路径链表;$\varepsilon_{sc}(\cdot)$中可捎带数据分组的相关信息.

© 中国科学院软件研究所 http://www.jos.org.cn

RList 按路径长度阈值 $H_{\max}$ 设置为固定长.每个路径上,节点将自己的节点名称加入到 *RList* 中,并使用 PK_t 对 *RList* 进行一次加密.据 Π 计算 $RList=[\bar{E}_i,N_i,E_i^{pk}]$ 的洋葱加密方案 Π_{List} 如下:

$$N_s:[\bar{E}_0,N_0,E_0^{pk}]=[\bar{E}_{H_2(t_s)}(R_2,...,R_{H_{\max}},BEGIN),N_S,E_{PK_t}(t_s;H_1(t_s,BEGIN\,\|\,(seq)^{x_s}))],$$

$$N_1:[\bar{E}_1,N_1,E_1^{pk}]=[\bar{E}_{H_2(t_1)}(\bar{E}_0<<L,N_0,E_0^{pk}),N_1,E_{PK_t}(t_1;H_1(t_1,L(\bar{E}_0)\,\|\,N_0\,\|\,E_0^{pk}\,\|\,seq^{x_1}))],\ldots,$$

$$N_i:[\bar{E}_i,N_i,E_i^{pk}]=[\bar{E}_{H_2(t_i)}(\bar{E}_{i-1}<<L,N_{i-1},E_{i-1}^{pk}),N_i,E_{PK_t}(t_i;H_1(t_i,L(\bar{E}_{i-1})\,\|\,N_{i-1}\,\|\,E_{i-1}^{pk}\,\|\,seq^{x_i}))],\ldots$$

其中, $\bar{E}$ 仅表示对消息从右至左加密(非实际加密序);t_i 为节点 N_i 用以生成对称密钥的随机数; $R_2,...,R_{H_{\max}}$ 是填充 *RList* 的随机数,用以保持 *Rlist* 的定长;*BEGIN* 为路径链表开始标志;<<表示将消息左移;*L* 表示长度,等于 N_i 的位数与 E_i^{pk} 的位数之和,*BEGIN* 长度等于 *L*;函数 *L*(*m*)表示取消息 *m* 的最右 *L* 位; $(L(\bar{E}_{i-1})\,\|\,N_{i-1}\,\|\,E_{i-1}^{pk}\,\|\,seq^{x_i})$ 为节点 N_i 上被标记的明文.记 Π_{List} 中解密操作为 $DecOnion(SK,(N_i,x_i),RList_i,seq)\rightarrow(RList_{i-1},N_{i-1})$,加密操作为 $EncOnion(m,PK,(N_1,x_1),\ldots,(N_n,x_n))\rightarrow(RList_1,\ldots,RList_n)$.

节点 N_i 丢弃重复报文.对非重复报文通过 $D_{sc}(\varepsilon_{sc}(x_{seq},SK_t,N_s))$ 快速验证自己是否为目的节点:若是,则解密 *RList* 获得到成员节点 N_s 的路径;否则,自己不是目的节点,修改 *RList*,本地广播通告报文.

2.2 数据交换

当节点 N_s 需要扩散数据或交换缺失分组信息时,它从自己的成员节点视图中随机选择若干个成员节点进行 Gossip,Gossip 策略参照文献[17].对新发现的成员节点则以一定的概率[17]优先进行 Gossip,并捎带可达路径.在传输数据之前,生成一次性密钥对($x_R\in_R Z_p,N_R=g^{x_R}\in G$),称 N_R 为节点的随机名称.其余节点可在空闲时发送与真实分组等长的伪报文,各节点也可以打乱各分组及伪报文的收发顺序.

设对于 n_F 个目的节点有 n_F 条路径存在,*H* 为满足密码学要求的散列函数,*m* 为 N_s 需发送的消息,$C=\varepsilon_{sc}(m)$,匿名源路由组播算法如下:

(1) 对 n_F 条路径中每个节点 N_i,N_s 计算 N_i 与 N_R 的 DH 秘密数 $sh=(N_i)^{x_R}$;

(2) 设 N_i 下一跳节点为 $N'_1,N'_2,\ldots,N_s$,计算 $h_{ij}=H(sh,N'_j,C),1\le j\le n_F$;编码 h_{ij} 为 Bloom Filter 向量 *RBF*;

(3) 组播时,路由节点 N_i 计算其与 N_R 的 DH 秘密数 $sh'=(N_R)^{x_i}$,并对相邻的认证过的节点遍历,按步骤(2)的方法计算 h'_{ij} ,如果 h'_{ij} 在 *RBF* 中,那么该节点确实是路由节点,且找到为下一跳的多个节点.

N_s 在计算 *RBF* 时,若 n_F 条路径上节点总数少于系统中给定的阈值,则补充随机数,使节点总数达到此阈值,然后将它们编码到向量 *RBF* 中.

在源节点 N_s 上计算数据分组的过程如下:

(1) 令消息 *m*=(*DATA*,*option*),其中,*DATA* 为真正的数据项;*option* 为可选项,可包含可达路径、缺失数据分组的序号等,另外,还可能包含使分组达到定长的填充部分;

(2) 计算 $C=\varepsilon_{sc}(m)$,令 $M=(N_R,RBF,C)$;

(3) 计算数据分组 *Packet*=(*M*,*sig*),其中,*sig* 为 N_s 使用 x_R 对 *M* 进行的签名(基于 Π_{sig} 方案).

中间节点 N_i 可利用与下一跳节点间的共享密钥对数据分组进行混淆操作;通过 N_R 验证报文的重复性,使用 Bloom Filter 数据结构保存 N_R,以节省查询时间和存储空间.

3 匿名性分析

UC[9]安全模型描述了网络协议安全性分析的一般方法,本文遵照其框架来分析文中组播路由协议.

引理 1. 洋葱加密 Π_{List} 是 IND-CPA 安全的.即下列实验中,敌手非随机猜测而成功的概率可以忽略.

(1) 敌手以挑战公钥 *PK* 与节点名称 *N* 作为输入.

(2) 敌手选择任意的输入访问 Π_{List} 中的 *EncOnion*.

(3) 敌手选择消息 *m*,*j* 个节点及 $(N_i,x_i)(1\le i<j)$ 提交给挑战者.挑战者令 $(N_j,x_j)=(N,x)$,选择 $b\leftarrow_R\{0,1\}$.

a) 若 *b*=0,则计算 $EncOnion(m,PK,(N_1,x_1),\ldots,(N_j,x_j))\rightarrow(RList_1,\ldots,RList_j)$;

b) 若 *b*=1,则选择随机数 *r*,计算 $EncOnion(r,PK,(N_j,x_j))\rightarrow RList_j$.输出 $RList_j$.

© 中国科学院软件研究所 http://www.jos.org.cn

(4) 与步骤(2)相同.

(5) 敌手输出 b',若 $b'=b$,则敌手在实验中获胜.

在中继数据分组时的混淆操作、伪数据分组和随机序发送,可使窃听者不能获得进入与离开节点的数据分组的关系(将此功能称为中继混淆 F_{fwd}).假设 APM 中数据分组中继时进行的混淆等操作实现了 F_{fwd}.

3.1 理想过程

定义 4(加入通告的理想过程 F_{Join}). F_{Join} 具有安全参数 κ、参与节点 $P_1,\ldots,P_n$、敌手 S 时,执行下列指令.

F_{Join} 的内部数据结构:被攻陷节点集合 Bad;被窃听节点集合 $Ead(Ead\cap Bad=\varnothing$,即它们无交集);以 gID 为标识的组成员集合 Grp;节点 P_i 的路径集合 B_i,B_i 中记录项结构为 $(sid,P_s,P_{j_1},P_{j_2},\ldots,P_i)$,sid 是会话标识,P_s 是源节点,P_{j_1} 与 P_{j_2} 等是路径上的中间节点.文中的符号"→"表示消息由左至右流动,"∧"为逻辑与,"∨"为逻辑或,$NB_A(P_i)$为 P_i 邻居集合,$NB_H(P_i)$为 P_i 未被攻陷(诚实)的邻居集合.

(1) P_s:$(Join,sid,P_s,gID)\rightarrow F_{Join}$,即源节点 P_s 发出会话请求,若$(sid,\ldots)\notin B_s$,F_{Join} 开始执行,记录(sid,P_s)到 B_s.

a) $^{(*)}P_i\notin Bad$,则 F_{Join}:$(Join,sid,P_i)\rightarrow NB_H(P_i)$.

b) $^{(\#)}P_j\in NB_H(P_i)$:$(sid,P_i,P_j,ok)\rightarrow F_{Join}$,若$(sid,\ldots)\notin B_j\vee P_j\in Grp$,则 F_{Join} 取 B_i 的首记录$(sid,P_s,\ldots,P_i)$,保存$(sid,P_s,\ldots,P_i,P_j)$到 B_j,并以 P_j 代替 P_i 执行$^{(*)}$.

执行结束时,对 $P_d\in Grp\wedge(P_d\neq P_s)$,$F_{Join}$:$B_d\rightarrow P_d$;若 $Grp\cap Bad=\varnothing$,则 F_{Join} 按路径选取规则 $\mathfrak{R}$ 从 B_d 中计算得到数据传输路径,并发送给 P_d.

(2) 执行$^{(*)}$时,若 $P_i\notin Bad\wedge P_x\in(NB_A(P_i)-NB_H(P_i))$,则 F_{Join}:$(Join,sid,P_i)\rightarrow S$.在$^{(\#)}$中,若 $P_x\in(NB_A(P_i)-NB_H(P_i))$ 且 $P_i\notin Bad\vee P_i\in Grp$,$S$: $(sid,P_i,P'_{y_1},P'_{y_2},\ldots,P_y,P_j,ok)\rightarrow F_{Join}$,其中,$P_y\in Bad\wedge(P_j\notin Bad\vee P_j\in Grp)$;若$(sid,\ldots)\notin B_j\vee P_j\in Grp$,则 F_{Join} 取 B_i 首记录$(sid,P_s,\ldots,P_i)$,得到 $Path=(sid,P_s,\ldots,P_i,P'_{y_1},P'_{y_2},\ldots,P_y,P_j)$,保存 $Path$ 到 B_j;P_i 与 P_y 之间可能存在连续多个被攻陷的节点 P'_{y_i} .

(3) 执行$^{(*)}$时,若 $P_x\in Ead\wedge P_x\in NB_A(P_i)$,则 F_{Join} 将$(Join,sid,P_i)$与$(Join,sid,P_x)$发送给 S.

(4) 若 $Grp\cap Bad\neq\varnothing$.由 S 决定组内各成员间的路径.

F_{Join} 是 APM 中加入通告过程在理想环境下的实现,它隐藏了源与目的节点,并保持距离私密.F_{Join} 在$(Join,sid,P_s,gID)$发生时未通知 S,是对局部窃听与入侵的建模,局部攻击可获得本地事件的时序,但不能判断出系统中转发事件的最早发生时间.给 S 发送$(Join,sid,P_i)$,建模了窃听与入侵可获取部分网络拓扑信息,这与文献[10]中攻陷路由器获得上下游路径节点类似.由部分事件的时序 S 能够判断相应中间节点到源节点距离的相对值,但不能获得绝对值.即使在理想过程中,当路径穿越被攻陷节点区域时,敌手 S 可以完全控制此部分路径的构成,F_{Join} 将 S 提供的路径当作完整路径的一部分来建模这种情况.当组成员节点被攻陷时,S 可以获知源节点,协议的匿名性不再被保证,因而允许由 S 生成路径.

定义 5(数据交换的理想过程 $F_{Achannel}$). $F_{Achannel}$ 在具有安全参数 κ、参与节点 $P_1,\ldots,P_n$、敌手 S 的情况下执行指令.

$F_{Achannel}$ 的内部数据结构:Bad,Ead,Grp 的含义同定义 4.所用符号同定义 4.

(1) 给定源路由.P_s:$(Gossip,sid,P_s,P,gID)\rightarrow F_{Achannel}$,其中,$P$ 为组播路径,P 到每个端节点的路径上至少有一个诚实节点(包括源与目的节点).若 $P_s\notin Bad$,则 $F_{Achannel}$:$(sid,P',NR)\rightarrow S$,其中,P'为 S 知晓的路径,包括被攻陷节点本身与非法路径部分;NR 为 P'中节点的上、下游诚实节点.

(2) 在 $P_s\notin Bad$ 的情况下.P_s:$(Send,sid,m)\rightarrow F_{Achannel}$,$F_{Achannel}$ 选取与 m 等长的随机数 m_R 作为消息标识,若 $Grp\cap Bad\neq\varnothing$,则 $m_R=m$.

对于 $P_x\in(P-P')\wedge P_{x-1}\in(P-P')$($P_{x-1}$ 为 P_x 上游节点),$F_{Achannel}$ 进行内部计算,若 $P_x\in Grp$,则 $F_{Achannel}$:$(Received,sid,P_s,P_x,m)\rightarrow P_x$.

对于 $P_x\in P'\wedge P_{x-1}\in(P-P')$,$F_{Achannel}$ 分两种情况处理:

a) 若从 P_x 到 $P_d\in Grp$ 的路径上不再有诚实节点(目的节点也被攻陷),则 $F_{Achannel}$:$(Received,sid,P_s,P_d,m)\rightarrow S$.

© 中国科学院软件研究所 http://www.jos.org.cn

b) 若存在诚实节点,则 $F_{Achannel}$: $(Route, sid, P_{x-1}, P_x, P_{x+1}^1, P_{x+1}^2, ..., m_R) \rightarrow S$,其中,$P_{x-1}$ 为 P_x 的上游节点,P_{x+1} 为 P_x 的下游节点.

S 可能返回消息,即 S: $(Foward, sid, P_{x-1}, P_x, (P_{i-1}^1, P_i^1), (P_{i-1}^2, P_i^2), ..., m_R) \rightarrow F_{Achannel}$,其中,$(P_{i-1}^j, P_i^j)$ 为上下游节点对,表示由诚实节点 P_{x-1} 转发给被攻陷节点 P_x 的消息经过 S 处理后,再从被攻陷节点 P_{i-1}^j 路由到诚实节点 P_i^j.

(3) 在 $P_s \in Bad$ 的情况下.S:$(Send, sid, m) \rightarrow F_{Achannel}$.

对于 $P_x \in P' \wedge (P_{x+1}^1, P_{x+1}^2, ... \in (P-P'))$ (其中,P_{x+1}^j 为 P_x 的下游节点),S 可能发送消息给 $F_{Achannel}$,即 S: $(Foward, sid, P_x, P_{x+1}^1, P_{x+1}^2, ..., m) \rightarrow F_{Achannel}$.若 $P_{x+1}^j \in Grp$,则 $F_{Achannel}$: $(Received, sid, P_s, P_{x+1}^j, m) \rightarrow P_{x+1}^j$.

对于 $P_x \in (P-P') \wedge (P_{x+1}^1, P_{x+1}^2, ... \in (P-P'))$,$F_{Achannel}$ 进行内部计算.若 $P_{x+1}^j \in Grp$,则

$$F_{Achannel}: (Received, sid, P_s, P_{x+1}^j, m) \rightarrow P_{x+1}^j.$$

(4) $((P_x \notin P \wedge P_x \in Bad) \vee P_x \in Ead) \wedge (Grp \cap Bad = \varnothing)$,则 $F_{Achannel}$:$(NB_H(P_x), P_x, |m|) \rightarrow S$,$|m|$为与 m 等长的随机数.

$P_x \in Ead \wedge (Grp \cap Bad = \varnothing)$,$F_{Achannel}$:$(P_x, NB_H(P_x), |m|) \rightarrow S$.

3.2 APM的匿名性

定理 1. APM 中的加入通告协议π在(F_{SC}, F_{RKR})-混合模型中是匿名的.

证明:设运行于(F_{SC}, F_{RKR})-混合模型中的加入通告协议π的攻击者为A,我们构造 F_{Join} 的攻击者 S,S 运行一个模拟的 A.与文献[10]的证明思路一样,S 将 A 与 Z 当作一个黑盒进行访问,与 F_{Join} 交互时执行理想中被攻陷节点的功能,与 A 及 Z 交互时执行真实环境中诚实节点的功能.模拟的目的是证明无法区分环境 Z 是与 F_{Join} 中的 S 交互还是与 A 及在(F_{SC}, F_{RKR})-混合模型中运行π的网络节点交互.

S 维护两个数据结构:参数表 $List_c$,用于向 A 发送加入通告;消息链表 $List_{Join}$,用于向 F_{Join} 发送消息.S 模拟 F_{RKR} 为所有的诚实节点生成密钥对,并将公钥发送给 A,并接收 A 发送的被攻陷节点的公钥.

S 首次收到 F_{Join} 消息$(Join, sid, P_i)$时,若 $Grp \cap Bad = \varnothing$,则随机生成$(seq, x_{seq})$、一次性密钥对$(R_{PK}, R_{SK})$,以随机数输入 F_{SC} 中$\varepsilon_{sc}(\cdot)$得到的 C_1 作为$\varepsilon_{sc}(x_{seq}, K_t, N_s)$,保存$(sid, seq, x_{seq}, R_{PK}, R_{SK}, C_1)$到 $List_c$ 中.

S 窃听时.若 $P_x \in Ead \wedge P_i \notin Bad \wedge (Grp \cap Bad = \varnothing) \wedge (F_{Join}:(Join, sid, P_i) \rightarrow S)$,则 S 使用两个随机数与 N_i 组成的 C_2 作为 $RList$,以 sid 查找 $List_c$ 得到$(sid, seq, x_{seq}, R_{PK}, R_{SK}, C_1)$,将 $Join, seq, R_{PK}, C_1$ 与 C_2 组成π中的加入通告消息 m.S: $(N_i, N_x, m) \rightarrow A$,即 S 模拟 N_x(对应 F_{Join} 中的 P_x)收到 N_i 转发的加入通告.S 选择 C_2',形成加入通告消息 m',S: $(N_x, m') \rightarrow A$,即 S 模拟 N_x 转发加入通告.

在 $Grp \cap Bad = \varnothing$的情况下.若 $P_x \in Bad \wedge P_i \notin Bad \wedge (F_{Join}:(Join, sid, P_i) \rightarrow S)$,则与窃听相同,即 S:$(N_i, N_x, m) \rightarrow A$,并保存$(sid, N_i, N_x, m)$到 $List_{Join}$ 中.设从 P_x 到 P_y 路径上的节点都被攻陷,N_y 转发到 $N_j \notin Bad$ 的加入通告 m'由 A 发送到 S.S 以 m'中的 seq, PK_t 与$\varepsilon_{sc}(x_{seq}, SK_t, N_s)$查找 $List_c$ 得到 R_{SK} 与 x_{seq},按照π协议使用 R_{SK} 处理 $RList$ 获得 A 加入的路由序列$(N_{y_1}', N_{y_2}', ..., N_y)$.$S$ 使用 m'中的 seq, PK_t 及$\varepsilon_{sc}(x_{seq}, SK_t, N_s)$在 $List_{Join}$ 中查找,获得(sid, N_i, N_x, m);从而

$$S: (sid, P_i, P_{y_1}', P_{y_2}', ..., P_y, P_j, ok) \rightarrow F_{Join}.$$

若在 $List_c$ 与 $List_{Join}$ 中未有相应数据项或$(N_{y_1}', N_{y_2}', ..., N_y)$中存在诚实节点,则丢弃此路径$(Abort_{discard})$.

在 $Grp \cap Bad \neq \varnothing$的情况下.$S$ 为诚实节点运行π,对诚实节点的被攻陷邻居发送执行协议π后的消息给 A.

从上述模拟的过程中可知,环境 Z 与 S 交互的输出和与 A 及运行π的节点交互的输出,计算不可区分.二者可能的差别有:其一,A 通过窃听与被攻陷节点,除了获得上一跳节点名称外,它还接收到了上一跳节点发送的包含 $RList$ 的消息 m,与模拟中 S 所给的随机数 C_2 不同,A 有可能从 $RList$ 中判断出其他节点(或随机数)在 $RList$ 中;其二是与 C_1 不同,A 接收到的$\varepsilon_{sc}(x_{seq}, SK_t, N_s)$中含有一次性私有密钥;其三是 A 可能篡改 $RList$,使两者 $Abort_{discard}$ 发生的概率不一致.可如文献[10]构造混合机器来证明不可区分性,本文略去混合机器的构造过程.对于第 1 种情况,Π_{List} 的 IND-CPA 安全性决定了敌手在不能访问解密预言时,判断出一个随机数或节点名称在 m 中不可行,见 Claim 1.对于第 2 种情况,由 F_{SC} 保证私有密钥不可获得且不可区分$\varepsilon_{sc}(x_{seq}, K_t, N_s)$与 C_1.对于最后一种情况,由

CDH 假设与 H_1 抗冲突性保证,其证明与声明 1 相似(略). □

声明 1. 如果存在攻击者 A'在不访问Π_{List} 中解密预言的情况下,能够判断一个节点名称是否在协议π的消息 m 中,那么,存在攻击者 S'破解Π_{List} 的 IND-CPA 安全性.

证明:构造这样的 S',S'的动作与理想过程的敌手 S 相似.不同的是,S'接收Π_{List} 中的公钥 PK 作为挑战公钥,Π_{List} 拥有密钥对(PK,SK).任何对 $EncOnion$ 的访问,S'访问Π_{List} 中的加密预言,并返回Π_{List} 的返回.S'生成随机数 x_{seq} 与 seq,以源节点名称 N_s,seq 与初始 $RList=(R_2,...,R_{H_{\max}},BEGIN)$ 询问Π_{List} 的加密预言,获得返回值 $RList$,以随机数输入 F_{SC} 中$\varepsilon_{sc}(\cdot)$得到 C,让 N_s 发出加入通告[$JOIN$,seq,PK,C,$RList$],其中,PK 作为一次性密钥对中的公钥.任选一条路径 $Path$ 上 3 个相邻节点 N_{x-1},N_x 与 N_{x+1},若 N_{x-1},N_x 与 N_{x+1} 中有被攻陷者或 $Grp\cap Bad\neq\varnothing$,则 S'输出 $b'\leftarrow_R\{0,1\}$,停止模拟;否则,对于 $Path$ 中的诚实节点,以其节点名称与上一跳的 $RList$ 作为输入询问Π_{List} 中的加密预言,得到返回值 $RList$ 并修改加入通告.对于 $Path$ 中的被攻陷节点,将加入通告发送给 A'.对于(N_{x-1},N_x,N_{x+1}),S'将(N_{x-1},(N_x,R),N_{x+1})及 N_{x-2} 的 $RList$ 输入Π_{List},其中,R 为随机数,(N_x,R)作为 S'的测试值,Π_{List} 选取随机值 $b\leftarrow_R\{0,1\}$,若 b=0,选择 N_x 作为节点名称,否则选择 R 作为节点名称,S'获得返回值 $RList$ 并用它修改 N_{x-2} 加入通告中的 $RList$,获得新的加入通告 $Join$.S'继续模拟后续协议的运行过程.若后续的模拟中存在 $P_i\in Bad$,则 S'将 $Join$ 发送给 A',如果 A'返回 N_x,则 S'返回 b'=0;若 A'返回 R,则 S'返回 b'=1.

设 A'成功的概率为 1/2+ε(ε不可忽略),S'正常模拟(即满足假设条件)的概率为 p,不能正常模拟的概率为 1−p.S'未能正常模拟时,$b'=b$ 的概率为 1/2;当 S'正常模拟时, $b'=b$ 的概率为 1/2+ε.因此,S'赢的概率为 1/2+$p\varepsilon$,即具有不可忽略的概率优势 $p\varepsilon$破解Π_{List}. □

定理 2. 若群 G 上的 DDH 假设成立,那么,APM 中的数据交换协议σ在(F_{SC},F_{Join},F_{fwd},F_{sig})-混合模型中是匿名的.

证明:设数据交换协议σ调用理想的 F_{Join} 发现路径,它的攻击者为 A.我们构造 $F_{Achannel}$ 的攻击者 S,S 运行一个模拟的 A,并为 A 运行协议σ,从而使环境 Z 无法区分它是与 $F_{Achannel}$ 中的 S 交互还是与 A 及在(F_{SC},F_{Join},F_{fwd},F_{sig})-混合模型中运行σ的网络节点 $N_1,N_2,\ldots,N_n$ 交互.$F_{Achannel}$ 中的节点记为 $P_1,P_2,\ldots,P_n$.

S 收到 $F_{Achannel}$ 的消息有:($NB_H(P_x)$,P_x,$|m|$)混淆消息、($Route,sid,P_{x-1},P_x,P_{x+1}^1,P_{x+1}^2,...,m_R$) 路由消息和($Received$,$sid$,$P_s$,$P_d$,$m$)分组到达消息等 3 类,处理如下:

(1) S 收到($NB_H(P_x)$,P_x,$|m|$)时,S 将其改为($NB_H(N_x)$,N_x,$|m'|$)转发给 A($|m'|$是与数据分组等长的随机数),A 进行递交.收到(P_x,$NB_H(P_x)$,$|m|$),S:(N_x,$NB_H(N_x)$,$|m'|$)$\rightarrow A$.模拟的合理性由 F_{fwd} 保证.

(2) 在 $P_s\notin Bad$ 的情况下.若首次收到 ($Route,sid,P_{x-1},P_x,P_{x+1}^1,P_{x+1}^2,...,m_R$) ,$S$ 以 m_R 为密文或在 $Grp\cap Bad\neq\varnothing$时使用组密钥计算 $m_R=\varepsilon_{sc}(m_R)$为密文,并生成随机的 N_R' 作为协议σ中的 N_R;据协议σ中的源路径向量 RBF 的计算方法,将攻陷路径 P'编码到 RBF 中,再选取若干随机数直接编码到 RBF 中;最后据协议σ生成“假”数据分组 $Packet$,保存(sid,m_R,$Packet$)到分组链表 $List_{packet}$ 中,并将 $Packet$ 发送给 A 作为路由到节点 N_x 的数据分组.若 S 非首次收到该消息,可据 sid 与 m_R 从记录 $List_{packet}$ 中查到(sid,m_R,$Packet$),将 $Packet$ 发送给 A.若 S 收到消息($Received$,sid,P_s,P_x,m),使用 sid 与 m 在记录 $List_{packet}$ 中查找,若有,则直接将 $Packet$ 发送给 A,否则按接收到 $Route$ 消息时的方法生成 $Packet$ 并处理.

S 从 A 处接收到的由被攻陷节点 N_x 发送给诚实节点的数据分组 $Packet$ 后,处理如下:

(1) 在 $P_s\notin Bad$ 的情况下.S 首先用 $Packet$ 中的密文 C 查找 $List_{packet}$ 得到 $Packet'$,检查 $Packet$ 与 $Packet'$中 N_R 是否相同,若不同,则停止模拟($Abort_{inconsistent}$);否则,S 据协议σ中 RBF 的算法,分析 $Packet$ 中 RBF,找出从 P_x 开始的后续各条路径上的诚实节点 ($P_i^1,P_i^2,...$) ,取 $Packet$ 中的密文 C 作为 m_R,

$$S:(Foward,sid,P_{x-1},P_x,(P_{i-1}^1,P_i^1),(P_{i-1}^2,P_i^2),...,m_R)\rightarrow F_{Achannel}.$$

若 S 计算得到某路径上存在连续多个诚实节点(即 A 伪造了路径),则停止模拟($Abort_{inconsistent}$).

(2) 在 $P_s\in Bad$ 的情况下.若 S 是首次收到此 $Packet$,那么,当存在诚实的组成员节点时,S 解密 $Packet$ 中密文获得 m,否则直接使用 $Packet$ 中的密文作为 m;S 生成随机的 sid 并向 $F_{Achannel}$ 发送($Send$,sid,m)消息.对 A 发送的

Packet,*S* 按照上述步骤(1)中的方法生成消息 $(Foward, sid, P_{x-1}, P_x, (P_{i-1}^1, P_i^1), (P_{i-1}^2, P_i^2), ..., m)$,并向 $F_{Achannel}$ 发送,其中,*m* 的计算与首次处理 *Packet* 分组时相同.

由上述模拟过程中可知,环境 *Z* 与 *S* 交互的输出和与 *A* 及运行 π 的节点交互的输出,计算不可区分.二者可能的差别有:一是实际协议 σ 中的 *A* 攻陷一个节点,除了获得上一跳节点名称外,它接收到的上一跳节点发送的数据分组中的 *RBF* 与 *S* 中所模拟的 *RBF* 不同,*A* 有可能从其中判断出其他节点在 *RBF* 中;二是 *A* 攻陷节点接收到的密文 *C* 与随机数 m_R 不同,*A* 有可能将不同的密文联系起来;三是 *A* 伪造路由,使二者 $Abort_{inconsistent}$ 发生概率不同.对于其二,由 F_{SC} 保证 *A* 不能判断真实数据与随机数的差别;对于第 3 种情况,由 F_{sig} 保证在未知 N_R 秘密数的情况下 *A* 成功修改 *RBF* 的概率可以忽略(略);对于第 1 种情况,我们断言在 DDH 假设成立的情况下,*A* 不能判断出是一个随机数还是一个节点名称包含在 *RBF* 中.这由下面的声明 2 保证. □

声明 2. 如果存在攻击者 *A′*能够判断与被攻陷路径节点不相邻的诚实节点的节点名称是否在协议 σ 的 *RBF* 中,那么存在算法 *D* 破解群 *G* 上的 DDH 假设.

证明:证明思路与声明 1 相似,略. □

对于数据交换所获得的路径以及利用它进行传输的匿名性证明,可通过合成理论进行.

4 性能仿真实验

4.1 模拟环境

在本文的模拟实验中,在 Gossip 时选取的出度参数 *F*=3,重复次数参数 τ_q=2.采用文献[18]中的混合加密方案,它使用了椭圆曲线密码体制,实验中,公钥长度为 160 比特,对称密钥长度为 128 比特.节点名称为 160 比特,*seq* 序列号为 128 位,最大步跳数设为 10.数据传输报文中,源路由编码向量 *RBF* 长度为 45 字节,对 3 条长度为 6 的独立路径同时进行组播传输,当散列函数个数取 10 时,其错判的概率小于万分之三.

模拟平台为 2.27 版的 ns-2,模拟 50 个节点放入 1200m×1200m 的区域中.节点传输范围是 250m,信道传输速率为 2Mb/s.采用节点随机移动模型,节点以 1~30m/s 的速度移动,平均停留时间为 0,10,20,40 秒.网络中一个组成员节点以 CBR 方式产生数据流,每秒产生 4 个数据分组,每个分组有效载荷大小为 256 个字节.使用 IEEE 802.11 的媒体访问控制协议.每次仿真运行 360s,结果是多次运行的平均值,运行场景文件由 ns-2 产生.

4.2 结果及分析

图 1 是在不同运动速度时,数据分组的平均递交率.图中的多个曲线是当节点拥有不同的停留时间时的数据递交率.由图中可以看出,APM 具有高的分组递交率,实现了可靠组播.不同的停留时间对数据递交率的影响并不明显.当运动速度适度地逐渐加大时,分组的递交率反而有所增大,但当节点的运动速度进一步加大时,分组的递交率则下降.

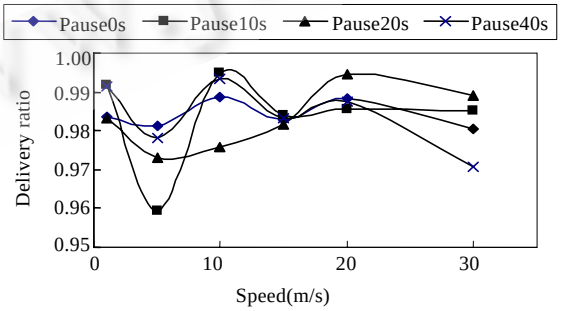

Fig.1 Packet delivery ratio

图 1 数据递交率

图 2 是在不同运动速度时,数据分组的平均扩散时延.平均扩散时延是指数据分组从产生到传输到各个成

员节点所用时间的平均值,未接收到分组的节点不参与统计.匿名组播的平均扩散时延在几种运动速度下都在 5s 附近波动.不同的停留时间对数据递交率的影响并不明显,当节点停留时间进一步加大时,数据分组的平均扩散时延有加大的趋势.当节点的运动速度进一步加大时,平均扩散时延也有加大的趋势.

图 3 中用文献[17]中的标准 RDG 协议作为比较对象,使用它是因为它有较好的组播性能,可用于较大规模的自组网,并与本文 APM 协议的 Gossip 策略相近.图 3 是节点停留时间为 40s 时,不同运动速度情况下的分组递交率.该图中表示 100 个节点在 1000m×1000m 的区域中运行,其中组成员节点的个数为 50.从图 3 可以看出,本协议传输可靠性与 RDG 相比有很大提高,这是由于每次 Gossip 时采用组播方式进行,而不是 RDG 的单点 Gossip,提高了 Gossip 消息的扩散效率.

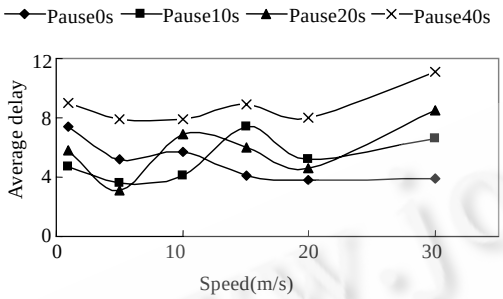

Fig.2 Average delay

图 2 扩散时延

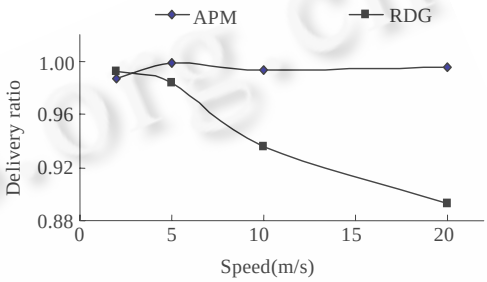

Fig.3 Packet delivery ratio

图 3 数据递交率

5 结 论

本文研究了 MANET 组播匿名通信技术,提出了一种组播匿名通信协议 APM,它抗静态局部的窃听与入侵敌手跟踪数据分组,解匿通信者.设计中采用一次性密钥对保持加入通告过程的路由记录私密与完整,采用 Gossip 机制、DH 秘密路径及 Bloom Filter 编码完成数据分组的匿名交换.随后,通过模拟理想过程来分析 APM 的匿名性.最后对 APM 的性能进行了仿真,通过仿真与分析得知:APM 在实现匿名性的同时,提供了较好的可靠性.

References:

[1] Kong J, Hong X. ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In: Proc. of the 4th ACM Int'l Symp. on Mobile Ad Hoc Networking and Computing. Annapolis: ACM Press, 2003. 291−302.

[2] Zhu B, Wan ZG, Kankanhalli MS, Bao F, Deng RH. Anonymous secure routing in mobile ad-hoc networks. In: Proc. of the 29th Annual IEEE Int'l Conf. on Local Computer Networks. Tampa: IEEE Computer Society, 2004. 102−108.

[3] Song RG, Korba L, Yee G. AnonDSR: Efficient anonymous dynamic source routing for mobile ad-hoc networks. In: Proc. of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks. 2005. 33−42.

[4] Zhang Y, Liu W, Lou W. MASK: Anonymous on-demand routing in mobile ad hoc networks. IEEE Trans. on Wireless Communication, 2006,5(9):2376−2385.

[5] Chandra R, Ramasubramanian V, Birman K. Anonymous gossip: Improving multicast reliability in mobile ad-hoc networks. In: Proc. of the 21st Int'l Conf. on Distributed Computing Systems. 2001. 275−283.

[6] Perng G, Reiter MK, Wang CX. M2: Multicasting mixes for efficient and anonymous communication. In: Proc. of the 26th IEEE Conf. on Distributed Computing Systems. IEEE Computer Society, 2006. 59−59.

[7] Wang JL, Wu QH, Chen DR, Wang YM. A survey on the technology of anonymity. Journal on Communications, 2005,26(2): 112−118 (in Chinese with English abstract).

[8] Wikstrom D. A universally composable mix-net. In: Proc. of the Theory of Cryptography Conf. LNCS 2951, Springer-Verlag, 2004. 317−335.

[9] Canetti R. Universally composable security: A new paradigm for cryptographic protocols. In: Proc. of the IEEE Symp. on Foundations of Computer Science. IEEE Press, 2001. 136−145.

[10] Camenisch J, Lysyanskaya A. A formal treatment of onion routing. In: Proc. of the Crypto 2005. LNCS 3621, 2005. 169−187.

[11] Burmester M, van Le T, de Medeiros B. Provably secure ubiquitous systems: Universally composable RFID authentication protocols. 2006. http://eprint.iacr.org/2006/131

[12] Ateniese G, Camenisch J, de Medeiros B. Untraceable RFID tags via insubvertible encryption. In: Proc. of the ACM Conf. on Computer and Communication Security. ACM Press, 2005. 92−101.

[13] Lee SJ, Gerla M, Chiang CC. On-Demand multicast routing protocol. In: Proc. of the IEEE Wireless Communications and Networking Conf. 1999. 1298−1302.

[14] Ji LS, Corson MS. Differential destination multicast—A MANET multicast routing protocol for small groups. In: Proc. of the INFOCOM 2001. 2001. 1192−1201.

[15] Floyd S, Jacobson V, Liu CG, McCanne S, Zhang L. A reliable multicast framework for light-weight sessions and application level framing. IEEE/ACM Trans. on Networking, 1997,5(6):784−893.

[16] Eugster P, Handurukande S, Guerraoui R, Kermarrec AM, Kouznetsov P. Lightweight probabilistic broadcast. In: Proc. of the IEEE Int'l Conf. on Dependable Systems and Networks. 2001. 443−452.

[17] Luo J, Eugster PT, Hubaux JP. Route driven gossip: Probabilistic reliable multicast in ad hoc networks. In: Proc. of the INFOCOM 2003. 2003. 2229−2239.

[18] Boneh D, Franklin M. Identity based encryption from the weil pairing. SIAM Journal of Computing, 2003,32(3):586−615.

[19] Fujisaki E, Okamoto T. Secure integration of asymmetric and symmetric encryption schemes. In: Proc. of the Advances in Cryptology-Crypto'99. LNCS 1666, Springer-Verlag, 1999. 537−554.

[20] R. Canetti and H. Krawczyk. Universally composable notions of key exchange and secure channels. In: Proc. of the Advances in Crypotology. LNCS 2332, Springer-Verlag, 2002. 337−351.

[21] Abe M, Gennaro R, Kurosawa K, Shoup V. Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM. In: Proc. of the Advances in Crypotology-EUROCRYPT. LNCS 3494, Springer-Verlag, 2005. 128−146.

[22] Goldwasser S, Micali S, Rivest RL. A digital signature scheme secure against adaptive chosen-message attacks. SIAM Journal on Computing, 1988. 281−308.

[23] Katz J, Shin JS. Modeling insider attacks on group key-exchange protocols. In: Proc. of the 12th ACM Conf. on Computer and Communications Security. Alexandria, 2005. 180−189.

[24] Bloom B. Space/time tradeoffs in hash coding with allowable errors. Communications of ACM, 1970,13(7):422−426.

附中文参考文献:

[7] 王继林,伍前红,陈德人,王育民.匿名技术的研究进展.通信学报,2005,26(2):112−118.

章洋(1970－),男,安徽安庆人,博士,主要研究领域为网络安全,分布式计算.