文章编号:1001 - 893X(2010)10 - 0118 - 06

无线传感器网络密钥管理研究进展*

米 波[1],段书凯[2],宋 军[1],王 勇[1]

(1.重庆交通大学 信息科学与工程学院,重庆 400074;2.西南大学 电子信息工程学院,重庆 400715)

摘 要:分析了当前无线传感器网络密钥管理协议设计中所存在的主要问题,在对具有代表性的最新研究成果进行系统论述的基础上,全面分析了其利弊以及适应性问题。考虑到传感器网络应用背景的细化和结构、功能的多元化,提出了今后的研究方向。

关键词:无线传感器网络;密钥管理;预分配;公钥

中图分类号:TP393.08 **文献标识码:**A doi:10.3969/j.issn.1001 - 893x.2010.10.023

Advances on Key Management of Wireless Sensor Networks

MI Bo[1], *DUAN Shu-kai*[2], *SONG Jun*[1], *WANG Yong*[1]

(1.School of Information Science and Technology, Chongqing Jiaotong University, Chongqing 400074, China;
2.School of Electronic Information Engineering, Southwest University, Chongqing 400715, China)

Abstract: The critical problem of key distribution in wireless sensor networks(WSN) is analysed. Based on systematic characterization of up-to-date typical key management schemes, their advantages and disadvantages are described as well as their applicability. Through considering the application background and the diversification of architectures and functions of WSN, some promising research orientations are presented.

Key words: wireless sensor network(WSN); key management; pre - distribution; symmetric key

1 引 言

集电子信息技术、嵌入式计算技术、无线通信技术及分布式信息处理技术于一身的无线传感器网络(Wireless Sensor Network, WSN)因其成本低廉、自组织等特点,受到军事、国防、工农业、城市管理、生物医疗、环境监测、抢险救灾、反恐、危险区域远程控制等诸多领域的广泛关注。美国《商业周刊》将其列入未来四大新兴技术之中,足见其巨大的科研价值和广阔的应用前景。

作为传感器网络的主要组成部分,传感器节点通常集成了一个感知器(sensor)、一个数据处理单元、一个小容量的内存、一个短程无线通信设备以及电池电源。散布在目标区域的传感器节点利用感知器协作地监测、感知和采集各种环境或监测对象的信息,并通过自组织无线通信网络以多跳中继方式通信,而数据处理单元则对传送中的数据实时地进行处理融合以达到减少通信负荷等目的。通信的数据最终会到达基站或一系列的接收器(sink),并作为网关与外网连接。

* **收稿日期:**2010 - 05 - 21;**修回日期:**2010 - 07 - 22

基金项目:国家自然科学基金资助项目(60972155);中国博士后科学基金资助项目(CPSF20080430741);重庆市科委自然科学基金资助项目(CSTC2009BB2305,2007BB2331);重庆市高等教育教学改革研究重点项目(09 - 2 - 011);西南大学教学改革重点项目(2008JY029);西南大学博士科研资助项目(SWUB2007008,20710906)

Foundation Item: The National Natural Science Foundation of China(No. 60972155); China Postdoctoral Science Foundation(No. CPSF20080430741); National Natural Science Foundation of Chongqing(No. CSTC2009BB2305, 2007BB2331); Key Projects of Chongqing High Educatioanl Reform(No.09 - 2 - 011); Key Projects of High Educatioanl Reform in Southwest University(No.2008JY029) and Ph.D. Research Fund of Southwest University(No.SWUB2007008, 20710906)

近年来,随着传感器节点成本的下降、路由技术的成熟、隐蔽性的增加以及稳定性的提高,无线传感器网络已逐步投入军事、医疗、教育甚至是商业应用。然而,由于其巨大的应用规模,全向射频通信方式和特殊的分布环境,网络极易遭受窃听、篡改、重放以及物理俘获等各种形式的攻击,从而为敏感数据的传输和处理带来安全方面的隐患。为打破这方面的使用瓶颈,国内外对无线传感器网络的认证、加密、入侵检测以及访问控制等安全机制进行了全面而深入的研究。

为提供无线传感器网络中机密性、完整性、鉴别等安全特性,实现一个安全的密钥管理协议是前提条件,也是传感器网络安全研究的主要问题。尽管密钥管理协议在传统网络中已经有了非常成熟的应用,但无线传感器网络有限的电源、有限的计算能力和存储容量、有限的通信能力、自组织的分布特性以及拓扑结构的动态变化等诸多限制,使得其密钥管理面临着一系列新的挑战。尽管当前大规模集成电路技术发展迅猛,但我们认为这些技术的发展不会使传感器网络的诸多限制有所缓解。与摩尔定理不同,我们认为技术的发展将推动传感器节点成本的迅速降低,而不是资源和能力的提高,这是由传感器网络巨大的应用规模所决定的。在传统方案中,一个密钥管理协议的优劣往往取决于其安全程度的高低。然而,综合考虑无线传感器网络中严格的资源限制及其自组织特点,我们认为一个好的密钥管理协议除了安全性方面的考虑外还应该满足协议的轻型化、节点捕获的可承受力(Resilience)、网络的连通性、可扩展性以及支持网络动态变化等其它要求。

尽管基于无线传感器网络的密钥管理方法在近十年来被大量提出,但它们都具有各自的局限性和相应的优缺点。另一方面,随着技术的发展,传感器网络应用背景的细化也为密钥管理方案的设计提出了更为具体的要求和更加广阔的空间。因此,对无线传感器网络密钥管理问题的最新代表性成果进行系统、深入的分析具有重要的现实意义。

2　无线传感器网络密钥管理方案

密钥管理是信息安全技术中的重要一环,其目的在于确保密钥的真实性和有效性,贯穿着密钥产生、存储、分配、使用、废除、归档、销毁的整个过程。考虑到无线传感器网络的成本、通信方式、组织结构以及分布环境等特定因素,密钥分配无疑成为密钥管理中的核心问题。

典型的密钥管理协议主要有基于信任服务器的密钥管理方案、基于公钥的密钥管理方案、基于初始信任的密钥管理方案、密钥预分配方案以及基于逻辑密钥树的密钥管理方案等。信任服务器模型的安全性取决于基站运行的鲁棒性[1,2];基于公钥的密钥管理模型需要非对称密码学的支撑,但却存在效能方面的缺陷;基于初始信任的密钥管理模型往往难以平衡初始信任时间 $T_{\min}$与建立密钥所需时间 T_{est}之间的矛盾[3];密钥预分配模型是目前认为最适合无线传感器网络的密钥分配方法,但以往的算法通常不支持节点的身份认证,难以确定密钥池与密钥环之间的大小关系[4-8];而基于逻辑密钥树的密钥管理模型尽管很好地保证了组、簇密钥的前向安全性和后向安全性,但位于不同分枝的节点间无法建立起独享的通信密钥且存在与信任服务器模型相同的安全瓶颈问题[9]。由此可见,早期的方法往往试图建立一套普遍适用的密钥管理体系而忽略了不同种类传感器网络自身的特点。这种自上而下的设计方法不仅造成实际应用的困难,更使得传感器网络自身的优势难以得到充分利用,限制了密钥管理协议的优化空间。幸运的是,目前一些最新的研究成果表明,人们已经逐渐意识到传感器网络多元化趋势为密钥管理方案的设计所带来的机遇和挑战。下面就一些具有代表性的研究进展进行简要介绍和分析。

2.1　基于明文交换的密钥管理协议

Anderson 等人认为由于传感器节点布置的随机性,在最初的一定时间内,敌人只能监控很小一部分区域的无线通信,根据这种信任关系我们完全可以用明文交换来快速建立对偶密钥。事实上,这种假设可以看作是基于初始信任的密钥管理方案的一种推广。

利用无线信道和节点位置的差异性(diversity),Miller 对 Anderson 的方法进行了改进[10],使密钥分配更加安全。网络部署前,服务器首先为每个节点分配 α 个唯一的密钥,并计算相应的 Bloom filter 和 Merkle tree[11-12]。节点部署后,每个传感器节点使用一个相同的信道广播其 Bloom filter 和相应的 Merkle 值以便在将来对其所拥有密钥的合法性进行验证。在初始化阶段,每一个节点随机选择一个信道(channel)并在切换到另一个信道之前广播其拥有的密钥且同时进行侦听(listen),而停留在每个信道的时间也是随意的。密钥交换结束后,传感器节点利用所有已知的密钥计算并广播一个 Bloom filter,而通过收到的 Bloom filter,节点就可以判断它与其它节点共享哪些密钥,从而建立起安全通信。实验

结果表明,在不使用多路径密钥增强的情况下,网络的连通性几乎达到了 100%。另外,该方法将节点捕获的威胁限制在了一个局部的范围内,并实现了链路的认证。然而,攻击者有可能对收到的消息进行重放而不被发现,他们也可以使用多频设备(Multiple Radio Device)或多个工作于不同频率的节点来窃取有用的密钥信息,因此该方案的安全性问题还有待进一步研究。

2.2 利用网络不对称结构的密钥管理协议

密钥预分配方案由于不知道节点的准确位置,导致大量的冗余信息存储在传感器节点中,而无线通信的范围有限,这些信息中的大部分可能永远都用不上,从而造成了资源的极大浪费。为解决这个问题,一个直观的方法就是在节点部署后使用公钥为它们按需建立密钥。

然而,公钥机制的使用需要消耗大量资源,致使传感器节点迅速失效,很难直接用于密钥协商。为此,研究者建议利用一些公钥算法加解密的不对称性,将计算负担分配给那些具有更多资源或特殊的节点,从而延长工作节点的使用寿命。

Liu 等人提出的方法使用一种称为 Rabin′s cryptosystem 的公钥体制,其加密过程的复杂度明显小于解密[13]。节点部署后,它首先按照一定的规则决定成为服务节点还是工作节点,服务节点在完成密钥分配任务后将被废弃,因此可以用于大量的公钥计算。使用 Rabin′s cryptosystem,服务节点产生一对密钥并将其公钥发送给一定范围内的工作节点。使用这个公钥,工作节点加密一个随机数返还给服务节点,从而建立起一条安全信道。利用这条安全信道,服务节点就可以将密钥信息(如基于多项式或矩阵的密钥空间[6,7,14-17])秘密发送给工作节点。该方法具有很好的可扩展性和很高的可连通度,节点捕获的可承受能力强,且存储需求低。然而,该方案需要一个初始信任时间,在这段时间内,一旦有节点被捕获,它就可以成为服务节点分配密钥,危害网络的安全性。

基于同样的思想,Huang 等人使用椭圆曲线密码体制(ECC)建立安全服务器(Security Manager)与传感器节点之间的密钥,并将计算负载置于拥有更多资源的安全服务器之上[18]。

2.3 密钥预分配方案研究进展

2.3.1 超立方体多变元密钥预分配方案

Delgosha 与 Fekri 在文献[15,19]中提出一种基于多变元对称多项式的密钥预分配方案,这里对称是指对于变量 $x_1,x_2,\cdots,x_n$ 的任意置换(permutation)$x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)}$,我们有 $f(x_{\sigma(1)},x_{\sigma(2)},\cdots,x_{\sigma(n)})=f(x_1,x_2,\cdots x_n)$。该方案首先创建一个 n 维的超立方体,并为立方体的每一个面分配一个 n 元多项式。同时,我们将超立方体的顶点与每一个传感器节点相对应,用顶点的位置信息作为节点的 ID,且利用节点 ID 和节点所在面的多项式计算出 n 个单变量多项式存储在传感器节点中。这样,汉明距离(Hamming distance)为 1 的节点间就可以使用共享的 $n-1$ 个多项式建立起会话密钥。具体来说,对于一个节点个数为 N 的传感器网络,服务器首先计算 $m=\lceil m'\rceil$,其中 $m'=\sqrt[n]{N}$,随机产生 nm 个对称 n元多项式$f_l^j(x_1,x_2,\cdots,x_n)(i=1,2,\cdots,m;j=1,2,3,\cdots,n)$,并将 n 个单变元多项式 $f_{i_j}^j(I(j),x_n)(j=1,2,\cdots,n)$分配给标识符为 I 的节点,这里 $I(j)$表示在节点的标识符 $I=(i_1,i_2,\cdots i_n)$中去掉元素 i_j。最后,标识符中只有一个元素不同的节点间就可以计算出 $n-1$ 个共享密钥 $k_{I,I',l}=f_{i_l}^l(I(j,l),i_j,i'_j)=f_{i_l}^l(I(j,l),i'_j,i_j)$($l$ 为 $1,2,\cdots,n$ 中除 j 以外的任意一个元素,而 $I(j,l)$表示在节点的标识符中除去元素 i_j 和 i_l),建立起安全链接。显然,由于超立方体是连通的,任意两个汉明距离大于 1 的节点间也一定能够找到一条安全路径建立起会话密钥。与以往的密钥预分配协议相比,该方案具有更高的安全性,但是,多项式的使用增加了系统额外的计算负担,而网络的规模也必须事先决定,这不利于新节点的加入。

2.3.2 基于概率密度函数的节点预分配方案

无线传感器网络中,节点的部署过程虽然是随机的,但根据部署的方式,节点之间成为邻居还是呈现出一定的概率分布,而且,这种概率分布在一定程度上可以提前预知。利用这些信息,我们可以在保持较高连通性的条件下,大幅降低传感器节点的存储需求,这就激发起诸多基于配置知识的密钥预分配方案的研究。

在 Liu、Huang 等人提出的方法中[8,20],传感器节点必须以一定的方式分组进行部署(如水平单元格[8]),这在很大程度上限制了其使用范围。然而,不管采用哪种部署方式,节点之间成为邻居还是呈现一定概率分布的,我们可以根据这些概率密度函数来决定预先存储于节点上的密钥,以避免不必要的密钥预存储。基于这样的思想,Ito 等人直接使用概率密度函数来指导密钥的预分配[21]。首先,我们将全部 n 个密钥分配给分成 n 份的待部署区域,创

造一个密钥 - 位置图(key-position map)。然后根据节点分布的概率密度函数,我们选择一个期望的配置点(expect resident point) P,并以 P 为中心在节点的通信范围内随机选择一点 Q,将位置 Q 所对应的密钥存储在该节点上。反复使用这样的方法,我们就可以为每个节点分配 m 个密钥并利用它们建立相邻节点间的安全通信。该方案具有连通性好、存储空间小、使用灵活等优点。但是,取得正确的概率密度函数是一件非常困难的事情,所以该问题还需要更进一步的研究。

2.4　面向节能的密钥管理协议

传感器网络通常采用电池供电,而且由于规模巨大,又常常分布在无法驾驭的环境,一旦电源耗尽就很难再补充。因此,密钥管理不能消耗太多的能源,这就需要对协议进行必要的优化。例如, 传感器传输信息要比执行计算更消耗电能,传感器传输 1 位信息所需要的电源足以执行 3 000 条计算指令[22],因此,我们就需要尽可能地减少消息的传输。

为此,Jolly 等人设计了一个面向节能的密钥管理协议[23],包括密钥的分配、增加、撤消以及更新。他们使用一个由控制中心、多个网关以及节点所组成三级网络结构,尽可能地避免了节点之间的通信以节约内存空间和能量消耗。

(1)密钥的分配

每个节点预置两个密钥,一个与网关通信,另一个与控制节点(command node)通信。每个网关也拥有与其它网关和控制节点通信的密钥,以及一个组密钥。首先,我们为每个网关分配 $|S|/|G|$ 个与节点通信的密钥,其中 $|G|$ 是网关的数目, $|S|$ 是传感器的数目。每个网关用簇信息算法建立起簇,并从其它网关获得该簇内节点与网关通信的密钥,在网关层的密钥交换完成后,每个网关保存簇内传感器的密钥,并将其它的密钥清除掉。

(2)节点的增加

新节点像其它节点一样被预置两个密钥,同时控制中心发送新节点的 ID 及其与网关通信的密钥(预置信息)给随机选择的一个网关 i。然后,新节点广播一个 HELLO 信息以加入到某个簇中,簇头网关广播节点的 ID 给被选择的网关 i。最后,被选择的网关 i 发送密钥到节点簇的网关。

(3)节点或网关的撤消

如果一个节点或者一组节点被攻破,就将被网关或者控制中心驱逐出网络,并从列表上删除。而如果一个网关被攻破,则控制中心首先将该网关 i 驱逐出去,然后选择一个未被攻破的网关 h,向其发送被撤销的网关所对应簇中节点的 ID、新网关的标识符 j 以及新的通信密钥。在控制中心将新密钥分别发送给每个节点之后,网关 h 也需将这些新密钥秘密发送给它们所对应的新网关 j。

(4)密钥更新

控制中心产生新的密钥,并使用与撤销网关相同的方法把密钥发送给网关和节点。

该方案实现了密钥分配、增加、撤消和更新的功能,节点不需要存储大量的信息,在保持多跳路由功能的同时,排除了直接端到端(end-to-end)的通信,减少了节点的能量消耗。此外,该模型通过保持静态节点处于休眠模式,进一步延长了网络的使用寿命。这是利用基于 MAC 的时分多路接入(TDMA)技术来实现的,由网关分配给节点不同的活动时间段。然而,由于该网络具有特殊的分级结构且网关和控制点需要存储大量的密钥,因而变得非常复杂。同时,该方案的形式分析和安全强度仍然有待研究,网络启动阶段仍然需要一些其它的协议来支撑,网络中如何引入一个轻便有效的入侵检测机制来寻找被攻破节点也仍旧是一个难题。

3　发展趋势

上面的研究结果表明,针对不同的网络环境和资源配置,不同的密钥管理方案都表现出各自的优缺点和相应的适用性。传感器网络应用背景的细化和功能、结构的多元化,在为密钥管理协议的设计提出更加具体甚至是苛刻要求的同时,也为协议的拓展和优化带来更多的思考空间。尽管目前涌现出大量基于无线传感器网络的密钥管理方案,但这方面的研究还远远落后于其自身的发展,因此,我们认为将来的工作还需从以下几个方面着手:

(1)根据以往的开发经验,不少研究者指出,一个好的协议应该在设计之初就考虑其安全性问题,而不是在系统完成后才为其打上安全补丁。然而,目前设计的密钥管理方法却很少考虑对其它协议或应用的支持。为此,面向路由转发等底层协议和内网处理(in-network processing)等具体应用,我们有必要对密钥管理的结构、方法等加以额外的考虑,并为这些协议或应用的开发者提供有价值的建议;

(2)安全性问题是传统网络中一个重要的,往往也是唯一的评估指标。介于传感器网络的独特性,仅考虑其密钥管理方案是否安全是远远不够的。尽管许多文章都或多或少地提到了一些评价协议好坏

的标准,但都不够全面,还有很多方面都缺乏考量。而采用一些系统的方法,如在评估的过程中采用分类的思想并尽可能地将主观因素限制在很小的范围内,可以明显提高评估方案的准确度、可信度和完整性。显然,一个好的评估指标能够很好地指导协议的应用和开发,这就需要我们更加仔细深入地对密钥管理方案的性能评估加以研究;

(3)尽管目前有众多的密钥管理方法被提出,但它们都有各自的侧重点,适用于不同的需求。另一方面,随着技术的发展,基于各种应用的传感器网络也各不相同。因此,根据实际需要选取和修改现有的密钥管理方案是一个重要的研究方向;

(4)由于传感器网络安全性方面的研究才刚刚开始,设计一个健壮、适用的密钥管理方案仍是当前有待解决的一个重要问题。面向传感器网络能源、通信、拓扑等各方面的特点,我们有必要加强密钥分配、密钥更新机制的研究,以一个好的评价体系为目标,增强协议的安全性、可扩展性和自适应性等;

(5)混沌系统具有良好的伪随机特性、轨道的不可预测性、对初始状态及控制参数的敏感性等一系列特性,这些特性与密码学的很多要求是吻合的。近年来,将混沌理论应用到信息安全已成为研究的一个热点,出现了一大批有价值的研究成果。然而,目前我们还没有看到利用混沌密码学进行传感器网络密钥管理的文章,因此,这将是一个全新的研究方向;

(6)目前,传感器网络中关于公开密码密钥体制的研究还很少,公钥体制不适用于无线传感器网络密钥管理的结论还有待商榷。虽然对称密钥体制具有速度快、计算负荷小等特点,但它的使用远不如公钥方法灵活和安全。已有研究表明,经过优化的公钥密码算法在无线传感器网络中仍具有很高的实用价值。与 RSA 相比,椭圆曲线加密具有更高的计算速度,更短的密钥且使用更小的内存和更低的带宽。而利用中国剩余定理(Chinese Remainder Theorem)则可以加快 RSA 的运行速度。另外,使用 Montgomery multiplication 和优化的 squaring 方法也可以让 RSA 的复杂度降低 25%。基于类似的思想,我们有可能设计出适用于无线传感器网络的公钥体制,并通过实验证明其可行性;

(7)在传感器网络中,由于节点易被捕获,攻击者很容易利用获得的密钥信息,部署众多的恶意节点,截取、伪造和篡改传输中的数据,从而危害系统的安全性。传统网络通常使用基于公私钥的认证和签名体系来确保节点的合法身份,但这无法直接应用于传感器网络。因此,设计一个适合于传感器网络的密钥管理认证体系是 WSN 密钥管理亟待解决的问题。值得一提的是,基于无线网络的通信特征,我们应该着重加强组播、广播认证机制的研究,有效地减少网络流量,延长其生命期;

(8)无线传感器网络自身的特点和严格的资源限制使其比传统的网络更难抵抗各种攻击。我们应当从密钥管理的角度出发,详细审查其可能面临的攻击,并提出相应的对策;

(9)尽管一些基于配置知识的密钥管理方案被不断提出,但它们通常都假设传感器节点分组进行部署。而实际上,节点部署的方式往往更加复杂。即使直接使用单个节点的分布信息,要想取得正确的概率密度函数也是一件非常困难的事情。这就需要我们对基于配置知识的密钥分配模型作进一步的研究。

随着时间的推移,传感器网络可用的资源可能会逐步减少。为适应这种变化,我们可能需要不断降低安全服务等级来满足资源限制。为此,设计一种能够不断变换安全等级的密钥管理体制是有价值的。

4 结 论

无线传感器网络部署区域的开放性和无线网络的广播特性使其安全性问题成为发展、应用的重要瓶颈。我们在对 WSN 密钥管理问题的最新研究进展进行系统分析、论述的基础上,指出了亟待解决的根本问题,提出了一系列有价值的研究方向,并对无线传感器网络密钥管理的发展趋势进行了展望。

参考文献:

[1] Carman D W, Kruus P S, Matt B J. Constraints and Approaches for Distributed Sensor Network Security[R]. [S. l.]: NAI Labs, 2000.

[2] Perrig A, Szewczyk R, Wen V, et al. SPINS: Security Protocols for Sensor Networks[J]. Wireless Networks, 2002, 8(5): 521 – 534.

[3] 李志军, 秦志光, 王佳昊. 无线传感器网络密钥分配协议研究[J]. 计算机科学, 2006, 33 (2): 87 – 91.
LI Zhi – jun, QIN Zhi – guang, WANG Jia – hao. Key Distribution Protocols in Sensor Networks[J]. Computer Science, 2006, 33(2): 87 – 91. (in Chinese)

[4] Perrig A, Song D, Tygar J D. A New Protocol for Efficient Large-group Key Distribution[C]// Proceedings of IEEE Sympium on Security and Privacy. Oakland: IEEE, 2001: 247.

[5] Huang S, Shieh S P, Wu S Y. Adaptive Random Key Distribution Schemes for Wireless Sensor Networks[C]//Proceed-

ings of Computer Security in the 21st Century. Berlin: Springer,2005:91 – 105.

[6] Blundo C, Santis A D, Herzberg A, et al. Perfectly Secure Key Distribution for Dynamic Conferences[C]//Proceedings of 12th Annual Int'l Cryptology Conf on Advances in Cryptology. Berlin: Springer,1992: 471 – 486.

[7] 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: ACM, 2003:52 – 61.

[8] Liu D, Ning P. Location – Based Pairwise Key Establishments for Static Sensor Networks[C] // Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM,2003:72 – 82.

[9] Dini G, Savino I. S2RP: a Secure and Scalable Rekeying Protocol for Wireless Sensor Networks[C] // Proceedings of IEEE MASS. Washington DC: IEEE,2006: 457 – 466.

[10] Miller M J, Vaidya N H. Leveraging Channel Diversity for Key Establishmen in Wireless Sensor Networks[C]// Proceedings of IEEE Infocom. New York:IEEE,2006:1 – 12.

[11] Camtepe S A, Yener B. Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor[J]. IEEE/ACM Transactions on Networking, 2007,15(2):346 – 358.

[12] Han S, Tian B, He M, et al. Efficient Threshold Self – healing Key Distribution with Sponsorization for Infrastructureless Wireless Networks[J]. IEEE Transactions on Wireless Communications, 2009,8(4):1876 – 1887.

[13] Liu F, Cheng X. A Self – Configured Key Establishment Scheme for Large – Scale Sensor Networks[C]// Proceedings of IEEE MASS. Washington DC:IEEE,2006:447 – 456.

[14] Liu D, Ning P, Li R. Establishing Pairwise Keys in Distributed Sensor Networks[J]. ACM Transactions on Information and System Security, 2005 8(1): 41 – 77.

[15] Delgosha F, Fekri F. Key Pre – distribution in Wireless Sensor Networks using Multivariate Polynomials[C] // Proceedings of 2nd IEEE Conference on Communication, Society Sensor and Ad Hoc Communication. Santa Clara, New York: IEEE, 2005: 118 – 129.

[16] Blom R. An Optimal Class of Symmetric Key Generation Systems[C] // Proceedings of EUROCRYPT'84. Berlin: Springer,1984: 335 – 338.

[17] Du W L, Deng J, Yunghsiang S, et al. A Pairwise Key Predistribution Scheme for Wireless Sensor Networks[C] // Proceedings of 1st ACM Workshop on Computer and Communications Security. New York: ACM,2003:42 – 51.

[18] Huang Q, Cukier J, Kobayashi H, et al. Fast Authenticated Key Establishment Protocols for Self – organizing Sensor Networks[C]//Proceedings of 2nd ACM International Conference on Wireless Sensor Networks and Applications. New York: ACM, 2003:141 – 150.

[19] Delgosha F, Fekri F. Threshold Key – establishment in Distributed Sensor Networks using a Multivariate Scheme[C] // Proceedings of IEEE Conference on Computer Communications. New York: IEEE, 2006:134 – 145.

[20] Huang D, Mehta M, Medhi D, et al. Location – Aware Key Management Scheme for Wireless Sensor Networks[C] // Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks. New York: ACM, 2004:29 – 42.

[21] Ito T, Ohta H, Matsuda N, et al. A Key Predistribution Scheme for Secure Sensor Networks using Probability Density Function of Node Deployment[C] // Proceedings of SASN'05. New York: ACM,2005:69 – 75.

[22] Akyildiz I F ,Su W ,Sankarasubramaniam Y, et al. A Survey on Sensor Networks[J]. IEEE Communications Magazine, 2002,40(8): 102 – 114.

[23] Jolly G, Kuscu M C, Kokate P, et al. A Low – Energy Key Management Protocol for Wireless Sensor Networks[C] // Proceedings of IEEE Symposium on Computers and Communications. Washington DC: IEEE, 2003:335 – 340.

[24] Oliveira L B, Aranha D F. TinyPBC: Pairings for Authenticated Identity-based Non-interactive Key Distribution in Sensor Networks[C]//Proceedings of 5th International Conference on Networked Sensing Systems. Kanazawa:IEEE,2008: 173 – 180.

作者简介:

米　波(1982 –),男,重庆人,2009 年获博士学位,现为讲师,主要研究方向为无线传感器网络、信息安全;

MI Bo was born in Chongqing, in 1982. He received the Ph. D. degree in 2009. He is now a lecturer. His research interests include wireless sensor network and information security.

Email: mi_bo@163.com

段书凯,男,重庆人,博士后,教授,主要研究方向为非线性系统、嵌入式系统;

DUAN Shu – kai was born in Chongqing. He is now a professor with the Ph. D. degree. His research interests include nonlinear system and embedded system.

宋　军(1971 –),男,重庆人,博士,教授,主要研究方向为物联网、CPA;

SONG Jun was born in Chongqing, in 1971. He is now a professor with the Ph. D. degree. His research interests includethe internet of things and CPA.

王　勇,男,重庆人,硕士,讲师,主要研究方向为计算机应用技术。

WANG Yong was born in Chongqing. He is now a lecturer with the M. S. degree. His research direction is computer application technology.