第42卷 第6A期
2015年6月

计 算 机 科 学
Computer Science

Vol. 42 No. 6A
June 2015

# 无线传感器网络安全算法研究

谭 龙[1] 裴 超[2]

(河北外国语职业学院 秦皇岛 066000)[1] (北京理工大学秦皇岛分校 秦皇岛 066000)[2]

摘 要 拜占庭错误节点是影响整个网络可靠性及可用性的重要因素,设计轻量级的拜占庭容错路由算法对于提高大规模无线传感器网络容错问题具有重要的意义。对拜占庭将军问题(Byzantine Generals Problem,BGP)及无线传感器网络中的容错问题的国内外发展现状进行了了解。通过对无线传感器网络的安全目标及所面临的安全威胁的详细分析,得出选择合适的网络拓扑和合适的密码体制是无线传感器网络中解决拜占庭容错问题的技术难点。用OPNET进行仿真基于快速ECDSA的轻量级拜占庭容错路由算法ELBFT。结果表明,ELBFT方案采用基于分簇的双层拓扑,通过在不同的网络层面运行不同的拜占庭容错协议使簇间通信轮数减少,网络总通信量下降,有效地平衡了网络负载,在网络容错性能方面有了极大的改进。

关键词 无线传感器网络,拜占庭将军问题,椭圆曲线数字签名算法

中图法分类号 TP393.0 文献标识码 A

## Research of Wireless Sensors Network Security Algorithms

TAN Long[1] PEI Chao[2]

(Hebei Institute of Foreign Languages, Qinhuangdao 066000, China)[1]

(Beijing Institute of Technology QHD Branch, Qinhuangdao 066000, China)[2]

**Abstract** The influences from Byzantine nodes are important for the reliability and the usability of the entire network. The design of light weight Byzantine fault-tolerant protocols has a key significance to enhance the fault-tolerant ability for large-scale wireless sensor network. We first researched the status and development of Byzantine generals problem and fault-tolerant problem for WSN briefly. We analyzed the security targets and the security threats for WSN in detail, then on its basis, summed up the focus and technological difficulty about Byzantine fault-tolerant in WSN, which are choosing the appropriate network topology and the appropriate cryptography. Combining with fast ECDSA optimal threshold scheme, we proposed a lightweight Byzantine fault-tolerant protocol (ELBFT) through OPNET simulation. ELBFT based on double levels hierarchical architecture, operates different BFT to reduce the communication messages. ELBFT balances energy consumption and vastly improves the fault-tolerant capability for large-scale wireless sensor network.

**Keywords** Wireless sensor network, Byzantine generals problem, ECDSA

## 1 无线传感器网络安全技术概述与研究现状

### 1.1 无线传感器网络概述

无线传感器网络[1]是一种由大量锂电池供电的,具有有限感知、通信和计算能力的微型传感器节点所组成的无线自组织网络,通常情况下可简称为传感器网络。在无线传感器网络中,微型传感器节点通过内置传感器采集和感知环境或监测对象的信息,并通过协同工作方式将原始感知信息计算处理后传送到用户终端,极大扩展了人类认识和感知世界的能力,可以实现“无处不在计算”的普适计算理念[2]。

无线传感器网络已经被许多国家高度重视,很多研究单位及公司纷纷投入研发力量从事无线传感器网络技术的研发:2002年欧盟开始实施的自组织和协作的能量有效传感器网络计划;2003年美国国家自然基金会的Center for Embedded Networked Sensing计划;2004年日本总务省成立“泛在传感器网络调查研究会”等[3]。

### 1.2 无线传感器网络的安全需求

1. 网络通信与服务安全需求

网络通信的安全目标和典型计算机网络系统一样要保证数据的机密性、完整性、真实性和新鲜性。数据机密性是网络安全中的一个重要问题,要求所有敏感信息在存储和传输过程而中都应保证其机密性,不得向任何非授权用户或系统泄漏。有了机密性保证,攻击者可能无法获取信息的真实内容,但接收者并不能保证其收到数据是正确的。所以数据完整性也是确保数据正确的一种手段。通过数据完整性鉴别,可以确保数据没有因为传输过程而有任何改变。但是防范数据包被篡改还不够,攻击者还可以在网络中插入伪造的数据包来影响或改变网络数据流。通常情况下,基于发送者特有的属

谭 龙(1980—),男,硕士,讲师,主要研究方向为计算机网络安全、数据挖掘,E-mail:441830515@qq.com;裴 超(1987—),女,助讲,主要研究方向为计算机网络安全、电子制作。

性(如私钥)生成 MAC 可实现数据源的真实性认证。解决了数据的机密性和完整性问题,还需要保证数据的新鲜性,避免接收重复的信息。

网络服务包括可用性、自组织性及其它服务组件的安全。鉴于无线传感器网络的资源约束特性,移植传统计算机网络的安全算法和协议是有代价的,所以针对应用任务进行轻量级的适度安全设计对兼顾安全性和可用性相当重要。无线传感器网络中没有专门用于网络管理的服务器和路由器等固定基础设施,每个传感器节点既独立又灵活,自组织地构建自愈性多跳无线网络。在无线传感器网络的许多应用中,除了各层网络协议需正常运行以外,传感器节点间的时间同步、定位及网内信息的融合处理都是必不可少的基本服务。

2. 无线传感器网络安全性能评价指标

较早提议对无线传感器网络协议的性能评价应包括如下指标[4]:能量效率、延迟、精度、容错和可扩展性。除了满足前述安全需求外,安全机制或协议也应满足相应性能指标。在无线传感器网络中,恢复力是安全协议特有的评价指标,用于表述安全协议或机制的容侵能力;在共享密钥分配协议中,安全连通性也是评价指标之一。

### 1.3 无线传感器网络安全技术研究现状

无线传感器网络是一个多学科高度交叉的前沿热点研究领域,其中能量高效加密技术、安全框架、密钥管理、安全服务、入侵检测、隐私保护等研究是该领域的主要研究内容。

从无线传感器网络中密码算法的使用问题得出[5]:第一,鉴于对称密码算法的计算速度通常远比非对称密码算法快,无线传感器网络主要采用对称密码算法;第二,满足基本安全目标的安全协议集合构成无线传感器网络的安全框架,是构建安全无线传感器网络的重要手段;第三,共享密钥的分配是无线传感器网络面临的基本安全问题,密钥管理是无线传感器网络的安全基石,随机型密钥预分配具有较好的抗毁性[6];第四,维护无线传感器网络的正常设计功能,保证网络中各种协议模块的安全可信是必不可少的;第五,无线传感器网络易于受到多种攻击,而且未知的攻击新方法无从预料,入侵检测和反应机制是维护网络安全的第二道防线;第六,无线传感器网络的位置隐私、时间隐私和数据隐私等问题在很多文献中也在进行研究[7]。

## 2 拜占庭将军问题概述

### 2.1 拜占庭概述及其协议

BGP 是容错计算技术中的一个古老的问题,源于古罗马帝国的军事战略。1982 年提出 BGP 的原型是拜占庭军队战略规划的一个重要部分,目前用于解决现代密码学和分布式系统中的容错及可信问题,广泛应用于军事、金融、因特网等领域[8]。

同步拜占庭一致性协议几个经典算法包括 Lamport 提出的口信算法(Oral Message, OM);Berman 提出的议会投票算法(Cloture Vote);P. Feldman 提出的共同投币技术(Common Coin)[8]。这几种算法都是在同步环境中取得拜占庭问题的一致性协议,共同特点均依赖于节点间的多轮通信,并且都存在对同步系统的假设性限定,因此单纯的同步拜占庭算法不能较好地适应目前更为开放的包括 Internet 在内的分布式网络系统。

异步系统相对同步系统更为复杂,一个分布式异步系统中,其消息延迟、时钟漂移,甚至执行每一步操作所消耗的时间都没有上限[7]。而异步系统中的拜占庭一致性问题更是容错技术所研究的一个关键课题。上述拜占庭一致性算法基本上都是在系统初始化时,根据系统运行的环境来假设系统可能出现拜占庭错误节点的最大数目,并根据这个数目来确定系统中服务器的个数。

### 2.2 拜占庭群成员协议及安全分析

伴随系统规模的扩大及网络技术的发展,出现多种类型的网络系统的安全问题也亟待解决。在系统长时间的运行过程中,服务器由于物理原因或攻击者的原因极易出现处于错误状态而无法恢复的情况。针对前期提出的拜占庭一致性算法不能动态变更服务器的问题,研究人员又提出了拜占庭群成员协议(Byzantine group membership protocol, BGM)。BGM 协议不基于管理者,适用于异步系统。视图中的所有成员地位平等,共同发表意见,共同决策。由于成员的意见不需要由管理者来传达,因此协议的通讯轮数降低,通讯时间减少,也由于各成员只需表达自己的意见,因此传送的消息量小,同时也排除管理者本身的可信度问题。

BGM 协议采用前摄性签名共享机制建立系统密钥体系和签名体系。当前群视图成员共同分享系统密钥,即使有部分成员坏了也不能破坏系统,这使得系统安全性得到一定的提高。当系统成员被攻击者攻击之后(甚至成员私钥被偷盗),使用前摄性秘密共享机制来更新新视图成员的密钥分片,使得攻击者所控制的节点在新视图中无效。

## 3 无线传感器网络中的拜占庭问题

### 3.1 拜占庭问题解决的技术难点

无线传感器网络的特点给网络安全协议、安全路由、通信安全的保障等工作带来极大挑战,它应具备较好的抗毁容错性能来保障网络的稳定运行。无线传感器网络与传统网络及其他自组织网络相比有诸多不同之处,许多网络加密体制及网络安全路由解决方案不适用于其中。它的容错问题体现在在监测对象的目标信息探测中存在远近效应问题,不同传感器节点距检测目标的距离不同,且噪声的影响会导致不同节点的探测值有很大差异;其次拜占庭错误节点的存在,对信息探测构成直接的影响。针对这些 Clouqueur 等在 OM 算法及信息融合理论的基础上提出了值融合容错算法 VFA;在 VFA 的基础上 Hiroyuki 提出了分层拜占庭算法 HBA[17]。随着芯片集成技术水平的提高、大规模无线传感器网络应用的普及以密码安全体制的逐步健全,人们对通信环境、信息安全等级、通信质量等有了更高的要求,我们把无线传感器网络中拜占庭容错问题的技术难点总结为选择合适的网络拓扑结构与选择合适的密码体制两个方面。

### 3.2 网络拓扑结构的选择

1. 平面网络拓扑

最初的也是最常见的无线传感器网络拓扑结构为平面式,其网络节点是对等的,各节点在功能上没有大的不同,都负责实现数据的采集、处理、融合与传输,源节点与目的节点间可存在多条路径以供选择。

在平面式网络拓扑的无线传感器网络中,典型的平面路由协议有[9]:SPIN 系列(SPIN-BC、SPIN-PP、SPIN-EC 等)、

DD、Rumor Routing、Minimum Cost Forwarding Algorithm、Gradient-based Routing、Information-Driven Sensor Querying and Constrained Anisotropic Diffusion Routing、Cougar Approach to In-network Query Processing in Sensor NetWorks、ACQUIRE、Energy-Aware Routing、Routing Protocols with Random walks 等。虽然 Flooding 与 Gossiping 是无线传感网应用最早最简单的路由协议，不需要任何路由算法，也不需要维护网络拓扑结构，但端到端的数据传输延迟大。SPIN 是以数据为中心的自适应路由协议，通过协商机制来解决洪泛算法中的“内爆”和“重叠”问题，但其扩张性差，且功耗在所有节点之间分布不均匀；定向扩散(DD)算法中引入了网络梯度概念，并将其与局部算法相结合。SPIN 和 DD 算法推动了后来协议的发展。

2. 层次网络拓扑

层次式与平面网络拓扑相比路由开销较小，适合在大规模网络中采用。分层路由协议的可扩展性、高效性的特点对系统扩展性、生命周期和能效都有很大影响。在层次式网络拓扑的无线传感器网络中，分层路由协议包括[10]：LEACH、TEEN、APTEEN、MECN、SOP、SAR、HPAR、VGAR、TTDD 等。LEACH 是最早提出的专为无线传感网设计层次化协议，主要通过随机选择聚类簇头，平均分担中继通信业务来实现。拜占庭一致性问题的解决需要进行多轮的信息交换，为了保证通信质量，每轮信息交换都应涉及到相应的加解密机制。通过两种网络拓扑的比较可看出，针对大规模的无线传感器网络应采用分层拓扑来实现拜占庭一致性问题。

### 3.3 密码体制的选择

加解密算法是所有安全体制的基础，选择合适的密码体制是所有安全应用可行的关键。早期的无线传感器网络多采用传统的对称密码体制，使用广泛的有 RSA、DH、DSA 和 ECC 公钥体制[11]。DH 和 DSA 基于离散对数分解难题；RSA 的安全性基于大整数因子分解问题；ECC 的安全性基于指数级难度椭圆曲线离散对数问题。ECC 与 RSA 相比计算量小、处理速度快、密钥长度和系统参数小、带宽要求低。加拿大 Certicom 公司对椭圆曲线密码体制与 RSA 的安全性、密钥长度、密钥长度比进行了详细的比较[12]，对比结果如表 1 所列，通过以上对公钥密码体制的对比，ECC 更适合用于无线传感器网络。

表 1 RSA 与 ECC 安全性能比较

| MIPS 年数 | RSA 或 DSA 密钥长度 | ECC 密钥长度 | RSA 和 ECC 密钥长度比 |
|---|---|---|---|
| $10^4$ | 512 | 106 | 5:1 |
| $10^8$ | 768 | 132 | 6:1 |
| $10^{11}$ | 1024 | 160 | 7:1 |
| $10^{20}$ | 2048 | 210 | 10:1 |
| $10^{78}$ | 21000 | 600 | 35:1 |

## 4 优化的快速 ECDSA 算法

### 4.1 椭圆曲线数字签名算法

椭圆曲线密码系统(Elliptic Curve Cryptosystem，ECC)是把实数域上的乘法运算、指数运算等映射成了椭圆曲线上的加法运算，使得软硬件实现比其他公钥密码体系更快，成本更低，且其属于离散对数问题，安全性比较高，因此成为了人们研究的热点[13]。椭圆曲线数字签名算法 ECDSA 是对基于椭圆曲线的 ELGamal 签名算法的改进版，是数字签名算法 DSA 在椭圆曲线上的对等表示[14]。Scott Vanstone 提出 ECDSA 算法在 1998 年被国际标准化组织 ISO 采纳，于 2000 年被 IEEE 标准及 FIPS 所承认。

### 4.2 优化的快速 ECDSA 算法

基于椭圆曲线的数字签名算法都是将原有的基于离散对数的数字签名方案移植到椭圆曲线密码体制中，基于离散对数的通用签名方程同为 $u=dv+kw \bmod (p-1)$。方程的 5 个元素 $(d,k,u,v,w)$ 转换到椭圆曲线上，但并非得到的所有方案都安全。从安全可行的签名方案可以看出，影响椭圆曲线签名体制计算速度的关键是椭圆曲线中的倍点和模逆运算。倍点运算及模逆运算的计算量很大，时耗与能耗多，基于椭圆曲线的 ELGamal 签名算法及椭圆曲线数字签名算法 ECDSA 这两种签名算法的使用目前比较普遍，但在其签名效率上，其签名过程中含有大量的求逆运算。对于节点能量及计算能力均十分有限的无线传感器网络，其应用的可行性并不是很高。

为了提高椭圆曲线数字签名的效率，签名算法在参数生成、签名过程及验证过程中一方面应该避免或减少求逆运算，以减少其计算量，另一方面要设计适合的快速认证算法，以降低点乘[15]。针对无线传感器网络的特点，在轻量级拜占庭容错路由方案中采用优化的快速 ECDSA 算法，其签名方案如下：

定义椭圆曲线域参数 $D=(F,a,b,p)$，$F$：有限域 $GF(p^n)$，$a,b\in GF(p^n)$，$P$ 是基点，$\#E(GF(p^n))$ 为椭圆曲线的阶。节点 $A$ 要给节点 $B$ 发送消息 $M$，其快速 ECDSA 签名算法的签名过程与验证过程流程如图 1 所示。

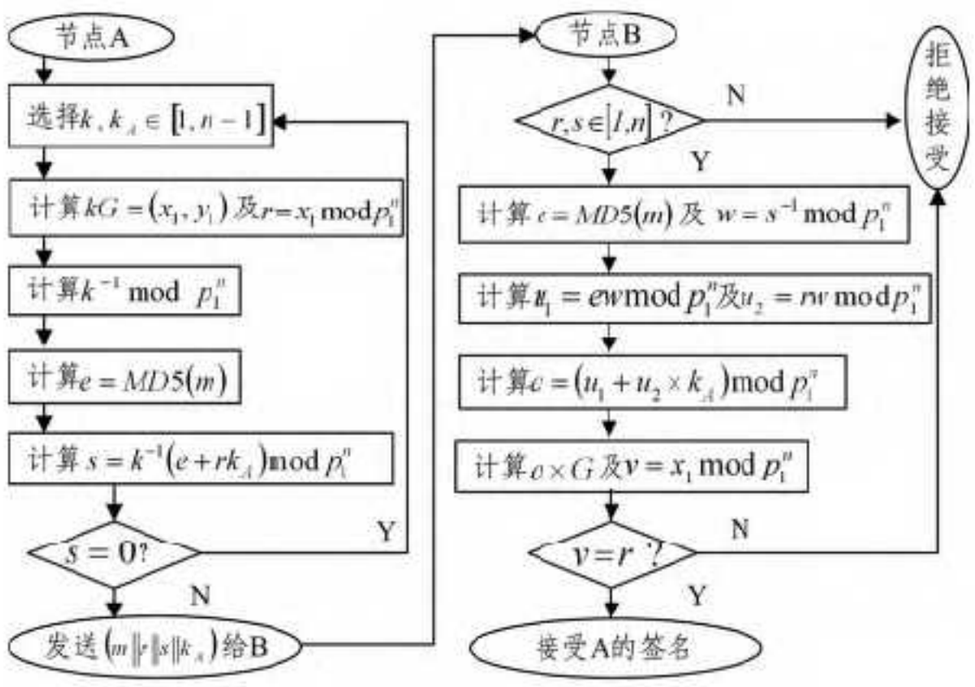


图 1 快速 ECDSA 签名算法流程

(1)节点 $A$ 随机秘密选择整数 $k,k_A\in[1,n-1]$；

(2)节点 $A$ 计算 $kG=(x_1,y_1)$(其中 $y_1$ 不计算)和 $r=x_1 \bmod p_1^n$；

(3)节点 $A$ 计算 $k^{-1} \bmod p_1^n$；

(4)节点 $A$ 计算 $e=MD5(m)$；

(5)节点 $A$ 计算 $s=k^{-1}(e+rk_A) \bmod p_1^n$，若 $s=0$ 则返回 1；

(6)消息 $M$ 的快速 ECDSA 签名即整数对 $(r,s)$，$A$ 发送 $(m|r|s|k_A)$ 给节点 $B$。

快速 ECDSA 验证过程为：

(1)节点 $B$ 收到签名 $(r,s)$，验证 $r$ 和 $s$ 是否为 $[1,n-1]$ 间的整数，若不是，则直接拒绝此签名；

(2)节点 $B$ 计算 $e=MD5(m)$ 及 $w=s^{-1} \bmod p_1^n$；

(3) 节点 $B$ 计算 $u_1=ew \bmod p_1^n$ 和 $u_2=rw \bmod p_1^n$；

(4) 节点 $B$ 计算 $a=(u_1+u_2\times k_A) \bmod p_1^n$；

(5) 节点 $B$ 在 Montgomery 曲线上计算 $a\times G$ 的倍点运算及 $v=x_1 \bmod p_1^n$；

(6) 若 $v=r$，接受节点 $A$ 的签名。

优化的快速 ECDSA 算法在求欧拉函数时只进行一次模幂、一次模除、一次模减，大大降低了求欧拉函数的计算复杂度，将验证签名与产生签名的时间之比减少约 40%，从 2 倍降低到约 1.2 倍，因此可在存储空间有限的条件下实现比较适合的无线传感器网络。

## 5 基于快速 ECDSA 的大规模 WSN 轻量级拜占庭容错路由方案

### 5.1 ELBFT 方案可行性分析与整体框架

基于快速 ECDSA 的轻量级拜占庭容错路由方案 ELBFT(Lightweight Byzantine fault-tolerant protocol based on ECDSA)用于解决大规模无线传感器网络的安全容错问题。ELBFT 方案采用基于分簇的双层拓扑，在不同的网络层面执行不同通信轮数的拜占庭容错，有效减少通信轮数，平衡网络负载。我们通过对两个预设算法进行理论分析与仿真数据对比来进行方案的可行性分析。无线传感器网络总节点数为 $N$，拜占庭错误节点数为 $f$。通信量定义为一轮通信中传输数据包的个数，以某节点开始广播信息起计算，到其它节点均收到此信息的时间为一轮；通信轮数定义为完成全部通信所需要的轮数，仿真流程如图 2 所示。

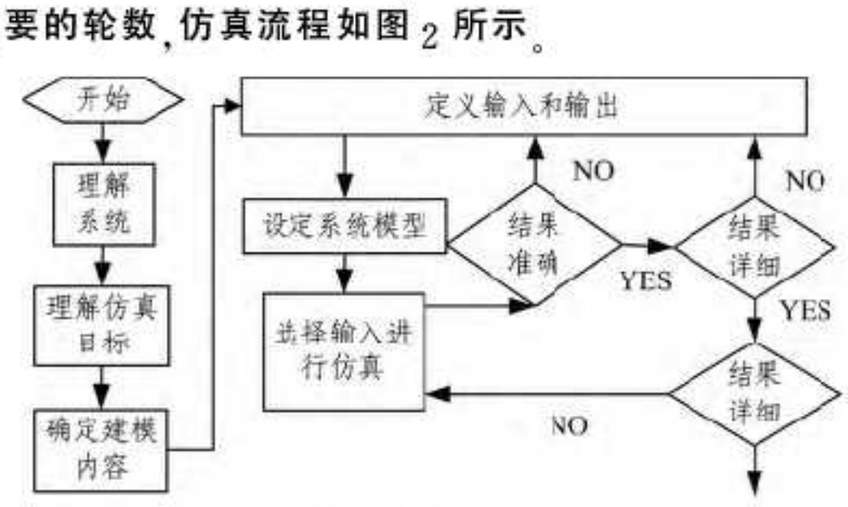


图 2 仿真流程

ELBFT 方案的网络拓扑采用基于分簇的双层拓扑，对于不同的网络层面运行不同的拜占庭容错协议。在局部范围的各簇内节点间执行 $OM(f)$ 算法，通过 3 轮通信的拜占庭容错协议来实现。簇内信息传输安全机制采用基于快速 ECDSA 算法轻量优化了的 $(2f+1,3f+1)$ 门限签名体制，各簇头向外发送的消息同样携带基于快速 ECDSA 的数字签名。

对于网络全局范围，各簇之间的通信仅通过簇头间执行 $OM(f)$ 算法及两轮通信的轻量级良性容错协议来实现。在承载层面搜索建立可信路由时，采用添加了节点认证因子和可信因子的蚁群优化增强算法，快速实现节点的安全认证并搜索建立可信路由。ELBFT 方案的整体框架如图 3 所示。




图 3 ELBFT 方案的整体框架示意图

### 5.2 分簇的划分

ELBFT 网络结构为基于分簇的双层拓扑。分簇的双层拓扑结构便于管理，有利于分布式算法的应用，可以对系统变化作出快速反应，具有较好的可扩展性，适合大规模网络。

根据算法采用典型的 LEACH 协议[16]做为分簇的原始模型：各簇选举产生簇头节点作为本簇节点的代表，簇内节点只和本簇节点通信，簇头融合了成员节点的数据之后再进行转发，簇与簇之间及簇与基站之间的通信则由簇头节点完成，在保证了原有覆盖范围内的数据通信的基础上减少了数据通信量。簇头选举在 LEACH 协议优化版本 DCHS 协议[18]的基础上进行改进。

第一步 以 $E_{n\text{-}current}$ 表示节点当前能量，$E_{n\text{-}\max}$ 表示节点初始能量，门限值调整为：

$$T(n)'_{optimize}=\frac{p}{1-p*(r \bmod \frac{1}{p})}*\frac{E_{n\text{-}current}}{E_{n\text{-}\max}} \tag{1}$$

第二步 以 $N_d=n_{neighbor}*p$ 来表示节点密度，门限值调整为：

$$T(n)''_{optimize}=\frac{p}{1-p*(r \bmod \frac{1}{p})}*[\frac{E_{n\text{-}current}}{E_{n\text{-}\max}}+N_d(1-\frac{E_{n\text{-}current}}{E_{n\text{-}\max}})] \tag{2}$$

第三步 以 $r_s$ 表示节点连续没有成功竞选簇头的轮数，且在当选后重置为 0，门限值又调整为：

$$T(n)_{optimize}=\frac{p}{1-p*(r \bmod \frac{1}{p})}*[\frac{E_{n\text{-}current}}{E_{n\text{-}\max}}+N_d(r_s div \frac{1}{p})(1-\frac{E_{n\text{-}current}}{E_{n-\max}})] \tag{3}$$

此门限 $T(n)_{optimize}$ 考虑到了节点当前能量、节点密度及 $T(n)_{optimize}$ 对簇头数目的影响，使簇的划分和簇头的产生更加合理。

### 5.3 签名和验证

簇、簇头确定之后，由基站统一颁发安全性基于 Montgomery 型椭圆曲线加密体制证书给各簇头节点。选取一条安全的 Montgomery 型的 ECC 曲线，确定曲线的所有参数权值[15]。先求选定的某一范围的椭圆曲线的阶，然后判断所求阶是否含有大素数因子，若计算出来的椭圆曲线的阶中含有 $>10^{14}$ 的大素数因子则为有效曲线。Montgomery 型的 ECC 曲线计算点乘运算可以仅计算 $x$ 坐标，不计算 $y$ 坐标值。加密时要将明文分组嵌入 ECC 曲线中，$(x,y)$ 坐标比单权 $x$ 坐标更具有扰乱性，因此具有更高的安全性。

各分簇内部传输信息采用基于快速 ECDSA 算法轻量优化了的 $(2f+1,3f+1)$ 门限体制进行签名，每个簇有一个公私密钥对，其公钥被分割成 Partial Key 分摊给簇内各节点，各节点用其可对信息进行 Partial Signature，并且节点拥有验证簇内各部分标记有效性的验证信息，簇头可对收集到的多个簇内标记进行信息整合。各簇头向外发送的消息中携带基于快速 ECDSA 算法的数字签名。

### 5.4 簇内、簇间层面容错问题

簇内间层优化拜占庭容错协议：若网络有 $N$ 个节点，被分为 $M$ 个分簇，每个分簇内包含差不多 $k$ 个节点，总的拜占庭错误节点数为 $f$，在每个簇内执行 $OM(f)$ 算法并由 3 轮通

信的拜占庭容错协议来实现，领袖节点角色由本簇簇头节点来担任。限制簇内节点只和本簇节点通信，通过 BFT 协议三轮通信来保证更新信息已通过一致性协议且被执行。

当拜占庭错误节点数 $f<\min(k/3)$ 时，簇内拜占庭错误节点 $f_i$ 与簇内节点数 $k$ 满足 $f_i\leqslant f\leqslant\min(k/3)\leqslant k/3$，执行一次 $OM(f)$ 算法即可消除。当 $f_i>k/3$ 时，则需通过簇间层面的轻量级良性拜占庭容错协议来消除这一部分簇拜占庭错误节点的影响，如图 4 所示。

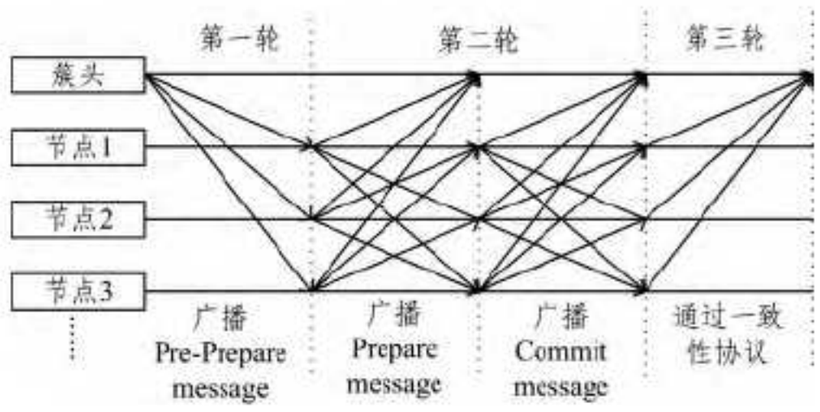


图 4　簇内层面拜占庭容错

簇间层面轻量级良性容错：通过在局部范围的簇内层面执行 $OM(f)$ 算法之后，对于簇内拜占庭错误节点 $f_i$ 与簇内节点数 $k$ 满足 $f_i<k/3$ 的分簇，在簇内执行一次 $OM(f)$ 算法即可消除拜占庭错误节点的影响。而对于簇间层面簇头之间的通信，则通过轻量级的两轮通信 $OM(f)$ 算法来消除拜占庭错误节点的影响。在簇间层面，限制簇与簇之间及簇与基站之间的通信则由簇头节点完成。$OM(f)$ 算法通过良性拜占庭容错协议的两轮通信来实现，以确保簇间视图信息一致性，如图 5 所示。

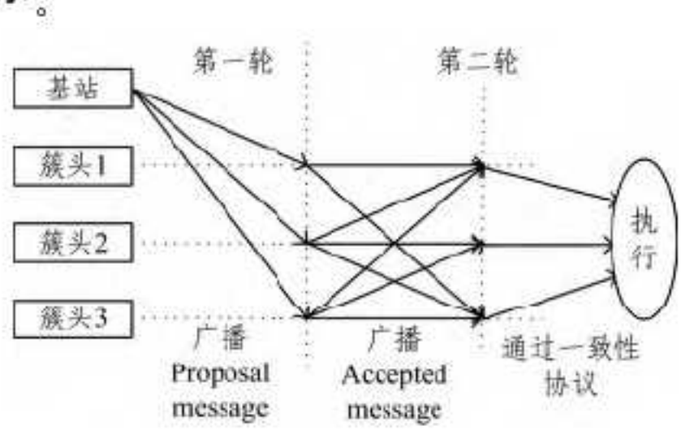


图 5　簇间层面拜占庭容错

### 5.5　承载层面的安全增强算法

在整个网络的承载层面采用与群体智能优化算法相结合的方法，添加了节点认证因子和可信因子的蚁群优化增强算法，快速实现节点的安全认证并搜索建立可信路由。改进后的前向及后向蚂蚁数据包格式如图 6 所示。

| Ant-ID (4 bits) | S-addr (4 bits) | Cred (4 bits) | Date (64 B) | Pre-PK (20 B) |
|---|---|---|---|---|
| T-stamp (4 bits) | Dest (4 bits) | Nodes (4 bits) | Hops (4 bits) | |

| Ant-ID (4 bits) | S-addr (4 bits) | Dest (4 bits) |
|---|---|---|
| Cred (4 bits) | Nodes (4 bits) | Hops (4 bits) |

图 6　前向蚂蚁包格式(上)、后向蚂蚁包格式(下)

无线传感器网络相邻两节点 $A$、$B$ 间的可信度为[19]：

$$W_{Credibility}(A,B)=\frac{\alpha}{D_{AB}}+\frac{\beta}{L_{AB}}+\lambda*E \tag{4}$$

其中，通过前向蚂蚁包对后向蚂蚁包的计时来获取节点 $A$ 到节点 $B$ 的时延 $D_{AB}$；通过对接收到的数据包包头序列号字段的连续性进行丢包检测来获取丢包率 $L_{AB}$；$E$ 是节点 $B$ 的剩余能量，$\alpha$、$\beta$、$\lambda$ 是加权系数，保障时延、丢包率和剩余能量这 3 项值分别在 0 到 1 之间。

结束语　随着科技的发展，互联网方便了人们的信息交流。无线传感器网络将大量多种类传感器节点通过静态配置把客观世界的物理信息与传输网络连接在一起，扩展了人们的信息获取能力并应用于多个领域中，为人们提供直接、真实、有效的信息。

本文以大规模无线传感器网络为研究对象，针对无线传感器网络的安全与容错，详细分析了拜占庭容错问题的解决方案，通过对无线传感器网络中这个问题进行技术难点分析，提出一种基于快速 ECDSA 的轻量级拜占庭容错路由方案 ELBFT。之后在两个预设算法中：预设算法一以 VFA 算法为模型，总的通信量为 $F(N,f)=(N-1)\cdots(N-f-1)$；预设算法二以 HBA 算法为模型，将 $N$ 个节点分为 $M$ 组，每个分组内包含 $k$ 个节点，拜占庭错误节点数同为 $f$，总通信量为 $F(M,f)+MF(k,f)$，仿真实验数据对比分析说明了 ELBFT 容错路由方案的可行性。ELBFT 方案采用基于分簇的双层拓扑，针对不同的网络层面执行不同轮数的拜占庭容错，簇间通信轮数减少 1/3，网络总通信量下降为 $\frac{2}{3}F(M,f)+MF(k,f)$，有效地平衡了网络负载。

## 参 考 文 献


[1] Ozaki K, Watanabe K, Itaya S, et al. A fault-tolerant model of wireless sensor-actor network[C] // Proceedings of the Ninth IEEE International Symposium on Object and Component-Oriented Real-Time Distributed computing(ISORC'06). 2006: 186-193

[2] Castro M, Liskov B. Practical Byzantine Fault Tolerance and Proactive Recovery[J]. ACM Transactions on Computer Systems(TOCS), 2002, 20(4): 398-461

[3] Coan B. A communication efficient canonical form for fault-tolerant distributed protocols [C] // Proc. 5th PODC. August 1986: 63-72

[4] 任丰原，黄海宁，林闯. 无线传感器网络[J]. 软件学报，2003(7): 1281-1291

[5] Tseng H C. Sinkhole intrusion indicators in DSR MANETs Culpepper[C] // Proceedings of BroadNets. October 2004: 681-688

[6] Heinzelman W. Energy-Efficient Communication Protocol for Wireless Microsensor Networks[C] // Proc. 33rd Hawaii Int'l. Conf. Sys. Sci. . Jan. 2000

[7] Cachin C, kursawe K, Shoup V. Random Oracles in Constantinople: Practical Asynchronous Byzantine Agreement using Cryptography [J]. Journal of Cryptology, 18(3): 219-246

[8] Lamport, Shostak R, Pease M. The Byzantine generals problem [J]. ACM Transactions on Programming Languages and Systems, 1982, 4(3)

[9] Yu H B, Zeng P, Wang Z F. Study of communication protocol of distributed sensor network[J]. Journal of China Institute of Communications, 2004, 25(10): 102-110

[10] Chan H, Perrig A. ACE: An emergent algorithm for highly uniform cluster formation[C] // Proc. of the 1st European Workshop on Wireless Sensor Networks. LNCS2920, Berlin: Springer-Verlag, 2004: 154-171

[11] Eberle H, Gura N, Shantz S C, et al. A Public-Key Cryptogra-

phic Processor for RSA and ECC[C]// 15th IEEE International Conference on Application-Specific Systems, Architectures and Processors(ASAP'04). ASAP,2004:98-110

[12] Mohammed E, Emarah A E, El-Shennawy K. Elliptic curve cryptosystems on smart cards[C]// 2001 IEEE 35th International Carnahan Conference on Security Technology. Oct 2001:213-222

[13] Koblitz N. Elliptic Curve Cryptosystems [J]. Mathematics of Compution American Mathematical Society, 1987(48):203-309

[14] Johnson D, Menezes A, Vanstone S. The Elliptic Curve Digital Signature Algorithm(ECDSA)[J]. International Journal of Information Security, IJIS, 2001(1):36-63

[15] 王潮,时向勇,牛志华. 基于 Montgomery 曲线改进 ECDSA 算法的研究[J]. 通信学报,2010,31(1):9-13

[16] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks[C]// Proc. 33rd Hawaii Int'l. Conf. Sys. Sci., Jan., 2000

[17] Clouqueur T, Saluja K K, Ramanathan P. Fault Tolerance in Collaborative Sensor Networks for Target Detection [J]. IEEE Transactions on Computers, 2004, 53(3):320-333

[18] Handy M J, Haase M, Timmermann D. Low energy adaptive clustering hierarchy with deterministic cluster-head selection [C]// Proceedings of the 4th IEEE Conference on Mobile and Wireless Communications Networks. IEEE Communications Society, 2002:368-372

[19] 王潮,贾翔宇,林强. 基于可信度的无线传感器网络安全路由算法[J]. 通信学报,2008,29(11):105-112

(上接第 428 页)

法对矩阵进行标准化处理后,得到标准化矩阵 $R$:

$$R=\begin{bmatrix}0.218&0.164&0.205&0.232&0.181\\0.176&0.205&0.192&0.187&0.222\\0.195&0.203&0.183&0.211&0.208\\0.203&0.206&0.189&0.226&0.176\\0.346&0.285&0&0.369&0\\0&0.533&0.467&0&0\\0&0.45&0&0.22&0.33\\0.375&0&0&0.422&0.203\\0.214&0.2&0.176&0.224&0.186\\0.188&0.215&0.205&0.195&0.197\\0.203&0.197&0.189&0.207&0.205\\0.2&0.198&0.207&0.191&0.204\\0.208&0.188&0.202&0.208&0.194\\0.199&0.203&0.206&0.197&0.195\\0.202&0.198&0.181&0.212&0.207\\0.217&0.197&0.209&0.186&0.191\\0.215&0.195&0.2&0.207&0.183\\0.2&0.2&0.2&0.2&0.2\\0&0&0.515&0.485&0\\0.196&0.204&0.202&0.199&0.199\\0.197&0.203&0.201&0.201&0.198\\0.201&0.204&0.195&0.192&0.208\\0.196&0.198&0.212&0.193&0.201\\0.194&0.205&0.202&0.211&0.188\\0.195&0.202&0.192&0.199&0.212\\0.196&0.203&0.191&0.199&0.211\\0.199&0.195&0.202&0.209&0.195\\0.199&0.195&0.202&0.209&0.195\\0.199&0.201&0.199&0.204&0.197\\0.202&0.207&0.197&0.192&0.202\\0.202&0.211&0.183&0.205&0.199\end{bmatrix}^{T}$$

(6) 综合评价值计算

由 3.3 节计算公式,可得 5 节中入侵检测系统的最后综合评测值为:

$$Z=R\times W_C=[0.168,0.196,0.249,0.226,0.161]$$

如图 2 所示,综合评测结果显示,IDS3 评测结果最好,IDS4 评测次之,IDS5 最差。

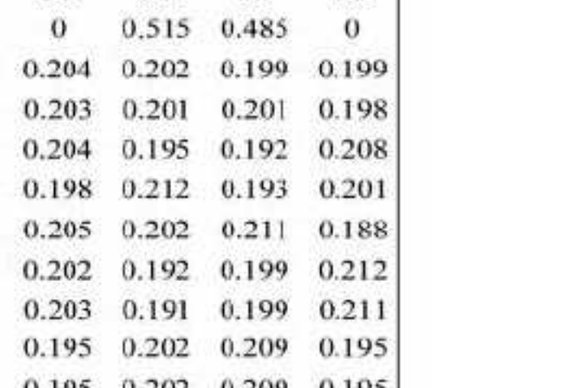


图 2 IDS 综合评测结果

对比表 5 可知,虽然 IDS3 系统在功能方面有 3 项指标为 0,即没有实现该功能,但是由于性能指标以及安全性指标的综合得分高,并且在该两项的权重影响下,评测结果依然是最优的。IDS4 系统在功能方面只有 1 项指标为 0,但是有 3 项性能指标比 IDS3 较差,在性能权重的影响下,综合评测结果比 IDS3 稍差。因此本次实验结果较为真实地反映了入侵检测系统之间的优劣。

如果用户在实际购买 IDS 系统时,还需要综合评估性价比、系统适应场合等因素进行选购,比如性价比最高的 IDS 可能因为没有某一项用户必须要有的重要功能或者检测率没有达到所要求 95% 以上等原因,用户只能退而求其次进行选购。

结束语 本文针对目前入侵检测系统的评价指标体系完整性不足以及大部分采用主观评价法进行评价,对评价模型进行了改进,提出一种基于多层次混合评价模型,该模型算法综合主观和客观评价方法开展对 IDS 的评价,减少了主观因素,同时构建了一套较为完整的指标体系,并且通过本文提出的一种指标量化方法,使得评价结果更具可靠性,对实际选择和评价 IDS 更有现实指导意义。通过实验评测,本文提出的多层次混合评价模型能较为真实地反映入侵检测系统的优劣。本文在指标量化方法中,对指标体系中非性能指标的难度系数采用的是专家打分方法,存在一定的主观因素,在后续的研究工作中将开展对指标难度系数的研究。

## 参 考 文 献

[1] 甘早斌,何建国. 入侵检测系统的多层次模糊综合评价研究[J]. 计算机应用研究,2006(4):90

[2] 中华人民共和国国家质量监督检验检疫总局,中国国家标准化管理委员会 GB/T 20275-2006 信息安全技术 入侵检测系统技术要求和测试评价方法[Z]. 2006:1-43

[3] 左国超,段利华. 基于属性测度的入侵检测系统评价方法[J]. 云南大学学报,2006,28(S2):182-186

[4] 曾一五,肖红叶. 统计学导论[M]. 北京:科学出版社,2006:233

[5] 罗嵘. 入侵检测产品的评价指标[J]. 通信技术,2001(2):45-52

[6] 朱珊毅,朱怡安. 基于双层混合法的计算机系统性能评价模型[J]. 微处理机,2010,12(6):114-118

[7] 孙凯,鞠晓峰,李煜华. 基于变异系数法的企业孵化器运行绩效评价[J]. 哈尔滨理工大学学报,2007,12(3):166-167