国 际 电 信 联 盟

ITU-T

X.1366

（09/2020）

国际电信联盟
电信标准化部门

X系列：数据网、开放系统通信和安全性

安全应用和服务（2）– 物联网（IoT）安全

物联网（IoT）环境的汇集消息认证方案

ITU-T X.1366建议书

国际电信联盟

ITU-T X系列建议书

数据网、开放系统通信和安全性

公用数据网	X.1–X.199
开放系统互连	X.200–X.299
网间互通	X.300–X.399
消息处理系统	X.400–X.499
号码簿	X.500–X.599
OSI组网和系统概貌	X.600–X.699
OSI管理	X.700–X.799
安全	X.800–X.849
OSI应用	X.850–X.899
开放分布式处理	X.900–X.999
信息和网络安全	
一般安全问题	X.1000–X.1029
网络安全	X.1030–X.1049
安全管理	X.1050–X.1069
生物测定	X.1080–X.1099
安全应用和服务（1）	
组播安全	X.1100–X.1109
家庭网络安全	X.1110–X.1119
移动安全	X.1120–X.1139
网页安全	X.1140–X.1149
安全协议（1）	X.1150–X.1159
对等网络安全	X.1160–X.1169
网络身份安全	X.1170–X.1179
IPTV安全	X.1180–X.1199
网络空间安全	
网络安全	X.1200–X.1229
反垃圾信息	X.1230–X.1249
身份管理	X.1250–X.1279
安全应用和服务（2）	
应急通信	X.1300–X.1309
泛在传感器网络安全	X.1310–X.1319
智能电网安全	X.1330–X.1339
验证邮件	X.1340–X.1349
物联网（IoT）安全	**X.1360–X.1369**
智能交通系统（ITS）安全	X.1370–X.1389
分布式账簿技术安全	X.1400–X.1429
分布式账簿技术安全	X.1430–X.1449
安全协议（2）	X.1450–X.1459
网络安全信息交换	
网络安全概述	X.1500–X.1519
漏洞/状态信息交换	X.1520–X.1539
事件/事故/启发式信息交换	X.1540–X.1549
政策的交换	X.1550–X.1559
启发式和信息请求	X.1560–X.1569
标识和发现	X.1570–X.1579
确保交换	X.1580–X.1589
云计算安全	
云计算安全概述	X.1600–X.1601
云计算安全设计	X.1602–X.1639
云计算安全最佳做法和指导原则	X.1640–X.1659
云计算安全实施方案	X.1660–X.1679
其他云计算安全	X.1680–X.1699
量子通信	
术语	X.1700–X.1701
量子随机数发生器	X.1702–X.1709
QKDN安全框架	X.1710–X.1711
QKDN安全设计	X.1712–X.1719
QKDN安全技术	X.1720–X.1729
数据安全	
大数据安全	X.1750–X.1759
5G安全	X.1800–X.1819

欲了解更详细信息，请查阅ITU-T建议书目录。

ITU-T X.1366建议书

物联网环境的汇集消息认证方案

摘要

物联网（IoT）设备的数量正在持续增加，在不久的将来，将会有大量设备连接到物联网网络，包括5G。ITU-T X.1366建议书说明了两种消息认证方案：一种是作为基础机制的物联网汇集消息认证（AMA）方案；另一种是以轻量和安全的方式、采用交互协议的交互式汇集消息认证（IAMA）方案。两种汇集消息认证方案都可用于确保“实体（身份）认证”以及确保“消息认证”。这些方案可能并不适用于使用物联网设备的所有用例，但方案在以下条件下对用例非常有效和适合：

- 数以万计的物联网设备需要消息认证；
- 为频繁和间或发生的认证过程处理数据或消息。

例如，“使用图像数据的监控应用”和“远程遥测”，如厂房或工厂操作的监测和健康监测，是这些方案的典型候选用例。

历史沿革

版本	建议书	批准日期	研究组	唯一识别码*
1.0	ITU-T X.1366	2020-09-03	17	11.1002/1000/14262

关键词

汇集消息认证、AMA、IoT。

* 欲查阅建议书，请在您的网络浏览器地址域键入URL http://handle.itu.int/，随后输入建议书的唯一ID，例如，http://handle.itu.int/11.1002/1000/11830-en。

前言

国际电信联盟（ITU）是从事电信、信息和通信技术（ICT）领域工作的联合国专门机构。国际电信联盟电信标准化部门（ITU-T）是国际电信联盟的常设机构，负责研究技术、操作和资费问题，并且为在世界范围内实现电信标准化，发表有关上述研究项目的建议书。

每四年一届的世界电信标准化全会（WTSA）确定ITU-T各研究组的研究课题，再由各研究组制定有关这些课题的建议书。

WTSA第1号决议规定了批准建议书须遵循的程序。

属ITU-T研究范围的某些信息技术领域的必要标准，是与国际标准化组织（ISO）和国际电工技术委员会（IEC）合作制定的。

注

本建议书为简明扼要起见而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

遵守本建议书的规定是以自愿为基础的，但建议书可能包含某些强制性条款（以确保例如互操作性或适用性等），只有满足所有强制性条款的规定，才能达到遵守建议书的目的。“应该”或“必须”等其它一些强制性用语及其否定形式被用于表达特定要求。使用此类用语不表示要求任何一方遵守本建议书。

知识产权

国际电联提请注意：本建议书的应用或实施可能涉及使用已申报的知识产权。国际电联对无论是其成员还是建议书制定程序之外的其它机构提出的有关已申报的知识产权的证据、有效性或适用性不表示意见。

至本建议书批准之日止，国际电联已收到实施本建议书可能需要的受专利保护的知识产权的通知。但需要提醒实施者注意的是，这可能并非最新信息，因此大力提倡他们通过下列网址查询电信标准化局（TSB）的专利数据库：http://www.itu.int/ITU-T/ipr/。

目录

页码

1 范围 1
2 参考文献 1
3 定义 1
3.1 他处定义的术语 1
3.2 本建议书定义的术语 1
4 缩写词和首字母缩略语 1
5 惯例 2
6 概述和基本概念 2
6.1 概述 2
6.2 汇集消息认证系统的基本概念 3
7 汇集消息认证 4
7.1 概述 4
7.2 特定记法 4
7.3 算法规范 4
8 交互式汇集消息认证 5
8.1 概述 5
8.2 特定记法 6
8.3 交互协议的规范 6
附件A – 指南和限制 8
A.1 关于使用汇集消息认证（AMA）的指南 8
A.2 关于使用AMA的限制 8
附件B – 与现有一对一认证协议的结合 9
附录一 – 关于使用AMA的用例 10
I.1 引言 10
I.2 用例-1：主题公园和休闲中心 10
I.3 用例-2：监测传感器 11
附录二 – AMA方案的有关活动 14
附录三 – 自适应组测试协议 15
参考书目 16

ITU-T X.1366建议书

物联网的汇集消息认证方案

1 范围

本建议书说明了两种消息认证方案：一种是作为基础机制的物联网汇集消息认证（AMA）方案；另一种是以轻量和安全的方式、采用交互协议的交互式汇集消息认证（IAMA）方案。两种汇集消息认证方案都可用于确保“实体（身份）认证”以及确保“消息认证”。

如何在特定的物联网环境中实施这些方案以及汇集签名技术不在本建议书的讨论范围内。

2 参考文献

下列ITU-T建议书及含有本建议书引用条款的其它参考文献构成本建议书的条款。所注明版本在出版时有效。所有建议书及其它参考文献均可能进行修订；因此鼓励建议书的使用方了解使用最新版本的下列建议书和其它参考文献的可能性。ITU-T建议书的现行有效版本清单定期出版。本建议书在引用某一独立文件时，并未给予该文件建议书的地位。

无。

3 定义

3.1 他处定义的术语

本建议书使用下列他处定义的术语：

3.1.1 消息认证码（message authentication code）（MAC）[b-ITU-T X.813]：用于提供数据来源认证和数据完整性的密码校验值。

3.2 本建议书定义的术语

本建议书定义下列术语：

3.2.1 消息认证（message authentication）：指的是一种属性，它保证在传输过程中不对消息进行修改，以确保数据完整性，并允许接收方对消息来源进行验证。

3.2.2 汇集消息认证（aggregate message authentication）（AMA）：指的是一种属性，它允许将多个发送方生成的多个消息认证码汇集为一个较短的认证码，对该认证码，仍可由拥有发送方密钥的收件方进行验证。

3.2.3 认证标签（authentication tags）：用于消息认证的一条数据。

4 缩写词和首字母缩略语

本建议书使用下列缩写词和首字母缩略语：

AGT 自适应组测试协议

AMA 汇集消息认证

AMAC 汇集消息认证码

IAMA 互动消息认证

IoT 物联网

MAC 消息认证码

XOR 异或运算

5 惯例

无。

6 概述和基本概念

6.1 概述

物联网（IoT）设备的数量正在持续增加，在不久的将来，将会有大量设备连接到物联网网络，包括5G。本建议书提供了一种可以在这种情况下应用的、轻量和安全的认证系统。

消息认证码（MAC）是最基本的密码原语之一，并且MAC可以用作消息认证的一种轻量级密码原语。不过，如图1所示，在当前的物联网系统中，对于从物联网设备发送的消息，认证标签（请参阅第3.2.3节）是在物联网设备侧单独生成的，带有生成之标签的每条消息基本上都在接收器侧通过验证过程进行验证。在当前物联网场景中认识到的主要问题是，现有认证和验证过程的负载正与物联网设备数量的增加成比例地在增加。

汇集消息认证码（AMAC）是一项现有技术，允许将不同设备生成的多个消息上的多个MAC标签压缩为单个汇集标签，而不影响安全性（请参阅附录二）。AMAC的优势在于以下事实，即汇集标签的大小比MAC标签的总和要小得多，因此，它将在连接许多发送消息之设备的移动网络或物联网的应用中很有用。具体来说，AMAC可以用在许多应用中，以使使用MAC的网络更高效。不过，通常在AMAC中使用汇集标签，一旦这些消息被视为无效，则该方法就无法在多个消息中确定无效消息。在本建议书中，对现有的AMAC方案进行了扩展，从而使之可以压缩具有检测能力的多个MAC标签，以指定无效消息。

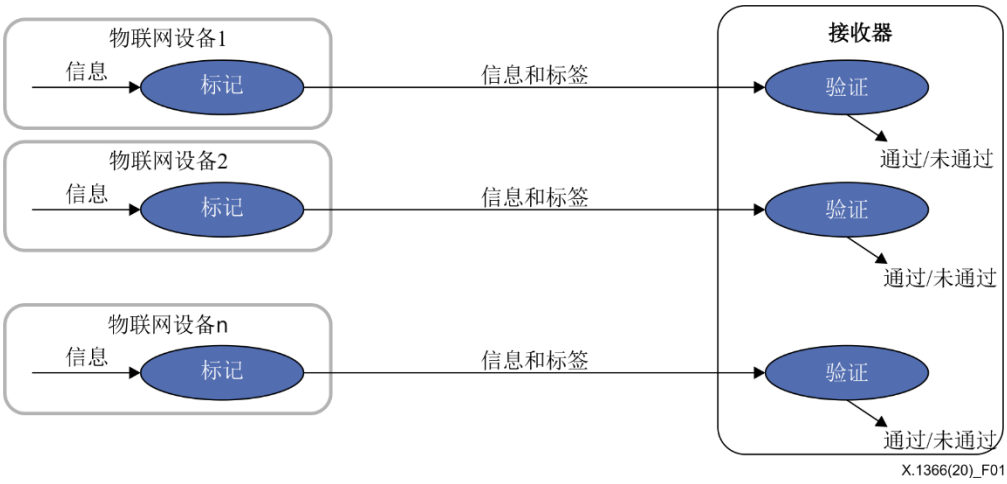


图1 – 一对一认证系统（常规系统）

6.2 汇集消息认证系统的基本概念

6.2.1 概述

图2显示了在本建议书中提出的汇集消息认证（AMA）的基本方案。汇集节点安装到物联网网络系统中，用于汇集MAC标签/认证标签，而无需更改网络中现有MAC的输入格式或结构。汇集节点将附着在由不同设备生成的多个消息中的多个MAC标签压缩为单个汇集标签，而不会影响安全性，并且该汇集标签通过主信道传输到接收器，以执行标签的验证过程。接收器通过使用汇集标签来检测多个消息的有效性，并可以从汇集标签中确定无效消息或数据。当汇集标签的大小远小于多个MAC标签的总大小时，该技术可以有效减少传输的数据量。

本建议书将物联网的AMA方案描述为一种基本机制，并介绍了一种交互式AMA（IAMA）方案来说明如何执行汇集和验证过程。在AMA方案中，仅使用从汇集节点到接收器的主信道来发送汇集标签。AMA方案的汇集和验证算法在第7节中予以规定。在IAMA方案中，除了主信道之外，还使用一个反馈信道，该信道是一个从接收器到汇集节点的、具有低带宽的、经认证的信道。通过经反馈信道将验证结果从接收器发送到汇集节点，汇集节点可以比第7节中的AMA更有效地压缩MAC标签。执行汇集节点与接收器之间的交互协议以进行验证，见第8节中予以规定。

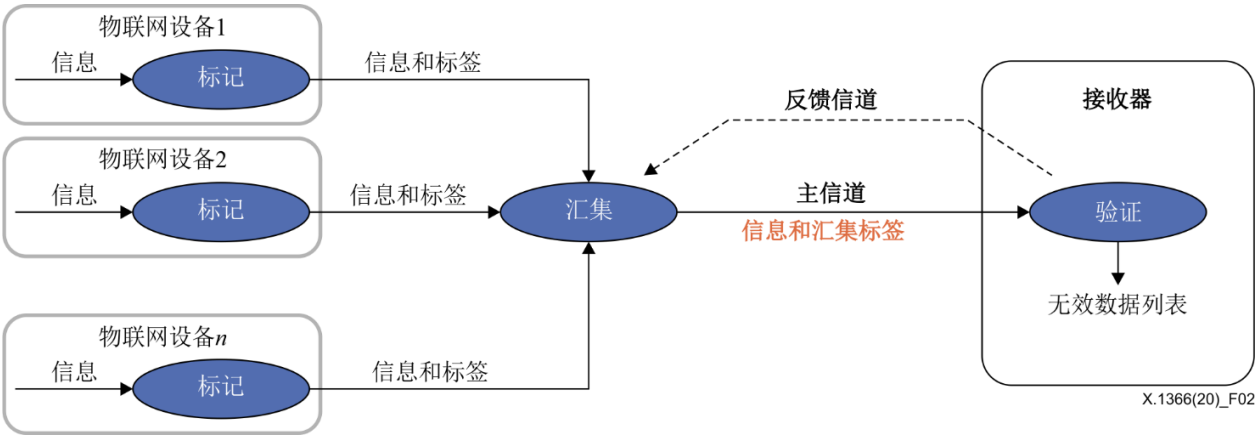


图2 – 汇集消息认证系统的基本概念

注 – 在多个设备通过使用“加密-然后-MAC”方案发送隐私数据的情况下，可以运用本建议书中的汇集技术来压缩多个MAC标签。

在本建议书中，用于执行AMA和IAMA方案的四个过程为：密钥生成、标记、汇集和验证，如下所述：

1） 密钥生成将一个安全参数和以一个ID作为输入，而后为该ID生成一个密钥。

2） 标记将一个消息、一个ID和对应该ID的一个密钥作为输入，而后输出一个标签。

3） 汇集将来自多个设备的ID、消息和标签的多个元组作为输入，而后生成一个汇集标签元组作为输出。

4） 验证将所有密钥、来自多个设备的多对ID和消息以及一个汇集标签元组作为输入。它指定无效消息，并输出消息无效的设备的ID列表。

7 汇集消息认证

7.1 概述

本建议书中概述的AMAC方案提供了将多个MAC标签汇集为1个较短标签并从中确定无效消息的功能。本节说明如何构造四个算法（密钥生成、标记、汇集、验证）以生成AMAC。

7.2 特定记法

在本建议书中，使用以下特定记法：

n： 设备数量。

d： 来自设备的无效消息数量。

id： 设备ID。令$ID = \{id_1, id_2, \ldots, id_n\}$为所有ID的集合。

m： 消息。

k_{id}： 设备id的密钥。为简单起见，用k_i而不用k_{id_i}来表示对应id_i的密钥。

$F()$： MAC函数，它将1个密钥和1个消息作为输入，并输出1个MAC标签。

$G = (g_{i,j})$： u行n列的d-析取矩阵。矩阵G在$\{0,1\}$中有条目，列通过ID进行索引，$id_1, id_2, \ldots, id_n$。如果G的任何d列的布尔和不包含任何其他列，其中对每一个$1 \le i \le u$，若$x_i \ge y_i$，则$x = (x_1, x_2, \ldots, x_u)$包含$y = (y_1, y_2, \ldots, y_u)$，那么称$G$ 为d-析取。

$I(G, i)$： 对集合j $(1 \le j \le n)$，对每个$i = 1,2, \ldots, u$，$g_{i,j} = 1$。

$\oplus$： 按位异或（XOR）运算。

$H()$： 哈希函数。

7.3 算法规范

为了覆盖更广泛的应用，提供了两种具有检测功能的汇集MAC。一种基于异或（第7.3.1节），另一种基于哈希函数（第7.3.2节）。

7.3.1 基于异或的构造

7.3.1.1 密钥生成

对每个id，本过程都会生成一个随机密钥，表示为k_{id}。

7.3.1.2 标记

标记将1个消息（表示为m）、1个ID（表示为id）、对应ID的1个密钥（表示为k_{id}）作为输入，并输出1个MAC标签t（通过$F(k_{id}, m)$计算得到）。

7.3.1.3 汇集

汇集将来自n个设备的ID、消息及其MAC标签作为输入，表示为$(id_1, m_1, t_1), \ldots, (id_n, m_n, t_n)$。对每个$i$ $(1 \le i \le u)$，对MAC标签进行按位异或，其对应的ID包括在$I(G, i)$中，并将之定义为T_i，即$T_i = \oplus_{j \in I(G,i)} t_j$。然后，输出$(T_1, T_2, \ldots, T_u)$作为一个汇集标签。

7.3.1.4 验证

验证将所有密钥（表示为$(k_1, \ldots, k_n)$）、来自n个设备的多对ID和消息（表示为$(id_1, m_1), \ldots, (id_n, m_n)$）、1个汇集标签（表示为$(T_1, T_2, \ldots, T_u)$）作为输入。然后，在以下过程后，它输出1个列表$J$。

步骤1：$J \leftarrow \{id_1, id_2, \ldots, id_n\}$

步骤2：对$i = 1,2, \ldots, u$，执行：

对所有$j \in I(G, i)$，若$T_i = \oplus_{j \in I(G,i)} t_j$，则$J \leftarrow J \setminus \{id_j\}$。

7.3.2 基于哈希的构造

7.3.2.1 密钥生成

对每个id，本过程都会生成一个随机密钥，表示为k_{id}。

7.3.2.2 标记

标记将1个消息（表示为m）、1个ID（表示为id）、对应ID的1个密钥（表示为k_{id}）作为输入，并输出1个MAC标签t（通过$F(k_{id}, m)$计算得到）。

7.3.2.3 汇集

汇集将来自n个设备的ID、消息及其MAC标签作为输入，表示为$(id_1, m_1, t_1), \ldots, (id_n, m_n, t_n)$。对每个$i$ $(1 \leq i \leq u)$，对MAC标签计算哈希值，其对应的ID包括在$I(G, i)$中，并将之定义为T_i，即 $T_i = H(t_{j_1}, t_{j_2}, \ldots)$，其中$I(G, i) = \{j_1, j_2, \ldots\}$，$1 \leq j_1 < j_2 < \cdots$。

然后，输出$(T_1, T_2, \ldots, T_u)$作为一个汇集标签。

7.3.2.4 验证

验证将所有密钥（表示为$(k_1, \ldots, k_n)$）、来自n个设备的多对ID和消息（表示为$(id_1, m_1), \ldots, (id_n, m_n)$）、1个汇集标签（表示为$(T_1, T_2, \ldots, T_u)$）作为输入。然后，在以下过程后，它输出1个列表$J$。

步骤1：$J \leftarrow \{id_1, id_2, \ldots, id_n\}$

步骤2：对$i = 1,2, \ldots, u$，执行：

如果 $T_i = H(t_{j_1}, t_{j_2}, \ldots)$，其中 $I(G, i) = \{j_1, j_2, \ldots\}$，$1 \leq j_1 < j_2 < \cdots$，则对所有$j \in I(G, i)$，$J \leftarrow J \setminus \{id_j\}$。

8 交互式汇集消息认证

8.1 概述

本建议书中提出的IAMA方案提供了功能，以便IAMA可以以比第7节所述之AMA方案中的标签更少的标签数量来标识无效消息。IAMA方案由两个算法（密钥生成和标记）和一个汇集与验证之间的交互协议构成。本节说明如何构造这些算法和协议。

8.2 特定记法

在本建议书中，使用以下特定记法：

n： 设备数量。

d： 来自设备的无效消息数量。

id： 设备ID。令$ID = \{id_1, id_2, \ldots, id_n\}$为所有ID的集合。

m： 消息。

k_{id}： 设备id的密钥。为简单起见，用k_i而不用k_{id_i}来表示对应id_i的密钥。

$F()$： MAC函数，它将1个密钥和1个消息作为输入，并输出1个MAC标签。

AGT： 自适应组测试协议。

$\oplus$： 按位异或（XOR）运算。

$H()$ 哈希函数。

8.3 交互协议的规范

可以通过MAC函数$F()$和AGT来构造IAMA，有关自适应组测试，请参阅附录三。通过使用如AMA构造中所介绍的两种运算，即异或或哈希函数，来介绍这种构造。

8.3.1 基于异或的构造

8.3.1.1 密钥生成

对每个id，本过程都会生成一个随机密钥，表示为k_{id}。

8.3.1.2 标记

标记将1个消息（表示为m）、1个ID（表示为id）、对应ID的1个密钥（表示为k_{id}）作为输入，并输出1个MAC标签t（通过$F(k_{id}, m)$计算得到）。

8.3.1.3 汇集和验证

基于如图3所示的AGT协议构造汇集和验证。汇集将整个ID集合$ID = \{id_1, id_2, \ldots, id_n\}$、来自$n$个设备的消息及其MAC标签（表示为$(m_1, t_1), \ldots, (m_n, t_n)$，其中$(m_i, t_i)$ $(1 \le i \le n)$为对应id_i的消息-标签对）。验证获取整个ID集合ID以及所有对应id_i的密钥k_i $(1 \le i \le n)$。首先，汇集选择一个子集$S \subseteq ID$，通过压缩S的MAC标签来生成汇集标签T_S：可以通过异或MAC标签来生成T_S，即$T_S = \oplus_{j \in S} t_j$。然后汇集利用消息$(m_1, \ldots, m_n)$将$T_S$发送给验证。接下来，验证设$J = ID$，并通过使用$S$的密钥对$T_S$的有效性进行校验：若$T_S = \oplus_{j \in S} t_j$（其中$t_j = F(k_j, m_j)$），则认为$T_S$有效；否则认为$T_S$无效。若$T_S$有效；则设$J \leftarrow J \setminus S$。验证将$T_S$的校验结果（即1比特信息）发送给汇集。然后，汇集选择另一个子集$S' \subseteq ID$，通过压缩S'的MAC标签来生成汇集标签$T_{S'}$，并将$T_{S'}$发送给验证。验证通过使用S'的密钥对$T_{S'}$的有效性进行校验；若$T_{S'}$有效，则$J \leftarrow J \setminus S'$。验证将$T_{S'}$的校验结果发送给汇集。在汇集与验证之间重复上述过程后，验证最终输出一个由消息为无效的设备之ID组成的列表J。

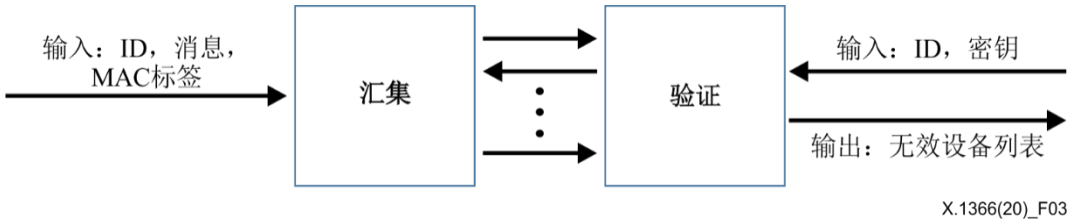


图3 – 汇集与验证之间的交互协议

8.3.2 基于哈希的构造

8.3.2.1 密钥生成

对每个id，本过程都会生成一个随机密钥，表示为k_{id}。

8.3.2.2 标记

标记将1个消息（表示为m）、1个ID（表示为id）、对应ID的1个密钥（表示为k_{id}）作为输入，并输出1个MAC标签t（通过$F(k_{id}, m)$计算得到）。

8.3.2.3 汇集和验证

基于如图3所示的AGT协议构造汇集和验证。汇集将整个ID集合$ID = \{id_1, id_2, \dots, id_n\}$、来自$n$个设备的消息及其MAC标签（表示为$(m_1, t_1), \dots, (m_n, t_n)$，其中$(m_i, t_i)$ $(1 \le i \le n)$）为对应id_i的消息-标签对）。验证获取整个ID集合ID以及所有对应id_i的密钥k_i $(1 \le i \le n)$。首先，汇集选择一个子集$S \subseteq ID$，通过计算哈希值$T_S = H(t_{j_1}, t_{j_2}, \dots)$（其中$S = \{id_{j_1}, id_{j_2}, \dots\}$，$1 \le j_1 < j_2 < \cdots$）来生成汇集标签$T_S$，然后汇集利用消息$(m_1, \dots, m_n)$将$T_S$发送给验证。接下来，验证设$J = ID$，并通过使用$S$的密钥对$T_S$的有效性进行校验。若$T_S = H(t_{j_1}, t_{j_2}, \dots)$（其中$t_j = F(k_j, m_j)$），则认为$T_S$有效；否则认为$T_S$无效。若$T_S$有效；则设$J \leftarrow J \setminus S$。验证将$T_S$的校验结果（即1比特信息）发送给汇集。然后，汇集选择另一个子集$S' \subseteq ID$，通过压缩S'的MAC标签来生成汇集标签$T_{S'}$，并将$T_{S'}$发送给验证。验证通过使用S'的密钥对$T_{S'}$的有效性进行校验；若$T_{S'}$有效，则$J \leftarrow J \setminus S'$。验证将$T_{S'}$的校验结果发送给汇集。在汇集与验证之间重复上述过程后，验证最终输出一个由消息为无效的设备之ID组成的列表J。

附件A

指南和限制

（本附件是本建议书不可分割的组成部分。）

A.1 关于使用汇集消息认证（AMA）的指南

本建议书讨论了将汇集节点嵌入现有消息验证码（MAC）协议而不改变基础MAC输入格式或网络连接的适用性。另外，汇集是一个无密钥过程，不需要维护汇集节点中的任何密钥。此外，仅通过按位异或运算或计算哈希函数来执行汇集，因此，本建议书中的AMA方案适用于以轻量级方式来进行认证。

在第7节所述的汇集处理中，需要生成和存储一个d-析取矩阵。已知若干可用来生成d-析取矩阵的方法，如[b-TM05]中所述，并且还有可能使用一种如[b-MK19]中所述的、压缩的d-析取矩阵形式。本建议书甚至建议在AMA方案中使用这些技术。对于具有u行和n列的d-析取矩阵，若$u < n$，则AMA方案将比传统的一对一认证更有效；若$d \ll \sqrt{n}$，则更有效。

注 – 根据[b-HS18]和[b-SS19]中所述的方案，此处描述了通过按位异或或哈希函数构造的AMA（或IAMA）方案的安全等级。安全概念分为三种，即不可伪造性、可识别性-完备性和可识别性-（弱）-稳健性：不可伪造性确保没有任何消息可被伪造；可识别性-完备性确保通过该方案将任何有效的消息判定为有效；可识别性-稳健性确保通过该方案将任何无效的消息判定为无效消息，除了假定敌对者在发起攻击之前不会获得任何有效的MAC标签且不会破坏任何设备，可识别性-弱-稳健性等同于可识别性-稳健性。弱-稳健性在应用中仍然有用，因为它涵盖消息篡改。

本建议书中AMA（或IAMA）方案的安全等级描述如下。如果基础MAC满足不可伪造性的要求，则基于异或的构造将满足不可伪造性、可识别性-完备性和可识别性-弱-稳健性的要求。如果基础MAC满足不可伪造性的要求并将哈希函数视为随机函数，则基于哈希的构造将满足不可伪造性、可识别性-完备性和可识别性-稳健性的要求。

A.2 关于使用AMA的限制

本建议书假设在AMA方案中无效消息的数量最多为d，并将该参数设为一个系统参数。这意味着需要预先估计数量d。

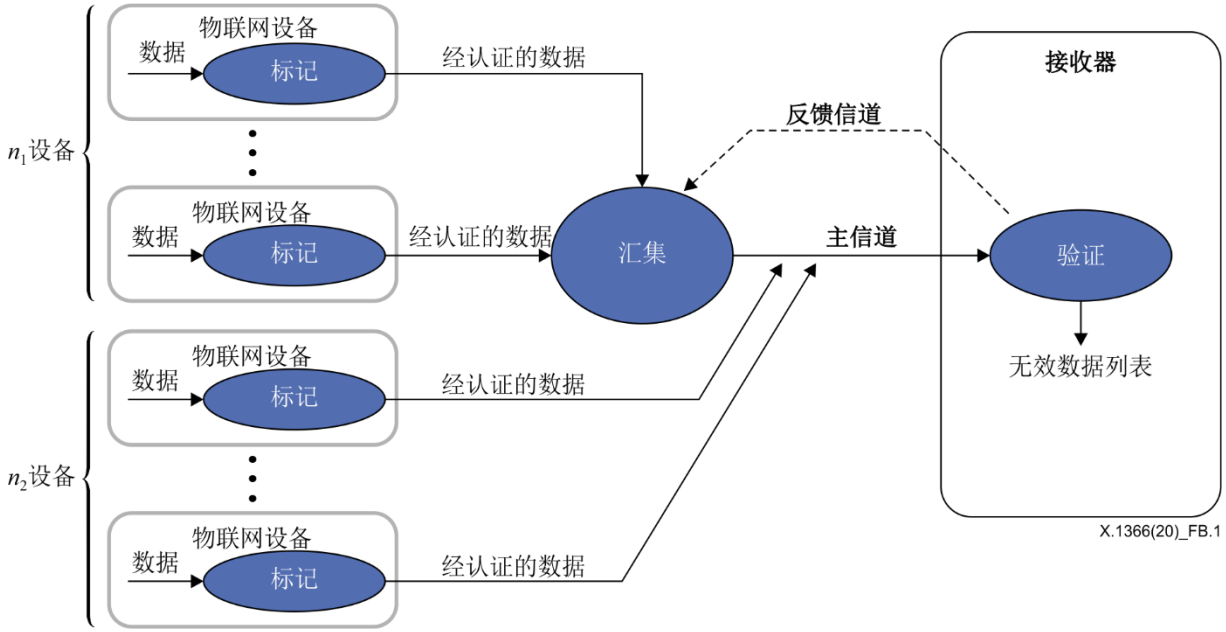
如果无效消息的数量超过假设的值d会怎样呢？在这种情况下，验证最终会输出一个列表J，它包含超过d个设备ID；列表J中包括发送了无效消息的设备的ID；但是，未发送无效消息的设备的某些ID也可能包括在列表J中。在这种情况下，建议再次为AMA方案设置更大的值d。

附件B

与现有一对一认证协议的结合

（本附件是本建议书不可分割的组成部分。）

本建议书中的AMA（或IAMA）方案可以与传统的一对一认证结合使用。传统的一对一认证被认为是AMA方案，其中基础析取矩阵是身份矩阵。对于$n = n_1 + n_2$个设备，若最好是仅汇集n个MAC标签中的n_1个MAC标签，则执行以下操作：对n_1个设备应用AMA（或IAMA）方案，并对其他n_2个设备应用一对一认证，如图B.1所示。



图B.1 – 与一对一认证协议的结合

附录一

关于使用AMA的用例

（此附录非本建议书不可分割的组成部分。）

I.1 引言

汇集消息认证方案可用于确保实体（身份）认证以及确保消息认证。此外，方案可能并不适用于使用物联网（IoT）设备的所有用例。特别地，本方案在以下条件下对用例非常有效和适合：

- 数以万计的物联网设备需要消息认证；
- 为频繁和间或发生的认证过程处理数据/消息。

以下是可以特别假定将利用汇集认证技术的应用示例：

a） 简洁而频繁地发送数据/消息（例如，半电影（静止图像）数据）的应用

- 使用图像数据的监视应用

b） 远程遥测应用：

- 监控工厂运行的应用
- 受众动态调查的应用
- 健康监测的应用，例如“公民马拉松”
- 设施管理的应用，例如在城市地区安装的路灯
- 交通监控的应用
- 河流水位监测的应用

通过在上述物联网应用中运用这种汇集认证技术，可以显著提高整个物联网系统中消息传输和认证处理的效率。

以下用例是利用本建议书中规定的这种汇集认证方案的示例。

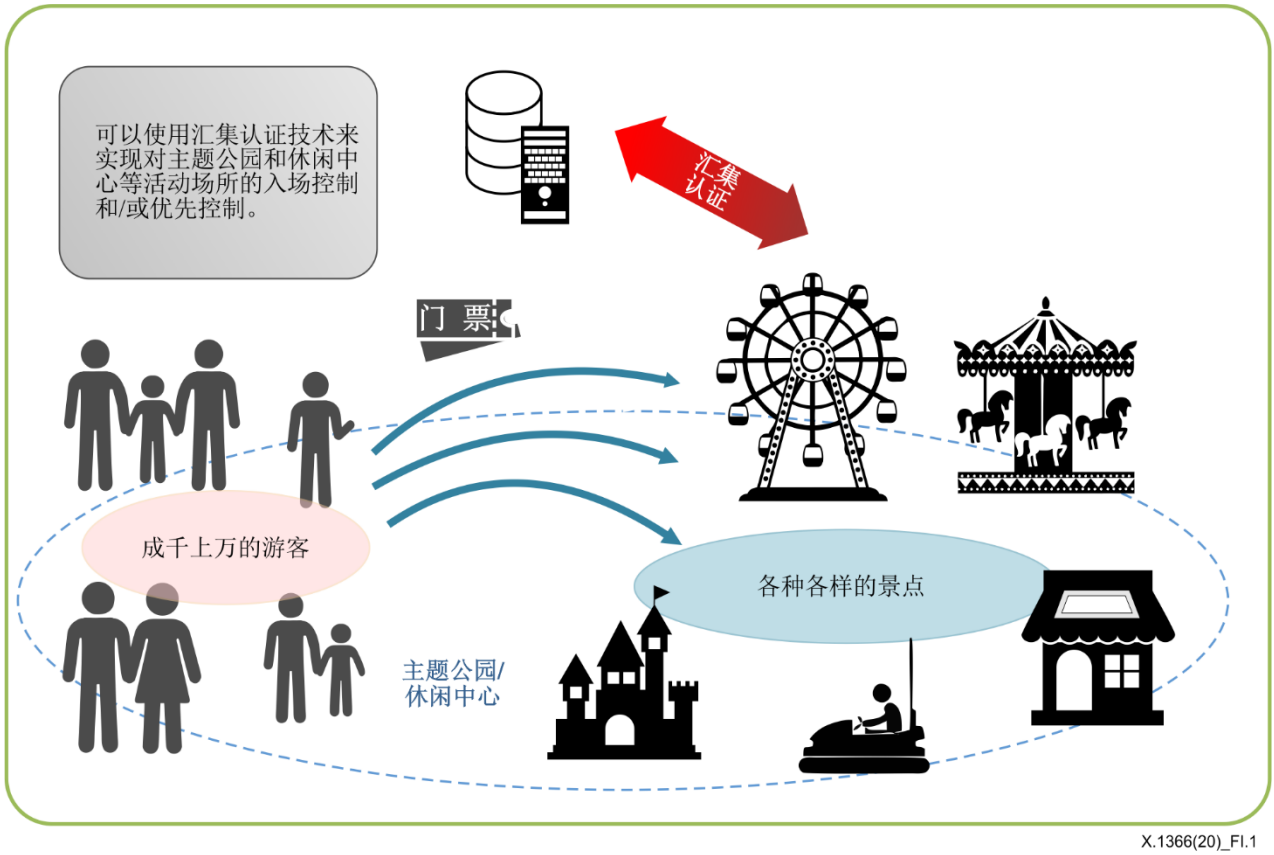
I.2 用例-1：主题公园和休闲中心

对于公园和休闲中心等，可假设同时有 1 000 到 10 000 名游客。也就是说，成千上万的游客具有使用公园/中心景点的适当权限，可能需要同时对这进行验证。在这种情况下，汇集认证方案可能非常适合用来执行高效的授权管理。如图 I.1 所示，汇集服务器可以置于每个景点设施中，用于收集和汇集认证标签，以便从后端认证服务器请求验证。

更具体地说，游客预先购买门票，其上有关于活动、景点入场以及可提供之万维网服务的信息，这些信息嵌入于芯片中。这项技术广泛用于马拉松比赛中。带嵌入式芯片的腕带也可以被视为门票的替代品。

在活动场所正门或每个景点的单独入口处，使用汇集认证技术读取、汇集入场门票的内容，而后发送给汇集认证服务器。

汇集认证服务器中心对提供给游客的服务内容和要求进行分析，通知各个景点和万维网服务提供商，并将之用于拥塞的分析和预测。验证后，游客可以通过诸如自己的智能手机或玻璃型可穿戴设备等，来享用各种经注册的万维网服务。



图I.1 – 主题公园和休闲中心中的汇集认证方案

I.3 用例-2：监测传感器

I.3.1 概述

为了在自然灾害和事件/事故中得到早期警报和干预，使用监视传感器（例如，用于物联网设备的摄像头）对活动进行监测可以作为本建议书提供之汇集认证方案的一个用例。在这种情况下，由多个监视摄像机捕获的准视频或静止图像几乎实时地（或定期地）发送到监视中心，但重要的是要确保所发送数据的可靠性和完整性。

不过，当监视传感器的数量变得很多时，通过逐个检测每台摄像机的认证码来利用每台摄像机的图像数据对认证码进行验证将不再显得高效。在这样一种环境中，汇集认证方案是有效的。在发送到监视中心之前，可在汇集服务器中对带有数据的认证码进行汇集，以便整个物联网系统可以提供高效的认证和通信。汇集服务器的数量取决于监视传感器的数量。图I.2显示了汇集认证方案中的监视传感器。

图I.2 – 汇集认证方案中的监测传感器

I.3.2 特定用例

1) 社区和住房等生活环境的监测

来自各种传感器（例如，连接于公寓楼、智能社区、私人住宅等的监视摄像头）的生活环境信息在网关（物联网集聚中心）处汇集，并使用汇集认证技术传送到中心服务器。

该中心将对收到的信息进行分析，并将之用于协助监视居住环境、预测异常与故障、及时做出响应以及预防犯罪和灾难。

更具体地说，在各种环境传感器、家用电器传感器、监视摄像机、门/窗打开/关闭状态传感器、燃气/水/电基础设施运行状态传感器、电梯监测传感器等中捕获的数据被发送到外部中心。使用终端认证和数据认证的汇集认证方案作为一种用于收集各种大量数据并高效发送数据的认证手段是有效的。

2) 社会基础设施的维护与监测、灾害的响应

在桥梁、隧道和道路等社会基础设施的维护和管理中，正在方方面面引入和使用物联网，普遍期望不久的将来物联网服务能在营造安全的社会中发挥极其重要的作用。例如，在桥梁和高架道路老化的情况下，通过各种传感器来详细捕获诸如应变、振动、位移、倾斜等相关数据以及视频信息。应予发送到中心的数据量正变得越来越大。

当前，作为用于提高无线互联网电路使用效率和避免拥塞的措施之一，汇集认证方法被证明是非常有效的。除了维护和管理这些社会基础设施之外，还有可能将汇集认证方法应用于物联网系统的网关，以使用这些系统来持续监测农业环境中河流和湖泊的水位和流量变化。

3) 使用监视摄像机的防灾系统

安装和操作于世界各地各种地方的监视摄像机用于各种目的，包括预防犯罪和防灾。通常，在处理图像和音频信息的网络中，需要连续地将大量的数据发送到中心侧，对高效传输而言，运用汇集认证技术是有效的。也就是说，有可能通过运用汇集认证方法来提高物联网设备与物联网网关之间以及物联网网关与中心之间的通信效率。

4) 物流的监测、运输系统效率的提高

在物流和运输业务系统中，物联网系统越来越多地用于提高业务效率和高功能性。例如，一种用于精确管理从运输到交付的货物和包裹状态信息的解决方案正在各种领域得到实际应用。在这样一个系统中，可以通过将汇集认证技术应用于将所有包裹上的各种传感器信息发送到中心的系统，来实现更加稳定和高效的物流管理。还可以想到的是，为诸如配备有大量传感器的轿车之类的车辆提供物联网网关，并在运输系统的车辆网关上应用汇集认证技术。

附录二

AMA方案的有关活动

（此附录非本建议书不可分割的组成部分。）

一种与第7节中所述方案不同的AMA方案是由Katz和Lindell在[b-KL08]中首先提出的，它允许将多个消息的多个MAC标签汇集为一个较短的标签。具体来说，Katz和Lindell [b-KL08]对AMA的模型和安全性做了规范，并通过对所有MAC标签进行按位异或来简单构造AMA。仅使用一个较短的单个标签就有可能对多个消息的有效性进行验证，不过，一旦判定多个消息对单个标签是无效的，则通常就不可能在其AMA方案中鉴别无效消息。本建议书中的AMA方案实现了将多个MAC标签汇集为一个较短标签并从中鉴别无效消息的功能。本建议书第7节中提供的AMA代码基于[b-HS18]，而第8节中提供的、有关AMA使用的交互式认证协议则基于[b-SS19]。

附录三

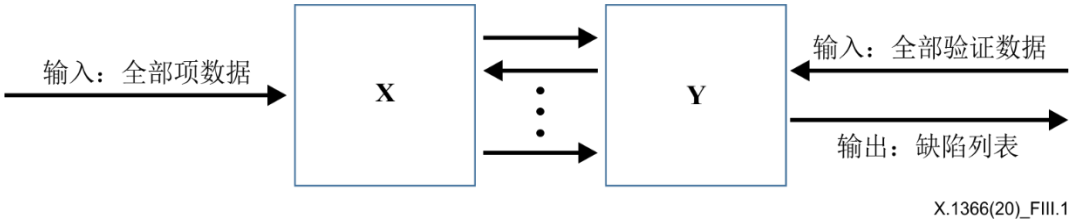
自适应组测试协议

（此附录非本建议书不可分割的组成部分。）

如[b-DH00]中所讨论，组测试是一种使用少量测试而非对每个项都做单独测试以在大量、全部的项中指定称为缺陷的特殊项的方法。

在下面图III.1中所示的组测试协议示例中，假定总共有n个项，其中有d个缺陷。

在自适应组测试中，可以进行若干次测试，以便在对先前测试的结果进行观察后可以选择一个待测试项的子集。竞争性组测试是一种自适应组测试，它不需要事先知道缺陷数d。



图III.1 – 自适应组测试协议

形式上，自适应组测试是X与Y之间的一种交互协议，如图III.1所示。

X获取整个ID集合$ID = \{id_1, id_2, \ldots, id_n\}$以及对应$\mathrm{id_i}$的全部项数据$\mathrm{data_i}$ $(1 \le i \le n)$。Y获取整个ID集合ID以及对应id_i全部验证数据$\mathrm{ans_i}$ $(1 \le i \le n)$。首先，X选择一个子集$S \subseteq ID$，通过压缩S的项数据生成$\mathrm{test_S}$，然后将$\mathrm{test_S}$发送给Y。接下来，Y设$J = ID$，并通过使用S的验证数据对$\mathrm{test_S}$的有效性进行校验。若$\mathrm{test_S}$有效，则设$J \leftarrow J \setminus S$。$Y$将$\mathrm{test_S}$的校验结果（即1比特信息）发送给$X$。然后，$X$选择ID的另一个子集，并在$X$与$Y$之间重复该过程。在$X$与$Y$之间重复上述过程后，$Y$最终输出一个由缺陷的ID组成的列表$J$。

例如，自适应组测试协议包括二进制搜索、rake-and-winnow算法[b-EGH07]、李氏多级算法[b-Li62]以及[b-DH00]第4.6节中所述的挖掘算法。

参考书目

[b-ITU-T X.813] Recommendation ITU-T X.813 (1996）, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

[b-DH00] D. Z. Du and F. K. Hwang, *Combinatorial Group Testing and Its Applications*, Series on Applied Mathematics, vol. 12, 2nd edn. World Scientific, Singapore, 2000.

[b-EGH07] D. Eppstein, M. T. Goodrich, and D. S. Hirschberg, *Improved Combinatorial Group Testing Algorithms for Real-world Problem Sizes*, SIAM J. Comput. 36(5）, pp. 1360-1375, 2007.

[b-HS18] S. Hirose and J. Shikata, *Non-adaptive Group-Testing Aggregate MAC Schemes*, The 14th International Conference on Information Security Practice and Experience (ISPEC 2018）, LNCS 11125, pp. 357-372, Springer, 2018.

[b-KL08] J. Katz and A.Y. Lindell, *Aggregate message authentication codes*, CT-RSA 2008, LNCS 4964, pp. 155-169. Springer, 2008.

[b-Li62] C. H. Li, *A Sequential Method for Screening Experimental Variables*, J. Am. Stat. Assoc. 57 (298）, pp. 455-477, 1962.

[b-MK19] K. Minematsu and N. Kamiya, *Symmetric-key Corruption Detection: When XOR-MACs meet combinatorial group testing*, ESORICS 2019, Part I, LNCS 11735, pp. 595-615, Springer, 2019.

[b-MOV96] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, October 1996, Fifth Printing (August 2001）.

[b-SS19] S. Sato and J. Shikata, *Interactive Aggregate Message Authentication Scheme with Detecting Functionality*, The 33rd International Conference on Advanced Information Networking and Applications (AINA-2019）, pp. 1316-1328, Springer, 2019.

[b-TM05] N. Thierry-Mieg, *A New Pooling Strategy for High-throughput Screening: the Shifted Transversal Design*, *BMC Bioinformatics*, vol. 7, no. 28, 2005.

ITU-T系列建议书

系列A	ITU-T工作的组织
系列D	资费及结算原则和国际电信/ICT的经济和政策问题
系列E	综合网络运行、电话业务、业务运行和人为因素
系列F	非话电信业务
系列G	传输系统和媒介、数字系统和网络
系列H	视听及多媒体系统
系列I	综合业务数字网
系列J	有线网络和电视、声音节目及其他多媒体信号的传输
系列K	干扰的防护
系列L	环境与ICT、气候变化、电子废物、节能；线缆和外部设备的其他组件的建设、安装和保护
系列M	电信管理，包括TMN和网络维护
系列N	维护：国际声音节目和电视传输电路
系列O	测量设备的技术规范
系列P	电话传输质量、电话设施及本地线路网络
系列Q	交换和信令，以及相关的测量和测试
系列R	电报传输
系列S	电报业务终端设备
系列T	远程信息处理业务的终端设备
系列U	电报交换
系列V	电话网上的数据通信
系列X	**数据网、开放系统通信和安全性**
系列Y	全球信息基础设施、互联网协议问题、下一代网络、物联网和智慧城市
系列Z	用于电信系统的语言和一般软件问题

瑞士印刷
2021年，日内瓦