维普资讯 http://www.cqvip.com

一种 Ad Hoc 网络中的安全匿名按需路由协议*)

陈 晶 崔国华 洪 亮 付 才

(华中科技大学计算机科学与技术学院 武汉 430074)

摘 要 虽然现在研究 Ad Hoc 网络中安全的文章很多,但是很少有人考虑到匿名的问题。本文中,匿名性的定义更加严格,将匿名性细分为身份保密、位置保密和路由匿名三个部分。文章提出安全匿名按需路由协议(SADR, Secure Anonymous Routing)不但保证了路由安全形成和维护,数据安全传输,并且同时满足了匿名性各个方面的要求,特别是很容易被忽略的身份匿名性和强位置保密性,使得恶意节点无法获得合法节点的身份与位置信息,从而难于进行攻击。为了清晰准确的表达 SADR 协议的过程,引入了 DFA (deterministic finite automaton)进行描述,并使用 BAN 逻辑推理规则进行了安全性证明。最后,对比仿真数据,分析了加入安全匿名机制后,给性能上带来的影响。

关键词 Ad Hoc,网络安全,匿名性,路由协议

A Secure Anonymous on Demand Routing Protocol in Ad Hoc

CHEN Jing CUI Guo-Hua HONG Liang FU Cai

(Department of Computer Science and Technology, Huazhong University of Science & Technology, Wuhan 430074)

Abstract Though many papers are about security in Ad Hoc now, few consider the anonymous problem. This paper defines the anonymity more strictly. It divides anonymity into three parts which are identity privacy, location privacy, routing anonymity. SADR (Secure Anonymous on Demand Routing) is proposed. It can ensure routing and transporting data securely and satisfy the various anonymity requirements, especially identity privacy and strong location privacy that are neglected easily. The vicious nodes can't get the identity and location information of the legal nodes, so they are hard to originate attacking. To represent the SADR protocol well, DFA (deterministic finite automaton) is quoted. On the other side, BAN is used to analyse the protocol's security. At last, comparing the simulated data, it shows the affect after guaranteeing security and anonymity.

Keywords Ad Hoc, Network security, Anonymity, Routing protocol

1 引言

相对于有线网络,无线 Ad Hoc 网络更容易受到各种攻击。这主要是因为无线 Ad Hoc 网络的无中心、动态拓扑、自组织、多跳路由等特点。现在的研究工作主要集中在移动 Ad Hoc 网络中的机密性、完整性、有效性和公平性方面,很少有文章考虑匿名性问题。但是,匿名性应该是安全方案中很重要的部分。特别是在某些至关重要的环境下。例如,在战场上,不但要求攻击者不能窃听到通讯的内容(机密性),不能中断通讯(有效性和完整性),还要求通信双方的身份和位置信息对攻击者是匿名的。否则,攻击者可能推算出有关位置、移动或者通信模式等重要信息,从而发起物理上的攻击。

设计安全路由的时候,不能忽略对匿名性的要求,很多公认的安全路由协议,如 SRP[1], ARAN[2], AODV-S[3], Ariadne[4], SEAD[5]在安全性上可以抵御很多常见的攻击,但是由于一些内在的因素,没有能满足匿名性的要求,比如在 ARAN 中,中间节点需要验证路由请求报文和路由恢复报文中,源节点和目的节点的证书,该证书中包含了源与目的节点的身份信息。SDDR[6], ANODR[7], ASR[8]三种协议在提出的时候都考虑到路由的匿名性,但是,SDDR, ANODR 在匿名性方面,由于对匿名性定义上的模糊,SDDR 没有能保证中间节点的身份保密性,也达不到强位置保密性。ANODR 虽然可以对路由外的节点保证强位置保密性,但是对路由内的节点同样达不到强位置保密性,最重要的是,ANODR 无法保证源与目的节点的身份保密性。ASR 的提出,对匿名性有了一个相对严格的定义,ASR 对匿名性的实现也优于前面两者,但是,ASR 很多的信息都是公开的,非认证节点完全有可能利用监听到的路由信息伪造出路由信息,所以其本身的安全性存在着漏洞。所以,在设计匿名路由协议的时候,也应该同时保证安全性,而不是后期在加入相关的安全方案。

在本文中,首先定义更加严格的 Ad Hoc 中匿名性要求。提出的安全匿名按需路由协议(SADR)不光可以保护节点和路由的私有信息,也能确保路由查找的安全。然后,详细的分析了 SADR 在匿名性方面的各个指标,并利用 BAN 逻辑推理规则对安全性做出形式化的分析。

本文第 2 部分和第 3 部分,定义了协议的目标和初始假设。第 4 部分描述了协议的细节。在第 5 部分和第 6 部分,对 SADR 的匿名性和安全性做出了详细的分析。最后总结了 SADR 协议的优势和不足,指出了今后研究的方向。

*)国家自然科学基金(60403027)。陈 晶 博士研究生,主要研究领域为无线网络安全与路由协议安全与仿真;崔国华 教授,博士生导师,主要研究领域为信息安全、网络安全和密码学;洪 亮 博士研究生,研究方向为无线网络安全、路由协议安全仿真;付 才 助教、博士研究生,主要研究方向为网络安全、数据库安全以及访问控制。

维普资讯 http://www.cqvip.com

2 设计目标

2.1 匿名性

(1)身份保密。身份保密由下面的要求组成:(a)除了源和目的节点,其他节点都不知道它们的真实身份;(b)源和目的节点没有中间节点的真实身份。

(2)位置保密。位置保密由下面的要求组成:(a)除了源和目的节点,其他节点都不知道它们的真实位置;(b)其它节点,甚至是源和目的节点间的路由中间节点,不知道它们间的距离,如到源、目的节点的跳数,或者它们两者之间的跳数。一个协议只满足(a),那么称这个协议为"弱位置保密",如果同时满足(a)和(b),那么称这个协议为"强位置保密"。

(3)路由匿名。路由匿名有下面的要求:(a)在路由中或者路由外的节点,不能跟踪到报文的源或者目的节点;(b)对于不在路由内的攻击者,他们没有任何路由信息。(c)攻击者很难推断源和目的节点的传输与运动模式。

2.2 安全性

协议能保护必要的功能,能在常见主动攻击和被动攻击下,安全的发现与维护路由,安全并高效的传输数据。

3 假设

在本文中,做如下假设:

(1)初始化的过程中,源与目的节点有一个共享密钥;

(2)无线链路是对称的;

(3)攻击者有很强的窃听能力,但是计算和节点入侵能力有限。

(4)在初始化过程中,只有合法节点能获得 CA 颁布的证书和 CA 的公钥,且该节点在证书有效期内不会叛变。

4 安全匿名按需路由协议(SADR)

这部分中,将介绍 SADR 的细节。整个协议由下面的部分组成:路由请求(RREQ),路由响应(RREP),匿名数据传输(ADT, Anonymous Data Transmission)和路由维护(RERR)。源节点,路由中间节点和目的节点分别用 $S, X_i (i = 1,2,\cdots,n)$ 和 D。n 表示在源和目的节点之间的节点数。

4.1 路由请求

在请求过程中,路由中表示为 X_{i-1} 的节点按下面的公式发送路由请求:

$$[RREQ, Cert_{i-1}, \{Dest, K_g, U_0, Tick\}K_T, \{\{Tick+1, seq\}K_g, seq\}K_{i-1}^{-1}, U_i]$$

其中,参数如表 1 所示。

在 RREQ 中的 U_i, X_{i-1} 按下式计算:

$$U_i = f(U_{i-1}, S_i) = (U_{i-1} ? px) \cup ((U_{i-1} \oplus S_i) = px \cdot H\max) \quad (1)$$

对 $i=1,2,\cdots,n$,当 S_i 是 X_{i-1} 以是 p_x 宽度选出的随机数。U_0 是源节点以 p_l 宽度选出的随机数 $p_l = (H_{\max}+1) \cdot px$。在公式(1)中,$\oplus$ 表示操作符异或。因此,公式(1)的计算相当于有 2 个步骤。

(1)数 U_i 的低位由 S_i 和 U_{i-1} 位异或所得结果的最小 p_x 位,而 U_i 高位和 U_{i-1} 的高位相同。

(2)将(1)的计算结果循环右移 p_x 位。

为了清晰准确的说明节点 X_i 在接收到 RREQ 报文后的处理流程,本文使用 DFA(deterministic finite automaton)来进行描述[9]。定义 $M_{RREQ} = (Q_Q, \Sigma_Q, \delta_Q, q_{0Q}, F_Q)$, $Q_Q = \{q_0, q_1, q_2, q_3, q_4, q_5, q_6, q_7\}$, $\Sigma_Q = \{0,1\}$ 其中 1 表示成功,0 表示失败。$\delta_Q = \{\delta(q_0,0)=q_7, \delta(q_0,1)=q_1, \delta(q_1,0)=q_7, \delta(q_1,1)=q_2, \delta(q_2,0)=q_7, \delta(q_2,1)=q_3, \delta(q_3,0)=q_6, \delta(q_3,1)=q_4, \delta(q_4,0)=q_7, \delta(q_4,1)=q_5\}$, $q_{0Q}=q_0$, $F_Q=\{q_5,q_6,q_7\}$ 其中 q_0 表示检验 $Cert_{i-1}$,是否可以得到公钥 K_{i-1}。q_1 表示检验是否能以 K_{i-1} 解密 $\{\{Tick+1, seq\}K_g, seq\}K_{i-1}^{-1}$。$q_2$ 表示检验得到的 seq 是否大于路由表中记录的 seq。q_3 表示检验是否能解密 $\{Dest, K_g, U_0, Tick\}K_T$。$q_4$ 表示检验 U_0 和 U_i 是否能用 Length 算法计算出正确的跳数。q_5 表示接受 K_g 为会话密钥,存储 seq 和 U_i 作为 RREP 的构造参数。q_6 重新计算 U_i、$\{\{Tick+1, seq\}K_g, seq\}K_i^{-1}$,将计算结果和 $Cert_i$ 替换相应位置的值,重新广播处理后的报文。存储 $\{Tick+1, seq\}K_g$、seq 到路由表作为 RREP 的判断依据。q_7 丢弃报文。RREQ 的状态转换图如图 1 所示。

表 1 本文定义的符号

符号	意义	符号	意义
		$Tick$	源节点选取的随机数,最后由目标节点处理后,在 RREP 中返回
seq	当前报文的序列号		
K_T	源和目的节点之间的共享密钥	K_g	当前要协商的会话密钥
		U_0	源节点选择的一个随机数
$Dest$	目标 D 的 ID 号		
$Cert_{i-1}$	系统在初始化的时候颁布给节点 $i-1$ 的证书,证书中包含该节点的公钥 K_{i-1},证书基本格式为 $Cert_{i-1}=\{K_{i-1}, Cert_v, stamp\}K_{CA}^{-1}$, K_{i-1} 表示节点 $i-1$ 的公钥,$Cert_v$ 表示证书的版本,$stamp$ 表示时间戳	U_i	节点 X_{i-1} 计算出的数,其中 X_{i-1} 表示第 $i-1$ 个中间节点,和节点本身的 ID 无关
		K_{i-1}^{-1}	第 $i-1$ 个节点的私钥
		K_{i-1}	第 $i-1$ 个节点的公钥

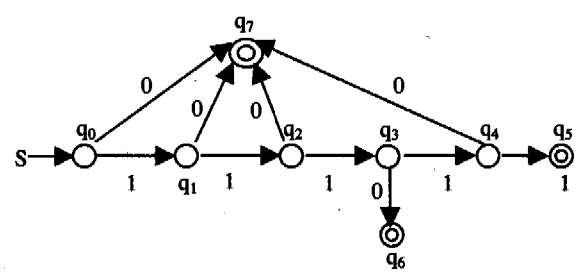

图 1 RREQ 的状态转换图

Length 算法如下,其中 U_S 和 U_D 是 p_x 位,U_0 和 U_n 是 $p_l = (H_{\max}+1)p_x$ 位,X 的初始值为 1:

(1)$U_S = U_0 ? H_{\max} \cdot p_x$

(2)$U_D = (U_n = X \cdot px) ? H_{\max} \cdot p_x$

(3)如果 $U_S = U_D$,那么 Length $= X$,算法成功。返回 SUCCESS 如果 $U_S \neq U_D$ 且 $X < H_{\max}$,那么 $X = X+1$,返回(2)。如果 $U_S \neq U_D$ 且 $X \geqslant H_{\max}$,返回 ERROR 标志,该标志表示不能正确计算出路由长度。

Length 算法如果返回 SUCCESS 那么表明报文中的路由长度信息正确而且在最大路由跳数范围内,如果返回 ERROR,那么丢弃该报文,该报文可能是路由长度超过规定的最大长度,也可能是被篡改或者伪造。

维普资讯 http://www.cqvip.com

在路由请求过程的最后，在路由中的每个节点认证了前一节点，并存储其公钥，但并不知道前一节点是哪一个节点。目标知道 S 与 D 之间的距离，且该距离小于等于 H_{max}。

4.2 路由回复

在路由回复过程中，每个中转节点 X_i 会收到如下格式的路由回复：

$[RREP,\{T_{i+1}\}K_i,\{seq,\{seq,Tick+1\}_{K_g},U_n\}_{T_{i+1}}]$

其中，$\{seq,Tick+1\}_{K_g}$ 可证明目标节点能正确的从 RREQ 报文中恢复出 K_g。T_{i+1} 表示由 X_{i+1} 选出的随机数，是路由查找后 X_i 与 X_{i+1} 之间的单跳共享密钥。如果 X_i 是 S，那么，S 可由 U_0 和 U_n 计算出路由长度。接受路由回复的流程 DFA 描述如下：

定义 $M_{RREP}=(Q_P,\Sigma_P,\delta_P,q_{0P},F_P)$，$Q_P=\{q_0',q_1',q_2',q_3',q_4',q_5',q_6'\}$，$\Sigma_P=\{0,1\}$，其中 1 表示成功，0 表示失败。

$\delta_P=\{\delta(q_0',0)=q_6',\delta(q_0',1)=q_1',\delta(q_1',0)=q_6',\delta(q_1',1)=q_2',\delta(q_2',0)=q_6',\delta(q_2',1)=q_3',\delta(q_3',0)=q_5',\delta(q_3',1)=q_4'\}$，$q_{0P}=q_0'$，$F_P=\{q_4',q_5',q_6'\}$。其中 q_0 表示检验是否能用本节点私钥解密 $\{T_{i+1}\}_{K_i}$，并获得 T_{i+1}。q_1 表示检验是否能解密 $\{seq,\{seq,Tick+1\}_{K_g},U_n\}_{T_{i+1}}$，并获得 seq 和 $\{seq,Tick+1\}_{K_g}$ 以及 U_n。q_2 表示检验得到的 seq 和 $\{seq,Tick+1\}_{K_g}$ 是否能在路由表的记录中查询到。q_3 表示检验是否能解密 $\{seq,Tick+1\}_{K_g}$，且得到的 seq 和 $Tick$ 是否匹配。

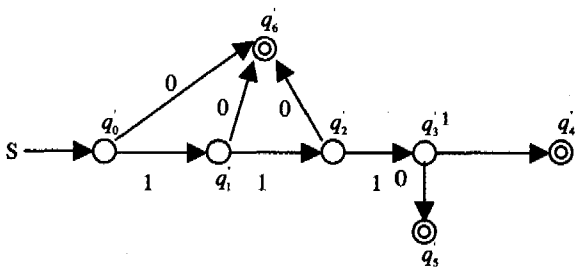

图 2 RREP 的状态转换图

q_4 表示完成会话密钥协商，路由已形成，并通过 U_0 和 U_n 计算出路由长度。q_5 表示重新计算 $\{T_i\}_{K_{i-1}}$ 和 $\{seq,\{seq,Tick+1\}_{K_g},U_n\}T_i$，将计算结果替换相应位置的值，重新广播处理后的值。q_6 表示丢弃报文。

RREP 的状态转换图如图 2 所示。

在路由回复的最后，每个中转节点 X_i 和其前后节点都协商了单跳共享密钥。在 X_i 路由表中的格式如表 2。

表 2 节点的路由表格式

seq	PK_{i-1}	T_i	T_{i+1}	$\{seq,Tick+1\}_{K_g}$
128 bits	1024 bits	128 bits	128 bits	256 bits

4.3 匿名数据传输

为了实现数据传输的匿名性和安全性，必须保证攻击者不能从数据报文中读懂或者推断出源和目的节点的信息。数据报文在广播到它们邻居之前，数据报文的内容需要用源与目的节点间的共享密钥加密。为了保证信息是沿刚才查找到的路径转发的，这些信息还需要用相应的单跳共享密钥加密。用单跳共享密钥去加密整个数据报文虽然在理论上是可行的，但不是一个好方法。这样一来，每个节点就必须在判断是否接受和抛弃报文前，解密整个报文。所以，这个方法的代价是巨大的。

在 SADR 中，提供了一种解决方案。主要的想法是构造些随数据发送的小信息，使得转发节点仅仅需要验证这些信息而不用验证整个报文。数据传输报文的格式如下：$[ADT,M,TAG]$，其中 M 是传输的内容，是经过源与目的节点间的共享密钥加密的。那些作为标记(TAG)的小信息构造如下。

节点 X_i 和 X_{i+1} 单跳共享密钥为 T_{i+1}。H_K 为单向散列函数，使用 K 作为其密钥。从 X_i 到 X_{i+1} 的报文的 TAG 是由 $H_{T_{i+1}}(M)$ 计算而得。而 i 则表示在被选择路由上的节点的编号，这与节点 ID 号是没有任何关系的，对于不同的路由，相同节点在其中的节点号可能不同。

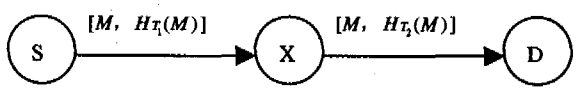

图 3 节点 S 传递报文给节点 D

假设有三个节点 S、X、D(如图 3 所示)，X 是节点 S 和 D 的邻居节点。但是 S 和 D 不是相邻。S 要发送报文给节点 D。T_1、T_2 是 S、X 和 X、D 之间的单跳共享密钥。M 是要传输的经过加密的数据。

(1)$S\rightarrow X:[M,H_{T_1}(M)]$

(2)节点 X 收到报文后，计算用 M 和本地存储的 T'_1，计算出 $H_{T'_1}(M)$。如果 $H_{T'_1}(M)$ 等于 $H_{T_1}(M)$，跳到 (3)，否则丢弃该报文。

(3)$X\rightarrow D:[M,H_{T_2}(M)]$

(4)节点 D 收到后计算 $H_{T'_2}$，如果等于 $H_{T_2}(M)$，接受该报文，否则就丢弃该报文。

4.4 路由维护

假设，当重传次数超过一个预定值的时候，节点会认为路由失败。节点在它的路由表中查找相应的项，并用与前一节点的单跳共享密钥为参数求散列值，构造 TAG 信息，并发送路由报错报文(RERR)。格式如下：$[RERR,\{seq,Tick+1\}_{K_g},TAG]$。节点 X_i 和 X_{i+1} 共享密钥为 T_{i+1}。从 X_{i+1} 到 X_i 的报文的 TAG 是由 $[N,H_{T_{i+1}}(N)]$ 计算而得。其中 N 是 RRER 报文内容。节点 X_i 在接受到报文后在路由表中查找相应的项并检查是否能解密 $\{seq,Tick+1\}_{K_g}$，从而判断该报文是重计算转发、接受或者是丢弃。

5 匿名性分析

这里检查一下 SADR 是否达到在第二部分中定义的匿名性问题，分别是身份保密性、位置保密性还有路由匿名性。

(1)身份保密性：在 SADR 中，RREQ 报文除了目标节点的身份(Dest)以外，没有其他任何节点身份。而源节点使用与目的节点之间的共享密钥加密，所以只有目标节点可以正确接收 RREQ，保证了在 RREQ 中源与目的节点身份保密性。在 RREP、ADT、RERR 都是依赖单跳共享密钥或者邻节点的公钥进行传递，确保源与目的节点身份的保密。同时在节点的路由表中，只有和上一跳或者下一跳之间的共享密钥 T_i，所以源节点与目的节点并不知道中间节点的身份，从而保证了路由中间节点的身份保密性。

(2)位置保密性：现阶段的位置攻击，主要是通过窃听路由请求和路由回复报文，获得报文的跳数信息，来推断源与目的节点的位置。在 SDDR 中，使用了洋葱路由技术(Onion Routing)[10]，在路由请求报文中，每个中转节点添加一个固

维普资讯 http://www.cqvip.com

定长度信息，包括节点 ID 和一个会话密钥等。因此，每个节点接收到路由请求报文可以推断出源节点和自己的距离。在 ANODR 中，作者提出添加随机数到报文中来阻止这种攻击。但是，选取路由的中间节点必须知道与源与目的节点的距离。这就没有保证强位置保密性。为了对所有节点都达到强位置保密性，SADR 提出了 Length 算法，由于 U_0 只有源与目的节点知道，U_0 和 U_n 长度并不随路由跳数变化而改变。所以，其它节点，不论是路由内的，还是路由外的，都无法推断报文的跳数信息。

(3)路由匿名性：现在对于路由匿名性的攻击主要是 2 种情况。第一种基于流量分析[11]。其原理主要是探测在监听到的报文里的公共信息，并假设如果有公共信息，那么说明 2 个报文是从同一路由进行传送。公共信息有可能是相同的报文内容。或者是根据某些模式的变化(如，增加报文的长度)来分析。在 SADR 中，单跳间的共享密钥不同，加大了攻击者匹配的难度，使得这样的攻击在实际中难于实现。而且 SADR 中，报文的长度在传输中不被更改，因为增加的报文长度可以成为路由跟踪的一个信号。第二种情况，是基于时间分析。攻击者可以使用传输的时间依赖关系来跟踪受害节点的信息转发路径。通常用来防范时间分析的方法是，使用混淆技术[12~14]。在 SADR 中，每个节点有自己独特的序列号。而且，可以使用缓存来存储和改组接收到的报文的序列号，并同时在缓存中记录所做的改动，使得攻击者难于实施时间分析。

6 安全性分析与证明

因为数据加密算法的安全性与路由的匿名性与安全性是 2 个不同的部分。所以这里的讨论不考虑加密算法本身安全性的不足。BAN 逻辑是一种基于广义逻辑信任概念的协议分析工具[15,16]，广泛应用于认证和密钥分配等协议的安全分析。具有直观、简洁、高效的特点，能够发现协议中存在的缺陷与不足。为了分析 SADR，本文也引入了部分扩展的 BAN 逻辑推理规则。由于 BAN 逻辑主要是对安全性做分析与证明的，匿名性在前一部分已经分析，而所有的路由消息都是加密过的。所以这里可以认为，路由消息的传递可以被抽象为在一个可能被监听的秘密信道上传输的路由请求和路由回复两种消息。

协议描述如下：

(1)$S\rightarrow D:[RREQ,Certs,\{K_g,Tick\}_{K_T}]$

(2)$D\rightarrow S:[RREP,\{T\}_{K_s},\{\{Tick+1\}_{K_g}\}_T]$

6.1 BAN 的逻辑推理规则

为了分析 SADR 的安全性，下面列出在证明过程中用到的逻辑推理规则或者扩展的逻辑推理规则：

(1)信息的意义：如果 $P\models Q\overset{K}{\leftrightarrow}P\wedge P\lhd\{X\}_K$，则 $P\models Q\mid\sim X$。

(2)信息的现时性验证：如果 $P\models\#(X)\wedge P\models Q\mid\sim X$，则 $P\models Q\models X$。

(3)信息的新鲜性：如果 $P\models\#(X)$，则 $P\models\#(X,Y)$。

(4)如果 $P\lhd\{X\}K_Q^{-1}\wedge P\models\xrightarrow{KQ}Q$，则 $P\models Q\mid\sim X,P\models X$。

(5)如果 $P\lhd\{X\}_{K_P}$ 或者 $P\models R\mid\sim\{X\}_{K_P}$，则 $P\models P\overset{X}{\Leftrightarrow}Q$。

(6)信息的传送规则：如果 $P\lhd(X,Y)$，则 $P\lhd X\wedge P\lhd Y$。

6.2 SADR 的初始化假设

(1)$S\models\xrightarrow{K_{CA}}CA$　(2)$D\models\xrightarrow{K_{CA}}CA$　(3)$S\models\#(Certs)$

(4)$D\models\#(Certs)$　(5)$S\models\#(Tick)$　(6)$D\models\#(T)$

(7)$D\models\#(Tick)$　(8)$S\models\#(T)$　(9)$S\models\#(K_g)$

(10)$S\models S\overset{K_g}{\leftrightarrow}D$　(11)$S\models\xrightarrow{K_S}S$　(12)$S\models S\overset{K_T}{\leftrightarrow}D$

(13)$D\models S\overset{K_T}{\leftrightarrow}D$　(14)$D\models\#(K_g)$　(15)$D\models\#(K_S)$

6.3 SADR 协议的理想化

由上面的 2 个步骤进行相应的理想化，可以得到

(1)$S\rightarrow D:\{\xrightarrow{K_S}S\}K_{CA}^{-1},\{S\overset{K_g}{\leftrightarrow}D,S\models Tick\}_{K_T}$

(2)$D\rightarrow S:\{S\overset{T}{\leftrightarrow}D\}_{K_S},\{\{Tick+1\}_{K_g},S\overset{K_g}{\leftrightarrow}D\}_T$

6.4 SADR 协议的安全性分析

由理想化的步骤(1)，S 发送到 D 的信息有 2 个部分。由这 2 部分可以分别得到

$$D\lhd\{\xrightarrow{K_S}S\}K_{CA}^{-1} \tag{2}$$

$$D\lhd\{S\overset{K_g}{\leftrightarrow}D,S\models Tick\}_{K_T} \tag{3}$$

由式(2)和假设(2)，根据逻辑推理规则(4)，可得

$$D\models CA\mid\sim\{\xrightarrow{K_S}S\} \tag{4}$$

由式(4)和假设(15)，根据逻辑推理规则(2)信息的现时性验证，可得

$$D\models CA\models\xrightarrow{K_S}S\quad\text{即}\quad D\models\xrightarrow{K_S}S \tag{5}$$

由式(3)和假设(13)，根据逻辑推理规则(1)信息的意义，可得

$$D\models S\mid\sim\{S\overset{K_g}{\leftrightarrow}D\wedge S\models Tick\} \tag{6}$$

由式(6)和假设(7)，根据逻辑推理规则(3)信息的新鲜性，可得

$$\#(S\overset{K_g}{\leftrightarrow}D\wedge S\models Tick) \tag{7}$$

由式(7)根据逻辑推理规则(2)信息的现时性验证，可得

$$D\models S\models(S\overset{K_g}{\leftrightarrow}D\wedge S\models Tick)\quad\text{即}\quad D\models S\models S\overset{K_g}{\leftrightarrow}D \tag{8}$$

由理想化步骤 2，可以得到

$$S\lhd\{S\overset{T}{\leftrightarrow}D\}_{K_S}\wedge S\lhd\{\{Tick+1\}_{K_g},S\overset{K_g}{\leftrightarrow}D\}_T \tag{9}$$

由式(5)、式(9)根据逻辑推理规则(5)，可得

$$S\models S\overset{S\overset{T}{\leftrightarrow}D}{\Leftrightarrow}D\quad\text{即}\quad S\models S\overset{T}{\leftrightarrow}D \tag{10}$$

此处是基于本文的协议假设(4)，也就是合法节点不会在证书有效期内叛变。否则合法节点是可以伪造出 T 使得证明过程不成立。但合法节点的信任管理不是本文讨论的范围。

由式(9)、式(10)和逻辑推理规则(1)和(6)，可得

$$S\lhd\{Tick+1\}_{K_g}\wedge S\lhd S\overset{K_g}{\leftrightarrow}D \tag{11}$$

由式(11)和假设(10)，根据逻辑推理规则(1)信息的意义，可得

$$S\models D\mid\sim Tick+1 \tag{12}$$

由式(12)和假设(5)，根据逻辑推理规则(2)信息的现时性验证，可得

$$S\models D\models Tick+1 \tag{13}$$

由式(11)、式(13)和假设(5)，根据逻辑推理规则(3)信息新鲜性，可得

$$S\models\#(\{Tick+1\}_{K_g},S\overset{K_g}{\leftrightarrow}D) \tag{14}$$

维普资讯 http://www.cqvip.com

由式(11)、式(14)根据逻辑推理规则(2) 信息的现时性验证,可得

$$S\models D\models\{\{Tick+1\}_{K_g}, S\overset{K_g}{\leftrightarrow}D\}\text{即}$$

$$S\models D\models S\overset{K_g}{\leftrightarrow}D \tag{15}$$

最后,由式(8)和式(15)可得 $S\models S\overset{K_g}{\leftrightarrow}D\wedge D\models S\overset{K_g}{\leftrightarrow}D$,得证。

7 仿真实验

实验平台为 Pentium 1.8 GHz, 512 MB RAM ,使用的操作系统是 Windows 2000 下 Cygwin 平台 ,网络仿真平台是 ns2.27(network simulator version2.27)。仿真中,节点总数设置为 40 个,连接数为 15,节点运动范围 1000m × 1000m ,网络中节点的运动方式采用随机运动模型,即每个节点在该区域内从一点向另一点运动,运动速度在零到最大速度之间随机选取,到达目标点后,停留一段时间,然后随机选择一个新的目标点和一个新的速度,向新的目标点运动,依此类推,直至仿真结束。MAC 层使用的 802.11 协议 ,节点传输半径为 150m ,链路带宽为 2Mbps,数据包大小为 512 字节,模拟时间为 300s。

测试收集两种数据:分组传递率(packet delivery rate) ,是应用层信源发送的分组数目与信宿接收分组数目之比。它描述的是通过应用层观察到的报文丢失率,又反映了网络所支持的最大吞吐量。它是路由协议完成性和正确性的指标。平均延迟(average delay) ,它是报文从源节点到目标节点的平均传输时间,它反映了网络性能。

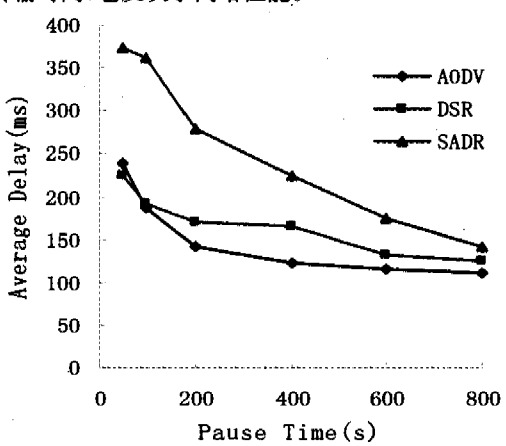

图 4 平均时延随停留时间的变化

图 4 与图 5 主要反映了系统中平均时延和拓扑图变化之间的关系。当节点的移动速度增加,而停留时间减少的时候,网络的拓扑图的变化就会变得更加激烈。由于网络拓扑图的变化,节点之间的路由也会产生相应的变化。网络中的 RREQ、RREP、RRER 等控制报文也相应增加。在 SADR 中,因为为了保证安全性与匿名性,所以这些控制报文都需要加解密。这些操作将占用部分资源,特别是公私钥的加解密,会影响节点传输报文的效率。所以在拓扑图变化激烈的时候,SADR 传输报文的平均时延要高于 AODV[17] 和 DSR[18],而当拓扑图变化缓和下来,三者的平均时延则比较接近。在图 4 的仿真场景中,SADR 与 AODV 和 DSR 的最大的时延差不超过 150ms,当停留时间到达 800s 的时候,SADR 与 AODV 和 DSR 的时延差只有 20ms。在图 5 的仿真场景中,时延差最小,大约 40ms。最大约为 100ms。

图 6 反映了节点停留时间与报文递送率之间的关系。节点停留时间越长,说明路由越稳定,在重新寻找路由的过程中的报文丢失数也就越少。由于在数据报文的传输过程中,节点是用对称密钥加解密,而对称密钥加密算法的效率非常高,所以对于性能的影响是非常小的,SADR、AODV 和 DSR 三者的分组传输率比较接近。

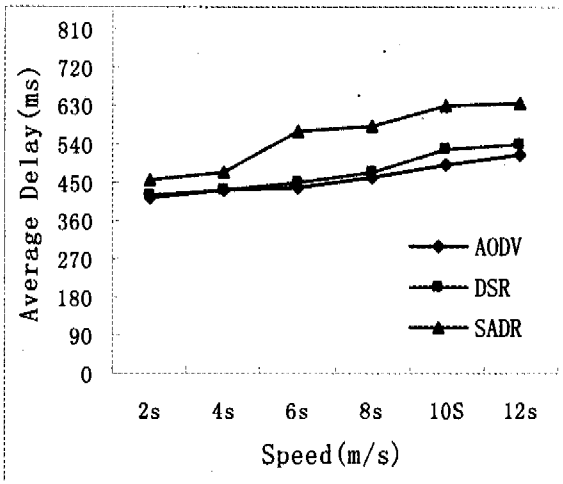

图 5 平均时延随速度的变化

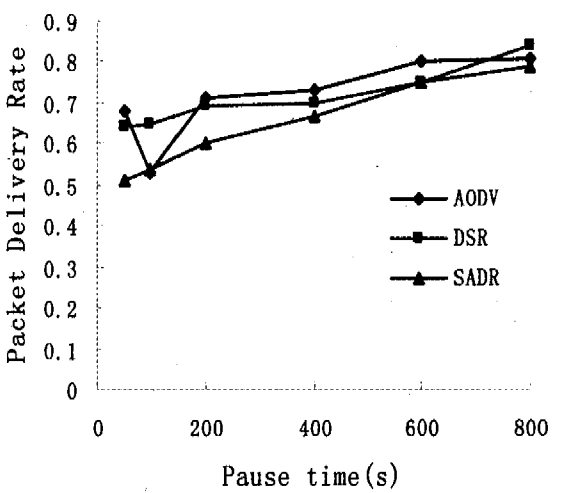

图 6 分组传递率随停留时间的变化

图 7 反映了 CBR(constant bit rate)与报文递送率之间的关系。由于 802.11 协议采用一种基于二进制指数退避的冲突避免机制,即带有冲突检测的载波侦听多路访问(CSMA/CA)。节点发送与接收报文由 MAC 层的 RTS 和 CTS 来控制。一旦整个网络系统中,CBR 达到一个阈值的时候,出现大量的多个节点请求与同一节点通信的情况,CSMA/CA 保证在同一时间信道的独用性,所以很多需要被转发的报文被延迟发送甚至超时被丢弃,从而导致报文递送率会显著下降。SADR 在数据报文的传输中,需要用源与目的节点之间的会话密钥加密,要占用一定的系统资源,所以 SADR 的阈值要小于 AODV 和 DSR。

总之,仿真结果表明,SADR 的性能效率要略低于 AODV 和 DSR。协议在安全性、匿名性和性能之间找到一个相对的平衡,即在保证安全性与匿名性的情况下,略微的牺牲性能与效率。

(下转第 60 页)

维普资讯 http://www.cqvip.com

0.2722%，而集中式路由算法的丢包率为0.3896%，而且随着背景流量的不断增加，DTRA算法的丢包率性能更加明显优于集中式路由，同时时延性能也在一定范围内有所提高。

模拟结果表明，在网络负载较低的情况下，集中式路由和DTRA路由性能基本一致；但当网络负载增大时，DTRA路由的时延性能、丢包率性能都明显优于集中式路由，而且链路利用率也较高。可见，DTRA算法通过备份路由，充分利用了网络资源，缓解了拥塞问题。

结束语 对卫星网络路由算法的模拟由于其特殊的网络环境一直以来都是一个比较活跃的研究课题。利用ns2进行卫星网络协议的模拟与仿真是一个非常复杂的过程，需要大量时间和工作的积累。同时，在具体的模拟过程中也需要结合卫星网络技术的发展不断改进和调整模拟仿真的手段和方法，以便能够指导和推动整个卫星网络的综合模拟与仿真。卫星网络协议的模拟与仿真是卫星网络实际应用的重点和难点，值得不断深入探讨和研究。

参考文献

1 王鹏，白建军，卢泽新. 卫星网络协议的仿真与模拟技术研究. 计算机工程与科学，2004，26(5)：4～6

2 续欣，等. 卫星信道性能的网络模拟. 系统仿真学报，2002，14(8)：1056～1059

3 Wood L, Clerget A, Andrikopoulos I, et al. IP Routing Issues in Satellite Constellation Networks[J]. International Journal of Satellite Communications, January/February 2001, 19(1): 69～92

4 Brunt P. IRIDIUM: Overview and Status[J]. Space Commun., vol. 14, no. 2, 1996, 14(2): 61～68

5 Sturza M A. Architecture of the TELEDESIC Satellite System [C]. In: Proceedings of International Mobile Satellite Conference, 1995. 212～218

6 孙利民，卢泽新，吴志美. LEO卫星网络的路由技术. 计算机学报，2004，27(5)：659～667

7 Henderson T R, Katz R H. Network Simulation for LEO Satellite Networks[A]. In: Proceeding of 18th Internation Communication Satellite Systems Conference[C]. Oakland, CA, Apr 2000

8 Hu Y, Li V O K. Satellite-based internet: A tutorial[J]. IEEE Communications Magazine, March 2001, 39(3): 154～162

（上接第33页）

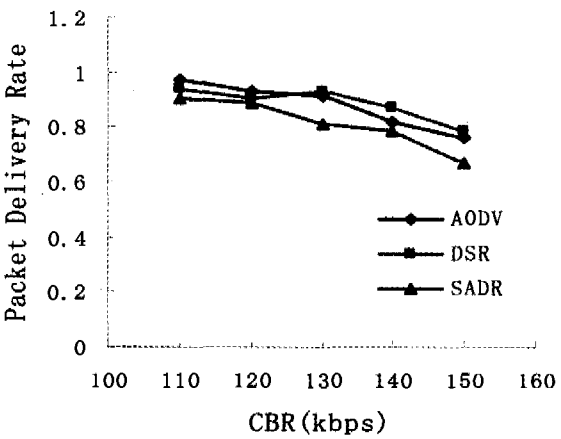

图7 分组传递率随CBR的变化

结论 本文提出了一种安全匿名的按需路由协议SADR。通过对安全性和匿名性的分析，SADR可以阻止重放、伪造、篡改等等的攻击。并且在保证安全性的同时，也实现了身份保密、强位置保密和路由匿名性，使得恶意节点的被动攻击难于实施。当然SADR也存在不足之处，比如对新加入节点与网络中其它节点之间的共享密钥的协商问题，还有在性能效率上有待进一步的提高的问题，这些将是以后研究的方向。

致谢 在此，我们向对本文的工作给予支持和建议的同行，尤其是华中科技大学信息安全实验室各位老师和同学表示感谢。

参考文献

1 Papadimitratos P, Haas Z J. Secure routing for mobile ad hoc networks. In: SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002), January 2002. 2～21

2 Sanzgiri K, Dahill B, Levine B N, et al. A secure routing protocol for ad hoc networks. In: Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP), 2002. 78～87

3 Yang H, Meng X, Lu S. Self-organized network-layer security in mobile ad hoc network. In: Proceedings of the ACM Workshop on Wireless Security, 2002. 11～20

4 Hu Y C, Perrig A, Johnson D B. Ariadne: A secure ondemand routing protocol for ad hoc networks. In: Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), 2002. 12～23

5 Hu Y C, Johnson D B, Perrig A. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. In: Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2002), June 2002. 3～13

6 El-Khatib K, Korba L, Song R, et al. Secure dynamic distributed routing algorithm for ad hoc wireless networks. In: International Conference on Parallel Processing Workshops (ICPPW'03), 2003. 359～366

7 Kong J, Hong X. ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In: Fourth ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'03), 2003. 291～302

8 Zhu Bo, Wan Zhiguo, Kankanhalli M S, et al. Anonymous secure routing in mobile ad-hoc networks. Local Computer Networks, 2004. 29th Annual IEEE International Conference, 2004. 102～108

9 Hopcroft J E, Ullman J D. Introduction to Automata Theory, Languages, and Computation. Addison-Wesley Publishing Company, 1979

10 Reed M G, Syverson P F, Goldschlag D M. Anonymous connections and onion routing. IEEE Journal on Selected Areas in Communications, 1998, (Special Issue): 482～494

11 Raymond J F. Traffic analysis: Protocols, attacks, design issues, and open problems. In: DIAU00, Lecture Notes in Computer Science 2009, 2000. 10～29

12 Pfitzmann A, Pfitzmann B, Waidner M. ISDN-MIXes: Untraceable communication with very small bandwidth overhead. In: Proc. GI/ITG-Conference "Kommunikation in Verteilten Systemen" (Communication in Distributed Systems), 1991. 451～463

13 Berthold O, Federrath H, Kohntopp M. Project anonymity and unobservability in the internet. In: Computers Freedom and Privacy Conference 2000 (CFP 2000), Workshop on Freedom and Privacy by Design, 2000

14 Kesdogan D, Egner J, Bschkes R. Stop-and-go-MIXes providing probabilistic anonymity in an open system. In: Second International Workshop on Information Hiding, Lecture Notes in Computer Science 1525, 1998. 83～98

15 蒋宗礼，姜守旭. 形式语言与自动机理论. 北京：清华大学出版社，2003

16 Gong L, Needham R, Yahalom. Reasoning about Belief in Cryptographic Protocols. In: Proceeding of the 1990 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, 1990. 234～248

17 Perkins C E, Royer E M. Ad-hoc on-demand distance vector routing. Mobile Computing Systems and Applications, 1999. In: Proceedings WMCSA '99. Second IEEE Workshop, 1999. 90～100

18 Johnson D B, Maltz D A. Dynamic source routing in ad hoc wireless networks. Mobile Computing, 353, 1996