

一种无线传感器网络的访问控制协议

谢招彝, 郑 旋, 赖晓涛

(赣南医学院 信息工程学院, 江西 赣州 341000)

摘 要: 传感器网络中的节点存在由于能量耗尽或恶意攻击而丧失作用的威胁, 因此需要新节点的加入. 利用 Bloom Filter 技术, 提出了一种访问控制协议. 本协议不仅便于实现新节点、旧节点的双向认证和密钥协商, 而且便于实现节点的加入与撤销. 通过性能分析和安全性分析说明了该协议的有效性.

关键词: 传感器网络; 双向认证; 访问控制; Bloom 过滤器

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2011)08-0087-03

An Access Control Protocol for Wireless Sensor Networks

XIE Zhao-ben, ZHENG Xuan, LAI Xiao-tao

(School of Information Engineering, Gannan Medical College, Ganzhou 341000, China)

Abstract: Nodes in a sensor networks may be lost because of power exhaustion or malicious attacks. Therefore it's necessary for new nodes' deployment. Using Bloom Filter, we propose an access control protocol including the mutual authentication procedure and common key generation. It's efficient for the nodes' adding, deleting and authentication. At last, the paper makes an analysis of the performance and safety about the proposed protocol.

Key words: sensor network; mutual authentication; access control; Bloom Filter

1 引言

目前, 无线传感器网络内部存在恶意节点注入非法信息和篡改数据、节点复制、节点伪造等诸多威胁^[1-2], 因此提出一种安全、高效、低能耗的认证协议是无线传感器网络的研究热点. 由于传感器节点的存储容量、计算能力、电池能量等有限的特点, 安全认证还需要考虑旧节点能量耗尽而新节点加入^[3]等情况.

2007 年 Yun Zhou^[3]等人基于 ECC 公钥算法提出了一种访问控制协议. 在认证过程中, 通过比较新节点加入网络的启动时间, 然后验证签名来实现新节点的认证, 并且可以完成相邻节点间共享密钥的建立. 但是, 恶意节点可以利用新节点启动时间的这段短暂间隔实施恶意攻击. 另一方面, 公钥数字签名算法能量消耗大.

本文结合文献^[4-5]Bloom Filter 和 Counting

Bloom Filter 的思想, 利用对称加密算法来实现双向认证, 并利用 Diffie-Hellman 算法建立节点间的共享密钥. 本协议无需利用新节点的启动时间, 也能完成新节点的双向认证. 在认证过程中, 节点只需存储基站产生的过滤器数据, 利用 Bloom Filter 技术验证对方公钥的真实性, 不用传输数字证书, 从而提高了认证效率, 降低了通信成本.

2 访问控制协议

本存取控制协议包括三个阶段: 系统初始化、双向认证和密钥协商过程、节点的加入与撤销.

基于椭圆曲线的算法具有密钥短、处理速度快和带宽要求低等优点, 在密钥协商过程, 我们选择 Diffie-Hellman 算法. 令 F_q 是一个有限域, q 是一个素数. 基站选择合适的椭圆曲线构造点集 $E(F_q)$, G 是 $E(F_q)$ 的 n 阶生成元, FR 是 F_q 中的一个元素. 选取安全的 hash 函数 $h(\cdot)$, 得到系统参数 $D = (q,$

$E(F_q), FR, G, n, h)$.

2.1 系统初始化

假设在 WSN 的某一固定区域有 r 个相邻节点, 记为 $\{N_1, N_2, \dots, N_r\}$. 令 (pk_i, sk_i) 表示节点 N_i 的公钥和私钥. 在基站端安装一个 Bloom Filter 和 Counting Bloom Filter, 基站为每个节点 $N_i (i \in [1, r])$ 分配不同的密钥对 (pk_i, sk_i) 并利用单向哈希函数对 sk_i 计算 z 次 (z 是本固定网络的最大节点数), 产生一个长度为 $z+1$ 的哈希链 $h^0(sk_i), h^1(sk_i), h^2(sk_i), \dots, h^i(sk_i), \dots, h^z(sk_i)$, 有 $h^m(sk_i) = h(h^{m-1}(sk_i))$. 然后构造集合: $S_N = \{ \langle N_1, pk_1 \rangle, \langle N_2, pk_2 \rangle, \dots \}$, $\# \{ \}$ 表示集合的基数, 这里 $\# \{ S_N \} = r$.

利用系统提供的 k 个相互独立的哈希函数 $\{h_l(\cdot)\}_{l=1}^k$ (如 SHA-1), 基站应用 Bloom Filter 技术计算一个 m -bit 的 v_N 向量, 记为 $v_N = v_N^0 v_N^1 \dots v_N^{m-1}$. 其中每个 $v_N^i, i \in [0, m-1]$, 满足

$$v_N^i = \begin{cases} 1, & \text{if } \exists l \in [1, k], j \in [1, r], \text{ s.t. } h_l(N_j \parallel pk_j) = i \\ 0, & \text{otherwise} \end{cases}$$

这样, $\langle N_j, pk_j \rangle \in S_N$ 当且仅当所有哈希函数 $h_l(N_j \parallel pk_j) = i$ 的分量 $v_N^i = 1$. 基站应用 Counting Bloom Filter 对 v_N 计算向量 $\overline{v_N} = \overline{v_N^0} \overline{v_N^1} \dots \overline{v_N^{m-1}}$, 每个 $\overline{v_N^i}, i \in [0, m-1]$, 满足:

$$\overline{v_N^i} = \# \{ (N_i \parallel pk_i) \mid h(N_i \parallel pk_i) = i, \text{ for } \exists l \in [1, k], j \in [1, r] \}.$$

最后, 基站将密钥对 (pk_i, sk_i) 、单向哈希链 $h(\cdot)$ 和向量 v_N 预装载到每个节点, 并将 $\overline{v_N}$ 秘密保存. 基站还对参数 $D, h^z(sk_i), i \in [1, r], z, \{h_l(\cdot)\}_{l=1}^k$ 进行广播.

2.2 双向认证密钥协商过程

在本协议的认证过程中, 节点每成功验证一次, 基站就对其广播的哈希值更新一次. 即若节点 N_i 已成功验证 m 次, 则基站广播 $h^{z-m}(sk_i)$.

这里, 假设节点 N_i 已成功验证 u 次, 节点 N_j 已成功验证 w 次, 基站先将 $h^{z-u}(sk_i)$ 和 $h^{z-w}(sk_j)$ 进行广播. 则其双向认证和密钥协商过程如下:

(1) N_i 向 N_j 发送 $N_i \parallel pk_i$, 启动双向认证.

(2) N_j 将 $N_j \parallel pk_j$ 发送给合法注册的节点 N_i .

• 验证 N_i 是合法注册的节点;

N_j 应用 k 个相互独立的哈希函数 $\{h_l(\cdot)\}_{l=1}^k$ 计算 $v_N[h_l(N_i \parallel pk_i)] = ?1$. 当且仅当所有的 $l \in [1, k]$, 满足 $v_N[h_l(N_i \parallel pk_i)] = 1$, 则 pk_i 为 N_i 真实的公钥. 若验证 pk_i 为真, 则继续下一步; 若为假, 则取消连接.

• N_j 将 $N_j \parallel pk_j$ 发送给 N_i .

(3) N_i 将 $C_i = E_{\sigma_{ij}}(h^{z-u-1}(sk_i))$ 发送给合法注册的 N_j .

• 验证 N_j 是合法注册的节点;

应用类似的方法, N_i 计算 $v_N[h_l(N_j \parallel pk_j)] =$

1. 当且仅当所有的 $l \in [1, k]$, 满足 $v_N[h_l(N_j \parallel pk_j)] = 1$, 则 pk_j 为 N_j 真实的公钥. 若验证 pk_j 为真, 则继续下一步; 若为假, 则取消连接.

• N_i 计算 $\sigma_{ij} = sk_i \cdot pk_j$,

$C_i = E_{\sigma_{ij}}(h^{z-u-1}(sk_i))$.

• N_i 将 $C_i = E_{\sigma_{ij}}(h^{z-u-1}(sk_i))$ 发送给 N_j .

(4) N_j 将 $C_j = E_{\sigma_{ij}}(h^{z-w-1}(sk_j))$ 发送给 N_i .

• N_j 计算 $\sigma_{ij} = sk_j \cdot pk_i$, 验证 $h(D_{\sigma_{ij}}(C_i)) = ? h^{z-u}(sk_i)$. 若相等, 则 N_i 为可信节点, 继续下一步; 若不相等, 则取消连接.

• N_j 计算 $C_j = E_{\sigma_{ij}}(h^{z-w-1}(sk_j))$, 将 C_j 发送给 N_i .

(5) N_i 验证 $h(D_{\sigma_{ij}}(C_j)) = ? h^{z-w}(sk_j)$. 若相等, 则 N_j 为可信节点, 可继续用共享密钥 σ_{ij} 进行通信; 若不相等, 则取消连接.

这样, 节点 N_i 和节点 N_j 都向对方表明了自己的合法身份, 实现了双向认证和密钥协商. 具体如图 1 所示.

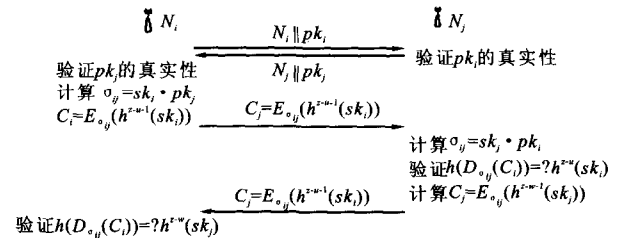


图 1 节点双向认证图

2.3 节点的撤销与加入

当发现有伪造传感器节点等恶意情况时, 需要撤销该节点; 当传感器节点能量耗尽等情况时, 需要加入新的节点. 基站利用 Counting Bloom Filter 技术可实现节点的撤销与加入.

2.3.1 节点的撤销

假设撤销节点 N_j , 基站执行以下操作:

(1) 首先检查 N_j 的哈希值 $\{h_l(N_j \parallel pk_j)\}_{l=1}^k$.

若有 $h_l(N_j \parallel pk_j) = i$, 则基站的 $\overline{v_N}$ 做减 1 操作.

(2) 根据更新的 $\overline{v_N}$ 向量, 基站可获得一个更新的 v'_N 向量, 记为 $v'_N = v'_N{}^0 v'_N{}^1 \dots v'_N{}^{m-1}$. 此时 $v'_N{}^i = 1$, 当且仅当 $\overline{v_N}^i \geq 1$; 否则 $v'_N{}^i = 0$.

(3) 计算 $v_{\Delta N} = v'_N \oplus v_N$ ($\oplus$ 表示异或运算), 然

后删除 v_N 向量. 显然 $v_{\Delta N}$ 也是一个 m -bit 向量, 且至多有 k bits 置为 1.

(4) 基站在该区域广播向量 $v_{\Delta N}$.

(5) 传感器节点根据 $v_{\Delta N}$ 向量更新 v_N 向量. 若 $v'_{\Delta N} = 1$, 则 $v'_N = 0, i \in [0, m-1]$.

这样就完成了一个传感器节点的撤销. 节点撤销后, 也将其对应的 pk_j/sk_j 密钥对销毁.

2.3.2 新节点的加入

假设有新节点 N_{r+1} 要求加入网络, N_{r+1} 首先在基站进行注册, 获得密钥对 (pk_{r+1}, sk_{r+1}) . 基站利用 Bloom Filter 技术, 将 $\langle N_{r+1}, pk_{r+1} \rangle$ 映射到 $\{0 \cdots m-1\}$ 的范围中, 获得更新的 v_N 向量, 利用 Counting Bloom Filter 技术获得更新的 $\overline{v_N}$ 向量. 使用与撤销节点相同的方法, 基站根据更新的 $v_N, \overline{v_N}$ 向量计算得到 $v_{\Delta N}$ 向量, 将 $v_{\Delta N}$ 广播. 节点对向量 v_N 进行更新, 若 $v'_{\Delta N} = 1$, 则 $v'_N = 1, i \in [0, m-1]$. 这样就实现了新节点的加入.

新节点 N_{r+1} 注册完后, 基站计算此节点的单向哈希链 $h(sk_{r+1})$, 并装载在该新节点端. 与 N_{r+1} 进行初次认证时, 基站广播 $h^z(sk_{r+1})$, 依此, 该区域的其他节点知道有新节点的加入. 接下来认证步骤相同.

3 安全性分析与性能分析

3.1 安全性分析

本协议建立在基站是绝对可信的基础上, 恶意节点不可能获得私钥. 在认证过程中, 恶意节点可通过窃听网络流量获得公钥, 但无法计算得到正确的共享密钥, 在用共享密钥验证哈希值时必定失败, 从而取消连接.

本协议的安全性依赖于 Diffie-Hellman 算法的求离散对数的困难性、哈希函数的安全性及节点私钥的保密性. 安全假设建立在只有真正的节点知道私钥的基础上, 所以, 一旦节点的私钥泄露, 协议将失去作用.

3.2 性能分析

在双向认证和密钥协商过程中, 节点的主要计算是一次基于 ECC 的点积计算、一次对称加解密计算和哈希计算. 文献[2]中, 节点的主要计算是一次点积计算、一次 ECDSA 签名和 ECDSA 解签名. 因此, 本协议具有计算量更小、无需携带数字证书的优点. 另一方面, 节点只需存储基站产生的过滤器数据、哈希链值和节点的密钥对.

4 结束语

本文提出了一种适用于无线传感器网络的访问控制协议, 此协议可以实现节点间的双向认证和密钥协商, 当有新节点加入时, 此协议同样发挥作用. 另外, 本协议还便于实现节点的动态管理.

参考文献:

- [1] Zhou Y, Fang Y, Zhang Y. Securing wireless sensor networks: a survey[J]. IEEE Communications Surveys, 2008(10):6-28.
- [2] 郑耿忠, 刘秋梅. 基于模糊控制的移动无线传感器网络部署优化[J]. 微电子与计算机, 2011, 28(2):20-22.
- [3] Zhou Y, Zhang Y, Fang Y. Access control in wireless sensor networks[J]. Security issues in Sensor and Ad Hoc Networks, 2007(5):3-13.
- [4] Ren K, Lou W, Zhang Y. Multi-user broadcast authentication in wireless sensor networks[C]// 4th Annual IEEE Communications Society Conference. San Diego, CA, United States, 2007:223-232.
- [5] Mitzenmacher M. Compressed bloom filters[J]. IEEE/ACM Transactions on Networks, 2002(10):613-620.

作者简介:

谢招彝 男, (1974-), 硕士, 讲师. 研究方向为网络软件与智能信息处理.

郑旋 女, (1984-), 硕士, 助教. 研究方向为计算机网络与安全.

(上接第 86 页)

- [16] Paolucci M K. Semantic matching of Web service capabilities [C]// The First International Semantic Web Conference. Greece, Heraklion, 2002.
- [17] Bansal S M. Matchmaking of web services based on the DAML-S Service Model [C]// 2nd AAMAS. Australia: Victoria, 2003.
- [18] Agarwal S A. Automatic matchinaking of web services

[C]// The 15th International Conference on world wide Web. China: Beijing, 2006.

作者简介:

熊芳 女, (1979-), 工程师. 研究方向为信息服务、语义关联度.