Journal of System Simulation

Volume 27 | Issue 4 Article 13

8-20-2020

Research of Multi-factor Identity Authentication Scheme for ZigBee Network Nodes

Weiwei Zhou
Information Engineering University, Zhengzhou 450000, China;

Yuntian Yue
Information Engineering University, Zhengzhou 450000, China;

Bin Yu
Information Engineering University, Zhengzhou 450000, China;

Research of Multi-factor Identity Authentication Scheme for ZigBee Network Nodes

Abstract

Abstract: To solve the problem of the man-in-the-middle attack and impersonation attack in ZigBee networks, a scheme based on multi-factor identity authentication for ZigBee network nodes was proposed. The scheme bound the fresh factor updated in a particular cycle with hardware information via a one-way hash function to generate hardware information factor. On this basis, the scheme achieved the authentication mechanism for the nodes through the comparison among key factor, hardware information factor and configuration information factor received by control center. Meanwhile, the nodes completed control center authentication through the signature verification of the message received. Thus, the bidirectional authentication between nodes was achieved. The link key was updated to defense the illegal invasion of the nodes. The BAN-logic security analysis and experiment results show that the new scheme can not only resist the man-in-the-middle attack and impersonation attack effectively, but also has a distinct advantage over computing and storage.

Keywords

identity authentication, multi-factor, signature verification, frame structure, fresh factor

第 27 卷第 4 期 系统仿真学报© Vol. 27 No. 4
2015 年 4 月 Journal of System Simulation Apr., 2015

ZigBee 节点多因子身份认证方案研究

周伟伟，岳云天，郁滨
(信息工程大学，郑州 450000)

摘要：针对 ZigBee 网络所面临的中间人攻击和假冒攻击，*提出了一种 ZigBee 节点多因子身份认证方案，该方案引入以特定周期更新的新鲜因子，并将其与节点硬件信息绑定，调用单向杂凑函数生成硬件信息因子，由控制中心匹配节点上传的密钥信息因子、硬件信息因子和配置信息因子完成对节点的身份认证；同时，节点对接收到的消息进行签名验证，完成节点对控制中心的身份认证，从而实现节点间的双向身份认证，并对节点持有的对密钥实施更新，以防止非法节点入网对整个网络造成危害*。BAN 逻辑安全性分析及实验结果表明，该方案可有效抵御中间人、假冒等攻击，同时在计算开销和存储需求上有明显优势。

关键词：节点身份认证；多因子；签名验证；帧结构；新鲜因子
中图分类号：TP309.1 文献标识码：A 文章编号：1004-731X (2015) 04-0762-08

Research of Multi-factor Identity Authentication Scheme for ZigBee Network Nodes

Zhou Weiwei, *Yue Yuntian*, *Yu Bin*
(Information Engineering University, Zhengzhou 450000, China)

Abstract: To solve the problem of the man-in-the-middle attack and impersonation attack in ZigBee networks, *a scheme based on multi-factor identity authentication for ZigBee network nodes was proposed. The scheme bound the fresh factor updated in a particular cycle with hardware information via a one-way hash function to generate hardware information factor.* On this basis, *the scheme achieved the authentication mechanism for the nodes through the comparison among key factor, hardware information factor and configuration information factor received by control center.* Meanwhile, the nodes completed control center authentication through the signature verification of the message received. *Thus, the bidirectional authentication between nodes was achieved. The link key was updated to defense the illegal invasion of the nodes.* The BAN-logic security analysis and experiment results show that the new scheme can not only resist the man-in-the-middle attack and impersonation attack effectively, but also has a distinct advantage over computing and storage.

Keywords: identity authentication; multi-factor; signature verification; frame structure; fresh factor

引言

ZigBee 作为无线传感器网络(WSNs)技术的鲜明代表，其开放性、自组网等特征使得物理层到应用层都面临着来自网络外部和内部的潜在安全威胁和攻击。因此，出现了一系列针对 ZigBee 入网及通信安全的研究，如针对网络安全威胁与攻击[1]、信任机制[2]、节点身份认证[3]等。

ZigBee 节点身份认证问题一直是近几年来研究的热点。文献[3]指出适合 ZigBee 节点身份认证

收稿时期：2014-06-04 修回时期：2014-10-24;
作者简介：周伟伟(1990-)，男，河南洛阳人，硕士生，研究方向为 ZigBee、信息安全技术；岳云天(1968-)，男，河南开封人，博士，副教授，硕导，研究方向为数字隐写、信息安全、通信技术；郁滨(1964-)，男，河南郑州人，博士，教授，博导，研究方向为信息安全、无线网络安全技术、视觉密码等。

的几项技术，其中消息认证码可以对节点实施认证，但其仅适合单播通信节点的认证，在多播通信节点中会使组密钥信息泄露，导致网络不安全；基于 ECC 的身份认证机制通过建立分级认证机构并配合节点的认证信息以及签名验证机制实施认证，该方案计算量和存储需求较小，但仅通过密钥单因子身份认证机制其安全强度并不高，被捕获节点密钥信息泄露会直接威胁整个网络的安全。“密钥+配置信息”的双因子认证机制虽然引入了新的认证因子，但配置信息本身需受到密钥因子保护，当密钥因子泄露时会导致系统处于不安全状态。因此，应当引入不受密钥因子制约的认证因子，同时配合其他技术实现高安全的 ZigBee 节点身份认证方案。目前，身份认证主要分为基于密码技术的身份认证和基于硬件信息的身份认证。

基于密码技术的节点身份认证主要包括Hash-Lock[4]、随机化Hash-Lock[5]，TinyPK[6]，E-G[7]、强身份认证[8]和分布式身份认证[9]。Sarma等人提出的Hash-Lock使用替代的思想来防止信息泄露,但其经无线信道明文传送真实*ID*导致假冒攻击和重传攻击能够对本协议发起有效攻击。随机化Hash-Lock认证方法中中间节点以明文的方式经不安全的无线信道将终端标识ID_k传送给终端，因此，其不能抵抗假冒攻击且易被追踪。TinyPK方案虽然采用了多方认证代替单一认证方式，但通信开销过大，在WSNs中会导致效率下降，而且如果某个认证节点被捕获会导致信息泄露。E-G方案采用各自持有的密钥匹配实现认证，随着被捕获节点的增加，其安全性会受到严重威胁。相对于TinyPK，Z Benenson等人提出的强用户认证方案可有效抵抗节点复制攻击，但节点认证中能耗过大，对拒绝服务攻击没有较好的防御措施。K Bauer等人提出的分布式身份认证方案虽计算量小、容错性好，但通信量过大，容易造成网络拥堵。

基于硬件信息的身份认证通过计算机或者通信设备本身的唯一硬件特征来标识用户身份，这种身份认证方式认证快速，但仅靠硬件信息来识别用户身份，其硬件信息易被获取，安全性并不高，需要将此技术与其他认证方式或技术相结合、拓展。ZigBee协议规范中并未考虑节点身份的合法性问题,当非法节点获取网络中的密钥等关键信息后，可以轻易地操纵节点对整个ZigBee网络实施窃听、重放、伪造等攻击[10]。

本文结合现有非对称密码体制认证方案、对称密码体制认证方案以及ZigBee节点所持有的硬件信息，提出一种适用于ZigBee网络的“密钥+硬件信息+配置信息”多因子身份认证方案，设计控制中心、簇头、终端的双向认证流程，保证入网节点的合法性，抵御中间人攻击以及因认证信息泄露所导致的假冒攻击。

1 多因子身份认证方案

本方案中所用到的符号及其含义如表 1 所示。

表 1 方案中所用符号含义表

符号	含义	符号	含义
NC	控制中心	PuK_{NC} $\Pr K_{NC}$	网络控制中心的公私钥对
CH_n	簇头	PuK_{CH_n} $\Pr K_{CH_n}$	簇头的公私钥对
ED_n	终端节点	key_{ic} key_{id}	簇头与控制中心的对密钥
Ad	*IEEE* 地址	key_{i1} key_{i0}	终端与控制中心的对密钥
G	杂凑函数	D	控制中心生成的新鲜因子
t_2	接收帧时间	T_2	最大接收延迟时间
T_0	帧发送周期	T_1 T_3 T_4 T_5	帧发送时间戳
T_{date}	初始时间	$\|$	字符串连接操作
TL_i	认证有效期	PuK_{ED_n} $\Pr K_{ED_n}$	终端的公私钥对

第 27 卷第 4 期 系统仿真学报 Vol. 27 No. 4
2015 年 4 月 Journal of System Simulation Apr., 2015

1.1 MAC 层未定义帧字段的设计

采用“密钥+硬件信息+配置信息”的多因子身份认证方案，需要对协议中 MAC 命令帧的未定义字段进行重新设计，如图1所示，目的地址采取广播的形式，以保证簇节点(路由)能够准确接收并响应请求认证的设备，*IEEE* 地址字段通过固件读取 XDATA 中的 INFORMATION PAGE 存储字段获取，硬件信息因子为源64位 *IEEE* 地址与网络新鲜因子通过单向函数产生，即 $H = G\ (Ad\ ,\ D)$，以此保护设备的真实 *IEEE* 地址。其中 H 为硬件信息因子，G 为单向杂凑函数，Ad 为请求设备的真实 *IEEE* 地址，D 为控制中心(协调器)向全网发送的新鲜因子。同时，新设计的 MAC 帧中还添加了初始配置时间 T_{data} 字段。

MAC报头（MHR）							MAC负载	MFR
BYTE:2	1	2	8	2	8	2	变量	2
帧控制	序列号	寻址字段				配置时间 T_{date}	帧负载	FCS
		目的PANID	目的地址(广播)	新鲜因子D	源IEEE地址 Ad			

位0-2	3	4	5	6	7-9	10-11	12-13	14-15
帧类型	安全性启动位	等待帧	确认请求	PAN网内	保留位	目的寻址模式	保留位	源寻址模式

图 1　请求认证的 MAC 层帧结构

控制中心向下广播的信标帧中添加了上述协议帧中的 R 字段，该字段中随机数 R 会随着信标帧以周期 T_0 更新而不断更新，以保证随机数的新鲜性。其他字段与请求认证的 MAC 层的帧结构保持一致，方案中的帧传输采取加密保护。

1.2 簇头与中心、簇头与终端分级双向身份认证

本认证方案中采用椭圆曲线密码机制[11]，网络控制中心(*NC*)选择安全的椭圆曲线域参数 e，并生成密钥对 $(\Pr K_{NC}, PuK_{NC})$。其中椭圆曲线的域参数和 *NC* 的公钥 PuK_{NC} 是全网公开的，网络中的簇头 CH_1，CH_2，…… CH_n 分别使用相同的椭圆曲线域参数生成各自的密钥对 $(\Pr K_{CH_1}, PuK_{CH_1})$，$(\Pr K_{CH_2}, PuK_{CH_2})$，……，$(\Pr K_{CH_n}, PuK_{CH_n})$，其中，私钥由各节点保存，各自公钥对外公开。

当节点部署后开始上电认证入网。首先，簇头发送入网请求帧，控制中心经认证通过后与簇头建立网络连接。然后，终端节点发送入簇请求帧，经簇头认证通过后建立整个网络结构。依据控制中心向全网发送的信标帧对各簇头节点和终端节点进行重新认证，及时删除非法节点，保证整个网络安全可靠。

1.2.1 簇头(CH_j)与控制中心(*NC*)双向认证

当簇头上电后首先读取自身硬件地址信息并保存，准备需要请求认证的信息，然后检测信道。当信道空闲时向网络控制中心请求认证入网，其具体的认证入网流程如图 2 所示。

(1) CH_j 在获取到 *NC* 的公钥 PuK_{NC} 后，将初始对称密钥 key_{ic}、*IEEE* 地址 (Ad)、配置信息（初始配置时间 T_{date} 和网络 *PAN ID* ）加密发送给 *NC*，$C = En^{ECC}_{PuK_{NC}}(key_{ic} \| Ad \| T_{data} \| PAN.ID)$。

(2) *NC* 计算 $De^{ECC}k(C)$ 得到 key_{ic}、Ad、T_{data}、*PAN ID* 后生成索引编号 $index(i)$ 及生存期 T_i，将该索引项信息存入控制中心合法节点库中。*NC* 构造 $m = \{index(i), Sig^{ECC}_{NC}(index(i)), T_i\}$，将 $En_{key_{ic}}(m)$ 发送给 CH_j。

(3) *NC* 生成初始网络新鲜因子 D，并将含有该随机数的信标帧 M 以周期 T_0 广播发送到各节点。

(4) CH_j 接收到 *NC* 发送的包含有新鲜因子 D 的信标帧后，利用单向函数变换得到自身硬件信息因子 H 并保存。

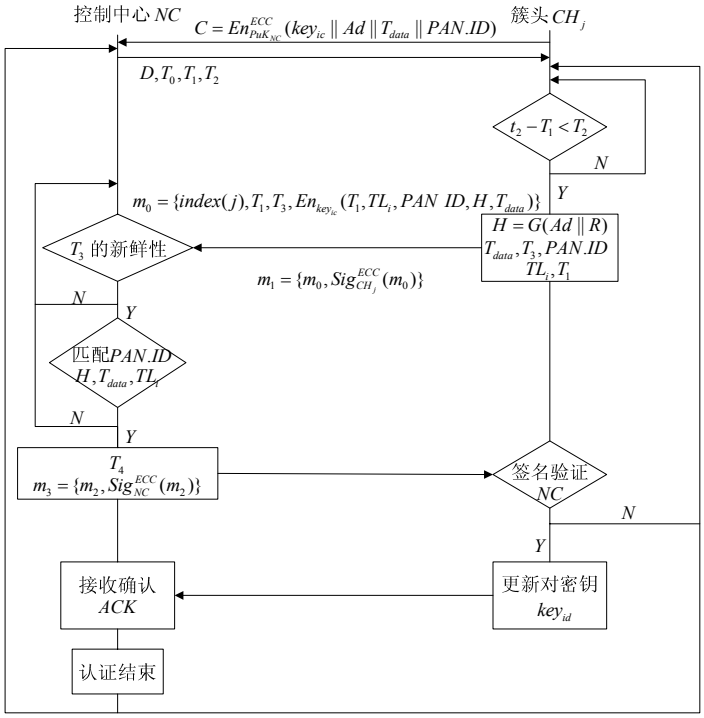

图 2 簇头与控制中心的认证流程

(5) CH_j 获取当前的时间戳 T_3，构造消息 $m_0 = \{index(j), T_1, T_3, En_{key_{ic}}(T_1, TL_i, PAN\ ID, H, T_{data})\}$，向 NC 发送申请入网帧，其中包含消息 $m_1 = \{m_0, Sig^{ECC}_{CH_j}(m_0)\}$。

(6) NC 接收到消息 m_1，检测 T_3 是否新鲜，检测通过后验证签名的有效性，查找索引项 $index(j)$，利用当前的新鲜因子 D 计算硬件信息因子 H 并提取 TL_i、T_{data} 与消息 m_1 中的字段匹配，匹配成功时 NC 获取当前时间戳 T_4 并构造消息 $m_2 = \{En^{ECC}_{PuK}(key_{ic}), En_{key_{ic}}(\{T_1, key_{id}\}), T_2\}$，向 CH_j 发送消息 $m_3 = \{m_2, Sig^{ECC}_{NC}(m_2)\}$。

(7) CH_j 提取 m_3 的签名验证字段，当验证通过时，检测 T_3，T_4 的合理性，确定 m_2 来自于 NC，更新两者之间的对密钥 key_{id}，完成 CH_j 与 NC 的双向认证。

1.2.2 簇头(CH_j)与终端节点(ED_i)双向认证

由于认证过程是个签名验证以及匹配的过程，计算量较大。因此，在簇头与终端节点的双向认证中，终端节点的认证需要由簇头做媒介最终由网络控制中心完成认证过程，其具体的认证流程如图 3 所示。(1) ED_i 在获取到 NC 的公钥 PuK_{NC} 后，将初始对称密钥 key_{ic}、$IEEE$ 地址 (Ad)、配置信息(初始配置时间 T_{date} 和网络 $PAN\ ID$)加密发送给 NC，$C = En^{ECC}_{PuK_{NC}}(key_{i0} \| Ad \| T_{data} \| PAN.ID)$。

(2) NC 计算 $De^{ECC}k(C)$ 得到 key_{i0}，Ad，T_{data}，$PAN\ ID$ 后生成索引编号 $index(i)$ 及生存期 T_i，将该索引项信息存入控制中心合法节点库中。NC 构造消息 $m = \{index(i), Sig^{ECC}_{NC}(index(i)), T_i\}$，将 $En_{key_{i0}}(m)$ 发送给 ED_i。

(3) NC 生成初始网络新鲜因子 D，并将含有该随机数的信标帧 M 以周期 T_0 广播发送到各节点。

(4) ED_i 接收到 NC 发送的包含有当前新鲜因子 D 的信标帧后，利用变换 $H = G(Ad, R)$ 得到自身硬件信息因子 H 并保存。

(5) ED_i 获取当前时间戳 T_1，构造消息 $m_0 = \{index(i), T_1, T_3, En_{key_{i0}}(T_1, TL_i, PAN\ ID, H, T_{data})\}$ 发送给 CH_i。CH_i 收到 m_0 后验证签名和 T_1 的新鲜性，获取时间戳 T_3 验证通过后构造 $m_1 = \{index(i), H, T_1, T_4, En_{key_{i0}}(T_1, TL_i, PAN\ ID, H, T_{data})\}$，向 NC 发送 $m_2 = \{m_1, Sig^{ECC}_{CH_i}(m_1)\}$。

(6) NC 收到 m_2 后，验证 CH_i 的签名，有效后

第 27 卷第 4 期 系统仿真学报 Vol. 27 No. 4
2015 年 4 月 Journal of System Simulation Apr., 2015

查找 $index(i)$，与接收消息中的 H 、TL_i 、T_{data} 匹配，当匹配失败时删除非法节点，匹配成功时检验 T_1 、T_4 的合理性，通过后生成成功标志位 Y。

(7) 当上述检测通过后获取时间戳 T_5，随机选取 key_{i1} 作为 ED_i 的临时密钥，添加标志位构造 $m_3=\{Y,En^{ECC}_{PuK_{CH_i}}(key_{i1}),T_5,En_{key_{i0}}(\{T_1,key_{i1}\})\}$ ，向 CH_i 发送 $m_4=\{m_3,Sig^{ECC}_{NC}(m_3)\}$。

(8) CH_i 验证 NC 的签名，签名验证通过后检测 T_1, T_2, T_3, T_4, T_5 的合理性，CH_i 从消息 m_4 中获取临时密钥 key_{i1} ，然后构造消息 $m_4=En_{key_{i0}}(\{T_1,key_{i1}\})$ 发送给终端 ED_i。

(9) 终端 ED_i 接收到消息后解析验证 T_1 是否正确且整个过程是否在合理的延时范围之内，若验证通过则确认 CH_i 是可以信任的合法簇头，终端 ED_i 与簇头节点 CH_i 建立安全的对称密钥 key_{i1}。

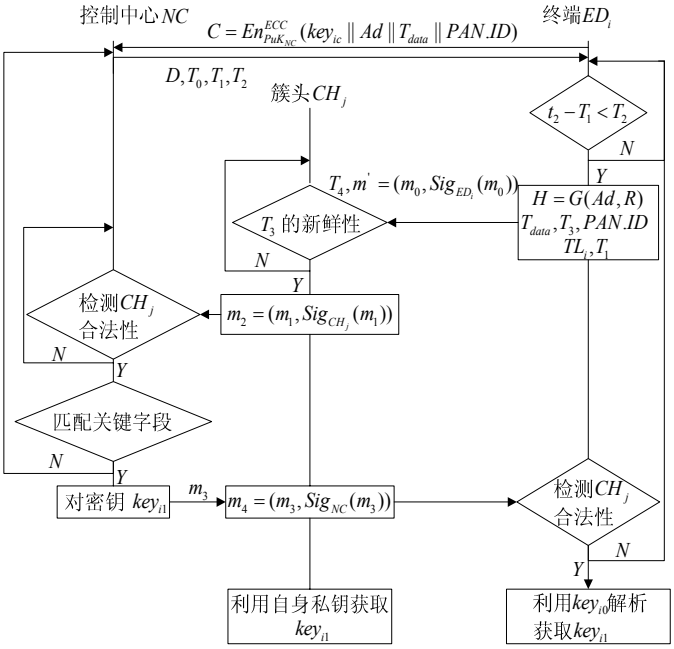

图 3 簇头与终端的认证流程

2 安全性证明与分析

本方案采取 BAN 逻辑方法对其安全性进行证明与分析。利用 BAN 逻辑对方案假设分析，其中 C 代表控制中心，R 代表簇头节点，E 代表终端节点，T 代表三者之间的通信规则，D 代表控制中心产生的随机数，H_E 为硬件地址替代标识，H_R 为簇头节点地址标识，S 为中心反馈的节点敏感信息，K_i 为 C 与 R 的共享对密钥，K 为 C 与 E 的共享对密钥，P 为 C 与 R 共享的秘密认证信息，Q 为 C 与 E 共享的秘密认证信息。

1. 方案中的初始假设集合(见表 2)：

表 2 多因子身份认证方案的初始假设集合

P1: $C\mid\equiv C\overset{K_i}{\leftrightarrow}R$	C 与 R 相信 K_i 为它们之间的通信密钥
P2: $C\mid\equiv C\overset{K}{\leftrightarrow}E$	C 与 E 相信 K 为它们之间的通信密钥
P3: $R\mid\equiv C\overset{K_i}{\leftrightarrow}R$	R 与 C 相信 K_i 为它们之间的通信密钥
P4: $E\mid\equiv C\overset{K}{\leftrightarrow}E$	E 与 C 相信 K 为它们之间的通信密钥
P5: $C\mid\equiv C\overset{P}{\rightleftarrows}R$	C 与 R 相信 P 为它们之间的共享秘密
P6: $R\mid\equiv C\overset{P}{\rightleftarrows}R$	R 与 C 相信 P 为它们之间的共享秘密
P7: $C\mid\equiv\#(D)$	C 相信它所发送的 D 是新鲜的
P8: $C\mid\equiv C\overset{Q}{\rightleftarrows}E$	C 与 E 相信 Q 为它们之间的共享秘密
P9: $E\mid\equiv\#(H_E)$	E 相信它所发送的 H_E 是新鲜的
P10: $E\mid\equiv C\overset{Q}{\rightleftarrows}E$	E 与 C 相信 Q 为它们之间的共享秘密
P11: $R\mid\equiv\#(H_R)$	R 相信它所发送的 H_R 是新鲜的
P12: $C\mid\Rightarrow(H_E)$	C 对 H_E 有管辖权
P13: $E\mid\equiv\#(S)$	E 相信 S 是新鲜的

2. 协议达到的预期目标：

(1) $C|\equiv R|\sim \#(H_R)$

(2) $C|\equiv E|\sim \#(H_E)$

(3) $R|\equiv C|\Rightarrow (S)$

(4) $E|\equiv R|\sim \#(S)$

3. 理想化模型：

M_1: $R\rightarrow C: P,\{Ad\}_{K_i}$

M_2: $E\rightarrow C: Query,Q$

M_3: $E\rightarrow R: \{Q\|H_E\}_K$

M_4: $R\rightarrow C: P,\{Q\|\{Q\|H_E\}_K\}_{K_i}$

M_5: $C\rightarrow R: \{K\|S\}_{K_i}$

M_6: $R\rightarrow E: \{S\}_K$

4. 认证协议 BAN 逻辑语言化

M1: $C\lhd P,\{Ad\}_{K_i}$

M3: $R\lhd \{Q\|H_E\}_K$

M4: $C\lhd P,\{Q\|\{Q\|H_E\}_K\}_{K_i}$

M5: $R\lhd \{K\|S\}_{K_i}$

M6: $E\lhd \{S\}_K$

5. 认证协议的 BAN 逻辑证明

① 证明：$C|\equiv R|\sim \#(H_R)$

由初始假设 $R|\equiv \#(H_R)$ 及推理规则 $\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$ 可得：$\frac{R|\equiv \#(H_R)}{R|\equiv \#(P,\{H_R\}_{K_i})}$，推出 $R|\equiv \#(P,\{H_R\}_{K_i})$。

又因为 $C|\equiv C\overset{K_i}{\leftrightarrow}R$ 且由 $C\lhd P,\{H_R\}_{K_i}$，结合推理规则 $\frac{(P|\equiv Q\overset{K}{\leftrightarrow}P,P\lhd \{X\}_K)}{P|\equiv Q\sim X}$ 与信仰规则 $P|\equiv Q|\sim (X,Y)\rightarrow P|\equiv Q\sim X$ 推出：$C|\equiv R|\sim \#(H_R)$。预期目标得到证明。

② 证明：$C|\equiv E|\sim \#(H_E)$

由初始假设 $C|\equiv \#(D)$ 及推理规则 $\frac{P|\equiv \#(X)}{P|\equiv \#(X,Y)}$ 得：$\frac{C|\equiv \#(D)}{C|\equiv \#(D,\{D\|H_E\}_K)}$，推出 $C|\equiv \#(D,\{D\|H_E\}_K)$。

又因为 $C|\equiv C\overset{K}{\leftrightarrow}E$，结合推理规则 $\frac{(P|\equiv Q\overset{K}{\leftrightarrow}P,P\lhd \{X\}_K)}{P|\equiv Q\sim X}$、理想化模型 $C|\equiv E|\sim (H_E)$；又由 $E|\equiv \#(H_E)$，推出 $C|\equiv R|\sim \#(H_R)$。

③ 证明：$R|\equiv C|\Rightarrow \#(S)$

理想化模型 $R\lhd \{Q\|H_E\}_K$，因 R 不知道 C 与 E 所共享的 K；所以 R 不能理解所收到的加密后的内容，只能用自己与 C 共享的密钥 K_i 再次加密接收到的信息后转发给 C，即：$C\lhd P,\{Q\|\{Q\|H_E\}_K\}_{K_i}$。

又因为 $C|\equiv C\overset{K}{\leftrightarrow}E$，结合推理规则 $\frac{(P|\equiv Q\overset{K}{\leftrightarrow}P,P\lhd \{X\}_K)}{P|\equiv Q\sim X}$ 与信仰规则 $P|\equiv Q|\sim (X,Y)\rightarrow P|\equiv Q\sim X$，可得：$C|\equiv E|\sim (H_E)$。

由 $C|\equiv E|\sim (H_E)$，则 $C|\equiv E|\Rightarrow (H_E)$，因而 C 向 R 发送消息，其消息模型为 $C\rightarrow R:\{K\|S\}_{K_i}$，BAN 逻辑语言化即为 $R\lhd \{K\|S\}_{K_i}$。

由 $R|\equiv C\overset{K_i}{\leftrightarrow}R$ 及推理规则 $\frac{(P|\equiv Q\overset{K}{\leftrightarrow}P,P\lhd \{X\}_K)}{P|\equiv Q\sim X}$，得到：$R|\equiv C|\sim S$。

由 $R|\equiv C|\sim S$ 且 $R|\equiv C$、$C|\equiv R$、$C|\Rightarrow S$ 推出：$R|\equiv C|\Rightarrow \#(S)$。

④ 证明：$E|\equiv R|\sim \#(S)$

同上述证明过程，结合 $R|\equiv C|\Rightarrow (S)$、理想化模型 $R\rightarrow E:\{S\}_K$、$E|\equiv C\overset{K}{\leftrightarrow}E$ 以及推理规则 $\frac{(P|\equiv Q\overset{K}{\leftrightarrow}P,P\lhd \{X\}_K)}{P|\equiv Q\sim X}$ 得到：$E|\equiv C|\sim S$。

由秘密共享规则 $P|\equiv R\overset{X}{\rightleftarrows}R_1\rightarrow P|\equiv R_1\overset{X}{\rightleftarrows}R$ 可得：$E|\equiv C\overset{K_i}{\rightleftarrows}R\rightarrow E|\equiv R\overset{K_i}{\rightleftarrows}C$。

又因为 $R\rightarrow E:\{S\}_K$，所以可得：$E|\equiv R|\sim (S)$。

由初始假设 $E|\equiv \#(S)$ 以及 E 对接收到的 S 进行比对，因此，$E|\equiv R|\sim \#(S)$。

上述的分析和证明过程充分说明了该协议是安全的，也是合理的。

3 实验及结果分析

为验证本文设计的身份认证方案性能，采用自行设计的 ZigBee 硬件开发平台，将嵌入多因子身份认证的固件下载到 CC2530 芯片。系统包括 ZigBee 协调器 1 个，ZigBee 路由器 12 个(其中包

第 27 卷第 4 期 系统仿真学报 Vol. 27 No. 4
2015 年 4 月 Journal of System Simulation Apr., 2015

含 6 个非法路由节点)，ZigBee 终端 35 个(其中包含 15 个未注册的非法终端节点)。协调器与控制中心相连构成 NC，路由器节点为 CH_j，终端节点为 ED_i。

3.1 方案安全性测试

在实验室的环境下，对协调器配置完成后，向下提供入网认证前的注册服务。当合法的 CH_j 和 ED_i 都成功注册完成后，通过控制变化含有不同认证因子的非法节点请求入网对整个网络系统的认证机制进行测试。各非法测试节点的配置如表 3 所示。

表 3 非法节点参数设置

$PANID$	T_{data}	Ad	key_{ic}	$\Pr K_i$	CH_j	ED_i
×	√	√	√	√	1	2
√	×	√	√	√	1	2
√	√	×	√	√	1	2
√	√	√	×	√	1	2
√	√	√	√	×	1	2
√	√	√	√	√	1	5

如上表所示，其中×表示该项为节点缺失的认证因子，即非法认证因子，√表示该项为合法认证因子。设置 15 个 CH_j 和 ED_i 的非法节点分别携带有不同的非法因子，同时有 6 个非法节点拥有全部合法的认证因子，但不具有生成合法 H 的单向杂凑函数 G。将这 21 个测试节点上电请求加入当前的 ZigBee 网络当中，实验结果为 21 个测试节点在请求入网时全部被 NC 成功检测并删除。

通过 SmartRF Packet Sniffer 数据帧捕获工具分析全网中的帧应答机制后发现，当合法 ED_i 由非法 CH_j 转发请求入网认证时，NC 删除非法 CH_j 拒绝其入网，该合法 ED_i 最终通过合法 CH_j 成功入网，有效抵御了节点的中间人攻击。

以上测试结果表明，“密钥+硬件信息+配置信息”的认证方案在所有关键认证信息都泄露的情况下仍能检测并删除非法路由和终端节点，可同时抵御中间人攻击和假冒攻击，具有较高的安全强度。

3.2 方案效率分析

假设 ZigBee 网络中共有 N 个簇头节点，每个簇头节点平均拥有 M 个终端节点，记号 $o(1)$ 表示一个当 $N \to \infty$ 时趋向于 0 的函数，p 表示 N 的最小素因子。由于 1024 位的 RSA 算法与 160 位的 ECC 算法的安全性相当[7]，以下计算开销的对比中 TinyPK 采用 RSA 算法，密钥长度为 1024 bit，本方案采用 ECC 算法，密钥长度为 160 bit。

(1) 存储开销

本方案中 ED_i 需要存储一个与 NC 共享的对称密钥 key_{i0}、自身的私钥 $\Pr K_{ED_n}$ 以及 NC 的公钥 PuK_{NC}。由于 ECC 密钥长度为 20 Byte，设对称密钥的长度为 m，则 ED_i 的存储开销为 $(m+40)$ Byte。CH_j 需要存储与 NC 共享的对称密钥 key_{ic}、ED_i 的公钥 PuK_{ED_n}、自身私钥 $\Pr K_{CH_n}$ 以及 NC 的公钥 PuK_{NC}，则其存储开销为 $(m+20M+40)$ Byte。

(2) 通信开销

本方案中通信开销的计算以各通信节点收发数据报文的数量来表示。CH_j 在请求认证过程中收发数据报文各 2 次，在 ED_i 请求认证中收发各 2 次，每个 CH_j 平均有 M 个待认证 ED_i，其通信开销为自身及 ED_i 认证中收发报文的总量。因此，其通信开销为 $4M+4$，单个 ED_i 的通信开销为 3。

(3) 计算开销

在节点认证过程中，设 E 是有限域 F 上的椭圆曲线，G 是 E 的一个循环子群，a 是 G 的一个生成元，则其计算复杂度为 $0.88\sqrt{ord(a)}$ [11]，其中 $ord(a)$ 表示 a 的阶。对于对称加解密算法，用节点需要进行加解密运算次数来表示计算开销。CH_j 和 ED_i 请求认证过程中均分别采用了 2 次 ECC 算法和 2 次对称密码算法，ED_i 请求认证过程中 CH_j 调用 2 次 ECC 算法，因此，CH_j 计算开销为 $1.76(M+1)\sqrt{ord(a)}+2$，ED_i 计算开销为 $1.76\sqrt{ord(a)}+2$。

表 4 和表 5 是本方案与文献[6]、文献[7]的开销对比。由表可知，本文的存储开销和通信开销明显比文献[7]小，且计算开销也优于文献[6]，文献[7]虽然在各方面的开销较小，但其采用对称密码

算法安全性差、认证成功率低、可扩展性差，而本文所采用的方案具有较高的安全性，可同时抵御中间人攻击和假冒攻击。

表 4 本方案开销情况

	本文	
	CH_i	ED_i
存储开销	$(m+20M+40)$ Byte	$(m+40)$ Byte
通信开销	$4M+4$	3
计算开销	$1.76(M+1)\sqrt{ord(a)}+2$ (公钥+对称密码运算)	$1.76\sqrt{ord(a)}+2$ (公钥+对称密码运算)

表 5 其它方案开销情况

	文献[6]	文献[7]
存储开销	$o(128M)$	m
通信开销	$o\left(MN^{\frac{1}{2}}\right)$	2
计算开销	$o\left(e^{(1+o(1))\sqrt{2\ln p \ln\ln p}}\right)$ （公钥密码运算）	M 次 NM 元多项式运算(对称密码运算)

4 结论

本文在深入研究无线传感器网络(WSNs)节点身份认证机制和 ZigBee 协议栈的基础上，提出了一种“密钥+硬件信息+配置信息”的多因子身份认证方案，相比于传统的 WSNs 身份认证方案，本方案引入了多因子认证机制，在几乎不增加原有协议开销的基础上，提升了 ZigBee 网络通信的安全性，有效解决了 ZigBee 网络中的中间人攻击和假冒攻击问题，保证了 ZigBee 网络在实际应用中的安全，适合于安全性要求较高的应用场合。

参考文献：

[1] Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks [J]. Communications of the ACM.ISSN: (S1617-7975), 2004, 47(6): 53-57.

[2] Bankovic Z, Fraga D, José M, *et al*. Detecting and confining sybil attack in wireless sensor networks based on reputation systems coupled with self-organizing maps [C]// IFIP Advances in Information and Communication Technology. NanChang,China: Springer, 2010: 311-318.

[3] Roszainiza Rosli, Yusnani Mohd Yusoff, Habibah Hashim. Performance Analysis of ID-Based Authentication on Zigbee Transceiver [C]// 2012 IEEE Symposium on Wireless Technology and Applications, Bandung, Indonesia, 2012. USA: IEEE, 2012.

[4] S Weis. Security and Privacy in Radio Frequency Identification Device [D]. Cambridge, MA, USA: MIT, 2003.

[5] Weis S A, Sarma S E, Rivest R L. Security and Privacy Aspects of Low-cost Radio Frequency Identification System [C]// Proceedings of the 1st International Conference on Security in Pervasive Computing. Berlin, Germany: Springer-Verlag, 2004: 201-212.

[6] Watro R, Kong D, Cuti S, *et al*. TinyPK: Securing sensor networks with public technology [C]// Proceedings of the 2nd ACM Workshop on Security of Ad Hoc Networks and Sensor Networks. Washington DC, USA: ACM, 2004: 59-64.

[7] 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, New York, USA. USA: ACM, 2002: 41-47.

[8] Zinaida Benenson, Nils Gedicke, Ossi Raivio. Realizing Robust User Authentication in Sensor Networks [C]// Workshop on Real World Wireless Sensor Networks (REALWSN). Italy: Springer,2005: 135-142.

[9] K Bauer, H Yunyoung Lee. A Distributed Authentication Scheme for a Wireless Sensing System [C]// Proceedings of the 2nd International Workshop on Networked Sensing Systems (INSS 2005). Japan: IEEE, 2005: 210-215.

[10] Wei Chen, Xiaoshuan Zhang, Dong Tian, Zetian Fu. An Identity-Based Authentication Protocol for Clustered ZigBee Network [C]// 6th International Conference on Intelligent Computing. Changsha, China: Springer, 2010: 503-510.

[11] 金晨辉, 郑浩然, 张少武, 等. 密码学 [M]. 北京: 高等教育出版社, 2009, 11.