

文章编号:1001-9081(2016)11-3108-05

DOI:10.11772/j.issn.1001-9081.2016.11.3108

物联网环境下移动节点可信接入认证协议

张 鑫^{1,2*}, 杨晓元^{1,2,3}, 朱率率^{1,2}, 杨海滨^{1,3}

(1. 武警工程大学 电子技术系, 西安 710086; 2. 武警工程大学 网络与信息安全武警部队重点实验室, 西安 710086;

3. 武警工程大学 信息安全研究所, 西安 710086)

(*通信作者电子邮箱 zhang0551xin@163.com)

摘要:无线传感器网络(WSN)中的移动节点缺乏可信性验证,提出一种物联网(IoT)环境下移动节点可信接入认证协议。传感器网络中移动汇聚节点(Sink 节点)同传感器节点在进行认证时,传感器节点和移动节点之间完成相互身份验证和密钥协商。传感器节点同时完成对移动节点的平台可信性验证。认证机制基于可信计算技术,给出了接入认证的具体步骤,整个过程中无需基站的参与。在认证时利用移动节点的预存的假名和对应公私钥实现移动节点的匿名性,并在CK(Canetti-Krawczyk)模型下给出了安全证明。在计算开销方面与同类移动节点认证接入方案相比,该协议快速认证的特点更适合物联网环境。

关键词:物联网;可信认证;移动节点;CK 安全模型

中图分类号:TP309.7 **文献标志码:**A

Trusted access authentication protocol for mobile nodes in Internet of things

ZHANG Xin^{1,2*}, YANG Xiaoyuan^{1,2,3}, ZHU Shuaishuai^{1,2}, YANG Haibing^{1,3}

(1. Department of Electronic Technology, Engineering College of Chinese People's Armed Police Force, Xi'an Shaanxi 710086, China;

2. Key Laboratory of Network & Information Security under People's Armed Police,

Engineering College of Chinese People's Armed Police Force, Xi'an Shaanxi 710086, China;

3. Institute of Information Security, Engineering College of Chinese People's Armed Police Force, Xi'an Shaanxi 710086, China)

Abstract: In view of the problem that mobile nodes lack trusted verification in Wireless Sensor Network (WSN), a mobile node access authentication protocol was proposed in Internet of Things (IoT). Mutual authentication and key agreement between the sensor nodes and mobile sink nodes were realized, when they were authenticated. At the same time, the trustworthiness of mobile node platform was authenticated by sensor nodes. The authentication scheme was based on trusted computing technology without using base station and its concrete steps were described in detail. Pseudonyms and the corresponding public/private keys were used in authentication to achieve the protection of the user privacy. The proposed scheme was provably secure in the CK (Canetti-Krawczyk) security model. Compared to similar mobile node schemes, the protocol is more suitable for fast authentication in IoT, with less computation and communication overhead.

Key words: Internet of Things (IoT); trusted authentication; mobile node; Canetti-Krawczyk (CK) security model

0 引言

无线传感器作为物联网(Internet of Things, IoT)的重要组成部分,得到了广泛的应用。物联网主要是由感知子网、传输子网和应用子网组成的混合异构网络。无线传感器网络(Wireless Sensor Network, WSN)是由大量廉价的、计算和通信能力弱、电量有限的传感器节点组成。传感器节点收集到感知数据后,节点以移动自组网的方式将数据发送给基站的后台服务器,实现任意时间对特定区域的信息采集、处理以及分析。通常部署的传感器网络节点能力有所差异,主要分为普通传感器节点和簇头节点。簇头节点比普通传感器节点拥有更加强的计算和通信能力,所以普通传感器节点一般将采集到数据发送给簇头节点,然后簇头节点将簇内的数据统一上传给基站。

文献[1–2]提出在传感器网络中加入移动汇聚节点来收集感知子网中的数据,以减少传感器节点在传输感知数据时的能量开销,延长传感器的使用寿命。在传感器网络中引入移动汇聚节点后带来诸多便利,但同时移动汇聚节点同传感器节点之间的安全认证成为关键的问题。传感器必须能够确定自己所采集的感知数据被传递到了合法、可信的移动汇聚节点中,而同时移动汇聚节点也必须能够确认接收到合法传感器发送的感知数据。同时未来在物联网中,移动节点也将大量存在,深入研究移动节点在物联网中的接入认证安全性问题十分必要。

为了确保移动设备的安全,同时考虑到移动终端在处理器、电源容量和存储空间等限制,可信计算组织(Trusted Computing Group, TCG)^[3]的移动电话工作组以可信平台模块(Trusted Platform Module, TPM)为基础针对移动设备的特

收稿日期:2016-05-12 ;修回日期:2016-06-15。

基金项目:国家自然科学基金资助项目(61402530, 61272492, 61572521); 武警工程大学基础研究基金资助项目(WJY201520)。

作者简介:张鑫(1991—),男,安徽合肥人,硕士研究生,主要研究方向:信息安全、可信计算; 杨晓元(1959—),男,湖南湘潭人,教授,硕士,主要研究方向:信息安全、密码学; 朱率率(1985—),男,山东淄博人,讲师,主要研究方向:信息安全、可信计算、密码学; 杨海滨(1982—),男,河北林榆人,讲师,硕士,主要研究方向:信息安全、密码学。

性重新定义和修改,发布可信移动模块(Mobile Trusted Module, MTM)规范。

现有移动 Sink 节点的研究工作较多关注节点的数据收集和生存周期^[4-5],传感器网络在引入移动节点后带来的安全和认证的问题受到了越来越多的关注。移动 Sink 节点安全认证方面,文献[6]提出了一个基于双线性配对认证与密钥协商方案,安全性分析讨论了重放攻击、伪装攻击等各种攻击,计算复杂度满足无线传感器网络环境要求。文献[7]提出了物联环境下的组合安全的漫游认证协议,在实现移动传感器节点的身份认证同时对移动节点的隐私进行保护。文献[8]通过移动节点持有漫游证明信息,完成物联网移动节点的匿名认证。文献[9]提出了无线传感器网络下双因素的身份认证,但文献[10]指出其相互认证方面的安全漏洞,并提出新的双向认证方案。对无线环境下移动节点的可信接入,国内外人员进行了许多研究。在文献[11]提出了可信无线匿名认证协议,对移动用户身份和终端平台可信性进行认证,认证每个阶段使用不同的密钥保证匿名性,但协议执行时外地服务器都需要在本地服务器协助下才完成漫游信息的证明。文献[12]提出了移动互联网下移动可信匿名漫游协议,外地网络通过本地为移动终端颁发的漫游证明完成认证,但用户变换漫游地时需要重新向本地服务器申请漫游证明。

针对现有物联网下移动节点认证缺乏可信验证,本文提出一种物联网下可信接入协议,研究了移动汇聚节点和传感器簇头节点间高效切换认证。协议通过基于身份的密钥交换机制实现用户认证和密钥交换,利用可信计算技术完成平台的完整性验证。同现有物联网中的移动节点接入协议相比具有更高的效率和灵活性。

1 协议框架模型

如图 1 所示,物联网移动节点认证模型主要由物联网管理中心(CA-IoT)、移动汇聚终端(Mobile Sink Node, MSN)、基站(Base Station, BS)、传感器节点(Sensor)和簇头节点(Cluster Head, CH)组成。

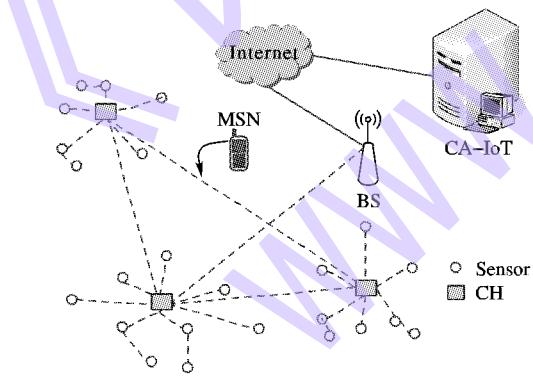


图 1 物联网移动节点认证基本架构

协议中的网络接入实体 MSN 需要同簇头节点 CH 完成用户身份认证以及密钥协商,同时 CH 完成对 MSN 平台的身份和完整性的验证,以免接入不可信移动节点。为简化协议,本文给出以下假设:

- 1) 协议中的移动节点具有可信平台模块;
- 2) 同传统无线网络一样,传感器节点和簇头节点已经建立了安全信道;

3) MSN 已经向证书中心申请了身份认证证书 $Cert(AIK_p)$ 。

2 认证协议

本文使用的相关符号定义如下: n 为大素数, r_A 代表 A 选取的随机数, ID_A 代表 A 的身份标识, pid_i 表示用户所使用的第 i 个假名; $Cert_A$ 代表 A 的身份证书; $\langle PK_A, SK_A \rangle$ 代表 A 的一对公私钥; $\langle AIK_p, AIK_s \rangle$ 代表安全芯片(TPM 或 MTM)的身份密钥; T_s 为时间戳; SK_A^{-1} 代表 A 的私钥 SK_A 的求逆运算值,并且要使得用户的私钥求逆运算值与公钥的乘积为常数,即 $SK_A^{-1}PK_A = Q$ (Q 为常数)。

本文使用的相关运算定义如下: $E(K, m)$ 和 $D(K, c)$ 代表使用对称密钥进行加密/解密; $ENC(SK, m)$ 和 $DNC(PK, c)$ 分别代表使用非对称密钥进行加密/解密运算; $SIG_A(m)$ 代表 A 对消息 M 进行数字签名; $H(m)$ 代表标准散列算法。

2.1 系统初始化

在系统初始化阶段,MSN 使用自身的真实身份向 CA-IoT 注册时,CA-IoT 提供一系列不可链接的随机假名身份(Pseudonym ID, PID), $PID = \{pid_1, pid_2, \dots, pid_n\}$ 。本地验证服务器(Home Authentication Server, HAS)将会预先给每个假名身份 $pid_i \in PID$ 公钥 pk_{pid_i} 和相应的私钥 sk_{pid_i} ,然后 CA-IoT 将所有的元组 $(pid_i, pk_{pid_i}, sk_{pid_i})$ 安全地发送给 MSN。在当前的工作中文献[13],就对预先装载长期使用假名的匿名密钥和相关证书的存储空间进行详细定量的研究。本文使用的预装载的假名,存储开销是在合理范围内的。

假名 pid_i 的公钥 pk_{pid_i} 和私钥 sk_{pid_i} 通过以下具体步骤生成。CA-IoT 初始化:令 G 为一个 q 阶的循环加法群, G_T 为一个 q 阶的循环乘法群。令 P 为 G 的一个任意的生成器,且 $\hat{e}: G \times G \rightarrow G_T$ 为双线性映射。CA-IoT 选择一个随机数 $s \in \mathbb{Z}_q^*$ 作为主密钥, $P_{pub} = sP$ 为公钥,另外 HAS 选择了两个安全的散列函数 H_1 和 H_2 ,其中 $H_1: \{0, 1\}^* \rightarrow G, H_2: \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ 。CA-IoT 对每个 PID 计算 $H_1(pid_i)$ 作为 pid_i 的公钥, $sH_1(pid_i)$ 作为其私钥。最后,CA-IoT 公开发布公共参数 $params_{HAS}: \{G, G_T, q, P, P_{pub}, H_1, H_2\}$ 。

2.2 MSN 同基站认证服务器 BS 可信认证

MSN 在进行感知数据收集前,将自身平台的完整性信息发送给基站认证服务器 BS 完成平台可信性的验证。时间戳 T_s 用于抵御重放攻击,随机数 $Nonce$ 用于保证消息的新鲜性。

1) 当 BS 收到一个验证请求消息,BS 生成随机数 $r_{BS} \in \mathbb{Z}_q^*, sid$ 为会话标识。

$BS \rightarrow MSN: sid, ID_{BS}, r_{BS}, Nonce$

2) MSN 收到消息后,对自身平台的可信性信息进行收集。MSN 调用 TPM 指令 $TPM_PcrRead()$ 获取平台配置寄存器值 $PCRs$ 值,从 TPM 中读取证明身份密钥 AIK_p ,调用 $TPM_Quote()$ 对 $PCRs$ 进行签名 $SIG_{TPM}(PCRs \parallel r_{BS}) = ENC(AIK_p, PCRs \parallel r_{BS})$,生成平台完整性验证信息, SML (Store Measurement Log) 为度量日志; $PIV = SML \parallel PCRs \parallel Cert(AIK_p) \parallel SIG_{TPM}(PCRs, r_{BS})$,利用 BS 的公钥 pk_{BS} 进行加密 $C = ENC(pk_{BS}, PIV)$ 。

$MSN \rightarrow BS: sid, C, Nonce$

3) BS 收到消息后执行以下验证操作。

① 使用自身私钥解密 $PIV = DEC(sk_{BS}, C)$, 获得平台可信性验证消息。利用 AIK_p 验证 $SIG_{TPM}(PCRs, r_{BS})$, 获得 $SML, PCRs$ 。

② 根据终端平台的可信验证策略, 验证平台的状态是否满足: 若不满足则拒绝 MSN 的接入; 若满足生成可信证明 $Tproof = SIG_{BS}(M_{proof}), M_{proof} = ID_{BS} \parallel EDate' \parallel N$ 。其中: $EDate'$ 为 BS 设定的可信证明有效期, N 为 BS 颁发给 MSN 可信证明序列号。

$BS \rightarrow MSN: sid, ID_{BS}, Tproof, M_{proof}, Nonce$

2.3 移动 Sink 节点接入认证

当簇头节点 CH 在 MSN 的直接通信范围内, MSN 提出接入认证申请;

1) MSN 选择一个未使用的假名身份 pid_j , 作为自己的身份。MSN 使用私钥 sk_{pid_j} 和消息 $M_j = (sid \parallel pid_j \parallel ID_{CH} \parallel Ts \parallel Nonce_{MSN})$ 计算签名 $\sigma_j = H_2(M_j) \cdot sH_1(pid_j)$ 。接着, MSN 选取秘密随机数 r_{MSN} , 计算 $D_{MSN} = (r_{MSN} + sk_{MSN})pk_{CH}$ 。

$MSN \rightarrow CH: M_j, \sigma_j, D_{MSN}, Tproof, M_{proof}$

2) CH 收到消息后执行以下验证操作, 检查时间戳 T_s , 以抵御重放攻击, CH 根据 $params_{CA}$, 来验证 $\hat{e}(\sigma_i, P) = \hat{e}(H_2(M_i) \cdot H_1(pid_i), P_{pub})$ 是否成立, 从而检查签名 σ_i 是否有效; 验证可信证明 $Tproof$ 签名的有效性。若未通过, 拒绝该连接, 否则发送消息。

CH 选择秘密随机数 r_{CH} , 计算 $D_{CH} = (r_{CH} + sk_{CH})pk_{MSN}$, 共享密钥 $K_{(CH, MSN)} = sk_{CH}^{-1}(r_{CH} + sk_{CH})D_{MSN}$ 验证码 $Aut = H_2(K_{(CH, MSN)} \parallel sid \parallel pid_j \parallel ID_{CH} \parallel Ts \parallel Nonce_{MSN} \parallel Nonce_{CH})$ 。

$CH \rightarrow MSN: sid, pid_j, ID_{CH}, Nonce_{CH}, D_{CH}, Aut$

3) MSN 收到消息验证时间戳, 并计算共享密钥 $K_{(MSN, CH)} = sk_{MSN}^{-1}(r_{MSN} + sk_{MSN})D_{CH}$, 生成 $Ver = H_2(K_{(MSN, CH)} \parallel sid \parallel pid_j \parallel ID_{CH} \parallel Ts \parallel Nonce_{MSN} \parallel Nonce_{CH})$, 若与 Aut 相同, 则 MSN 确定 CH 是合法并且建立了会话密钥 $K_{(MSN, CH)}$, 否则拒绝该连接。

3 协议分析

3.1 协议安全性

CK 安全模型^[14]的基本思想是基于模块化观点, 首先把协议定义在理想模型 (Authenticated-linksadversarial Model, AM) 中, 利用计算的不可区分性来定义理想模型中的安全性, 利用编译器将协议编译为现实模型 (Unauthenticated-linksadversarial Model, UM) 中的协议。理想模型 AM 表示认证的链路模型, 攻击者是被动的, 不能伪造消息, 只是忠实地传递消息同一消息一次。现实模型 UM 表示未认证链路模型, 在 UM 中的攻击者拥有 AM 中所有攻击外, 还具有伪造、篡改和重放消息的能力。

定义 1 设 π 是运行在 AM 中的 n 方消息驱动协议, π' 是运行在 UM 中的 n 方消息驱动协议。若对于任何 UM 敌手 U , 始终存在一个 AM 敌手 A 使得两个协议的全局输出在计算上是不可区分的, 则称协议 π' 在 UM 中仿真了 AM 中的协议 π 。

定义 2 编译器 C 是一个算法。它的输入和输出都是协议的描述。若一个编译器 C 对于任何协议 π , 均有协议 $C(\pi)$

在 UM 中仿真 π , 则这个编译器成为认证器。AM 中的协议可以由认证器转化为 UM 中的安全协议。

定义 3 会话密钥安全。若对于 AM 中的任何敌手 A , 当且仅当下列性质都满足时, 该协议在 AM 中是会话密钥安全的。

性质 1 未被攻陷的参与双方完整执行协议后, 参与者获得相同的密钥。

性质 2 敌手 A 进行测试会话查询攻击, 它猜中正确会话输出值 b 概率不超过 $1/2 + \varepsilon$, 其中 ε 是安全参数范围内可忽略的任意小数。

定理 1 假设 λ 是一个消息传输认证器, 即 λ 在 UM 中仿真了简单消息传输协议, 假设 C_λ 是在 λ 基础之上定义的一个编译器, 则 C_λ 也是一个认证器。

3.1.1 AM 中的漫游协议

为了简化协议证明过程, 将移动 Sink 节点接入认证抽象为协议 δ 。描述如下:

1) MSN 使用假名 pid_j 私钥 SK_{pid_j} 和消息 $M_j = (sid \parallel pid_j \parallel ID_{CH} \parallel Ts \parallel Nonce_{MSN})$ 计算签名 $\sigma_j = H_2(M_j) \cdot sH_1(pid_j)$ 。选取秘密随机数 r_{MSN} , 计算 $D_{MSN} = (r_{MSN} + sk_{MSN})pk_{CH}$ 。最后发送消息 $\{M_j, \sigma_j, D_{MSN}, Tproof, M_{proof}\}$ 。

2) CH 验证时间戳和签名 M_j 实现对 MSN 的身份验证。选择秘密随机数 r_{CH} , 计算 $D_{CH} = (r_{CH} + sk_{CH})pk_{MSN}$, 共享密钥 $K_{(CH, MSN)} = sk_{CH}^{-1}(r_{CH} + sk_{CH})D_{MSN}$ 验证码 $Aut = H_2(K_{(CH, MSN)} \parallel sid \parallel pid_j \parallel ID_{CH} \parallel Ts \parallel Nonce_{MSN} \parallel Nonce_{CH})$ 向 MSN 发送 $\{sid, pid_j, ID_{CH}, D_{CH}, Nonce_{CH}\}$

3) MSN 收到消息后验证时间戳。通过 D_{CH} 计算共享密钥 $K_{(MSN, CH)} = sk_{MSN}^{-1}(r_{MSN} + sk_{MSN})D_{CH}$, 最后由校验码 $Ver = H_2(K_{(MSN, CH)} \parallel sid \parallel pid_j \parallel ID_{CH} \parallel Ts \parallel Nonce_{MSN} \parallel Nonce_{CH})$, 若与 Aut 相同, 则 MSN 确定 CH 是合法并且建立了会话密钥 $K_{(MSN, CH)}$, 否则拒绝该连接。

定理 2 当签名、非对称加密、对称加密等算法均安全时, 协议 δ 在 AM 中是安全的。

证明 在 AM 中, 由于在协议交互的过程中, 参与者未被敌手 A 攻陷, 在协议执行完时 MSN 和 CH 获得正确的密钥的协商参数 D_{MSN} 和 D_{CH} , CH 计算会话密钥如下:

$$K_{(CH, MSN)} = sk_{CH}^{-1}(r_{CH} + sk_{CH})D_{MSN} = sk_{CH}^{-1}(r_{CH} + sk_{CH})(r_{MSN} + sk_{MSN})pk_{CH} = (r_{CH} + sk_{CH})(r_{MSN} + sk_{MSN})Q$$

MSN 计算会话密钥过程相同, 因此会话密钥 $K_{(CH, TMN)} = K_{(TMN, CH)}$, 所以协议 δ 满足会话密钥安全的性质 1。

命题 1 敌手 A 能以概率 P_0 区分会话密钥协商参数中的随机数, 敌手能以概率 P_1 攻破非对称加密算法, 则概率 P_0, P_1 都是可以忽略的。

协议中的会话都是经过公钥加密获得, 敌手 A 只能攻破 PK_{MSN} 和 PK_{CH} 才能获得密钥的协商参数 D_{MSN} 和 D_{CH} 。那么敌手 A 攻破共享密钥的概率为 P_0P_1 , 不被攻破的概率为 $1 - P_0P_1$ 。若敌手获得共享密钥, 则必有 $1 - P_0P_1 \ll P_0P_1$ (P_0P_1 远远大于 $1 - P_0P_1$) 成立, 即是 $P_0P_1 \gg 1/2$, 所以 P_0 和 P_1 是不可以忽略的。这同命题 1 相矛盾, 因此敌手 A 正确猜中会话密钥的概率不超过 $1/2 + \varepsilon$, 协议 δ 满足会话密钥安全的性质 2。

在 AM 中, 敌手 A 不能进行伪造、篡改和重放消息, 因此敌手仅能参与真实地将合法参与者产生的消息转发, 所以协

议 δ 在 AM 中是安全的。

3.1.2 认证器构造

协议中 CH 对 MSN 的认证信息流采用基于时间戳的签名认证器 $\lambda_{SIG,T}$, 文献[15]详细证明了认证器的安全性和匿名性。其具体过程如下:

1) A 先产生时间戳 T_A ,之后计算消息 M 的签名为 SIG ,将发送给 B。

2) B 收到 A 的认证消息,验证时间戳新鲜性,再验证消息 M 的签名 SIG 正确性,若验证均正确则 A 通过了 B 的合法性验证。

3.1.3 构造 UM 下会话安全协议

运用基于时间戳的签名认证器^[15],将协议 δ 直接转化为 UM 中会话安全密钥协议。由于协议中采用的签名算法,非对称签名算法安全且难解,所以 CK 安全模型编译 UM 中的协议 δ 是可证安全的。

3.2 正确性

在协议中移动汇聚节点同传感器节点实现了双向的身份认证。CH 对 MSN 的认证使用公钥算法,CH 验证签名是基于随机身份的签名,验证通过检查 $\hat{e}(\sigma_i, P) = \hat{e}(H_2(M_i) \cdot H_1(pid_i), P_{pub})$ 是否成立,具体验证过程如下:

$$\begin{aligned}\hat{e}(\sigma_i, P) &= \hat{e}(H_2(M_i) \cdot sH_1(pid_i), P) = \\ &= \hat{e}(H_2(M_i) \cdot H_1(pid_i), sP) = \\ &= \hat{e}(H_2(M_i) \cdot H_1(pid_i), P_{pub})\end{aligned}$$

由于在服务器 CA-IoT 才保存秘密数 $s \in \mathbf{Z}_q^*$,敌手无法通过公开参数 $params_{CA}$ 计算出 MSN 的私钥 $sH_1(pid_i)$,因此敌手无法伪造合法签名。敌手无法获得 CH 的私钥,生成共享密钥,则无法伪造合法的验证码 Aut 。在通信的过程中,对主要消息进行散列值运算保证消息的完整性,同时采用了时间戳和随机数保证消息的新鲜性并防止重放攻击。

会话密钥正确性如下:

$$\begin{aligned}K_{(CH,MSN)} &= sk_{CH}^{-1}(r_{CH} + sk_{CH})D_{MSN} = \\ &= sk_{CH}^{-1}(r_{CH} + sk_{CH})(r_{MSN} + sk_{MSN})pk_{CH} = \\ &= (r_{CH} + sk_{CH})(r_{MSN} + sk_{MSN})Q\end{aligned}$$

同样可得 MSN 生成的密钥 $K_{(CH,MSN)}$,因此会话密钥正确性成立。会话密钥由双方选择的秘密随机数 r_{CH} 和 r_{MSN} 共同决定,任何一方无法单独伪造合法密钥, r_{CH} 和 r_{MSN} 分别由 MSN 和 CH 安全保存,秘密随机数每次接入认证时才生成,从而保证了会话密钥的新鲜性。

3.3 平台可信性

在服务器安全可靠的情况下,MSN 的平台的软硬件配置信息不会泄露给网络之中的其他合法用户,也不会泄露给 CH,有效保护了平台的有效隐私性。当 MSN 在 CH 认证时,使用 BS 颁发的可信证明 T_{proof} 进行验证,由于可信证明 T_{proof} 是由是基站 BS 的签名,不包含 MSN 的平台度量值信息,使得 CH 或其他用户无法获得平台的配置信息。

3.4 接入认证灵活性

传统的移动节点接入认证方案采用三方结构^[7,16],验证时需要可信的第三方参与。两方漫游协议通常使用一些复杂的密码技术^[17]会给协议双方带来较高的计算开销。在本协议中,MSN 在身份验证和可信验证时,使用预存的假名 $PID = \{pid_1, pid_2, \dots, pid_n\}$ 及其公私钥对进行匿名通信。CH

事先已发送的公共参数 $params_{CA}$, CH 便可以利用 $params_{CA}$,对移动节点进行独立验证。因此 CH 无需同基站 BS 进行通信交互,减少通信延迟及验证服务器负担。

3.5 性能分析与评估

物联网中感知子网中的节点计算能力有限,方案中节点不能有过多的计算开销。协议执行效率由认证过程中的各个实体的运算开销来衡量,主要包括对称加解密、非对称加解密、双线性对运算、指数运算、消息验证码、消息交换轮数。方案的分析主要对比文献[7]和文献[12],计算开销分别是 MSN-CH-BS 三方,消息交换轮数为 MSN-CH/CH-BS 之间交互的轮数。相比文献[7]虽消息交换轮数多一轮,但是高运算量的操作少。文献[12]采用了三方的验证方式,基站 BS 进行较多运算操作。整体相比,本文方案具有通信延迟低、执行效率高特点。

表 1 三种方案效率分析

运算开销	文献[7]方案	文献[12]方案	本文方案
对称加解密	—	1/1/2	—
非对称加解密	1/2/0	—	—
双线性对运算	0/2/0	—	0/1/0
签名及验证	1/1/0	—	1/1/0
消息验证码	—	1/2/3	1/1/0
消息交换轮数	1/0	1/1	2/0

注:—表示方案未涉及此运算。

4 结语

物联网中移动节点缺乏平台的可信认证需求,本文提出物联网环境下移动节点可信接入认证协议。移动节点在同簇头节点进行切换认证时,将身份认证同平台可信性认证结合起来,实现了高效的可信接入。移动节点使用预存的假名保证匿名性,假名与用户真实身份没有关联,实线了身份和位置等信息机密性和隐私保护,分析表明协议计算开销相比相关同类认证减少并且接入认证更加灵活、自主。

参考文献:

- [1] YUN Y S, XIA Y, BEHDANI B, et al. Distributed algorithm for lifetime maximization in a delay-tolerant wireless sensor network with a mobile Sink [J]. IEEE Transactions on Mobile Computing, 2013, 12(10): 1920–1930.
- [2] BEHDANI B, SMITH J C, XIA Y. The lifetime maximization problem in wireless sensor networks with a mobile sink: mixed-integer programming formulations and algorithms [J]. LIE Transactions, 2013, 45(10): 1094–1113.
- [3] Trust Computing Group. TPM main part 1: design principles specification, version 1.2 revision 62 [S]. Geneva: International Organization for Standardization (IOS), 2009.
- [4] YANG Y, FONOAGE M I, CARDEI M. Improving network lifetime with mobile wireless sensor networks [J]. Computer Communications, 2010, 33(4): 409–419.
- [5] VUPPUTURI S, RACHURI K K, MURTHY C S R. Using mobile data collectors to improve network lifetime of wireless sensor networks with reliability constraints [J]. Journal of Parallel & Distributed Computing, 2010, 70(7): 767–778.
- [6] ZHANG J, LI X, MA J, et al. Secure and efficient authentication scheme for mobile sink in WSNs based on bilinear pairings [J]. International Journal of Distributed Sensor Networks, 2014, 2014(1): 84–88.
- [7] 王良民, 姜顺荣, 郭渊博. 物联网中移动 Sensor 节点漫游的组

- 合安全认证协议[J]. 中国科学信息科学, 2012, 42(7): 815 – 830. (WANG L M, JIANG S R, GUO Y B. Composable-secure authentication protocol for mobile sensors roaming in the Internet of things[J]. Science China Information Sciences, 2012, 42(7): 815 – 830.)
- [8] 周彦伟, 杨波. 物联网移动节点直接匿名漫游认证协议[J]. 软件学报, 2015, 26(9): 2436 – 2450. (ZHOU Y W, YANG B. Provable secure authentication protocol with direct anonymity for mobile nodes roaming service in Internet of things[J]. Journal of Software, 2015, 26(9): 2436 – 2450.)
- [9] DAS M L. Two-factor user authentication in wireless sensor networks [J]. IEEE Transactions on Wireless Communications, 2009, 8(3): 1086 – 1090.
- [10] CHEN T H, SHIH W K. A robust mutual authentication protocol for wireless sensor networks[J]. ETRI Journal, 2010, 32(5): 704 – 712.
- [11] 杨力, 马建峰, 朱建明. 可信的匿名无线认证协议[J]. 通信学报, 2009, 30(9): 29 – 35. (YANG L, MA J F, ZHU J M. Trusted and anonymous authentication scheme for wireless networks [J]. Journal on Communications, 2009, 30(9): 29 – 35.)
- [12] 周彦伟, 杨波, 张文政. 可证安全的移动互联网可信匿名漫游协议[J]. 计算机学报, 2015, 38(4): 733 – 748. (ZHOU Y W, YANG B, ZHANG W Z. Provable secure trusted and anonymous roaming protocol for mobile Internet [J]. Chinese Journal of Computers, 2015, 38(4): 733 – 748.)
- [13] RAYA M, HUBAUX J P. Securing vehicular Ad Hoc networks [C]// Proceedings of the 2nd International Conference on Pervasive Computing and Applications. Amsterdam: IOS Press, 2007: 424 – 429.
- [14] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[C]// Proceedings of the 2001 International Conference on the Theory and Application of Cryptographic Techniques: Advances in Cryptology. London: Springer-Verlag, 2001: 453 – 474.
- [15] TIN Y S T, VASANTA H, BOYD C, et al. Protocols with security proofs for mobile applications[C]// Proceedings of the 9th Australasian Conference on Information Security and Privacy. Berlin: Springer, 2004: 358 – 369.
- [16] 侯惠芳, 季新生, 刘光强. 异构无线网络中基于标识的匿名认证协议[J]. 通信学报, 2011, 32(5): 153 – 161. (HOU H F, JI X S, LIU G Q. Identity-based anonymity authentication protocol in the heterogeneous wireless network [J]. Journal on Communications, 2011, 32(5): 153 – 161.)
- [17] 侯惠芳, 刘光强, 季新生, 等. 基于公钥的可证明安全的异构无线网络认证方案[J]. 电子与信息学报, 2009, 31(10): 2385 – 2391. (HOU H F, LIU G Q, JI X S. Provable security authentication scheme based on public key for heterogeneous wireless network [J]. Journal of Electronics & Information Technology, 2009, 31(10): 2385 – 2391.)

Background

This work is partially supported by the National Natural Science Foundation of China (61402530, 61272492, 61572521), the Basic Research Foundation of Engineering College of PAP (WJY201520).

ZHANG Xin, born in 1991, M. S. candidate. His research interests include information security, trusted computing.

YANG Xiaoyuan, born in 1959, M. S., professor. His research interests include information security, cryptology.

ZHU Shuaishuai, born in 1985, M. S., lecturer. His research interests include information security, trusted computing, cryptology.

(上接第 3107 页)

- [9] XIAO L, GREENSTEIN L, MANDAYAM N, et al. Fingerprints in the Ether: using the physical layer for wireless authentication[C]// Proceedings of the 2007 IEEE International Conference on Communications. Piscataway, NJ: IEEE, 2007: 4646 – 4651.
- [10] XIAO L, GREENSTEIN L J, MANDAYAM N B, et al. Using the physical layer for wireless authentication in time-variant channels [J]. IEEE Transactions on Wireless Communications, 2008, 7 (7): 2571 – 2579.
- [11] XIAO L, GREENSTEIN L, MANDAYAM N, et al. A physical-layer technique to enhance authentication for mobile terminals [C]// Proceedings of the 2008 IEEE International Conference on Communications. Piscataway, NJ: IEEE, 2008: 1520 – 1524.
- [12] PEI C C, ZHANG N, SHEN X S, et al. Channel-based physical layer authentication[C]// Proceedings of the 2014 IEEE Global Communications Conference. Piscataway, NJ: IEEE, 2014: 4114 – 4119.
- [13] 王映民, 孙韶辉. TD-LTE 技术原理与系统设计[M]. 北京: 人民邮电出版社, 2010: 7 – 60. (WANG Y M, SUN S H. TD-LTE Technology Principle and System Design[M]. Beijing: Posts and Telecommunications Press, 2010: 7 – 60.)
- [14] 梁循. 支持向量机算法及其金融应用[M]. 北京: 知识产权出版社, 2012: 3 – 25. (LIANG X. SVM Algorithm and Its Application in Finance [M]. Beijing: Intellectual Property Publishing House, 2012: 3 – 25.)
- [15] 白鹏, 张喜斌, 张斌, 等. 支持向量机理论及工程应用实例 [M]. 西安: 西安电子科技大学出版社, 2008: 1 – 21. (BAI P, ZHANG X B, ZHANG B, et al. SVM Theory and Engineering Application Example [M]. Xi'an: Xidian University Press, 2008: 1 – 21.)
- [16] CRISTIANINI N, SHAWE-TAYLOR J. An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods[M]. Cambridge: Cambridge University Press, 2000: 4 – 266.
- [17] IMAM T, TING K M, KAMRUZZAMAN J. z-SVM: an SVM for improved classification of imbalanced data[C]// Proceedings of the 19th Australian Joint Conference on Artificial Intelligence. Berlin: Springer-Verlag, 2006: 264 – 273.
- [18] BOTTOU L, LIN C J. Support Vector Machine Solvers [M]. Cambridge: MIT Press, 2007: 301 – 320.

Background

This work is partially supported by the Fundamental Research Funds for the Central Universities (328201537).

YANG Jianxi, born in 1973, Ph. D., associate professor. His research interests include wireless network security, communication network signal anti-interference processing.

DAI Chuping, born in 1990, M. S. candidate. Her research interests include 4G wireless communication, wireless communication physical layer security, machine learning.

JIANG Tingting, born in 1989, M. S. candidate. Her research interests include cloud computing network security, software defined network.

DING Zhengguang, born in 1993, M. S. candidate. Her research interests include cloud computing network security, Docker.