·安全技术·　　文章编号：1000-3428(2019)06-0188-05　　文献标志码：A　　中图分类号：TP393

军用 Ad Hoc 网络分层体系架构及安全协议

楼　俐，范建华，胡永扬，李　冉

（南京电讯技术研究所，南京 210007）

摘　要：为提高军用 Ad Hoc 网络的安全性与可靠性，提出一种分层的网络体系架构。基于时间戳的直接密钥交换签密（DKEUTS）方案，采用随机数替代时间戳，设计一种简化的基于随机数的签密（SRS）方案。根据不同层次节点的安全性需求以及通信和计算性能，选择 DKEUTS 方案或不同签密参数的 SRS 方案。通过网络割点判别，对网络连通度进行预测，重构网络拓扑，保障网络的可靠性。性能分析结果表明，该分层网络架构与安全协议可适用于节点非同构网络。

关键词：无线通信；军用 Ad Hoc 网络；网络安全；网络连通度；网络可靠性

中文引用格式：楼俐，范建华，胡永扬，等. 军用 Ad Hoc 网络分层体系架构及安全协议[J]. 计算机工程，2019，45(6)：188-192，198.

英文引用格式：LOU Li，FAN Jianhua，HU Yongyang，et al. Hierarchical architecture and security protocol for military Ad Hoc network[J]. Computer Engineering，2019，45(6)：188-192，198.

Hierarchical Architecture and Security Protocol for Military Ad Hoc Network

LOU Li，FAN Jianhua，HU Yongyang，LI Ran

（Nanjing Telecommunication Technology Research Institute，Nanjing 210007，China）

【Abstract】 In order to improve the security and reliability of military Ad Hoc network，this paper proposes a hierarchical network architecture and designs a Shortened Random-based Signcryption（SRS）scheme by using a random number instead of timestamp in Direct Key Exchange Using Timestamp Signcryption（DKEUTS）scheme. According to the security requirements，communication and computing performances of different nodes，this paper chooses the DKEUTS scheme or the SRS schemes with different signcryption parameters. By discriminating whether the network node is a cut-vertex，the network connectivity is predicted. The information of network connectivity can be used to reconstruct network topology and guarantee network reliability. Performance analysis results show that the proposed hierarchical network architecture and security protocol can be applied in node non-homogeneous networks.

【Key words】 wireless communication；military Ad Hoc network；network security；network connectivity；network reliability

DOI：10.19678/j.issn.1000-3428.0049815

0　概述

自 20 世纪 70 年代以来，由于 Ad Hoc 网络具有高度动态的拓扑结构，可快速部署、灵活扩展，并且具备较强的自组织能力和抗毁性能，被广泛应用在军用和民用领域。在 IEEE 802.11 中，Ad Hoc 网络被定义为“所有节点均由移动主机构成的多跳、无中心、自组织无线网络”，其最初应用于军用无线通信领域，且多在危险性较高的作战地区被用来延伸数据通信覆盖范围。对于战场前沿网络，这种自组织、无中心网络结构可为单兵作战系统提供可靠的联网保障。Ad Hoc 网络在民用领域也有较好的发展前景，近年来相关研究成果呈指数级增加，其基本架构和协议也日趋成熟。然而，Ad Hoc 网络所具备的一些重要基本特征，也造成一些缺陷：无需固定的传输基础设施（路由器和访问接入点），意味着实现通信的过程更加复杂；多跳传输，源到目标路径上的多个节点将进行重传操作；无线传输，信道的固有开放特性导致网络易受干扰；网络节点位置不固定，即使较简单的干扰都可能掩盖信号，使其难以检测。并且其 MAC 机制的设计和源到目标路由的构建都更加复杂。

军用 Ad Hoc 网络，除了需要解决广播方式传输导致无线信号冲突频繁，引发较高的数据丢失率的

基金项目：国防科技重点实验室基金（9140C020301140C02008）；中国博士后科学基金特别资助项目（2016T91016）。

作者简介：楼　俐（1982—），女，工程师、博士，主研方向为网络安全、网络可靠性；范建华，研究员、博士；胡永扬，高级工程师、硕士；李　冉，工程师、博士。

收稿日期：2017-12-20　　**修回日期：**2018-04-22　**E-mail：**louie1000@163.com

问题,还由于主要部署在难以提前架设网络基础设施的战场前沿或其他特定作战区域,执行侦察、监视、目标识别、态势感知等战场机动通信任务,面临比民用领域 Ad Hoc 网络更加复杂严峻的挑战,其信息数据和路由路径受到更多风险威胁,对许多安全攻击十分敏感,易受攻击影响,需重点抵御对网络的摧毁和破坏。安全性、可靠性是军用网络首先需要考虑的问题,因此,本文构建鲁棒的军用 Ad Hoc 网络体系架构,并在此基础上设计安全可靠的协议。

1　相关研究

目前,Ad Hoc 网络技术在国内外军用和民用领域均有成功应用的案例,尤其是美军在部队的各级网络中广泛采用 Ad Hoc 网络技术部署组网。例如:美军在战术互联网中使用近期数字电台(Near Term Digital Radio, NTDR)组网应用的 Ad Hoc 网络技术[1],采用双频分级结构。在这种分级结构的网络中,簇成员功能简单,无需维护复杂的路由信息。美军的地面武士计划,大力发展宽带化手持便携式个人移动终端。Ad Hoc 网络是建立完善单兵通信系统的核心技术,它的抗毁性能对增强单兵通信系统网络的稳定性起到关键作用。另外用于战场感知的战场前沿传感器网络以集成方式设置在被测目标附近,构成自组织无中心网络,实现远距离通信。

美军于 2001 年正式提出网络中心战(Network Centric Warfare, NCW)理论[2-3]。NCW 的主要目标是利用战术网络配置,通过信息网络将地理上分散的传感器、指挥控制中心、武器平台整合成完善的网络平台,以网络平台为中心,更高效地实现信息分发共享,协调诸兵种的联合作战行动。NCW 中的先进信息分发技术推动了 Ad Hoc 网络技术的进一步应用[4],例如将其应用于警用、搜救以及消防等应急领域。

由于工作在敌对环境下并缺乏固定基础设施,Ad Hoc 网络对各类攻击表现得非常脆弱。而军用网络需要同时保障网络的可靠性和安全性,尤其在战术环境下,对 Ad Hoc 网络有更高的安全性要求[2],主要体现在:可用性,在遭受拒绝服务等攻击时,依然能提供网络服务;机密性,某些信息不会暴露给未授权的实体;完整性,被传输的信息不会被恶意攻击等破坏;认证,未经授权的节点不能访问网络资源和信息;不可否认性,节点不能否认发送过信息。Ad Hoc 网络的可靠性为保证网络节点和链路在一定的失效概率情况下,维持网络一定的连通率。为了满足传统军用 Ad Hoc 网络结构的可靠性和安全性需求,本文提出一种多层自适应网络架构,并设计针对该架构的安全签密协议,为数字战场提供安全、实时的多播通信。

在军用 Ad Hoc 网络结构设计方面,采用多层网络结构化组织形式。在传统的军用战术网,移动骨干网络节点(如移动战术中心或车载通信节点)为一层,常规战术通信节点(如带宽和计算能力有限的手持通信节点)为一层。本文根据地面骨干节点的军事等级、通信能力等,将军用 Ad Hoc 网络中骨干网分成 2 层,第 1 层是升空飞行器到移动战术中心(称为 I 类移动地面骨干节点),第 2 层是移动战术中心到车载骨干节点(称为 II 类移动地面骨干节点)。这样更有利于密钥局部分发和管理。

在安全签密设计方面,目前网络加密方式主要是基于公钥和混合加密的密钥算法。Ad Hoc 网络由于缺乏基础设施,无法获取可信第三方密钥分发机构分发的静态密钥,因此,多采用 Diffie-Hellman 密钥交换方案[5-6]和分布式密钥管理机制[7]。另外,如果系统中某些部分被攻击、破坏或者控制,会引发单点失效(Single Point of Failure, SPoF)问题[8-9],重要程度较高的骨干节点尤其要注意这个问题。在密钥管理方面,为了适用于大范围的动态军用分层 Ad Hoc 网络,一般采用混合密钥管理技术[10],通过降低重定密钥的工作负载,保障网络前向和后向安全。同时,采用混合密钥管理结构还能够最小化 SPoF 问题。

本文军用分层 Ad Hoc 网络利用签密方案代替先签名后加密方案,以提高系统效率。除了集成基于时间戳的直接密钥交换签密(Direct Key Exchange Using Timestamp Signcryption, DKEUTS)[11-12]方案外,本文提出一种简化的基于随机数的签密(Shortened Random-based Signcryption, SRS)方案。和传统先签名后加密方案相比,DKEUTS 方案适合军用 Ad Hoc 网络高层骨干节点间的成对密钥交换,而 SRS 方案适用于带宽和计算资源受限的常规地面通信节点,如单兵手持电台等。多级安全机制为每一层提供了足够的安全保障的同时,防止网络因为不必要的密码操作导致过量负载。

2　军用分层 Ad Hoc 网络体系结构设计

2.1　军用 Ad Hoc 网络

一般的 Ad Hoc 网络协议设计,都是基于同构网络假设:所有节点具有相同的传输、计算和存储能力。然而根据战场任务需求不同,军用 Ad Hoc 网络通信节点具有异构性,即不同的节点具备不同的通信、计算和存储能力,并且部分节点或者所有节点都没有固定基础设施的支持。因此,同构网络的假设对于军用 Ad Hoc 网络不适用。

为了解决该问题,传统的军用空地分层 Ad Hoc 网络一般按照异构网络结构进行分层化设计[13],一般具有 3 个节点层:升空飞行平台(Flight Platform, FP)层,移动地面骨干节点(Mobile Ground Backbone, MGB)层和常规地面节点(Common Ground Node, CGN)层。FP 层是由有人或无人升空飞行器构成的空中移动骨干网,在现代战场通信中占据极其重要的

地位。因为可以配置阵列天线,FP 层具备很强的通信能力,可以和低层网络进行通信。传统军用移动 Ad Hoc 网络的第 2 层包括了 MGB,例如武装车辆和单兵,具有较强的通信和计算能力以及较快的移动性。MGB 可作为无基础设施的网络的骨干节点,为 FP 层和 CGN 层提供中间集成。CGN 层由通信和计算能力有限的单兵通信设备构成。在这 3 层结构中,FP 层具有极高的移动性,并负责通信覆盖区域内地面骨干节点通联。FP 和 MBG 层的 SPoF 问题,影响范围更广,其安全性和可靠性尤为重要。

2.2 本文网络体系结构

和传统军用 Ad Hoc 网络相似,本文采用了空地分层架构,并将地面节点按照军事重要度、职能、通信能力分为 I 类移动地面骨干节点 MGB1(移动战术中心和移动指挥基地)、II 类移动地面骨干节点 MGB2(车载台)和 CGN(手持台)。在这种多层架构下,分层内的每个单元管理自身所辖区域,选用各层适用的安全协议保证组内的通信安全。每个 FP 控制一个 MGB1 分组。同样地,每个 MGB1 控制一个 MGB2 分组,每个 MGB2 控制一个 CGN 分组,如图 1 所示。

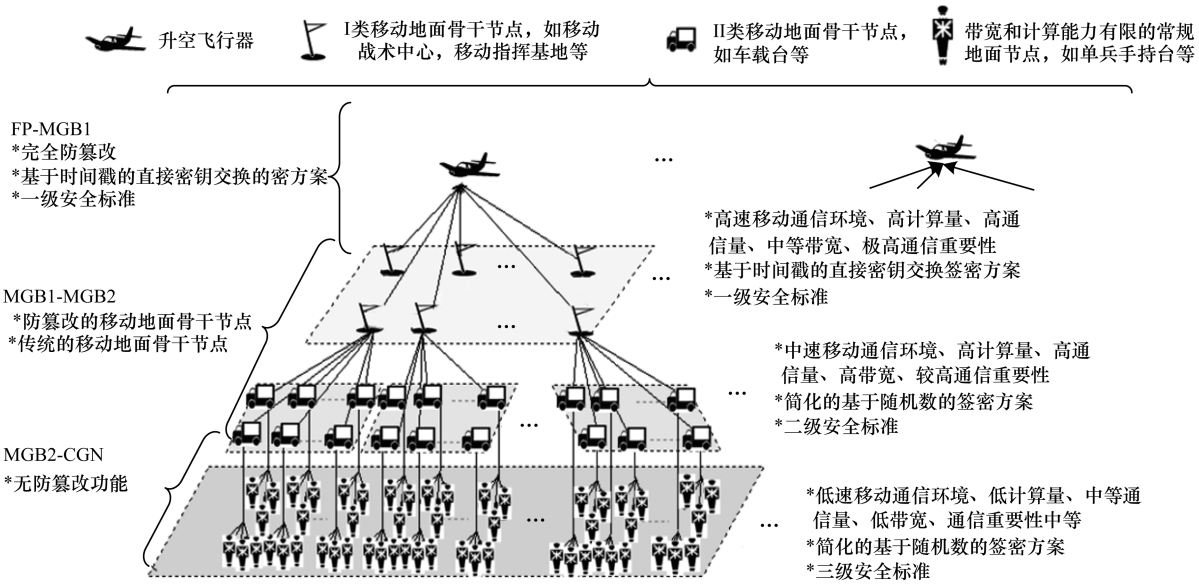

图 1 军用 Ad Hoc 网络层次结构及相应安全协议

本文在设计加密算法和密钥管理方案时考虑了 MGB 层的异构性。FP 的重要程度非常高,一般需要具有防篡改(Tamper Resistant Property,TRP)功能[14]。TRP 功能可由自毁机制或者特别的能够保护证书和加密密钥内容的硬件提供。一般 MBG1 因重要程度较高,也具有 TRP 功能。

如图 1 所示,“升空飞行器到 I 类移动地面骨干节点层(FP-MGB1)”包括了无人机等 FP 到具有扩展通信能力的 MGB 之间的通信(如移动战术中心、移动指挥基地)等,这些单元有足够的能力拥有 TRP 功能。FP 除了桥接不同的 MBG1 簇外,主要负责密钥分发和证书处理。由于直接与 FP 相连的 MGB1 数量有限,因此不需要考虑 FP 的存储和计算负载的问题。“I 类到 II 类移动地面骨干节点层(MGB1-MGB2)”是协议的第 2 层。MBG2 通常是比 CGN 有着更高通信能力的移动通信单元,比如武装车辆等。在不能获取 MGB1 时,MGB2 可以执行 MGB1 的功能,采用门限密码技术可解决证书的可信问题。“II 类移动地面骨干节点到常规地面节点(MGB2-CGN)层”是协议的第 3 层。每个 MBG2 控制着多个 CGN。在该层,根据不同的 CGN 需求配置不同的加密技术。

3 密钥技术和安全体系结构

3.1 SRS 方案

数据的机密性、完整性以及前向后向保密性是军用 Ad Hoc 网络的 3 个核心安全需求。在网络信道上实现既加密又得到签名认证的信息传输可保障安全,但传统的“先签名后加密”策略,耗费的通信和计算代价较高,不适用于战术环境下的移动 Ad Hoc 网络。因此,需要采用更为高效的算法,在保证安全需求的同时降低计算和传输代价。

本文对 DKEUTS[15-16] 技术进行改进。作为一种重要的加密技术,DKEUTS 方案可同时完成安全加密和数字签名,比先签名再加密方案的计算代价要小。本文将 DKEUTS 方案应用在第 1 层的 FP 和 MGB1,因为这 2 类节点不需要过多考虑计算和带宽耗费问题。而对于 MGB2 和 CGN,由于其计算、通信能力有限,本文对 DKEUTS 方案进行缩减,提出 SRS 方案。在该方案中,随机数被用来替代时间戳表明消息的时新性的同时,也作为签密三元组计算的重要参数。采用随机数的方案不仅避免了网络中

时钟难以同步带来的问题,也可以认证签名计算值、防范重放攻击。由于其可以随时在系统内部进行调整(设置随机算法参数和随机数位数),能增强系统抗截获能力。在 SRS 方案中需要用到符号和 DKEUTS 方案类似,如下所示。

p:发送双方已知的一个较大的质数。

q:$p-1$ 的一个较大的质数因子,$q|(p-1)$。

g:元素个数为 $p-1$ 的有限群$[1,2,\cdots,p-1]$内的一个整数。

x_a:发送方的私钥,随机从$[1,2,\cdots,p-1]$内选择,且 $x_a \nmid (p-1)$。

y_a:发送方的公钥,$y_a = g^{x_a} \bmod p$。

x_b:接收方的私钥,随机从$[1,2,\cdots,p-1]$内选择,且 $x_b \nmid (p-1)$。

y_b:接收方的公钥,$y_b = g^{x_b} \bmod p$。

SRS 方案分为 2 步:

1)发送方对消息 m 进行密签,具体步骤如下:

(1)发送方从$[1,2,\cdots,p-1]$中选择一个随机数 x,并计算哈希值 $k = H(y_b^x \bmod p)$,并以合适的长度将哈希值 k 划分为 k_1 和 k_2。

(2)计算 $r = KH_{k_2}(m)$。

(3)计算 $s = x/(r + x_a)$。

(4)计算 $c = E_{k_1}(m)$。

(5)发送方向接收方发送签密三元组(c,r,s)。

2)接收方对消息 m 进行解密签,具体步骤如下:

(1)接收方利用接收到的文本(c,r,s),根据公开的参数 p、q、g,以及接收方自身的私钥 x_b,发送方的公钥 y_a,进行解密签,计算公式如下:

$$k = (y_a \cdot g^r)^{s \cdot x_b} \bmod p$$

(2)用发送方和接收方都已知的合适的长度将 k 分为 k_1 和 k_2。

(3)计算 $m = D_{k_1}(c)$。

(4)如果接收方经过判断得到 $KH_{k_2}(m) = r$,接收方将认为 m 为有效的由 Alice 发送的消息。

上述步骤的证明,即证明接收方可以根据已知参数集(c,r,s,p,q,g,x_b,y_a),计算得到 $H((y_a \cdot g^r)^{s \cdot x_b} \bmod p)$ 等于发送方计算的 $H(y_b^x \bmod p)$,也就是证明:

$$(y_a \cdot g^r)^{s \cdot x_b} \bmod p = y_b^x \bmod p$$

将 $y_a = g^{x_a} \bmod p$ 代入,得:

$$\begin{aligned}
\text{左式} &= (g^{x_a} \bmod p \cdot g^r)^{x/(r+x_a) \cdot x_b} \bmod p = \\
&(g^{x_a} \cdot g^r \bmod p)^{x/(r+x_a) \cdot x_b} \bmod p = \\
&(g^{x_a + r} \bmod p)^{x/(r+x_a) \cdot x_b} \bmod p = \\
&g^{(x_a+r) \cdot x \cdot /(r+x_a) \cdot x_b} \bmod p = g^{x \cdot x_b} \bmod p
\end{aligned}$$

$$\text{右式} = y_b^x \bmod p = g^{x \cdot x_b} \bmod p$$

左式 = 右式,由此证明接收方可以恢复发送方用于签名和加密的 k。

签密方案协议效率如表 1 所示。对于军用 Ad Hoc 网络,尤其是主要由 CGN 构成的末端 Ad Hoc 网络,节点计算、通信能力有限,因此协议效率问题非常关键。由于加解密操作和消息长度有关,且加解密操作始终不可避免,因此要提高协议效率,需要尽量减少哈希函数计算和模数计算规模。SRS 方案依然采用加密哈希计算和模数计算保证安全性。对于传递的签密文本中的 s,必须同时截获发送方私钥和发送方自选随机数 x,才可能恢复 r。而 r 又利用了加密哈希函数的单向性,保证了发送消息的安全性。同时加密哈希函数参数 k_2 的安全性是由解离散对数问题的困难性来保证。从而 SRS 方案在减少计算量的同时保证了算法安全,应用在战场末端计算能力有限的无线通信节点上,其效率将体现得更加明显。

表 1　签密方案协议效率

通信端	DKEUTS 方案	SRS 方案
发送方	2 次模数计算,2 次哈希计算,1 次加密计算	1 次模数计算,2 次哈希计算,1 次加密计算
接收方	1 次模数计算,1 次哈希计算,1 次解密计算	1 次模数计算,1 次哈希计算,1 次解密计算
通信双方	3 次模数计算,3 次哈希计算,2 次加/解密计算	2 次模数计算,3 次哈希计算,2 次加/解密计算

3.2　多层级安全防护方案

在第 1 层(FP 层)和第 2 层(MBG1 层),需要高度安全保护(至少需要 256 bit 的哈希函数保证单向性),所以采用 DKEUTS 方案,称第 1 层、第 2 层采用的安全标准为“一级安全标准”。SRS 方案比 DKEUTS 方案减少分组密码、哈希函数和公钥密码参数的比特位数,降低了安全级别并减少了计算量,将其应用于第 3 层(MBG2)和第 4 层(CGN)。第 3 层的安全需求虽然低于第 1 层和第 2 层,但仍然很高,称这种安全级别为“二级安全标准”。第 4 层的 CGN 通信能力更弱,通信密度更高且通信的范围更小,因此,密钥算法需要更高速率、更低计算和存储需求。在该层中,SRS 方案可以进一步降低加密哈希函数和密码参数的位数,以提高计算效率,称该层安全标准称为“三级安全标准”。

4　网络连通度恢复策略

军用 Ad Hoc 网络节点移动或受干扰攻击影响均可能导致拓扑变化,需要对网络可靠性进行提前预测,进而实施拓扑控制、优化等恢复策略,维持网络连通,保证路由协议良好生命期。网络可靠性一般用网络持续执行预定功能的可能性来衡量,即需要保证网络运行时间内一定的网络连通度,维持可用性。

并非所有节点在维持网络可靠性过程中具有同等重要的拓扑控制作用,需要在存在无线干扰攻击和节点动态移动环境中,找到对网络拓扑变化和网络连通度起决定性作用的重要节点,即网络割点。

这些重要节点的密度、分布情况与邻居节点链路鲁棒性决定了网络的脆弱程度。

以时段$[T_0, T_W]$内网络性能测试为例，给出某 Ad Hoc 网络的多跳无线组网的逻辑拓扑图，根据节点间链路连接强度，判别网络中节点和链路受干扰和拓扑变化影响的大小，得到强依赖度链路和可靠转发节点的大致逻辑分布情况，如图 2 所示。

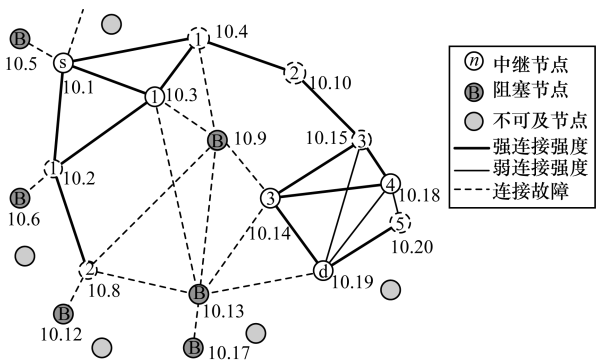

图 2 网络拓扑示意图

节点度用来评判节点重要性，节点度越大的节点重要程度越高。将受攻击干扰影响发生链路阻塞或因移动脱网后，可能引发网络割裂得节点设定为阻塞节点。如果该阻塞节点造成网络分割，即判定为网络割点。在图 2 中，处于网络边界外围的节点 10.5、10.6、10.12、10.17 发生链路阻塞而脱网成为阻塞节点，对剩余网络连通性影响不大，将网络边界收缩，即可保证剩余网络连通度。如果节点 10.9、10.13 成为阻塞节点，此时剩余网络连通性取决于节点 10.4、10.2，一旦其阻塞，将导致网络完全割裂成 2 个部分。此时节点 10.4 的节点度为 3，节点 10.2 的节点度为 3，而节点 10.18 节点度为 4，但即使 10.18 受干扰，并不影响网络其他节点连通性能，不会成为网络割点。因此，仅根据节点度来评判节点重要性以及是否可能成为网络割点并不合理，需要综合判断节点一跳近邻的状态。本文提出一种判别节点重要度方案，选取阻塞节点集合，计算去除某节点对网络拓扑的影响，影响越大则节点重要度越高。若重要节点数目较多，则说明网络脆弱程度较高，需要及时调整网络拓扑结构。具体的计算步骤为：

1）计算节点 x 的节点度。若节点度小于 2，则标记该节点此时为边界节点；否则执行步骤 2。

2）判断节点 x 的一跳近邻节点 $Nbr(x)$ 是否存在边界节点。若存在边界节点，则判断 x 为边界邻接节点，退出计算；否则其不为边界邻接节点。

3）判断一跳近邻节点的邻接节点集合除 x 外是否存在空集。若存在空集，则判断节点 x 为重要节点；否则 x 不是重要节点。

一旦节点标记为重要节点，说明当该处链路质量较差时，其可能成为网络割点，因此须对网络连通度变化进行预测。恢复网络可靠性的方案有：网络割点的邻居节点通过调整发射功率或移动路线控制改变拓扑结构，以最大程度减少能耗；通过在网络割点处增加冗余备份节点或增加冗余链路改善拓扑，消除单点故障或链路失效的影响。具体的网络拓扑重构手段限于篇幅，本文不再赘述。

5 军用 Ad Hoc 网络安全协议性能分析

本文所提军用分层 Ad Hoc 网络的安全性和可靠性，与 DKEUTS 与 SRS 方案的安全性直接相关。DKEUTS 方案提供了机密性、认证、完整性和不可否认性，其消息的时新性由时间戳提供。与传统的先签名再加密方案 RSA[9] 相比，DKEUTS 方案节省了 58% 的计算开销和 78% 的通信开销。SRS 方案同样提供了机密性、认证、完整性和不可否认性，其消息的时新性由随机数提供。该方案采用随机数替代时间戳，不仅避免了网络中时钟难以同步带来的问题，也可防范重放攻击，并且自适应更改随机数生成算法和随机数位数等手段更可提高系统抗截获能力。与 DKEUTS 方案相比，由于节省了模数计算开销，具有计算优势，可提高战场移动节点签名加密效率，适用于性能受限的常规战场通信节点。本文还提出一种基于网络割点预测的网络连通度恢复策略，为网络拓扑重构提供技术支撑。

6 结束语

本文提出一种分层的军用 Ad Hoc 网络体系结构和 SRS 方案。利用加密哈希函数的单向性和解离散对数问题的困难性保证协议的安全性，减少计算规模。根据不同层次节点重要程度、通信和计算性能等，分别应用不同的安全策略，在保证网络可靠性和安全性的基础上，提高网络效率。本文提出的分层网络架构和安全协议适用于节点非同构的军用 Ad Hoc 网络或其他民用多跳无线网络。下一步将结合网络层的安全路由、抗干扰路由、拓扑自适应重构等技术，验证和分析不同安全威胁和恶意干扰场景下的协议效率问题，减少信息数据泄露、路由暴露以及网络被恶意中断的风险，保证网络整体的安全性和鲁棒性。

参考文献

[1] ELMASRY G F. Tactical wireless communications and networks design concepts and challenges[M]. New York, USA: Wiley Publishing, 2012.

[2] 贾华杰，鲜明，陈永光. 网络中心战及其新技术[J]. 国防科技，2011，32(4)：44-49.

[3] HARRIS A C I. Effects-based operations: applying network centric warfare in peace, crisis, and war[J]. Naval War College Review, 2011, 57(2): 180-181.

[4] BURBANK J L, CHIMENTO P F, HABERMAN B K, et al. Key challenges of military tactical networking and the elusive promise of MANET technology[J]. IEEE Communications Magazine, 2006, 44(11): 39-45.

[5] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

（下转第 198 页）

本文方案计算复杂度较低,签名长度较短,在运算效率方面更有优势。

8 结束语

本文对无证书签名定义进行改进,并在此基础上提出一种随机预言机模型下可证安全的无证书短签名方案。本文方案在用户生成秘密值的同时计算用户的部分公钥,并在提取部分私钥时将用户身份与用户部分公钥进行关联,从而建立用户公钥与用户之间的认证关系。将本文方案与经典短签名方案以及相关无证书短签名方案进行运算效率的比较,结果表明,本文方案的性能较好,计算复杂度较低,能够满足实际应用的需求。

参考文献

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Proceedings of Workshop on the Theory and Application of Cryptographic Techniques. Berlin, Germany: Springer, 1984: 47-53.

[2] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing [C]//Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2001: 514-532.

[3] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography [C]//Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Germany: Springer, 2003: 452-473.

[4] GORANTLA M C, SAXENA A. An efficient certificateless signature scheme [C]//Proceedings of International Conference on Computational and Information Science. Berlin, Germany: Springer, 2005: 110-116.

[5] 明洋,詹阳,王育民,等. 一个改进的无证书签名方案[J]. 西安电子科技大学学报,2008,35(6):1094-1099.

[6] 徐晓琴,卢辉斌. 可证明安全的无证书短签名[J]. 电子技术,2009,46(4):56-58.

[7] 魏春艳,蔡晓秋. 标准模型下的高效无证书短签名方案[J]. 计算机工程,2012,38(13):119-121.

[8] TSO R, HUANG Xinyi, SUSILO W. Strongly secure certificateless short signatures [J]. Journal of Systems and Software, 2012, 85(6): 1409-1417.

[9] FENG Shurong, MO Jiao, ZHANG Hua, et al. Certificateless short signature scheme from bilinear pairings [J]. Applied Mechanics and Materials, 2013, 380/381/382/383/384: 2435-2438.

[10] 黄茹芬. 一个高效的基于证书的短签名方案[J]. 计算机应用与软件,2014,31(6):312-314.

[11] TSAI J. A new efficient certificateless short signature scheme using bilinear pairings [J]. IEEE Systems Journal, 2015, 11(4): 2395-2402.

[12] 汤永利,王菲菲,闫玺玺,等. 高效可证明安全的无证书签名方案[J]. 计算机工程,2016,42(3):156-160.

[13] HUNG Y, TSENG Y, HUANG Senshan. A revocable certificateless short signature scheme and its authentication application[J]. Informatica, 2016, 27(3): 549-572.

[14] 周彦伟,李骏. 可证安全的高效无证书签名方案[J]. 陕西师范大学学报(自然科学版),2017,45(5):17-22.

[15] 陈亚萌,程相国,王硕,等. 基于双线性对的无证书群签名方案研究[J]. 信息网络安全,2017(3):53-58.

编辑 刘盛龄

(上接第 192 页)

[6] JHARBADE N K, SHRIVASTAVA R. Network based security model using symmetric key cryptography (AES 256-Rijndael algorithm) with public key exchange protocol (Diffie-Hellman key exchange protocol)[J]. International Journal of Computer Science, 2012, 12(8): 69-73.

[7] 陈少华,樊晓光,禚真福,等. 一种基于身份的 Ad Hoc 优化密钥管理方案[J]. 计算机工程,2016,42(4):131-142.

[8] RACHEDI A, BENSLIMANE A. Security and pseudo-anonymity with a cluster-based approach for MANET[C]// Proceedings of Global Telecommunications Conference. Washington D.C., USA: IEEE Press, 2008: 1-6

[9] VODNALA D, KUMAR S P, ALUVALA S. An efficient backbone based quick link failure recovery multicast routing protocol[J]. Perspectives in Science, 2016, 8: 135-137.

[10] 孙斌. 移动自组网密钥管理体系的研究[D]. 北京:北京邮电大学,2009.

[11] ZHENG Yuliang. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)[C]//Proceedings of Annual International Cryptology Conference. Berlin, Germany: Springer, 1997: 165-179.

[12] PINTSOV L A, VANSTONE S A. Postal revenue collection in the digital age [C]//Proceedings of International Conference on Financial Cryptography. Berlin, Germany: Springer, 2000: 105-120.

[13] PEI Guangyu, LY H, GERLA M, et al. Hierarchical routing for multi-layer Ad-Hoc wireless networks with UAVs[C]// Proceedings of IEEE Military Communications Conference. Washington D.C., USA: IEEE Press, 2002: 310-314.

[14] IYER R K, DABROWSKI P, NAKKA N, et al. Reconfigurable tamper-resistant hardware support against insider threats: the trusted ILLIAC approach [M]// STOLFO S J, BELLOVIN S M, KEROMYTIS A D, et al. Insider Attack and Cyber Security. Berlin, Germany: Springer, 2008.

[15] YAVUZ A A, ALAGOZ F, ANARIM E. HIMUTSIS: hierarchical multi-tier adaptive ad-hoc network security protocol based on signcryption type key exchange schemes [C]// Proceedings of International Symposium on Computer and Information Sciences. Berlin, Germany: Springer, 2006: 434-444.

[16] AMIN R, BISWAS G P. A secure light weight scheme for user authentication and key agreement in multi-gateway based wireless sensor networks [J]. Ad Hoc Networks, 2015, 36: 58-80.

编辑 刘盛龄