EAP-AKA 协议的分析和改进*

张 胜，徐国爱，胡正名，杨义先
(北京邮电大学 信息安全中心，北京 100876)

摘 要：3G 与 WLAN 互连是当前研究的一个热点。EAP-AKA 是其对应的认证与密钥分配协议。详细分析 EAP-AKA 协议的流程和安全性，并针对其中的安全缺陷，提出一种改进的方案，同时对改进方案的安全性也进行了分析。

关键词：3G；WLAN；EAP-AKA；认证；密钥分配
中图法分类号：TP393.04 **文献标识码**：A **文章编号**：1001-3695(2005)07-0234-03

Analysis and Amendment of EAP-AKA Protocol

ZHANG Sheng, XU Guo-ai, HU Zheng-ming, YANG Yi-xian
(Information Security Center, Beijing University of Posts & Telecommunications, Beijing 100876, China)

Abstract: 3G-WLAN interworking is a research hotspot now, and EAP-AKA is its authentication and key agreement protocol. The paper analyses the procedure and security of EAP-AKA protocol, and the vulnerability and possible attack to this protocol are described. To the vulnerability and possible attack, an amended scheme is presented. Finally, an analysis of the amended scheme has been made.

Key words: 3G; WLAN; EAP-AKA; Authentication; Key Agreement

3G 与 WLAN 互连是指 WLAN 终端用户使用 3G 系统的资源和接入服务，互连的目的就是把 3G 系统的服务和功能扩展到 WLAN 接入环境，从而使 WLAN 有效地成为 3G 系统的补充无线接入网络。WLAN 的优势在于极高的接入速率，但覆盖范围有限。而 3G 系统有较大的覆盖能力，但是接入速率较低。因此，结合两者的优点进行网络建设已经成为大势所趋。

EAP-AKA(Extensible Authentication Protocol-Authentication and Key Agreement) 是 3G 与 WLAN 互连的认证和密钥分配协议，是保证其安全的基础。

1 基本标识符

本文采用如下标识符来描述协议：

(1) WLAN-UE。WLAN 用户的移动终端设备。WLAN-AN：WLAN 接入网络。3GPP AAA 服务器：3GPP 网络认证、授权、计费服务器。HSS/HLR：家乡用户服务器/家乡位置寄存器。IMSI：国际移动用户标志(International Mobile Station Identity)。A→B：X：A 向 B 发送消息 X。h：公开的散列函数。$E_K(X)$：使用对称密钥 K 加密 X 得到的密文。

(2) $f1$～$f5$。为 3G 安全结构中定义的算法，$f1$ 算法用于产生消息认证码，$f2$ 算法用于消息认证中计算期望响应值，$f3$ 算法用于产生加密密钥，$f4$ 算法用于产生完整性密钥，$f5$ 算法用于产生匿名密钥。

(3) NAI。网络接入标志(Network Access Identifier)，具体格式见 RFC 2486。NAI 中包含 WLAN-UE 的临时标志，该临时标志在 WLAN-UE 的上一次认证过程中取得。如果这是 WLAN-UE 的首次认证，则 NAI 中包含的是 WLAN-UE 的 IMSI。另外，NAI 中还包含 WLAN-UE 要进行认证的 3GPP AAA 服务器的地址。

收稿日期：2004-07-15；修返日期：2004-09-09
基金项目：国家自然科学基金资助项目(60372094)

2 EAP-AKA 协议流程

EAP-AKA 协议的实现由 WLAN-UE, WLAN-AN, 3GPP AAA 服务器和 HSS/HLR 来完成，实现流程如图 1 所示。

协议交互过程各个消息的组成如下：

① WLAN-UE→WLAN-AN: NAI
② WLAN-AN→3GPP AAA: NAI
③ 3GPP AAA→WLAN-AN: RAND, AUTH, WLAN-UE 的临时标志，消息鉴别码
④ WLAN-AN→WLAN-UE: RAND, AUTH, WLAN-UE 的临时标志，消息鉴别码
⑤ WLAN-UE→WLAN-AN: RES, 消息鉴别码
⑥ WLAN-AN→3GPP AAA: RES, 消息鉴别码
⑦ 3GPP AAA→WLAN-AN: WLAN-UE 的认证结果，WLAN-AN 与 WLAN-UE 的共享密钥
⑧ WLAN-AN→WLAN-UE: WLAN-UE 的认证结果

EAP-AKA 协议由 WLAN-AN 发起，WLAN-AN 首先向 WLAN-UE 发送一个 EAP 请求/身份标志消息，然后就开始了认证与密钥分配过程。下面对协议进行详细的描述：

①收到消息后，WLAN-UE 向 WLAN-AN 发送 EAP 回应/身份标志消息，其中包含 NAI 形式的身份标志。

②WLAN-AN 将收到的 EAP 回应/身份标志消息发送给 3GPP AAA 服务器。

③收到 WLAN-UE 的身份标志后，3GPP AAA 服务器首先询问 HSS，该用户是否有使用 WLAN 提供的服务权限。然后从 HSS/HLR 中取得与该用户相关的认证向量 AV，同时也获得与该用户 IMSI 对应的新的临时标志。其中，AV = RAND ‖ XRES ‖ CK ‖ IK ‖ AUTN，RAND 为随机数，XRES = $f2_k$(RAND)，CK = $f3_k$(RAND)，IK = $f4_k$(RAND)，AUTN = SQN⊕AK ‖ AMF ‖ MAC；SQN 为序列号，AK = $f5_k$(RAND)，AMF 为认

证管理域, MAC = $f1_k$(SQN ‖ RAND ‖ AMF) 。随后, 从 IK 和 CK 中生成共享密钥, 这些共享密钥一方面可用于 WLAN 通信的机密性和一致性保护, 另一方面也用于保护 WLAN-UE 的临时标志。构造 EAP 请求/AKA 挑战消息, 消息包含 RAND、AUTH、临时标志, 并计算消息鉴别码。最后, 将 EAP 请求/AKA 挑战消息发送给 WLAN-AN。

④WLAN-AN 将收到的 EAP 请求/AKA 挑战消息发送给 WLAN-UE。

⑤WLAN-UE 首先验证 AUTH, 并确认接收的序列号 SQN 是否在有效范围内, 如果都正确, 则实现了对 3G 网络的认证。计算 IK 和 CK, 从 IK 和 CK 中生成共享密钥, 然后验证消息鉴别码是否正确, 并保存收到的临时标志。计算 RES = $f2_k$ (RAND) , 构造 EAP 回应/AKA 挑战消息, 消息包含 RES, 并计算消息鉴别码。最后, 将 EAP 回应/AKA 挑战消息发送给 WLAN-AN。

⑥WLAN-AN 将收到的 EAP 回应/AKA 挑战消息发送给 3GPP AAA 服务器。

⑦3GPP AAA 服务器首先验证消息鉴别码, 然后计算 XRES, 并与收到的 RES 进行比较。如果正确, 则认证了 WLAN-UE 的身份, 并向 WLAN-AN 发送 EAP 成功的消息。同时一起发送的还有在 WLAN 通信中用于机密性和一致性保护的共享密钥。

⑧WLAN-AN 保存共享密钥, 此共享密钥将用于与 WLAN-UE 通信时的机密性和一致性保护, 同时将 EAP 成功的消息发送给 WLAN-UE。

上述流程完成后, WLAN 用户与 3G 网络之间就实现了双向认证。并且, WLAN-UE 与 WLAN-AN 之间共享了会话密钥, 这些密钥可用于 WLAN 通信中的机密性和一致性保护。

3　EAP-AKA 协议的安全性分析

EAP-AKA 协议基于 WLAN-UE 与 HSS/HLR 之间共享的秘密密钥 K, 实现 WLAN 用户与 3G 网络的相互认证和密钥分配。对该协议的安全性分析具体描述如下:

(1) WLAN 用户与 3G 网络之间的双向认证。WLAN 用户对 3G 网络的认证是在上述第⑤步实现的。WLAN-UE 收到 3GPP AAA 服务器发送过来的 AUTN = SQN⊕ AK ‖ AMF ‖ MAC, 确认序列号 SQN 是否在有效范围内, 并验证 AUTH 是否正确。因为只有使用正确的秘密密钥 *K* 才能生成正确的 AUTN, 而只有合法的 HSS/HLR 才有秘密密钥 *K*, 因此上述过程实现了对 3G 网络合法性认证。

3G 网络对 WLAN 用户的认证是在上述第⑦步实现的。3GPP AAA 服务器首先计算 XRES = $f2_k$(RAND) , 然后与收到的 RES = $f2_k$(RAND) 进行比较。也因为只有合法的 WLAN 用户才有秘密密钥 *K*, 因此如果 XRES = RES, 就可以认证 WLAN 用户的合法身份。

(2) WLAN-UE 与 WLAN-AN 之间的密钥分配。合法的 WLAN-UE 收到正确的随机数 RAND 后, 能正确生成 CK = $f3_k$ (RAND) 和 IK = $f4_k$ (RAND) , 进而能正确生成用于 WLAN 通信中机密性和一致性保护的会话密钥。而 WLAN-AN 的会话密钥是从 3GPP AAA 服务器得到的, 3GPP AAA 服务器首先生成 CK 和 IK, 然后生成会话密钥, 再传送给 WLAN-AN。因此, EAP-AKA 协议能确保 WLAN-UE 与 WLAN-AN 之间能共享会话密钥, 并且会话密钥没有在无线接口中传输, 具有一定的安全性。

(3) 密钥的新鲜性。在 EAP-AKA 协议的每次认证过程中, WLAN-UE 与 WLAN-AN 共享的会话密钥通过 CK 与 IK 生成, 而 CK 与 IK 是采用随机数计算得到的, 从而确保了密钥的新鲜性。

(4) 防重放攻击。协议传递的消息使用了随机数和不断递增的序列号 SQN 作为输入, 因而保证了消息的新鲜性。并且, 该随机数包含在保证消息完整性的消息鉴别码, 而响应方在响应消息的鉴别码中也包含了该随机数, 因此任何第三方都无法利用先前截获的消息发起重放攻击。

(5) 潜在的漏洞。与 3G 的认证与密钥分配协议 AKA 一样, EAP-AKA 协议也没有 WLAN 用户与 3G 网络之间共享的秘密密钥 K 的更新机制, 这可能会导致 USIM 克隆攻击。

另外, 当 WLAN 用户首次进行认证, 或 3G 网络不认识 WLAN 用户的临时标志时, WLAN 用户需传送 IMSI, 并且使用的是明文, 这会影响用户身份的机密性。

(6) 可能的攻击。文献[6] 中提到, 3G 网络的认证与密钥分配协议 AKA 存在 MS(移动站) 假冒攻击的可能。事实上, 同样的攻击也可能发生在 EAP-AKA 协议上。并且, 由于 WLAN 的覆盖范围小, WLAN-AN 与 WLAN-UE 一样, 都处在比较开放的环境中, 因而还有可能发生 WLAN-AN 假冒攻击。具体描述如下: ①WLAN-AN 假冒攻击。EAP-AKA 协议实现了 WLAN 用户与 3G 网络之间的相互认证, 但双方都没有对 WLAN-AN 的身份进行认证。并且, 在协议第⑧步中, 3GPP AAA 服务器将用于 WLAN 通信中机密性和完整性保护的会话密钥, 直接以明文的形式发送给 WLAN-AN。如果攻击者首先利用某种方式(如 DoS 攻击) 攻陷 WLAN-AN, 然后假冒成 WLAN-AN, 则可以获取 WLAN 中的会话密钥, 这样就使得 WLAN 的通信失去了保密性。②WLAN-UE 假冒攻击。攻击者 A 还可利用截获的合法用户身份标志进行攻击(图 2) 。

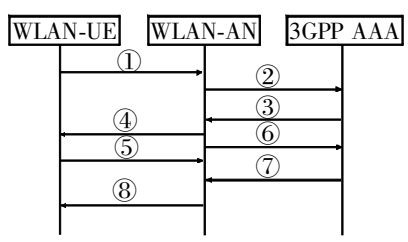

图 1　EAP-AKA 协议实现流程示意图

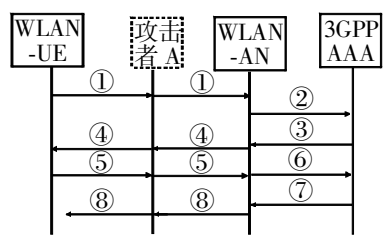

图 2　WLAN-UE 假冒攻击实现示意图

这样, 攻击者 A 就可以假冒该用户的身份入网。因为没有会话密钥, 因此攻击者 A 此时还不能进行正常的通信。而如果攻击者 A 同时对 WLAN-AN 与 3GPP AAA 服务器之间的通信进行窃听, 则可以获取 WLAN-UE 的会话密钥。此时攻击者 A 就可以假冒该用户, 在 3G 与 WLAN 互联网络中进行正常的通信。

4　改进方案

对于 EAP-AKA 协议缺乏主密钥 *K* 更新机制和明文传送 IMSI 的潜在漏洞, 最终只能通过公钥密码来解决。而针对 EAP-AKA 协议可能导致 WLAN-AN 假冒攻击与 WLAN-UE 假冒攻击的安全缺陷, 可借鉴文献[6] 的思路来改进。本文的改

进方案基于 WLAN-UE 与 WLAN-AN 之间的共享秘密,实现了对 WLAN-AN 的认证,并对 3GPP AAA 服务器传送的共享密钥进行了安全处理,从而有效地防止了 WLAN-AN 假冒攻击与 WLAN-UE 假冒攻击。

假设 WLAN-UE 与 WLAN-AN 之间有共享的秘密密钥 K,r 是一个任意的秘密随机数。改进方案与原方案相比,交互流程和传递的消息次数完全一样,只是对某些消息的内容作了改动。改进方案的消息组成如下:

① WLAN-UE→WLAN-AN: NAI

② WLAN-AN→3GPP AAA: NAI

③ 3GPP AAA→WLAN-AN: RAND, AUTH, WLAN-UE 的临时标志, $E_K(r)$, 消息鉴别码

④ WLAN-AN→WLAN-UE: RAND, AUTH, WLAN-UE 的临时标志, $E_K(r)$, 消息鉴别码

⑤ WLAN-UE→WLAN-AN: RES, $E_K(r)$, 消息鉴别码

⑥ WLAN-AN→3GPP AAA: RES, $h(r)$, 消息鉴别码

⑦ 3GPP AAA→WLAN-AN: WLAN-UE 的认证结果, E_r(WLAN-AN 与 WLAN-UE 的密钥)

⑧ WLAN-AN→WLAN-UE: 对 WLAN-UE 的认证结果

在改进方案的第③步中,3GPP AAA 服务器秘密选择一个随机数 r,然后用与 WLAN-UE 共享的秘密密钥 K 加密,将密文 $E_K(r)$ 随同其他消息一起发送给 WLAN-AN。

在第⑤步,WLAN-UE 将 $E_K(r)$ 解密,得到 r,然后用与 WLAN-AN 共享的秘密密钥 K 加密,将密文 $E_K'(r)$ 发送给 WLAN-AN。

在第⑥步,WLAN-AN 将 $E_K'(r)$ 解密,得到 r,然后计算 $h(r)$,将 $h(r)$ 随同其他消息一起发送给 3GPP AAA 服务器。

在第⑦步,3GPP AAA 服务器验证 $h(r)$,因为只有合法的 WLAN-AN 才能从 $E_K'(r)$ 中得到正确的 r,从而可以认证 WLAN-AN 的合法身份。然后用 r 加密 WLAN-AN 与 WLAN-UE 之间的共享密钥,将密文随同其他消息一起发送给 WLAN-AN。

在第⑧步,WLAN-AN 将 E_r(WLAN-AN 与 WLAN-UE 之间的共享密钥)解密,从而可以得到会话密钥。因为只有合法的 WLAN-AN 才能得到正确的 r,因此可以保证会话密钥不被窃听。

5 改进方案的安全性分析

改进方案通过 WLAN-UE 与 WLAN-AN 之间的共享秘密密钥 K,增加了原有协议的安全特性。具体描述如下:

(1) 3GPP AAA 服务器对 WLAN-AN 的身份认证。由于 3GPP AAA 服务器与 WLAN-AN 之间没有共享秘密,因此无法实现直接认证,只有通过 WLAN-UE 来间接实现。3GPP AAA 服务器对 WLAN-AN 的认证依赖随机数 r 的机密性,3GPP AAA 服务器发送的 $E_K(r)$ 只有合法的 WLAN-UE 才能正确解密,而 WLAN-UE 发送的 $E_K'(r)$ 也只有合法的 WLAN-AN 才能正确解密。因此,当 3GPP AAA 服务器接收到 WLAN-AN 发送来的正确的 $h(r)$ 后,就能确认 WLAN-AN 的合法身份。

(2) 会话密钥的机密性。改进方案中,3GPP AAA 服务器发送给 WLAN-AN 的会话密钥通过随机数 r 进行了加密处理。由于 r 的机密性,从而可以保证会话密钥不被窃听,保证了会话密钥的机密性。

通过上述分析,我们得知改进方案在保持原有协议安全性的基础上,能有效地防止 WLAN-AN 假冒攻击与 WLAN-UE 假冒攻击。并且与原协议相比,没有增加消息的传递次数,仅增加了认证过程的运算量。而这些运算是产生随机数、加/解密、计算散列值等,因此对协议效率不会产生较大的影响。

6 结论

本文通过对 EAP-AKA 协议安全性的分析,发现存在发生 WLAN-AN 假冒攻击与 WLAN-UE 假冒攻击的可能,并提出一种改进方案。改进方案通过 WLAN-UE 与 WLAN-AN 之间的共享秘密,增加了 3GPP AAA 服务器对 WLAN-AN 的身份认证和会话密钥的机密性保护,有效地防止了上述攻击。改进方案没有增加认证消息的传递次数,对原协议效率没有造成较大的影响,具有一定的应用价值。

参考文献:

[1] 3GPP TS 33.102. 3G Security: Security Architecture[EB/OL]. http://ftp.3gpp.org/Specs/, 2000-10.

[2] 3GPP TS 33.234 v0.6.0. 3G Security: Wireless Local Area Network (WLAN) Interworking Security, Release 6, 2003-9[EB/OL]. http://ftp.3gpp.org/Specs/, 2004-03.

[3] 3GPP TS 33.234 v0.7.0. 3G Security: Wireless Local Area Network (WLAN) Interworking Security, Release 6, 2003-11[EB/OL]. http://ftp.3gpp.org/Specs/, 2004-03.

[4] 3GPP TS 33.234 v1.0.0. 3G Security: Wireless Local Area Network (WLAN) Interworking Security, Release 6, 2003-12[EB/OL]. http://ftp.3gpp.org/Specs/, 2004-03.

[5] 3GPP TS 33.234 v1.0.1. 3G Security: Wireless Local Area Network (WLAN) Interworking Security, Release 6, 2004-2[EB/OL]. http://ftp.3gpp.org/Specs/, 2004-03.

[6] 刘东苏,韦宝典,王新梅.改进的 3G 认证与密钥分配协议[J]. 通信学报, 2002, (5): 119-122.

作者简介:

张胜(1974-),男,博士生,研究方向为密码学与网络安全;徐国爱(1972-),男,副教授,研究方向为密码学与网络安全;胡正名(1931-),男,博士生导师,研究方向为编码密码学;杨义先(1961-),男,博士生导师,研究方向为编码学与信息安全。

(上接第 162 页)

[3] 宋建社. 小波分析及其应用例选[M]. 北京:现代出版社, 1998. 23-60, 204-231.

[4] Marr D, Hildreth E. Theory of Edge Detection[C]. Proc. R. Soc. Lond 1980, B207. 187-217.

[5] 姬光荣,王国宇,王宁. 基于小波变换的多尺度边缘检测[J]. 中国图像图形学报, 1997, 2(10): 717-720.

[6] 郦苏丹. SAR 图像特征提取与目标识别方法研究[D]. 长沙:国防科技大学, 2001. 10-18.

[7] 唐正军,宋建社. SAR 图像边缘的小波抽取算法研究[J]. 上海航天, 1999, (1): 1-5.

[8] J Chanussot, G Mauris. Fuzzy Fusion Techniques for Linear Feature Detection in Multitemporal SAR Images[J]. IEEE Trans. Geosc. and Remote Sensing, 1999, 31(3): 1292-1305.

作者简介:

廖增为(1980-),学士,硕士,研究方向为雷达图像自动识别;宋建社(1954-),教授,硕博导师,博士,研究方向为军事运筹学信息系统分析与处理方向。