Journal of Computer Applications
计算机应用,2013,33(7):1842 - 1845,1857
ISSN 1001-9081
CODEN JYIIDU
2013-07-01
http://www.joca.cn

文章编号:1001-9081(2013)07-1842-04
doi:10.11772/j.issn.1001-9081.2013.07.1842

无线传感器网络中基于节点行为和身份的可信认证

刘　涛[1,2*],熊　焰[1],黄文超[1],陆琦玮[1],龚旭东[1]
(1.中国科学技术大学 计算机科学与技术学院,合肥 230027;　2.安徽工程大学 计算机与信息学院,安徽 芜湖 241000)
(*通信作者电子邮箱 dqcltdz@126.com)

摘　要:针对无线传感器网络(WSN)开放性和资源受限导致易受外部和内部攻击以及节点失效等问题,提出了一种高效、安全的可信节点间身份认证方案。方案采用基于身份和双线性对理论实现认证密钥协商与更新,通过基于Beta分布的节点行为信誉的管理计算其信任度,利用信任度识别节点是否可信并采用对称密码体制结合信息认证码实现可信节点间认证。方案不仅能防范窃听、注入、重放、拒绝服务等多种外部攻击,而且能够抵御选择性转发、Wormhole攻击、Sinkhole攻击和女巫攻击等内部威胁。与SPINS方案相比,所提方案在同一网络环境下有较长的网络生命期、较小的认证时延、更高的安全性及可扩展性,在无人值守安全性要求较高的WSN领域具有较好的应用价值。

关键词:无线传感器网络;可信认证;节点行为;基于身份;Beta分布;双线性对
中图分类号:TP309　　**文献标志码**:A

Node behavior and identity-based trusted authentication in wireless sensor networks

LIU Tao[1,2*], XIONG Yan[1], HUANG Wenchao[1], LU Qiwei[1], GONG Xudong[1]
(1. *College of Computer Science and Technology, University of Science and Technology of China, Hefei Anhui* 230027, *China*;
2. *School of Computer and Information, Anhui Polytechic University, Wuhu Anhui* 241000, *China*)

Abstract: Concerning the vulnerability to attack from external and internal nodes and node failure due to openness and limited resources in Wireless Sensor Network (WSN), an efficient, secure trusted authentication scheme was proposed. The theory of identity-based and bilinear pairings was adopted in the authentication key agreement and update. The node trust value was computed by node behavior reputation management based on Beta distribution. The symmetric cryptosystem combined with message authentication code was used in certification process between trusted nodes which were identified by the trust value. The scheme not only can prevent eavesdropping, injection, replay, denial of service and other external attacks, but also is able to withstand internal threats such as the selective forwarding, Wormhole attack, Sinkhole attack and Sybil attack. The analysis and comparison with SPINS scheme show that the scheme can achieve longer network lifetime, smaller certification delay, greater security and scalability in the same network environment. The scheme has good application value in unattended WSN with high safety requirements.

Key words: Wireless Sensor Network (WSN); trusted authentication; node behavior; identity-based; Beta-distribution; bilinear pairing

0　引言

无线传感器网络(Wireless Sensor Network, WSN)主要由具有感知能力、计算能力和通信能力的微型无线传感器节点构成,具有低成本、低功耗、多功能等特点,能够协调地实时监测、感知和采集网络分布区域内的各种环境或监测对象的信息,并对这些数据进行处理后传送到特定的用户。由于WSN无需预先部署基础设施,在战场环境、抢险救灾、环境威胁探索等领域具有广泛的应用前景。在各种应用中节点将信息通过转发的形式传送到目的地,即WSN采用多跳通信,在多跳传输过程中,无线通信使得攻击者有机会将无效的信息注入网络,导致传感器转发无效数据并消耗能量,因此转发路径上的节点需要进行身份认证[1]。与传统移动通信的单跳通信不同,节点需要与其周围的邻居节点进行认证。另外无人值守的环境导致传感器节点容易被捕获,如何既能抵御外部恶意节点的入侵又能防止内部妥协节点的攻击是目前WSN安全认证研究的重要问题之一。

1　相关工作

文献[2]传感器网络安全协议(Security Protocols for Sensor Networks, SPINS)协议中的网络安全密码协议(Secure Network Encryption Protocol,SNEP)利用对称密码体制实现通信的机密性、完整性及点到点的认证,其中用于节点到基站加密和认证的两个密钥都是通过与基站共享的主密钥按照相同算法推演出来,而节点间的共享密钥是通过基站临时分配的。文献[3]首次提出公钥体制的WSN用户实体认证,但该协议抗捕获性较差。文献[4]基于椭圆曲线密码体制(Elliptic Curve Cryptosystem, ECC)算法的强用户认证协议方案对文献

收稿日期:2013-01-23;**修回日期**:2013-02-26。
基金项目:国家自然科学基金资助项目(61170233,61232018,61272472);国家自然科学基金青年科学基金资助项目(61202404);安徽省教育厅自然科学基金资助项目(KJ2013A040, KJ2012B012);安徽省自然资金资助项目(1308085MF88)。
作者简介:刘涛(1973 -),女,安徽六安人,副教授,硕士,CCF会员,主要研究方向:计算机网络、信息安全;　熊焰(1960 -),男,安徽合肥人,教授,博士生导师,主要研究方向:计算机网络、信息安全、移动计算、移动网络、分布式处理;　黄文超(1982 -),男,湖北宜昌人,博士,主要研究方向:信息安全、移动计算;　陆琦玮(1988 -),男,江苏太仓人,博士研究生,主要研究方向:移动社交网络、信息安全;　龚旭东(1988 -),男,四川资阳人,博士研究生,主要研究方向:移动社交网络、数据挖掘。

[3]方案作出了改进。文献[5]提出了分布式节点认证模型,该类方案不需要基站作为认证的中心,但认证时需要大量的节点参与,计算和通信的开销将会随着认证请求次数的增加而不断增大,而且必须采用相应的协同机制来协调信息的收发。文献[6]针对无人值守 WSN 敌手将欺骗性数据注入网络或修改网络数据,运用对称密码体制,提出多个传感器节点相互协作的数据认证方案,该方案假定每个节点与汇聚节点都共享一对密钥,容易引起单点失效问题。

认证是整个安全体系的重要环节,同时认证也离不开密钥协商。WSN 由大量资源受限特别是能量有限的传感器节点组成,而通信活动会消耗大部分能量,因此理想的密钥协商是不需要交互信息。文献[7]提出了一种典型的基于身份的加密方案(Identity-Based Encryption, IBE)实现密钥的交换与数据加密,该方案虽采用公钥密码体制思想但不需要公钥基础设施(Public Key Infrastructure, PKI)对公钥的认证,因为是以用户的身份标识作为公开信息,其他用户可根据其身份推导用户的公钥。文献[8]将此思想应用在 WSN 加密方案中;文献[9]进一步提出并实现了基于身份且无信息交换的可认证密钥分配方案,这种无信息交换的密钥协商难以实现密钥的更新;文献[10]使用基于身份的签名提出一个认证框架,其中的认证仍然采用广播/多播式认证;文献[11]提出基于身份签密的 WSN 认证及密钥协商协议;文献[12 – 13] 针对不同环境下分别提出了基于身份签密方案;文献[14]将基于 ECC 的组合公钥体制思想引入 WSN 节点的认证与密钥协商,避免了公钥证书的传递与认证,但其过程要经过多个步骤的运算与信息交互,消耗能量较多。

另一方面,上述协议都假定网络中所有的节点本身是可信并乐于提供服务,然而网络中节点有可能由于被捕获或者自私行为而不提供服务或提供错误的服务,采用完全信任的方式将导致泛洪和拒绝服务等攻击,使得网络性能急剧下降或引发大量安全问题,因此需要建立一种可信机制对节点进行管理。文献[15]指出节点间的可信关系可以通过可信管理系统实现或者通过增加额外的安全芯片实现。可信平台模块(Trusted Platform Module, TPM)以芯片的形式实现可信计算组织(Trusted Computing Group, TCG)提出的规范[16],在当前网络安全领域的应用中备受关注,其目的是为各类计算平台提供信任根,文献[15]以 TCG 规范为目标在节点认证前提供硬件级别的强安全机制保证节点的可信性。这类可信计算模式因为其签名和加密运算造成计算开销、通信造成能量损耗以及芯片本身的安全设计与成本,使其目前在资源受限的传感器节点中难以推广。相比较而言,近年来关于 WSN 可信研究最多的是基于节点行为的信任管理,文献[17]指出信誉分布服从 Beta 分布的特点,文献[18]将文献[17]的思想应用于 WSN,提出了一种基于 Beta 分布的传感器网络信誉框架(Reputation-based Framework for high integrity Sensor Networks, RFSN),文献[19]也采用同样的方法计算节点的信任度,这类模型是目前比较经典的信任管理模型,可较好地识别低信誉度节点。文献[20]同样指出为了评测节点的不良行为,需要引入信誉系统。本文目标是针对 WSN 拓扑多变、资源受限和且易受攻击等特点设计一种轻量级的可信认证方案,保证网络提供安全有效的服务。

2　基于节点行为和身份的可信认证方案设计

认证方案可分成两个阶段,分别为认证前期工作和认证过程。认证前期工作包括网络部署前节点初始化、部署后节点针对邻居进行的初始化以及邻居间基于身份产生共享的认证密钥。认证过程包括计算待认证节点的信任度和与可信节点的认证。根据节点行为的表现计算其信任度,再依据信任度对节点进行评测与识别,相互信任的节点间进行认证,这不仅避免与恶意节点进行认证从而提高网络安全性,同时避免与无效节点进行认证造成的浪费从而提高认证的效率,并且最终剔除网络内部行为不端的节点。下面详细介绍方案的设计过程。

2.1　网络初始化

在基于身份的认证方案中需要一个可信的实体(Trusted Authority,TA),在 WSN 中基站可以充当 TA。首先,TA 为每个传感器节点在椭圆曲线上选择一个点作为标识 id,经过映射函数 ϕ 处理后得到节点的公钥,如对于节点 X, $P_X = \phi(id_X)$。接着,TA 产生主密钥 s 并计算每个节点的私钥 $S_X = sP_X$。网络节点部署前,为每个节点加载节点标识 id_X、节点的私钥 S_X,除了 TA,只有节点 X 知道 S_X[7]。另外加载系统参数 $(q, E/F_q, G_1, G_2, e, W, H_1, H_2, f, \phi)$,其中:$q$ 为素数,E 为有限域 F_q 上的椭圆曲线,G_1 和 G_2 分别是 F_q 上的加法群和乘法群,e 为椭圆曲线双线性映射,W 是在 G_1 上选取的生成元,H_1 和 H_2 为不同的散列函数,f 为对称密码函数,ϕ 即前述映射函数。网络部署以后,每个节点在邻域内广播自己的标识 id,邻居节点保存其收到的 id,并设置该节点信誉参数的初值。

2.2　基于身份的一次交互密钥协商方案

密钥是实现认证的基础,本节基于节点身份利用公钥体制中双线性映射技术实现认证密钥的生成与更新。

部署后开始,WSN 节点一般属于同一利益实体,所以可以认为节点是可信的。节点 A 与邻居节点 B 通过获取的公开 id 推导出公钥,即 $P_A = \phi(id_A)$, $P_B = \phi(id_B)$。建立认证密钥 K_{AB} 信息流如下:

$A \rightarrow B$: id_A, N, h

计算密钥具体过程:

$S1$:A 发送消息(id_A, N, h)给 B,其中 $N = nP_A$(n 是 A 秘密选取的随机数), $h = H_1(id_A \| id_B, N)$, 计算 $K_{AB} = e((n+h)S_A, P_B)$;

$S2$:B 收到(id_A, N, h)后,验证 N 的有效性,计算 $K_{BA} = e(N + hP_A, S_B)$;

在密钥协商过程中只要一次数据的传送,即可获得双方共有的密钥对 K_{AB}。为了保证安全性,计算 K_{AB} 后将 n 丢弃。随着网络的运行,很多情况下密钥需要更新,本文方案中两个互相信任的节点之间可以重新选择随机数 n 利用上述步骤更新配对密钥。

2.3　基于节点行为的信任度计算与决策

WSN 经常部署在无人值守环境,易受外部攻击;同时内部节点可能因被妥协从而发起内部攻击行为,如恶意节点的行为可能交替性地表现为正常或异常,自私节点有选择性转发或不转发上一跳节点发送的信息等。这些行为不仅降低网络的服务质量,而且可能提供虚假反馈等危害网络信息安全的服务,另外节点可能因为自身能量消耗等原因而变得不可靠,因此需引入可信评估机制,确保在节点相互认证前确认对方是可信的。本节根据节点间交互行为的结果,对节点进行评价,这种评价称为节点的信誉,被看作一种概率分布[17],再根据信誉的分布状况计算其信任度,为节点下一步的认证提

供决策依据。

文献[17]指出用户行为的信誉分布服从 Beta 分布，本文方案和 RFSN 模型[18]一样采用 Beta 分布来表示传感器节点行为的信誉，并对文献[17]中信誉更新进行改进，求得节点 A 对 B 的直接信任。考虑到 WSN 高度自治，且为了减少通信量、计算量和存储空间，本文方案只考虑一个节点与另一节点直接交互的结果，并以其计算节点的信任度，与信任阈值比较判断节点是否可信。

Beta 分布有两个参数，利用伽玛函数 Γ 表示 Beta 分布 $f(x\mid\alpha,\beta)$[17-18] 如下：

$$Beta(\alpha,\beta)=f(x\mid\alpha,\beta)=\frac{\Gamma(\alpha+\beta)}{\Gamma(\alpha)\Gamma(\beta)}x^{\alpha-1}(1-x)^{\beta-1};$$

$$x\in[0,1],\alpha>0,\beta>0 \tag{1}$$

Beta 分布的概率期望值为：

$$E(x)=\alpha/(\alpha+\beta) \tag{2}$$

节点交互的事件发生后有两种结果，成功或失败。用 r 表示某时段成功通信事件发生的总次数，s 表示某时段失败通信事件发生的总次数。那么经过 $r+s$ 次事件后，后验分布仍然服从 Beta 分布，函数中参数满足：

$$\alpha=r+1,\beta=s+1;r,s\geqslant 0 \tag{3}$$

根据文献[17]思想，假设在 t_1 时刻节点 A 关于节点 B 的信誉分布的先验概率为 X，服从 Beta 分布，记为 $X\sim Beta(\alpha+1,\beta+1)$，$t_2$ 时刻节点 A 和节点 B 又执行了 $r+s$ 次事件之后，信誉的分布仍然服从 Beta 分布且新的分布 X' 满足：

$$X'\sim Beta(\alpha+r+1,\beta+s+1) \tag{4}$$

式(4)中没有考虑节点信誉动态性问题，引入时间遗忘因子 $\theta(\theta\in[0,1])$ 调整历史信誉对最近信誉的影响，则 Beta 分布参数[18]变化为：

$$\begin{cases}\alpha'=\alpha\theta+r\\ \beta'=\beta\theta+s\end{cases} \tag{5}$$

随着时间改变 t_2 时刻的信誉变成了历史信誉，t_3 时刻需重新计算新的信誉，如此循环下去。为了便于计算，采用递归的方法即可表示最新的 Beta 分布的参数，如式(6)：

$$\begin{cases}\alpha=\alpha\theta+r\\ \beta=\beta\theta+s\end{cases} \tag{6}$$

节点信任度 T 为信誉分布的统计期望：

$$T=E(Beta(\alpha+1,\beta+1))=\frac{\alpha+1}{\alpha+\beta+2} \tag{7}$$

网络部署后(假定网络初始时不存在攻击)相邻节点可以利用认证密钥直接进行认证，随着网络的运行，节点行为不断变化，节点的信誉也在改变，节点每隔一段时间对邻居信誉进行维护。维护的方法是节点 A 根据存储的节点 B 的历史信誉参数以及最近周期内与 B 交互的结果(r,s)，利用式(6)即可更新信誉。

尽管节点之间的信任关系在变化，但在一段时间内其信任值相对固定，所以 A 与 B 认证之前只需根据保存的对方最新的信誉利用式(7)计算其信任度。若信任度低于系统信任阈值，则认为该节点不可信，不与之交互；否则认为该节点可信，继而利用节点之间已经拥有的认证密钥进行身份认证，提高网络的安全性与认证的效率。

2.4 可信节点间的认证过程

基于共享的密钥，两节点之间可以采用对称密钥认证体制进行身份认证，假定相邻节点间时钟松散同步。若节点 A 和 B 要进行相互认证，两者的共享密钥为 K_{AB}，A 为发起者。加入时间戳保持新鲜性并防止重放攻击，利用 Hash 函数 H_2 保证消息的完整性，防止消息被篡改。认证过程信息流如下：

$A\rightarrow B$: C_A, id_A, $Time_1$, MAC_A

$B\rightarrow A$: C_B, id_B, $Time_2$, MAC_B

认证具体过程如下。

步骤 1　节点 A 将消息$(C_A, id_A, Time_1, MAC_A)$发送给 B，其中 n_1 是一随机数，$C_A=f_{K_{AB}}(n_1)$ 即利用加密函数 f 对 n_1 加密，$Time_1$ 是时间戳，$MAC_A=H_2(n_1\parallel id_A\parallel id_B\parallel Time_1)$。

步骤 2　节点 B 根据时间戳 $Time_1$ 判断消息的新鲜性，若是新消息，则用 K_{AB} 解密 C_A，得 n'_1，计算 $H_2(n'_1\parallel id_A\parallel id_B\parallel Time_1)$并判断是否等于 MAC_A，若相等 B 可以确认 A 的身份。同时 B 产生一随机数 $n_2(n_2\neq n_1)$，计算 $C_B=f_{K_{BA}}(n_2)$ 和 $MAC_B=H_2(n_2\parallel id_B\parallel id_A\parallel Time_2)$，将$(C_B, id_B, Time_2, MAC_B))$发送给 A，其中 $Time_2$ 是新的时间戳。

步骤 3　同理，节点 A 收到信息后，根据时间戳判断消息的有效性。若有效，则用 K_{AB} 解密 C_B 得 n'_2，若 $n'_2\neq n_1$ 再验证 MAC_B，即可确定 B 的身份。

在认证的过程中每个节点只需要发送一次信息。

3 方案分析

对于资源受限的 WSN，在设计认证方案时，既要保证方案的安全性，又要考虑运行的效率。

3.1 安全性分析

1)密钥安全性。

先利用双线性函数 e 的特性[9]证明 $K_{BA}=K_{AB}$ 的正确性，已知：$S_A=sP_A$，$S_B=sP_B$，$N=nP_A$。

证明
$$\begin{aligned}K_{AB}&=e((n+h)S_A,P_B)=e((n+h)sP_A,P_B)=\\ &e((n+h)P_A,P_B)^s=e((n+h)P_A,sP_B)=\\ &e((n+h)P_A,S_B)=e(nP_A+hP_A,S_B)=\\ &e(N+hP_A,S_B)=K_{BA}\end{aligned}$$

在密钥协商过程中，只有掌握了 S_A 才能正确计算$e((n+h)S_A,P_B)$，只有掌握了 S_B 才能正确计算 $e(N+hP_A,S_B)$，另外密钥是在本地计算而得，因此密钥是安全的。而 SPINS 中节点间的密钥是基站分发的，虽然经过了加密和认证处理，但需要在无线信道上传输，所以相比较而言，其安全性会有所下降。

2)认证安全性。

无线链路信道易遭受干扰、窃听、注入、重放等多种外部攻击，本文方案与 SPINS 中外部节点因为没有掌握认证密钥，而无法实现干扰、窃听、注入等攻击，同时在认证信息中加入随机数和时间戳(或计时器)可抵御重放攻击。节点通信前需要认证操作，减少了拒绝服务(Denial of Service, DoS)攻击、Hello Flood 攻击。

3)实体安全性。

在无线传感器网络中，若内部节点被俘，则会存在着 Sybil 攻击、选择性转发攻击、Sinkhole 攻击和 Wormhole 攻击等节点级内部攻击。本文方案中实体(节点)安全性是通过信任管理实现的，信任系统可以有效提高自治网络性能，并通过计算节点信任度，有效抵御选择性转发攻击、Sinkhole 攻击和 Wormhole 攻击。引入节点的身份标识，保证身份与实体唯一对应关系，避免节点通过非法宣称多个身份而实现 Sybil 攻击，同时预防节点通过有意的离开再加入系统来消除以前身份的低信任度的 Newcomer 攻击。SPINS 协议没有考虑内部

节点被俘问题,不能抵御内部节点的攻击。

3.2　性能分析

1)认证过程通信负载与计算量。

本文方案和 SPINS 协议实体间的认证都是基于两者共享的密钥,认证过程相似,但产生的密钥方法不同。两者产生共享密钥的通信与计算量如表 1 所示。

表 1　本文方案与 SPINS 对比

方案	通信次数	消息摘要	运算	基站
SPINS	至少 4 次	3 次	2 次加密与解密	密钥由基站产生
本文方案	1 次	1 次	2 次双线性映射	基站不参与运算

SPINS 节点间产生共享密钥需要经过基站的分配,在每个节点都能和基站直接通信的前提下,需要进行 4 次的信息交互,否则将增加信息转发的次数,故本文方案在通信负载和能耗方面明显优于 SPINS,因为发送信息在传感器运行过程中是最耗能的。

2)网络生命期与认证速度。

SPINS 基站附近的节点因为频繁转发数据包而很快耗尽能量,缩短了网络生命期。节点间认证前都需要向基站发送请求信息,基站需为双方分配密钥,导致网络认证缓慢。本文方案中将网络负担分配到各节点,即增加节点侦听机制,用于确认每次交互结果,再周期性地计算节点可信度。相邻节点根据可信度自组织式进行认证,不需要中间节点的转发,也不需要基站的参与,认证速度快,也避免了 SPINS 基站附近节点易成为瓶颈问题,延长了网络生命周期。

3)存储需求。

SPINS 中节点需要存储系统参数和与基站共享的密钥,本文方案需要存储系统参数、私钥以及邻居节点的信誉参数,因此本文方案占用更多的存储空间。但是随着传感器技术的发展,其存储能力和运算能力都在提高。

4)可扩展性。

如果传感器节点数目大量增加,由于本文方案是自组织式认证,不会给网络带来额外的负担,便于扩展,只是每个节点存储邻居节点的信誉参数可能会有所增加,因为假定网络节点总数 $n=400$,其邻居节点数平均约为 $\sqrt{n}=20$ [21];若 $n=500$,其邻居节点数约为 $\sqrt{n}\approx 22$。当网络规模较大时,邻居增加量可以忽略不计。但是随着节点的大量增加,SPINS 方案会因为大量的信息交互使网络负担极速提高,所以其扩展性相对较差。

4　结语

无线信道的开放性以及传感器节点经常部署在恶劣环境,使得 WSN 比传统网络面临更多的安全威胁,因此在与节点进行通信前不仅要进行身份认证,更要确认节点是可信的。由于 WSN 具有节点资源受限和网络拓扑结构变化大的特点,传统的认证措施无法在无线传感器网络中有效地应用。因此,本文提出了一个灵活的、轻量级的 WSN 可信认证方案。方案中利用节点唯一的身份和双线相对理论进行密钥的协商,其算法计算量小,交互的消息少。引入基于节点行为的信誉与信任管理思想,在认证前根据节点的信任度判断节点是否可信,若可信才进行下一步的认证或密钥更新,避免与内部恶意节点或无效节点的认证,提高了认证的有效性。因为方案中信任度的计算、密钥协商与认证过程都是自组织式且不需要第三方的参与,认证时延低,而且便于节点的加入与离开,网络可扩展性好。方案既能抵御外部节点入侵又能防范内部被俘节点的威胁,适合用在无人值守安全性要求较高的 WSN 应用领域。

参考文献:

[1] LUK M, PERRIG A, WHILLOCK B. Seven cardinal properties of sensor network broadcast authentication [C]// SASN'06: Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2006: 147 – 156.

[2] PERRIG A, SZEWCZYK R, TYGAR J D, *et al*. SPINS: security protocols for sensor networks [J]. Wireless Networks, 2002, 8(5): 521 – 534.

[3] WATRO R, KONG D, CUTI S-F, *et al*. TinyPK: securing sensor networks with public key technology [C]// Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2004: 59 – 64.

[4] MALAN D J, WELSH M, SMITH M D. A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography [C]// Proceedings of the 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks. Piscataway: IEEE Press, 2004: 71 – 80.

[5] BAUER K, LEE H. A distributed authentication scheme for a wireless sensing system [J]. ACM Transactions on Information and System Security, 2008, 11(3): 1 – 35.

[6] di PIETRO R, SORIENTE C, SPOGNARDI A, *et al*. Collaborative authentication in unattended WSNs [C]// WiSec'09: Proceedings of the Second ACM Conference on Wireless Network Security. New York: ACM Press, 2009: 237 – 244.

[7] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing [C]// Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology. Berlin: Springer-Verlag, 2001: 213 – 229.

[8] OLIVEIRA L B, DAHAB R, LOPEZ J, *et al*. Identity-based encryption for sensor networks [C]// Proceedings of the Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops. Piscataway: IEEE Press, 2007: 290 – 294.

[9] OLIVEIRA L B, SCOTT M, LOPEZ J, *et al*. TinyPBC: pairings for authenticated identity-based non-interactive key distribution in sensor networks [J]. Computer Communications, 2011, 34(3): 485 – 493.

[10] YASMIN R, RITTER E, WANG G. An authentication framework for wireless sensor networks using identity-based signatures [C]// Proceedings of the 2010 10th IEEE International Conference on Computer and Information Technology. Piscataway: IEEE Press, 2010: 882 – 889.

[11] 庞辽军,焦李成,王育民. 无线传感器网络节点间认证及密钥协商协议[J]. 传感技术学报,2008,21(8):1422 – 1426.

[12] 李聪,闫德勤,郑宏亮. 标准模型下高效安全的基于身份多签密方案[J]. 计算机应用,2012,32(4):957 – 959.

[13] 赵秀凤,徐秋亮. 一个有效的多 PKG 环境下基于身份签密方案[J]. 计算机学报,2012,35(4):673 – 681.

[14] 王潮,胡广跃,张焕国. 无线传感器网络的轻量级安全体系研究[J]. 通信学报,2012,33(2):30 – 35.

[15] YUSSOFF Y M, HASHIM H, BABA M D. Identity-based trusted authentication in wireless sensor networks [J]. International Journal of Computer Science Issues, 2012, 9(2): 1694 – 0814.

(下转第 1857 页)

1)数据库收到 M3 后,由初始假设 P2 根据消息含义规则 R1 从而有:

$$D \mid\equiv D \overset{K}{\longleftrightarrow} T,\ D \lhd \{r_1, r_2, T \overset{S_T}{\longleftrightarrow} D\}_K \mid - D \mid\equiv T \mid\sim \{r_1, r_2, T \overset{S_T}{\longleftrightarrow} D\} \tag{1}$$

2)由式(1)和初始假设 P1,根据消息新鲜性规则 R11,有:

$$D \mid\equiv \#\{r_1, r_2, T \overset{S_T}{\longleftrightarrow} D\} \tag{2}$$

3)由式(1)~(2),根据临时值验证规则 R4,有:

$$D \mid\equiv \#\{r_1, r_2, T \overset{S_T}{\longleftrightarrow} D\},\ D \mid\equiv T \mid\sim \{r_1, r_2, T \overset{S_T}{\longleftrightarrow} D\} \mid - D \mid\equiv T \mid\equiv \{r_1, r_2, T \overset{S_T}{\longleftrightarrow} D\} \tag{3}$$

4)由式(3),根据信念规则 R14,有:

$$D \mid\equiv T \mid\equiv \{T \overset{S_T}{\longleftrightarrow} D\} \tag{4}$$

5)由式(4)和初始假设 P2,根据管辖规则 R5,有:

$$D \mid\equiv T \mid\Rightarrow T \overset{S_T}{\longleftrightarrow} D,\ D \mid\equiv T \mid\equiv \{T \overset{S_T}{\longleftrightarrow} D\} \mid - D \mid\equiv \{T \overset{S_T}{\longleftrightarrow} D\} \tag{5}$$

6)标签收到 M5 后,由初始假设 P6,根据消息含义规则 R1,有:

$$T \mid\equiv T \overset{K}{\longleftrightarrow} D,\ T \lhd \{r_1, r_2, T \overset{S'}{\longleftrightarrow} D\}_K \mid - T \mid\equiv D \mid\sim \{r_1, r_2, T \overset{S'}{\longleftrightarrow} D\} \tag{6}$$

7)由式(6)和初始假设 P5,根据消息新鲜性规则 R11,有:

$$T \mid\equiv \#\{r_1, r_2, T \overset{S'}{\longleftrightarrow} D\} \tag{7}$$

8)由式(6)~(7),根据临时值验证规则 R4,有:

$$T \mid\equiv \#\{r_1, r_2, T \overset{S'}{\longleftrightarrow} D\},\ T \mid\equiv D \mid\sim \{r_1, r_2, T \overset{S'}{\longleftrightarrow} D\} \mid - T \mid\equiv D \mid\equiv \{r_1, r_2, T \overset{S'}{\longleftrightarrow} D\} \tag{8}$$

9)由式(8),根据信念规则 R14,有:

$$T \mid\equiv D \mid\equiv \{T \overset{S'}{\longleftrightarrow} D\} \tag{9}$$

10)由式(9)和初始假设 P4,根据管辖规则 R5,有 $T \mid\equiv D \mid\Rightarrow T \overset{S'}{\longleftrightarrow} D$, $T \mid\equiv D \mid\equiv \{T \overset{S'}{\longleftrightarrow} D\} \mid - T \mid\equiv T \overset{S'}{\longleftrightarrow} D$。

证毕。

3　结语

重放攻击和数据篡改攻击是攻击者利用的主要形式,目前提出协议大多数不能抵抗这些攻击。本文基于矩阵理论设计了一个抵抗这些攻击的低成本安全协议 MSP。通过不同算法门电路分析,MSP 所需算法门电路不超过 1 000,满足低成本要求。在同等算法规模下,MSP 大大降低了标签存储量和标签计算复杂度。经 BAN 逻辑分析,MSP 实现了安全认证。因此,MSP 适用于 RFID 环境。

参考文献:

[1] DUC D N, LEE H, KIM K. Enhancing security of EPC global GEN-2 RFID tag against traceability and cloning[EB/OL]. [2012 - 12 - 20]. http://www.autoidlabs.org/uploads/media/AUTOIDLABS-WP-SWNET-016.pdf.

[2] CHIEN H Y, CHEN C H. Mutual authentication protocol for RFID conforming to EPC Class 1 Generation 2 standards [J]. Computer Standards and Interfaces, 2007, 29(2): 254 - 259.

[3] PERIS-LOPEZ P, HERNANDEZ-CASTRO J C, TAPIADOR J M E, *et al*. Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard [J]. Computer Standards and Interfaces, 2009, 31(2): 372 - 380.

[4] SARMA S E, WEIS S A, ENGELS D W. RFID systems and security and privacy implications [C]// Proceedings of the 4th International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2003: 454 - 469.

[5] SARMA S E, WEIS S A, ENGELS D W. Radio frequency identification: secure risks and challenges [J]. RSA Laboratories Cryptobytes, 2003, 6(1): 2 - 9.

[6] WEIS S A, SARMA S E, RIVEST R L, *et al*. Security and privacy aspects of low-cost radio frequency identification systems [C]// Proceedings of the 1st International Conference on Security in Pervasive Computing. Berlin: Springer, 2004: 201 - 212.

[7] OHKUBO M, SUZUKI K, KINOSHITA S. Hash-chain based forward-secure privacy protection scheme for low-cost RFID [C]// Proceedings of the 4 th Symposium on Cryptography and Information Security. Berlin: Springer, 2004: 719 - 724.

[8] CHOI E Y, LEE S M, LEE D H. Efficient RFID authentication protocol for ubiquitous computing environment [C]// EUC 2005: Proceedings of the 2005 International Conference on Embedded and Ubiquitous Computing. Berlin: Springer, 2005: 945 - 954.

[9] FELDHOFER M, DOMINIKUS S, WOLKERSTORFER J. Strong authentication for RFID systems using the AES algorithm [C]// CHES' 04: Proceedings of 2004 Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2004: 357 - 370.

[10] GOLLE P, JAKOBSSON M, JUELS A, *et al*. Universal re-encryption for mixnets [C]// Proceedings of the 2004 RSA Conference, Cryptographer' s Track. Berlin: Springer, 2004: 163 - 178.

[11] STALLINGS W. Computer security: principles and practice [M]. 2nd ed. Upper Saddle River, NJ: Prentice Hall, 2011.

[12] 裴友林, 杨善林. 基于密钥矩阵的 RFID 安全协议[J]. 计算机工程, 2008, 34(19): 170 - 173.

[13] 游相柏, 刘毅敏. RFID 安全认证协议研究[J]. 电视技术, 2012, 36(15): 104 - 107.

(上接第 1845 页)

[16] GRAWROCK D. TCG specification architecture overview [EB/OL]. [2012 - 12 - 15]. http://www.trustedcomputinggroup.org/resources/tcg_architecture_overview_version_14.

[17] JØSANG A, ISMAIL R. The Beta reputation system [C]// Proceedings of the 15th Bled Electronic Commerce Conference. Bled, Slovenia: Electronic Commerce Center Press, 2002: 41 - 55.

[18] GANERIWAL S, SRIVASTAVA M B. Reputation-based framework for high integrity sensor networks [C]// SASN'04: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM Press, 2004: 66 - 77.

[19] 肖德琴, 冯健昭, 杨波, 等. 基于无线传感器网络的信誉形式化模型[J]. 计算机科学, 2007, 34(6): 84 - 87.

[20] AHMED M R, HUANG X, SHARMA D. A novel misbehavior evaluation with Dempster-Shafer theory in wireless sensor networks [C]// MobiHoc'12: Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing. New York: ACM Press, 2012: 259 - 260.

[21] 蹇波, 郭永辉, 罗长远, 等. 基于 ECC 的无线传感器网络密钥管理协议[J]. 计算机工程, 2010, 36(3): 142 - 144.