网络安全技术

大作业

BSN 中密钥体系的安全防护综述

姓名：董璐
学号：3113034016
学院：电子与信息工程学院
专业：计算机软件与理论
班级：硕 3035
Email：donglu6@126.com

BSN 中密钥体系的安全防护综述

董璐　硕 3035　3113034016

摘要：

无线传感器网络的飞速发展宣告着感知时代的到来，除了在军事、环境监控和工业控制上的广泛应用，人体生理状态的监控成为新的研究热点。无线体感网（Wireless Sensor Networks， BSN）就是针对人体状态进行普适实时监控的传感器网络应用。介于病人医疗信息（Patient Healthcare Information，PHI）的特殊性，BSN 必须保证网络传输的安全和隐私性。针对各种不同类型的攻击，密钥体系的安全防护是建立网络安全机制的基础，因此得到了广泛的关注。本文结合 BSN 的自身特点，对近年来 BSN 的密钥体系安全防护研究成果进行综述，同时，对安全防护机制形式化安全证明进行了讨论。

关键词： 无线传感网　BSN　密钥体系　安全防护　形式化安全证明

Abstract:

The rapid development of wireless sensor networks announces the arrival of senescing era. Beside the application in military or environmental surveillance and industrial controlling, human physiological status monitoring has become one of the latest research hotspot for sensor networks. Wireless body sensor networks are sensor network applications that perform real-time pervasive monitoring on human physiological status. As the specialism of Patient Healthcare Information (PHI), the security and privacy of network transmission has to be guaranteed in the BSN.For different types of attacks, proper security defense is the foundation of network security scheme. This paper surveyed relevant security defense schemes in BSN. In the meantime, it proposed a discussion about necessary formal security proof in BSN .

Keywords： WSN　BSN　Key system　security defense　formal security proof

一、 引论

随着无线网络的飞速发展，无线体感网（Wireless Sensor Networks， 下简称 BSN）指在人体周围部署的无线传感器网络系统，该系统主要负责对人体的生理健康状态和动作模式等进行持续精确的监测。BSN 不仅能够将人体的生理数据传递到远程医疗中心，还能够在人体上实现自动化治疗（如实现药物精确注射），并应用在与健康保健、远程医疗、运动监控等有关的智能医疗领域。可见 BSN 这个新兴的研究领域具有广阔的发展前景。

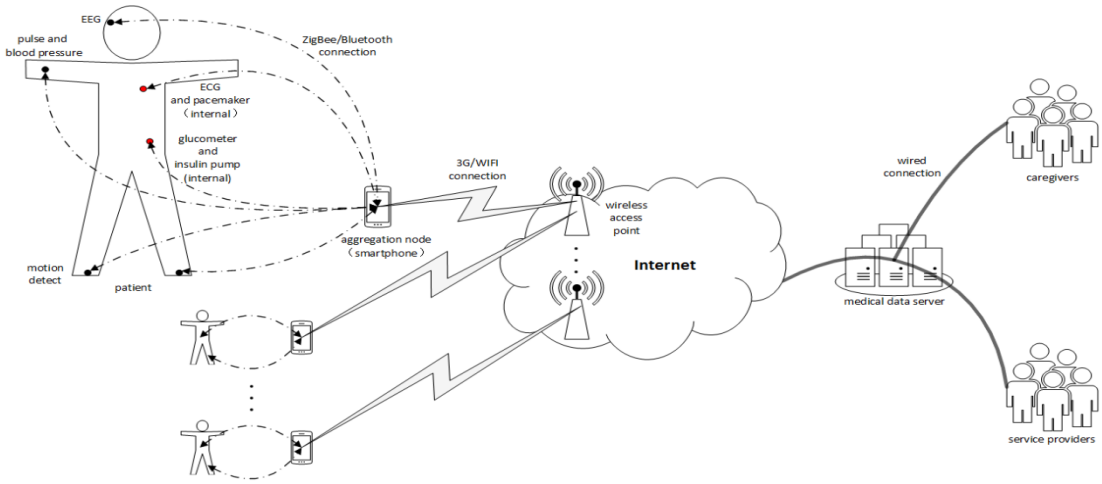

图 1 BSN 结构示意图

BSN 通过无线方式传输有关人体状态的数据，因此对数据精确性和私密性有很高要求。一套完整、可靠的安全机制是 BSN 系统必不可少的组成部件。对于现有的网络系统，基于密钥技术的加/解密、认证、签名过程是最为常见且有效的安全机制，而网络运行过程难免遇到各种攻击，所以安全、完整、可靠的密钥管理机制是网络系统正常运行的必要条件。

近年来，出现了许多针对 BSN 的综述研究成果。Cao 等人[1]对 BSN 实现过程中的基本技术进行综述，主要分析了 BSN 的应用环境、其中使用的生理数据测量设备、射频系统以及 BSN 之前的互连；Beno 等人[2]对 WBSN 的概念进行综述，对其中使用的物理实现技术进行比较分析，从原型系统的实现角度进行总结；Chen 等人[3]集中讨论了 BSN 系统中使用的节点设备、系统物理层和数据链路层的设计以及可以使用的通信技术。这些综述的讨论侧重点在于 BSN 原型系统的实现，但其中涉及 BSN 系统安全防护的内容的讨论并不充分。

二、 BSN 的本质特点

作为 WSN 的一种具体应用，BSN 具有自己的特点如网络无冗余、节点需认证、数据传输规律、传输延迟要求高、节点间确定性连接、节点移动性以及系统间协同工作等。下面详细列举出了这些不同：

1) 网络资源受限

本地 BSN 是一种单跳/双跳的星形无线传感器网络。因此也受到与 WSN 相同的限制：节点资源受限。尽可能地降低计算和传输开销可以延长节点寿命，尽量精简处理程序和存储密钥和原材料能够节省节点存储资源，这是 BSN 中密钥管理机制设计所需面对的问题。

2) 强安全要求

苛刻的安全性要求是 BSN 的显著特点之一。BSN 测量的人体生理状态数据涉及个人隐私，社会伦理和法律法规都要求保证此类敏感数据的安全性。强安全保护和受限制的网络资源之间存在矛盾，如何在安全性和资源消耗之间进行权衡具有研究潜力。

3) 组网灵活性

BSN 组网需要根据用户自身情况决定，本地网络中的功能节点需要能够灵活地添加和删除，同时节点加入的初始化过程和节点删除时的清除过程不能够影响系统的正常运行。

4) 确定的网络连接

确定的节点连接是 BSN 的另一个重要特点。由于本地 BSN 中没有冗余节点，需要保证网络中每个节点的确定连接。此外，BSN 要求对用户进行实时持续的监测，大量的数据和苛刻的数据传输延迟要求也是需要解决的问题。

从上面的研究中可以看到，BSN 很多自己的特性，因此现有的关于 WSN 的一些技术不能满足 BSN 的特殊要求，比如：BSN 中不能直接使用的预置密钥方法会限制了网络结构的可扩展性和组网灵活性。在这些本质特点中，最值得注意的就是它的强安全性要求，因个人医疗和健康数据属于个人隐私，许多国家制定了相应的法律对其进行保护。我们知道许多安全技术，如数据加密、数据完整性检验、数字签名技术、认证技术等，都将密钥作为安全凭证，在针对 BSN 环境下密钥管理问题的研究中，研究工作者考虑到 BSN 可能受到的各种安全威胁和

恶意攻击，在设计密钥管理机制的过程中都采取了相应的应对措施。

三、 BSN 密钥体系的安全防护

BSN 以无线传输的方式组织传感器形成用来监测与人体生理状态相关的敏感数据，因此整个系统的安全性是 BSN 技术实用化进程中必须解决的问题。不论是本地 BSN 节点的数据测量，还是控制器与数据中心之间的数据通信，都有可能受到各种无意或故意的安全威胁。相比传统 WSN 网络的应用环境，BSN 网络所测量的人体生理数据更容易引起攻击者的注意；同时，通过无线信道的数据传输方式更便于攻击者窃听或篡改网络中的数据流量。作为 BSN 系统安全运行的基础，网络中密钥体系的建立过程需要受到更加有效、完善的安全防护。

3.1 针对窃听攻击（Eavesdropping）

介于 BSN 的无线信道传播方式，在消息节点传输范围之内的任何实体都能够监听到节点发出的所有消息，这无疑增加了 BSN 通信数据受到恶意攻击的可能性。攻击者希望通过窃听 BSN 节点的无线通信消息获得 BSN 使用者的实时生理数据，或者通过对消息的发送频率、类型、目的地进行分析得到与 BSN 使用者相关的隐私[4]（在医疗环境下，可以通过对消息类型和目的地进行分析可以得知患者的患病情况）。为了保证生理测量数据的安全无线广播，需要使用相应密钥在发送消息前对其进行加密。在系统初始化过程中，用于协商共享秘密的广播消息也可能受到窃听攻击。对于对称密钥加密方法，通信双方使用的密钥不能直接在不安全的无线信道上广播发送，通常通过密钥预置或利用本地原材料直接生成[5, 6]；对于非对称加密来说，由于窃听攻击者无法通过通信双方发送的公开密钥部分推出私有密钥部分，因此可以直接在不安全的无线信道上直接发送密钥协商材料[7, 8]。

3.2 针对共谋攻击（Collusion Attack）

当 BSN 中的成员节点被攻击者捕获后，可能出现节点中持有的密钥或密钥材料泄露。对于多数预置方法而言，单个节点被捕获而导致的密钥材料泄露可能不会造成过多共享秘密的失效，因为节点中只存有有关自身密钥建立或者部分组

密钥建立材料，不会对全局网络产生严重影响；但是，如果攻击者能够捕获多个节点，并且获得其中预置的秘密建立信息，就有可能恢复出完整的组共享秘密从而威胁到全网的通信安全，这种通过连理多个被捕获节点中预置秘密而恢复全局共享秘密的攻击称为共谋攻击。共谋攻击通过利用多个节点持有的秘密协商材料恢复完整的共享秘密，其对全网范围内的安全通信形成威胁，因此在相应机制的设计过程中受到了重点考虑。

在 He 等人[9]提出的预置多项式方法中，节点通过预置的共享多项式部分在节点本地根据通信方 ID 可以建立共享密钥。对于 t 阶的共享多项式，攻击者仅仅捕获单个节点是无法恢复整个共享多项式的，但是如果攻击者能够捕获至少 t 个节点，并且获得其中的共享多项式部分，通过将其中的共享多项式联立可形成由 t 个 t 元方程组成的方程组，进而可以解出完整多项式中的所有系数，这会导致攻击者能够获得与网络内所有持有该共享多项式部分的节点之间的成对密钥。这是基于共享多项式方法的本质缺点。为了避免这种情况的发生，研究工作者提出在保证计算可行的情况下，尽量提高共享多项式的阶数。对于 BSN 环境而言，由于网络规模小，网络节点数量较少，因此可以保证共享多项式的阶数大于网络节点数目。这样处理使得攻击者即使捕获了网络中所有的节点也无法恢复出完整的共享多项式，而我们知道，对于攻击者来说，捕获网络中所有的节点是不现实的。

FoSBaS[6]是一种 BSN 环境下的组密钥建立协议，它能够保证组密钥的前向和后向安全性，同时能够抵御共谋攻击。FoSBaS 采用的贡献式组密钥协商方法能够有效地抵御共谋攻击，因为所组密钥的协商是由当前组内所有合法成员共同实现的，组密钥生成依赖于所有合法组成员的组密钥协商部分。只要组中出现成员变动，共享组密钥就需要重新建立，以此保证了不再组中的成员即使共享持有秘密也无法获得当前的会话组密钥。Ming Li 等人[10, 11]提出的 GDP 方法所建立的组密钥同样具有这样的特点。

3.3 针对组合攻击（Combinatorial Attack）

在前文介绍的基于人为操作实现实体认证的方法中，网络中成员共享秘密的建立过程由 BSN 操作者在物理上确定，组秘密协商节点通过蜂鸣器提醒、LED

闪烁或者数字显示等方法向 BSN 操作者展示自己获得的共享秘密，由操作者对其进行比较和确认。考虑到 BSN 操作者的接受能力，需要通过物理方式进行对比确认的消息长度不能过长。多数研究工作者提出使用共享消息的哈希值代替相对较长的原始消息来进行比较，其中使用的摘要函数可以根据任意长度的输入消息生成固定长度的消息摘要（32bit）[12]。摘要函数是一类特殊的哈希函数，其主要区别在于摘要函数生成的摘要长度小于哈希函数生成的哈希值（above 256bit），因此更加适用于 BSN 操作者进行物理比对。但是更短的消息摘要函数带来了问题：摘要函数不具有普通哈希函数抵御次原像攻击（second preimage resistance）的能力，即摘要函数可能根据两个不同的原始消息生成相同的摘要消息值。利用摘要函数的这个特性，攻击者可以通过组合手段针对确定的原始消息和消息摘要伪造出具有相同消息文摘的伪造消息，从而通过 BSN 操作者的认证过程，这种攻击称为组合攻击[12]。

为了抵御组合攻击，研究工作者在基于人为操作实现实体认证的过程中引入了承诺机制（commitment scheme）[12]。承诺机制允许承诺方先对选定的声明值进行承诺，在保证声明值私密的情况下先利用承诺值进行秘密协商，之后再发出揭示值，利用揭示值可以验证承诺值的有效性。使用承诺机制的共享秘密协商方法将整个协商过程分为两部分：承诺阶段和揭示阶段。承诺阶段中所有参与共享秘密协商的实体相互发送承诺值，根据收到的承诺值数量确定参加共享秘密协商的实体个数，只有确定所有参与实体收到正确数量的承诺值的前提下才能同步进入揭示阶段；在揭示阶段，之前对声明值进行承诺的实体发出揭示值，参与秘密协商的实体收到揭示值后可以在本地验证之前收到承诺值的有效性，确定有效之后可以根据揭示值、承诺值和声明值同时建立共享秘密。因此只有在揭示阶段网络中的其他成员才能够生成共享文摘消息，攻击者不能事先确定摘要消息，因而也无法实行组合攻击。还有许多 BSN 中共享秘密协商机制利用承诺方法抵御组合攻击[10, 11]，其本质思想是一致的，即防止攻击者在秘密协商开始时即可预知最终用来比对的共享秘密。

3.4 针对认证过程的攻击（Authentication Attack）

在 BSN 认证过程中，对于交互式认证方法，认证双方需要进行多次的消息

交互以建立和验证认证共享秘密。攻击者可以针对交互式的认证过程进行攻击，试图在通信双方进行认证时加入认证过程，通过修改或劫持双方的认证消息，通过网络认证或者阻止合法成员加入网络。

在使用预置密码实现认证的方法[13,14,15]中，通信双方的认证凭据为只有双方共享的认证密码。尽管密码本身只由认证双方持有，但实际认证过程则是通过对比由认证密码加密的消息实现的。攻击者可能并不能得知对称密码，但是其可能直接通过监测网络流量，截取双方用来认证的消息，直接向通信方发送，由于攻击者截取的消息是由有效的认证密码生成的，因此可能能够通过对称认证过程。这种攻击称为重放攻击（replay attack）。

为了避免重放攻击，认证过程中需要保证消息的新鲜性，即消息接收方需要能够确定收到消息是最新生成的，同时消息的接受顺序需要得到保证。Nonce 是一个在一定时间段内只出现一次的随机数，在消息通信中常常用来保证消息顺序和新鲜性。通信双方在进行消息交互时需要同时发送 nonce，并且后发送的 nonce 要与之前的相关(通常情况下是+1 关系，特殊安全机制里对 nonce 有特殊要求)。消息接收者通过 nonce 可以判断消息是否新鲜、消息是否按照顺序发送，这种方法被广泛应用在 BSN 中的认证和密钥建立协议当中[15]

对于使用非对称方法协商认证密钥的机制来说，共享密钥本身不会受到安全威胁。但是，由于最初的 DH 密钥协商方法中没有消息认证机制，消息接收者不能确定收到公钥与公钥持有者真实身份之间的对称关系，使得攻击者得以实施中间人攻击：攻击者在通信双方之间充当中间人，分别截获双方的交互消息，并且冒充双方身份与通信双方基于攻击者的密钥建立共享秘密，从而得以在双方不知情的情况下掌握双方之间的所有通信流量，这种共享秘密协商方法会受到攻击的原因在于双方直接将公开密钥部分在非安全信道上传送，同时协商过程缺少认证机制，双方不能确定收到公钥与公钥持有者之间的绑定关系。在针对 BSN 的密钥管理机制设计中，研究工作者提出了相应措施来应对可能出现的中间人攻击。

Singh, K 等人[13]提出的 DHEKE 是 BSN 环境下的一种可认证高效密钥建立协议，协议中基于 DH 方法实现节点认证密钥的协商。在进行 DH 交换之前，认证双方首先在本地根据同类节点测得的生理信息生成对称密码；随后进行双方公开密钥部分交换时，先使用密码对公开密钥部分进行加密，之后再发送密文；接

收方收到密文后，使用根据本地生理信息生成的对称密码对密文进行解密，获得公开密钥部分，最终根据 DH 方法实现密钥协商。总而言之，为了抵御中间人攻击，通信双方不能在无认证的前提下直接进行消息通信，需要借助双方共享的秘密（对称密码、签名等）对消息来源进行确定，避免攻击者对双方交互过程进行消息劫持而发动中间人攻击。

四、安全防护机制形式化证明

在 BSN 环境下，所建立协议的安全性需要有所保证。随着协议规模和功能的日趋复杂，仅凭人为简单的理论分析并不能保证其正确性。BSN 就是这样的一种应用，其中运行协议的正确性需要得到保证。如果出现错误或非安全状态，对于 BSN 使用者而言后果可能是致命的。

有许多研究工作者针对 BSN 环境下密钥管理协议进行了形式化证明，这是由密钥管理协议在系统安全中的基础地位决定的：几乎所有的安全机制都需要基于密钥体系建立，因此如何保证密钥体系建立过程的安全性至关重要。形式化证明能够较为全面细致地分析相应协议的正确性、安全性和可靠性，并且增强说服力。

Singh, K 等人[16]针对 BSN 环境下基于生理信息的密钥建立协议进行了形式化分析和验证。在文中，Singh, K 等人根据协议过程中提出的原始需求对协议本身和使用环境进行建模，建模过程使用了基因设计方法[17]。基因设计方法根据协议的原始需求建立行为树（behavior tree），通过协议的行为树和 BSN 使用者事件可以产生 SAL 码（SAL code）[18]；模型监测器对 SAL 码进行验证从而实现对传感器环境下的协议的验证。

Lin X[4]在提出的 BSN 隐私保护机制中对协议的隐私保护过程进行了形式化证明。文中讨论了内容相关隐私和上下文相关隐私的保护过程。由于隐私性的保护基于加密过程的语义安全性，因此 Lin X 等人基于 M Bellare 等人[19]提出的随机预言（random oracle）模型对协议中的消息交互过程的正确性和安全性进行了形式化证明。随机预言使用一种挑战者/攻击者的形式对协议交互过程进行抽象，所建立的模型根据实际环境赋予挑战者和攻击者相应的能力；在不同的能力假设情况下，根据概率论计算攻击者在自己能力范围内能够获取加密信息明文的可能

性。文中证明在根据实际环境所设置的能力下，攻击者获取加密信息明文的概率是可以忽略不计的。与此类似，Ming，Li 等人[11]对其建立的 BSN 安全初始化和密钥管理机制中实体认证以及可认证密钥协商的通信过程进行了形式化证明，证明过程基于 M Bellare 等人[20]根据随机预言模型建立的实体认证与密钥分配方法。文章对 BSN 中节点认证和对称密钥协商过程进行抽象，根据 M Bellare 等人提出的 Matching Conversation 模型对整个通信过程进行建模，进而实现形式化的安全分析。

Chaudhry J 等人[21]认为：从本质上讲，任何安全协议在攻击者持有足够资源的情况下都有可能被攻破。研究工作者所设计的安全协议可能存在或多或少的不足或漏洞，这些问题仅仅依靠人为的简单理论分析很难排除，许多情况下当协议部署后系统运行一段时间后才会慢慢显现出来。BSN 的安全运行对于使用者来说至关重要，因此在协议部署之前需要针对其安全性进行验证。安全性验证并不能保证协议的完全安全性，但是能够排除大多数协议不足和漏洞，并且对协议的运行状态有大致的了解。Chaudhry J 等人[21]针对 BSN 安全协议中可能出现的漏洞和受到的攻击、用来检测这些漏洞的验证方法以及这些协议在 BSN 中的实现前景进行了讨论。随后，Chaudhry J 等人对已有的用于验证加密协议安全性的方法进行了分类讨论，主要包括模型检测方法、演绎/理论证明方法、基于逻辑编程的方法、基于类型系统的方法和基于抽象的方法。针对具体协议应该使用哪一种方法需要根据协议本身特点决定，如是否为有限状态系统、系统内回话数量多少等，验证方法本身也可分为非全自动方法和自动化方法。要想对相应的协议进行验证，需要首先对协议通信过程进行抽象，之后根据协议的本质特性选择相应的验证方法，利用相应验证工具对协议安全性进行验证。

五、结论

随着 WSN 和嵌入式计算技术的发展以及社会各行业对人体监控系统的需求，BSN 已经成为当前的研究热点。为了使 BSN 达到实用要求，要首先了解 BSN 的本质特点，才能建立基于密钥的安全机制。而现实的系统运行时会遇到各种各样的攻击，因此密钥体系的安全防护是所有安全机制的重点。关于 BSN 中密钥体

系的安全防护机制的研究有很多，但各有侧重，仍处于理论研究阶段。针对 BSN 环境下安全防护机制进行了形式化证明使理论分析正确性得到保证。从现状分析和研究趋势来看，BSN 中的安全问题具有很强的研究潜力。

参考文献

[1] Cao H, Leung V, Chow C, et al. Enabling technologies for wireless body area networks: A survey and outlook[J]. Communications Magazine, IEEE, 2009, 47(12): 84-93.

[2] Beno, et al., A survey on wireless body area networks. Wirel. Netw., 2011. 17(1): p. 1-18.

[3] Chen, M., et al., Body Area Networks: A Survey. Mobile Networks and Applications, 2011. 16(2): p. 171-193.

[4] Lin X, Lu R, Shen X, et al. SAGE: a strong privacy-preserving scheme against global eavesdropping for ehealth systems[J]. Selected Areas in Communications, IEEE Journal on, 2009, 27(4): 365-378

[5] Morchon O G, Baldus H, Sanchez D S. Resource-efficient security for medical body sensor networks[C]//Wearable and Implantable Body Sensor Networks, 2006. BSN 2006. International Workshop on. IEEE, 2006: 4 pp.-83.

[6] Ren Y, Oleshchuk V, Li F Y, et al. FoSBaS: A bi-directional secrecy and collusion resilience key management scheme for BANs[C]//Wireless Communications and Networking Conference (WCNC), 2012 IEEE. IEEE, 2012: 2841-2846.

[7] Tan C C, Wang H, Zhong S, et al. Body sensor network security: an identity-based cryptography approach[C]//Proceedings of the first ACM conference on Wireless network security. ACM, 2008: 148-153.

[8] Tan C C, Wang H, Zhong S, et al. IBE-lite: a lightweight identity-based cryptography for body sensor networks[J]. Information Technology in Biomedicine, IEEE Transactions on, 2009, 13(6): 926-932.

[9] He D, Chen C, Chan S, et al. Secure and Lightweight Network Admission and Transmission Protocol for Body Sensor Networks[J]. 2011.

[10] Li M, Yu S, Lou W, et al. Group device pairing based secure sensor association and key management for body area networks[C]//INFOCOM, 2010 Proceedings IEEE. IEEE, 2010:

1-9.

[11] Li M, Yu S, Guttman J D, et al. Secure ad hoc trust initialization and key management in wireless body area networks[J]. ACM Transactions on Sensor Networks (TOSN), 2013, 9(2): 18.

[12] Huang X, Chen B, Markham A, et al. Human interactive secure key and identity exchange protocols in body sensor networks[J]. Information Security, IET, 2013, 7(1): 30-38.

[13] Singh K, Muthukkumarasamy V. Authenticated key establishment protocols for a home health care system[C]//Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on. IEEE, 2007: 353-358.

[14] Kanjee M R, Divi K, Liu H. A two-tiered authentication and encryption scheme in secure healthcare sensor networks[C]//Information Assurance and Security (IAS), 2010 Sixth International Conference on. IEEE, 2010: 271-276.

[15] Drira W, Renault E, Zeghlache D. A hybrid authentication and key establishment scheme for WBAN[C]//Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on. IEEE, 2012: 78-83.

[16] Singh K, Muthukkumarasamy V. Verification of key establishment protocols for a home health care system[C]//Intelligent Sensors, Sensor Networks and Information Processing, 2008. ISSNIP 2008. International Conference on. IEEE, 2008: 363-368.

[17] Sithirasenan E, Zafar S, Muthukkumarasamy V. Formal verification of the IEEE 802.11 i WLAN security protocol[C]//Software Engineering Conference, 2006. Australian. IEEE, 2006: 10 pp.

[18] Rushby J. The needham-schroeder protocol in sal[J]. CSL Technical Note, 2003.

[19] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols[C]//Proceedings of the 1st ACM conference on Computer and communications security. ACM, 1993: 62-73.

[20] Bellare M, Rogaway P. Entity authentication and key distribution[C]//Advances in Cryptology—CRYPTO'93. Springer Berlin Heidelberg, 1994: 232-249.

[21] Chaudhry J, Qidwai U A, Rittenhouse R G, et al. Vulnerabilities and verification of cryptographic protocols and their future in Wireless Body Area Networks[C]//Emerging Technologies (ICET), 2012 International Conference on. IEEE, 2012: 1-5.