物联网安全网关认证与密钥协商协议设计

杜大海,范 红,王 冠,李程远
(公安部第一研究所 检测中心, 北京 100048)

摘 要: 分析研究了物联网节点认证与密钥管理技术. 针对大量节点同时对物联网网关集中访问的特点,提出了一种快速认证与密钥协商协议. 采用会聚认证算法,提高了认证效率,密钥协商过程中每个节点都贡献一份因子参与密钥协商,提高了密钥生成的安全性.

关键词: 物联网;认证;密钥协商;密码学
中图分类号: TN915.08 **文献标识码**: A **文章编号**: 1000-7180(2014)07-0098-03

A Design of Authentication and Key Agreement Protocol for Secure Gateways in IoTs

DU Da-hai, FAN Hong, WANG Guan, LI Cheng-yuan
(Testing Center, The First Research Institute of Ministry of Public Security, Beijing 100048, China)

Abstract: Access control and key agreement technology of IoTs is studied in this paper. Since many nodes in IoTs may access the gateway at the same time, a fast authentication and key agreement protocol is proposed in this paper. We use an aggregated verification scheme to improve the authentication efficiency. Each node participates in the key agreement procedure and contributes a key parameter, which improves the security level of the key establishment scheme.

Key words: internet of things; authentication; key agreement; cryptography

1 引言

目前,国内外对物联网安全方面的研究尚不够成熟,文献[1]中提出一种基于椭圆曲线密码体系和节点身份的单点登录认证技术. 每个感知节点在RA(Registration Authority)进行注册获取私钥. 该节点只需要通过自己的HRA(Home Registration Authority)认证,就可以在整个网络中不同的域进行登录认证. 文献[2]中提出了一种单个移动节点在物联网中不同簇之间的游牧认证方案. 文献[3]中提出了采用数字证书的方式进行相互认证. 每个节点和认证服务器都拥有一个由CA(Certificate Authority)颁发的数字证书.

上述方案实现了物联网中单个节点接入认证的问题,但是,由于物联网中节点数目众多,而对大量节点进行认证要在短时间内完成. 因此,需要有一种较为快速有效的认证与密钥协商方案.

2 系统结构图

本文提出的物联网感知层节点认证与密钥协商方案中采用的网络结构图. 如图1所示,感知层由物联网网关、簇头节点以及普通节点组成. 每个普通节点在接入网络的时候都需要通过物联网网关的认证.

3 SAKAP方案

3.1 系统参数生成

物联网注册管理中心RC(Registration Center)

收稿日期: 2013-11-16; **修回日期**: 2014-01-03
基金项目: 国家发改委2012年信息安全专项([2012]2091); 国家高技术发展计划("八六三")(2009AA01Z437, 2009AA01Z439)

选择两个阶为 q 的群 G_1 和 G_2，q 为一个大素数. 存在以下映射运算 $\hat{e}: G_1 \times G_1 \rightarrow G_2$. RC 选择一个生成元 P，$P \in G_1$[4]. RC 选择一个参数 $\alpha \in \mathbb{Z}_q^*$ 作为安全网关系统私钥，公布网关认证公钥 $P_{\text{pub}} = \alpha P$；选择一个单项 Hash 函数 $H_1: \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.

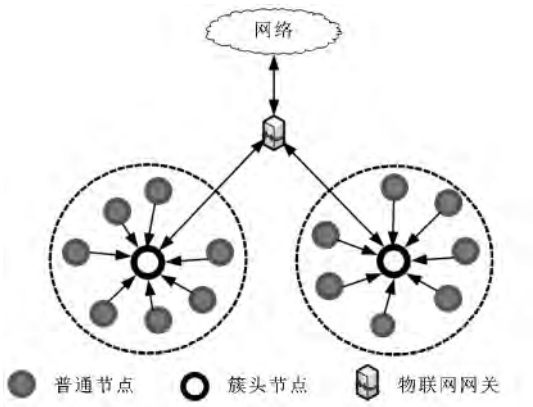

图 1　物联网感知层结构图

3.2　感知节点注册

物联网中的感知节点 U_i 都在 RC 进行注册，获取一个 $ID_i \in \{0,1\}^*$，RC 随机选择一个 $x_i \in \mathbb{Z}_q^*$，计算 $h_i = H_1(ID_i)$，$X_i = x_i P$，$P_i = (x_i + h_i\alpha)P$，$s_i = \dfrac{1}{x_i + h_i\alpha}$，$< P_i, s_i >$ 是感知节点 U_i 的公私钥对. s_i 作为安全网关和感知节点之间的共享密钥. 节点 U_i 在收到公私钥对 $< P_i, s_i >$ 之后，可以通过验证 $P_i = X_i + H_1(ID_i)P_{\text{pub}}$，$\hat{e}(s_i P, P_i) = \hat{e}(P, P)$，来确认密钥对的合法性.

3.3　节点认证与密钥协商

由于物联网中感知节点数量较多，在使用过程中，会有多个节点同时对网关发送认证请求. 因此物联网网关需要对感知节点身份进行快速认证，以提高认证效率. 认证与密钥协商过程如下：

(1) 感知节点广播自己的公钥 P_i，计算认证参数，向网关发出认证请求，然后广播对其他节点公钥的签名. 感知节点首先获取时间 T_i，选择一个随机数 $r_i \in \mathbb{Z}_q^*$，计算 $R_i = r_i P$，$A_i = s_i R_i = s_i r_i P = r_i P/(x_i + h_i\alpha)$. 每个节点在收到网络中其他节点的公钥之后，选择一个随机数 $k_i \in \mathbb{Z}_q^*$，计算 $\text{Sig}_{i-j} = k_i P_j = k_i(x_j + h_j\alpha)P$，$Sig_{i-gw} = k_i P_{\text{pub}} = k_i\alpha P (1 \leqslant i \leqslant n, 1 \leqslant j \leqslant n, i \neq j)$，然后广播 Sig_{i-j}，将参数 $msg_i: \{ID_i, T_i, R_i, A_i, Sig_{i-gw}\}$ 发送给网关.

(2) 网关对感知节点进行如下认证.

① 延时验证. 网关首先获取时间 $T_G^i (1 \leqslant i \leqslant n)$，验证 $\Delta t_i = T_G^i - T_i \leqslant T_{\max}$（$T_{\max}$ 是物联网网关预先设置的从感知节点到网关的最大传输延迟）是否成立. 如果成立，则进行下一步；否则，放弃.

② 单个节点认证. 网关根据节点的 ID_i 寻找相应的私钥 s_i，计算 $A_i' = s_i R_i = s_i r_i P$，验证 $A_i' = A_i$ 是否成立. 如果等式成立，则该感知节点为合法节点；否则，拒绝该节点接入网络.

③ 多个感知节点同时认证. 为了提高感知节点身份验证效率，我们采用了批量验证方法. 然而，多个用户同时申请验证时，存在碰撞的可能性，为了降低碰撞的概率，我们采用了文献[5]中的方法来提高批量验证算法的安全性.

① 网关选择一系列参数 $l_i \in \mathbb{Z}_q^* (1 \leqslant i \leqslant n)$，计算 $\Psi = l_1 A_1 + \cdots + l_i A_i + \cdots + l_n A_n = \sum_{i=1}^{n} l_i A_i$，$\Psi' = l_1 A_1 + \cdots + l_i A_i' + \cdots + l_n A_n' = \sum_{i=1}^{n} l_i A_i'$.

② 验证 $\Psi \stackrel{?}{=} \Psi'$，如果成立，则验证成功.

③ 如果 ② 中等式不成立. 网关开始对 n 个感知节点的认证请求信息采用折半查找验证，直到找出不合法节点为止.

(3) 在网关对感知节点成功认证之后，随机选择 $b \in \mathbb{Z}_q^*$，反馈 $B = bP$ 给各个节点，计算 $K_{gw-i} = bR_i = br_i P$，作为安全网关和感知节点 U_i 之间的共享密钥. 计算 $Sig_{gw-i} = bP_i = b(x_i + h_i\alpha)P (1 \leqslant i \leqslant n)$，广播所有签名信息.

(4) 各个感知节点收到网关的反馈信息之后，计算 $K_{i-gw} = r_i B = r_i bP$，作为感知节点和安全网关之间的共享密钥.

(5) 组密钥计算. 网络中每个节点（包括安全网关）在收到其他节点的签名信息之后，计算 $Sig_{i-i} = k_i P_i = k_i(x_i + h_i\alpha)P$，然后计算组密钥 $K_{G_i} = \hat{e}(Sig_{1-i} + \cdots + Sig_{n-i} + Sig_{gw-i}, s_i P) (1 \leqslant i \leqslant n)$；网关计算 $Sig_{gw-gw} = bP_{pub}$ 及 $K_{G_{gw}} = \hat{e}(Sig_{1-gw} + \cdots + Sig_{n-gw} + Sig_{gw-gw}, \alpha^{-1}P)$.

4　方案分析

4.1　方案正确性分析

由第 3 节中的介绍容易得到 $A_i' = A_i$，$\Psi = \Psi'$ 及 $K_{i-gw} = r_i B = r_i bP = bR_i = K_{gw-i}$ 的结论，这里主要证明每个节点生成的组密钥相等.

定义 1　网络中每个组成员所计算的组密钥是一致的.

证明：每个节点计算的组密钥

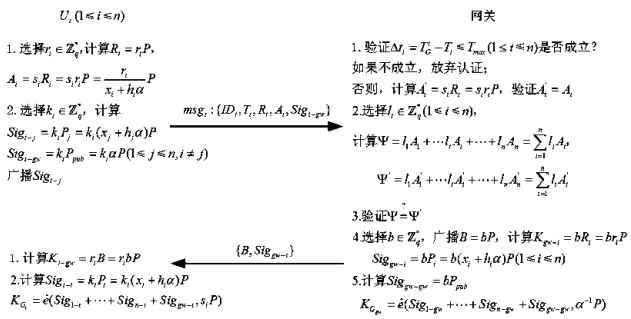

图 2 认证与密钥协商流程图

$$
\begin{aligned}
K_{G_i} &= \hat{e}(Sig_{1-i} + \cdots + Sig_{n-i} + Sig_{gw-i}, s_i P) \\
&= \hat{e}(k_1 P_i + \cdots + k_n P_i + bP_i, s_i P) \\
&= \hat{e}(k_1 (x_i + h_i \alpha) P + \cdots + k_n (x_i + h_i \alpha) P + \\
&\quad b(x_i + h_i \alpha) P, \frac{1}{x_i + h_i \alpha} P) \\
&= \hat{e}((b + \sum_{i=1}^{n} k_i)(x_i + h_i \alpha) P, \frac{1}{x_i + h_i \alpha} P) \\
&= \hat{e}(P, P)^{(b + \sum_{i=1}^{n} k_i)(x_i + h_i \alpha) \frac{1}{x_i + h_i \alpha}} \\
&= \hat{e}(P, P)^{(b + \sum_{i=1}^{n} k_i)} \quad (1 \leqslant i \leqslant n)
\end{aligned}
$$

网关计算

$$
\begin{aligned}
K_{G_{gw}} &= \hat{e}(Sig_{1-gw} + \cdots + Sig_{n-gw} + Sig_{gw-gw}, \alpha^{-1} P) \\
&= \hat{e}(k_1 P_{\text{pub}} + \cdots + k_n P_{\text{pub}} + bP_{\text{pub}}, \alpha^{-1} P) \\
&= \hat{e}(k_1 \alpha P + \cdots + k_n \alpha P + b\alpha P, \alpha^{-1} P) \\
&= \hat{e}((b + \sum_{i=1}^{n} k_i) \alpha P, \alpha^{-1} P) \\
&= \hat{e}(P, P)^{(b + \sum_{i=1}^{n} k_i) \alpha \alpha^{-1}} \\
&= \hat{e}(P, P)^{(b + \sum_{i=1}^{n} k_i)}.
\end{aligned}
$$

可得 $K_{G_i} = K_{G_{gw}} = \hat{e}(P, P)^{(b + \sum_{i=1}^{n} k_i)} (1 \leqslant i \leqslant n)$，**因此，网络中的每一个组成员所计算的组密钥是一致的.**

4.2 安全性分析

由于 SAKAP 方案中的密钥生成是基于 BDH 难题[4]和 ECDLP 难题[6]，因此这里主要证明认证的安全性.

定义 2 通过认证的节点都是合法节点.

证明：一个非法节点企图伪装成合法节点通过认证，那么它必须获得(或者猜测出)这个合法节点的私钥 s_i. 通过发送的参数 msg_i 和系统参数 P 很难计算出 s_i，这需要解决 ECDLP 难题[8]. 如果通过猜测的方法获得 s_i，由于 $s_i \in [0, q-1]$，q 是一个大素数(至少有 256 bit)，那么猜对 s_i 的概率为 $1/2^{256}$，是可以忽略不计的. 由此可知，通过认证的节点都是合法节点. 证明完毕.

4.3 方案比较

将本文提出的方案和文献[3]中的方案进行比较，主要从通信次数上进行了分析. 方案比较如表 1 所示，这里只取文献[3]中方案的认证部分的通信量. 可以看出，SAKAP 在通信量上明显小于文献[3]中的方案.

表 1 通信次数比较

方案	单个节点	n 个节点
文献[3]	7	$7n$
SAKAP	2	$n+1$

5 结束语

本文提出了一种快速的认证和密钥协商协议. 该协议针对物联网中节点众多的特点，提出了一种会聚的验证方案，提高了认证的效率；协议中每个节点都参与密钥协商，提高了密钥生成的安全性.

参考文献：

[1] Liu J, Xiao Y, C L Philip Chen, et al. Authentication and access control in the internet of things[C]//32nd International Conference on Distributed Computing Systems Workshops. China: IEEE, 2012: 588-592.

[2] Miao J, Wang L. Rapid identification authentication protocol for mobile nodes in internet of things with privacy[J]. Journal of Networks, 2012, 7(7): 1099-1105.

[3] Kothmayr T, Schmitt C, Wen Hu, et al. A DTLS based end-to-end security architecture for the internet of things with two-way authentication[C]// Proceedings of the 7th IEEE International Workshop on Practical Issues in Building Sensor Network Applications. [s. l.]: IEEE, 2012: 956-963.

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

(下转第 104 页)

karate club 网络的真实情况完全一致，再次验证了本文所提改进新算法的可行性与有效性.

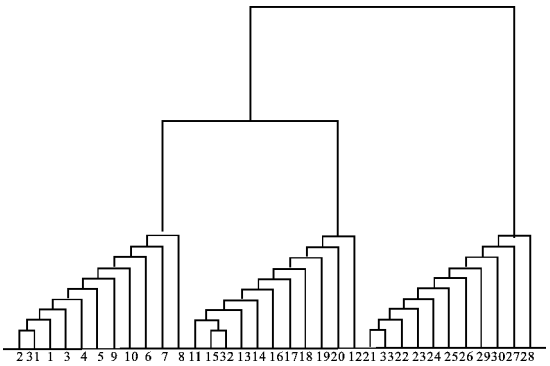

图 4 本文新算法对三团网络的划分

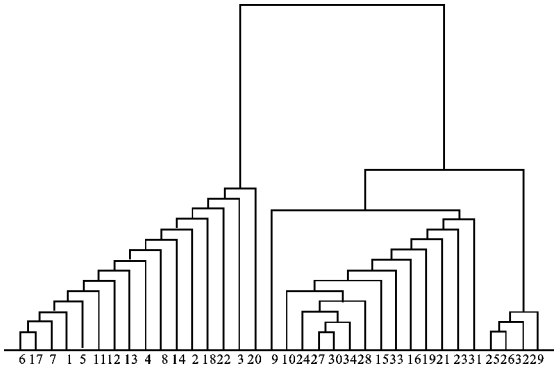

图 5 本文新算法对 karate club 网络的划分

4 结束语

本文提出一种适度贪心算法思路，即引入适度原则，对每次迭代中的贪婪幅度进行约束，以避免过度贪婪、谬误累积、最终结果误差较大的情况，并在此基础上，构建了一种基于适度贪心算法思路的社团划分算法，并通过算例对新算法进行了验证与分析.

参考文献：

[1] 汪小帆，李翔，陈关荣. 复杂网络理论及其应用[M]. 北京：清华大学出版社，2006.

[2] 解伯，汪小帆. 复杂网络中的社团结构分析算法研究综述[J]. 复杂系统与复杂性科学，2005，2 (3)：1-12.

[3] 金弟，杨博，刘杰，等. 复杂网络簇结构探测——基于随机游走的蚁群算法[J]. 软件学报，2012，23(3)：451-464.

[4] Newman M E J，Girvan M. Finding and evaluating community structure in networks [J]. Physical Review E，2004(69)：026113.

[5] 解伯. 复杂网络的社团结构建模与分析[D]. 上海：上海交通大学，2007.

[6] 莫春玲. 复杂网络中聚类方法及社团结构的研究[D]. 武汉：武汉理工大学，2007.

[7] 王波. 基于派系的复杂网络及其在公交网络上的应用研究[D]. 杭州：浙江工业大学，2009.

[8] 邓智龙，淦文燕. 复杂网络中的社团结构发现方法[J]. 计算机科学，2012，39(6)：103-108.

[9] Newman M E J. Fast algorithm for detecting community structure in networks [J]. Physical Review E，2004(69)：066133.

[10] Zachary W. An information flow model for conflict and fission in small groups [J]. Journal of Anthropological Research，1977，33(4)：452-473.

[11] 王铮，吴静. 计算地理学[M]. 北京：科学出版社，2011.

[12] 百度百科. 贪心算法[EB/OL]. [2013-04-20]. http://baike. baidu. com/view/298415. htm？fromId=1628576.

[13] 付俐. 马钢铁矿石采购物流成本核算与优化控制研究[D]. 马鞍山：安徽工业大学，2012.

[14] 汪晓银. 数学建模与数学实验[M]. 北京：科学出版社，2010.

[15] 李博权，李绪志，王红飞，等. 贪婪算法与动态规划结合的任务规划方法[J]. 微电子学与计算机，2013，30(2)：144-147.

作者简介：

武 澎 男，(1981-)，博士研究生，讲师. 研究方向为社团划分、超网络、网络分析等.

王恒山 男，(1948-)，教授，博士生导师. 研究方向为管理信息系统、复杂网络等.

(上接第 100 页)

[5] Ferrara A，Green M，Hohenberger S. et al. Practical short signature batch verification [C]//Proceedings of Topics in cryptology-CT-RSA 2009. Berlin：Springer Heidelberg，2009：309-324.

[6] Standards for Efficient Cryptography. SEC1. Elliptic curve cryptography [S]. Mississauga：Certicom Corp，2000.

作者简介：

杜大海 男，(1982-)，博士，工程师. 研究方向为信息安全、物联网安全.

范 红 女，(1969-)，博士，副研究员. 研究方向为信息安全.

王 冠 女，(1985-)，硕士，助理工程师. 研究方向为信息安全.

李程远 男，(1984-)，硕士，工程师. 研究方向为信息安全.