文章编号:1005-0523(2019)05-0120-09

LTE-R认证与密钥协商协议的安全分析及改进

张利华[1],姜攀攀[2],蒋腾飞[2],李晶晶[1]

(华东交通大学 1. 软件学院; 2. 电气与自动化工程学院,江西 南昌 330000)

摘要:安全高效的车地身份认证方案是铁路安全运行的基础,结合列控系统数据安全传输对移动通信系统的需求和铁路无线通信网的发展方向,提出一种基于伪随机数和哈希函数的LTE-R车地通信身份认证协议。设计了由国际移动用户识别码(IMSI)和随机数生成的能够替换IMSI传输的匿名身份(PID),解决了由IMSI泄露导致的安全问题;利用临时生成的认证密钥*NK*代替永久根密钥*K*完成认证流程,提高了根密钥*K*的安全性。利用认证测试方法对协议的正确性进行了证明。分析证实,本文提出的LTE-R身份认证方案具有很好的安全性和匿名性,计算效率与通信消耗较好。

关键词:车地通信;LTE-R;身份认证;认证测试

中图分类号:TN929.5 **文献标志码**:A

目前,我国铁路使用的移动通信系统GSM-R(global system for mobile communications-railway)是建立在第二代无线通信系统GSM的基础上,然而现有的GSM-R已无法满足高速铁路日益增长的宽带业务需求而且3G网络所使用的频率也相对较高,所以,国际铁路联盟(UIC)已确认铁路下一代移动通信系统将跨过3G技术,由GSM-R向LTE-R(long term evolution-railway)发展。

可是,LTE-R在沿用LTE的系统结构和技术手段的同时,LTE AKA (authentication and key agreement)中存在的一些问题也同样存在于LTE-R之中, 例如国际移动用户认证码IMSI (international mobile subscriber identification number)、SNID(服务网络ID)和AVs(authentication vectors,认证向量组)未受保护,UE(user equipments,用户设备)与HSS(home subscriber server,归属用户服务器)共享的根秘钥*K*没有完善安全的措施防止其泄漏等[1]。本文分析了这些问题,随之提出一种安全且适用于铁路环境的的LTE-R身份认证方案。

许多专家学者针对GSM-R身份认证过程的存在的问题,对GSM-R中的认证协议进行了改进,改进方案[2-5]都相继被提出。但是上述的几种改进方案并没有跳脱出GSM固有的框架,没有彻底解决GSM-R中存在的安全问题。为了满足未来铁路运输高速数据业务和高安全性的需求, 发展下一代铁路无线通信系统LTE-R的要求已被提出,那么LTE身份认证过程中的问题也将存在于LTE-R中,例如,用户首次接入网络时,用户唯一身份标识IMSI在传输过程中不受保护,存在被攻击者截获、收集而产生信息泄漏问题的风险,针对这一问题,文献[6]提出一种基于公钥密码体制的安全有效的公司密码体制方案SE-AKA,解决了IMSI与SDID泄露的问题,但其采用无线公钥基础设施方案WPKI,认证过程中的通信开销和证书库的管理和维护问题将不可忽视。文献[7]提出HSK-AKA,其采用数字签名达到抵御伪MME攻击的效果,利用随机移动用户身份标识(RMSI)代替IMSI,牺牲用户端少量的运算资源对IMSI进行加密,从而保护了IMSI。文献[8]提出EPS-AKA,此方案采用私钥密码体制,解决了IMSI泄露的问题,能够利用更少的计算消耗来达到更高的安全性。文献[9-11]采用群认证的方案,设计了一种能够保护IMSI的认证方案,即同时接入网络的大量用户成立一个组,随后选择一可信用户组为组长,组成替代组员向网络发送认证请求,但是,组长身份信息泄

收稿日期:2019-02-27

基金项目:江西省教育厅科技项目(2GJJ14271)

作者简介:张利华(1972—),男,副教授,博士,研究方向为无线与移动通信网络安全,工业控制网络安全。

露将导致组内成员的身份信息承担巨大泄露风险。

在整个 LTE 身份认证过程中,K 作为长期保存在用户端和网络端的根密钥, 其安全是整个认证流程安全的基础,K 若被攻击者窃取,那么整个协议便毫无安全性可言,针对解决根密钥 K 泄露的问题,国内外专家学者进行了大量的研究,文献[12]提出的 ES-AKA 中,的生成由根密钥和临时密钥 DK 共同决定,解决了 K 泄露的问题,但是在该方案中,用户的 IMSI 并未受到保护,文献[13]提出一种基于公钥体制的 D-AKA,该方案利用随机数生成接入安全管理实体密钥,实现了密钥的更新,其安全性将不再过度依赖 K 的安全存储,但此方案中公钥证书的传递将产生巨大的通信开销,证书管理工作过于繁杂。文献[14]提出一种基于混合密码体制的 I-AKA,解决了文献[13]中特有的伪 UE 攻击,但公钥证书管理的问题仍存在。由上述分析可知,目前并没有一个比较完善的 LTE-AKA 方案可以直接沿用于 LTE-R 之中。针对上述问题,本文提出一种基于哈希和伪随机数的 LTE-R 身份认证方案,在保护用户隐私的同时,解决了根密钥K 泄露的问题。

1　LTE-R 认证流程及存在的问题

1.1　LTE-R AKA 具体流程

LTE/SAE AKA 是 3GPP 组织提出的一种 LTE 环境中标准身份认证与秘钥协商方案,是后续 LTE 安全问题研究的基础。LTE-R 继承了 LTE/SAE AKA 的身份认证的基本流程, 沿用了“挑战/响应”的认证机制。具体流程如图 1 所示。

Message 1:用户设备 UE 向移动性管理实体 MME 以明文的方式发送其唯一身份标识 IMSI。

Message 2:MME 收到 IMSI 后,发送 IMSI\ 服务网络标识 SNID 和服务网络类型给所属的归属用户服务器 HSS。

Message 3:如果 HSS 验证 IMSI 成功,便利用所收到的参数生成认证向量 AVs 并将其发送给 MME。认证向量包括参数 $RAND$,$AUTN$,$XRES$ 和密钥 K_{ASME}。

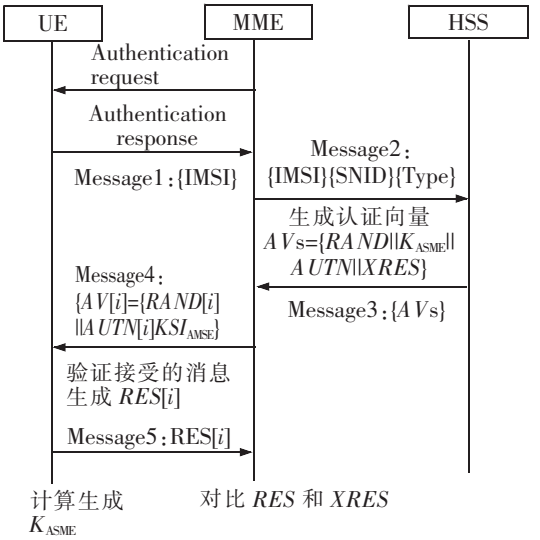

图 1　LTE-R AKA 具体流程

Fig.1　Specific flow chart of LTE-R AKA

Message 4:MME 将随机选择一组认证向量,然后向 UE 发送 $RAND(i)$,$AUTN(i)$,和 KSI_{AMSE}(为 K_{ASME} 的标识)。

Message 5:UE 验证 $AUTN$ 中的消息认证码 MAC 认证 MME,生成加密密钥 CK,完整性密钥 IK 和中间密钥 K_{AMSE},然后计算 $RES(i)$并发送给 MME。收到 $RES(i)$后,将其与 $XRES(i)$比较,如果相等,则网络认证用户成功;之后 UE 利用 CK 和 IK 计算生成主密钥 $K_{AMSE}(i)$,MME 也从认证向量中取出 $K_{AMSE}(i)$,至此身份认证流程结束。

1.2　LTE-R AKA 中存在的问题

在 LTE-R AKA 中,通过实现网络和用户的双向认证,解决了 GSM-R 中单向认证的问题;通过对各类密钥进行分层,提高了协议通信的整体安全级别。但是,协议中也存在一些问题:

1) IMSI 明文传输。在协议中 IMSI 以明文的方式在协议流程中进行传输,攻击者能够轻易得到大量的合法 IMSI,便可以利用这些 IMSI 进行非法攻击。

2) 根密钥 K 泄露。在协议中,认证流程依赖共享密钥 K,若 K 遭到泄露,整个协议便无安全性可言。

3) 重定向攻击。攻击者可以伪装成服务网络/移动管理实体(SN/MME)截取合法用户的请求消息,同时伪装成合法用户向合法的 SN/MME 发送所截获的消息。由于请求消息本身合法,所以 HSS 便会向合法的发送认证向量,然后 SN/MME 将会认证用户,这时攻击者便可以将用户重新定向到攻击者预设的网络。

4) 服务网络标识明文传输。在协议中,服务网络标识在传输之前并未被加密,攻击者可以轻易得到合

法的服务网络标识,并通过它对目标用户发起中间人攻击。

5) 认证向量明文传输。MME 和 HSS 之间在传输认证向量时,认证向量并未加密,会被攻击者轻易截获,攻击者可以对所截获的认证向量进行分析,并以发起严重的攻击。

2 改进的 LTE-R 身份认证协议

2.1 系统架构

本协议主要参与者有 3 个,分别是列车上的移动台 MS(mobility station),移动性管理实体 MME/VLR 和认证中心 HSS/AuC,在认证过程中,MS 与 MME/VLR 通过无线的空中信道进行通信,MME 与 HSS/AuC 则通过安全的有线信道进行通信,系统整体架构如图 2 所示。

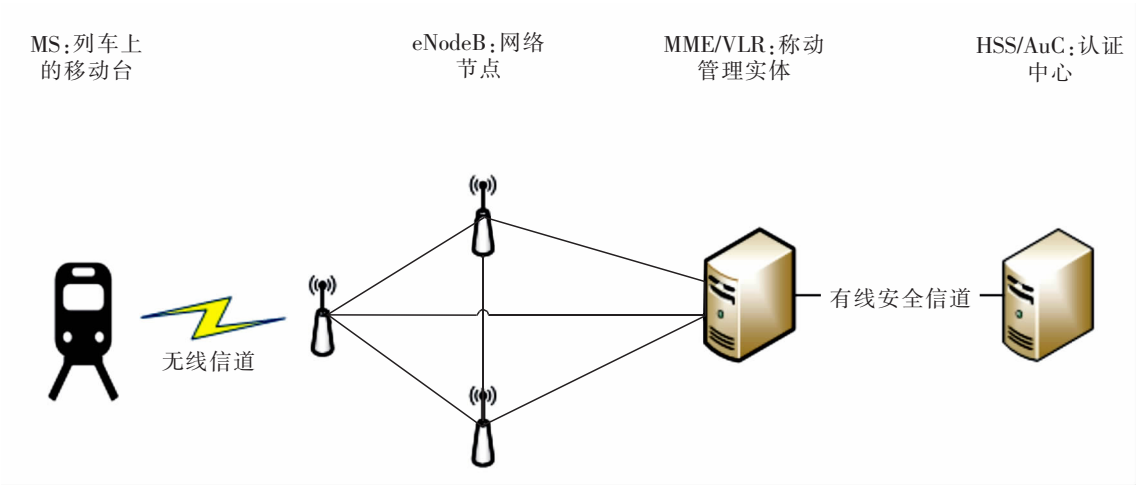

图 2 LTE-R 系统架构图

Fig.2 System architecture diagram of LTE-R

2.2 安全假设

在 LTE-R 系统中,MME/VLR 与 HSS/AuC 是通过骨干网进行通信,使用的是有线信道进行信息传递,而且可以认为 MME/VLR 与 HSS/AuC 的计算能力是强大的,二者在传输信息时候,可以使用如 RSA、AES 等算法进行加解密运算,所以本文认为攻击者想要从 MME/VLR 和 HSS/AuC 之间的有线信道上截获信息是极其困难的,即 MME/VLR 与 HSS/AuC 之间的通信时安全的。为了设计出适用的 LTE-R 身份认证协议和更方便的分析协议的安全性,本方案进行如下假设:

1) 消息在 MME/VLR 与 HSS 之间传输是安全的,即 MME/VLR 与 HSS/AuC 之间的有线信道是安全的;

2) MS 与 MME/VLR 之间是通过空中无线信道进行信息传递,是不安全的;

3) 攻击者可以拦截、存储无线信道中的任何消息;

4) 攻击者无法预测协议运行过程中生成的随机数。

2.3 注册阶段

列车上的移动台 MS 在正式上线运行前,需要先到合法的列车控制管理机构进行注册,以获得相关的密钥、算法等重要参数,确保其能正常进行工作。具体的注册流程如下:

MS 将其 *IMSI* 发送至 MME/VLR,MME/VLR 将 *IMSI* 连同其自身唯一身份标识 ID_{VLR} 发送给 HSS/AuC,HSS/AuC 存储 *IMSI* 与 ID_{VLR};

HSS/AuC 生成密钥 K、身份识别序列码 NC 和相关加密算法 f_1, f_2, f_3, f_4, f_5, 并将它们发送给 MME/VLR,MME/VLR 将其转发给 MS;

MS 将根密钥 K、身份识别序列码 NC 和加密算法 f_1, f_2, f_3, f_4, f_5 安全地存储在其 SIM 卡内。

上述流程中的密钥 K 为存储在 MS 与 HSS/AuC 中的通信加密根密钥,身份识别序列码 NC 是由 HSS/

AuC 产生,*NC* 与用户的 *IMSI* 和密钥 *K* 一一对应,HSS/AuC 根据 *NC* 来快速确认用户身份,而算法 f_1, f_2, f_3, f_4, f_5 均为公开的加密算法,比如:DES,AES,Hash,SNOW 3G 等。注册流程图如图 3 所示。

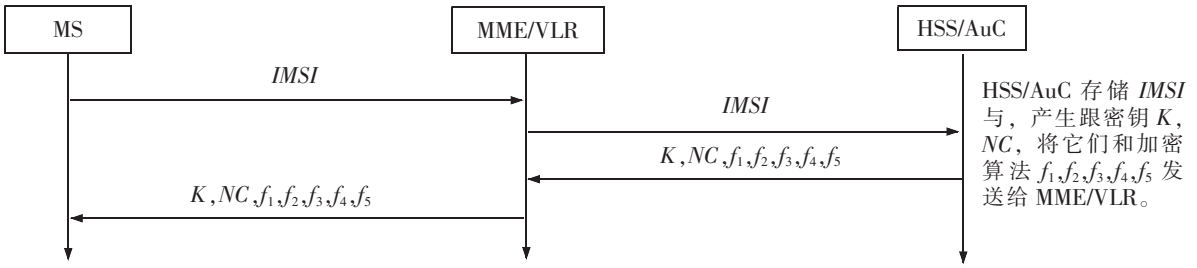

图 3　注册流程图

Fig.3　Registration flow chart

2.4　协议流程

列车上的移动台 MS 要接入 LTE-R 网络进行网络通信之前,先要进行 MS 与 HSS 之间的互相认证与密钥协商,具体认证过程包括以下步骤,如图 4 所示。

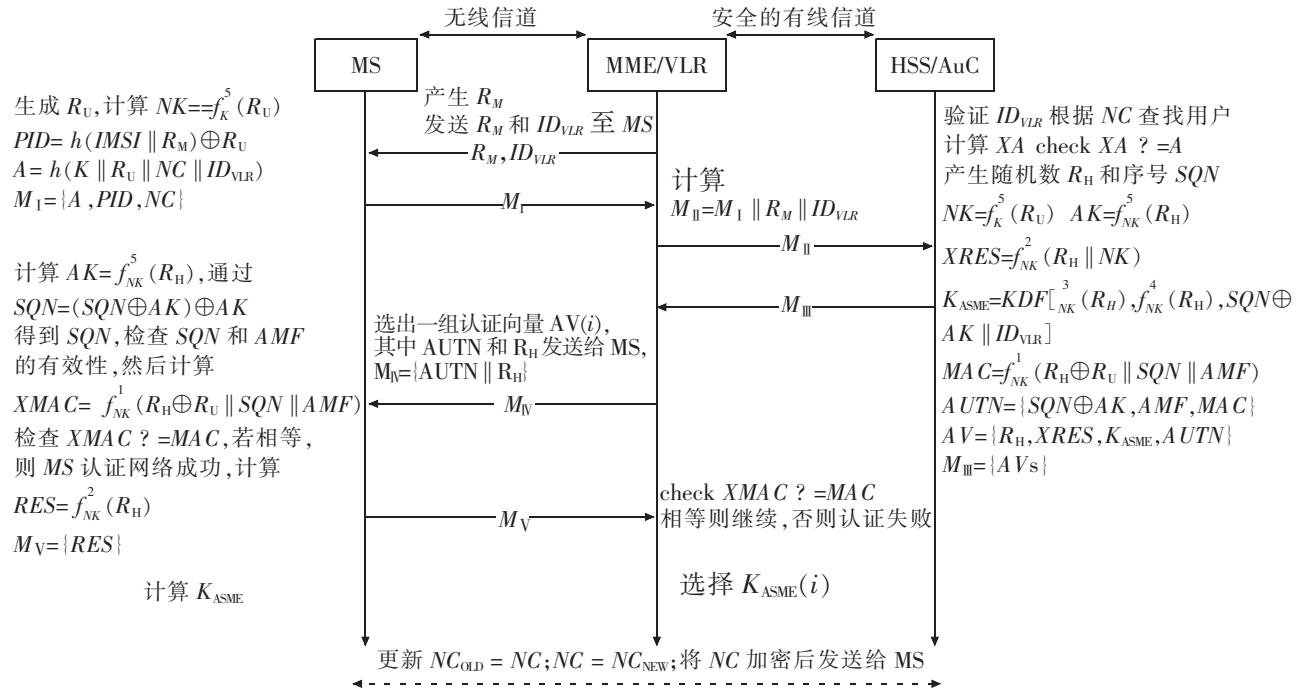

图 4　认证协议流程图

Fig.4　Flow chart of the authentication protocol

1) 当一个 *MS* 首次进入到一个 MME/VLR 后,MME/VLR 生成一个私密随机整数 R_M,随之将 R_M 和其唯一身份标识 ID_{VLR} 通过无线信道发送给 MS。

MS 收到 R_M 和 ID_{VLR} 后,生成用户随机整数 R_U,计算临时密钥 $NK=f_K^5(R_U)$,假身份 $PID=h(IMSI \| R_M)\oplus R_U$,认证参数 $A=h(K \| R_U \| NC \| ID_{VLR})$,然后将消息 $M_I=\{A, PID, NC\}$ 发送给 MME/VLR,其中 $f_K^n(m)$ 表示利用加密算法 f^n 对 m 进行加密,而 k 则为相关加密密钥。

2) MME/VLR 把它生成的随机数 R_M 和身份 ID_{VLR} 附在 M_I 之后,即 $M_{II}=M_I \| R_M \| ID_{VLR}$,然后将消息 M_{II} 发送给 HSS/AuC。

3) HSS/AuC 收到 M_{II},先验证 ID_{VLR} 是否合法,然后根据身份识别码 *NC* 在数据库中搜索,来确定用户的身份,如果搜索失败则中断认证,否则提取出用户的身份识别码 *IMSI* 和根密钥 *K*,接着计算

$$R_U'=h(IMSI \| R_M) \oplus PID \tag{1}$$

$$XA=h(K \| R_U' \| NC \| ID_{VLR}) \tag{2}$$

检查 $XA=A$，如果二者相等，即验证成功，然后 HSS/AuC 生成认证随机数 R_H 和序列号 SQN，接着计算

$$NK=f_K^5(R_U) \tag{3}$$

$$AK=f_{NK}^5(R_H) \tag{4}$$

$$XRES=f_{NK}^2(R_H \| NK) \tag{5}$$

$$K_{ASME}=KDF[f_{NK}^3(R_H), f_{NK}^4(R_H), SQN \oplus AK \| ID_{VLR}] \tag{6}$$

$$MAC=f_{NK}^1(R_H \oplus R_U \| SQN \| AMF) \tag{7}$$

$$AUTN=\{SQN \oplus AK, AMF, MAC\} \tag{8}$$

$$AV=\{R_H, XRES, K_{ASME}, AUTN\} \tag{9}$$

其中：NK 为临时密钥；AK 为匿名密钥；$XRES$ 为预期响应；K_{ASME} 为介入安全管理实体密钥；KDF 为密钥导出函数；MAC 为消息认证码；$AUTN$ 为认证令牌；AMF 为鉴权管理域；AV 为认证向量。然后把认证向量组 AVs 发送到 MME/VLR，即 $M_{III}=\{AVs\}$。

4）MME/VLR 收到 AVs 后，从认证向量组选出一组 $AV(i)$，将其中 $AUTN$ 和 R_H 发送给 MS，即 $M_{IV}=\{AUTN \| R_H\}$。

5）MS 收到消息后，首先计算

$$AK=f_{NK}^5(R_H), SQN=(SQN \oplus AK) \oplus AK \tag{10}$$

MS 得到 SQN 和 AMF 后，先检查其有效性，然后计算预期消息认证码

$$XMAC=f_{NK}^1(R_H \oplus R_U \| SQN \| AMF) \tag{11}$$

检查 $XMAC=MAC$，若二者相等，则证明 HSS/AuC 是合法的。然后 MS 计算响应

$$XMAC=f_{NK}^2(R_H) \tag{12}$$

然后将 RES 发送给 MME/VLR，即 $M_V=\{RES\}$。

6）MME/VLR 检查 $RES=XRES$，如果二者相等，说明 MS 是合法的，否则网络拒绝 MS 的接入请求。

7）认证结束后，MS 计算出 K_{ASME}，即密钥协商完成，双方开始生成接下来会话需要的加密密钥和完整性密钥。然后 HSS/AuC 对 NC 进行更新

$$NC_{OLD}=NC;\ NC=NC_{NEW} \tag{13}$$

NC_{NEW} 代表用户身份识别序列码的最新值，HSS/AuC 在数据库中存储和 NC，并且把加密后安全的发送给 MS。下一次认证时，用新的 NC 查找用户身份。

3 安全性验证

3.1 正确性证明

本文利用认证测试法对所提协议的正确性进行证明，首先介绍认证测试的相关定义和定理[7]。

定义 1 分量：项 t_0 成为项的分量，当且仅当 t_0 不属于连接项，且对任意 $t_0 \neq t_1$，都有 $t_0 \subset t_1 \subset t$。即分量是原子项或加密项。

定义 2 新分量：若 t_0 是$<S,i>$的新分量，当且仅当 t_0 是$<S,i>$的分量，且不是其他任意节点 t_0 是$<S,i>(j<i)$的分量。

定义 3 变换边/变换进行边：若$<S,i> \Rightarrow^+ <S,j>$是关于 a 的变换边，当且仅当 a 从$<S,i>$发送，在$<S,j>$处以新分量的形式被接收；若$<S,i> \Rightarrow^+ <S,j>$是关于 a 的变换进行边，当且仅当 a 在$<S,i>$处被接收，且在$<S,j>$处以新分量的形式发送。

定义 4 测试分量/测试：$t=\{h\}_k$ 是节点 n 关于 a 的测试分量，如果 $a \subset t$，且 t 是结点 n 的分量，t 不是串集合 $\sum$ 中其他节点分量的子项。如果 a 唯一起源于节点 n_0，且 $n_0 \Rightarrow^+ n$ 是关于 a 的转换边，则称 $n_0 \Rightarrow^+ n$ 是 a 的一个测试。

定义 5 输出测试:边 $n_0 \Rightarrow^+ n_1$ 是分量 $t=\{h\}_k$ 关于 a 的输出测试,即:① 边 $n_0 \Rightarrow^+ n_1$ 是 a 的一个测试;② $K \notin K_p$,即 K 不为攻击者所知;③ a 不出现在节点 n_0 除 t 以外的其他任何分量;④t 是节点 n_0 关于 a 的一个测试分量。

定义 6 输入测试:边 $n_0 \Rightarrow^+ n_1$ 是分量 $t=\{h\}_k$ 关于 a 的输入测试,即:① 边边 $n_0 \Rightarrow^+ n_1$ 是 a 的一个测试;② $K \notin K_p$;③ t 是节点 n_0 关于 a 的一个测试分量。

定理 1 输出测试定理:假设在从 C 中,$n_0, n_1 \in C$,边 $n_0 \Rightarrow^+ n_1$ 是分量 t 关于 a 的输出测试,即有:① 存在节点 $m, m' \in C$ 满足 t 是 m 的组成分量,且 $m \Rightarrow^+ m'$ 是 a 的测试进行边;② 若 a 在 m 的分量 $t=\{h\}_k$ 中出现,且 t 不是其他任何结点的分量,$K \notin K_p$,则必然存在一个包含 t 为分量的负结点。

定理 2 输入测试定理:假设在从 C 中,$n_0, n_1 \in C$,边 $n_0 \Rightarrow^+ n_1$ 是分量 t 关于 a 的输入测试,则必然存在结点 $m, m' \in C$ 满足 t 是 m' 的组成分量,且 $m \Rightarrow^+ m'$ 是 a 的测试进行边。

定理 3 主动测试定理:假设在从 C 中,$n \in C$,且 n 是分量 t 关于 a 的主动测试,则必然存在正结点 $m \in C$,使得 t 是 m 的分量。

在本方案中,MME/VLR 代替了 HSS/AuC 进行对 MS 的认证。所以, 在对本方案形式化分析时,MME/VLR 与 HSS/AuC 被视为一体,用 AuC 来表示。本方案的形式化描述如下:

1) AuC→MS : R_M;

2) MS→AuC : A ;

3) AuC→MS : $R_H \| AUTN$;

4) MS→AuC : RES。

下面给出本协议基础术语的代数描述:

MS 的串和轨迹

$$S_{MS}=\{R_M, A, AUTN, R_H, RES\} \tag{14}$$

$$Trace_{MS}=< -R_M, +A, -\{R_H, AUTN\}, +RES > \tag{15}$$

AuC 的串和轨迹

$$S_{AuC}=\{R_M, A, AUTN, R_H, RES\} \tag{16}$$

$$Trace_{AuC}=< +R_M, -A, +\{R_H, AUTN\}, -RES > \tag{17}$$

假设随机数 R_H 由唯一由 AuC 产生,C 为包含 S_{AuC} 的从,AuC 认证 MS 证明如下:

R_H 唯一产生于$< S_{AuC}, 4 >$,并且$< S_{AuC}, 4 > \Rightarrow^+ < S_{AuC}, 5 >$构成变换边,又因为 $RES=f_{NK}^2(R_H)$,$NK \notin K_p$,则边$< S_{AuC}, 4 > \Rightarrow^+ < S_{AuC}, 5 >$构成 RES 关于 R_H 输入测试,RES 是 R_H 的测试分量。根据定理 2,存在 $m, m' \in C$,使得 RES 为 m' 的分量,并且 $m \Rightarrow^+ m'$ 是 R_H 的变换进行边。

根据定理 2,结点 m' 为正结点,而且 m' 是串 S_{MS} 中的结点,$m'=< S_{AuC}, 4 >$,且 RES 是 m' 的分量,由于常规正结点中包含 RES 形式的只有$< S_{AuC}, 4 >$,所以 C中必然包含一个串 $S_{MS}=\{R_M, A, AUTN, R_H, RES\}$。根据上述分析,AuC 能成功地对 MS 的身份进行认证。

假设 $R_H \neq R_U$,且 R_U 唯一由 MS 产生,C 为包含串 S_{MS} 的从,MS 对 AUC 的认证如下:

$R_H \neq R_U$, 且 R_U 是唯一产生于结点$< S_U, 2 >$的随机数, 并且$< S_{MS}, 2 > \Rightarrow^+ < S_{MS}, 3 >$构成变换边, 又因为 $ATUN$ 中的 $MAC=f_{NK}^1(R_H \oplus R_U \| SQN \| AMF)$,$NK \notin K_p$,则边$< S_{MS}, 2 > \Rightarrow^+ < S_{MS}, 3 >$构成 $AUTN$ 关于 R_U 的输入测试,AUTN 是 R_U 的测试分量。根据定理 2,存在 $m, m' \in C$,使得 $AUTN$ 为 m' 的分量,并且 $m \Rightarrow^+ m'$ 是 R_U 的变换进行边。

根据定理 2,结点 m' 为正结点,而且 m' 是串 S_{AuC} 中的结点,$m'=< S_{AuC}, 3 >$,且 $AUTN$ 是 m' 的分量,由于常规正结点中包含 AUTN 形式的只有$< S_{AuC}, 3 >$,所以 C 中必然包含一个串 $S_{AuC}=\{R_M, A, AUTN, R_H, RES\}$。根据上述分析,MS 能成功地对 AuC 的身份进行认证。

3.2 安全性分析

本方案在沿用 LTE/SAE AKA 基本框架的同时,克服了其中的一些漏洞,提出 LTE-R 身份认证方案中

加强了对IMSI的保护,实现了MS和网络的双向认证,有效的解决了现有GSM-R中存在的安全问题。本方案主要实现了以下安全功能:

1)双向认证:本方案中MS和AuC之间实现了双向认证。MME/VLR代表HSS/AuC向MS发送随机数R_M作为挑战,MS返回了包含随机数R_U的*PID*、认证参数*A*和身份识别序列码*NC*作为响应,HSS/AuC通过*NC*确定MS身份,由*A*得出R_U,验证*PID*通过后,HSS/AuC响应MS的挑战,生成认证向量*AV*s,由MME/VLR选择一组认证向量发送给MS,MS验证MAC,通过后双向认证完成。

2)保护IMSI:在本方案中,MS发送的请求信息是$M_1=\{A,PID,NC\}$,IMSI并没有在信道中传输,攻击方就算截获了此信息,也无法获得MS的IMSI,认证中心通过*NC*识别MS,而*NC*在使用一次之后作废。攻击者不能根据*NC*来追踪用户。

3)克服根密钥泄露问题:传统GSM-R方案中根密钥长期在MS端储存并且使用,一旦泄露,协议便毫无安全性可言。本方案中*K*只被用来与随机数一起生成临时根密钥*DK*,而且协议主体认证过程均有*DK*完成,所以协商出的密钥K_{ASME}由随机数和*K*共同决定,这样*K*若意外泄露,攻击者也无法获取K_{ASME},提升协议整体的安全性。

4)机密性:只有同时拥有根密钥*K*和随机数生成*DK*才能从所截获的消息中得到有用的信息,即本方案满足机密性要求。

5)完整性:在本方案中,所发送的信息包含了用户匿名身份*PID*和*MAC*,AuC通过检查*XPID=PID*来确定所收到的消息又没有被篡改,而MS通过验证*XMAC=MAC*来确定所受信息的完整性。

同时本方案可以抵抗下列攻击:

1)拒绝服务攻击:在GSM-R协议执行时,IMSI以明文的方式发送给AuC,攻击者可以获得大量合法IMSI,若将这些IMSI发送给AuC会造成AuC生成大量认证参数,阻碍合法用户进行正常认证服务。本方案中IMSI不进行传输,而且AuC用来查询用户身份的*NC*只使用一次,攻击者既无法通过IMSI进行拒绝服务DoS攻击,而拦截获得的NC也已作废。

2)重放攻击:本协议每执行一次,MS、MME/VLR和HSS/AuC均会生成一个随机数,这些随机数相当于新鲜因子。若攻击者向AuC重放之前消息,因为MME/VLR每次都会生成新的随机数,所以AuC会验证失败;若向MS重放之前的消息,由于MS生成了新的随机数,验证MAC时将会失败。

3)重定向攻击:攻击者伪装合法的MS截获本地VLR_1和外网VLR_2消息之后,伪装成本地VLR_1将篡改后的消息发送给真MS即可发起重定向攻击。在本协议中,MS计算并发送$\{PID,A\}$至假VLR,攻击者伪装MS将$\{PID,A\}$发送至外网VLR_2,试图将网络重定向至VLR_2。但是由于两个VLR生成的随机数不同,HSS/AuC在验证PID时会验证失败,中止认证。

本方案与GSM-R方案及文献[4-5,12]之间安全属性比对如表1所示。

表1 安全属性对比

Tab.1 Security attribute contrast

安全属性	GSM-R方案	文献[4]	文献[5]	文献[12]	LTE-R方案
双向认证	N	Y	Y	Y	Y
IMSI保护	N	N	N	N	Y
克服*K*泄露	N	N	N	Y	Y
数据完整性	N	N	Y	Y	Y
抗DoS攻击	N	Y	Y	Y	Y
抗重放攻击	N	Y	Y	Y	Y
抗重定向攻击	N	N	N	Y	Y

注:表中N为该方案未达到此项要求,Y为达到要求。

4　效率分析

本方案与其他方案效率对比如表 2 所示，其中 T_e/T_d 表示对称加解密运算,T_x 代表异或运算,T_h 代表哈希运算。

表 2　各方案效率对比

Tab.2　Efficiency contrast

项目	GSM-R 方案	文献[4]	文献[12]	文献[5]	LTE-R 方案
MS 计算量	$2T_e+1T_d$	$4T_e$	$9T_h+1T_x$	$4T_e$	$4T_e+2T_h+T_x$
MME/VLR 计算量	$1T_e$	0	$3T_h+T_x$	0	0
HSS/AuC 计算量	$2T_e$	$4T_e$	$7T_h+1T_x$	$4T_e+1T_d$	$6T_e+2T_h+3T_x$
通信量/bit	608	960	1 779	1 776	1 712

由表 2 可知,本方案的计算量较 GSM-R 方案、文献[4]来说稍微多一点,通信量约为 GSM-R 方案的 3 倍,与文献[12]和文献[5]相差不大。但是本方案在安全性上较其他方案有较大优势,但随着网络技术和硬件技术的发展,网络传输速率和硬件处理数据的速率在不断地加快,本方案的运算量与通信在可以接受的范围之内。

5　结论

随着高速铁路的快速发展，传统 GSM-R 将不能满足铁路环境日益增长的安全需求,GSM-R 势必要向 LTE-R 发展。本文提出一个基于哈希和伪随机数的 LTE-R 认证方案,伪身份 PID 代替 IMSI 在信道中传输,同时,协议中的根密钥 K 只用来与随机数一起生成临时认证密钥 DK,由 DK 代替 K 执行协议接下来的认证与密钥协商过程,提高了根密钥的安全性。使用认证测试法证明了协议的正确性,即 MS 与 AuC 能完成双向认证。通过效率对比分析本方案的计算量和通信量均在可接受的范围之内,因此,本文提出的方案对于铁路部门制定安全性更高的 LTE-R 车地认证方案具有重要的参考价值。

参考文献:

[1] Third Generation Partnership Project (3GPP). Security architecture (Release11)[S]. France,ralbnne: 3GPP organiational Parlners, 2011.

[2] 杨达. 基于用户口令的 GSM-R 身份认证协议[J]. 兰州交通大学学报,2010,29(1):5-8.

[3] 吴昊,史晓华,谷勇浩. GSM-R 系统的安全策略研究与改进[J]. 北京交通大学学报,2009,33(2):127-130.

[4] 吴昊,史小华,范絮妍,等. CTCS-3 级列控系统车-地无线通信端到端通信安全增强技术的研究[J]. 铁道通信信号,2010,46(10):16-19.

[5] ZHANG M X. Security analysis and enhancements of 3 GPP authentication and key agreement protocol[J]. IEEE Transactions on Wireless Communications,2005,4(2):734-742.

[6] 许名松,李谢华,曹基宏,等. 一种安全增强型无线认证与密钥协商协议[J]. 计算机工程,2011,37(17):116-118,135.

[7] HAMANDI K,SARJI I,CHEHAB A,et al. A Privacy enhanced and computationally efficient HSK-AKA LTE scheme[C]// Advanced Information Networking and Applications Workshops(WAINA) 2013, Barcelona,2013:929-934.

[8] ALEZABI K A,HASHIM F,HASHIM S J,et al An efficient authentication and key agreement protocol for 4G (LTE) networks[P]. Region 10 Symposium, 2014 IEEE,2014.

[9] LAI C, LI H, LU R, et al. SE-aka: a secure and efficient group authenticaition and key agreement protocol for LTE networks[J]. Computer Networks, 2013, 57(17):3492-3510.

[10] CAO J, MA M, LI H, A group-based authentication and key agreement for MTC in LTE networks[C]// IEEE Global Communicaitons Conference (GLOBECOM), California,USA,2012:1017-1022.

[11] CAO J, LI H, MA M. GAHAP: a group-based anonymity handover authentication protocol for MTC in LTE-a networks[C]// IEEE International Conference on Communications. London,UK,2015:3020-3025.

[12] 白媛,王倩,贾其兰,等. 一种高效安全的 EPS AKA 协议[J]. 北京邮电大学学报,2015,(1):10-14.

[13] DENG Y P,FU H,XIE X Z, et al.A novel 3GPP sae authentication and key agreement protocol[C]// Network Infrastructure and Digital Content(IC-NIDC)2009.Beijing,2009:557-561.

[14] HWANG S J, CHAI M J. A new authenticated key agreement protocol for wireless mobile net-works[C]// Information Assurance and Security, 2009, IAS'09, Fifth International Conference 2009:53-56.

Security Analysis and Improvement of LTE-R Authentication and Key Agreement Protocol

Zhang Lihua[1], Jiang Panpan[2], Jiang Tengfei[2] , Li Jingjing[1]

(1. School of Software, East China Jiaotong University, Nanchang 330013, China; 2. School of Electrical and Automation Engineering, East China Jiaotong University, Nanchang 330013, China)

Abstract:Safe and efficient vehicle-ground identity authentication scheme is the basis for the safe railway operation. Combined with the requirements of secure data transmission of train control system for mobile communication system and the development direction of railway wireless communication network, a LTE-R vehicle-ground identity authentication protocol based on pseudo-random number and hash function is proposed. The IMSI transmission is replaced by the anonymous identity PID generated by IMSI and random number, which solves the security problem caused by IMSI leakage. The authentication process is completed by using the temporarily generated authentication key NK instead of the permanent root key K, and the security of root key K is improved. The correctness of the protocol is proved by the certification test method. The analysis confirms that the LTE-R identity authentication scheme proposed in this paper has good security and anonymity, and the computational communication consumption meets the efficiency requirements.

Key words: vehicle-ground communication; LTE-R; identity authentication; certification test method