无线传感器网络EMSR协议的安全性分析

韩坚华[1]，吴柳飞[2]

(1. 广东工业大学计算机学院 广州 510006; 2. 西安电子科技大学通信工程学院 西安 710071)

【摘要】针对目前无线传感器网络密钥管理方案存在的安全问题，给出了一种可证明安全的无线传感器网络的认证密钥建立方案(EMSR)，使用公钥证书实现网络节点的双向认证，同时产生双方共享与相互控制的会话密钥，有效地防止了纯粹使用对称加密机制产生的认证问题。在CK安全模型下，对EMSR协议进行了安全性证明，并对几种基于公钥机制的密钥建立方案进行了性能分析。结果表明，EMSR方案具备CK安全模型下相应的安全属性以及支持资源受限的网络节点的优势，符合传感器网络的通信要求。

关 键 词 认证; CK安全模型; 密钥管理; 无线传感器网络

中图分类号 TP309 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.03.020

Analysis on Security of EMSR Protocol in Wireless Sensor Network

HAN Jian-hua[1] and WU Liu-fei[2]

(1. School of Computer, Guangdong University of Technology Guangzhou 510006;

2. School of Telecommunications Engineering，Xidian University Xi'an 710071)

Abstract According to the security problem existing in current key management scheme of wireless sensor network, an authenticated key establishing scheme (EMSR) which is used in wireless sensor network and can be proved to be safe is put forward. By applying public key certificate, the mutual authentication is realized. At the same time, the authentication problem caused by the absolute use of symmetric encryption mechanism can be efficiently avoided. In CK security model, security proof for EMSR protocol has been carried out and the performance of key establishing scheme based on several kinds of public key mechanism has been analyzed. The results of security proof and performance analysis show that the EMSR has the advantages on the responding security properties in security model and supporting the net node whose resources are limited, and satisfies the communication requirements of wireless sense net.

Key words authentication; Canetti-Krawczyk security model; key establishment; wireless sensor network

无线传感器网络(wireless sensor network, WSN)是新一代的传感器网络，具有非常广泛的应用前景，其发展和应用将会给人类的生活和生产的各个领域带来深远的影响。但是，其通信是通过集成在其上的射频设备来实现的，因为使用了全向天线，所以只要在接受范围内的任何人都可以接受到该网络的信息。目前，无线传感器网络安全面临了传感器节点易被捕获控制、网络拓扑结构动态变化、传感器节点的资源高度受限以及信息的安全受到极大威胁等一系列的问题。由于传感器网络节点的低耗能、低计算能力的条件限制，传统的基于可信第三方的加密体制已经不适用于节点繁多的WSN。随着WSN的广泛应用，对高效轻量的安全密钥管理方案的需求也越来越迫切。

近年来，各种基于公钥体制的密钥交换协议[1-3]在无线传感器网络中交迭出现，但是这些方案对于WSN代价高昂。文献[3]假设存在可信第三方，且每个节点与服务器共享一个密钥，使存储开销随着网络规模的增加成为瓶颈，且节点与基站通信频繁，有较大的局限性。文献[4]对SPINS方案改进后，将节点多次广播降低为一次广播，减少了能源消耗，但是对主密钥依赖过高，网络抗毁性差，密钥更新困难。利用RSA公钥技术，文献[5]给出了一个WSN分配方案。然而，其密钥建立过程只是简单套用Diffie-Hellman密钥交换机制，而且对节点存储能力要求较高。该机制在复杂的传感器网络环境中易受各类攻击，如重放攻击、交错攻击、中间人攻击等。文献[6]给出了基于ECC的具有半前向保密性的证书

收稿日期：2008 –01 – 11；修回日期：2008 – 05 – 25
基金项目：国家自然科学基金(60573048)
作者简介：韩坚华(1955 –)，女，副教授，主要从事分布式协同软件方面的研究.

建立方案(modular square root，MSR)，提出了WSN的认证和密钥建立协议。该协议通信量大，且密钥建立方案不能抵抗传感器网络环境中的常见攻击。针对WSN能源有限的特点，文献[7]提出一种高效的认证公钥分配方案。文献[8]分析了一般的公钥密钥算法在WSN中的能源消耗，说明了灵活的公钥技术适用大规模的WSN。一些文献提出了很多基于对称的密钥分配方案[9-11]，可以有效地解决密钥分配问题；但是容易受到外界攻击，单点失效将对整个网络造成毁灭性打击。所以，基于公钥技术的协议更具有灵活性，而且适用于大规模的传感器网络。

从安全性出发，本文在高效证书建立机制的基础上[6]，给出了一种安全的WSN认证的密钥建立方案EMSR。该方案通信开销小，计算速度快，可以有效地防止单点失效对整个网络带来的负面影响，并且适用于大规模的传感器网络。同时，该方案可以提供CK安全模型下安全性的形式化证明，抵抗已知攻击，具有较高的安全性。

1 密钥分配方案

1.1 系统假设

(1) WSN采用已知的层次路由协议，自组织成簇，应用拓扑，如图1所示。

(2) 基本的无线通信是不安全的。

(3) 每个传感器节点在应用上对等，并且可能被俘获。

(4) 每个传感器节点有唯一的身份标识ID。

(5) 基站WSN与外部世界的网关，主要负责颁发和验证节点的证书。

⑹ 基站的功能强大，能直接向所有的节点广播消息。

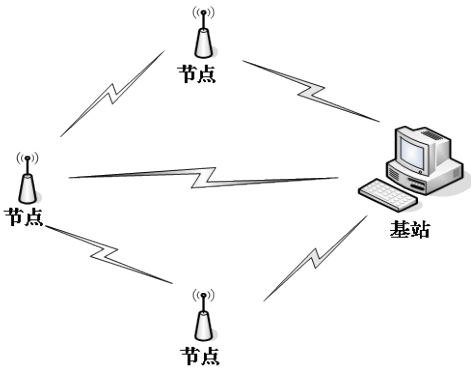

图1 传感器网络应用场景

1.2 协议的整体步骤

本文使用带有证书的密钥建立协议防止冒充，它提供一个用来检查公钥持有人是否是该网络的合法成员的机制。证书[6,12]包括一个简单公钥、CA签名的节点ID和证书使用期限。在节点部署前，所有的节点向CA进行证书申请，CA对证书申请实体的身份进行确认后，为其制作和颁发证书。该证书的较低通信复杂度十分适用于传感器网络。在此基础上，本文给出无线传感器网络的密钥分配协议EMSR，其协议的执行如下：

P_i P_j分别代表各自的身份，并满足前提条件：同一个系统范围内的用户共享一个非超奇异高阶椭圆曲线$E(F_q)$，$P\in E(F_q)$且阶为n，其中s为会话密钥标识，则P_i、P_j通过以下步骤的会话，实现双向认证和双向认证的密钥交换：

$P_i \to P_j$： P_i,s,α

$P_j \to P_i$： $P_j,s,\beta,\mathrm{SIG}_j(k,P_j,s,\beta,\alpha,P_i)$

$P_i \to P_j$： $P_i,s,\mathrm{SIG}_i(k,P_i,s,\alpha,\beta,P_j)$

(1) 当P_i关联或者重新关联至P_j时，P_i随机选择x，计算$\alpha=x\cdot P$，产生会话标识s；然后向P_j发送激活消息P_i、s、α。(2) P_j收到P_i发送的激活消息后，检查s的新鲜性。如果验证失败，则丢弃该消息；否则，产生用于ECDH(基于ECC的Diffie-Hellman协议)交换的临时私钥y，临时公钥$\beta=y\cdot P$及计算共享密钥$k=y\cdot\alpha$，并且发送自己的挑战P_j、s、β、$\mathrm{SIG}_j(k,P_j,s,\beta,\alpha,P_i)$给$P_i$。(3) P_i收到P_j的挑战后，验证s的新鲜性、P_j的身份。如果失败，则解除链路请求；否则，产生自己的一个签名消息发送给P_j，并且计算共享密钥$k=x\cdot\beta$。(4) P_j收到P_i的消息后，验证签名的有效性，成功后确认对方与之共享会话密钥，可以进行下一步的通信。

该协议运行成功之后，P_i、P_j共享了会话密钥k，同时擦除了临时私钥x和y。

只要节点不被攻破，P_i和P_j就可以利用已经得到的会话密钥进行下一步的通信。节点部署好后，按照上述协议与其他节点建立共享密钥。完成密钥建立后，传感器网络就可以形成一个安全的通信拓扑结构。

2 安全性分析

2.1 CK安全模型

CK模型给出了会话密钥安全的定义，采用模块化的思想设计和分析密钥交换协议，简化了安全协议设计和分析的难度，同时，采用不可区分性的概念定义安全性如下：在允许的攻击能力下，如果攻击者不能区分协议产生的密钥和一个独立的随机

数，就认为该协议是安全的。

非认证链路(UM)下的敌手模型如下：将敌手U作为一个概率多项式时间的图灵机，控制整个通信网络。它可以通过会话状态泄漏、会话密钥询问和参与方破坏3种形式的攻击获得秘密信息。会话状态泄漏针对的是一个未完成的会话，敌手仅获得会话的内部状态；会话密钥询问针对已完成的会话，敌手获得会话密钥；参与方破坏表明敌手得到该参与方的所有内部状态，包括长期密钥和会话信息。

为了定义协议的安全性，CK中还引入测试会话询问为：敌手可以对一个已完成、未过期和未暴露的会话进行测试询问。设k是会话密钥，掷币b，$b \leftarrow_R \{0,1\}$。如果$b=0$，把k给U；否则，从密钥空间中随机选取一值r给U。允许进行测试会话询问的敌手称为KE-敌手。

认证链路模型(AM)下的敌手模型如下：类似于UM的定义方式，可以给出认证链模型AM下的敌手$\mathcal{A}$的定义。区别在于$\mathcal{A}$只能如实地传递由合法参与方产生的消息。

认证器定义为：认证器是一个特殊的协议编译器，以AM下的安全协议为输入，输出UM下安全属性相同的协议。

匹配会话定义为：CK安全模型中，参与方A产生一个以(A,B,s,role)为输入的会话，B产生一个以(B,A,s',role')为输入的会话。若$s=s'$，则称这两个会话匹配。其中，s、s'是会话密钥标识，$\text{role},\text{role}' \in \{\text{initiator},\text{responder}\}$，且$\text{role} \neq \text{role}'$。

此外，CK模型中还定义了会话“过期”，敌手不允许对已经过期的会话进行会话密钥询问或会话状态泄漏，但是允许参与方破坏。

定义 1　SK-安全。称协议π是SK-安全的，如果对任意的KE-敌手$\mathcal{E}$，π满足：

(1) 若未破坏的参与方A、B完成一个匹配会话，则A、B输出相同的密钥。

(2) $\mathcal{E}$正确猜测b的概率小于$1/2$加上一个可忽略的量。

定义1不仅具有简洁的形式，并且保证了密钥交换协议的良好性质。如保证会话密钥被合理分配，认证性得到交换，抗击中间人攻击，抵抗已知密钥攻击，具有完善的前向保密性(perfect forward secrecy，为PFS)等。

2.2　安全性证明

AM下SK-安全的ECDH协议如下：设$P \in E(F_q)$，P的阶n为素数。P_i、P_j共享会话密钥$k = x \cdot \beta = y \cdot \alpha$。

(1) $P_i \to P_j$：$s, P_i, \alpha = x \cdot P$。(2) $P_j \to P_i$：$s, P_j, \beta = y \cdot P$。

ECDDH假设如下：给定定义于有限域F_q上的非超奇异椭圆曲线E，点$P \in E(F_q)$，阶为n，$x,y,z \in_R [1, n-1]$，则对于任何多项式时间的算法$\mathcal{D}$，$Q_0 = \langle P, x \cdot P, y \cdot P, x \cdot y \cdot P \rangle$和$Q_1 = \langle P, x \cdot P, y \cdot P, z \cdot P \rangle$计算不可区分。

另外，假定协议中用到的一些极微本原(如数字签名、消息鉴别码和伪随机函数)为安全的。

定理 1　在ECDDH假设下，ECDH协议是AM中的SK-安全协议。

证明　(1) 证明ECDH协议满足定义1的条件(1)。显然，两个未破坏的P_i和P_j如果都完成该协议，则双方共享密钥$k = x \cdot \beta = y \cdot \alpha$；而且会话标识将$x \cdot P$和$y \cdot P$与该匹配会话绑定，保证了会话密钥的唯一性。(2) 证明ECDH协议满足定义1的条件(2)。假设存在一个AM中的KE-敌手$\mathcal{A}$，以一个不可忽略的优势ε'猜到测试会话中的b，则可以构造算法$\mathcal{D}$，能够以不可忽略的优势区分Q_0和Q_1。算法$\mathcal{D}$的具体描述如下：

输入：$\langle q, P, \alpha^*, \beta^*, \gamma^* \rangle$

(1) 选择$r \leftarrow_R \{1, 2, \cdots, l\}$。

(2) 激活AM中的敌手$\mathcal{A}$和协议的合法参与方运行ECDH，将q和P作为协议的公开参数发给$\mathcal{A}$。

(3) 当$\mathcal{A}$激活一个参与方建立一个新会话(除第r次会话)或收到消息时，$\mathcal{D}$替代该参与方，执行协议ECDH。会话过期时，参与方将相应的会话密钥从记忆中擦除；若参与方破坏或会话(除第r次会话)泄漏时，$\mathcal{D}$将参与方或会话的相关信息提交给$\mathcal{A}$。

(4) 当第r次会话被激活时，$\mathcal{D}$通过P_i把消息(P_i, s, α^*)发送给P_j。

(5) 当P_j收到消息(P_i, s, α^*)时，$\mathcal{D}$通过P_j把消息(P_j, s, β^*)发送给P_i。

(6) 如果会话(P_i, P_j, s)被$\mathcal{A}$选中进行测试询问，则$\mathcal{D}$将γ^*作为响应给$\mathcal{A}$。

(7) 如果会话(P_i, P_j, s)已经泄漏，或其他会话被选中作为测试会话，或$\mathcal{A}$没有选测试会话就停止了，则$\mathcal{D}$输出$b' \leftarrow_R \{0,1\}$，然后停止。

(8) 如果$\mathcal{A}$停止且输出b'，则$\mathcal{D}$输出相同的b'，停止。

由此可知，由$\mathcal{D}$激发的$\mathcal{A}$的执行和$\mathcal{A}$直接执行ECDH协议是完全相同的。

设 P_0、P_1 分别表示为输出b(0或1)的概率，有 $P_0+P_1=1$，$|P_0-P_1|\geqslant\varepsilon$ (ε为一个可忽略的量)，由 $\mathcal{D}$ 激发 $\mathcal{A}$ 的执行时，$\mathcal{A}$ 与 $\mathcal{D}$ 的视图是相同的，考虑以下两种情况：

(1) 如果 $\mathcal{A}$ 选中第 r 次会话作为测试会话，则 $\mathcal{A}$ 得到的响应是 γ^*。因为 $\mathcal{D}$ 的输入分别以 P_0、P_1 的概率来自 Q_0 和 Q_1，Q_0 和 Q_1 的分发是同等分布的，所以 $\mathcal{D}$ 区分输入是来自 Q_0 还是 Q_1 的概率为 $(P_0+P_1)/2$。

(2) 如果 $\mathcal{A}$ 没有选中第 r 次会话作为测试会话，$\mathcal{D}$ 输出一个随机数，$\mathcal{D}$ 区分输入是来自 Q_0 还是 Q_1 的概率还是 $(P_0+P_1)/2$。

设 $P_0>P_1$，有 $(P_0+P_1)/2=(2P_1+\varepsilon)/2<1/2+\varepsilon/2$。

第 r 次会话中，情况(1)出现的概率是 $1/l$，情况(2)出现的概率是 $1-1/l$，所以 $\mathcal{D}$ 正确猜测 b 的概率小于 $1/2+\varepsilon/2l$，这与 $\mathcal{D}$ (也是 $\mathcal{A}$)能够以一个不可忽略的优势区分输入是来自 Q_0 还是 Q_1 的假设矛盾，因此，$\mathcal{D}$ 满足ECDDH假设(即定义1的条件(2))，协议ECDH满足AM下的SK-安全定义。

定理 2 令 π 是AM模型中的SK-安全协议，λ 是MT-authenticator，则 $\pi'=C_\lambda(\pi)$ 是UM模型中的SK-安全协议。

已知：π 为ECDH协议，是AM模型中的SK-安全协议。

构造 λ (基于签名的MT-authenticator[13])如下：

(1) $P_i\rightarrow P_j$： m。

(2) $P_j\rightarrow P_i$： m,s。

(3) $P_i\rightarrow P_j$： $m,SIGN_i(m,s,P_i)$。

结合piggy-baking技术，将ECDH协议的每步应用MT-authenticator，可以得到 $\pi'=C_\lambda(\pi)$，是本文给出的EMSR协议。

证明 λ 是一个基于签名的认证器，C_λ 是将协议 π 的每一步应用 λ 运算法则而转换为协议 π' 的认证器[13]，根据CK安全模型中认证器的编译功能可知，以AM下的安全协议为输入，输出UM下安全属性相同的协议。所以，EMSR协议是UM下满足SK-安全的协议。

2.3 小 结

由上述分析可知，EMSR协议可以提供CK计算模型下安全性的形式化证明，从而具有以下的安全属性：

(1) 抵抗重放攻击，可由会话密钥标识 s 的新鲜性保证。

(2) 双向身份认证，双方通过各自的身份进行相互认证，基站的鉴别结果和签名保证了节点身份的合法性和真实性，从而达到双向身份认证的安全目标。

(3) 双向认证的密钥协商和密钥控制，证书鉴别过程以Diffie-Hellman密钥交换协议为基础，密钥协商的新鲜性由双方各自适当选取的随机数来保证。双方独享确认密钥由双方对于密钥生成素材的数字签名来保证。安全参数 α 和 β 每次分别由 P_i 和 P_j 随机选取，因此，P_i 或 P_j 均无法单独控制密钥的生成。

(4) 双向密钥确认，协议结束后，通过 P_i 和 P_j 分别计算 $k=x\cdot\beta$ 和 $k=y\cdot\alpha$，双方可以确保对方同时具有某一特定的密钥。

(5) 完善前向保密性，基密钥的建立过程是通过Diffie-Hellman密钥交换机制正确协商得到的，所以该协议具有PFS特性。

3 性能分析

由前面的分析可知，EMSR协议具备了较高的安全属性，保证了通信的安全性和可靠性。传感器网络的最大特点之一就是存储容量有限，所以在保证网络能以安全方式进行通信的情况下，应当尽可能少地占用存储资源。EMSR方案的性能如下：

(1) 协议的轻型化。各个节点中存储一个96 bit的静态公私钥对和证书以及存储内存[6]。对于目前传感器节点是可以接受的，而且在基于公钥的密钥管理方案中也是较好的。

(2) 可扩展性。随着网络规模的增大，各个节点的存储不变，通信开销、计算开销和存储负担增加不明显，所以该方案具有较好的可扩展性，且适用大规模传感器网络。

(3) 抗毁性。临时密钥的及时撤销有效地保障了网络的可持续使用性，并且使网络具有较好的弹性和健壮性。而且网络中任何一个会话密钥都是唯一的，能防止单点失效对其余部分的影响。即使敌手通过物理捕获传感器节点，得到该节点的密钥信息，但得不到该节点以前的会话密钥信息，也不会对其他节点和节点间链路造成破坏。

(4) 自组织性。各个节点随时可以向基站申请证书，各自发起自己的密钥协商和认证过程。因此，该方案十分适用具有动态变化拓扑结构的传感器网络的密钥建立。另外，密钥的更新可以与密钥建立使用同一协议，大大减少了保密机制的能量开销。

因此，EMSR方案在与MSR方案等同计算量的

前提下，两个节点实现双向认证和密钥交换仅需5步，比MSR方案少。另外，EMSR方案还克服了MSR方案安全性方面存在的漏洞，给出了CK安全模型下的安全性证明。同时，EMSR方案继承了MSR方案良好的特性，同样适用自组织的传感器网络环境。相对其他基于公钥的传感器网络密钥分配方案，本文给出一个基本比较，如表1所示。n为网络规模，PRF代表伪随机函数计算开销。

表1　基于公钥方案间的比较

解决方案	扩展性	抗毁性	计算开销	通信开销	安全性	安全性证明
SPIN	一般	一般	1个PRF	$O(n^2)$	依赖基站	无
BROSK	一般	差	1个PRF	$O(n^2)$	依赖主密钥	无
TinyPK	一般	一般	2个PRF	$O(n^2)$	易受常见攻击	无
MSR	较好	较好	1个PRF	$O(n^2)$	易受常见攻击	无
EMSR	较好	较好	1个PRF	$O(n^2)$	抵抗常见攻击	CK模型下可证明安全

4　结　论

本文分析了无线传感器网络密钥分配问题，提出了一种可证明安全的无线传感器网络密钥分配方案。该方案可以抵抗无线传感器网络复杂环境中的常见攻击，保证节点间的安全通信。对该方案的形式化分析结果表明，EMSR方案可以提供CK安全模型下安全性的形式化证明，保证会话密钥被合理分配，实现了双向认证，抗中间人攻击，并且具有完善的前向保密性。

参　考　文　献

[1] Hubaux J P, Buttyan L, Capkun S. The quest for security in mobile Ad hoc networks[C]//ACM Symposium on Mobile Ad hoc Networking and Computing. Long Beach, California, USA: ACM Press, 2001: 146-155.

[2] SHOUP V. Practical threshold signatures[C]//Proc of Advances in Cryptology, Eurocrypt'00. Berlin: Springer-Verlag, 2000: 207-220.

[3] PERRIG A, SZEWCZYK R, WEN V, et al. SPINS: security protocols for sensor networks[C]//Mobile Computing and Networking. Rome, Italy: ACM Press, 2001: 189-199.

[4] CHENG B, SUNGHA D. Reduce radio energy consumption of key management protocol for wireless sensor networks [C]//ISLPED'04. California, USA: ACM Press, 2004.

[5] RONALD W, DERRICK K, SUE-FEN C, 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, USA: ACM Press, 2004: 59-64.

[6] HUANG Qiang, CUKIER J, KOBAYASHI H, et al. Fast authenticated key establishment protocols for self-organizing sensor networks[C]//Proceedings of 2nd ACM Workshop on Wireless Sensor Networks and Applications. New York, USA: ACM Press, 2003: 141-150.

[7] DU Wen-liang, WANG Rong-hua, NING Peng. An efficient scheme for authenticating public keys in sensor networks[C]//MobiHoc'05. Urbana-Champaign, Illinois, USA: ACM Press, 2005: 58-67.

[8] JOHANN G, ALEXANDER S, STEFAN T. The Energy cost of cryptographic key establishment in wireless sensor networks (extended abstract)[C]//ASIACCS'07. Singapore: ACM Press, 2007: 380-382.

[9] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[C]//Proceedings of the 9th ACM Conference on Computer and Communications Security. Washington, USA: ACM Press, 2002: 41-47.

[10] ALAN P, KRISTIE K, SAMIR C. A secure key management scheme for sensor networks[C]//Proceeding of the 10th Americas Conference on Information System. New York, USA:[s.n.], 2004: 1739-1745.

[11] LIU D, NING P. Establishing pairwise keys in distributed sensor networks[C]//Proceedings of the 10th ACM Conference on Computer And Communication Security. New York, USA: ACM Press, 2003: 52-61.

[12] RENE S, GREGG R. Mandatory ECC security algorithm suite[C]//IEEE P802.15 Wireless Personal Area Networks. [S. l.]: [s. n.], 2002.

[13] CANETTI R, KRAWCZYK H. Analysis of key-exchange protocols and their use for building secure channels[C]// Proc of Advances in Cryptology, Eurocrpt'01. Lecture Notes in Computer Science 2045. Berlin: Springer-Verlag, 2001: 453-474.

编　辑　黄　莘