ICS 35.040
L 80

中华人民共和国国家标准

GB/T 39205—2020

信息安全技术
轻量级鉴别与访问控制机制

Information security technology—
Light-weight authentication and access control mechanism

2020-10-11 发布　　2021-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:西安西电捷通无线网络通信股份有限公司、中关村无线网络安全产业联盟、国家无线电监测中心检测中心、国家密码管理局商用密码检测中心、中国电子技术标准化研究院、天津市无线电监测站、中国科学院软件研究所、国家信息技术安全研究中心、北京数字认证股份有限公司、数安时代科技股份有限公司、重庆邮电大学、北京大学深圳研究生院、中国通用技术研究院、北京计算机技术及应用研究所。

本标准主要起草人:李琴、杜志强、黄振海、张国强、颜湘、陶洪波、李冬、李冰、许玉娜、刘景莉、铁满霞、王月辉、吴冬宇、于光明、龙昭华、朱跃生、张永强、张严、熊克琦、刘科伟、赵晓荣、张变玲、高德龙、郑骊、王莹、赵慧、张璐璐、朱正美、黄奎刚、傅强。

引　言

本文件的发布机构提请注意，声明符合本文件时，可能涉及与5.2相关的ZL201410041837.0、US9，860，070B2、JP6353548B2、EP15743408.5、KR10-1857048，与5.4相关的ZL201010567506.2、US9，450，756B2、EP10858333.7，与6.2相关的ZL201010153096.7，与6.3相关的ZL201010153734.5等专利的使用。

本文件的发布机构对于上述专利的真实性、有效性和范围无任何立场。

该专利持有人已向本文件的发布机构保证，他愿意同任何申请人在合理且无歧视的条款和条件下，就专利授权许可进行谈判。该专利持有人的声明已在本文件的发布机构备案。相关信息可通过以下联系方式获得：

专利权人：西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路68号西安软件园秦风阁A201

联系人：冯玉晨

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

网址：http://www.iwncomm.com

专利权人：国家无线电监测中心检测中心、西安西电捷通无线网络通信股份有限公司

地址：西安市高新区科技二路68号西安软件园秦风阁A201

联系人：冯玉晨

邮政编码：710075

电子邮件：ipri@iwncomm.com

电话：029-87607836

传真：029-87607829

网址：http://www.iwncomm.com

请注意除上述专利外，本文件的某些内容仍可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

信息安全技术
轻量级鉴别与访问控制机制

1 范围

本标准规定了轻量级的鉴别机制与访问控制机制。

本标准适用于无线传感器网络、射频识别、近场通信等资源受限的应用场景下鉴别与访问控制机制设计开发和应用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 15629.3—2014 信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第3部分：带碰撞检测的载波侦听多址访问(CSMA/CD)的访问方法和物理层规范

GB/T 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3密码杂凑算法

GB/T 32907 信息安全技术 SM4分组密码算法

ISO/IEC 29180:2012 信息技术 系统间远程通信和信息交换 泛在传感器网络安全框架(Information technology—Telecommunications and information exchange between systems—Security framework for ubiquitous sensor networks)

3 术语和定义

GB/T 25069界定的以及下列术语和定义适用于本文件。

3.1

鉴别机制 authentication mechanism

证实实体是其所声称的实体的机制。

3.2

访问控制 access control

保证数据处理系统的资源只能由被授权主体按照授权方式进行访问的手段。

3.3

可信第三方 trusted third party

在同安全相关的活动方面，被其他实体信任的安全机构或其代理。

注：可信第三方是实体A和实体B所信任的第三方实体，可对实体A和实体B的身份真实性进行验证。

4 符号和缩略语

4.1 符号

下列符号适用于本文件。

⊕：异或运算(XOR)

‖：消息串联

<<<：左循环移位

＋：模加

－：模减

O_n：长度为 n 比特的二进制常量

Q：用户对某一资源的访问请求

4.2 缩略语

下列缩略语适用于本文件。

ACL：访问控制列表(Access Control List)

ACr：访问控制器(Access Controller)

ADT：授权的数据类型(Authorized Data Type)

AI：鉴别信息(Authenticated Information)

CT：密文(Cryptographic Text)

DAE：目的访问实体(Destination Access Entity)

ET：加密后的文本(Encrypted Text)

HMAC：基于密码杂凑产生的消息鉴别码(Hash Based Message Authentication Code)

KD：密钥推导(Key Derivation)

MAC：消息鉴别码(Message Authentication Code)

MEK：消息加密密钥(Message Encryption Key)

MIC：消息完整性校验(Message Integrality Check)

MIK：消息完整性密钥(Message Integrality Key)

PSK：预共享密钥(Pre-Shared Key)

SK：会话密码(Session Key)

VP：有效期(Valid Period)

5 轻量级鉴别机制

5.1 概述

轻量级鉴别机制在实现实体之间的身份真实性确认的同时降低鉴别过程中的计算和通信复杂度。较之通常的机制，轻量级鉴别机制有如下几个衡量角度：

a) 计算资源占用少；

b) 交互消息少；

c) 耗时短；

d) 所需要的存储空间少。

5.2 基于异或运算的鉴别机制

基于异或运算的鉴别机制，通过简单的异或、移位运算来实现实体 A 和实体 B 之间的身份真实性的确认，鉴别过程见图 1。

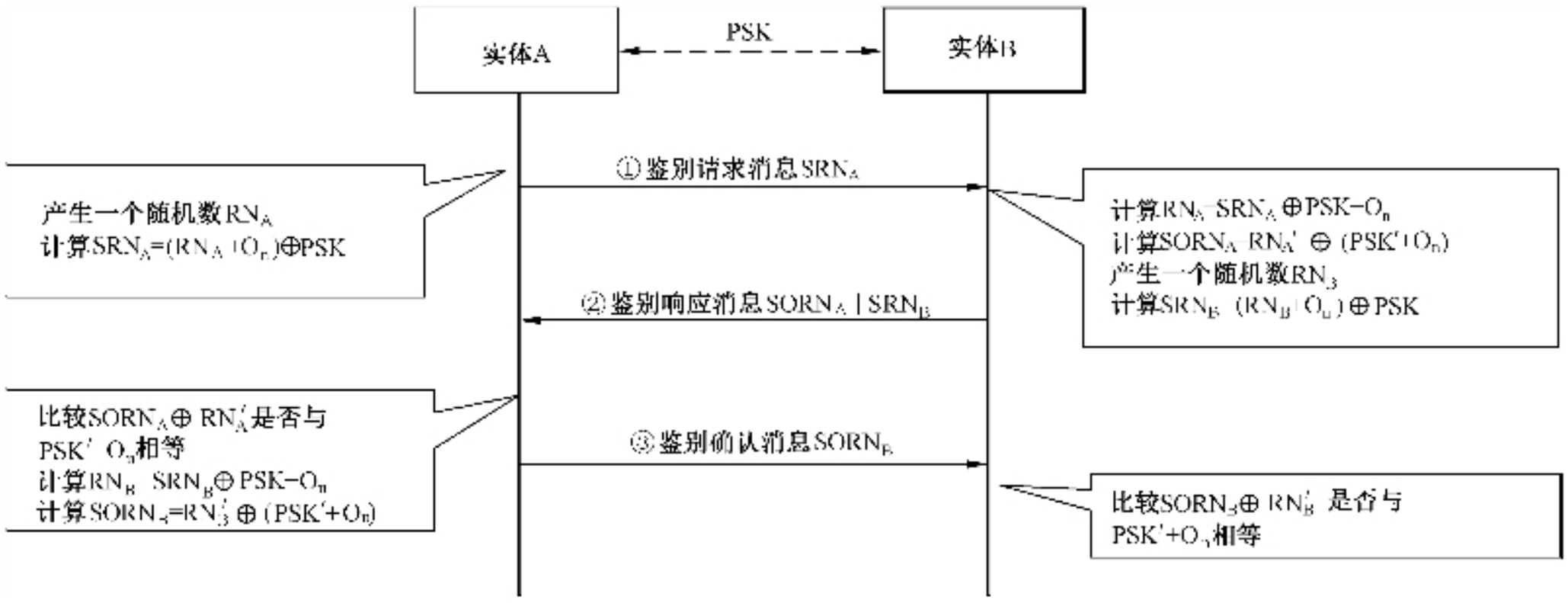

图 1　基于异或运算的鉴别机制消息交互示意图

鉴别之前，实体 A 和实体 B 应具备预共享密钥 PSK 和共享常量 O_n，用 n 表示机制中随机数和密钥的长度，预共享密钥 PSK 的使用应符合特定场景的需求，随机数的长度应和 PSK 长度保持一致。鉴别过程如下：

a) 实体 A 产生一个随机数 RN_A，计算 $SRN_A=(RN_A+O_n)\oplus PSK$，并向实体 B 发鉴别请求消息 SRN_A。其中 O_n 是长度为 n 的二进制常量，n 的长度选择与机制中所使用的 PSK 和随机数长度一致，推荐 O_n 为长度为 n 比特的 01 交替的二进制常量；其中 + 是在 2^n 模加；

b) 实体 B 收到鉴别请求消息后，首先计算 $RN_A=SRN_A\oplus PSK\text{-}O_n$，并计算 $SORN_A=RN_A'\oplus(PSK'+O_n)$，其中 $RN_A'=RN_A<<<s$，$PSK'=PSK<<<s$，即 RN_A' 和 PSK' 分别表示 RN_A 和 PSK 在随机数长度比特向量上向左循环移位 s 比特后的值，s 的取值为 RN_A 中值为 1 的比特的个数；实体 B 产生一个随机数 RN_B，计算 $SRN_B=(RN_B+O_n)\oplus PSK$。实体 B 发送鉴别响应消息 $SORN_A \| SRN_B$ 给实体 A；

c) 实体 A 收到鉴别响应消息后，分别计算 $SORN_A\oplus RN_A'$ 和 $PSK'+O_n$，比较 $SORN_A\oplus RN_A'$ 是否与 $PSK'+O_n$ 相等，如果不相等，则实体 A 丢弃该消息；如果相等，则实体 A 对实体 B 鉴别成功。然后实体 A 计算 $RN_B=SRN_B\oplus PSK-O_n$，并计算 $SORN_B=RN_B'\oplus(PSK'+O_n)$，其中 $RN_B'=RN_B<<<m$，$PSK'=PSK<<<m$，m 的取值为 RN_B 中值为 1 的比特的个数，实体 A 向实体 B 发送鉴别确认消息 $SORN_B$；其中 − 是在 2^n 模减；

d) 实体 B 收到鉴别确认消息后，分别计算 $SORN_B\oplus RN_B'$ 和 $PSK'+O_n$，比较 $SORN_B\oplus RN_B'$ 是否与 $PSK'+O_n$ 相等，如果相等，则实体 B 对实体 A 鉴别成功。

注 1：上述机制中 RN_A、RN_B 的运算均先算异或后算模减；

注 2：基于异或运算的鉴别机制，利用了异或、移位运算实现鉴别，计算量小，鉴别过程耗时短，所需存储空间少；其安全性相对于 5.3 和 5.4 两种机制较弱，适用于计算资源、存储资源受限，但对安全有一定需求的应用场景。

5.3　基于密码杂凑算法的鉴别机制

基于密码杂凑算法的鉴别机制利用密码杂凑算法实现实体 A 和实体 B 之间的身份真实性的确认，交互过程见图 2。该机制中密码杂凑算法应使用 GB/T 32905 定义的 SM3 算法，使用 SM3 算法时，HMAC 为 HAMC-SM3，KD-HMAC 为 KD-HMAC-SM3；其中 HMAC-SM3 和 KD-HMAC-SM3 定义见 GB/T 15629.3—2014 的附录 I 中 I.10.4 和 I.10.5。

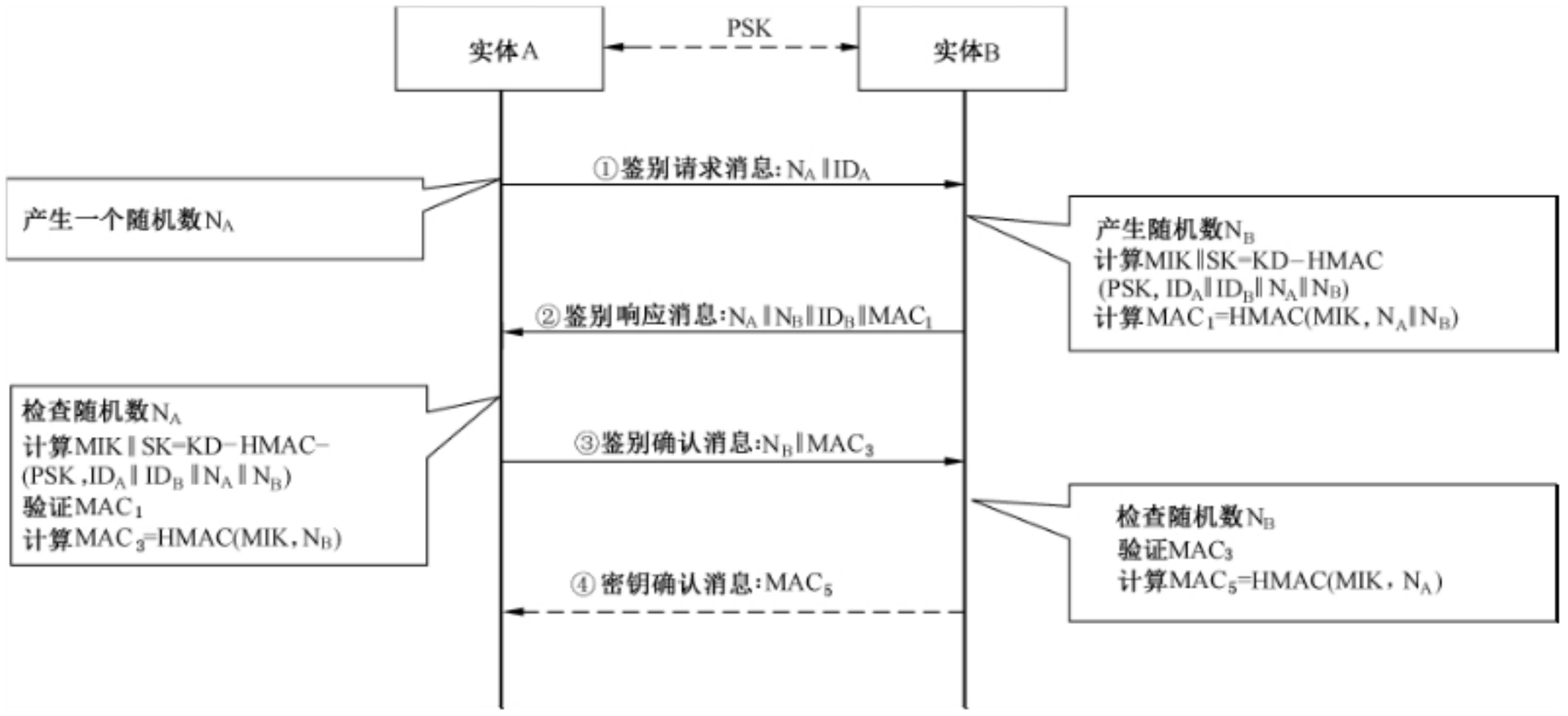

图 2　基于密码杂凑算法的鉴别机制消息交互示意图

鉴别之前，实体 A 应具备身份信息 ID_A，实体 B 应具备身份信息 ID_B，实体 A 和实体 B 应具备预共享密钥 PSK，预共享密钥 PSK 的使用应符合特定场景的需求，随机数的长度应和 PSK 长度保持一致。鉴别过程如下：

a)　实体 A 产生一个随机数 N_A，并向实体 B 发送包含 N_A 和 ID_A 的鉴别请求消息。

b)　实体 B 收到实体 A 的鉴别请求消息后，产生随机数 N_B，并利用密钥列表中与实体 A 预共享的密钥 PSK，根据 ID_A、ID_B、N_A、N_B 计算 $MIK \| SK = KD\text{-}HMAC(PSK, ID_A \| ID_B \| N_A \| N_B)$，其中，$ID_A$ 和 ID_B 分别是实体 A 和实体 B 的身份标识，MIK 为实体 A 与实体 B 之间的消息完整性密钥，SK 为实体 A 与实体 B 之间的会话密钥。然后，实体 B 利用 MIK 计算消息鉴别码 $MAC_1 = HMAC(MIK, N_A \| N_B)$，并构造鉴别响应消息 $N_A \| N_B \| ID_B \| MAC_1$ 发送给实体 A。

c)　实体 A 收到实体 B 的鉴别响应消息后，首先检查鉴别响应消息中的随机数 N_A 与其在步骤 a)中发送给实体 B 的随机数 N_A 是否一致，若不一致，实体 A 对实体 B 鉴别失败；若一致，实体 A 计算 $MIK \| SK = KD\text{-}HMAC(PSK, ID_A \| ID_B \| N_A \| N_B)$，并利用 MIK 计算消息鉴别码 $MAC_2 = HMAC(MIK, N_A \| N_B)$，如果 $MAC_2 \neq MAC_1$，实体 A 对实体 B 鉴别失败；如果 $MAC_2 = MAC_1$，则实体 A 将 SK 保存为与实体 B 的会话密钥，并计算 $MAC_3 = HMAC(MIK, N_B)$，构造鉴别确认消息 $N_B \| MAC_3$ 发送给实体 B；若实体 A 和实体 B 使用该机制且不含密钥确认消息时，实体 A 在发出鉴别确认消息后的一段时间后或在正确解密实体 B 使用该会话密钥加密发来的消息后，实体 A 对实体 B 鉴别成功，实体 A 启用该会话密钥；若实体 A 和实体 B 使用该机制且含密钥确认消息时，按照步骤 e)执行后续操作。

d)　实体 B 收到实体 A 的鉴别确认消息后，检查鉴别确认消息中的随机数 N_B 与其在步骤 b)中发送给实体 A 的随机数 N_B 是否一致，若不一致，实体 B 对实体 A 鉴别失败；若一致，实体 B 计算消息鉴别码 $MAC_4 = HMAC(MIK, N_B)$，如果 $MAC_4 \neq MAC_3$，实体 B 对实体 A 鉴别失败；如果 $MAC_4 = MAC_3$，则实体 B 对实体 A 鉴别成功，实体 B 将 SK 保存并启用作为与实体 A 之间的会话密钥。若实体 A 和实体 B 使用该机制且不含密钥确认消息时，实体 B 完成鉴别过程开始与实体 A 进行会话；若实体 A 和实体 B 使用该机制且含密钥确认消息时，计算 $MAC_5 = HMAC(MIK, N_A)$，并发送密钥确认消息 $N_A \| MAC_5$ 给实体 A，用于通知实体 A 启用会话密钥 SK。

e) 实体 A 收到实体 B 的密钥确认消息后，实体 A 计算 $MAC_6 = HMAC(MIK, N_A)$，如果 $MAC_6 \neq MAC_5$，实体 A 对实体 B 鉴别失败；如果 $MAC_6 = MAC_5$，则实体 A 对实体 B 鉴别成功，实体 A 启用会话密钥 SK，开始与实体 B 进行会话。

5.4 基于分组密码算法的鉴别机制

基于分组密码算法的鉴别机制，利用分组密码算法实现实体 A 和实体 B 之间的身份鉴别，交互过程见图 3。该机制中分组密码算法应使用 GB/T 32907 定义的 SM4 算法。

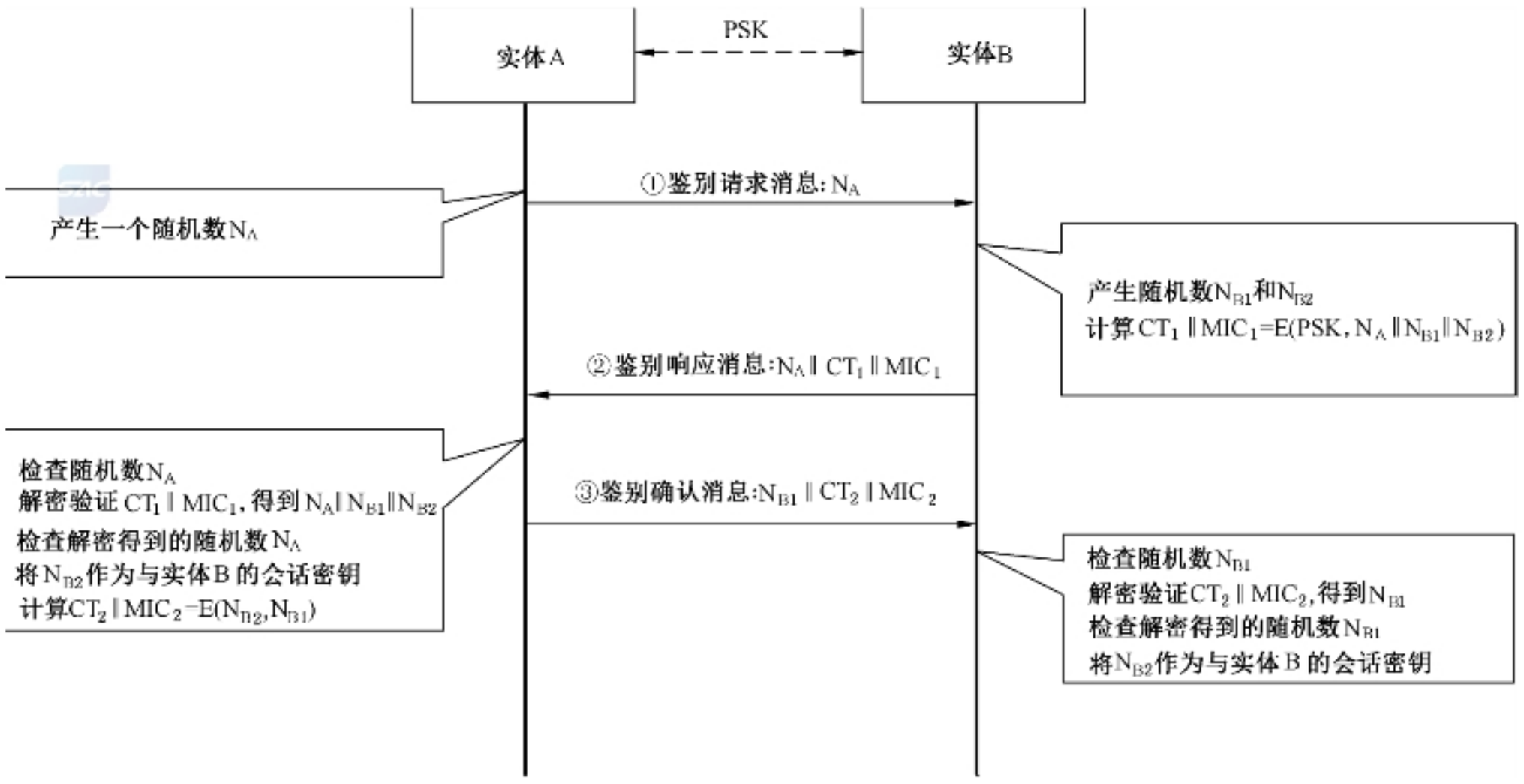

图 3 基于分组密码算法的鉴别机制消息交互示意图

鉴别之前，实体 A 应具备身份信息 ID_A，实体 B 应具备身份信息 ID_B，实体 A 和实体 B 应具备预共享密钥 PSK，预共享密钥 PSK 的使用应符合特定场景的需求，随机数的长度应和 PSK 长度保持一致。鉴别过程如下：

a) 实体 A 产生一个随机数 N_A，并向实体 B 发送包含 N_A 的鉴别请求消息；

b) 实体 B 收到实体 A 的鉴别请求消息后，生成随机数 N_{B1} 和 N_{B2}，计算 $CT_1 \| MIC_1 = E(PSK, N_A \| N_{B1} \| N_{B2})$，并向实体 A 发送包含 $N_A \| CT_1 \| MIC_1$ 的鉴别响应消息；

c) 实体 A 收到实体 B 发送的鉴别响应消息后，首先判断该消息中的 N_A 与其在步骤 a)中发送给实体 B 的 N_A 是否一致，如果不一致，则实体 A 对实体 B 鉴别失败；如果一致，实体 A 利用 PSK 解密验证 $CT_1 \| MIC_1$，如果 MIC_1 验证不通过，则实体 A 对实体 B 鉴别失败；如果 MIC_1 验证通过，则进一步验证解密得到 N_A 与其在步骤 a)中发送给实体 B 的 N_A 是否一致，如果不一致，则实体 A 对实体 B 鉴别失败；如果一致，则实体 A 对实体 B 鉴别成功，实体 A 将解密得到的 N_{B2} 作为与实体 B 的会话密钥，计算 $CT_2 \| MIC_2 = E(N_{B2}, N_{B1})$，并向实体 B 发送鉴别响应确认消息，该消息中包括字段 $N_{B1} \| CT_2 \| MIC_2$；

d) 实体 B 收到实体 A 的鉴别响应确认消息后，首先判断该消息中的 N_{B1} 与其在步骤 b)中发送给实体 A 的 N_{B1} 是否一致，如果不一致，则实体 B 对实体 A 鉴别失败；如果一致，则实体 B 利用 N_{B2} 解密验证 $CT_2 \| MIC_2$，如果 MIC_2 验证不通过，则实体 B 对实体 A 鉴别失败；如果 MIC_2 验证通过，则进一步验证解密得到 N_{B1} 与其在步骤 b)中发送给实体 A 的 N_{B1} 是否一致，如果不一致，则实体 B 对实体 A 鉴别失败；如果一致，则实体 B 对实体 A 鉴别成功，实体 B 将 N_{B2} 作为

与实体 A 的会话密钥。

注：E 为一种分组加密算法，CT ‖ MIC=E(KEY,S)表示将 KEY 对 S 进行加密并计算完整性校验码，其中 CT 表示密文，MIC 表示完整性校验码，CT 和 MIC 的拆分取决于具体的应用。在一些模式中，需先基于 KEY 导出消息完整性校验密钥和消息加密密钥，然后再分别使用该两个密钥计算完整性校验码和密文。在解密验证时，根据所使用的模式不同，验证完整性校验码和解密的先后顺序可能不同。

6 轻量级访问控制机制

6.1 概述

轻量级访问控制机制基于分组密码算法或访问控制列表 ACL 等实现对用户的访问控制。较之通常的机制，轻量级访问控制机制从 5.1 所列出的几个角度进行衡量。

6.2 基于分组密码算法的访问控制机制

本机制基于分组密码算法实现访问控制。其中，ACr 是访问控制器，User 是用户，DAE 是目的访问实体。ACr 对 User 访问 DAE 的控制过程见图 4。该机制中分组密码算法应使用 GB/T 32907 定义的 SM4 算法；该机制中密码杂凑算法应使用 GB/T 32905 定义的 SM3 算法，使用 SM3 算法时，HMAC 为 HAMC-SM3。分组密钥算法分组的长度应符合特定场景的需求，随机数的长度应和 PSK 长度保持一致。

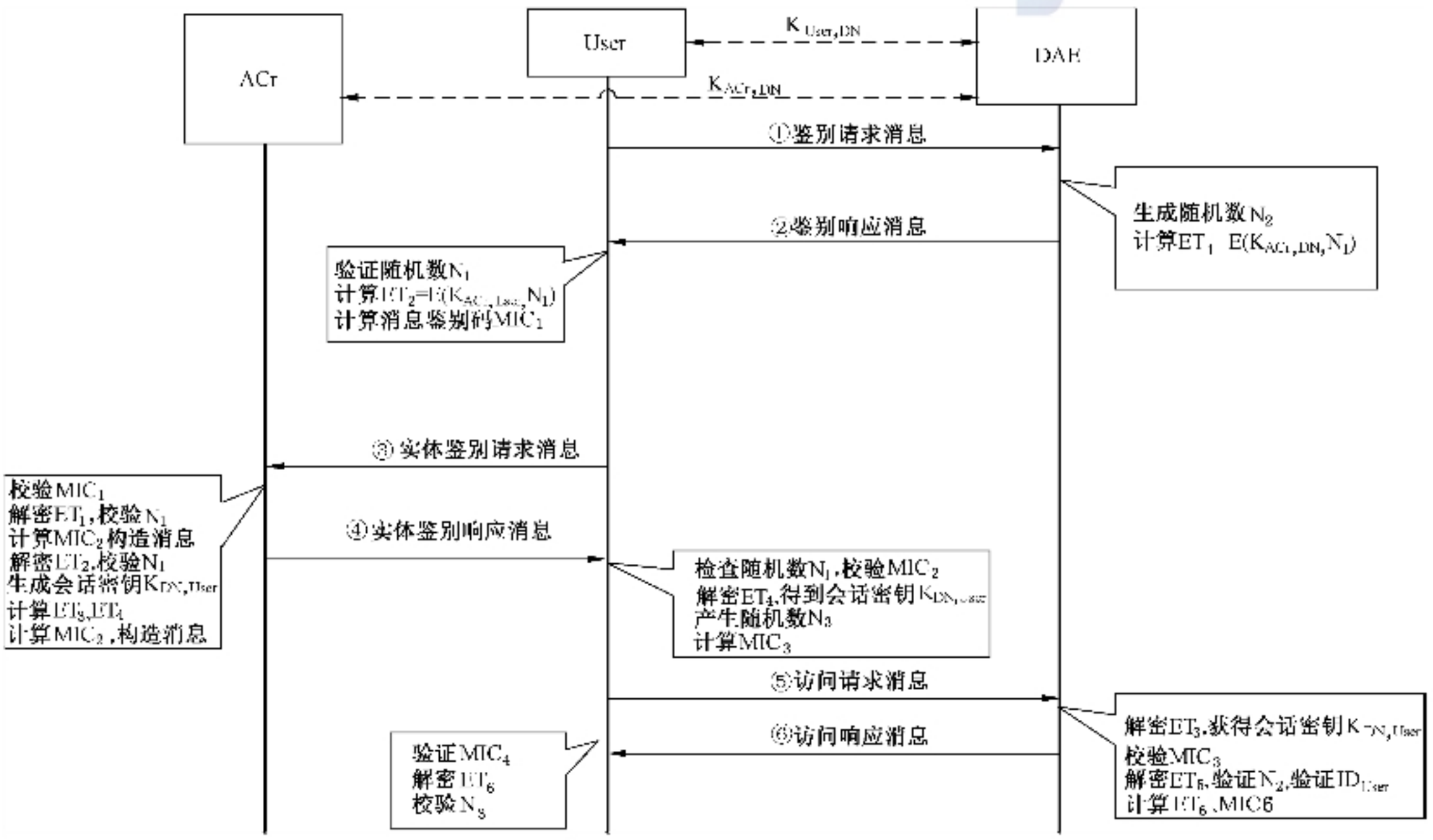

图 4 基于分组密码算法的访问控制机制消息交互示意图

访问控制过程如下：

a) User 在向网络中的 DAE 发送访问请求之前，首先向 DAE 发送鉴别请求消息，该消息中主要包含 User 产生的随机数 N_1；

b) DAE 收到 User 的鉴别请求消息后，产生随机数 N_2，并利用与 ACr 之间的共享密钥 $K_{ACr.DAE}$ 计算 $ET_1=E(K_{ACr.DAE},N_1)$，将 $N_1 \| N_2 \| ET_1$ 作为鉴别响应消息发送给 User，其中，E 为对称

加密算法；

c) User 收到 DAE 的鉴别响应消息后，首先判断消息中的随机数 N_1 是否是 User 选择的随机数，若不是，直接丢弃该消息；若是，则利用与 ACr 之间的共享密钥 $K_{ACr,User}$ 计算 $ET_2 = E(K_{ACr,User}, N_1)$，计算消息鉴别码 $MIC_1 = HMAC(K_{ACr,User}, N_1 \| ID_{DAE} \| ET_1 \| ET_2)$，构造实体鉴别请求消息 $N_1 \| ID_{DAE} \| ET_1 \| ET_2 \| MIC_1$ 发送给 ACr，其中，ID_{DAE} 是 DAE 的身份标识；

d) ACr 收到 User 的实体鉴别请求消息后，首先根据 MIC_1 判断消息的完整性，若验证不通过，丢弃该消息；若验证通过，利用与 DAE 之间的共享密钥 $K_{ACr,DAE}$ 解密 ET_1，若解密后得到的 N_1 与 User 在步骤 c)中发送的 N_1 不相等，ACr 构造实体鉴别响应消息 $N_1 \| ID_{DAE} \| RES(DAE) \| MIC_2$ 发送给 User，其中 $MIC_2 = HMAC(K_{ACr,User}, N_1 \| ID_{DAE} \| RES(DAE))$，Res(DAE)＝Failure 表示 ACr 对 DAE 鉴别失败；若解密后得到的 N_1 与 User 在步骤 c)中发送的 N_1 相等，ACr 利用与 User 共享的密钥 $K_{ACr,User}$ 解密 ET_2，若解密后得到的 N_1 与 User 在步骤 c)中发送的 N_1 不相等，终止鉴别；若解密后得到的 N_1 与 User 在步骤 c)中发送的 N_1 相等，ACr 生成 User 和 DAE 间的会话密钥 $K_{DAE,User}$，并根据 User 的身份标识查询 ACL，获得 User 的访问控制信息 ACL_{User}，连同 User 的访问期限 T_V，利用 $K_{ACr,DAE}$ 计算 $ET_3 = E(K_{ACr,DAE}, ID_{User} \| K_{DAE,User} \| T_V \| ACL_{User})$，并利用 $K_{AC,User}$ 计算 $ET_4 = E(K_{ACr,User}, K_{DAE,User})$，计算 $MIC_2 = HMAC(K_{ACr,User}, N_1 \| ID_{DAE} \| RES(DAE) \| ET_3 \| ET_4)$，构造实体鉴别响应消息 $N_1 \| ID_{DAE} \| RES(DAE) \| ET_3 \| ET_4 \| MIC_2$ 发送给 User，其中，RES(DAE)＝True 表示 ACr 对 DAE 鉴别成功；

e) User 收到 ACr 的实体鉴别响应消息后，首先判断随机数 N_1 是否是 User 选择的随机数，若不是，丢弃该消息；若是，根据 MIC_2 判断消息的完整性；若验证不通过，丢弃该消息；若验证通过，User 根据 RES(DAE)判断 DAE 的合法性，若 RES(DAE)＝Failure，表示 DAE 非法，User 终止访问；若 RES(DAE)＝True，User 解密消息中的 ET_4，产生随机数 N_3，连同 DAE 的随机数 N_2 以及 User 的访问请求利用解密后获得的与目的访问实体间的会话密钥 $K_{DAE,User}$ 计算 $ET_5 = E(K_{DAE,User}, N_2 \| N_3 \| ID_{User} \| Q_{User})$，计算 $MIC_3 = HMAC(K_{DAE,User}, ET_3 \| ET_5)$，构造访问请求消息 $ET_3 \| ET_5 \| MIC_3$ 发送给 DAE；

f) DAE 收到 User 的访问请求后，首先解密 ET_3，获得会话密钥 $K_{DAE,User}$，根据 MIC_3 判断消息完整性，若校验不通过，拒绝访问；若校验通过，利用 $K_{DAE,User}$ 解密 ET_5，判断解密后得到的 N_2 是否是 DAE 选择的 N_2，若不是，拒绝访问；若是，则确认解密 ET_5 后获得的 ID_{User} 是否是请求访问的 User 的身份标识，若不是，拒绝访问；若是，记录当前时刻 T_C，从 T_C 到($T_C + T_V$)这段时间即为 User 的访问有效期，用户只能在此有效期内访问网络数据，DAE 根据 ACL_{User} 判断 User 的访问请求 Q_{User} 是否合法，若不合法，拒绝访问；若合法，生成应答数据 R_{DAE}，连同 N_3 利用 $K_{DAE,User}$ 计算 $ET_6 = E(K_{DAE,User}, N_3 \| R_{DAE})$，计算 $MIC_4 = HMAC(K_{DAE,User}, ET_6)$，构造访问响应消息 $ET_6 \| MIC_4$ 发送给 User；

g) User 收到访问响应消息后，首先根据 MIC_4 判断消息完整性，若不完整，丢弃该消息；若完整，利用 $K_{DAE,User}$ 解密 ET_6，判断解密得到的 N_3 是否是 User 选择的 N_3，若不是，丢弃该消息；若是，User 保存应答数据 R_{DAE}，后续 User 与 DAE 之间的访问请求和应答数据均利用 $K_{DAE,User}$ 加以保护。

6.3 基于访问控制列表的访问控制机制

基于访问控制列表的访问控制机制适用于网络对各类用户的访问控制，该机制见 ISO/IEC 29180：2012，交互过程见图 5。

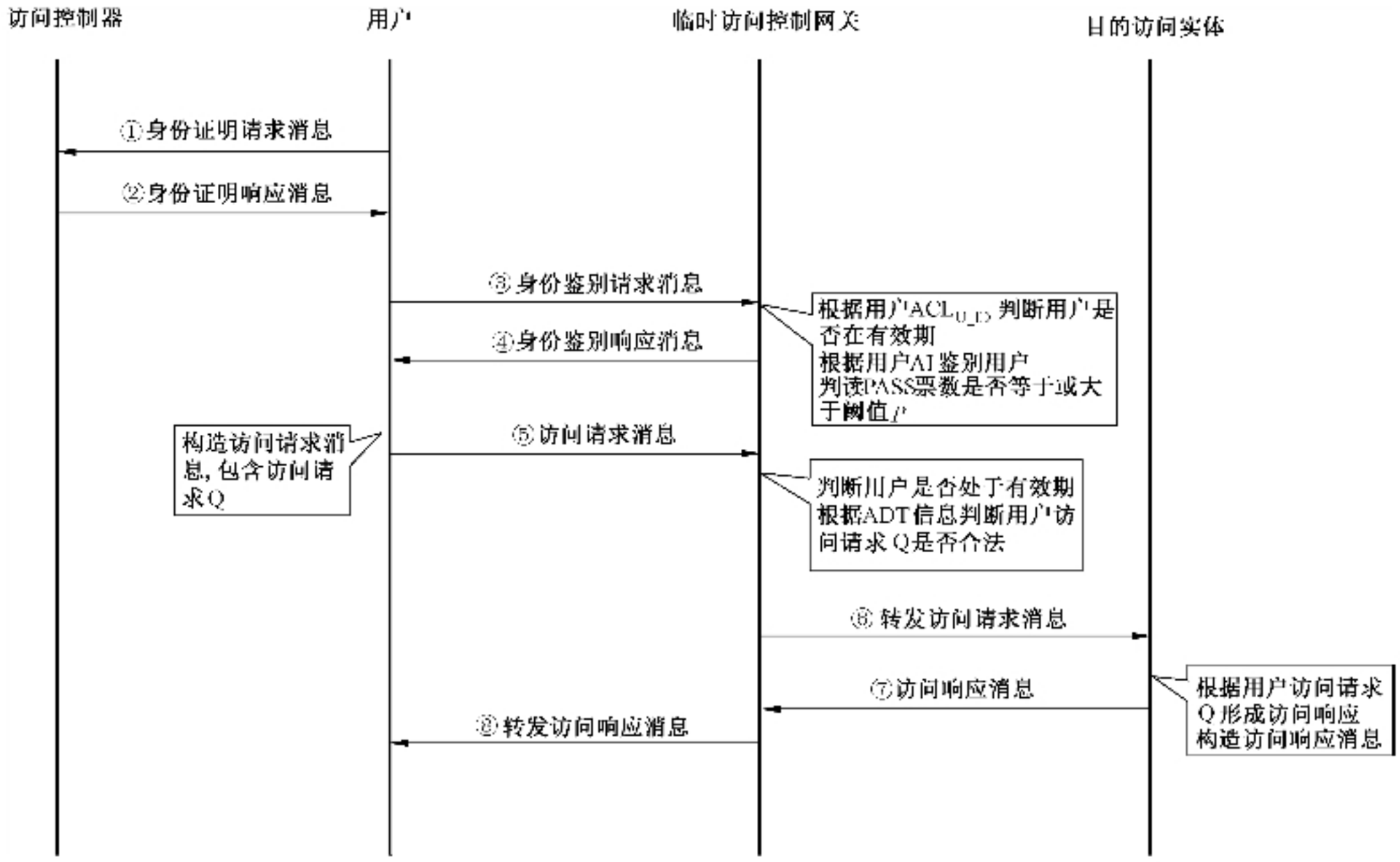

图 5　基于访问控制列表的访问控制机制消息交互示意图

访问控制过程如下：

a) 访问控制器 ACr 构造访问控制列表 ACL 以及用户身份信息，并在用户访问网络之前进行协议初始化：

1) ACr 本地构造 ACL，该 ACL 包括 U_ID 字段、ADT 字段、VP 字段、AI 字段，各字段定义如下：U_ID 字段：用户的身份标识；ADT 字段：用户被授权访问的数据类型；VP 字段：用户被授权访问网络的期限；AI 字段：用于鉴别用户身份的依据，可以是证书或者密钥或其他可作为用户身份的依据。在构造 ACL 后，ACr 对用户进行注册，注册过程如下：ACr 首先根据网络用户的身份标识 U_ID 确定该用户的 ADT 和 VP，然后构造用于鉴别该用户身份的依据 AI。ACr 将 U_ID、ADT、VP、AI 作为新条目插入 ACL 列表中，记做 ACL_{U_ID}。

2) 用户访问网络之前，先向 ACr 发送身份证明请求消息。ACr 收到身份证明请求消息后，判断该用户是否已注册，若已注册，则 ACr 发送身份证明响应消息给该用户，该响应消息中包含 ACr 为用户构造的 AI。同时，ACr 将 ACL 列表中与该用户 U_ID 对应的包含 U_ID、ADT、VP、AI 的 ACL_{U_ID}以安全的方式发送给网络内的所有实体，实体在该用户 VP 截止之前保存该 ACL_{U_ID}；若用户未注册，则 ACr 丢弃该用户的身份证明请求消息。

注：安全的方式是指以加密传输等方式保护消息的机密性和完整性。实体间可使用预共享密钥实现加密传输，不限定具体的实现方法，下同。

b) 在用户访问目的访问实体前，先向网络发送身份鉴别请求消息，此时由网络中用户的单跳通信区域内的所有实体构成临时访问控制网关对用户进行鉴别，过程如下：

1) 临时访问控制网关收到用户的身份鉴别请求消息后，临时访问控制网关中的实体首先判断是否存有该用户的 ACL_{U_ID}信息，如果存有该信息，表明该用户处于有效期内，实体根据 ACL_{U_ID}中的用户 AI 对用户进行身份鉴别，若实体对用户身份鉴别成功，则投 PASS 票，并广播该 PASS 票，若临时访问控制网关中的实体收到的 PASS 票数大于或等于阈值

P，表示用户鉴别成功；如果网关中的实体收到的 PASS 票小于阈值 P，表示鉴别失败，终止该用户的访问；其中阈值 P 由网络所有者定义，可以是一个 PASS 票数的固定值，也可以是一个 PASS 票的比例值等；

2） 鉴别成功后，在用户访问网络的过程中，当前临时访问控制网关中的实体将根据用户的运动方向、运动速度等对用户将要到达的位置进行测算，并由测算得到的用户将要到达的位置为中心的所有单跳区域内的所有实体构成下一个临时访问控制网关。当前临时访问控制网关中的实体在 t 时间后将用户鉴别成功消息发送给下一个临时访问控制网关中的实体，下一个临时访问控制网关将根据收到的用户鉴别成功的消息条数是否达到阈值 P 来判断该用户是否鉴别成功。若用户仍处于有效期 VP 内，且收到的用户鉴别成功的消息条数大于或等于阈值 P，则下一个临时访问控制网关将承认用户的合法性，并将在时间 t 后将鉴别成功消息再次发送到下一个新的临时访问控制网关内的实体。鉴别成功消息在实体间以安全的方式传输。

c） 用户鉴别成功后，通过临时访问控制网关访问目的访问实体，过程如下：

1） 用户鉴别成功后，以安全的方式发送访问请求消息给临时访问控制网关，该请求消息中包含访问请求 Q，Q 中包含用户请求访问的数据类型；

2） 临时访问控制网关收到用户的访问请求消息后，首先判断用户身份鉴别是否通过且用户是否处于有效期，若用户身份鉴别通过且身份处于有效期，则根据 ADT 信息判断用户的 Q 的合法性，若合法，则将 Q 以安全的方式发送给目的访问实体，该实体将认为由临时访问控制网关转发的 Q 是合法的，并将根据 Q 产生访问响应消息，并将该响应消息发送给临时访问控制网关，该网关将转发访问响应消息给用户。访问过程中，如果用户不在有效期内、或用户在有效期内但 Q 不合法，目的访问实体将直接丢弃用户的 Q，终止该用户的访问。