SPINS 安全框架协议研究*)

程宏兵[1,2]　王江涛[1]　杨　庚[1]

(南京邮电大学计算机学院　南京 210003)[1]　(江苏广播电视大学信工院　南京 210017)[2]

摘　要　无线传感器网络(WSN)是一种新形式的网络,与传统的有线网络和一般的无线网络有较大的差异。论文在阐述了无线传感器网络(WSN)及其安全问题的同时,重点讨论了依赖基站的安全框架协议——SPINS 并对其一些缺陷提出了一些改进方法,最后对 SPINS 协议具体实现时所需的研究问题进行了展望。

关键词　无线传感器网络,网络安全,SPINS 协议

Research of Secure Frame Protocol Based-on SPINS

CHENG Hong-Bing[1,2]　WANG Jiang-Tao[1]　YANG Geng[1]

(School of Computer Science & Technology, Nanjing University of Post Telecommunications, Nanjing 210003)[1]

(School of information engineering, Jiangsu Radio&Tv University, Nanjing 210017)[2]

Abstract　Wireless sensor network is a new form network, unlike traditional wire network or general wireless network. The paper first expatiates on wireless sensor network and it's security, then argues about the security frame protocol—SPINS, which is based on base-station in WSN. Aiming at SPINS' deficiency, the paper presents some improved approaches. Finally the paper concludes the vista of research concerns about SPINS when it will be applied in the future.

Keywords　Wireless sensor network, Betwork security, SPINS protocol

1　引言

计算机网络自产生之日起,尤其是上世纪 90 年代初的迅猛发展,使人们的生活发生了极大的变化。具有无线通信、数据采集和处理、协同合作等功能的无线传感器节点协同组织起来形成的 WSN 是一类无线 ad hoc 网络[1]。WSN 是当前信息技术的前沿之一。它是由大量无处不在的、具有无线通信与计算能力的微小传感器节点构成的自组织分布式网络系统,在整个网络系统中,大量的传感器节点收集,处理,并且交换来自于外界环境的数据,最终传输到外部基站。该系统是能根据环境自主完成指定任务的"智能"系统,它集成了传感器技术、微机电系统(MEMS)技术、无线通信技术和分布式信息处理技术。图 1 给出了目前一种公认的 WSN 体系结构。

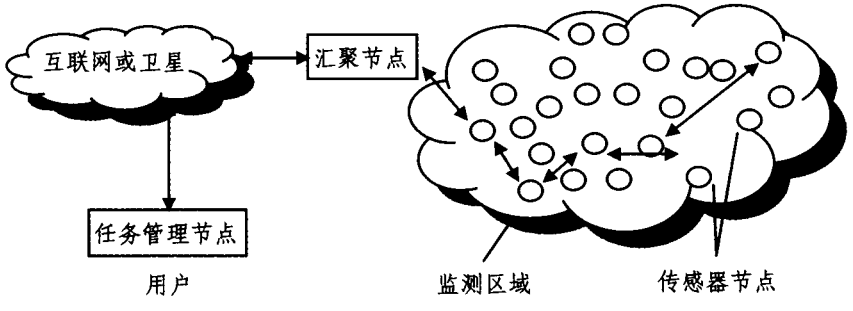

图 1　WSN 体系结构

目前,WSN 已经在很多方面得到了应用,在大多数的非商业应用中,如环境监测、森林防火、灾难急救、候鸟迁徙跟踪等应用,安全问题并不是一个非常紧要的问题。而在另外一些领域,如军事上对敌方的情报监测,商业上的一些利益相关的应用,安全问题就显得尤为重要。

论文将在第 2 部分对 WSN 的安全进行分析;第 3 部分讨论 WSN 中依赖基站的安全框架协议—SPINS,同时对其一些缺陷提出了一些改进方法;最后是文章的总结。

2　WSN 的安全

2.1　WSN 的安全问题

WSN 的安全和一般的网络安全的出发点都是相同的,都需要解决如下问题:

(1) 网络数据的机密性、完整性鉴别问题

机密性是指在网络中,所有敏感数据在存储和传输过程中都要保证其机密性,让任何人在截获物理通信信号的时候不能直接获得消息内容;完整性鉴别是指网络中的节点在接收到一个数据包的时候,能有相应的机制确认这个数据包和发出来的时候是一模一样的,没有被中间节点篡改或在传输中出现错误。

(2) 点到点的消息确认、数据新鲜性问题

点到点的消息确认是指网络节点在接收到另外一个节点

*)国家自然科学基金资助项目(编号:60573141),江苏省自然科学基金资助项目(编号:BK2004218)。程宏兵　博士研究生,讲师,主要研究方向为信息安全、网格计算、计算机网络。王江涛　博士研究生,主要研究方向为信息安全、网格计算、计算机网络。杨　庚　教授,博士生导师。

发过来的消息时，能够确认这个数据包确实是从该节点发过来的，而不是别人冒充的；数据新鲜性是指数据本身具有时效性，网络节点必须能够判断最新接收到的数据包是发送者最新产生的数据包。造成新鲜性问题一般有两种原因：一是由网络多路径延时的非确定性导致数据包的接收错序而引起，二是由恶意节点的重放攻击[2]而引起。

(3) 认证组播/广播、安全管理问题

认证组播/广播解决的是单一节点向一组节点/所有节点发送统一通告的认证安全问题。认证广播的发送者是一个，而接收者是很多个，所以认证方法和点到点通信认证方式完全不同。在SPINS安全框架中将详细分析广播认证问题；安全管理包括安全引导和安全维护两个部分，安全引导是指一个网络系统从分散的、独立的、没有安全通道保护的个体集合，按照预定的协议机制，逐步形成统一完整的、具有安全信道保护的、连通的安全网络的过程。在INTERNET网络中安全引导过程包括通信双方的身份认证、安全通信加解密密钥/认证密钥的协商等。安全引导过程对于传感器网络来说是最重要、最复杂，而且也是最富挑战性的内容，因为传统解决安全引导问题的各种方法由于其计算性在传感器网络中基本不能使用。安全维护主要研究通信中的密钥更新，以及网络变更引起的安全变更，方法往往是安全引导过程的一个延伸。

2.2 WSN的安全分析

随着传感器网络的深入研究，研究人员提出了多个传感器节点上的协议栈[3]，图2给出了一种目前处于主导地位的无线传感器网络协议栈。

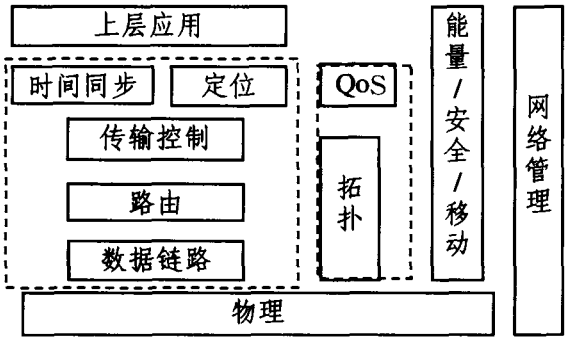

图2 WSN协议栈

上述协议栈包括物理层、数据链路层、网络层、传输层和应用层，与互联网协议栈的五层协议相对应，且功能基本一致。定位和时间同步子层在协议栈中的位置比较特殊。它们既要依赖于数据传输通道进行协作定位和时间同步协商，同时又要为网络协议各层提供信息支持，如基于时分复用的MAC协议，基于地理位置的路由协议等很多传感器网络协议都需要定位和同步信息。另外，由于无线传感器网络本身的特殊性，在协议栈中充分考虑了QoS、拓扑以及传感器的能量、移动及安全方面的因素。

针对无线传感器网络的特点，对于WSN协议栈各层的攻击、防御手段的解决思路和方法与传统网络安全问题不同，主要是由WSN自身的特点决定的：有限的存储空间和计算能力、缺乏后期节点布置的先验知识、布置区域的物理安全无法保证、有限的带宽和通信能力、不仅是点到点的安全，更是整个网络的安全、应用的相关性。

我们对传感器网络在网络协议栈的各个层次中可能受到的攻击方法和主要防御手段进行了分析，结果如表1所示。

表1 WSN攻击-防御手段

网络层次	攻击方法	防御手段
物理层	拥塞攻击(jamming)	宽频(跳频)、优先级消息、低占空比、区域映射、模式转换
	物理破坏(tampering)	破坏证明、节点伪装和隐藏
链路层	碰撞攻击(collision)	纠错码
	耗尽攻击(exhaustion)	设置竞争门限
	非公平竞争(unfairness)	使用短帧策略和非优先级策略
网络层	丢弃和贪婪破坏(neglect and greed)	使用冗余路径、探测机制
	汇聚节点攻击(homing)	使用加密和逐跳认证机制
	方向误导攻击(misdirection)	出口过滤；认证、监视机制
	黑洞攻击(blackholes)	认证、监视、冗余机制
传输层	洪泛攻击(flooding)	客户端谜题
	失步攻击(desynchronization)	认证

针对上表的攻击、防御措施，目前传感器网络的安全研究已经全面展开，它是一个开放的、活跃的领域。SPINS[4](Security Protocols for Sensor Network)安全体系是目前所提出的安全机制中比较流行、实用的传感器网络安全方案。它在数据机密性、完整性、新鲜性、可认证等方面都作了充分的考虑，但SPINS协议对传感网络中隐秘信道的信息泄露、节点被俘情况的处理、DoS的攻击等问题考虑不周，下面先对SPINS协议进行介绍，然后针对其存在的问题进行改进。

3 SPINS安全体系及其一些改进

在对SPINS安全框架进行描述之前，首先定义一些符号来描述协议过程：A，B表示安全对象，即传感节点；Na表示A产生的一个nonce随机数；$M_1 \mid M_2$ 表示两个消息的合并，要保持先后顺序；K_{AB} 表示A和B之间的共享密钥；$\{M\}K_{AB}$ 表示用密钥 K_{AB} 加密的西欧系密文；$\{M\}(K_{AB}, IV)$ 表示以IV(initial vector)作为初始化向量，用密钥 K_{AB} 加密的消息密文；IV是加密的初始向量，在很多块加密模式中需要IV数据。

3.1 SPINS安全框架协议

鉴于传感器网络面临的诸多威胁，必须要为传感器网络设计合适的安全防护机制，保证整个网络安全通信。SPINS安全协议是可选的传感器网络安全框架之一，包括SNEP(Secure Network Encryption Protocol)和μTESLA(micro Timed Efficient Streaming Loss-tolerant Authentication Protocol)两个部分。下面对SNEP和μTESLA进行讨论。

3.1.1 网络安全加密协议SNEP

SNEP协议是一个低通信开销的、实现了数据机密性NEP用以实现通信的机密性、数据认证、完整性认证、新鲜性保护的简单高效的安全通信协议。SNEP本身只描述安全实施的协议过程，并不规定实际使用的算法，具体的算法在具体实现时考虑。

SNEP协议采用预共享主密钥的安全引导模型，假设每个节点都和基站之间共享一对主密钥，其他密钥都是从主密钥衍生出来的。SNEP协议的各种安全机制是通过信任基站完成的。

SNEP协议的机密性：SNEP协议实现的机密性不仅仅具有加密功能，还具有语义安全特性。语义安全特性是针对数据机密性提出的一个概念，它的含义是指相同的数据信息在不同的时间、不同的上下文，经过相同的密钥和加密算法产

生的密文不同。语义安全可以有效抑制已知明密文攻击[2]SNEP 协议采用计数器模式的加密方法实现语义安全机制，其加密公式如下所示：

$E=\{D\}(K_{enc},C)$

其中 E 表示加密后的密文；D 表示加密前的明文；K_{enc} 表示加密密钥；C 表示计数器，用作块加密的初始向量。

SNEP 协议的完整性和点到点认证：SNEP 协议实现消息完整性和点到点认证是通过消息认证码(message authentication code，MAC)协议实现的。消息认证码协议的认证公式定义如下：

$M=\mathrm{MAC}(K_{mac},C|E)$

其中 K_{mac} 表示消息认证算法的密钥，$C|E$ 为计数器值 C 和密文 E 的粘接，表明消息认证码是对计数器和密文一起进行运算。消息认证的内容可以是明文也可以是密文，*SNEP* 采用的是密文认证。

K_{enc} 和 K_{mac} 这两个密钥都是通过基站共享的主密钥 K_{master} 按照相同的算法推演出来的。SNEP 没有定义推演算法，实现者可以按照一定的规则生成。

SNEP 协议的新鲜性认证：SNEP 协议通过 CTR 模式支持数据通信的弱新鲜性。所谓弱新鲜性是指一种单向的新鲜性认证。假设节点 A 给节点 B 连续发送 n 个请求数据包

$A\rightarrow B:\{R_{A1}\}(K_{enc},C_1),\mathrm{MAC}(K_{mac},C_1|\{R_{A1}\}(K_{enc},C_1))$

$A\rightarrow B:\{R_{A2}\}(K_{enc},C_2),\mathrm{MAC}(K_{mac},C_2|\{R_{A2}\}(K_{enc},C_2))$

…

$A\rightarrow B:\{R_{An}\}(K_{enc},C_n),\mathrm{MAC}(K_{mac},Cn|\{R_{An}\}(K_{enc},C_n))$

通过计数器值 B 能够知道这 n 个请求数据包是顺序从 A 发出来的。得到这 10 个请求包以后，B 会将强求交给其上层应用处理，并将相应消息回复给 A。A 从 B 收到 n 个 RSP 消息：

$A\leftarrow B:\{RSP_{A1}\}(K_{enc},C_{11}),\mathrm{MAC}(K_{mac},C_{11}|\{R_{A1}\}(K_{enc},C_{11}))$

$A\leftarrow B:\{RSP_{A2}\}(K_{enc},C_{22}),\mathrm{MAC}(K_{mac},C_{22}|\{R_{A2}\}(K_{enc},C_{22}))$

…

$A\leftarrow B:\{RSP_{An}\}(K_{enc},C_{m}),\mathrm{MAC}(K_{mac},C_{m}|\{R_{An}\}(K_{enc},C_{m}))$

A 同样根据计数器值可以判断这 n 个响应包是从 B 顺序发送出来的，并且对于任何响应包的重放攻击都能够有效抑制，即实现了弱新鲜性认证。弱新鲜性认证存在的一个问题是 A 不能判断它所收到的响应包 $\mathrm{RSP_{A1}}$ 是不是针对它发出的 $\mathrm{R_{A1}}$ 请求包的回应。因此，SNEP 协议定义了解决此问题的强新鲜认证方法。

SNEP 协议实现强新鲜特性使用 Nonce 机制。Nonce 是一个惟一标识当前状态的、任何无关者都不能预测的数，通常可由随即数产生器产生。SNEP 协议在其强新鲜性认证过程中，在每个安全通信的请求数据包中增加 Nonce 段，惟一标识请求包的身份。通信过程描述如下：

$A\rightarrow B:N_A,\{R_K\}(K_{enc},C),\mathrm{MAC}(K_{mac},C|\{R_K(K_{enc},C)\}$

$A\leftarrow B:\{RSP_K\}(K_{enc},C),\mathrm{MAC}(K_{mac},N_A|C|\{RSP_K\}(K_{enc},C))$

用 SNEP 协议完成节点间通信：使用 SNEP 协议完成节点间通信的一种可选方法是通过信任基站为将要通信的两个节点建立临时的通信密钥，现假设 A 和 B 都与基站 S 存在共享密钥 K_{AS} 和 K_{BS}，安全通道的建立过程如下：

$A\rightarrow B:N_A,A$

$B\rightarrow S:N_A,N_B,A,B,\mathrm{MAC}(K_{BS},N_A|N_B|A|B)$

$S\rightarrow A:N_A,\{SK_{AB}\}K_{AS},\mathrm{MAC}(K_{AS},N_A|B|\{SK_{AB}\}K_{AS})$

$S\rightarrow B:N_A,\{SK_{AB}\}K_{BS},\mathrm{MAC}(K_{BS},N_B|A|\{SK_{AB}\}K_{BS})$

SK_{AB} 是基站 S 为节点 A 和 B 设定的临时通信密钥，N_A 和 N_B 是强新鲜认证的 Nonce 随机数，在节点间通信完成以后，双方可以直接丢弃这个信任密钥。若以后再需要通信，可以重新协商新密钥。

3.1.2 μTESLA 协议

μTESLA 协议是基于时间的高效的容忍丢包的流认证协议，该协议的主要思想是先广播一个通过密钥 K_{mac} 认证的数据包，然后公布密钥 K_{mac}。这样就保证了在密钥 K_{mac} 公布之前，没有人能够得到认证密钥的任何信息，也就没有办法在广播包正确认证之前伪造出正确的广播数据包。这样的协议过程恰好满足流认证广播的安全条件。

μTESLA 协议的运行过程[5]包括基站安全初始化、网络节点加入安全体系和节点完成数据包的广播认证三个过程。

基站一旦在目标区域内开始工作，首先生成密钥池，确定密钥同步时钟。密钥池的尺寸 N 和密钥同步周期 T 一般根据实际的存储空间大小、网络生命周期以及广播频率来确定。假如密钥池密钥使用完毕，需要重新启动依次初始化和节点同步过程。

基站完成广播安全初始化以后，就开始接受节点的加入。每个节点通过 SNEP 协议与基站之间建立同步。现假设节点 A 在某一时间段 $[i\times T_{int},(i+1)\times T_{int}]$ 向内向基站 S 要求假如网络，则其加入的具体过程描述如下：

$A\rightarrow S:(N_M|R_A)$

$S\rightarrow A:(T_s|K_i|T_i|T_{int}|d),\mathrm{MAC}(K_{as},N_M|T_s|K_i|T_i|T_{int}|d)$

其中，N_M 是一个随机 Nonce，表示使用强新鲜性认证；R_A 是请求加入网络的数据包；K_{as} 是节点 A 与基站 S 之间的认证密钥，通过预共享主密钥产生；T_s 是当前时间；K_i 是初始化密钥；T_i 是当前同步间隔的起始时间；T_{int} 是同步间隔；d 是密钥发布的延迟时间尺寸，单位为 T_{int}。经过这样一轮认证过程，节点将获得关于认证广播的所有消息。

节点的加入过程可以穿插在整个网络运行的任何时段，而认证广播的过程在基站初始化完成以后就可以进行了。

3.2 SPINS 安全协议的改进

如前所述，在传感网络中，一个节点要加入网络，需要与基站使用 SNEP 协议完成密钥初始化和同步过程，此过程是一个点对点的单播过程，对于一个规模很大的网络来说，源端认证的广播协议初始化会耗费非常大的宝贵的传感器网络资源，这一点在传感器网络的实际应用中是不现实的。因此 μTESLA 协议适用的网络规模受到很大限制。例如在一个速率是 10kbps、支持 30 字节包长的通信平台上，在最好的信道状态下，2000 个节点的 μTESLA 初始化过程需要收发 4000 个数据包，至少花费 $4000\times30\times8/10240=93.75$ 秒。

(下转第 143 页)

ping Web Services to Implementation Platforms. Atlas Group, INRIA and LINA University of Nantes: [Research Report]. March 2004
11 Bordbar B, Staikopoulos A. Automated Generation of Metamodels for Web Service Languages. Atlas Group, INRIA and LINA University of Nantes: [Research Report]. 2004
12 MDA Guide Version 1.0. http://www.omg.org/cgi-hin/doc?mda-guide
13 Thöne S, Depke R, Engels G. Process-Oriented, Flexible Composition of Web Services with UML. In: Int Workshop on Conceptual Modeling Approaches for e-Business: A Web Services Perspective(eCOMO 2002), Tampere, Finland, 2002
14 Gardner T. UML Modeling of Automated Business Processes with a Mapping to BPEL4WS. In: 17th European Conference on Object-Oriented Programming(ECOOP), Darmstadt, Germany, 2003
15 Grønmo R, Solheim, I. Towards Modeling Web Services Composition in UML. In: The 2nd International Workshop on Web Services: Modeling, Architecture and Infrastructure(WSMAI-2004), Porto, Portugal, 2004
16 v d Aalst W M P. Don't go with the flow: Web Services composition standards exposed. Trends & Controversies Jan/Feb 2003 issue of IEEE Intelligent Systems, 2003
17 van der Aalst W M P, ter Hofstede A H M. Kiepuszewski B, et al. Workflow Patterns. Distributed and Parallel Database, 2003, 14(1): 5～51
18 Wohed P, v d Aalst W M P, Dumas M, t Hofstede A H M. Pattern Based Analysis of BPEL4WS, [FIT-TR-2002-04 Technical Report]. Queensland University of Technology, Australia, QUT 2003
19 v d Aalst W M P, Dumas M, t Hofstede AH M, et al. Pattern Based Analysis of BPML(and WSCI): [FIT-TR-2002-05 Technical Report]. Queensland University of Technology, Australia, QUT 2003
20 Wohed P, v d Aalst W M P, Dumas M, et al. Pattern-based Analysis of UML Activity Diagrams. BETA Working Paper Series, WP 129, Eindhoven University of Technology, 2004
21 Skogan D, Grønmo R, Solheim I. Web Service Composition in UML. 8th International IEEE Enterprise Distributed Object Computing Conference(EDOC 2004), California, 2004
22 Bezivin J, Hammoudi S, Lopes D, et al. An Experiment in Mapping Web Services to Implementation Platforms. Atlas Group, INRIA and LINA University of Nantes: [Research Report]. March 2004
23 OMG. Object Constraint Languange Specification. Object Mangament Group, Adopted Specification, 2003
24 Bezivin J, Breton E, Dupe G, et al. The ATL Transformation-based Model Management framework: [Research Report]. Atlas Group, INRIA and IRIN, September 2003
25 Unified Modeling Language: Superstructure(version 2.0), http://www.omg.org/docs/ptc/03-08-02.pdf
26 BEA, IBM, Microsoft. SAP AG and Siebel Systems: Business Process Execution Language for Web Services, Version 1.1. May 2003
27 W3C, Web Services Choreography Interface (WSCI) 1.0. W3CNote, August 2002
28 Grønmo R, Skogan D, Solheim I, et al. Model-driven Web Services Development. The 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service(EEE-04), Taipei, Taiwan, 2004
29 Bézivin J, Dupé G, Jouault F, et al. First Experiments with the ATL Model Transformation Language: Transforming XSLT into XQuery. 2nd OOP'SLA Workshop on Generative Techniques in the context of Model Driven Architecture, October 2003

(上接第 108 页)

另外，μTESLA 并没有考虑 DoS 攻击的问题[4,6]。恶意节点广播错误数据包，节点会将这些数据包保存起来等待密钥公布后验证，这样将可能耗尽节点的资源。

针对上述问题我们提出以下方案来对 SPINS 安全框架协议进行改进。

对于 μTESLA 协议在基站安全初始化时，如果在某一节点在中途需要加入网络时，可以先让该节点只与基站使用 SNEP 协议进行密钥分配和相关认证，此时无须与其它节点进行数据包的收发，而在网络中有数据包进行传送时，而此加入节点正处于该通信链路时，再进行相关的密钥分配和相关认证工作。利用这种节点加入方式会增加通信过程的开销，但避免了通信开始前节点加入时的巨大耗费，这样可以使整个传感器网络的资源耗费降到最低。

另外，对于 μTESLA 协议运行时节点加入过程存在的两个问题：

第一：$A \rightarrow S$ 的过程没有进行认证，所以比较容易受到 *DoS* 的攻击。

第二：整个过程没有加密。下面就 *μTESLA* 协议的运行中节点加入过程进行改进，可以使用加密的方法对其进行改进，加密过程如下：

$A \rightarrow S: (N_M | R_A), \mathrm{MAC}(K_{asm}, N_M | R_A)$

$S \rightarrow A: (T_s | K_i | T_i | T_{int} | d) K_{ase}, \mathrm{MAC}(K_{asm}, N_M | T_s | K_i | T_i | T_{int} | d)$

其中，K_{ase} 为节点与基站之间的通信加密密钥，K_{asm} 是通信认证密钥，都是通过共享的主密钥产生。这样，上述加密过程对于 $A \rightarrow S$ 进行了认证，同时对于 $S \rightarrow A$ 过程也进行了加密考虑。理论上该改进过程解决了 μTESLA 协议运行时节点加入过程存在的问题。

对于 μTESLA 中另一类 DoS 攻击的问题，即在传感器网络中存在恶意节点广播错误数据包，节点会将这些数据包保存起来等待密钥公布后验证，这样将可能耗尽节点的资源，对于这样的问题可以使用如下改进方案解决：首先在整个传感器网络中设置一个鲁棒性很好的初始密钥(非公开)对每个广播包进行一次预处理，可以让节点先过滤掉那些纯粹的错误广播包，避免浪费节点资源去存储它，当然此方法中初始密钥的选择非常重要。

针对 DoS 攻击，多级 μTESLA 协议[4,7]有较好的特性，但由于其难于实现并且又会占用更多的节点内存和计算资源，因此在具体实现时我们可以针对目标应用系统选择使用或者部分使用其中的安全处理机制，以此来部分解决 SPINS 安全框架协议存在的问题。

总之，SPINS 定义的是一个安全协议框架，在传感器网络中具体使用时，很多方面需要进行进一步深入的研究。

结束语 传感器网络的安全问题随着其应用逐渐成为现实而备受关注。文中就传感器网络的安全问题进行了讨论，对目前一种比较流行的传感器网络安全框架协议——SPINS 进行了深入的研究，并就其存在的问题提出了一些改进措施，并进行了相关的理论分析。但对于改进的 SPINS 协议在实际应用中还需考虑诸多问题，如加密算法的选择、消息认证算法的选择、密钥生成算法、随机数产生器。所有这些都是我们以后的研究方向。

参 考 文 献

1 Pottie G J, Kaiser W J. Embedding the internet: wireless integrated network sensors [C]. Communications of the ACM, 2000, 43(5): 51～58
2 Wood A D, Stankovic J A. Denial of service in sensor networks. IEEE Computer, 2002, 35(10): 54～62
3 Pister K, Hohlt B, Jeong J, Doherty L, Vainio J P. Ivy——A sensor network infrastructure. 2003. http://www-bsac.eecs.Berkeley.edu/projects/ivy
4 Perrig A, Szewczyk R, et al. SPINS: Security protocols for sensor networks. Wireless Networks, 2002, 8(5): 521～534
5 Li Dan, Wong K D, Hu Yu Hen, Sayeed A M. Detection, classification, and tracking of targets. Signal Processing Magazine, IEEE, 2002, 19(2): 17～29
6 Asada G, Dong M, Lin T S, et al. Wireless Integrated Network Sensor: Low Power System on a Chip. In: Proc. of the European Solid State Circuits Conf. 1998
7 Elson J, Estrin D. Time Synchronization for Wireless Sensor Networks. In: Proc. of the Intl Parallel and Distributed Processing Symposium(IPDPS). Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, San Francisco, CA, Apr. 2001