一种基于空中接口和核心网协同的 LTE 系统密钥推演方法*

张文建, 彭建华, 黄开枝
(国家数字交换系统工程技术研究中心, 郑州 450002)

摘　要: 从窃听方的角度,基于空中接口与核心网协同的思想提出了一种 LTE 系统密钥推演方法。首先,在实现根密钥同步的基础上,根据空中未加密信息提供的安全算法列表,遍历有限安全算法集;然后,将遍历的安全算法与获取的父密钥共同作为参数,通过密钥生成函数生成空中接口子密钥;最后,通过比对明文和解密密文确定密钥。可行性分析表明,窃听方可以利用该方法推演出空中接口子密钥;误码率小于 10^{-3} 时,可使密钥推演成功率达到 90% 以上,具有实际应用意义。

关键词: 长期演进; 安全算法; 密钥推演; 误码率
中图分类号: TN 918.82　　**文献标志码:** A　　**文章编号:** 1001-3695(2013)09-2755-04
doi:10.3969/j.issn.1001-3695.2013.09.049

Cooperative method of key derivation for LTE systems based on radio interface and core network

ZHANG Wen-jian, PENG Jian-hua, HUANG Kai-zhi
(*National Digital Switching System Engineering & Technological Research Center, Zhengzhou* 450002, *China*)

Abstract: This paper put forward a cooperating method for key derivation based on the idea of combination of radio interface and core network. It produced the radio child-keys according to the security algorithm list provided by plain radio message and obtained parent-key, and decided the right key by comparing the plain context and the decrypted context. It proves that the correct rate of key derivation is more than 90% in the case that the symbol error rate (SER) is less than 10^{-3} according to the analysis of feasibility. Therefore it has practical application values.

Key words: long time evolution(LTE); security algorithm; key derivation; SER

LTE 的网络架构、协议体系及业务提供方式都发生了较大变化,提供了比第三代(3G)移动通信系统更好的网络性能。目前,以 LTE 为代表的超三代(B3G)和第四代(4G)移动通信网在亚太、欧洲、拉丁美洲、中东和北美等地都已开始出现商用。

与 2G 和 3G 移动通信体制相比较,LTE 的安全机制[1]和安全防护措施更加完善:引进了控制层与用户层相分离的安全分层思想;应用标志本地网络的双向鉴权机制;构建体系化的密钥结构等。目前,很多专家和学者在 LTE 系统漏洞挖掘方面进行了深入研究。文献[2,3]给出了 LTE 系统中常见的几种安全威胁:用户身份明文传输;AKA(authentication and key agreement,鉴权与密钥协商)脆弱性;异系统切换安全脆弱性等,并针对各种威胁提出了改善思路。Forsberg 等人[4]针对 LTE 系统无线接口进行了安全脆弱性分析,列举了攻击者可以获取的信息,并且阐述了 LTE 系统内应用的临时标志符可读、小区水平测量报告消息、报文序列号、错误缓存状态报告等存在的安全漏洞。MjØlsnes 等人[5]利用计算安全模型分析了 LTE AKA 协议的漏洞,并阐述了可能对 LTE AKA 造成的攻击。Fuhr 等人[6]对新近提出的 ZUC 安全算法进行研究,阐述了 LTE 系统在应用 ZUC 安全算法时会遭到简单伪造攻击的脆弱性。可见,现有文献的研究重点在于空中接口未加密消息的获取及 AKA 过程,针对鉴权之后的安全性研究相对较少。

针对这一问题,本文根据 RRC(radio resource control,无线资源控制)信令传输以及安全算法存在的漏洞,从窃听方(eavesdropper)的角度,设计了一种基于空中接口与核心网协同的 LTE 密钥推演方法。

1　LTE 系统安全流程分析

如图 1 所示,3GPP LTE 的系统由 EPC(evolved packet core,演进的核心网)、E-UTRAN(evolved UTRAN,演进后的接入网)和 UE(user equipment,用户设备)三部分组成。EPC 主要网元包括 MME(mobility management entity,移动性管理实体)和 S-GW(serving gateway,服务网关);E-UTRAN 由多个 eNB(evolved node-B,演进基站)组成。此外,HSS(home subscriber server,归属用户服务器)是存储有终端和网络相关信息的数据库,如用户签约信息、安全信息等。

LTE 系统将安全分为 AS(access stratum,接入层)安全和 NAS(non-access stratum,非接入层)安全。其中,NAS 安全是指 UE 与 MME 之间的安全,执行 NAS 信令的机密性和完整性保护;AS 安全是 UE 与 eNB 之间的安全,执行 AS 信令的加密和完整性保护,以及用户平面数据的机密性保护。

收稿日期: 2013-01-06; **修回日期:** 2013-03-09　　**基金项目:** 国家自然科学基金资助项目(61171108)

作者简介: 张文建(1987-),男,河南商丘人,硕士,主要研究方向为移动通信技术(wenjian0509@163.com);彭建华(1966-),男,教授,硕士,主要研究方向为移动通信技术;黄开枝(1973-),女,副教授,博士,主要研究方向为移动通信技术、网络信息安全.

用户要完成一次正常的业务通信过程,需要经历注册请求、AKA 和安全模式命令等过程。UE 通过 RRC 信令消息向 eNB 发起注册请求消息,与 eNB 建立联系;AKA 实现 UE 和网络的相互认证;安全模式命令用于实现密钥的分发、加密及完整性保护。UE 进入 eNB 覆盖范围之后,首先通过 RRC 信令消息向其发起注册请求消息。注册请求消息包含用户的身份信息以及 UE 的安全能力信息等。由于 LTE 采用对称密钥机制,在 AKA 过程之前,系统无法对 RRC 消息进行加密和完整性保护,因此存在关键信息泄露的风险。

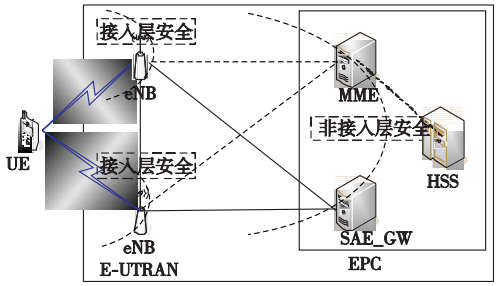

图1 LTE/SAE系统安全架构

1.1 LTE AKA 过程

AKA 过程如图 2 所示。

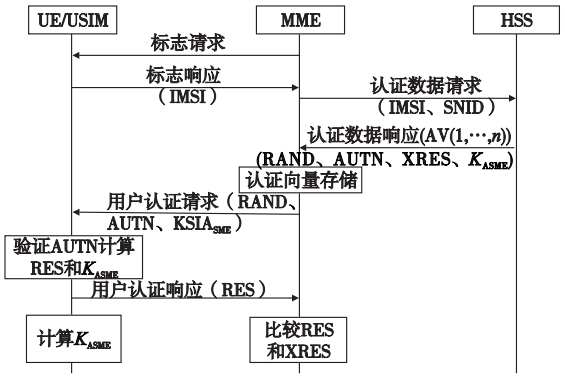

图2 AKA过程

具体流程如下所述:

a) MME 向 HSS 发起认证数据请求。首先 MME 通过向用户请求标志而收到移动用户的注册请求后,向用户所注册的 HSS 发送该用户的 IMSI(international mobile subscriber identifier,国际移动服务识别码),向所在的服务网络发送 SNID(serving network ID,服务网络号),对该用户身份和所在网络进行认证,并请求认证数据。

b) HSS 收到 MME 的认证数据请求之后,根据 SNID 对用户所在的服务网络进行验证。若验证通过,则生成 SQN(sequence number,序列号)和 RAND(随机数),并与长期密钥 K 共同作为密钥生成函数的参数产生包含 K_{ASME} 的 AV(authentication vector,鉴权向量),以单个或分组的形式发送给 MME。

c) MME 收到 AV 或 AV 组之后,按序存储 AV 或 AV 组,并选择一个序号最小的 AV 的 RAND 和 AUTN(认证令牌)发送给 UE,请求 UE 产生认证数据。

d) UE 收到 MME 发来的认证请求后,首先验证 AUTN 中 AMF 的分离位;然后计算 XMAC,并与 AUTN 中的 MAC 相比较。若验证通过,则 UE 将计算 RES 和根密钥 K_{ASME},并将 RES 发送给 MME。

e) MME 收到 UE 发送的 RES 后,将 RES 与 AV 中的 XRES 进行比较,若两者相同则整个 AKA 过程成功。随后的本地认证过程中,AS 和 NAS 将根据相应的密钥产生算法和相应的 K_{ASME} 生成加密密钥和完整性保护密钥。

MME 中没有可用 AV 时,则 AKA 过程通过以上五个步骤完成;否则,直接进行步骤 c) ~ e)。完成双向鉴权后,系统将进入安全模式激活过程。

LTE 系统 AKA 过程与 UMTS 系统鉴权过程基本相同,采用 Milenage 算法,继承了五元组鉴权机制的优点,实现了 UE 和网络侧的双向鉴权。与 UMTS 系统相比,LTE 系统增加了 HSS 对服务网络的认证,防止了假冒服务网络的攻击行为。但是,LTE 系统 AKA 过程产生的认证向量在网络域仍然以明文方式传输,易被截获,是 LTE 系统安全机制潜在的安全威胁之一。

1.2 安全模式命令过程

安全模式命令过程包括 NAS 安全模式命令和 AS 安全模式命令,提供信令或用户数据的完整性和机密性保护。参与的主要网络实体包括 UE、eNB 和 MME 等,具体流程如图 3 所示。

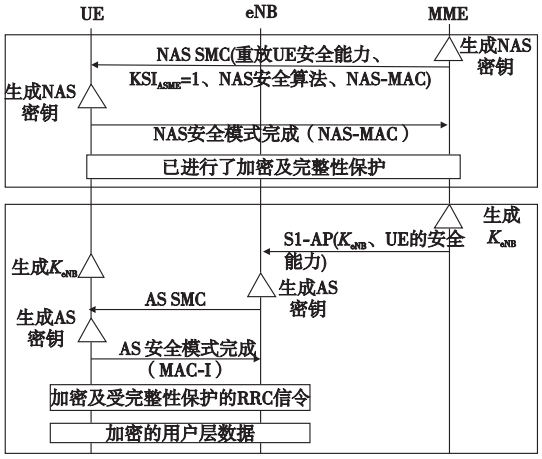

图3 安全模式命令过程

NAS 安全模式命令过程通过 MME 与 UE 之间往返的消息完成。MME 发送该消息之前,会根据 UE 的安全能力选择相应的加密及完整性保护算法。MME 发送的 NAS 安全模式命令消息包括重放的 UE 安全能力、选中的 NAS 安全算法和标志根密钥 K_{ASME} 的 KSI_{ASME}。其中,UE 安全能力携带 UE 所支持的安全算法列表。UE 在接收到该消息后,对其完整性进行验证。若成功,则 UE 对 NAS 安全模式完成消息进行 NAS 加密和完整性保护,并将其发送给 MME。

在发送 AS 安全模式命令消息之前,eNB 根据运营商安全算法优先级列表以及 UE 安全能力所支持的安全算法列表选择符合要求的安全算法,并将其发送给 UE。UE 接收到安全模式命令消息后,利用该安全算法达到加密和完整性保护的目的。

NAS 和 AS 安全模式命令过程结束后,就会对用户与网络之间传送的所有信令及业务消息进行加密和完整性保护。如果没有加密密钥,则无法获取通信双方的通话内容。针对 LTE 安全流程以及密钥分发过程的研究表明:含有用户安全能力的空中接口信息未加密;安全算法可遍历。这些漏洞为窃听方的密钥获取提供了可行性;此外,获取 AS 层通信子密钥需要根密钥 K_{ASME},核心网侧 HSS 与 MME 之间明文传递 AV(组)使得根密钥获取存在可能性。根据以上几方面的研究和分析,本文从窃听方的角度提出了一种基于空中接口与核心网协同的 LTE 系统密钥推演方法。结合空中接口的安全算法信息和核心网的密钥信息,并根据遍历安全算法信息和根密钥信息生成密钥。最后,通过比对利用密钥解密的数据和明文确定密钥。

2　基于空中接口与核心网协同 LTE 系统密钥推演方法

基于空中接口和核心网协同的 LTE 密钥推演方法包括四个步骤。具体流程如图 4 所示。

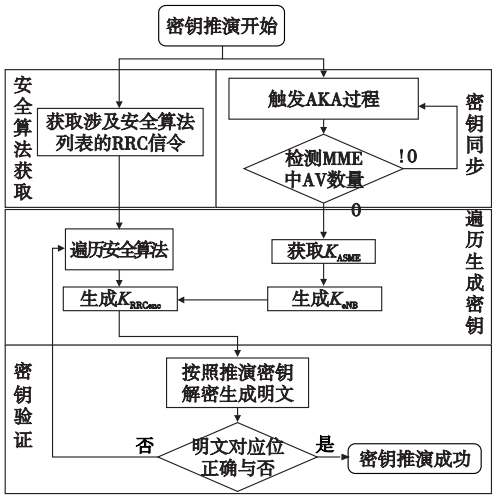

图4　密钥推演流程

1)密钥同步　密钥推演的前提是保证窃听方所使用的 K_{ASME} 与 UE 当前的 K_{ASME} 同步。当两者失步时,需要再经过多次触发 AKA 过程来获取新的 K_{ASME},从而达到与 UE 侧同步。

HSS 分发的 AV 按序存储于 MME 中。当 MME 需要重新发起 AKA 过程时,首先使用 MME 中的 AV。因此,窃听方窜改空中接口数据,触发 AKA 过程时,若 MME 中存在未使用 AV,HSS 就不分发 AV。必须通过多次 AKA 过程耗尽 MME 中存储的 AV,迫使 HSS 分发 AV。

在核心网部署监测设备,若监测设备没有在 HSS 与 MME 之间的信令消息中监测到涉及鉴权数据的消息,则窃听方窜改 UE 与网络之间的信令消息,使网络出现异常现象,迫使 MME 重新发起 AKA 过程。AKA 过程可以消耗存储在 MME 当中的密钥,直至向 HSS 请求新的鉴权数据。监测设备根据鉴权消息的特征提取鉴权数据,并排列其顺序,可以推断出 UE 当前需要的根密钥,达到窃听者的根密钥与 UE 中根密钥同步的目的。

2)UE 安全算法列表获取　3GPP 中规定的算法如表 1 所示。若生成底层密钥所选择的安全算法未知,必须遍历所有安全算法才能获取底层密钥。此密钥获取方法计算开销较大。

表 1　LTE 系统安全算法

4-bit 标志	加密算法	完整保护算法	使用算法
0000_2	EEA0	EIA0	NULL
0001_2	128-EEA1	128-EIA1	SNOW 3G
0010_2	128-EEA2	128-EIA2	AES
0011_2	128-EEA3	128-EIA3	ZUC

文献[7]中提到 UE 安全能力信息包含安全算法列表,而在 UE 与 eNB 交互的相关 RRC 消息(RRC connection setup complete)中承载了 UE 安全能力信息。若窃听方得到安全算法列表,获取到底层密钥的时间复杂度将缩减。该 RRC 消息在鉴权之前传递,没有加密,可以在空中接口获取。根据空中信号的特征,设计空口信息获取的方法如图 5 所示。

获取安全算法列表的具体流程为:a)向 UE 透明传输来自 eNB 的 RRC connection setup 消息;b)在向 eNB 透明传输来自 UE 的 RRC connection setup complete 消息的同时,获取 UE 所支持的安全算法列表,即 UE 安全能力。

利用 UE 安全算法列表生成密钥,相对于盲推密钥,减少了需要遍历的安全算法,即减少了计算开销。

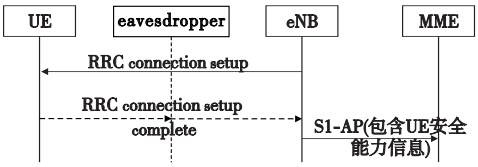

图5　UE支持安全算法获取

3)遍历生成密钥　根据提出的安全分层思想,LTE 系统设计了相应的 AS 密钥—K_{RRCint}、K_{RRCenc}、K_{UPenc} 及 NAS 密钥—K_{NASenc} 和 K_{NASint}。UE 和网络双方密钥的生成和分发流程如图 6 所示。HSS 和 UE 密钥生成体系结构对称,密钥生成函数的主要输入参数是安全算法和父密钥。图 6 中 1、2、3、4、5 和 1′、2′、3′、4′、5′表示选择的安全算法。根据密钥生成规则,KDF、Trunc 等密钥生成参数是已知和不变的,而 NAS UPLINK COUNT 在每次鉴权之后都会复位为 0。根据 NAS UPLINK COUNT 和根密钥 K_{ASME} 计算 K_{eNB}。再根据获取的 UE 安全算法列表,确定可能应用的安全算法,利用 K_{eNB} 遍历产生 AS 密钥($K_{RRCint/enc}$,K_{UPenc}),达到推演密钥的目的。

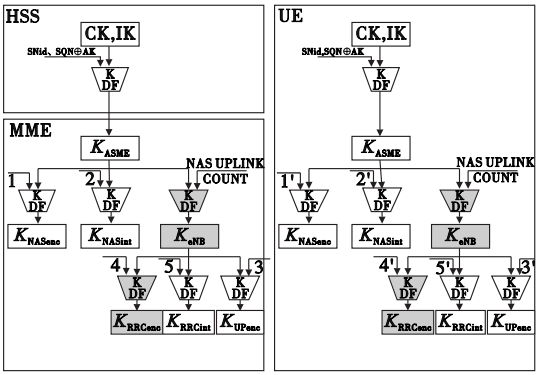

图6　UE和网络密钥分发过程

4)密钥验证　安全算法列表包含多种安全算法,仅仅通过安全算法列表的获取不能达到正确推演密钥的目的,还需要通过对生成的密钥进行检验来确定密钥推演的正确性。检验密钥正确性的常规方法是对解密密文的部分比特和明文块对应比特进行比对。

在安全模式激活之后,eNB 将通过向 UE 发送 RRC connection reconfiguration 消息结束附着过程。为验证密钥的正确性,窃听方在空口侧获取该消息,该消息包含 ATTACH ACCEPT type 消息:01000010[8],也可称之为确知消息。以确知消息为基准进行判决,若消息中对应位相同,则密钥正确。LTE 系统密钥流生成机制及消息比对原理如图 7 所示。解密消息为 RRC connection reconfiguration 消息,构造消息中确知消息是指 ATTACH ACCEPT type 消息。

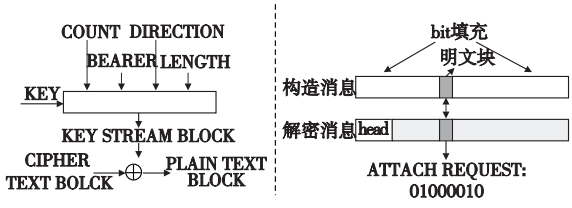

图7　解密过程及比对解密消息原理

假设 RRC connection reconfiguration 消息总长度为 K,第 $k \sim k+7$ 位是确知消息,标志了 ATTACH ACCEPT 消息。将解密消息和构造消息作异或运算。若计算结果的第 $k \sim k+7$ 位

全部为零,则证明该密钥所用的安全算法为当前选择的安全算法;否则继续遍历。据此,可以推出正确的底层密钥。

3 可行性分析

国内外相关领域很少从窃听者角度,通过密钥推演的方法来研究LTE的安全性,本方法具有创新性。因此,接下来本文针对K_{ASME}的获取可行性、密钥推演的复杂度以及密钥推演成功率进行分析。

3.1 获取根密钥K_{ASME}的可行性

在UE和网络进行鉴权时,HSS向MME分发承载K_{ASME}的AV组。3GPP规定,连接HSS与MME的标准接口是S6a接口。该接口应用Diameter协议承载交互数据,所有AVP(attribute value pairs,属性值对)在该接口上透明传输。因此,窃听方可以获取到承载AV的AVP组。

此外,为增加高效性和普遍性,全IP化的核心网开放性增强。某些未授权网络实体通过模拟MME的方式发送鉴权数据请求消息请求鉴权数据(AV),或者透明传输HSS与MME之间的信令和数据信息是可行的。综合考虑消息传递方式和网络接入限制,获取根密钥K_{ASME}是可行的。

3.2 密钥推演复杂度分析

为评估密钥推演方法的性能,需对比正常密钥生成与密钥推演方法之间的计算复杂度。假设信令传递时间忽略不计,只考虑遍历生成密钥和密钥验证两个主要功能模块的复杂度计算。

遍历密钥生成包括两个阶段,即密钥生成和密钥流生成。密钥生成所涉及的密钥分发函数为HMAC-SHA256,每个密钥的生成都经历一次加密哈希运算(H)。依据文中所述,本方法在整个密钥生成过程中需要进行的加密哈希运算次数为$n+2$。其中n为安全算法列表中安全算法的个数,$1 \leqslant n \leqslant 3$。

密钥流生成是以安全算法为前提的,选择不同的安全算法,其计算复杂度不同。根据文献[9~11]给出的安全算法,产生单位密钥块的计算开销如表2所示。

表2 SNOW 3G、AES和ZUC计算开销的比较

计算类型	SNOW 3G	AES	ZUC	计算类型	SNOW 3G	AES	ZUC
点加运算	2 026	4 752	2 254	或运算	2 456	0	2 350
与运算	4 320	24	4 443	异或运算	3 764	288	1 610
移位运算	3 378	24	6 632	点乘运算	0	4 608	0

密钥比对方法是解密消息和构造消息进行异或运算,每次密钥推演需要进行n次异或运算。假设安全算法列表包含所有安全算法。另外,列举了可能出现的安全算法列表情况,并针对各种情况进行计算开销计算。根据以上分析,可对UE进行密钥分发和生成与各种可能的安全算法列表情况下窃听方协同密钥推演方法的计算开销进行比较。UE进行密钥分发时只用一种安全算法,其计算开销如表3所示。例如协同密钥推演方法的计算开销与安全算法列表中安全算法个数有关:当安全算法个数为1时,计算开销同UE密钥分发过程;当安全算法个数大于1时,计算开销如表3所示。

从表3中可以看出,UE在完成密钥生成与协同密钥推演方法获取底层密钥的线性开销基本上呈倍数关系,有AES参与的密钥生成或密钥获取的非线性计算开销较大。安全算法列表中存在两个安全算法时,线性计算开销方面,协同密钥推演方法获取底层密钥大约是UE完成密钥生成的两倍;存在三个安全算法时,线性计算开销变成了三倍。非线性计算开销会因安全算法列表中是否含有AES而不同。

表3 协同密钥推演计算开销的比较

计算类型	$S+A$	$S+Z$	$A+Z$	$S+A+Z$
哈希运算	4	4	4	5
点加运算	6 778	4 280	7 006	9 032
与运算	4 344	8 763	4 467	8 787
移位运算	3 402	10 010	6 656	10 034
或运算	2 456	4 806	2 350	4 806
异或运算	4 054	5 376	1 900	5 665
点乘运算	4 608	0	4 608	4 608

3.3 密钥推演成功率分析

当不考虑获取信息的误码率时,密钥推演的错误率主要体现在密钥验证过程中,即误判率。在仿真中假设确知消息可以变化,依据概率论知识可以得出如图8所示密钥推演误判率的结果。

结果表明,密钥推演的误判率大小取决于确知消息的位数,与之近似呈指数关系。另外,密钥推演的误判率还与安全算法列表中的安全算法个数有关。确知消息位数为8的情况下,密钥推演误判率小于10^{-2},基本满足密钥推演的需求。

假设HSS向MME分发AV组中的AV个数为3,UE安全算法列表中可能存在的安全算法个数分别为1、2、3个,考虑获取空中接口信息时存在误码率的情况,其范围为$10^{-6} \sim 10^{-1}$,考察在不同误码率下密钥推演的正确率。在获取安全算法列表、解密过程中所需参数(COUNT、BEARER、LENGTH、DIRECTION等)和加密消息时,一旦出现误码会导致密钥推演失败。10^8次蒙塔卡罗实验的结果如图9所示。

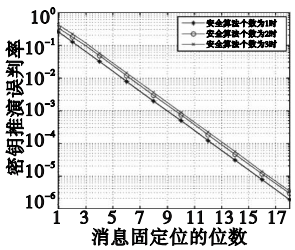

图8 密钥推演误判率

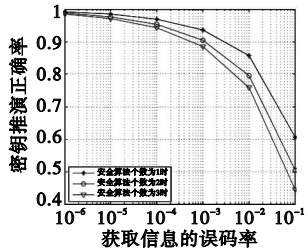

图9 获取信息误码率与密钥推演正确率之间的关系

图9结果显示,误码率在$10^{-6} \sim 10^{-1}$时,安全算法的个数越多,密钥推演正确率越小;安全算法个数一定时,随着误码率的增加,密钥成功率逐渐减小;当误码率低于10^{-3}时,密钥推演成功率可达到90%。考虑到物理层的实际误码率大小,该密钥推演方法具有一定的实际应用意义。

4 结束语

通过分析LTE安全过程,本文总结了在空中接口侧及核心网侧的安全漏洞,并基于空中接口与核心网相结合的思想设计了一种窃听方的协同密钥推演方法:通过触发AKA完成窃听方与UE密钥同步;利用获取的UE安全能力信息减少遍历安全算法次数;将解密密文与明文比对,确定推演的密钥。可行性分析表明,该方法具有一定的实际应用意义。

(下转第2771页)

个节点变量进行多次抽样,最后根据抽样组合数据统计分析后验概率。按照采样时间的不同进行抽样统计分析,每组抽样个数为 30 000 个。用 N_i 表示采样的时间点。以 $P(v_7|v_1,v_2,v_3)$ 的概率值作为抽样结果的统计项,$p = P(v_7 = \text{true}|v_1 = \text{true}, v_2 = \text{true}, v_3 = \text{true})$ 为所求概率值。本次实验总共进行了四次采样过程,用 P_i 表示每次采样的概率抽样组合,采样结果如表 1 所示。

表 1　采样结果

	N_1	N_2	N_3	N_4	N_5	N_6	N_7	N_8	N_9	N_{10}
P_1	0.278 9	0.333 1	0.496 5	0.542 5	0.606 1	0.677 8	0.747 5	0.798 2	0.853 6	0.952 7
P_2	0.192 7	0.265 0	0.302 4	0.452 1	0.534 7	0.602 4	0.718 9	0.803 4	0.815 6	0.830 0
P_3	0.124 9	0.302 4	0.365 4	0.453 6	0.536 7	0.602 4	0.678 9	0.724 6	0.790 0	0.820 0
P_4	0.250 0	0.354 7	0.482 1	0.527 8	0.619 6	0.705 6	0.759 8	0.823 6	0.895 6	0.920 0

由实验所得采样结果可以看出,随着采样时间的不同,攻击者的攻击概率逐渐增大,这与实际攻击途径中的效果是一致的。由于随着攻击进度的推进,攻击者拥有和熟悉的攻击资源越来越多,靠近攻击目标越来越近,对系统造成的威胁可能性也越来越大。

图 5 和 6 显示了本文提出的内部威胁预测模型计算得出的用户攻击进度。假设管理人员设定警戒值为 0.85,当监测到用户攻击概率达到 0.85 时,阻止用户的攻击行为。从走势图可以看出,该模型能够实时监测内部用户的攻击行为,通过后验概率值量化内部用户的攻击概率,从而给内部网络的管理决策人员提供参考,以便作出正确的决策。

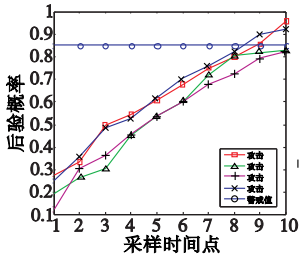

图5　内部威胁模型中用户攻击监测图1

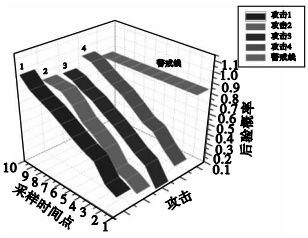

图6　内部威胁模型中用户攻击监测图2

4　结束语

本文提出用贝叶斯网络模型来描述内部威胁的网络结构。并且利用贝叶斯网络的推理算法—似然加权法,计算内部威胁网络攻击图中的后验概率问题。从而定性和定量分析了内部威胁的网络结构。最后通过实验证明,该模型能够准确有效地预测内部威胁。

参考文献:

[1] LIU Yu, MAN Hong. Network vulnerability assessment using Bayesian networks[C]//Proc of SPIE 5812. New York: ACM Press, 2005: 61-71.

[2] FRIGAULT M, WANG Ling-yu. Measuring network security using bayesian network-based attack graphs[C]//Proc of IEEE International Computer Software and Applications Conference. Washington DC: IEEE Computer Society, 2008: 698-703.

[3] 王桢珍,姜欣,武小悦,等. 信息安全风险概率计算的贝叶斯网络模型[J]. 电子学报,2010,38(2A):18-23.

[4] 张少俊,李建华,宋珊珊,等. 贝叶斯推理在攻击图节点置信度计算中的应用[J]. 软件学报,2010,21(9):2376-2386.

[5] GHINITA G. The optimization of situational awareness for insider threat detection[C]//Proc of the 1st ACM Conference on Data and Application Security and Privacy. New York: ACM Press, 2011: 231-235.

[6] NELLIKAR S, NICOL D M, CHOI J J. Role-based differentiation for insider detection algorithms[C]//Proc of ACM Conference on Computer and Communications Security. New York: ACM Press, 2010: 55-62.

[7] 王国玉,王会梅,陈志杰,等. 基于攻击图的计算机网络攻击建模方法[J]. 国防科技大学学报,2009,31(4):74-81.

[8] 杨健,高文逸,刘军. 一种基于贝叶斯网络的威胁估计方法[J]. 解放军理工大学学报:自然科学版,2010,11(1):43-48.

[9] 王辉,刘淑芬. 一种可扩展的内部威胁预测模型[J]. 计算机学报,2006,29(8):134-6-1355.

[10] CHINCHANI R, UPADHYAYA S, KWIAT K. Towards the scalable implementation of a user level anomaly detection system [C]//Proc of IEEE Military Communications Conference. 2002: 1503-1508.

[11] UPADHYAYA S, CHINCHANI R, KWIAT K. An analytical framework for reasoning about intrusions [C]//Proc of the 20th IEEE Symposium on Reliable Distributed Systerms. 2001: 99-105.

[12] FUNG R, CHANG K C. Weighting and integrating evidence for stochastic simulation in Bayesian networks[C]//Proc of the 1st Annual Conference on Uncertainty in Artificial Intelligence. 1989: 209-219.

(上接第 2758 页)

参考文献:

[1] 3GPP TS 33.401 v11.1.0, 3rd generation partnership project; technical specification group services and system aspects; 3GPP system architecture evolution (SAE) security architecture[S]. Valbonne: 3GPP, 2012.

[2] HAN C K. Security analysis and enhancements in LTE-advanced networks [D]. Seoul: Sungkyunkwan University, 2012.

[3] GINS E A, RAPHAEL C W, PARISH D J. Analysis and design of security for next generation 4G cellular networks[C]//Proc of the 13th Annual Post Graduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting. 2012.

[4] FORSBERG D, HUANG Le-ping, TSUYOSHI K, *et al*. Enhancing security and privacy in 3GPP E-UTRAN radio interface[C]//Proc of Personal, Indoor and Mobile Radio Communications. 2007: 1-5.

[5] MJØLSNES S, TSAY J K. Computational security analysis of the UMTS and LTE authentication and key agreement protocols [EB/OL]. (2012-03-17)[2013-01-08]. http://arxiv.org/abs/1203.3866.

[6] FUHR T, GILBERT H, REINHARD J R, *et al*. Analysis of the initial and modified versions of the candidate 3GPP integrity algorithm 128-EIA3[C]//Proc of the 18th International Workshop on Selected Areas in Cryptography. 2011: 230-242.

[7] 3GPP TS 33.102 v11.5.0, 3rd generation partnership project; technical specification group services and system aspects; 3G secu-rity; security architecture[S]. Valbonne: 3GPP, 2012.

[8] 3GPP TS 24.301 v11.4.1, 3rd generation partnership project; technical specification group core network and terminals; Non-access-stratum (NAS) protocol for evolved packet system (EPS) [S]. Valbonne: 3GPP, 2012.

[9] ORHANOU G, HAJJI S E, BENTALEB Y. SNOW 3G stream cipher operation and complexity study [J]. Contemporary Engineering Sciences, 2010, 3(3): 97-111.

[10] TUNSTALL M. Practical complexity differential Cryptanalysis and fault analysis of AES[J]. Journal of Cryptographic Engineering, 2011, 1(3): 219-230.

[11] ETSI TC SAGE v1.6, 3GPP confidentiality and integrity algorithms 128-EEA3 & 128-EIA3 [EB/OL]. (2011). http://www.etsi.org/index.php/services/security-algorithms/3gpp-algorithms.