ISSN 1673-9418 CODEN JKYTA8
Journal of Frontiers of Computer Science and Technology
1673-9418/2008/02(02)-0113-10
DOI:10.3778/j.issn.1673-9418.2008.02.001

E-mail:fcst@public2.bta.net.cn
http://www.ceaj.org
Tel:+86-10-51616056

无线传感器网络中的广播认证协议*

赵 鑫+,王晓东,周兴铭
ZHAO Xin+, WANG Xiaodong, ZHOU Xingming

国防科技大学 计算机学院,长沙 410073
College of Computer Science, National University of Defense Technology, Changsha 410073, China
+ Corresponding author: E-mail: xinzhao_remerci@nudt.edu.cn

ZHAO Xin, WANG Xiaodong, ZHOU Xingming. Broadcast authentication protocols in wireless sensor networks. Journal of Frontiers of Computer Science and Technology, 2008,2(2):113-122.

Abstract: With the summary about ideal properties of broadcast authentication protocols, the performance of proposed broadcast authentication protocols based on digital signature and symmetric cryptography is analyzed. It highlights some mechanisms in these protocols when designing broadcast authentication protocols in wireless sensor networks. The notion of integrality problems of broadcast authentication protocols, meaning relative key management problems of these protocols such as distribution of bootstrap parameters and update of keys, is presented. Furthermore, it also concludes the limitation of existing methods. It's considered valuable to support multiple security levels for broadcast authentication protocols in wireless sensor networks. A design of such protocols is also proposed.

Key words: wireless sensor networks; broadcast authentication; hash chain; hash tree; digital signature; one time signature

摘 要:在总结广播认证协议理想属性的基础上,对现有基于数字签名技术和对称加密技术的广播认证协议优缺点进行了分析讨论,并指出其对无线传感器网络广播认证协议设计的借鉴价值。将广播认证协议中的参数初始化和密钥更新等与密钥管理相关的问题归结为认证系统的完备性问题,并指出现有技术方案在解决该问题时存在的缺陷。初步探讨了无线传感器网络广播认证协议分级安全功能支持的意义,并给出了相应的方案设计思路。

关键词:无线传感器网络;广播认证;哈希链;哈希树;数字签名;一次性签名
文献标识码:A **中图分类号:**TP393.08

* the National Grand Fundamental Research 973 Program of China under Grant No.2006CB303000 (国家重点基础研究发展规划(973)).

Received 2007-11, Accepted 2008-03.

1 概述

无线传感器网络(以下简称无线传感网)由一组分布式部署的无线节点构成,可感测周围环境诸如温度、湿度、亮度等参数的变化,并通过多跳传输将数据反馈到数据中心。由于其节点价格低廉、部署灵活,具有一定的容错能力,近年来成为研究热点,提出了大量应用,如智能家居、办公环境监测、病人生理数据监测、精确农耕等。其中一些应用,如战场侦察、森林火险监测,对无线传感器网络的安全性提出了要求。

可认证性是一个实用的安全信息系统所需要的基本安全服务之一,其他的基本安全服务包括信息的私密性、完整性和实体行为的不可否认性。通过认证服务,系统可确认通信实体的身份,进而实现访问控制、授权服务等安全服务。认证服务提供两方面的安全属性,一是系统可确认通信实体的身份(简称实体认证),进而实现访问控制、授权服务等安全服务;二是通信中的接收方可确认所收到消息的发送源(简称消息源认证)。本文主要针对消息源认证进行讨论。

点对点通信的消息源认证可由对称加密技术完美解决:通信双方用共享的密钥对消息认证码加密即可。组播和广播通信的消息源认证若采用同样的机制,则任意接收节点都可用共享的密钥假冒某个发送节点发送报文而其他节点无法区分这两者。一旦某个节点共享的密钥被攻击者获取,所有节点的广播认证机制都不再安全。因此一般认为广播认证需要采用非对称加密的方式来实现,最直观的方法是采用基于公钥机制的数字签名算法。但由于无线传感网节点资源受限(包括计算、存储和能量等方面),普遍使用的公钥签名算法如 RSA[1]计算开销和能耗太大,无法适应无线传感网的要求。因此如何针对无线传感网设计相应的广播认证协议成为近年来的研究热点。

2 无线传感器网络广播认证协议的理想属性

对于一般意义上的广播认证协议,希望其具有以下一些属性:

(1)低计算、存储、通信开销。计算开销来自于产生和验证认证信息的过程,存储开销来自于认证过程中对报文或认证信息的缓存,通信开销来自于通信发送和接收方所需传输的认证信息,理想的广播认证协议希望这些开销在通信的发送方和接收方都尽可能小。

(2)无认证延迟。认证延迟来自于现实协议设计中为一部分协议性能进行权衡后付出的代价。许多低开销的认证协议中,信息发送方在发送经过认证的信息之前或接收方收到认证信息后都需等待一段时间。理想的广播认证协议希望消除这样的等待时间,实现无认证延迟。

(3)可容忍报文的丢失。理想的广播认证协议希望在报文可能丢失的通信信道中能够对丢失报文的后续报文进行认证,这对广播认证协议的健壮性提出了要求。

(4)协议完备性。非对称加密机制一般都需要一个参数初始化的过程,协议在长时间的运行过程中需要及时地更新密钥,理想的广播认证协议应该明确描述这些与密钥管理紧密联系的协议机制,保证协议的完备性。

(5)分级安全功能支持。安全支持是在应用系统正常运行之外附加的,必然带来额外的开销,且提供较强安全服务的协议一般开销也大。另一方面,不同应用对安全服务强度的要求也不同。因此可以认为理想的广播认证协议应该提供不同的分级安全功能,以确保满足应用系统所要求安全条件的同时尽可能降低开销。

然而事实上,目前提出的广播认证协议中还不能完全满足以上所有条件。如 RSA 数字签名算法可容忍报文的丢失、无认证延迟,但开销较大;一次性签名算法计算开销较低,但通信开销较大;基于对称加密技术的认证算法如 μTESLA[2]等开销较低,但引入了认证延迟,同时还存在初始化参数发布效率低下的问题。另外,已知的所有协议都没有提供协议安全级别支持。目前许多实用的广播认证协议大都针对特定网络环境或应用设计,并尽可能满足以上属性。

无线传感网的网络环境也对广播认证协议设计产生了一些硬性限制,包括:

(1)受限的资源:尽管由于硬件技术的发展,无线传感网节点计算能力和存储能力在可预见的未来会有较大的提高,但采用电池供电、能耗有限仍旧是无线传感网的软肋。因此低开销是无线传感网广播认证协议的主要要求。

(2)无线通信的不稳定性:无线传感网采用无线通信方式,报文的丢失率较传统网络高,因此要求广播认证协议能够容忍报文的丢失。

以下几章在对广播认证协议基本技术介绍的基础上,对现有的低开销广播认证协议进行介绍和分析,并指出其在无线传感网应用的可能性,及对无线传感网广播认证协议设计的启发意义,并进一步分析了在认证协议的完备性和分级安全功能支持方面可做的工作,最终得出一些具有指导意义的结论和建议。

3　广播认证协议中的基本技术

本章主要对现有低开销广播认证协议中常用到的基本技术进行介绍和分析,主要包括 hash 链、hash 树和一次性签名。

3.1　Hash 链

哈希链广泛应用在高效的不基于公钥签名机制的认证算法中,通常用于构造更为复杂的认证机制。如图 1 所示对给定信息 M(其长度通常也为哈希值长度)和单向哈希函数 H,由集合$\{H^n(M), n\geq 0\}$依照元素生成关系组成的链称为哈希链。由于哈希函数计算的单向性,当 $n\geq l>m\geq 0$ 时,给定 $H^l(M)$,无法逆推出 $H^m(M)$。而在 $H^l(M)$可信的前提下,可通过验证等式 $H^l(M)=H^{(l-m)}(H^m(M))$是否成立来判断 $H^m(M)$是否可信。

3.2　Hash 树

Hash 树[3]也称为 Merkle 树,由 Merkle 等人于1987年提出,主要用于对一组信息的认证。图 2 给出了可对 8 个信息进行认证的哈希树结构,其中深灰色节点代表需被认证的一组信息,黑色箭头代表对起始节点值进行一次哈希函数计算得到终止节点值。可以看出,哈希树是一个完全二叉树,叶子节点由对一组信息分别进行一次哈希函数计算后得到的值组成。非叶

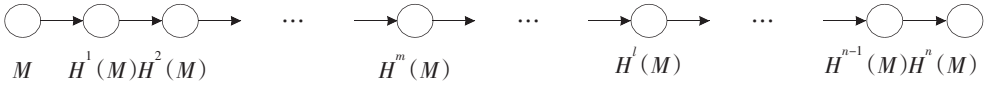


Fig.1　Hash chain

图 1　哈希链

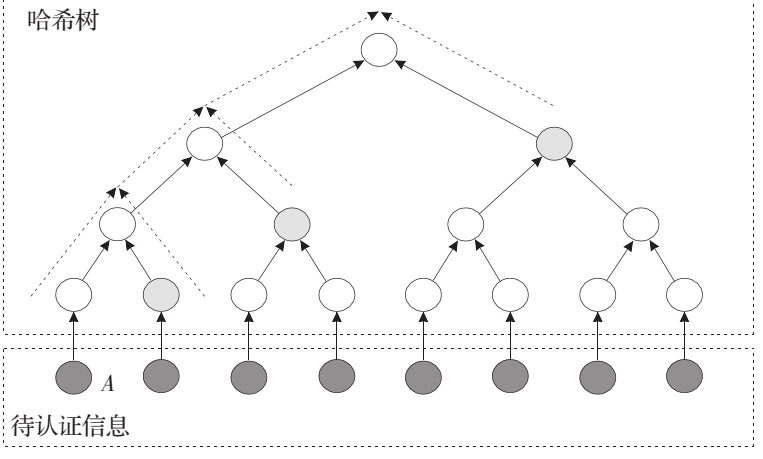


Fig.2　Merkle hash tree

图 2　Merkle 哈希树

子节点的值则由对其孩子节点值的连接进行一次哈希函数计算得到,即 $parent=H(child_{left} \| child_{right})$,其中 H 为单向哈希函数。

通过可信信道获得哈希树根节点的值后,数据的接收方即可对一组信息的任意一个进行认证。但数据发送方为了对该信息认证需要发送额外的认证信息,以确保数据接收方能够根据这些信息重建包括该原始信息的部分哈希树。这些信息就是该原始信息对应的哈希树叶子节点到根节点路径上所有节点的兄弟节点值。如要对图 2 中节点 A 所代表的原始信息认证,信息发送方需要额外发送所有浅灰色节点的值,以构造出浅灰色虚线箭头所示的部分树。接收方利用收到的认证信息通过对该部分树的重新计算并与已存储的根节点值比较即完成了一次认证过程。

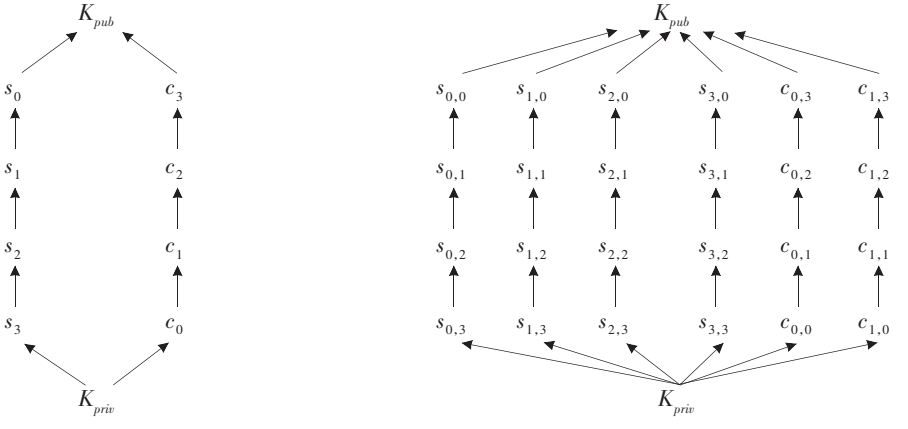
哈希树认证的优点是计算效率高、接收方认证快速、没有延迟,缺点是认证过程需要额外认证信息的支持,当树的规模较大时可能会带来较大的通信开销。另外哈希树需要在一组信息内容已知的情况下建立,树建好后可认证的信息也相应确定,不适合被认证信息动态产生的情况。

3.3 一次性签名

一次性签名最早由 Rabin[4]和 Lamport[5]分别于 1978 和 1979 年提出,而为人所熟知的一次性签名方案则由 Merkle 和 Winternitz[6]于 1987 年提出。一次性签名区别于基于公钥机制陷门单向函数的数字签名方案,它基于单向哈希函数,因此易于实现且计算效率很高。缺陷在于它的"一次性"特征,即一对密钥只能用于对一个报文进行签名和认证。另外一次性签名方案产生的签名很大,会带来较大的通信开销。Perrig 和 Reyzin 等人分别提出了新的一次性签名方案 BiBa[7]和 HORS[8],减小了签名的长度但又增加了公钥的长度。下面对 Merkle-Winternitz 一次性签名方案进行具体的介绍。

Merkle-Winternitz 一次性签名利用基于单向哈希函数构造的有向无环图来进行签名,如图 3 所示。其中每条有向边代表一次单向函数运算,有多条入边的节点值由单向函数作用于其前辈节点值的连接得到。图的起始节点为私钥,终节点为公钥。

图 3(a)所示的有向无环图中,单向哈希函数链的长度为 4,可对 0-3 的 2 位数据进行签名。其中 (s_3,s_2,s_1,s_0)称为签名链,链中的每个值 s_i 代表了被签名的值 i;(c_0,c_1,c_2,c_3)称为校验链,目的是防止签名的伪造。签名者首先随机产生私钥 K_{priv},利用一个伪随机函数(Pseudo-Random Function,PRF)和私钥 K_{priv} 分别产生 s_3 和 c_0,其余的值则由 s_3 和 c_0 通过单向哈希函数依次产生。对需被签名的值 $i(0\leqslant i\leqslant 3)$,用



(a)Directed acyclic graph to sign 2 bits (b)Directed acyclic graph to sign 8 bits

(a)可对 2 位数据签名的有向无环图 (b)可对 8 位数据签名的有向无环图

Fig.3 The illustration of Merkle-Winternitz one time signature

图 3 Merkle-Winternitz 一次性签名方案示例

s_i和c_i作为签名。接收节点通过计算$K_{pub}=F(F^i(s_i)\|F^{3-i}(c_i))$与存储的$K_{pub}$进行比较验证。由于$s_i$和$c_i$两个链的计算方向相反,因此攻击者要伪造一个签名必须能够逆向运算至少一个单向函数,这保证了该签名算法的安全性。

用两个单向哈希函数链构造的签名算法不具有可扩展性,如对32位数据的签名就需要2^{32}长度的单向哈希函数链。为此可用多个签名链来构造有向无环图,如图3(b)所示,用4个长度为4的签名链即可对8位数据产生签名。为进一步减少校验链数量,Merkle等人提出用校验链来代表签名链的和而不是实际数据。图3(b)所示的签名链的和为$4\times(2^4-1)=60$,因此只需要两个校验链。一般而言,对于k个签名链,其中每个签名链可对m位数据签名,所需要校验链的数量为$\lceil \mathrm{lb}\frac{k(2^m-1)}{m}\rceil$。当采用每个签名链可对4位数据进行签名的有向无环图对80位数据进行签名时,假设哈希函数的输出为10字节,通过计算可以得出签名的长度为230字节。

4　无线传感器网络中的广播认证协议

本章对现有的低开销广播认证协议进行综合分析和评价,按采用的主要技术不同分为基于数字签名的广播认证协议和基于对称加密技术的广播认证协议,指出其对无线传感网广播认证协议设计的启发和借鉴意义。总结部分分析了两类协议的优缺点和互补性。

4.1　基于数字签名的广播认证协议

由于基于公钥(或称双钥)机制的数字签名技术具有天然的非对称性,因而成为广播数据源认证的一个很自然的解决方案。除此之外,数字签名技术还能够提供实体行为不可否认性的安全服务。但目前被广泛使用的基于RSA公钥机制的数字签名技术会产生较大的计算开销和通信开销,由于无线传感器节点资源受限,学术界较长时间以来普遍认为基于公钥机制的数字签名技术不适用于无线传感器网络。

解决这一问题的思路有两个,一是设计或采用效率更高的数字签名方案;一是将一次签名产生的计算和通信开销平均到多个数据报文上。对于前者,主要的研究成果集中在对基于椭圆曲线公钥机制数字签名技术的应用和设计高效的一次性签名方案。对于后者,主要的技术手段是将基于公钥机制的数字签名和哈希函数链、哈希树、一次性签名等方案结合起来,目前的研究仍集中于传统网络的流认证(指音频视频流数据)和组播认证,但它们也对无线传感器网络中的广播认证协议设计具有借鉴意义。下面对这些研究中的主要成果简要介绍。

基于椭圆曲线密码(Elliptic Curve Cryptography, ECC)[9]的公钥机制比基于RSA的具有更高的效率,一般认为,160位椭圆曲线密码的安全性等同于1 024位的RSA密码,因此更适合于资源受限的环境。Piotrowski等人在文献[10]中得到的实验结果为:在Crossbow公司的小型传感器MICA2DOT(使用ATMEL公司4 MHz的ATmega128L芯片)上160位密钥长度的椭圆曲线签名的产生和认证分别需时1.65 s和3.26 s,已经接近于实用。事实上,Liu等人已针对MICAz、TelosB、Tmote Sky和Imote2等传感器节点设计实现了经过优化的椭圆曲线加密、认证和密钥交换算法tinyECC[11],Certicom公司也致力于将椭圆曲线加密技术应用于传感器网络[12]。

另一种方案是使用和设计高效的一次性签名算法进行认证,如Perrig等人提出的BiBa[7]和稍后Reyzin等人提出的HORS[8]等。这些一次性签名算法相对于Merkle-Winternitz一次性签名算法,一对密钥可以对有限制的若干个信息进行签名,减少了认证信息即签名的大小,大大加快了签名验证的速度,主要的问题是用于验证签名的公钥太大,如HORS的公钥约为10 KByte,因而难以在无线传感器网络中使用。Luk等人在文献[13]中提出用Merkle-Winternitz一次性签名算法对无线传感器网络中低熵的报文进行签名的思路,但不具有普遍意义。

在传统网络的流认证和组播认证的协议设计中,为了减少公钥签名算法带来的系统开销,研究工作者

提出了许多混合认证方案。如Gennaro 等人在文献[14]提出在流认证中只对第一个报文进行公钥签名,同时每个报文都附加下一个报文(包括附加在其上的哈希值)的哈希值,这一方案的主要问题是无法容忍报文的丢失。为解决这一问题,Wong 等人在文献[15]提出先对一组报文构建哈希树,然后再对哈希树根节点的值进行公钥签名的方案。这一方案仍旧有许多问题,如发送方缓存一组报文带来的延迟,哈希树认证所带来的额外通信开销等。后续又有 Rohatgi、Perrig 等人提出了改进方案[16,17]。图 4 给出了这些方案中的一个例子,图中每个报文附加下两个报文的哈希值,具有一定的抗报文丢失的能力。这些减少公钥签名算法系统开销的方案对于无线传感器网络广播认证协议的设计具有启发意义:将基于椭圆曲线公钥的签名算法和哈希链、哈希树以及一次性签名算法等高效认证方案结合有可能产生高效并且安全的无线传感网广播认证方案。

4.2 基于对称加密技术的广播认证协议

由于数字签名算法的系统开销较高,一些研究工作者开始寻求从高效的对称加密算法构造非对称认证算法的方案。这里主要介绍 Canetti 等人提出的多 MAC 方案[18]和 Perrig 等人提出的 μTESLA 协议[2]。

Canetti 等人在文献[18]中提出的基于多 MAC 的非对称方案中,每个发送方带有 k 个密钥,每个接收方拥有该组密钥的一个子集。发送方对每个报文都用这 k 个密钥计算出 k 个 MAC 值并附加到报文中,接收方可利用自己掌握的密钥对其中的一部分 MAC 进行验证,但无法伪造出 k 个合法的 MAC,从而实现了认证算法的非对称性。事实上,Canetti 指出通过适当的参数调整,可以确保任意 w 个接收方无法串通伪造出 k 个合法的 MAC 值。由于每个报文都要携带 k 个 MAC 值,该方案会带来较大的通信开销,同时只能提供有限的安全性(大于 w 个接收方的串通将攻破该认证系统)。

μTESLA 协议源于 Perrig 等人稍前的工作 TESLA[17],是作者所知最早提出针对无线传感器网络的广播认证协议,也是最为经典的一个。它利用哈希密钥链和延迟发布密钥等技术,在发送节点和接收节点宽松时间同步的条件下,以一定的认证延迟为代价,用对称加密机制实现了广播认证所需的非对称性,具有很高的效率。下面对其机制做较为详细的介绍。

发送节点建立一组长度为 $n+1$ 的单向函数密钥链,这组密钥链的第一个密钥 K_n 随机产生,其后的密钥则由单向函数 H(如单向哈希函数 MD5、SHA1 等)重复作用于上一个密钥产生,即 $K_j=H(K_{j+1})$。发送节点将时间划分成等长的时间片(设时间片长度为 D),每个时间片按序分配一个密钥,但分配密钥的顺序与密钥链产生的顺序正好相反,如图 5 所示。在时间片

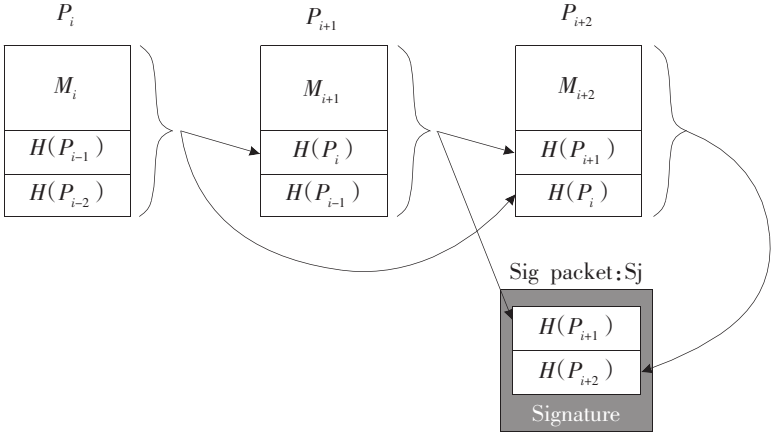


Fig.4 An example of amortizing signature overhead in stream authentication

图 4 流认证中签名开销分摊实例

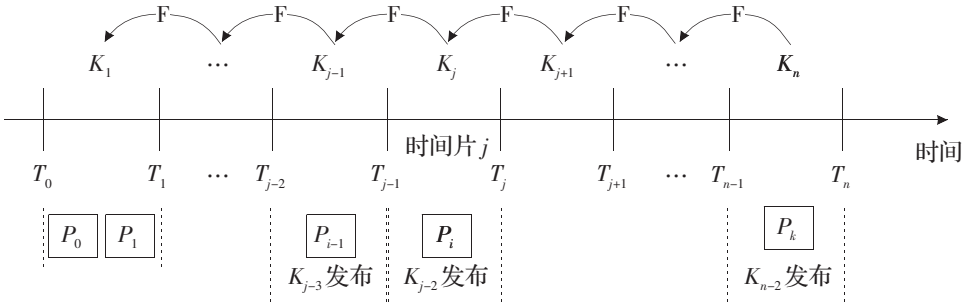


Fig.5　The basic mechanism of μTESLA protocol

图 5　μTESLA 协议的基本机制

j 内发送的任何报文 P_i 用密钥 K_j 计算报文的消息认证码($MAC_{K_j}(P_i)$)。发送节点以时间片长度为单位确定密钥发布延迟时间 δ,当前时间片 j 使用的密钥 K_j 将在 δ 后发布出去,如图 5 中 δ 为 2。为避免额外的通信开销,μTESLA 协议规定发布的密钥附在数据报文中发送，如果某时间片没有广播数据报文发送,则该时间片应发布的密钥也不发送,接收节点可由后续发布的密钥通过单向函数计算出该密钥。发送节点在发送广播认证报文之前需要将 K_0、δ、D 及开始时间 T_0 等参数发送给接收节点。

在宽松时间同步的条件下,接收节点收到广播认证报文后可利用存储的参数计算出该报文中使用的密钥是否已发布。如果已经发布,则任何收到该密钥的节点都可伪造或篡改该报文,因此该报文被视为不安全的,被丢弃;如果密钥还未发布,则该报文被缓存起来,直到该密钥发布,这一步称为报文的安全条件检查。收到发布的密钥 K_j 后,首先通过 K_0 或上一个已经被认证的密钥 K_i 验证该密钥的正确性，即检查 $K_i=H^{(j-i)}(K_j)$ 是否成立,从而完成源节点认证;然后再验证消息认证码的正确性,从而完成报文认证。如果两个认证都通过,则该广播报文正确接收。

μTESLA 协议不仅在计算和通信上的开销小,且能够容忍报文的丢失，如附带密钥 K_i 的某个数据报文在传输过程中丢失,接收节点可通过后续收到的密钥 K_j 通过公式 $K_i=H^{(j-i)}(K_j)$ 计算出 K_i,并继续进行报文的认证过程。

4.3　小结

基于对称加密技术的广播认证方案虽然效率较高,但这是在一定代价基础上的,如 μTESLA 协议需要节点间的宽松时间同步,接收节点需要缓存数据报文,从而带来认证延迟,且可能受到 DoS 攻击。数字签名算法开销较大，但提供了不可否认性的安全服务，并可通过多个广播报文分担一次签名的开销,或设计高效的可用于无线传感网的一次性签名算法来降低开销。随着硬件技术的提高,数字签名技术应用在无线传感网的可能性也越来越强。但硬件能力的提高主要在计算和存储方面,有限的能源供应始终是限制高能耗的数字签名技术应用的关键。因此这两种方案无法完全取代对方,具有一定的互补性。

5　无线传感网广播认证协议的完备性和分级安全功能支持

由于无线传感网分布式计算的特性,广播认证协议的初始化参数发布和密钥更新难以采用传统的证书中心完成,而必须另外设计方案。本文将这些与无线传感网广播认证协议相关的密钥管理问题归结为认证系统的完备性问题。通过对现有技术方案的分析,指出其在解决完备性问题时存在的缺陷。针对能源受限的无线传感网，提供分级的安全功能支持,有助于在确保系统安全的同时最大限度降低能耗,延长整个系统的生命周期。在这些分析研究的基础上,本

章给出了一些广播认证协议设计的原则和建议。

5.1 完备性问题

通过对以上各个协议的分析可知,非对称的认证方案都需要提供参数初始化的方案,如基于数字签名的认证方案需要将发送方的公钥预先发布到所有可能的接收方,基于多消息认证码的方案中需要将发送方产生的 k 个密钥中的部分子集发送到接收方,μTESLA 协议则需将 K_0、δ、D、T_0 等初始化参数发布到所有可能的接收方。

传统的公钥密码体系里主要使用额外的证书签署中心(Certification Authority,CA)完成公钥的管理和发布,无线传感网由于能耗和网络体系结构等原因不适合采用这种方式。另一个比较直观的方案是预置这些初始化参数,这一方案实现简单,不带来额外通信开销,但不具有可扩展性,当潜在的发送方很多时,需要预置的信息量可能超出了无线传感网节点的存储能力;另外预置参数也无法解决参数更新的问题。更为有效的、也是大多数认证协议中使用的方案是结合使用预置参数和哈希链、哈希树技术。

文献[19]和[20]分别利用哈希树来解决数字签名公钥和 μTESLA 协议初始化参数的发布问题,同时将哈希树根节点值预置到所有节点中。在文献[19]中,Du 等人进一步利用地理位置信息将位置相邻的节点初始化参数放在哈希树的同一个子分支中,并将子分支的根节点值也预置到这些节点中,从而将哈希树分解为哈希森林。这样相邻节点互相验证公钥时,发送节点只需附带少量的认证信息,而接收节点也只需进行较少的哈希函数计算。这一方案利用地理信息,以适度的存储空间为代价,减少了公钥验证时的计算和通信开销,当网络规模较大,即相应的哈希树高度较大时,具有一定的意义。

μTESLA 协议中,密钥链的生命周期(用于认证的时间)取决于其长度,一般来说它相对于无线传感网的生命周期较小,因此每个发送节点都需要多个密钥链进行广播认证,因而需要发布多个密钥链的初始化参数。在文献[20]中,Liu 等人进一步利用 2 个层次的哈希树来发布这些初始化参数:对于每个发送节点的多个 μTESLA 初始化参数构造一个下层的哈希树,再以这些树的根节点值作为叶子节点构造上层的哈希树。另外,Liu 等还用哈希树构造了回收树以收回被捕获节点的广播权限。

哈希树配合预置参数的方案是一种静态的初始化方案,对于需要认证的信息数量不确定或有动态变化的情况难以适应,并且额外的认证信息也带来了不可忽视的通信开销。Luk 等人在文献[13]中基于 μTESLA 协议提出了一个小巧的初始化信息发布方案 RPT(Regular-Predictable TESLA)。其主要思路是在初始化信息可以预知的前提下,先生成广播信息的消息认证码并广播出去,经过 δ 时间后再将广播信息和密钥同时发布。由于密钥在消息认证码被接收后才发布,因此攻击者无法对消息认证码进行篡改。这一方案的主要问题是被认证信息的内容必须预先明确,如对于一次性签名方案,需要动态发送公钥信息,RPT 方案难以适应这一需求。

无线传感网节点部署后初始网络的建立过程是系统安全的薄弱环节,设计恰当的参数初始化方案以提供足够的安全支持并避免过大的开销仍旧是一个开放性的问题。在传感器整个网络生命周期里广播认证协议所需的密钥更新和回收机制也是一个完备的广播认证方案所需包含的协议组成部分,与之紧密相关的密钥管理问题应在广播认证协议中加以明确。

5.2 分级安全功能支持

安全协议是应用系统正常运行之外的附加程序,因而在保证系统安全运行的同时也带来了额外的开销。一般而言,安全功能越强,对应的协议开销也越大。另一方面,对于大多数应用,不同的报文类型对于安全的需求往往不同。如不断记录和发送的环境数据相对于报警信息而言,对于安全的要求相对较弱。因此理想的安全协议应具有分级的安全功能支持,对于不同的应用和报文采用能保证安全需求且开销最小

的安全方案,以最大限度减小协议的开销。同一个协议提供不同的安全级别支持是较难的,折中的方案是采用混合策略。

无线传感网中基于数字签名的广播认证方案和基于对称加密技术的广播认证方案在安全和能耗两方面恰好形成了互补。对于一些应用或关键报文,如火灾报警信息,数字签名技术不可否认性的支持增强了网络的安全性,利于对恶意节点的检测。这种互补特性启示作者在广播认证协议设计时采用混合式的认证方案,即对于安全级别要求高的数据报文采用数字签名算法认证,其他报文则采用基于对称加密技术的认证方案。这种混合式策略可能带来较大的存储开销,需要谨慎的设计方案达到较好的权衡效果。

6　结束语

目前无线传感网中广播认证协议的研究工作以μTESLA 协议和对其的改进加强为主流,一部分工作集中于基于椭圆曲线数字签名算法在无线传感网中的实用。通过本文的分析和讨论,可以发现轻量级的一次性签名算法和将公钥签名开销分担到多个报文的认证方案也在无线传感网中有一定的应用价值。考虑到广播认证协议对于应用系统不同安全级别需求的适应性、安全协议初始化和密钥管理等方面的问题,无线传感网中的广播认证协议还有许多可研究的内容。

References:

[1] Rivest R L, Shamir A, Adleman L M. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978,21:120-126.

[2] Perrig A, Szewczyk R, Wen V, et al. SPINS: security protocols for sensor networks[J]. Wireless Networks, 2002, 8:521-534.

[3] Merkle R. Protocols for public key cryptosystems[C]//Proceedings of the IEEE Symposium on Research in Security and Privacy, 1980.

[4] Rabin M O. Digitalized signatures[J]. Foundations of Secure Computation, 1978:155-168.

[5] Lamport L. Constructing digital signatures from a one-way function, Technical Report SRI-CSL-98[R]. SRI International Computer Science Laboratory, October 1979.

[6] Merkle. A digital signature based on a conventional encryption function[C]//CRYPTO: Proceedings of Crypto, 1987.

[7] Perrig A. The BiBa one-time signature and broadcast authentication protocol[C]//ACM Conference on Computer and Communications Security, 2001:28-37.

[8] Reyzin. Better than BiBa: short one-time signatures with fast signing and verifying[C]//ACISP: Australasian Conference on Information Security and Privacy, 2002.

[9] Miller V S. Uses of elliptic curves in cryptography[C]// LNCS: Advances in Cryptology CRYPTO'85. [S.l.]: Springer-Verlag, 1986,218:417-426.

[10] Piotrowski K, Langendörfer P, Peter S. How public key cryptography influences wireless sensor node lifetime[C]// SASN, ACM, 2006:169-176.

[11] Liu An, Ning Peng. TinyECC: a configurable library for elliptic curve cryptography in wireless sensor networks, Technical Report TR-2007-36[R]. North Carolina State University, Department of Computer Science, November 2007.

[12] http://www.certicom.com.

[13] Luk M, Perrig A, Whillock B. Seven cardinal properties of sensor network broadcast authentication[C]//the Fourth ACM Workshop on Security of Ad Hoc and Sensor Networks, 2006:147-156.

[14] Gennaro R, Rohatgi P. How to sign digital streams[C]// CRYPTO. [S.l.]: Springer, 1997,1294:180-190.

[15] Wong C, Lam S. Digital signatures for flows and multicasts[C]//IEEE ICNP'98, Austin, TX, 1998.

[16] Rohatgi P. A compact and fast hybrid signature scheme for multicast packet[C]//Proceedings of the 6th ACM Conference on Computer and Communications Security, November 1999, 1999:93-100.

[17] Perrig A, Canetti R, Tygar J D, et al. Efficient au-

thentication and signature of multicast streams over lossy channels[C]//Proceedings of the IEEE Symposium on Research in Security and Privacy, May 2000, 2000:56-73.

[18] Canetti R, Garay J, Itkis G, et al. Multicast security: a taxonomy and some efficient constructions[C]//INFOCOMM'99, March 1999, 1999:708-716.

[19] Du W, Wang R. An efficient scheme for authenticating public keys in sensor networks[C]//MobiHoc. Illinois, USA: Urbana-Champaign, 2005.

[20] Liu D, Ning P, Zhu S, et al. Practical broadcast authentication in sensor networks[C]//MobiQuitous. [S.l.]: IEEE Computer Society, 2005:118-132.

ZHAO Xin was born in 1979. He received the M.S. degree in Computer Science from National University of Defense Technology, and now is a Ph.D. candidate at the university. His research interests include the security of mobile ad hoc networks and wireless sensor networks.

赵鑫(1979-),男,山西长治人,国防科技大学计算机学院博士研究生,2005 年于国防科技大学获计算机科学专业工学硕士学位,主要研究领域为移动自组网及无线传感器网络中的安全问题。

WANG Xiaodong was born in 1973. He received the Ph.D. degree in computer from National University of Defense Technology in 2001. He is an associate professor and master's supervisor at National University of Defense Technology. His research interest includes mobile computing technology.

王晓东(1973-),男,山东巨野人,2001 年于国防科技大学计算机学院获博士学位,国防科技大学计算机学院副研究员,硕士生导师,主要研究领域为移动计算技术。

ZHOU Xingming was born in 1938. He is a professor and doctoral supervisor at National University of Defense Technology, and an academician of Chinese Academy of Sciences. His research interests include high performance computing technology, network and distributed computing technology.

周兴铭(1938-),男,上海人,国防科技大学计算机学院教授,博士生导师,中科院院士,主要研究领域为高性能计算技术、网络与分布式计算技术。