文章编号:1007-5321(2018)02-0021-06 DOI:10.13190/j.jbupt.2017-193

一种分簇无线传感网轻量级匿名认证及密钥协商方案

石乐义[1,2], 崔玉文[1], 付文静[1], 陈鸿龙[3]
(1. 中国石油大学(华东) 计算机与通信工程学院, 山东 青岛 266580;
2. 上海财经大学 上海市金融信息技术研究重点实验室, 上海 200433;
3. 中国石油大学(华东) 信息与控制工程学院, 山东 青岛 266580)

摘要: 针对分簇无线传感网中的节点认证问题,使用轻量级的哈希函数和异或运算,设计了一种节点认证及密钥协商方案,将匿名机制引入节点认证过程中,保护了节点隐私安全,提高了网络抵御流量分析攻击的能力. 对认证方案抗攻击性能和资源开销的对比分析结果表明,提出的方案可以提供良好的安全认证,并具有较低的计算、存储和通信开销.

关 键 词: 分簇无线传感网; 认证; 密钥协商; 匿名
中图分类号: TN929.53 **文献标志码**: A

A Lightweight Anonymous Authentication and Key Negotiation Scheme for Clustered WSN

SHI Le-yi[1,2], CUI Yu-wen[1], FU Wen-jing[1], CHEN Hong-long[3]
(1. College of Computer and Communication Engineering, China University of Petroleum (East China), Shandong Qingdao 266580, China;
2. Shanghai Key Laboratory of Financial Information Technology, Shanghai University of Finance and Economics, Shanghai 200433, China;
3. College of Information and Control Engineering, China University of Petroleum (East China), Shandong Qingdao 266580, China)

Abstract: Focusing on the nodes authentication problem of clustered wireless sensor network, the paper proposes a lightweight authentication and key negotiation scheme using hash function and exclusive or (XOR) operation. The anonymity mechanism is introduced into the authentication process, which can thwart the traffic analysis attacks, and protect the privacy of nodes. In addition, by analyzing and comparing the anti-attack performance and the resource overhead of the authentication scheme, the results show that the proposed scheme can provide good authentication and also have a lower overhead at the cost of computation, storage and communication.

Key words: clustered wireless sensor network; authentication; key negotiation; anonymity

无线传感网(WSN, wireless sensor network)由数量众多的传感器节点构成,具有自组织、拓扑动态变化等特点. 分簇无线传感网则是具有簇结构的无线传感网,是当前无线传感网应用中普遍采用的结构. 通过对分簇无线传感网节点认证过程进行研究,提出了一种轻量级节点认证和密钥协商方案. 方案采用哈希函数和 XOR 异或运算,具有计算、存储和通信开销较小的优点;在节点认证中引入匿名机制,有效保护了节点隐私,并能够抵御流量分析攻击.

1 相关工作

Perrig A 等[1]提出了一种传感网络安全协议.

收稿日期: 2017-09-20
基金项目: 国家自然科学基金项目(61772551); 上海市金融信息重点实验室开放课题
作者简介: 石乐义(1975—), 男, 教授, E-mail: shileyi@upc.edu.cn.

该协议包括 SNEP(secure network encryption protocol)和 μTESLA(the micro version of the timed, efficient, streaming, loss-tolerant authentication protocol)协议,该协议将基站视为可信任第三方,负责所有节点初始密钥的分配. 但该安全协议扩展性不强,并且没有考虑节点隐私保护. 针对 WSN 存在的节点隐私泄露问题,Katiyar 等[2]提出了 RSA 算法和生物识别技术 2 种解决方案. 2 种方案都基于密码学进行身份的验证以及节点隐私的保护,为传感器节点的通信过程提供了较高的安全性. 但这 2 种方案对传感器节点的计算能力、存储量、带宽以及电量需求量较大,进而造成传感器节点体积过于臃肿、成本开销过大.

Peris-Lopez[3]证明了公钥技术可以在 WSN 中实现用户认证,但它同样带来了计算开销过大的问题. 此后,有学者提出了以椭圆曲线(ECC, elliptic curve crypto system)为基础的认证协议[4],并且在能耗方面比原始公钥加密技术更有优势. 张敏[5]针对公钥密码认证体制攻击问题,结合 Shamir 减扰动方法,提出一种基于轻量级彩虹签名的无线传感网认证方法. 该方法可以有效抵御油醋分离攻击、最小秩攻击、秩约减攻击,并且效率较高. 此外,还提出了基于口令和智能卡的 WSN 匿名认证机制,将匿名认证过程分为认证和口令更新等 4 个阶段,但由于采用了模指数运算,所以系统计算开销较大.

Turkanovic 等[6]提出了异构的无线传感网络(HWSN, hierarchical wireless sensor networks)方案,通过哈希和 XOR 计算实现了用户认证和密钥协商方案(UAKAS, user authentication and key agreement scheme). 用户可以通过 HWSN 方案在不与网关节点通信的状况下与特定的传感器节点进行认证. Farash 等[7]针对文献[6]中用户认证方案存在的节点隐私泄露、密码攻击等一系列安全问题提出了改进的 HWSN 方案,该方案在功能实现上与文献[6]相同,但修复了文献[6]存在的安全问题,提高了安全级别.

范修伟等[8]提出了一个轻量级的密钥协商算法认证方案,使用单向哈希函数和对称加密技术完成节点的认证和密钥会话过程的建立. 这与笔者的工作相似,但该方案在传感器网络节点认证过程中并没有进行角色区分,也没有进行匿名处理. 与笔者研究最相关的工作是 Abduvaliev 等[9]提出的基于共享秘密的哈希函数消息认证方案. 该方案采用伪随机数和改进的 SHA-1 安全哈希算法来计算消息认证码,并不具有匿名保护特性,并且资源开销较大.

2 本文方案

2.1 网络模型

分簇无线传感网结构如图 1 所示. 首先对分簇无线传感网模型进行如下假设:

1) 分簇无线传感网中,每个传感器节点和簇头节点都在基站注册身份唯一标识 ID,簇内节点将消息直接发送给簇头节点,簇头节点负责将收集到的簇内各节点的消息进行整合处理;

2) 簇头节点之间可以进行通信,距离基站较远的簇头节点可以经过多跳将消息发送到基站;

3) 传感器节点拥有一个预分配的密钥 K,在基站中该密钥根据传感器节点的身份唯一标识 ID 进行匹配,不同的传感器节点密钥 K 不同. 簇头节点与传感器节点类似,也拥有一个预分配的密钥 K_c 和身份唯一标识 ID_c,不同的簇头节点密钥 K_c 不同;

4) 基站和传感器节点都可以执行哈希函数操作:h 和 f.

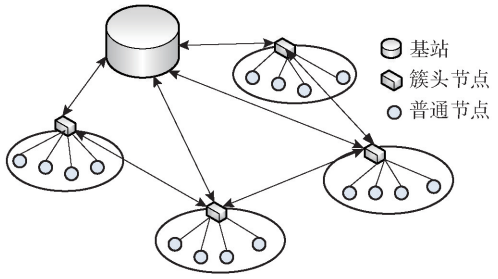

图 1 分簇无线传感网结构图

2.2 方案及符号说明

新方案以单向哈希函数和 XOR 异或操作为基础,为进一步提高节点的匿名保护力度,在认证过程中引入了匿名机制:当节点加入某个簇后,簇头会为该节点分配一个虚假的 ID 用来代替其在通信过程中的真实 ID. 在簇头认证其簇内节点过程中,同样使用虚假 ID 代替其真实 ID. 这样,既可以实现节点的认证,又可以达到保护节点隐私的目的,因此本文算法可以实现匿名认证的目的.

方案包含 2 个阶段:网络初始化时节点的认证阶段和网络稳定运行时节点的认证阶段. 对过程中应用到的符号进行说明,如表 1 所示.

表 1　符号说明

符号	含义
i	第 i 个簇内成员节点
h	用来计算认证消息的哈希函数
f	用来计算会话密钥的哈希函数
r	节点在认证过程中使用的随机数
ID	节点的身份标识
K	基站用来认证节点时使用的密钥
ID_c	簇头节点的身份标识
K_c	基站用来认证簇头节点时使用的密钥
Ken	簇头节点和其簇内节点的会话密钥
fake_id	簇内成员节点的虚假身份标识

2.3　初始化认证阶段

步骤 1　如果节点 i 想要加入到某个簇中，它首先要向选定的簇头节点发送认证请求.

首先根据哈希函数 f、h、随机数 r_i、节点 ID_i 计算 $M_i = K_i(h(\mathrm{ID}_i \parallel \mathrm{ID}_{ci}) \oplus r_i)$，$S_i = h(\mathrm{ID}_i \parallel \mathrm{ID}_{ci})$ 然后将消息 $\{M_i, \mathrm{ID}_i, r_i\}$ 发送给选定的簇头节点；

步骤 2　簇头节点收到节点发来的请求消息后使用自身的密钥 K_{ci} 对 M_i 加密，将加密后的消息 $M_{ci} = K_{ci}(M_i \parallel S_i)$，$S_i = h(\mathrm{ID}_i \parallel \mathrm{ID}_{ci})$ 以及自身 ID_{ci}、传感器节点随机数 r_i、传感器节点的源消息 M_i 发送给基站：$\{M_{ci}, M_i, \mathrm{ID}_i, r_i, \mathrm{ID}_{ci}\}$；

步骤 3　当基站收到该消息后，首先通过簇头节点 ID_{ci} 确认节点使用的加密密钥 K_{ci}，然后解密出消息 M'_{ci}，之后使用 $S_i = h(\mathrm{ID}_i \parallel \mathrm{ID}_{ci})$ 与 M_i 验证簇头节点的 ID_{ci} 是否合法，并验证源信息 M_i 的完整性. 如果簇头节点合法，则执行步骤 4，否则将该消息丢弃；

步骤 4　基站首先通过节点 ID_i 确认节点使用的加密密钥 K_i，然后解密出消息 M'_i 并将 M'_i 与 r_i 进行异或运算，得到值 S'，将 S' 与 S 进行比较，如果结果相同，则认为节点合法. 基站将向簇头发送节点 i 认证成功的消息. 如果节点认证失败，基站将发送一个消息告知簇头节点 i 不合法；

步骤 5　簇头节点收到基站发送的消息后，如果节点 i 不合法，簇头节点丢弃该消息并且拒绝 i 加入簇内；反之，如果节点 i 认证成功，簇头节点允许 i 加入簇，并且计算会话密钥 $\mathrm{Ken}_i = f(r_i \parallel \mathrm{ID}_i \parallel \mathrm{ID}_{ci})$. 同时为节点 i 分配假名 $\mathrm{fake\_id}_i$，并在之后的通信过程中使用该 $\mathrm{fake\_id}_i$ 代替其真实 ID_i. 然后，簇头节点向节点 i 发送消息 $\{M\}$，其中 $M = \mathrm{Ken}_i(\mathrm{ID}_i \oplus \mathrm{fake\_id}_i)$；

步骤 6　当节点 i 收到消息 M 后，首先计算会话密钥 $\mathrm{Ken}'_i = f(r_i \parallel \mathrm{ID}_i \parallel \mathrm{ID}_{ci})$，然后使用该密钥解密出消息 M，并且将结果与 ID_i 进行异或运算，即可得到假名 $\mathrm{fake\_id}_i$，在之后的通信过程中，节点使用 fake_id 代替数据包中的真实 ID.

2.4　稳定状态认证阶段

为了避免节点由于能量耗完或其他原因导致不可用情况的发生，簇头节点必须定期对成员节点进行认证. 也就是在网络稳定运行阶段簇头节点要定期对簇内节点进行认证. 这个认证过程按照如下步骤进行：

步骤 1　簇头节点在簇内广播认证请求消息；

步骤 2　簇内节点 i 收到簇头节点的认证广播请求消息后，首先计算消息 $S_m = h(r_m \parallel \mathrm{ID}_{ci})$，然后产生一个随机数 r_m，并且使用会话密钥 Ken_m 计算消息 $M_m = \mathrm{Ken}_m(h(r_m \parallel \mathrm{ID}_{ci}) \oplus \mathrm{fake\_id}_m)$. 之后，节点 i 将认证消息 $\{M_m, S_m, r_m\}$ 发送给簇头节点；

步骤 3　当簇头节点收到节点 i 发送的认证消息后，首先计算当前二者使用的会话密钥 $\mathrm{Ken}_m = f(r_m \parallel \mathrm{ID}_i \parallel \mathrm{ID}_{ci})$，然后用该密钥解密出消息 M'_m，将 M'_m 与 S_m 进行异或运算，则得到假名 $\mathrm{fake\_id}'_m$. 簇头节点对 $\mathrm{fake\_id}'_m$ 进行验证，如果与簇头节点存储的节点 i 的假名 $\mathrm{fake\_id}_m$ 一致，则节点 i 认证成功，否则节点 i 认证失败；

步骤 4　节点 i 认证成功后，簇头节点为 i 分配一个新的假名 $\mathrm{fake\_id}_{m+1}$，新的随机数 r_{m+1}，然后计算出新的密钥 $\mathrm{Ken}_{m+1} = f(r_{m+1} \parallel \mathrm{ID}_i \parallel \mathrm{ID}_{ci})$ 以及消息 $M_{m+1} = \mathrm{Ken}_{m+1}(h(r_{m+1} \parallel \mathrm{ID}_{ci}) \oplus \mathrm{fake\_id}_{m+1})$，最后簇头节点将 $\{M_{m+1}, r_{m+1}\}$ 发送给节点 i；

步骤 5　当节点 i 收到簇头节点发送的消息后，首先计算密钥 $\mathrm{Ken}'_{m+1} = f(r_{m+1} \parallel \mathrm{ID}_i \parallel \mathrm{ID}_{ci})$ 和哈希值 $h'(r_{m+1} \parallel \mathrm{ID}_{ci})$. 使用该密钥解密出消息 M'_{m+1}，则得到的结果是 $S'_m = h(r_{m+1} \parallel \mathrm{ID}_{ci}) \oplus \mathrm{fake\_id}_{m+1}$，最后将 S'_m 与 h' 进行异或运算即可反向得到新的假名 $\mathrm{fake\_id}_{m+1}$. 节点更新自身的假名与随机数. 如此一次新的匿名认证过程完成，新的会话密钥及新的假名都已建立.

3　方案分析

下面给出本文方案的安全性和性能开销的详细对比和分析.

3.1 安全性分析

1）窃听攻击. 在本文方案中,不同的时间不同的认证消息由于随机数 r 不同,可使用不同的会话密钥 Ken 进行加密. 此外,传感器节点的假名 fake_id$_{m+1}$在不同的时间也不相同. 因此即使攻击者可以执行流量分析,也无法获取消息内容.

2）拒绝服务攻击（DoS, denial of service）攻击. 在本文方案中,基站只在初始化阶段负责认证过程. 这有助于降低 DoS 攻击的破坏性. 另外,为了抵御针对簇内节点的 DoS 攻击,当节点不发送消息时,节点处于休眠状态.

3）重放攻击. 在提出的认证方案中,传感器节点拥有一个预分配的密钥 K. 在基站中该密钥根据传感器节点的身份唯一标识 ID 进行匹配,不同的传感器节点密钥 K 不同. 簇头节点与传感器节点类似,也拥有一个预分配的密钥 K_c 和身份唯一标识 ID$_c$. 基站可以通过传感器节点 ID 和簇头节点 ID$_c$ 匹配的 K 和 K_c,比对相应的密钥还原消息后的节点身份信息,从而验证传感器节点以及簇头节点身份的可靠性. 此外每个认证过程都使用不同的随机数 r,节点也会通过检查该随机数 r 来检查是否遭受到了重放攻击,从而采取有效抵御措施.

4）节点捕获攻击. 由于无线传感器节点自身的特性,使得节点的捕获非常容易,因而节点捕获攻击是 WSN 中最具有威胁性的攻击. 本文方案中,网络中每个节点与簇头节点共享会话密钥并且不与其他节点通用,节点捕获后并不影响其他节点,因而可以将捕获攻击的损失降到最低.

5）流量分析攻击. 由于将假名机制引入到了认证通信过程,本文方案中节点之间的通信具有良好的匿名特性,因而可以有效抵御流量分析攻击.

不同认证方案抵抗攻击能力对比如表 2 所示.

表 2 不同认证方案抵抗攻击能力对比

攻击	μTESLA	文献[7]方案	文献[9]方案	本文方案
窃听攻击	√	√	√	√
DoS 攻击	×	√	×	√
重放攻击	√	√	√	√
节点捕获攻击	√	√	√	√
流量分析	×	×	×	√

表 2 示出了本文方案与 μTESLA、文献[7]方案以及文献[9]方案在抗攻击性能方面的对比. 可以看出,本文方案引入的匿名机制与其他方案相比,除了能够有效抵御窃听、重放、节点捕获等常见攻击,还可以降低 DOS 攻击造成的破坏性以及有效抵御流量分析攻击,这正是本文方案的优势所在.

3.2 性能分析

1）存储性能

每个簇内节点需要存储的信息:虚假 fake_id、3 个加密密钥(K, Ken, K_c)和一个随机数 r.

为了方便定量分析,在此假设随机数的长度为 64 位,ID 的长度为 14 位,哈希运算的结果是 160 位,加密密钥是 128 位,同时设定本方案中引入的虚假 ID 长度和真实 ID 长度一致是 14 位. 则普通节点 i 需要存储的信息量为 462 位,而簇头节点必须要为每个节点存储的信息是(ID, fake_id, r, Ken),因此簇头节点的存储信息量为 $n \times 220$ 位,n 代表区域内进行通信簇头节点的节点数.

在文献[7]中的方案中,每个普通节点在执行注册和验证阶段需要存储的信息量为 421 位. 此外,文献[7]中的方案在节点之间进行通信时,接收每个传感器网络节点的响应以及对响应的进行处理运算总共需要存储的信息量为 437 位. 文献[9]中,网络中每个节点均需要存储密钥、随机数、邻居节点的 ID 以及与每个邻居节点的会话密钥,本文方案假设节点 i 的邻居节点数为 N,则节点 i 需要存储的信息总量为:$N \times 334$.

本文算法的设定条件是分簇无线传感网,如上一节提到的网络模型中,节点只与簇头节点进行通信,而文献[7]与文献[9]方案的网络条件是节点之间相互通信. 为了各方案存储性能的有效对比,采用计算一个簇内需要存储的总数据量. 在此,假设一个簇内共有 N 个节点,1 个簇头节点,节点之间互为邻居节点. 在文献[7]的方案中,一个节点总共需要存储 421 + 437 = 858 位数据量,N 个节点共需要 $N \times 858$ 位数据量;对于文献[9]中的方案,每个节点需要存储 $N \times 334$ 位数据量,则共需存储 $(N+1) \times N \times 334$ 位信息量;本文方案中,簇头需要保存 $N \times 220$ 位数据量,每一个节点需要保存 462 位数据量, N 个节点则共需要存储 $N \times 682$ 位数据. 如表 3 所示.

表 3 存储数据开销对比

方案	比特数
文献[7]	$N \times 858$
文献[9]	$(N+1) \times N \times 334$
本文	$N \times 682$

经过对表 3 中的公式进行分析对比，可以得出：N 大于 1 时，本文算法需要存储的信息量比其他 2 种方案中要小的多，也就是说本文方案在存储空间消耗方面具有较大的优势.

2）计算效率

为了便于讨论，先对计算能耗进行统一的定义：假设 t_h 代表一次哈希计算所需的时间，t_E 表示一次加密或解密所需的时间，$t_{\oplus}$ 表示一次 XOR（异或运算）的所需要的时间，而 t_g 表示节点产生一个随机数的所需的时间. 在一次认证过程中，簇头节点以及簇内节点的计算过程为：哈希运算、密钥计算、消息加解密等操作. 簇头节点还需产生假名 ID 以及随机数等. 这样，本文方案可以计算在一次认证过程中，簇头节点及簇内节点分别所需要的计算量. 但是这些计算量与文献[9]中使用的公钥加密相比，计算量要小得多. 具体的计算过程不再详细说明，本文方案只把计算结果列在表 4 中. 由于文献[7]的方案只计算了认证过程的时间总开销，并且其认证过程的时间总开销明显大于本文方案的认证过程总开销，故在本节不再对文献[9]的时间开销进行对比讨论.

表 4　计算时间开销对比

文献[9]的方案		本文方案	
初始化阶段	新节点加入	初始化阶段	稳定阶段
$5t_h+2t_{\oplus}+4t_E+t_g$	$9t_h+2t_{\oplus}+4t_E+t_g$	$5t_h+3t_{\oplus}+4t_E+t_g$	$6t_h+4t_{\oplus}+4t_E+2t_g$

在表 4 的数据中，虽然文献[9]新节点加入的认证过程与本文方案稳定阶段的时间开销进行了对比讨论，但认证的过程其实质还是一样的，因此，本文稳定阶段与之计算开销的对比是有效的. 通过表 4 的对比可以看出，由于文献[9]中采用公钥加密方式，所提出方案的计算量比文献[9]中的方案要小.

3）通信成本

本文方案采用在认证过程中发送消息的总量来衡量通信成本. 假设方案中使用的参数长度定义与上文提到的一样. 文献[9]方案中，节点必须要对其周围的邻居节点全部进行认证，因此必须在邻居节点中广播认证消息. 而广播是通信成本较高的消息发送模式. 文献[7]提出的方案虽然也采用广播的方式对邻居节点传输认证消息，但广播认证消息的过程不再需要传感器节点与网关节点进行通信，进而提高了通信效率. 而在本文方案中，簇头节点负责簇内节点的认证，节点之间不需要相互认证，因此不存在相互之间广播或发送认证消息. 这会极大的减少能量消耗，因此本文方案具有较高的通信效率.

在本文设计的方案中，每一次认证过程需要传输 398 位数据，略低于文献[7]中方案中一次认证过程的数据总传输量. 而在文献[9]中，一次认证过程总共需要传输 718 位数据. 三者之间的对比如表 5 所示. 在 3 种方案的通信传输数据开销对比中，虽然网络模型与本文算法有所不同，但本文通信传输数据开销分析的条件是一次认证过程所需的时间成本以及通信传输的数据量，因此分析结果仍然有效.

表 5　通信传输数据开销对比

方案	比特数
文献[7]	434
文献[9]	718
本文	398

综上所述，本文的方案不仅能够保证节点认证的安全，更能大大节省网络能量，增加网络存活时间. 更重要的是，可以提供节点的匿名性和防御网络流量分析.

4　结束语

针对节点认证问题，提出了一种用于分簇无线传感网的轻量级认证及密钥协商方案. 方案基于轻量级的哈希运算和 XOR 异或运算，并将匿名机制引入到认证过程中，从而实现了既能进行节点认证，又能保证节点的隐私安全，提高 WSN 的抵御流量分析攻击的能力. 随后，对方案的算法过程进行了详细描述，并对方案的安全性及高效性进行了理论分析以及与其他相关方案性能的对比. 结果表明，本文方案可以提供良好的安全认证特性，并且具有较低的资源开销.

参考文献：

[1] Perrig A, Szewczyk R, Tygar J D, et al. SPINS: security protocols for sensor networks [J]. Wireless networks, 2002, 8(5): 521-534.

[2] Katiyar S, Rizwan S, Gujral R. Network security described technology based on RSA and biometrics for authenticity in WSN [J]. International Journal of Advanced Research in Computer Science and Software Engineering, 2016, 6(2): 328-333.

[3] Peris-Lopez P, Hernandez-Castro J C, Estevez-Tapiador J

M, et al. Cryptanalysis of a novel authentication protocol conforming to EPC-C1G2 standard[J]. Computer Standards & Interfaces, 2009, 31(2): 372-380.

[4] Al-Mahmud A, Morogan M C. Identity-based authentication and access control in wireless sensor networks[J]. International Journal of Computer Applications, 2012, 41(13): 18-24.

[5] 张敏. 无线传感器网络中的认证技术研究[D]. 北京: 北京邮电大学图书馆, 2013.

[6] Turkanovic M, Holbl M. An improved dynamic password-based user authentication scheme for hierarchical wireless sensor networks [J]. Elektronika Ir Elektrotechnika, 2013, 19(6): 109-116.

[7] Farash M S, Turkanovic M, Kumari S, et al. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment [J]. Ad-Hoc Networks, 2016, 36(P1): 152-176.

[8] 范修伟, 卢建朱. 一种轻量级的 WSN 认证和密钥协商方案[J]. 计算机工程, 2013, 39(3): 146-151.
Fan Xiuwei, Lu Jianzhu. A light-weight authentication and key agreement scheme for wireless sensor network [J]. Computer Engineering, 2013, 39(3): 146-151.

[9] Abduvaliev A, Lee S, Lee Y K. Simple Hash based message authentication scheme for wireless sensor networks [C]// International Conference on Communications and Information Technologies. Dresden: IEEE Press, 2009: 982-986.