

具有私钥自愈能力的 DTN 密钥管理方案

李德全^{1,2}, 张习勇^{1,2}, 张婷婷^{1,2}, 郭冠军³

(1. 天地一体化信息技术国家重点实验室, 北京 100029;
2. 北京市天地一体化信息安全工程技术研究中心, 北京 100080;
3. 北京航天自动控制研究所, 北京 100084)

摘要: 由于时延容忍网络 (DTN, delay tolerant networks) 时延大, 节点无法及时收到私钥更新的广播消息, 从而无法及时更新某个时间段的私钥。针对该问题, 提出了一个允许私钥自愈的分簇密钥管理方案。该方案不但可以完成对节点私钥的分发与更新, 还可以实现节点以前私钥的自愈。安全性与效率分析表明, 该方案特别适合网络延时大、间歇性连接的 DTN。

关键词: 时延容忍网络; 密钥管理; 私钥自愈

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00156

Key management scheme with private key self-healing ability in DTN

LI De-quan^{1,2}, ZHANG Xi-yong^{1,2}, ZHANG Ting-ting^{1,2}, GUO Guan-jun³

(1. State Key Laboratory of Space-Ground Integrated Information Technology, Beijing 100029, China;
2. Beijing Engineering Research Center of Space-ground Integration Information Security, Beijing 100080, China;
3. Beijing Aerospace Automatic Control Institute, Beijing 100084, China)

Abstract: Because of the large delay of DTN network, node cannot receive broadcast updating private key messages in a timely manner, thus unable to update the private key for a certain time period. Aiming at this problem, an allowing private key self-healing clustering key was management scheme. The scheme can not only accomplish the distribution of the private keys of node and update, but also can self-heal the old time private keys. Security and efficiency analysis show that the scheme is particularly suitable for large network latency, intermittent connection DTN network.

Key words: delay tolerant networks, key management, private key self-healing

1 引言

现有的互联网基于 TCP/IP 体系架构, TCP/IP 要求高可靠、低时延。然而, 空间信息网络、移动传感器网络等存在高时延和经常中断等特点,

因此, TCP/IP 在此类场合是不适用的。为此, 研究人员提出了一种新型的网络体系结构, 即时延容忍网络 (DTN, delay tolerant networks), 又称容迟网络。不同于现今人们经常接触的网络结构, DTN 的典型特征是多个节点之间的链路存在间

收稿日期: 2017-01-15; 修回日期: 2017-02-23。通信作者: 李德全, lidequan@139.com

基金项目: 国家自然科学基金资助项目 (No.61572027, No.61300172); 软件开发环境国家重点实验室开放基金资助项目 (No.SKLSDE-2016ZX-17)

Foundation Items: The National Natural Science Foundation of China (No.61572027, No.61300172), The State Key Laboratory of Software Development Environment Fund (No. SKLSDE-2016ZX-17)

歇性中断, 且中断持续时间较长, 以至于在任意时刻一个节点和另一个节点间可能不存在可靠的路径(如卫星网络、ad hoc 传感器网络、地面移动通信网络等)^[1]。DTN 的网络环境较复杂, 信号的传输途径受许多因素的干扰, 因此某些节点进行会话通信时, 需要利用其他方法, 如通过中继节点(由其他节点代理)来转发信息, 才能实现信息的传输。与传统网络相比, 容迟网络面临更多的安全威胁。

密钥管理是容迟网络安全研究中的一个公开问题。因为在容迟网络中, 各个节点之间的距离短, 相互之间通信不能通过无线网络基础设施来实现。因此, 在容迟网络中, 设计密钥管理方案时, 不能假设有一个随时可以访问一个信任中心, 这给密钥管理方案的设计提出了新的挑战。DTN 拓扑结构具有不确定性和节点相对稀疏性的特点, 节点无法实时地连接固定的网关等基础设施, 相互间缺乏端到端的持续链路。因此, 原有基于公钥基础设施的密码系统不符合 DTN 的安全要求。DTN 与移动 ad hoc 网络有一定的类似性, 但 DTN 的网络特征使移动 ad hoc 网络的一些安全策略难以直接在 DTN 中得到应用。这些因素给 DTN 的安全研究带来了挑战^[2], 因此研究者需要寻找新的 DTN 安全问题解决方案。密钥管理方案分为 3 类: 集中式、非集中式和分布式, 但它们都不适合稀疏的 DTN 密钥管理任务, 如分布式方案没有考虑密钥管理中心的作用, 且降低了 DTN 资源利用率; 而集中式密钥管理方案不能保证密钥管理的实时性。

Seth 等^[3]将基于身份的分层密码系统(HIBC)引入 DTN 中, 用以构造 DTN 安全通信体系。针对 DTN 的特点, Kate 等^[4]提出了一种基于身份的匿名认证方案, 且给出了具体的协议设计方案。Asokan 等^[5]认为 DTN 现有的安全体系与传统的密码学技术相比, 在数据机密性方面, 基于身份的密码学(IBC)较适合 DTN 的安全体系。初始密钥协商是 DTN 安全体制中的一个难点, Defrawy 等^[6]利用社会网络原理实现了 DTN 的认证方案, 并使用真实数据验证了所给出的认证方案。Bhutta 等^[7]认为单一的密钥管理方案难以满足 DTN 的安全需要, 针对不同的 DTN, 应设计

不同的密钥传输与协商协议来应对; 他们给出了可在 DTN 中应用的轻量级密钥管理和 AAA 安全认证框架, 这在一定程度上解决了认证与授权、DoS 攻击以及匿名性等 DTN 安全问题。

上述密钥管理方案适合延时较短的地面与卫星间的通信网络, 密钥管理中心能够提供实时密钥管理服务, 但该类方案不适合长延时、间断连通的深空 DTN 组密钥管理任务需要。在 DTN 环境中, 密钥具有很强的时效性, 为了保证私钥的安全性, 需要对私钥进行更新。由于节点的不稳定性, 可能会出现与网络连接不畅甚至是长时间中断连接的情况, 节点不能及时收到更新私钥的广播信息, 从而导致节点不能及时更新私钥。针对上述问题, 本文提出一种新颖的 DTN 密钥管理方案, 该方案不但可以实现私钥的分发与更新, 而且可以完成私钥的自愈功能, 即节点可以从某次收到的广播信息中恢复出以往没收到广播消息的时间段的私钥。

2 DTN 模型与攻击模型

2.1 DTN 模型

假设在 DTN 中每个通信组有一个管理节点 GM(如信号基站)和 n 个组成员节点组成(如通信卫星节点), GM 安全可信, 且拥有功能强大的设备, 因此管理节点的能力强大, 有较强的运算能力和存储能力, 主要负责会话的初始化、密钥的生成、密钥的分发更新、存储用户数据等; 组成员节点受设备限制, 资源有限, 没有足够的存储空间和运算模块, 通信信道受限; 管理节点通过安全的路径与用户节点进行通信, 用于在以后的会话中建立安全通信。在 DTN 网络中, 用户来访不受限制, 随时有新用户的加入和合法用户的撤销。在整个过程中, 物理安全方面的内容不加入讨论。

2.2 攻击模型

Burgess 等在文献[8]中指出, DTN 具有不可预测移动和断续连接的特点, 其网络路由协议可应对较强的网络攻击。但密钥产生易遭受到恶意节点的攻击。为了设计安全的分布式密钥生成协议, 本文假设存在一个较强的攻击模型, 其中包含可移动、强有力的攻击者。

1) 恶意攻击 I——假冒用户身份。DTN 缺

乏端到端的可信第三方的身份认证实体,攻击者可冒充诚实用户的身份以获得其他用户的信任。

2) 恶意攻击II——发布错误的共享密钥。被腐化的节点试图发布不一致(也可能是前后2次密钥协商)的共享密钥,使其他网络节点无法提取正确的加密参数。

3) 恶意攻击III——破坏共享密钥的传输。攻击者修改正在传输中共享密钥发动拒绝解密服务攻击(DoD, denial-of-decryption)。接收者收到无效的共享密钥,不能正确提取加密参数。

3 密钥管理方案

新的密钥管理方案包括初始化算法、私钥生成算法、私钥更新算法和非交互的会话密钥协商协议等。新方案涉及的节点包括离线根PKG节点、簇头节点及簇内节点。其中,离线根PKG在系统初始化时产生系统主密钥,为所有节点产生初始私钥,设定密钥更新参数;簇头节点负责直接为簇内节点生成私钥并定期更新,为新加入的簇内节点生成私钥等。

系统运行时间分为不同阶段, m 表示系统运行时间的最大阶段数。设 $1 \leq k \leq m$, $Time_k$ 表示系统运行到 k 阶段的时间参数。节点的私钥形式为 (M, D) ,其中,第一部分私钥(M)为静态私钥,在整个系统运行期间固定不变,确保任意多节点被捕获也不会影响其他未被捕获节点私钥的安全性;第二部分私钥(D)为动态私钥,随时间参数 $Time_k$ 定期更新。在本文方案中,动态密钥的设置使簇内普通节点的叛变不会影响其他节点私钥的泄露,且簇头节点的叛变只影响该簇内节点私钥的安全性。

3.1 初始化算法

初始化过程包括由离线根PKG生成系统参数、为所有节点预置私钥及簇头为簇内成员预置私钥等。在此过程中,根PKG与所有节点之间均采用物理安全方式通信,其安全性不属于本文考虑范畴。

3.1.1 建立系统参数

令 k 为安全参数,假设椭圆曲线密码系统的参数为 (p, q, E, F_q, P) ,其中, p 和 q 是大素数, E 是非奇异椭圆曲线, F_q 表示有 q 个元素的有限

域, F_q^* 表示 F_q 中的非零元集合。 P 是 E 的生成元。 G 为椭圆曲线上的点组成的 q 阶加法循环群, $e: G \times G \rightarrow G_T$ 为 E 上一个可计算的非退化的双线性对,其中, G_T 是 q 阶乘法循环群。令 G^* 表示 G 中除去单位元的集合。该算法执行如下步骤产生系统参数。

步骤1 选择一个随机生成元 $P_0 \in G$ 。

步骤2 从 F_q^* 中随机选择主私钥 m_0 ,并计算PKG的公钥为 $W_1 = m_0 P_0$ 。

步骤3 给定主私钥 m_0 和系统公共参数,PKG计算 $M_i = m_0 H_1(ID_i)$,在离线状态下将 M_i 安全地传递给身份为 ID_i 的节点。

最终系统参数 $params$ 和主私钥 $master-key$ 分别为

$$params = \{q, G, G_T, P_0, e, H, H_1, Time_k\}$$

$$master-key = m_0$$

其中, $H: F_q \rightarrow F_q$, $H_1: \{0, 1\}^* \rightarrow G^*$ 为散列函数。

3.1.2 在线系统运行初始化算法

组网时,根据预先设置的分簇算法选举出簇头节点。簇头节点为簇内节点分发私钥。本文方案为节点预置了固定不变的私钥部分(M),利用该部分私钥实现了在线的身份认证,并且在线私钥分发和更新过程中的秘密信息可直接使用签名方案^[9]而无需另建安全通道。

选取 U 作为簇成员节点的集合, $U = \{u_1, u_2, \dots, u_n\}$,用 ID_i 表示节点 u_i 的公开身份。节点 u_i 的生命期记为 $LF_{i,v}^i \in [\text{时间段 } l, \text{时间段 } v]$,其中, $1 \leq l \leq v \leq m$,限定每个时间段的合法节点(不含撤销节点)的数目不大于 t 。具体算法如下。

步骤1 选取 t 次多项式 $h(x) = a_0 + a_1x + \dots + a_tx^t \pmod{q}$, $x, a_i \in F_q$, $i = 0, 1, \dots, t$ 。

步骤2 选取 $H(\cdot)$ 为散列函数,且 $H(x)^j = \begin{cases} H(H(x)^{j-1}), & j \geq 2 \\ H(x), & j = 1 \end{cases}$, $H(\cdot)$ 的定义域和值域在有限域 F_q 中。

步骤3 簇头从有限域 F_q 中随机选择2个随机数:前向密钥种子(FS, forward seed)和后向(BS, backward seed)密钥种子。

步骤4 簇头选择 m 个独立不相关 t 次多项式 $h_1(x), h_2(x), \dots, h_m(x)$ 。

步骤 5 簇头将赋予其的秘密身份 $id_i \in F_q$ 、与其生命期相对应的秘密 $S_i = \{h_1(id_i), h_2(id_i), \dots, h_v(id_i)\}$ 和 $SFK_i = H(FS)$ 以签密方式发送给节点 u_i 。

3.2 私钥生成算法

生成私钥需要进行如下步骤。

步骤 1 簇头节点计算 $d_1 = H(FS) + H(BS)^m$, 对于节点 u_i , 计算私钥 $D_C = d_1 H_1(ID_i \parallel Time_1)$ 。

步骤 2 簇头节点将 D_C 以签密的方式发送给节点 ID_C 。

初始化完成后, 簇头节点 ID_B 的私钥为 $(M_B, D_B) = (m_0 H_1(ID_B), d_1 H_1(ID_B \parallel Time_1))$, 簇内节点 ID_C 的私钥为 $(M_C, D_C) = (m_0 H_1(ID_C), d_1 H_1(ID_C \parallel Time_1))$, 其中, M_C 为系统私钥, 在整个系统运行过程中不会改变, D_C 为动态私钥, 定期更新。

3.3 私钥定期更新算法

系统运行到下一个时间段 $Time_k$ 时, 会进行密钥更新。

步骤 1 簇头节点选择当前时间段的秘密值 $d_k = H(FS)^k + H(BS)^{m-k+1}$, 并计算 $d_k H_1(ID_B \parallel Time_k)$ 。

步骤 2 簇头随机选择混淆数值 $Z_k \in F_q$, 设 $BK_k = H(BS)^{m-k+1}$, 设 $U' = U - \{\text{撤销的节点}\}$, 计算 $A_k(x) = Z_k \prod_{i=1}^{|U'|} (x - id_i) + 1 \in F_q[x]$, $u_i \in U'$; 计算 $W_k(x) = A_k(x)BK_k + h_k(x)$; 广播 $W_k(x)$ 。

步骤 3 节点 u_i 接到广播消息 $W_k(x)$ 后, 首先利用自身秘密 $h_k(id_i)$ 计算 $BK_k = \frac{W_k(id_i) - h_k(id_i)}{A_k(id_i)}$,

然后计算当前时间段的前向散列值 $FK_k = H(SFK_i)^{k-1} = H(FS)^k$, 最后计算 $d_k = FK_k + BK_k$ 。

步骤 4 节点 u_i 计算 $d_k H_1(ID_i \parallel Time_k)$ 。

3.4 私钥自愈算法

生命期为 $[j_1, j_3]$ 的节点 u_i 在时间段 j_2 中收到广播信息 $W_{j_2}(x)$, 在遗失以前时间段 j ($j_1 < j < j_2 \leq j_3$) 中私钥的情况下, 节点通过如下过程可以恢复 d_j 。

步骤 1 节点 u_i 从 $W_{j_2}(id_i)$ 中解得 $BK_{j_2} = H(BS)^{m-j_2+1}$, 计算 $BK_j = H(BK_{j_2})^{j_2-j} = H(BS)^{m-j+1}$ 。

步骤 2 节点 u_i 利用自身所保存的秘密计算 $FK_j = H(SFK_i)^{j-j_1} = H(FS)^j$, 并计算 $d_j = FK_j + BK_j$ 。

步骤 3 节点 u_i 计算 $d_j H_1(ID_i \parallel Time_j)$ 。

3.5 新节点加入

假设当前时间段为 $Time_j$, 新节点 ID_D 加入簇头为节点 ID_{II} 的簇内, 本算法具体步骤如下。

步骤 1 ID_{II} 通过双向认证协议认证 ID_D 身份, 之后赋予节点 ID_D 一个秘密身份 id_i 。

步骤 2 ID_{II} 计算并通过签密算法将秘密 $S_i = \{h_j(id_i), h_{j+1}(id_i), \dots, h_v(id_i)\}$ 、 id_i 和 $SFK_i = H(FS)^j$ 发送给 ID_D 。

步骤 3 ID_{II} 计算并通过签密算法将私钥 $d_j H_1(ID_D \parallel Time_j)$ 发送给 ID_D 。 ID_D 在该时间段的私钥为 $(m_0 H_1(ID_D), d_j H_1(ID_D \parallel Time_j))$ 。

3.6 非交互的会话密钥协商协议

假设簇头节点 ID_B 的私钥为 $(m_0 H_1(ID_B), d_k H_1(ID_B \parallel Time_k))$, 簇内节点 ID_C 的私钥为 $(m_0 H_1(ID_C), d_k H_1(ID_C \parallel Time_k))$, 簇内节点 ID_D 的私钥为 $(m_0 H_1(ID_D), d_k H_1(ID_D \parallel Time_k))$ 。

1) 簇内节点 ID_C 、 ID_D 之间的会话密钥协商

簇内节点 ID_C 使用自己的私钥计算会话密钥 $k_{CD} = e(m_0 H_1(ID_C), H_1(ID_D)) e(d_k H_1(ID_C \parallel Time_k), H_1(ID_D \parallel Time_k))$

簇内节点 ID_D 使用自己的私钥计算会话密钥

$$k_{DC} = e(m_0 H_1(ID_D), H_1(ID_C)) e(d_k H_1(ID_D \parallel Time_k), H_1(ID_C \parallel Time_k))$$

由于

$$\begin{aligned} k_{CD} &= e(m_0 H_1(ID_C), H_1(ID_D)) e(d_k H_1(ID_C \parallel Time_k), H_1(ID_D \parallel Time_k)) \\ &= e(H_1(ID_C), H_1(ID_D))^{m_0} e(H_1(ID_C \parallel Time_k), H_1(ID_D \parallel Time_k))^{d_k} \\ &= e(H_1(ID_C), m_0 H_1(ID_D)) e(H_1(ID_C \parallel Time_k), d_k H_1(ID_D \parallel Time_k)) \\ &= e(m_0 H_1(ID_D), H_1(ID_C)) e(d_k H_1(ID_D \parallel Time_k), H_1(ID_C \parallel Time_k)) \end{aligned}$$

因此 $k_{CD} = k_{DC}$ 。

2) 簇头节点 ID_B 与簇内节点 ID_C 之间的会话密钥协商

簇头节点 ID_B 使用自己的私钥计算会话密钥

$$k_{BC} = e(m_0 H_1(ID_B), H_1(ID_C)) e(H_1(ID_B \parallel Time_k), H_1(ID_C \parallel Time_k))^{d_k}$$

$$k_{CB} = e(m_0 H_1(ID_C), H_1(ID_B)) e(d_k H_1(ID_C \parallel Time_k), H_1(ID_B \parallel Time_k))$$

由于

$$\begin{aligned} k_{BC} &= e(m_0 H_1(ID_B), H_1(ID_C)) e(H_1(ID_B \parallel Time_k), H_1(ID_C \parallel Time_k))^{d_k} \\ &= e(H_1(ID_B), H_1(ID_C))^{m_0} e(H_1(ID_B \parallel Time_k), H_1(ID_C \parallel Time_k))^{d_k} \\ &= e(H_1(ID_B), m_0 H_1(ID_C)) e(H_1(ID_B \parallel Time_k), d_k H_1(ID_C \parallel Time_k)) \\ &= e(m_0 H_1(ID_C), H_1(ID_B)) e(d_k H_1(ID_C \parallel Time_k), H_1(ID_B \parallel Time_k)) \end{aligned}$$

因此 $k_{CB} = k_{BC}$ 。

4 方案分析

结合 DTN 环境的特点, 衡量在 DTN 环境中实际运行的密钥管理方案, 通常考虑安全性和资源开销这 2 个方面性能。

4.1 安全性分析

1) 本文方案的密钥更新过程中, 所有节点可抵御各种主动攻击。

这些主动攻击包括: 利用伪造、重放、假冒等手段欺骗合法节点, 从而获取系统秘密信息的攻击方式。在密钥分发过程中, 本文方案可抵御以下主动攻击。

①假冒攻击: 节点之间执行基于私钥 $m_0 H_1(ID_i)$ 的双向认证, 攻击者不可能伪造节点私钥来冒充合法节点, 因为认证的关键是计算 $k_{ji} = e(m_0 H_1(ID_j), X_i)^{R_i}$ 或 $k_{ij} = e(m_0 H_1(ID_i), X_j)^{R_j}$, 而根据 $m_0 P_0$ 、 $R_i H_1(ID_i)$ 、 $R_j H_1(ID_j)$ 计算 k_{ij} (或 k_{ji}) 可以归约于一个 CBDH 困难问题。

②重放攻击: 节点的双向认证采用的挑战/应答方式, 能有效抵抗重放攻击; 密钥更新过程中, 簇内节点产生的部分私钥是采用基于身份签名传输的, 攻击者若重放以前获得的数据, 但由于缺少私钥 $m_0 H_1(ID_i)$ 或签名过程选择的随机数 b , 也无法解密得到用户的私钥份额或部分私钥。

③内部攻击: 由于所有节点在离线状态下预装了私钥 $m_0 H_1(ID_i)$, 任何一个恶意节点 (被捕获) 都不能冒充其他合法节点, 也不能掌握其他任何

合法节点的全部私钥信息。假设节点的私钥为 $(m_0 H_1(ID_i), d_k H_1(ID_i \parallel Time_k))$, 即使攻击者捕获了某个节点, 攻击者只能获得 d_k , 不能获得 m_0 。这是因为根据可知的 $m_0 H_1(ID_i)$ 和 $H_1(ID_i)$, 求解 m_0 可以归约于一个 ECDLP 困难问题。

2) 本文方案的密钥分发和密钥更新过程能够抵御被动攻击。

①攻击者不能通过监听信道公开的系统参数中获得系统私钥信息。本文方案公开的与主密钥有关的系统参数有 P_0 、 $m_0 P_0$ 等, 而计算系统私钥 m_0 则将面临 ECDLP 困难问题。

②由于本方案中节点的私钥信息都通过签名方案传输, 所以不需要另外建立安全信道, 即使攻击者得到了会话记录, 也无法得到用户的私钥。

3) 本文方案具有遗失密钥的自愈能力、合法簇内节点可正确计算密钥的能力、簇头节点具备撤销能力。

证明 从上文所述可以看出, 节点可自愈计算出以前时间段的遗失密钥, 合法簇内节点也正确计算当前时间段私钥的能力。

簇头的撤销能力是指被撤销的节点不能正确计算当前时间段私钥的能力, 即节点在其生命周期未结束的情况下被簇头强制撤销。

设 $j_1 < j_3 < j_4 < j_5 \leq j_2$, 生命周期为 $[j_1, j_2]$ 的节点 u_i 在会话 j_4 阶段被簇头撤销, 但 u_i 希望参与会话 j_5 的通信。 U_i 利用加入簇时获得的秘密值 FK^{j_1} 可以得到 FK^{j_5} , 但由于被撤销节点 $u_i \notin U'$, 故 $A_{j_5}(id_i) \neq 1$, 于是无法从 $A_{j_5}(id_i) \neq 1$ 中解得正确的 BK_{j_5} , 从而无法得到正确的秘密值 d_{j_5} 。簇头节点的撤销能力得证。

4.2 效率分析

资源开销主要包含 3 种类型: 计算花销、存储花销、通信花销。由于用户节点 (如通信卫星) 电源能力受限, 同时通信带宽受限。因此衡量 DTN 密钥管理方案性能优劣的指标主要包括通信开销和计算开销, 本节从这 2 个方面来进行分析。在本文方案中, 系统初始化部分由离线的可信第三方完成, 因此考虑系统的性能, 主要需考虑节点的密钥分发过程和节点之间的会话密钥生成过程。

新方案是基于身份的密钥分发协议, 节点的公钥为其身份信息, 不需要额外的公钥生成计算

和信息传输。新方案的实现主要基于有限域上的椭圆曲线密码学, 该体制具有密钥短、计算效率高、显著优点, 如在安全性上, 160 bit 的椭圆曲线密码的安全性相当于 1 024 bit 的 RSA 的安全性, 计算效率高。因此, 本文方案相比基于传统公钥算法(如 RSA、ElGamal 算法)的 DTN 密钥管理方案具有更低的通信和计算代价, 因而更适合于 DTN。

在密钥分发过程中, 广播信息 $W(x)$ 使用广播多项式对被撤销和无关用户进行屏蔽, 不需要其他的多余广播信息, 从而减少了通信消耗。由于采用了散列链的结构, 用户不需要存储过多的冗余信息来恢复遗失的密钥, 广播信息数据量的开销只有 $W(x)$, 其广播通信所要占据的带宽大小为 $O((t+1)\lg q)$ 。

新方案的一个主要特点是在传输节点密钥时无需安全信道, 这大大节省了系统带宽和节点能量。具体而言, 在传送秘密信息时, 直接对待传递的消息进行签密, 使接收方仅使用预先设置的静态系统私钥即可解密, 从而无需预先在发送方和接收方之间建立任何安全通道。

密钥协商是 DTN 实现保密通信的关键环节。新方案中密钥协商算法主要考虑端到端的会话密钥协商, 使用的是非交互的基于身份的密钥协商算法, 无需交互信息就能在 2 个节点之间建立会话密钥, 有效地降低了端到端会话密钥协商的通信开销和计算开销。

5 结束语

针对现有 DTN 分簇式密钥管理中存在的问题, 本文提出了一个允许私钥自愈的、分簇的密钥管理方案。该方案不但可以完成对节点私钥的分发与更新, 还可以实现节点以前私钥的自愈, 特别适合网络延时大、间歇性连接的 DTN。由于引入了静态设置的系统私钥, 因此避免了传统方案中安全信道的使用。本文详细阐述了系统建立过程、用户密钥产生和发布过程、用户私钥更新过程及会话密钥建立过程, 并分析了方案的安全性及性能。

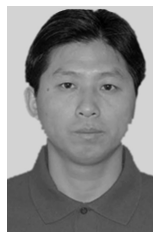
参考文献:

- [1] FARRELL S, CAHILL V. Security considerations in space and delay tolerant networks[C]//IEEE International Conference on Space Mission Challenges Fox Information Technology. 2006:

29-38.

- [2] 谢永明. 基于分布式密钥产生系统的延迟容忍网络安全研究[D]. 长沙: 中南大学, 2012.
XIE Y M. Research on delay tolerant network security based on the distributed key generation system[D]. Changsha: Central South University, 2012.
- [3] SETH A, KESHAV S. Practical security for disconnected nodes[C]//The International Conference on Secure Network Protocols. 2005:31-36.
- [4] KATE A, ZAVERUCHA G M, HENGARTNER U. Anonymity and security in delay tolerant networks[C]//The International Conference on Security and Privacy in Communications Networks and the Workshops. 2007:504-513.
- [5] ASOKAN N, KOSTIAINEN K, GINZBOORG P. Towards securing disruption tolerant networking[R]. 2007.
- [6] DEFRAWY K E, SOILS J, TSUDIK G. Leveraging social contacts for message confidentiality in delay tolerant networks[C]//IEEE International Computer Software and Applications Conference. 2009: 271-279.
- [7] BHUTTA N, ANSA G, JOHNSON E. Security analysis for delay/disruption tolerant satellite and sensor networks[C]//The International Workshop on Satellite and Space Communications. 2009: 385-389.
- [8] BURGESS J, BISSIAS G D, COMER M D, et al. Surviving attack-disruption tolerant networks without authentication[C]//ACM International Symposium on Mobile Ad Hoc Networking and Computing. 2007: 61-70.
- [9] 李发根, 胡予濮, 李刚. 一个高效的基于身份的签密方案[J]. 计算机学报, 2006, 29(9): 1641-1647.
LI F G, HU Y P, LI G. An efficient identity-based signcryption scheme [J]. Journal of Computers, 2006, 29 (9): 1641-1647.

作者简介:



李德全 (1969-), 男, 博士, 四川乐山人, 北京天地一体化信息安全工程技术研究中心高级工程师, 主要研究方向为信息安全。

张习勇 (1975-), 男, 博士, 湖北武穴人, 天地一体化信息技术国家重点实验室高级工程师, 主要研究方向为密码学。

张婷婷 (1989-), 女, 博士, 河南驻马店人, 天地一体化信息技术国家重点实验室工程师, 主要研究方向为密码学。

郭冠军 (1978-), 男, 硕士, 河南郑州人, 北京航天自动控制研究所工程师, 主要研究方向为异构计算与高速处理计算平台。