doi:10.3969/j.issn.1001-893x.2013.11.018

4G移动通信系统中协作通信的安全缺陷分析*

李 娜[1,**],王 盛[2],李 鸥[1]

(1.信息工程大学 信息系统工程学院,郑州 450001;2.信息工程大学 导航与空天目标工程学院,郑州 450001)

摘 要:4G移动通信系统引入的协作通信技术在提高系统性能的同时也带来了新的安全隐患。从挖掘协议安全缺陷出发,通过分析4G系统的安全协议和机制,讨论了系统中存在的安全缺陷,总结了可能遭受的攻击方式,并以此为基础给出了一种规避针对4G系统协作通信攻击的身份认证机制,该机制能够有效改善4G移动通信系统协作环境下的安全性。

关键词:4G;协作通信;空中接口;安全缺陷;身份认证

中图分类号:TN915.08 **文献标志码**:A **文章编号**:1001-893X(2013)11-1500-06

Analysis of Security Flaw in Cooperative Communication of 4G Mobile System

LI Na[1], WANG Sheng[2], LI Ou[1]

(1. College of Communication Engineering, Information Engineering University, Zhengzhou 450001, China;
2. College of Navigation and Space Target Engineering, Information Engineering University, Zhengzhou 450001, China)

Abstract: Cooperative communication technology that is introduced into the 4th generation (4G) mobile communication system can bring new security hazards while improving system performance. Starting with excavating security flaws of protocols, this paper discusses security flaws in system by analyzing the security protocols and mechanisms of 4G system, summarizes the possible attack modes, and on this basis provides an authentication mechanism to avoid attack aiming at cooperative communication in 4G system. This mechanism can improve effectively security in the cooperative environment of 4G system.

Key words: 4G; cooperative communication; air interface; security flaw; authentication

1 引 言

随着信息技术的高速发展,移动通信已成为全球用户数量最大、普及率最高、使用最为广泛的通信手段。当前,第三代移动通信(3G)系统的大规模应用已全面普及,3G-LTE正在迅速推进,预计2014年投入商用。作为准4G系统,3G-LTE被业界称为3.9G移动通信系统,其核心技术已能初步体现4G特征,除能提供3G所有的业务之外,更有跨越式提高,数据带宽可达100 Mb/s,而未来的4G移动通信,其终端的数据带宽则能达1 000 Mb/s[1]。

为了达到更高的数据速率,移动通信系统所使用的频段也越来越高,因而无线信道所特有的衰落特性、信号传播路径上的遮挡等因素对通信系统可靠性和有效性的影响更加明显。

为了对抗无线信道的衰落,提高系统的传输可靠性,在无线通信系统中广泛使用分集技术。多输入多输出(Multi Input Multi Output,MIMO)系统通过发送端和/或接收端配置的多根天线,可以实现空间分集,并且可以有效地提高系统的频谱效率和数据传输速率[2],已经被认为是新一代无线通信系统的关键技术之一。然而令人遗憾的是,在实际无线通信系统中,通常只在基站端配置多根天线,而对于移

* 收稿日期:2013-09-24;修回日期:2013-11-20 Received date:2013-09-24;Revised date:2013-11-20
** 通讯作者:pilimao64444@163.com **Corresponding author**: pilimao64444@163.com

动终端,由于受到体积、重量、功耗及成本等方面的限制,在其上配置多根天线难以实现。为了解决这个问题,实现移动终端的发送分集,产生了一种新的空间分集形式——协作分集。分集增益通过网内移动终端的相互协作获得:网内多个移动终端组成协作伙伴,协作伙伴之间对数据进行中继转发,即每个移动终端都不仅发送自己的信息,还要发送协作"伙伴"的信息。通过使用"伙伴"的天线来发送经历独立衰落的副本,从而使单天线的移动终端也可以实现空间分集。目前,协作分集主要以协作中继的方式应用于现有系统中。其中,WiMAX 系统于 2009 年在 IEEE 802.16j 协议版本中引入了协作中继技术,4G LTE Advanced 于 2008 年在 3GPP R1-82975 中引入了协作中继技术,这意味着协作中继技术开始正式启动其商用化进程。

尽管先进移动通信系统中纷纷引入了协作通信技术,却仍然没有形成有效的安全机制来约束通信节点在协作通信中的行为。本文将结合 LTE、LTE Advanced 系统,对引入协作通信后的通信过程中所存在的安全缺陷展开分析。为叙述方便,后文将引入了协作通信技术的移动通信网络简称为移动协作通信网。同时,本文仅讨论空中接口所存在的安全缺陷。

2　4G 系统空中接口上的主要安全机制

4G 移动通信系统为保持与 LTE 系统的完全兼容,在设计上沿用了 LTE 系统的安全机制,主要包括身份保密机制、双向鉴权和密钥协商机制、信令完整性保护机制和信令/数据加密机制[3]。这些安全机制保证了常规移动通信系统的安全运行,保护用户身份不被恶意用户冒用,用户通信不会遭到非法用户的窃取。

2.1　身份保密机制

用户身份信息属用户的个人隐私信息,同时作为用户接入网络、使用网络资源的凭据,受到系统的严格保护。为达到保护用户身份信息的目的,从 2G 移动通信系统开始,3GPP 协议就规定了有关使用临时身份标识(TMSI)替代永久身份信息(IMSI)的相关内容。在 4G 系统中,采用全球唯一临时标识(Global Unique Temporary Identity,GUTI)作为用户临时身份[4]。GUTI 由 MME(Mobility Management Entity)分配给用户,仅在所属 MME 范围内有效。与 TMSI 类似,GUTI 也是与用户 IMSI 绑定的。

在 4G 系统中,MME 向用户分配 GUTI 的过程被称为"再分配",如图 1 所示。

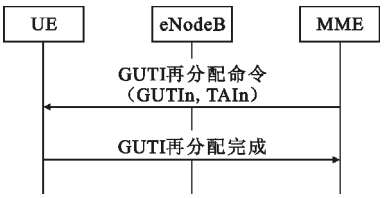


图 1　GUTI 再分配过程
Fig. 1 GUTI reallocating process

GUTI 的再分配过程是由 MME 发起的[5],在该过程中,MME 向 UE(User Equipment)发布一对新的临时用户身份 GUTIn/TAIn 用以在无线链路上标识用户身份,其中,TAI(Tracking Area Identity)是跟踪区域标识,用于标识用户当前所处区域。GUTIn 的生成是随机的、不可预测的,是与用户 IMSI 相关联的。用户收到新的 GUTI 后,需要撤销原 GUTI 与 IMSI 的关联关系,并建立新 GUTI 与 IMSI 的关联关系,然后向 MME 发送 GUTI 再分配完成消息。

当 UE 进行开机等操作时,网络中不存在用户永久身份与临时身份的匹配关联关系。此时,网络将请求使用用户永久身份 IMSI 来标识用户身份。该过程如图 2 所示。

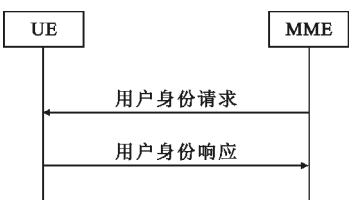


图 2　永久身份标识 IMSI 的识别机制
Fig. 2 Indentifying mechanism of IMSI

值得注意的是,在该过程中,用户永久身份标识 IMSI 是采用明文方式在空中接口上传输的,因此 IMSI 可能在该过程中被泄露。

2.2　双向鉴权和密钥协商机制

身份认证和密钥协商一直是移动通信系统中十分重要的安全机制。从 3G 系统起,移动通信系统开始采用双向鉴权的方式为用户和网络提供双向的身份认证,确保通信实体的真实性和可靠性,防止第三方恶意用户的攻击。而密钥协商机制则为通信双

方提供了加密方式的选择途径,以确保通信双方均可实现对通信内容的加密,保护业务数据[6]。为实现系统的平滑升级,4G 系统的双向鉴权和密钥协商机制沿用了 3G 的 AKA(Authentication Key Agreement)机制改进而来[7]。不同之处在于,HSS 将 128 位的密钥与网络身份一同生成了 256 位的 KASME,并在 AUTN 中增加了认证管理域(Authentication Management Field,AMF)。当 AMF 为 1 时,表明接入的是 4G 网络,执行 LTE AKA 机制;否则,执行 3G AKA 机制。

2.3 信令完整性保护机制

信令完整性保护机制是从 3G 起引入的安全机制,用于防止空中接口上传输的信令遭到恶意篡改。完整性保护机制是根据数据传输中信令数据的内容使用特定的数据完整性保护算法,向信令中添加完整性保护域,以便接收端通过对完整性保护域的检查来确认该信令是否合法[3]。通过该机制,可以有效避免来自攻击者对空中接口上传递的信令的篡改。完整性保护机制的实现方法如图 3 所示,其中,KEY 为加密密钥,长度为 128 b;COUNT 为加密计数器,长度为 32 b;BEARER 为无线信道标识,长度为 8 b;DIRECTION 为方向标识,长度为 1 b,用于指示上行(0)或下行(1);MESSAGE 为传递的消息。

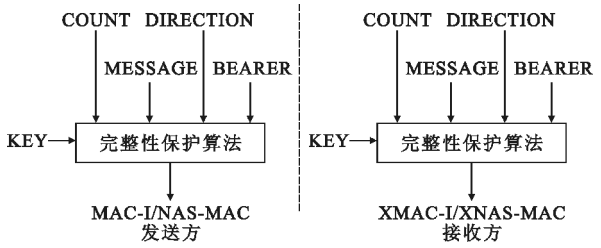


图 3 完整性保护算法实现方法

Fig. 3 Realization method of integrity protection algorithm

需要注意的是,信令完整性保护只保持对控制面的保护,而对用户面的数据并不提供保护。

2.4 信令/数据加密机制

信令在受到完整性保护的同时,大部分信令还受到加密算法的保护。同时,用户数据由于涉及到用户的隐私信息,不适宜采用明文传递,因此,用户数据也受到加密算法的保护。但需要指出的是,协议中所规定的加密算法是可选项,信令和用户数据是允许以明文方式在空中接口上传输的。加密机制的实现方法与完整性保护的实现方式基本一致,在此不再赘述。

3 移动协作通信网安全缺陷和攻击方式分析

移动协作通信网与传统的移动通信网络最大的不同之处在于,它引入了移动终端与终端之间、终端与中继转发节点之间的协作,改变了移动通信系统的网络结构。全新的网络形式带来了新的安全缺陷,也必将导致针对新型网络攻击方式的产生。

3.1 安全缺陷分析

传统的移动通信系统中,UE 单纯和 NodeB 相连,UE 间没有任何直接的数据交互,网络采用层次化的体系结构,并具有稳定的拓扑结构。同时,传统无线通信网络提供了多种服务以充分利用网络的现有资源来实现安全策略,如加密、认证、访问控制、防火墙和权限管理等,因此,某个恶意的用户很难对其他 UE 进行有效的攻击。而在移动协作通信网中,由于 UE 与其他 UE 或中继节点间存在协作关系,使得网络拓扑结构不断变化,产生了信息传输路径的不确定性,加上信息在进入 eNodeB 之前无法采用路由器、防火墙等设备对信息进行保护,在传统网络中能够较好工作的安全机制也不一定适用于移动协作通信网,故与传统移动通信系统相比,新型网络更易遭受攻击。针对新型网络可能的攻击方式主要出现在网络功能、动态拓扑、路由协议等 3 个方面。

(1)网络功能

由于移动协作通信网的主要功能是完成用户间的协作通信,因此通信发起用户的信息和数据必然通过其他用户进行中继和转发。在此过程中,恶意用户可以通过伪装成中继节点的方式对发送方的数据进行截获、侦听、篡改等攻击而不被发现。

(2)动态拓扑

移动协作通信网中节点的位置是不固定的,可随时移动,造成网络拓扑结构不断变化。一条正确的路由可能由于目的节点移动到通信范围之外而不可达,也可能由于路由途经的中间节点移走而中断。因此,难以区别一条错误的路由是因为节点移动还是虚假路由信息造成的。由于节点的移动性,在某处被识别的恶意节点移动到新的地点或改变标识后,它可重新加入网络而不被识别。另外,由于动态的拓扑结构,网络没有边界,防火墙也难以应用。

(3)路由协议

路由协议的实现是另一个安全弱点。路由算法

一般都假设网络中的所有节点是相互合作的,共同去完成网络信息的传递。如果某些节点故意去恶意地广播虚假路由信息,或散布大量无用数据,可能会导致整个网络的崩溃。另一方面,如果某些节点为节省自身资源而拒绝为其他节点转发数据,也将影响整个网络的性能。

3.2　攻击方式分析

针对网络特点,新型网络可能遭到的攻击方式有 8 种[8],下面分别介绍。

(1)侦听

任何无线通信系统都可能遭到侦听攻击。移动协作通信网采用无线信号作为传输媒介,其信息在空中传播,攻击者只需要从空中接口接收信号并将之还原,即可获取发送方的信息。

(2)干扰

干扰是一种简单而有效的物理层攻击方式。攻击者不需要加入网络,只要检测出网络节点所使用的发送和接收信息的频率,连续发送干扰信号,就能够有效地阻塞节点之间的正常通信。

(3)中间人

通常,总是假定网络中的节点都是相互合作的,转发报文的节点不会修改与其无关的任何信息,所以不检查信息的完整性和有效性。这使得攻击者能够十分容易实现中间人攻击,更改报文中的任意字段和数据,或向其中注入任意内容,从而产生错误的信息,导致网络性能下降或接收方接收到错误信息。导致篡改攻击的根本原因在于节点没有对转发的报文进行完整性检测。应对这种攻击的方法一般是对报文进行完整性验证。

(4)假冒

如果移动协作通信网所采用的路由协议不认证报文发送方的身份,攻击者将有机会声明其为某个合法节点,并以其身份加入网络发起通信,甚至屏蔽该合法节点并利用其身份接收报文。应对这种攻击的方法一般是在网络节点之间实现身份认证机制。

(5)伪造

攻击者可以伪造并发送任何信息,如路由信息、虚假通信内容等。应对虚假通信内容的方法同假冒攻击一样,一般是在网络节点之间实现身份认证机制。但要检测出虚假路由信息则比较困难,因为要随时掌握移动协作通信网络全局的连通状态,才能够辨识某节点发出信息的真伪。

(6)资源消耗

攻击者发送大量无用的报文,如路由查询报文或数据报文,消耗网络和节点资源,如带宽、内存、处理器、电池等,导致被攻击网络或用户迅速消耗可用资源,实现拒绝服务攻击的目的。

(7)重放

重放攻击又称重播攻击、回放攻击或新鲜性攻击(Freshness Attacks),是指攻击者发送一个目的节点已接收过的包,来达到欺骗系统的目的,主要用于身份认证过程,破坏认证的正确性。这种攻击会不断恶意或欺诈性地重复一个有效的数据传输,可以由传输发起者进行,也可以由拦截并重发该数据的敌方进行。攻击者利用网络监听或者其他方式盗取认证凭据,之后再把它重新发给认证服务器。加密可以有效防止会话劫持,却防止不了重放攻击。重放攻击在任何网络通信过程中都可能发生。应对这种攻击的方法一般采用时间戳、消息序号和提问-问答等。

(8)位置信息泄露

由于移动协作通信网中节点的协作关系,节点能够为其他节点转发信息。攻击者可以构造带有特殊标记的信息,通过向被攻击者不断发送协作请求,使被攻击者不断发送这些特殊信息内容,从而利用无线信号定位技术解算出被攻击者的地理信息,造成位置信息泄露。

4　移动协作通信网攻击的规避方法

通过分析移动协作通信网可能遭到的攻击方法可以发现,除侦听、干扰和定位外,空中接口上实施的攻击全部是基于欺骗的攻击,而这些攻击方式利用的都是新型网络难以对攻击者实施身份认证这一特点。因此,可以考虑设计一种适用于移动协作通信网节点间的身份认证机制,来避免上述攻击。

考虑到移动协作通信网构建于移动通信网络之上,因此,移动协作通信网节点间的身份认证协议也应当采用其承载网所采用的安全机制,避免给网络和节点带来新的负载。为此,以下描述一种基于 LTE 系统双向鉴权、完整性保护和加密机制的协作身份认证机制。

由于移动协作通信网的各节点能够与基站通信,可利用基础网络设施作为安全中心,故其身份认证机制可基于已有的双向鉴权机制展开。设计移动

协作通信网的身份认证机制如图 4 所示(以一次协作通信为例)。

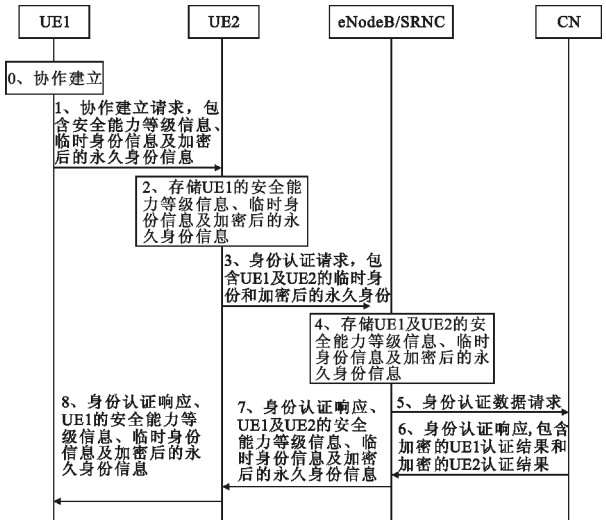


图 4 移动协作通信网鉴权流程图

Fig. 4 Authentication flow chart of mobile cooperative communication network

假设 UE1 选择 UE2 作为其协作通信的伙伴。

(1)首先,UE1 向 UE2 提出协作建立请求,并发出协作建立请求消息。在协作建立请求中,包含 UE1 所支持的加密算法、完整性保护算法等安全能力等级信息,并包含其临时身份标识 TMSI 和利用其在接入移动通信网时选定的加密算法加密的永久身份信息。

(2)UE2 收到协作建立请求后,先在本地保存一个 UE1 的安全能力等级信息、临时身份信息和加密后的永久身份信息的副本,然后向核心网提出身份认证请求。在该请求中除提交 UE1 的相关安全信息外,同时提交自己的身份信息和相关安全信息。

(3)eNodeB 收到 UE2 的身份认证请求后,同样先保存 UE1 和 UE2 安全信息的副本,然后向核心网提交身份认证数据请求。

(4)核心网验证收到的身份信息,并根据 UE1 和 UE2 正在使用的加密方式分别加密身份认证结果,即用 UE1 正在使用的加密算法加密 UE2 的认证结果,用 UE2 正在使用的加密算法加密 UE1 的认证结果。

(5)eNodeB 收到身份认证响应后,用 UE1 支持的加密算法加密 UE1 的安全能力等级信息副本,用 UE2 支持的加密算法加密 UE2 的安全能力等级信息副本,并将其附在认证响应信息末尾发送给 UE2。同时发送给 UE2 的还有选定的加密算法和完整性保护算法,并在此步骤启动对信令的完整性保护。

(6)UE2 接收到身份认证响应消息后,首先根据选定的完整性保护算法验证消息的合法性,然后解密认证消息中有关自己安全能力等级信息副本的数据,验证是否与自己发送的内容相符。若相符,表明鉴权信息没有遭到篡改,网络合法,则继续解密 UE1 的认证结果。若 UE1 的认证结果为通过,则表明 UE1 身份合法,UE2 记录选定的加密算法和完整性保护算法,并继续向 UE1 发送认证响应消息;否则,发送认证失败消息。

(7)UE1 收到认证响应消息后,与 UE2 的操作相同,首先验证消息的合法性,然后解密认证消息中有关自己安全能力等级信息副本的数据,再解密 UE2 的认证结果。认证通过后,身份认证完成,可以建立协作关系。

5 结束语

通过分析发现,协作通信技术的引入给新一代移动通信系统带来了安全隐患。攻击者利用这些安全隐患除可实现对用户信息的窃取外,还可能实现对用户终端和网络的攻击,导致用户终端资源急剧消耗、网络性能严重下降甚至瘫痪等严重后果。

通过增加协作通信的身份认证机制,能够有效改善协作环境下的安全性,规避基于欺骗的攻击方法带来的危害。对该方法的进一步完善,使其适用于实际网络和设备中是下一步研究的重点。

参考文献:

[1] 4G 移动通信关键技术及特征[EB/OL]. [2012-07-20]. http://www. hqew. com/tech/sheji/666185. html.
Key Technologies and Features of4G Mobile Communication[EB/OL]. [2012-07-20]. http://www. hqew. com/tech/sheji/666185. html. (in Chinese)

[2] 廖昕. MIMO 无线通信系统的跨层设计研究[D]. 北京:北京邮电大学,2010.
LIAO Xin. Research on Cross-layer Design for MIMO Wireless Communication System[D]. Beijing :Beijing University of Posts and Telecommunications, 2010. (in Chinese)

[3] 王盛, 崔维嘉, 郑娜娥. UMTS 系统空中接口接入协议的安全缺陷分析[J]. 计算机工程与应用, 2011, 47(21) : 91-94.
WANG Sheng, CUI Wei-jia, ZHENG Na-e. Analysis of Security Flaw in Access Protocol of UMTS Radio Interface [J]. Computer Engineering and Applications, 2011, 47

(21):91-94. (in Chinese)

[4] 3GPP TS 23.003(V10.1.0), Technical Specification Group Core Network and Terminals: Numbering, addressing and identification[S].

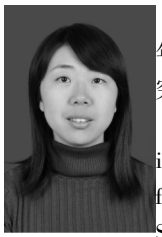
[5] 3GPP TS 23.401(V10.0.0), General Packet Radio Service(GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network(E-UTRAN) access[S].

[6] 裴胜鲁. 3G-WLAN 融合网络鉴权与密钥协商机制研究[D]. 兰州:兰州大学, 2011.
PEI Sheng-lu. Research on the AKA Mechanism in 3G-WLAN Integrated Networks[D]. Lanzhou: Lanzhou University, 2011. (in Chinese)

[7] 王丽丽. 4G 无线网络安全接入技术的研究[D]. 兰州:兰州理工大学,2011.
WANG Li-li. Research on Secure Access Technology for4G Wireless Network[D]. Lanzhou: Lanzhou University of Technology, 2011. (in Chinese)

[8] 吴义壮. LTE-Advanced 系统中 CoMP 的安全性研究[D]. 北京:北京交通大学, 2011.
WU Yi-zhuang. Research on the Security of Coordinated Multiple Point in LET-Advanced System[D]. Beijing: Beijing Jiaotong University, 2011. (in Chinese)

作者简介:



李　娜(1980—),女,山东威海人,2006 年于信息工程大学获硕士学位,现为博士研究生,主要研究方向为移动通信系统;

LI Na was born in Weihai, Shandong Province, in 1980. She received the M. S. degree from Information Engineering University in 2006. She is currently working toward the Ph. D. degree. Her research concerns mobile communication system.

Email: pilimao64444@163.com

王　盛(1984—),男,四川绵阳人,博士研究生,主要研究方向为移动通信系统;

WANG Sheng was born in Mianyang, Sichuan Province, in 1984. He is currently working toward the Ph. D. degree. His research concerns mobile communication system.

Email: wirelessmancs@163.com

李　鸥(1962—),男,河南郑州人,教授,主要研究方向为无线通信系统。

LI Ou was born in Zhengzhou, Henan Province, in 1962. He is now a professor. His research concerns wireless communication system.

Email: zzliou@126.com