移动 Ad Hoc 网络可认证安全匿名通信研究

周 曜 平 萍 徐 佳 刘凤玉
(南京理工大学计算机科学与技术学院 南京 210094)

摘 要 传统的移动 Ad Hoc 网络匿名路由协议无法鉴别伪造的路由控制分组,并且公钥运算过多导致路由建立时间延长。提出一种基于邻居认证的安全匿名路由协议以解决上述问题,通过基于临时身份公钥的邻居匿名认证机制鉴定邻居节点合法性并动态协商密钥,路由发现过程中利用邻居协商密钥对路由控制消息进行逐跳的验证与处理。上述机制使得伪造路由分组可被有效鉴别,并且中间节点基于对称密钥运算处理分组降低了路由发现时延。理论分析和仿真结果表明,该协议可对抗基于伪造分组的 DoS 攻击,并且较传统协议具有更低的路由建立时间。

关键词 网络安全,移动 Ad Hoc 网络,匿名路由,临时身份公钥,邻居匿名认证
中图法分类号 TP309.7 **文献标识码** A

Research on Anonymous and Authentic Communications in Mobile Ad Hoc Networks

ZHOU Yao PING Ping XU Jia LIU Feng-yu
(School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing 210094, China)

Abstract In traditional anonymous routing protocols in mobile Ad Hoc networks, forged route control packets can't be distinguished and too many public key operations make the route construction delay too long. A new secure anonymous routing protocol based on neighborhood authentications was proposed to solve such problems. By anonymous neighborhood authentications using temporary identity-based public key, shared keys were established between legal neighboring nodes. In anonymous route discovery process, route control packets were hop-by-hop authenticated and hanlded. Such schemes ensure that the forged packets could be efficiently distinguished and nodes en route could handle route control packets by symmetric key operations which decrease the total route discovery delay. Theoretical analysis and simulation results show that this protocol can resist DoS attacks based on forged route control packets and has lower route construction delay than traditional ones.

Keywords Network security, Mobile ad hoc networks, Anonymous routing, Temporary identity-based public key, Anonymous neighborhood authentication

1 引言

移动 Ad Hoc 网络具有通信介质开放、拓扑动态变化、信道与节点资源有限等特性,这使得其在具有组网灵活性的同时,也易遭受对手攻击。尽管传统的加密技术可应用于移动 Ad Hoc 网络中以提供对数据私密性、完整性和可鉴别性等的保护,但对手仍然能够通过对通信内容与传输模式的分析获知节点身份、位置等私密信息,并基于该类信息发起针对性的攻击。对于匿名通信的研究来源于上述安全威胁,并已成为移动 Ad Hoc 网络安全领域研究的热点问题。

有线网络中的匿名通信技术,如 MixNet[1],Onion Routing[2]等,主要采用重路由的方式实现匿名,即由通信路径上的关键节点通过对通信内容的重定向、乱序、混淆、解密/重加密等方式隐蔽通信者身份或盲化通信双方的连接关系。上述技术的实现关键是网络拓扑不变且对通信者可知,因此不能直接应用于拓扑多变的移动 Ad Hoc 网络。对此,Boukerche 等人在文献[3]中首先提出适用于移动 Ad Hoc 网络的动态分布匿名路由协议 SDAR,该协议采用按需路由方式获取中间节点的会话密钥,并基于有线网中的 Onion Routing 技术进行数据转发。随后提出的一些移动 Ad Hoc 网络匿名路由协议,如 ANODR[4],ASR[5],AnonDSR[6],MASK[7]等,多沿袭上述思想,只是在路由发现算法以及数据转发方式上存在差异。

在匿名的网络环境中,难以通过节点身份鉴别其发送分组的合法性,因此在匿名通信中如何提供有效的认证机制是目前研究的难点。基于传统的私钥签名的认证模式虽然可以提供合法性认证,但是在移动 Ad Hoc 网络中上述机制的应用存在局限性:其一,对签名的识别需要知道对方的带证书公钥,由于公钥唯一对应一个节点,会泄漏该节点的身份;其二,对于证书的鉴定与处理会带来比较大的计算开销,对于资源

到稿日期:2008-06-11 本文受国家自然科学基金资助项目(90718021)资助。
周 曜 博士研究生,主要研究方向为信息安全与移动自组织网络,E-mail:zhouyao@mail.njust.edu.cn;平 萍 博士研究生,主要研究方向为元胞自动机与加密技术理论;徐 佳 博士研究生,主要研究方向为拥塞控制与网络管理;刘凤玉 教授,博士生导师,主要研究领域为信息安全、入侵检测、可信软件等。

有限的节点是额外的负担。对于此类问题，目前的移动 Ad Hoc 网络匿名通信技术均未提出很好的解决方案，MASK[7] 中虽然提出基于预分配伪名的匿名认证方案，但其伪名管理成本过高，难以应用于节点资源有限的移动 Ad Hoc 网络。因此产生匿名环境下新的安全隐患，即难以对抗对手发起的基于伪造分组的 DoS 攻击，对于洪泛的路由请求分组，此类安全问题更为严重。

针对上述问题，本文提出一种新的可认证安全匿名路由协议 ANAR。ANAR 采用基于身份的公钥系统[8] 以简化密钥管理过程，公钥来自节点的身份等公开信息，不需公钥目录以及证书。节点利用随机生成的临时公钥隐藏真实公钥，与邻居进行双向匿名认证。在路由发现过程中，利用合法邻居间认证协商密钥，对路由控制分组进行逐跳的验证与处理。上述机制使得伪造路由控制分组可被接收节点有效鉴别，同时也保证了中间节点对于路由分组的处理基于对称密钥运算，较传统基于公钥处理的机制显著降低计算开销。理论分析和仿真实验表明，ANAR 可对抗基于伪造分组的 DoS 攻击，并且具有比传统匿名路由协议更低的路由建立时延。

2 预备知识

ANAR 采用基于身份公钥系统源于双线性对，定义如下[9]：

定义 1（具有密码学意义的双线性对，以下简称双线性对） 设 G_1，G_2 为两个阶同为素数 q 的群，其中 G_1 为加法群，G_2 为乘法群，P 是 G_1 的生成元。假设 G_1，G_2 中的离散对数难解，一个具有密码学意义的双线性对是指具有如下性质的映射 $e:G_1\times G_1\rightarrow G_2$：

· 双线性：对任意的 $P,Q\in G_1$，$a,b\in Z_q^*$（$Z_q^*=\{y\mid 1\leqslant y\leqslant q-1\}$），都有

$$e(a\cdot P,b\cdot Q)=e(P,Q)^{a\cdot b} \tag{1}$$

· 非退化性：对于生成元 P 有：$e(P,P)\neq 1$。

· 可计算性：对任意的 $P,Q\in G_1$，存在有效的算法计算 $e(P,Q)$。

椭圆曲线上的 Tate 对和 Weil 对是目前构造具有密码学意义双线性对所一致采用的途径，具体构造与计算方法可参见文献[9]。

3 协议描述

3.1 系统模型

在网络启动阶段，由可信的授权者 TA 建立基于身份的公钥系统[8]，公开参数 G_1，G_2，q，e 如定义 1 中所给。

系统建立：任选 $s\in Z_q^*$ 以及 G_1 的生成元 P，计算 $P_{pub}=s\cdot P$；s 做系统主密钥，P_{pub} 做系统公钥；选择两个 HASH 函数 $H_1:\{0,1\}^*\rightarrow G_1^*$（$G_1^*$ 表示 G_1 中非零元素集合）；$H_2:G_2\rightarrow\{0,1\}^n$，$n$ 表示明文分组的长度；公开系统参数 $params=(G_1,G_2,q,e,n,P,P_{pub},H_1,H_2)$。

授权用户私钥：对网络中每个节点，给定身份信息 $ID\in\{0,1\}^*$，计算公钥 $PK=H_1(ID)\in G_1^*$，并为其授权用户私钥 $SK=s\cdot PK$。

3.2 邻居安全管理策略

3.2.1 临时公钥与主密钥

节点以随机生成的临时公钥作为相邻节点间通信时的身份伪标识。以节点 A 为例，它的临时公钥按如下方法计算：A 随机选择 $a\in Z_q^*$，计算临时公钥 $TP_A=a\cdot PK_A=a\cdot H_1(ID_A)\in G_1^*$。

定理 1 无法由临时公钥得到真实公钥，且临时公钥的冲突率为 $1/q-1$，q 为 G_1 的阶。

证明：①临时公钥为 G_1 中的点，而 G_1 中的离散对数问题难解，因此无法由临时公钥反向计算出真实公钥。

②G_1 为素数阶循环群，其中任意非零元素均为生成元，所以 $H_1(ID_A)\in G_1^*$ 为 G_1 的生成元。由于 a 随机分布于 Z_q^* 中，因此临时公钥 $TP_A=a\cdot H_1(ID_A)$ 随机分布于 G_1^* 中。因为 G_1 的阶为 q，所以临时公钥的冲突率为 $1/q-1$，证毕。

从定理 1 中可以看出，采用临时公钥可有效隐藏节点的真实公钥，并且由于 G_1 的阶 q 为大素数，临时公钥的冲突率极低。同时定理 1 的证明过程也说明临时公钥随机分布于 G_1^* 中，不同临时公钥之间不具有比较性。

节点为每个临时公钥生成一个 128 位的秘密数作为对应主密钥，通过下文所述邻居匿名认证过程，节点将自己的主密钥秘密传送给合法邻居。在路由请求过程中，节点在广播的 RREQ 分组中包含使用主密钥的签名信息，所有合法邻居均可根据签名验证分组有效性。

3.2.2 HELLO 机制

节点通过本地广播 HELLO 消息提供连接信息。每隔 HELLO_INTERVAL（HELLO 消息周期）时间，节点检查自己在上一个 HELLO_INTERVAL 周期内是否已经发送了一条广播消息，如果检查出没有发送，那么该节点广播一个 $TTL=1$ 的 HELLO 消息，具有如下的消息组成域：

（1）该节点身份伪标识 PID，为该节点的临时公钥。

（2）身份变更标志 $ChangeTag$，0 或 1，设为 1 时表明身份变更，0 表示不变。

（3）欲更新身份（可选）$NewPID$，当变更标志为 1 时，此域包含该节点新生成临时公钥。

（4）寿命。ALLOWED_HELLO_LOSS（允许 HELLO 消息丢失数）×HELLO_INTERVAL。

节点通过接收其相邻节点集发送来的分组来确定连接，并在本地邻居表中记录邻居的身份伪标识。如果在过去的一段长于 ALLOWED_HELLO_LOSS×HELLO_INTERVAL 的时间内没有接收到任何来自该邻居的消息，那么该节点认为到达该邻居的连接已经丢失，并删除邻居表中相应记录。

3.2.3 邻居匿名认证

若节点接收到新邻居的 HELLO 消息，则需对消息中 PID 合法性进行认证，认证过程如下：

（1）假定节点 A 收到节点 B 的该消息，其中的 $PID=TP_B=b\cdot H_1(ID_B)(b\in_R Z_q^*)$。为了对 PID 进行认证，A 生成随机数 n_A，并以自己正在使用的身份伪标识，即临时公钥 $TP_A=a\cdot H_1(ID_A)(a\in_R Z_q^*)$ 计算

$$V_0=H(e(a\cdot SK_A,TP_B)||n_A)$$

其中 $SK_A=s\cdot H_1(ID_A)$ 为 A 的用户私钥，$H(.)$ 为随机 HASH 函数，“||”表示串联。A 向 B 发送一个包含 TP_A 与 n_A 的认证请求消息。

（2）B 接收到该认证请求后，需返回一个应答数 $V_1=H(e(TP_A,b\cdot SK_B)||n_A)$，其中 $SK_B=s\cdot H_1(ID_B)$ 为 B 的用户

私钥。由于

$$e(TP_A, b \cdot SK_B) = e(a \cdot SK_A, TP_B) = e(H_1(ID_A), H_1(ID_B))^{a \cdot b \cdot s} \quad (2)$$

因此 $V_0 = V_1$，并且由于 s 为秘密的系统主密钥，只有拥有用户私钥的合法节点才能返回正确的应答数，因此 A 可通过验证 $V_1 = V_0$ 来确定 B 为处于同一网络的合法节点，也即 PID 为合法的身份伪标识。

(3) B 类似地验证 A 的身份伪标识，即临时公钥 TP_A 的合法性。在双向认证完成后，A，B 分别计算相等的秘密数

$$K_{AB} = H(e(a \cdot SK_A, TP_B)) = H(e(TP_A, b \cdot TP_B))$$

作为邻居共享密钥，并以邻居共享密钥加密各自的主密钥后发送给对方。

节点在邻居表中记录所有通过认证邻居的身份伪标识、邻居共享密钥与主密钥。为了防止窃听者的跟踪行为，节点需定期更新身份伪标识，即临时公钥。当某个节点决定更新身份伪标识时，该节点生成新的临时公钥以及对应主密钥并包含于 HELLO 消息的 $NewPID$ 域中，该域被此节点原主密钥加密并签名，同时设置 $ChangeTag$ 为 1。该节点的邻居接收到此 HELLO 消息后，解密得到新的临时公钥以及对应主密钥，同时更新邻居表中相应记录。由于窃听者不知道该节点的新临时公钥，它无法将该节点在更新身份前后所发送的 HELLO 消息联系起来。

3.3 匿名路由发现

在本节叙述中，以 $S, D, N_i (1 \leqslant i \leqslant k)$ 分别表示源节点、目的节点和路由上的 k 个中间节点，如图 1 所示。所使用运算符号为：$EC_K(.)$，$H_K(.)$ 分别表示使用密钥 K 的对称加密和密码 HASH 函数，$EP_{PK}(.)$ 表示使用密钥 PK 的公钥加密函数。

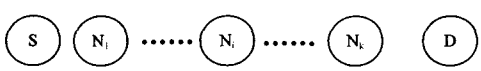

图 1 从源节点 S 到目的节点 D 的路由

3.3.1 路由请求

在路由请求过程中，每个中间节点 $N_i (1 \leqslant i \leqslant k)$ 接收到的 RREQ 消息具有以下格式：

$$\left[Seq, H_{MK_{i-1}}(Seq), EC_{MK_{i-1}}(H(ID_D \| Seq)), EP_{PK_D}(ID_S, K_S, SIG_S), EC_{K_S}(Seq, END) \right]$$

其中，Seq：本次会话序列号；MK_{i-1}：上游节点 N_{i-1} 的主密钥，$H_{MK_{i-1}}(Seq)$ 构成 N_{i-1} 的签名；PK_D：D 的公钥；K_S：本次会话验证密钥；SIG_S：S 的私钥签名；ID_S 和 ID_D：S 和 D 的真实身份；END：目的节点收到路由请求的一个标志数。

一旦接收到 RREQ 分组，每个节点 N_i 首先检查 Seq 是否已存在于路由表中，若是则丢弃分组；否则，用邻居表中记录的邻居主密钥验证分组第二部分有效性，并确定 MK_{i-1}，若邻居表中不存在相应记录，也丢弃分组；若存在，则解密第三部分，用自己的身份和 Seq 生成的 HASH 值与解密结果比较；若不等，N_i 在本地路由表中记录 $Seq, MK_{i-1}, EC_{K_S}(Seq, END)$，用 $H_{MK_i}(Seq), EC_{MK_i}(H(ID_D \| Seq))$ 分别取代分组中第二和第三部分，其中 MK_i 为 N_i 主密钥；最后重新广播改写后的分组。

若相等，说明此节点为目的节点 D，D 用自己私钥解密分组第四部分，根据 ID_S 生成 S 的公钥，验证 S 的签名是否有效，若无效则丢弃分组；否则，D 生成并广播 RREP 消息作为响应。

3.3.2 路由响应

在路由响应过程中，每个中间节点 N_i 接收到的 RREP 分组具有以下格式：

$$\lfloor R_{i+1}, H_{NK_{i+1,i}}(R_{i+1}), EC_{NK_{i,i+1}}(T_{i+1}, Seq, K_S') \rfloor$$

其中，R_{i+1}：下游节点 N_{i+1} 生成的随机数；$NK_{i,i+1}$：N_i 和 N_{i+1} 的邻居共享密钥，由 N_{i+1} 根据路由请求过程中记录的 MK_i 查询本地邻居表得到；T_{i+1}：N_{i+1} 生成的秘密数，作为本次会话中 N_{i+1} 与 N_i 共享临时会话密钥；K_S'：目的节点正确恢复出 RREQ 分组中会话验证密钥的证明。

一旦接收到 RREP 分组，每个节点用邻居表中记录的邻居共享密钥验证分组第二部分有效性，由于 N_{i+1} 和 N_i 的邻居共享密钥在 N_{i+1} 所有邻居中唯一，只有 N_i 可发现正确记录 $NK_{i,i+1}$，因此 N_i 接受分组，其他节点只是简单丢弃。N_i 解密分组第三部分，通过检查

$$EC_{K_S}(Seq, END) = EC_{K_S'}(Seq, END)$$

确认 RREP 来自正确目的节点，若上式不等则丢弃分组。

若相等，N_i 选择随机数 R_i 和 T_i，在路由表里对应 Seq 的记录中添加 T_{i+1} 和 T_i，用 $R_i, H_{NK_{i-1,i}}(R_i), EC_{NK_{i-1,i}}(T_i, Seq, K_S')$ 分别取代 RREP 分组中原对应部分，其中 $NK_{i-1,i}$ 为上游节点 N_{i-1} 和 N_i 的邻居共享密钥，重新广播改写后的分组。

路由响应过程结束后，每个中间节点 N_i 与其上下游节点分别拥有了共享临时会话密钥 T_i 和 T_{i+1}，N_i 的路由表中记录的格式，如图 2 所示。

Seq	MK_{i-1}	T_i	T_{i+1}
160 bits	128 bits	128 bits	128 bits

图 2 中间节点 N_i 路由表记录格式

3.4 匿名数据传输

数据分组格式为：$[DATA, RoutePseum, Payload, Padding]$。其中 $RoutePseum$ 为路由伪名；$Payload$ 为被加密的数据内容；$Padding$ 为每个转发节点附加的随机伪数据，用于对抗内容分析。

数据分组的转发与 ASR[5] 类似，分组中 $RoutePseum$ 域为一个二元组：$(Index, H_{T_{next}}(Index))$，其中 $Index$ 为当前发送节点生成的随机数，在每个分组中保持递增，T_{next} 为当前发送节点与下一跳节点的共享临时会话密钥。每个接收到该数据分组的节点检查路由表中是否有记录可正确验证 $RoutePseum$，若检查到相应记录 T_{next}，它接受分组，以 T_{next} 在路由表中对应项 T_{next}' 生成新的 $RoutePseum$ 并替代原值，将改写后的分组发往下一跳。为了对抗时间分析，每个节点在接收到分组后并不马上转发，而是缓存一部分分组后以乱序方式发送。

4 匿名性与安全性分析

4.1 匿名性分析

在 ANAR 的邻居信息交换中，与节点身份有关的公开信息是该节点的临时公钥，根据 3.2.1 节定理 1，临时公钥不可识别且不可比较，窃听者无法根据临时公钥获知节点身份以及移动路径。

在路由发现以及数据转发过程中，所有分组均不包含明

文的节点身份，窃听者无法从通信内容得知通信双方身份。RREQ 和 RREP 分组用邻居间密钥生成的 MAC 值标识，而非使用公开的临时公钥，窃听者无法识别，并且标识中包含变化的序列号或随机数，无法判断不同分组来自或发往同一节点。除了洪泛的 RREQ 分组，其他分组的内容都经过逐跳的混淆与加密，节点接收与发送的分组在内容及时间上没有任何关联关系，窃听者无法通过流量分析发现分组传输路径。

ANAR 较传统协议具有更好的匿名性。在传统协议中，RREQ 分组中目的节点身份被其公钥加密，若对手同时掌握目的节点身份与公钥，它可通过比较加密内容的异同来推知目的节点。在 ANAR 中，RREQ 分组中目的节点身份信息被每个转发节点的主密钥加密，对对手不可见，因此无从比较。

4.2 邻居匿名认证的安全性

ANAR 的邻居匿名认证机制是协议实现的关键，其算法安全性基于以下双线性计算 Deffie-Helleman(BDH)问题[9]的困难性：

定义 2(BDH 问题) 设 G_1，G_2 为两个阶同为大素数 q 的循环群，$e: G_1 \times G_1 \rightarrow G_2$ 为一个双线性映射，P 为 G_1 的生成元。则 (G_1, G_2, e) 上的双线性计算 Diffie-Hellman (BDH)问题是：给定 $P_1 = x \cdot P, P_2 = y \cdot P, P_3 = z \cdot P$，其中 $x, y, z \in_R Z_q^*$，由 (P_1, P_2, P_3) 计算 $e(P,P)^{x \cdot y \cdot z}$。

定理 2 非法节点无法通过 ANAR 中的邻居匿名认证。

证明：(以下所使用符号同本文 3.2.3 节内容)反证法。考虑 3.2.3 节的邻居认证过程，若 B 为非法节点，则它通过 A 的认证意味着它在认证过程中返回了正确的应答数 V_1。由于 A 对 V_1 的验证基于 A 计算的秘密数 $T_A = e(a \cdot SK_A, TP_B)$，因此 B 可以通过认证意味着存在多项式时间的算法 F，使得 B 可根据公开信息，即双方交换的临时公钥 TP_A，TP_B 以及系统公开参数 $params$ 有效计算出 T_A，即

$$F(params, TP_A, TP_B) = T_A \tag{3}$$

因为

$$T_A = e(a \cdot SK_A, TP_B) = e(s \cdot TP_A, TP_B) \tag{4}$$

所以

$$F(params, TP_A, TP_B) = e(s \cdot TP_A, TP_B) \tag{5}$$

假设存在上述算法 F，则可利用 F 解决 BDH 问题，方法是：以 P_1 作为 F 的输入 $params$ 中的系统公钥 P_{pub}，$params$ 的其他部分不变；以 P_2，P_3 分别作为 F 输入中的 TP_A，TP_B，调用 F 得到输出 e_0。注意此时系统公钥 $P_{pub} = x \cdot P$，因此原系统主密钥 s 此时为 x，根据(4)式有

$$e_0 = e(x \cdot P_2, P_3) = e(x \cdot y \cdot P, z \cdot P) = e(P,P)^{x \cdot y \cdot z}$$

易见 e_0 即 BDH 问题的解，也就是说，若存在上述算法 F，则 BDH 问题不再是困难的，产生矛盾。故不存在上述算法，也即非法节点无法通过邻居匿名认证，证毕。

4.3 DoS 攻击

根据攻击目标的不同，匿名环境下 DoS 攻击可分为两类：多对一攻击与一对多攻击。对于前者，由于 ANAR 满足身份与位置匿名，对手无法定位目标发起攻击；对于后者，由于每个转发节点需进行加解密运算以处理 RREQ 或 RREP 分组，常见攻击方式是发送伪造路由控制分组以耗尽转发节点计算资源。ANAR 可有效对抗此类攻击，第一：对 RREQ 分组逐跳验证有效性，由于非法节点无法通过邻居匿名认证过程获得相邻合法节点的主密钥，伪造分组中当前发送节点签名域将不能通过接收节点验证，分组被丢弃；第二：即使对手在伪造 RREQ 分组中包含它所监听到的合法分组中的上述签名，由于签名基于分组序列号，而重复序列号的分组被丢弃，此类重放攻击亦无效；第三：RREP 分组中所包含会话验证密钥被逐跳验证，攻击者不知道正确密钥，伪造分组无法通过验证。由于 ANAR 通过邻居认证机制在邻居间动态协商共享密钥，节点执行上述验证操作时只需执行简单的查表操作与对称密钥运算。

现有移动 Ad Hoc 网络匿名路由协议对于伪造 RREQ 消息未提供有效鉴别机制，对手可伪造 RREQ 分组发起资源耗尽类 DoS 攻击，由于 RREQ 消息的传播方式为网络洪泛，此类攻击可造成全网的性能衰退甚至瘫痪。在此方面，ANAR 具有更好的安全性。

4.4 路径劫持

ANAR 协议可以防止路径劫持，只有当可信赖的目的节点收到 RREQ 分组后，才触发路径响应过程；只有当源节点收到 RREP 分组后，数据传送阶段才开始进行。若非法节点只在它们之间传送 RREQ 分组，RREQ 分组将不会到达目的节点，也不会触发路径响应过程的进行，源节点同样不会收到 RREP 分组，此情况下，其它的未经过非法节点的 RREQ 分组也可能传送到目的节点，而完成路由发现过程。另一方面，若非法节点停止这种循环传送，而传送 RREQ 分组到一个合法节点，进而完成路由发现过程，尽管该路径经过了一些非法节点，但由于协议本身的安全和匿名特性，也不会影响到数据传送的安全性和匿名性。

4.5 虫洞攻击

虫洞攻击是攻击者在一个节点获取报文分组后，用隧道的方式传到另一个节点。虫洞形成后，攻击者可进行选择性通过之类被动攻击行为，也可与其他方法结合分割控制网络。ANAR 可有效对抗虫洞攻击：虫洞的形成需要非法节点参与到路由发现过程中，但 ANAR 的路由发现机制确保非法节点发送的 RREQ 或 RREP 分组无法通过相邻节点验证，非法节点无法参与路由发现而不能形成虫洞。

5 仿真实验与性能分析

5.1 仿真设定

为了检验 ANAR 的正确性并分析性能，使用网络模拟软件 NS2[10] 对其进行仿真，并将仿真结果同 ANODR[4] 和 SDAR[3] 进行比较，后两者在路由发现过程中使用公钥对控制消息进行加密。

在仿真中，3 种协议节点身份标识均为 128 位，随机数长度为 64 位，HASH 函数输出为 128 位，数据传输过程中通过附加伪数据 *Padding* 固定数据分组长度为 512 字节。为简单起见，不考虑网络启动阶段开销，也不考虑网络攻击行为；对于断裂链路，仅重新发起路由发现而不考虑路由修复。

不同的加密算法会导致不同的计算时延，为便于比较，假设 3 种协议的公钥体系均为基于身份公钥系统，且系统参数相同。由于基于身份的公钥体系更为适合无基础架构的 Ad Hoc 网络[12]，该假设有实际意义。公钥长度均为 160 位，双线性对设为椭圆曲线上 TATE 对，基于身份的加密与签名算法分别为 IBE[8] 算法和 BLS[11] 算法，计算时间采用文献[12]中对于移动终端的实测数据：IBE 加、解密分别为 35ms 和

27ms;BLS 签名与验证时间分别为 2.22ms 和 45.8ms。

网络场景设置为:采用 1000m×1000m 的区域面积,网络中的节点数目为 150,传输半径均为 200m,带宽为 2Mbps,MAC 协议为 IEEE802.11,无线传播模型为 Two Ray Ground,应用层流量类型为 CBR(以固定速率发送固定长度的分组),每个分组大小为 512 字节,连接数为 10,节点每秒发送 10 个分组,节点移动模型采用 Ramdom Way Point 模型,移动速度在 0～10m/s 之间变化。每次仿真时间为 900 秒,所有数据均为 5 次仿真平均值。

5.2 结果与分析

图 3 表示 3 种协议的分组投递率(目的节点接收数据分组数量/源节点发送数据分组数量)。在 8 个取样点,ANAR 的平均数据传输成功率分别比 SDAR 和 ANODR 高 16.6% 和 11.2%。原因是在 ANAR 的路由发现过程中,公钥运算只发生在通信两端,中间节点在交换路由控制分组时使用高效的对称密钥运算,可以有效加速路由发现过程,并使得建立的路由更为持久;在 ANODR 和 SDAR 中,RREQ 分组中目的节点身份被其公钥加密,路由请求过程中每个中间节点都需执行私钥解密以进行目的节点判断,由于公钥运算带来的计算延迟远大于对称密钥运算,它们的路由发现时延也远高于 ANAR,从而增加了路由建立与维护的难度,使得数据发送失败率加大。

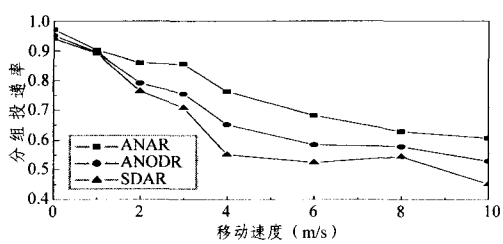

图 3 分组投递率

图 4 显示了不同协议的平均端到端时延(目的节点分组接收时间 − 源节点分组发送时间)。在 8 个取样点,ANAR 的数据传送时延平均值分别为 SDAR 和 ANODR 的 34.3% 与 67.5%。实验结果符合期望,SDAR 表现出最高的传输时延,原因是它以洋葱路由[2]作为匿名数据传送方式,在路由发现以及数据传输过程中,节点为构造"洋葱"需要进行大量密钥运算,显著延长了路由建立和数据传输时间。ANODR 和 ANAR 采用匿名虚电路[4]方式转发数据分组,节点处理分组时所需密钥运算较少,总体传输时延较低;同时,ANAR 基于对称密钥运算处理路由分组,其路由发现时延低于基于公钥的 ANODR。当移动性不高的时候,所有协议显示了低的传输时延,这是因为一旦路由建立完成,一个稳定的网络允许更长的平均路由生存时间。当移动性增加,传输时延也相应增加。

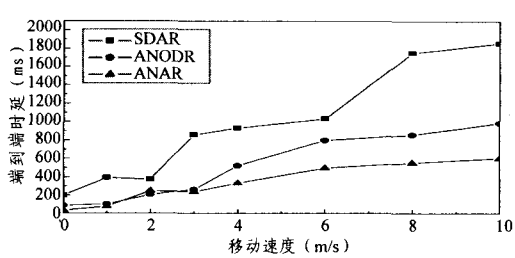

图 4 平均端到端时延

图 5 比较了不同协议的归一化路由开销(控制分组数量/目的节点接收数据分组数量),此处控制分组包括 RREQ,RREP 和 HELLO 分组。在 8 个取样点,ANAR 的控制分组占数据分组比例平均为 9.5%,SDAR 为 8.1%,ANODR 为 7.2%。虽然 ANAR 的邻居管理策略所需 HELLO 消息数量多于 SDAR 和 ANODR,但 ANAR 通过邻居认证协商对称密钥,降低了路由发现时延并进而减少了过期路由数量,因此 ANAR 的一次成功会话所需平均路由发现次数要低于其他二者,故总体路由开销差异并不明显。在实际应用中,还可通过改变 HELLO_INTERVAL 值来调节 ANAR 中 HELLO 消息发送频率,以适应不同的网络繁忙度。

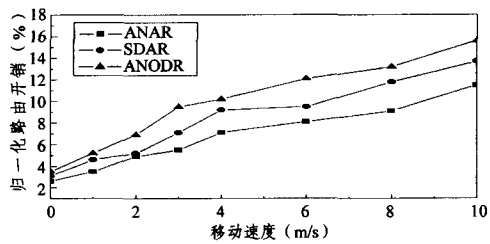

图 5 归一化路由开销

结束语 移动 Ad Hoc 网络的信道开放性和资源有限性决定了匿名路由协议的设计必须考虑安全与成本问题。在传统协议中,网络易遭受伪造路由控制分组的攻击,并且路由建立时间过长。本文提出一种基于邻居认证的安全高效匿名路由协议,通过基于临时身份公钥的匿名认证机制鉴定相邻节点合法性。在路由发现阶段,路由控制分组被逐跳验证与处理,伪造分组无法通过验证而不会造成危害,并且中间节点基于对称密钥运算处理分组,有效降低了转发时延。在下一步的工作中,将着重于邻居匿名认证算法的优化,进一步降低由此带来的额外通信开销。

参 考 文 献

[1] Berthold O, Federrath H, Kö psell S. Web MIXes: A System for Anonymous and Unobservable Internet Access [C] // Proc. Workshop Design Issues in Anonymity and Unobservability (DIAU '00). 2000: 115-129

[2] Greed M, Syverson P F, Goldschlag D M. Anonymous connections and onion routing[J]. IEEE Journal on Selected Areas in Communications, Special Issue on Copyright and Privacy Protection, 1998, 16(4): 482-494

[3] Boukerche A, El-Khatib K, Xu L, et al. SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks[C]// Proc. 29th IEEE Int'l Conf. Local Computer Networks (LCN '04). 2004: 618-624

[4] Kong J, Hong X, Gerla M. An Identity-Free and On-Demand Routing Scheme against Anonymity Threats in Mobile Ad Hoc Networks[J]. IEEE Transactions on Mobile Computing, 2007, 6(8): 387-409

[5] Zhu B, Wan Z, Kankanhalli M S, et al. Anonymous Secure Routing in Mobile Ad-Hoc Networks[C]// Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks (LCN'04). 2004: 102-108

(下转第 71 页)

样到当前时刻空间对象的最大移动距离为 d，d 值的大小反映了移动对象位置的不确定程度。设空间对象的不确定区间用最近一次采样得到的空间对象的位置为中心、以 d 为半径的圆表示，设对象位置在不确定区间中符合正态分布。试验中对于包含移动对象个数 $N=5000$ 的数据集，针对不同的 d 值，分别采用本文提出的 PDBSCAN 聚类算法和 FDBSCAN 聚类算法(参数取值与文献[7]中相同)对不确定性对象进行聚类，采用 DBSCAN 聚类算法对当前时刻对象的"确定"位置进行聚类，设结果分别表示为 P，F 和 D。由于无法及时知道当前时刻移动对象的准确位置，D 实际上是无法获得的，在试验中只是起基准的作用。P 和 F 中与 D 相似程度越高，说明对不确定性数据聚类的准确度越高。比较两个聚类结果相似程度的指标采用的是广为使用的 Adjusted Rand Index (ARI)[10]。ARI 的值越大，说明两个聚类结果越相似。对于不同 d 值 P 与 D 之间(用 PDBSCAN 标识)、F 与 D 之间(用 FDBSCAN 标识)的 ARI 值如图 3 所示。由图 3 可见，随着 d 值增加，两种算法聚类的结果与理想的对精确数据聚类的结果之间的误差都有所增加，说明数据不确定程度增大导致聚类的准确性下降；对于相同的 d 值，PDBSCAN 聚类算法得到的结果比 FDBSCAN 聚类算法得到的结果更接近理想的实际结果(ARI 值更大)，说明 PDBSCAN 聚类算法的有效性更佳。原因在于 FDBSCAN 聚类算法是通过对数据不确定区域的抽样(离散化)进行计算的，样本数量对计算精度影响很大；而本文提出的 PDBSCAN 聚类算法不存在这样的问题。

为了检验算法的效率，设对象的最大移动距离 $d=25$m，采用 PDBSCAN 聚类算法和 FDBSCAN 聚类算法分别对具有不同移动对象数的数据集进行聚类，比较聚类所需的时间，结果如图 4 所示。从图中可以看出，在运行时间方面对于不同的数据规模采用本文提出的 PDBSCAN 聚类算法明显优于 FDBSCAN 聚类算法。原因在于 FDBSCAN 算法对数据不确定区域离散化带来了额外的时间花销，而 PDBSCAN 算法虽然直接基于不确定性数据在其不确定区域上的概率分布进行计算，但通过 R 树索引和概率阈值索引 PTI 预先对绝大部分不满足要求的对象进行排除，因此提高了聚类过程的效率。

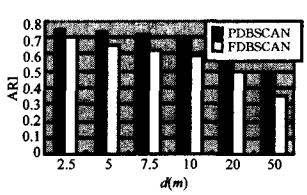

图 3 ARI 与最大移动距离 d 的关系

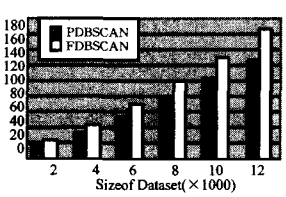

图 4 不同数据集规模所对应的聚类时间

结束语 随着传感器技术和无线通信技术的发展，对面向自然界的应用的需求越来越大，而从自然界采集到的数据内在的不确定性使得不确定性数据处理技术的研究成为当前科研的一个热点。本文分析了当前不确定性数据聚类的主要研究成果，并在此基础上提出基于密度的不确定性数据概率聚类算法 PDBSCAN，根据数据不确定区域的概率分布信息提高算法的准确性并通过 R 树索引和概率阈值索引 PTI 提高算法的效率。仿真试验表明，本文提出的方法在有效性和效率方面均优于当前主要的基于密度的不确定性数据聚类算法。概率阈值 p 的选取对聚类结果的影响有待于下一步的深入研究。

参 考 文 献

[1] Cheng R. Managing Uncertainty in Constantly - evolving Environments[D]. Purdue University, 2005

[2] Cheng R, Kalashnikov D V, Prabhakar S. Evaluating probabilistic queries over imprecise data[C]// The 2003 ACM SIGMOD International Conference on Management of Data. San Diego, 2003

[3] Cheng R, Xia Y, Prabhakar S, et al. Efficient indexing methods for probabilistic threshold queries over uncertain data[C]// The 30th International Conference on Very Large Data Bases. Toronto, 2004

[4] 许华杰，李国徽. 移动计算环境中易变数据的在线广播调度[J]. 计算机科学，2009，36(1)

[5] Dalvi N, Suciu D. Efficient query evaluation on probabilistic databases[C]// The 30th International Conference on Very Large Data Bases. Toronto, 2004

[6] Chau M, Cheng R, Kao B, et al. Uncertain Data Mining: An Example in Clustering Location Data[C]// The 10th Pacific-Asia Conference on Knowledge Discovery and Data Mining. Singapore, 2006

[7] Kriegel H-P, Pfeifle M. Density-based clustering of uncertain data[C]// The 11th ACM SIGKDD International Conference on Knowledge Discovery in Data Mining. Chicago, 2005

[8] Ester M, Kriegel H-P, Sander J, et al. A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise[C]// The 2nd International Conference on Knowledge Discovery and Data Mining. Portland, 1996

[9] Stonebraker M, Frew J, Gardels K, et al. The SEQUOIA 2000 Storage Benchmark[C]// The 1993 ACM SIGMOD International Conference on Management of Data. Washington, 1993

[10] Yeung K, Ruzzo W. An Empirical Study on Principal Component Analysis for Clustering Gene Expression Data[J]. Bioinformatics, 2001, 17(9): 763-774

(上接第 55 页)

[6] Song R, Korba L, Yee G. AnonDSR: Efficient Anonymous Dynamic Source Routing for Mobile Ad-Hoc Networks[C]// Proc. ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '05). 2005: 320-327

[7] Zhang Y, Liu W, Lou W. Anonymous Communications in Mobile Ad Hoc Networks[C]// Proc. INFOCOM. 2005: 1940-1951

[8] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]// Advances in Cryptology -Crypto'01, LNCS 2139. Berlin: Springer-Verlag, 2003: 213-229

[9] Barreto P, Kim H Y, Lynn B. Scott. Efficient Algorithms for Pairing-Based Cryptosystems[C]// Proc. CRYPT0 02. Springer Verlag, August 2002: 354-368

[10] Fall K, Varadhan K. ns notes and documentation [EB/OL]. http://www-mash.cs.berkeley.edu/ns/, 2003

[11] Boneh D, Lynn B, Shacham H. Short signatures from the Weil pairing[C]// Advances in Cryptology -Asiacrypt 2001 Volume 2248 of Lecture Notes in Computer Science. Berlin: Springer - Verlag, 2002: 514-532

[12] Bareeto P, Lynn B, Scott M. Efficient Implementation of Pairing-based Cryptosystems[J]. Journal of Cryptology, 2004, 17: 321-334