基于国密SM3和SM4算法的SNMPv3安全机制设计与实现

田昊, 王超

引用本文

田昊, 王超. 基于国密SM3和SM4算法的SNMPv3安全机制设计与实现[J]. 计算机科学, 2024, 51(6A): 230500209-7.

TIAN Hao, WANG Chao. Design and Implementation of SNMPv3 Security Mechanism Based on National Security SM3 andSM4 Algorithms [J]. Computer Science, 2024, 51(6A): 230500209-7.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.230500209

基于国密 SM3 和 SM4 算法的 SNMPv3 安全机制设计与实现

田 昊 王 超
华北计算机系统工程研究所 北京 102200

摘 要 随着网络技术的快速发展以及5G技术的日益普及,接入网络的设备呈指数级增加,网络结构日趋复杂,恶意网络攻击频发。如何安全、高效地管理数量庞大、复杂的网络设备正成为网络管理所面临的新挑战。简单网络管理协议 SNMPv3 版本相比 v1 和 v2,增加了基于用户安全模型,提供了数据机密性、完整性、防重放等安全服务。但 SNMPv3 依然存在默认认证算法与加密算法强度不高、密码算法未全面支持国家商密算法标准等问题。文中在分析 SNMPv3 协议现有安全机制的基础上,针对基于用户安全模型的 SNMPv3 现存问题提出了优化方案,将 SM3 和 SM4 国密算法嵌入 SNMPv3 安全机制,基于 SM3 和 SM4 国密算法为 SNMP 协议设计了 HMAC-SM3-192 认证协议和 PRIV-CBC-SM4 加密协议。在未明显增加响应时间的前提下,提升了 SNMP 消息传输过程中抵御伪装、信息篡改、信息泄露等安全威胁的能力,实现了 SNMP 协议安全性方面的优化。

关键词:SNMPv3;用户安全模型;SM3 杂凑算法;SM4 对称加密算法
中图分类号 TP311

Design and Implementation of SNMPv3 Security Mechanism Based on National Security SM3 and SM4 Algorithms

TIAN Hao and WANG Chao
National Computer System Engineering Research Institute of China,Beijing 102200,China

Abstract With the rapid development of network technology and the increasing popularity of 5G technology,the number of devices accessing the network is increasing exponentially,the network structure is becoming increasingly complex,and malicious network attacks are frequent. How to securely and efficiently manage the large number of complex network devices is becoming a new challenge for network management. Compared with v1 and v2,SNMP v3 adds a user-based security model that provides security services such as data confidentiality,integrity,and anti-replay. However,SNMPv3 still has problems,such as the default authentication algorithm and encryption algorithm strength,which are not high,and the cryptographic algorithm does not fully support the national standard for commercial confidentiality algorithms. Based on the analysis of the existing security mechanism of SNMPv3 protocol,this paper proposes an optimization scheme for the existing problems of SNMPv3 based on user security model,embedded SM3 and SM4 national security algorithms into SNMPv3 security mechanism,and designs HMAC-SM3-192 authentication protocol and PRIV-CBC-SM4 encryption protocol for SNMP protocol based on SM3 and SM4 national security algorithms. Without significantly increasing the response time,it improves the ability to resist security threats such as forgery,information tampering and information leakage during SNMP message transmission,and achieves the optimization of SNMP protocol in terms of security.

Keywords SNMPv3,User security model,SM3 hash algorithm,SM4 symmetric encryption algorithm

1 引言

近年来5G技术快速的普及和广泛应用正驱动社会进入IPv6、物联网时代,大量异构物联网设备接入网络导致网络结构复杂程度不断增加。由于物联网设备普遍缺乏高效的安全协议支持,容易受到协议层面的恶意攻击,网络管理所面临的安全威胁更加严峻。目前存在基于 TCP/IP 的简单网络管理协议(Simple Network Management Protocol,SNMP)和国际标准化组织发布的公共管理信息服务/公共管理信息协议(Common Management Information Service,CMIS/Common Management Information Protocol,CMIP)两种网络管理技术。CMIS 制定的服务标准最全面,但因为其实现难度大,所以目前支持 CMIS 的产品很少。SNMP 协议提供了一系列标准以实现访问任何生产厂商生产的任何网络设备,具有应用简单、易于实现和部署等优点,在实际网络管理应用中得到了广泛应用,并成为事实上互联网设备的管理标准。

1988 年国际互联网工程任务组(The Internet Engineering Task Force,IETF)首次定义 SNMPv1,SNMPv1 正式成为基于 TCP/IP 的网络管理协议标准。SNMPv1 仅依靠 SNMP 消息头部的团体名(community)作为授权认证字段。

基金项目:国家重点研发计划(2021YFB3101600)
This work was supported by the National Key Research and Development Program(2021YFB3101600).
通信作者:田昊(tianhao0315@outlook.com)

团体名字段明文传输，使 SNMPv1 从诞生开始就面临着伪装、信息篡改、信息泄露等一系列安全威胁[1]。1993 年 SNMPv2 被正式提出，SNMPv2 在 SNMPv1 的基础上进行了扩展。SNMPv2 不仅新增了协议数据单元(Protocol Data Unit，PDU)类型和表相关操作，还在安全方面引入了目标参加者、源参加者、上下文等对象，重新定义消息格式；采用 MD5 杂凑算法、DES 对称加密算法来保证数据的完整性和机密性，解决了源认证问题。然而，由于 SNMPv2 安全机制实现复杂且无法兼容 SNMPv1，SNMPv2 没有得到普及。SNMPv2 修改版 SNMPv2c 在安全机制方面回退到 v1 版本，才得到广泛应用[2]。SNMP 协议暴露的安全问题依然没有得到解决。1998 年互联网工程任务组提出了 SNMPv3。SNMPv3 增加了基于用户安全模型(User-based Security Model，USM)和视图访问控制模型(View-based Access Control Model，VACM)两个安全子系统，并提出了易于扩展且兼容 SNMPv1、SNMPv2 版本的组织架构，提供了数据加密、认证等安全服务。

2010 年，Peng 等[3]将 SNMP 协议与入侵检测系统结合，提升了管理域内网络系统的安全性。同年，Luo 等[4]对 SNMP 协议 MIB 树的构造算法进行了改进，提升了 MIB 树的访问效率。2012 年，Cheng 等[5]提出了一种支持组播的 SNMPv3 改进模型，增加组播密钥以保障组播数据的安全性；Zhang 等[6]为用户增加密钥生存时间属性，强制用户定时更换密钥，解决了 SNMPv3 基于用户安全模型用户密钥可能长时间不更换的问题。2021 年，Guo 等[7]将 SNMP 协议应用于船舶通信领域，并使用数据库技术存储 MIB 对象，提升了 SNMP 协议数据存储安全性和 MIB 库访问效率。

SNMPv3 新增的安全机制在一定程度上解决了 SNMPv1 和 SNMPv2 暴露的安全隐患，但依然存在以下安全问题。基于用户的安全模型，在默认情况下采用 CBC 模式的 DES 对称加密算法对消息进行加密。随着计算水平的提高，DES 已经可以在较短的时间内被暴力破解[8]，并且 DES 无法抵御差分分析等密文分析方法[9]，使用 DES 算法加密的 SNMP 消息存在被破解的威胁，消息的机密性得不到保证。

在密钥本地化和消息认证码生成过程中，基于用户的安全模型默认采用 MD5、SHA-1 等杂凑算法。2004 年我国密码学家 Wang 等[10]提出的模差分分析方法能够较为高效地检测到 MD5，SHA-1 等国际通用算法的碰撞[11]。

2 SNMPv3 概述

2.1 组织架构

在保持 SNMP 协议应用简单、易实现的前提下，为了解决伪装、信息篡改、信息泄露等安全问题，提高协议的通用性和可扩展性，SNMPv3 提出了新的组织架构[12]。

在 SNMPv3 架构中，管理进程与代理统称为 SNMP 实体。SNMP 实体由 SNMP 引擎和应用程序组成。SNMPv3 在 SNMP 引擎间建立了主从机制，在通信过程中指定其中一个 SNMP 引擎作为权威引擎，其他 SNMP 引擎通过同步权威引擎的时间、启动次数等信息防止重放攻击。当 SNMP 消息包含期望响应的信息时，将接收方作为权威引擎；当 SNMP 消息包含不需要响应的信息时，将发送方作为权威引擎。基于模块化思想，SNMP 引擎被划分为一系列模块，模块之间通过相互作用来提供服务。SNMP 引擎由调度器、消息处理子系统、安全子系统和访问控制子系统组成。

1)调度器

调度器负责应用程序与消息处理模型间交互、SNMP 消息的分发、传输和接收。一个 SNMPv3 具有一个调度器和 3 个分别用于处理简单网络管理协议 v1，v2，v3 版本消息的消息处理子系统。调度器根据消息的版本号，将消息转发给对应版本的消息进行处理。

2)消息处理子系统

消息处理子系统包括 SNMPv1，SNMPv2c，SNMPv3 等消息处理模块，分别处理不同版本的消息。消息处理模块定义了特定版本的 SNMP 消息的格式，以及如何对该版本的 SNMP 消息进行解析并提取数据，如何构造该版本的 SNMP 消息。

3)安全子系统

安全子系统提供 SNMP 消息的认证和加密服务。它可以包含多个安全模型，SNMPv3 协议使用的安全模型为基于用户的安全模型[13](User-Based Security Model，USM)。SNMPv3 基于模块化的组织架构支持用户定义自己的安全模型。安全模型需要定义它所防范的安全威胁、服务的目标和为提供安全服务所采用的安全协议。为了支持基于用户安全模型定义的安全机制，SNMP 协议的管理信息库(Management Information Base，MIB)新增了 SNMP-FRAMEWORK-MIB，SNMP-USER-BASED-SM-MIB 文件，并定义了认证协议、加密协议等新的 MIB 子树及对象节点。

4)访问控制子系统

访问控制子系统通过一个或多个访问控制模型确认管理设备的访问是否合法。SNMPv3 默认的访问控制模型为 RFC3415 所描述的基于视图的访问控制模型[14](View-based Access Control Model，VACM)。访问控制模型可以定义访问控制处理过程中使用的 MIB 模块，以实现对访问控制策略的远程配置。

2.2 消息格式

SNMPv3 的消息需要安全参数字段支持数据的加解密和认证功能。如图 1 所示，SNMPv3 重新定义了消息格式，整体上可将消息分为消息头部、安全参数、范围协议数据单元(Scoped Protocol Data Unit，Scoped PDU) 3 个部分。

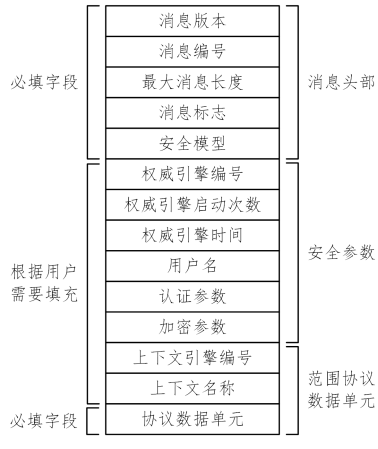


图 1 SNMPv3 消息格式

Fig. 1 SNMPv3 message format

消息头部由调度器产生，定义了消息相关的全局信息，包

括消息采用的协议版本、消息编号、发送方支持的最大消息长度、安全模型。为了兼容 SNMP 协议早期 v1，v2 版，协议版本号字段可取值为 1，2 或 3，分别代表 SNMP 协议的 3 个版本，调度器根据消息版本字段，选择将消息转发到对应的消息处理子系统；消息标志位使用 1 个字节表示消息状态，包括认证状态、加密状态等。安全模型字段取值为 0～3，分别代表任意安全模式、SNMPv1 安全模式、SNMPv2c 安全模式、基于用户的安全模式。

安全参数部分包含了基于用户安全模型提供身份认证、数据加密等安全服务需要的安全参数。其中认证参数字段用于存储根据认证协议（MD5 或 SHA1）计算的 12 字节消息认证码，加密参数字段存储加密算法（AES 或 DES）中所需要的随机数。

范围协议数据单元由 PDU、上下文引擎编号和上下文名称构成。PDU 是一个 SNMP 协议数据单元，包含上下文中的信息。上下文引擎编号用于唯一标识管理域中的一个 SNMP 实体；上下文名称用于唯一标识一个 SNMP 实体内的上下文。

3　基于用户安全模型优化方案

3.1　协议分析

在 RFC 3414 中，基于 MD5 和 SHA-1 杂凑函数分别定义了 HMAC-MD5-96 和 HMAC-SHA-96 两个认证协议。标准 MD5 哈希算法输出摘要的长度为 128 比特，在基于用户安全模型中 HMAC-MD5-96 认证协议对 MD5 哈希算法输出结果进行截断，保留 96 比特作为 HMAC-MD5-96 认证算法的最终计算结果。标准 SHA-1 哈希算法输出 160 比特，在基于用户安全模型中，HMAC-SHA-96 认证协议对 SHA-1 哈希算法进行截断，最终保留 96 比特作为最终计算结果。随着计算能力高速发展 96 比特的完整性密钥空间，容易遭受碰撞检测攻击。

SNMPv3 基于用户安全模型默认使用 CBC 模式的 DES 对称加密算法。每次加密时使用用户加密密钥的前 8 字节作为 DES 密钥，后 8 字节作为预初始化向量。4 字节权威引擎编号和 4 字节权威引擎本地维护的随机数组成盐，将预初始化向量与盐异或生成 DES 初始化向量。初始化向量变化空间仅依靠 4 字节随机数，使得密钥有效生存周期变短，需要定期更换密钥才能保障传输数据的机密性。DES 实际用到的密钥只有 56 比特，密钥空间较小，随着计算机计算能力的不断提高，使用 DES 算法加密 SNMP 消息数据无法有效应对暴力破解攻击。

3.2　优化方案设计

SM3 和 SM4 算法是我国自主设计的国密算法，目前已作为我国杂凑算法和对称加密算法，成为密码行业标准和国家标准，被广泛推广使用。

SM3 算法压缩函数整体结构与 SHA-256 相似，但新增了 P 置换等技术，可以有效应对强碰撞分析、弱碰撞的线性分析等主流的密码分析方法[15]。此外，SM3 密码杂凑算法使用了适合 32 比特微处理器的基本运算，具有跨平台实现、易优化的特点。SM3 密码杂凑算法在安全性、执行效率等方面均高于或等于国内外其他标准杂凑算法，总体性能优于国际上广泛使用的 SHA-256 算法[16]。

SM4 对称加密算法是一种分组密码算法，其分组长度为 128 bit，密钥长度也为 128 bit。相比 DES，密钥空间显著增加。相比 DES 算法，SM4 能更好地抵御暴力攻击。SM4 加密算法与密钥扩展算法都采用 32 轮非线性迭代结构，可抵抗差分攻击、线性攻击，具备更高的理论安全性。

为解决 3.1 节所述的安全隐患，本文采用 SM3 杂凑算法和 SM4 对称加密算法替换 SNMPv3 基于用户安全模型默认的 MD5、SHA-1 杂凑算法和 DES 算法。定义基于 SM3 杂凑算法的 HMAC-SM3-192 协议和基于 SM4 算法的 PRIV-CBC-SM4 协议分别作为 SNMPv3 基于用户安全模型的认证协议和加密协议。

3.2.1　基于 SM3 杂凑算法密钥本地化

基于用户安全模型在密钥本地化阶段默认使用 MD5、SHA-1 杂凑算法派生加密密钥和认证密钥，本文使用 SM3 算法替换 MD5、SHA-1 算法完成密钥的派生。

如表 1 所列，SM3 杂凑算法的输出结果长度为 32 字节，因此在派生密钥阶段将在 SM3 计算后对结果进行截取，最终保留最高有效位 16 字节作为派生密钥。

表 1　SM3，SHA-1，MD5 算法的输出长度

Table 1　Output length of SM3, SHAG1, MD5 algorithms

算法名称	输出长度/bit
SM3	256
SHA-1	160
MD5	128

3.2.2　HMAC-SM3-192 认证协议

基于用户安全模型默认的 HMAC-MD5-96 认证协议和 HMAC-SHA-96 认证协议对 MD5 和 SHA-1 杂凑算法输出结果进行截断，只保留前 12 字节作为最后的消息验证码填充至身份认证参数字段，消息验证码长度过短，抗碰撞性较弱。基于 SM3 算法的 HMAC-SM3-192 协议在对消息和用户认证密钥进行计算之后同样进行截取操作，但保留 24 字节作为消息验证码。

图 2 给出了 HMAC-SM3-192 协议处理 SNMP 实体对外发送 SNMP 消息（向外网发送）的过程。

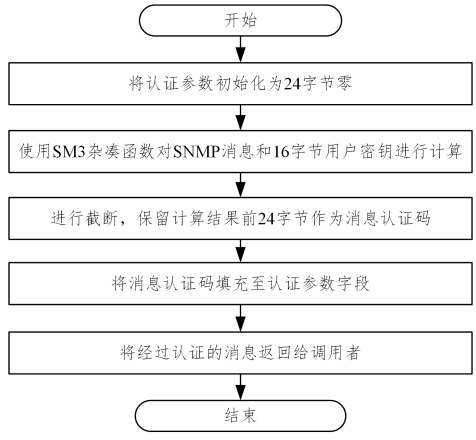


图 2　HMAC-SM3-192 协议处理传出消息的过程

Fig. 2　Processing of messages sent abroad using the HMAC-SM3-192 protocol

1）认证参数字段初始化为 24 字节零。

2）将 32 字节用户认证密钥和消息内容输入 SM3 哈希函数，输出 32 字节计算结果。

3)对计算结果进行截断,保留 SM3 杂凑算法前 24 字节输出结果作为消息认证码。

4)将消息认证码填充至认证参数字段。

图 3 给出了 HMAC-SM3-192 协议处理 SNMP 实体接收到 SNMP 消息的过程。

1)判断接到消息认证参数字段长度,若长度不等于 24 字节,则返回认证参数错误,处理流程结束。

2)将 SNMP 消息和 16 字节用户认证密钥作为 SM3 哈希算法的输入并进行计算。

3)对 SM3 哈希算法计算结果进行截断,保留 24 字节作为消息认证码(MAC)。

4)将新计算的消息认证码和认证字段缓存值进行对比,若两者一致则返回身份认证成功,否则返回认证失败。

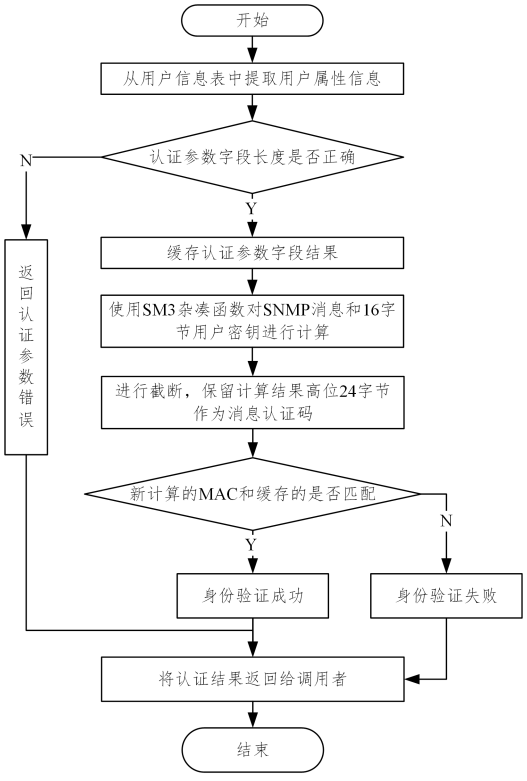


图 3 HMAC-SM3-192 处理传入消息的流程

Fig. 3 Processing of arriving messages using the HMAC-SM3-192 protocol

3.2.3 PRIV-CBC-SM4 加密协议

SNMPv3 基于用户安全模型默认使用 CBC-DES 加密协议,密钥空间小,易被暴力破解。本文采用 SM4 算法替换 DES 算法,定义 PRIV-CBC-SM4 协议。PRIV-CBC-SM4 协议使用 CBC 模式的 SM4 算法对 SNMP 消息进行加密。相比 CBC 模式的 DES 加密算法,CBC 模式的 SM4 算法需要更长的加密密钥和初始化向量,需要 16 字节的加密密钥和 16 字节的初始 IV 作为输入。

PRIV-CBC-SM4 协议使用密钥本地化派生的全部 16 字节用户加密密钥作为 SM4 算法加密密钥。4 字节权威引擎启动次数、4 字节权威引擎时间和 8 字节 SNMP 引擎本地维护的随机数构成 16 字节的初始化向量。

图 4 给出了 PRIV-CBC-SM4 协议加密数据的过程。

1)将加密参数字段初始化为 8 字节零。

2)根据权威引擎启动次数字段、权威引擎时间字段和本地维护的 8 字节随机数构造初始化向量。

3)CBC 模式的 SM4 算法根据 16 字节用户加密密钥和 16 字节初始化向量对 SNMP 消息数据字段进行加密。

4)将随机数填充至 SNMP 消息加密参数字段。

5)将加密后的 SNMP 消息返回给调用者。

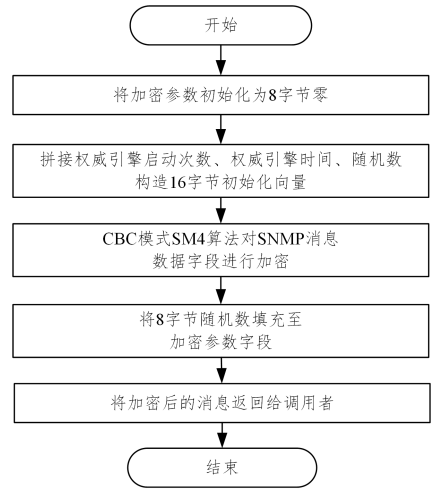


图 4 PRIV-CBC-SM4 协议加密数据的过程

Fig. 4 Process of encrypting data using the PRIV-CBC-SM4 protocol

图 5 给出了 PRIV-CBC-SM4 接收到消息后解密数据过程。

1)从接收到的 SNMP 消息中提取加密参数字段的值。

2)判断盐的长度是否正确,若正确则执行步骤 3);若错误则返回错误,结束解密过程。

3)提取引擎启动次数字段、权威引擎时间字段,将两者与加密参数字段中随机数的值进行拼接,构造 16 字节初始化向量。

4)将 16 字节用户加密密钥、16 字节初始化向量、SNMP 消息数据部分输入至 CBC 模式 SM4 算法,对消息数据部分进行解密。

5)将解密后的 SNMP 消息返回至调用者,解密过程结束。

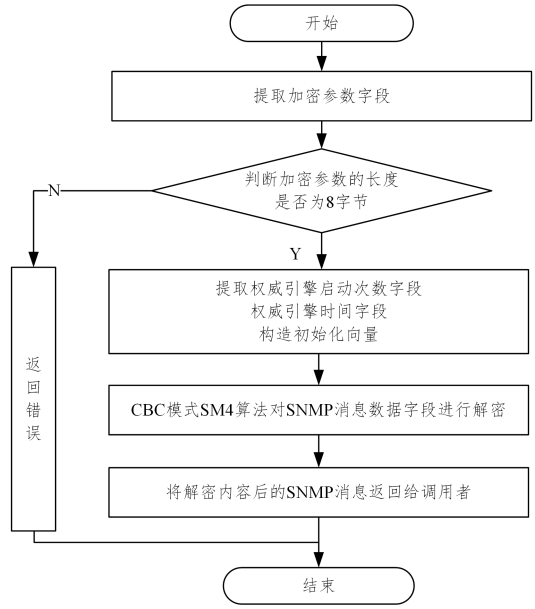


图 5 PRIV-CBC-SM4 协议解密数据的过程

Fig. 5 Process of decrypting data using the PRIV-CBC-SM4 protocol

3.3　优化方案实现

3.3.1　MIB 模块定义

SNMP 协议管理信息库声明了网络中所有可能的被管理进程查询和设置对象集合的数据结构。SNMP 协议管理信息库采用树形结构组织、存储数据信息。SNMP 协议管理信息文件是按照抽象语法标记规则（Abstract Syntax Notation One，ASN.1）定义的文本文件，用户可以根据需要，使用编码规则（BasicEncoding Rules，BER）在已定义的树结构上插入新的节点。

为实现 SNMP 协议对 SM3 算法和 SM4 算法的支持，本文定义了 SNMP-USM-HMAC-SM3-MIB 和 SNMP-USM-PRIV-SM4-MIB 两个 MIB 模块。SNMPv3 管理信息库的 SNMP-FRAMEWORK-MIB 模块中定义了认证协议子树和加密协议子树；SNMP-USER-BASED-SM-MIB 模块定义了分别基于散列函数 MD5 和 SHA-1 的身份认证协议节点以及 CBC-DES 加密协议节点。本文在相应子树下新增基于 SM3 杂凑算法的认证协议和基于 SM4 算法加解密协议的节点。

3.3.2　密钥本地化

基于 SM3 杂凑算法的密钥本地化通过 generate_user_localKey 函数实现。该函数输入为用户加密口令或认证口令；输出为用户加密密钥或用户认证密钥。generate_user_localKey 函数内部调用两次 SM3 哈希函数，并在计算后截取前 16 字节作为计算结果。第一次调用计算用户口令的哈希值 ku；第二次调用计算 ku||SNMPEngineID 哈希值作为密钥本地化的最终结果。

3.3.3　HMAC-SM3-192 协议实现

HMAC-SM3-192 协议通过 HMAC_SM3_192 函数实现。该函数用于完成 SNMP 消息认证码的计算，并返回消息认证码字段。HAMC_SM3_192 函数输入为 SNMP 消息、用户认证密钥、认证参数字段及上述 3 者的长度；输出为消息认证码计算结果，若计算成功则返回 true，若失败则返回 False。HAMC_SM3_192 函数内部调用 SM3 杂凑函数 HMAC 模式，截取计算结果的前 24 字节作为 SNMP 消息认证码；然后判断消息认证码字段是否非空，若非空则比较新计算的消息认证码和 SNMP 消息认证参数字段，返回两者的比较结果；否则将计算得到的 SNMP 消息认证码填入 SNMP 消息认证参数字段。

3.3.4　PRIV-CBC-SM4 协议实现

PRIV-CBC-SM4 协议通过 CBC_SM4_ENC 和 CBC_SM4_DEC 函数实现，两者分别负责完成 SNMP 消息的加密、解密。

CBC_SM4_ENC 函数输入参数为 SNMP 消息、用户加密钥和初始化向量；输出参数为加解密计算结果，若加密成功则返回 true，若失败则返回 False。SM4 算法一次只加密 128bit 数据，即 16 字节数据，因此当明文数据不足 16byte 或者非 16byte 倍数时，需要使用填充算法将明文填充至 16 的倍数。CBC_SM4_ENC 函数中使用 PKCS7 填充模式，以 16 字节划分 SNMP 消息数据部分，对于尾部不满 16 字节的数据，用 16 减去尾部数据块长度得到的字符进行填充。如果正好为 16 的倍数，则需要填充 16 字节 0x10。

CBC_SM4_DEC 函数输入参数为 SNMP 消息、用户加密钥和初始化向量；输出参数为加解密计算结果，若加密成功则返回 true，若失败则返回 False。根据解密后数据字段最后一个字节确定填充字节长度，在数据字段尾部删除对应长度的填充数据，得到最终解密结果。

3.4　安全性分析

3.4.1　身份认证与数据完整性

基于国密算法的 SNMP 采用 HMAC-SM3-192 协议计算消息认证码，实现身份验证和消息完整性保护。HMAC-SM3-192 协议将 16 字节的用户密钥和数据内容作为输入，计算消息认证码不仅能够抵御恶意篡改攻击，还可以实现对消息来源的认证。如表 2 所列，HAMC-SM3-192 协议输出消息认证码的长度为 192 bit，具备较高安全强度，能够有效抵御碰撞攻击、差分攻击。HMAC-SM3-192 协议通过采用安全性更高的 SM3 算法来扩展消息认证码长度，确保消息认证和完整性的强度，解决了 HMAC-MD5-96 存在的安全隐患。

表 2　HMAC-SM3-192 和 HMAC-MD5-96 协议的对比

Table 2　Comparison of HMAC-SM3-192 and HMAC-MD5-96 protocols

	HMAC-SM3-192	HMAC-MD5-96
核心算法	SM3	MD5
输出长度	192 bit	96 bit
抗碰撞性	强	弱
安全性	较高	存在安全隐患

3.4.2　数据机密性

基于国密算法的 SNMP 采用 PRIV-CBC-SM4 算法作为数据加密协议，实现通信内容的机密性保护。如表 3 所列，与 SNMP 默认的数据加密协议 CBC-DES 相比，PRIV-CBC-SM4 在算法安全性、密钥空间、初始化向量随机化程度上具有显著优势。在算法安全性方面，PRIV-CBC-SM4 协议采用 SM4 加密算法。相比 DES 算法，SM4 采用了更复杂的 S 盒设计、非线性变换以及更大的分组长度，使得其对差分攻击和线性攻击有更强的抵御能力。在密钥空间方面，PRIV-CBC-SM4 协议采用 128 bit（16 字节）的密钥长度，因此拥有庞大的 2^{128} 种可能的密钥组合。相比之下，CBC-DES 实际有效密钥长度为 56 bit，拥有 2^{56} 种不同的密钥可能性。这个密钥空间差异决定了 SM4 具有远远超过 DES 的密钥组合数目，使得 SM4 在暴力破解和密码分析攻击方面更为安全。密钥空间的扩大直接增强了加密算法的安全性，为加密通信提供了更加牢固的保障。此外，PRIV-CBC-SM4 协议在初始化向量随机性方面也做了进一步改进。SNMP 默认的数据加密协议 CBC-DES 初始化向量由 32 bit SNMP 权威引擎 ID 和 32 bit 时间戳组成。在单次通信中权威引擎 ID 固定不变，CBC-DES 协议由 32 bit 时间戳保证初始化向量的随机性，初始化向量随机化空间为 2^{32}。PRIV-CBC-SM4 协议初始化向量由 32 bit SNMP 权威引擎 ID、32 bit 时间戳、64 bit 随机数共同组成，初始向量随机化空间扩展至 2^{96}。PRIV-CBC-SM4 通过时间戳和随机数的组合增强了初始化向量的随机性，从而更好地保证了单次加密的唯一性。

综合来看，基于国密算法的 SNMP 协议在身份验证、消息完整性、机密性保护以及算法安全性方面表现更优，尤其对于国内涉及国家安全领域的通信和信息传输，更具合规性和安全性。

表 3 PRIV-CBC-SM4 和 CBC-DES 协议的对比

Table 3 Comparison of PRIV-CBC-SM4 and CBC-DES protocols

	PRIV-CBC-SM4	CBC-DES
核心算法	SM4	DES
密钥长度	128 bit	56 bit
分组长度	128 bit	64 bit
加密轮数	32 轮	16 轮
初始化向量	128 bit	64 bit
安全性	较强	易被暴力破解

4 实验及分析

为提升 SNMPv3 基于用户安全模型的安全性，本文设计并实现了 SM3、SM4 国密算法对 SNMPv3 基于用户安全模型中存在安全隐患的 MD5 杂凑算法和 DES 对称加密算法的替换。为验证其可行性及计算效率，将进行以下实验。

1)只认证不加密(AUTHNOPRIV)访问模式下，查询系统运行信息节点，遍历查询系统信息子树下的多个节点信息，验证单一节点查询请求的和块查询请求的结果是否正确。

2)认证加密(AUTHPRIV)访问模式下，查询系统运行信息节点，遍历查询系统信息子树下的多个节点信息，验证 SNMP 消息数据域是否被加密。

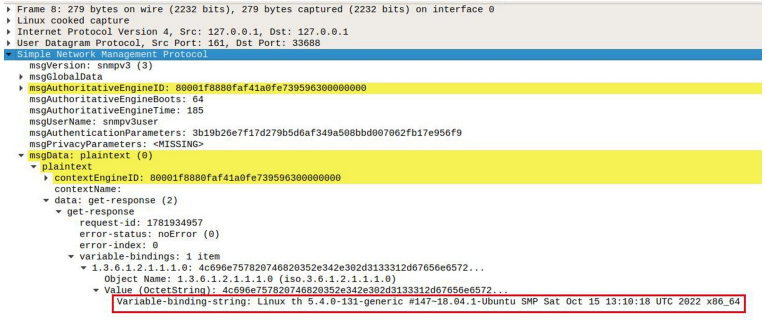
3)只认证不加密(AUTHNOPRIV)访问模式下，对比基于用户安全模型使用 HMAC-SM3-192 认证协议和 HMAC-MD5-96 认证协议情况下，对于代理端同一管理信息节点的查询结果及效率。

4)认证加密(AUTHPRIV)访问模式下，对比基于用户安全模型使用 HAMC-SM3-192 认证协议、PRIV-CBC-SM4 加密协议和 HMAC-MD5-96 认证协议、USM-CBC-DES 加密认证协议情况下，对于代理端同一管理信息节点的查询结果及效率。

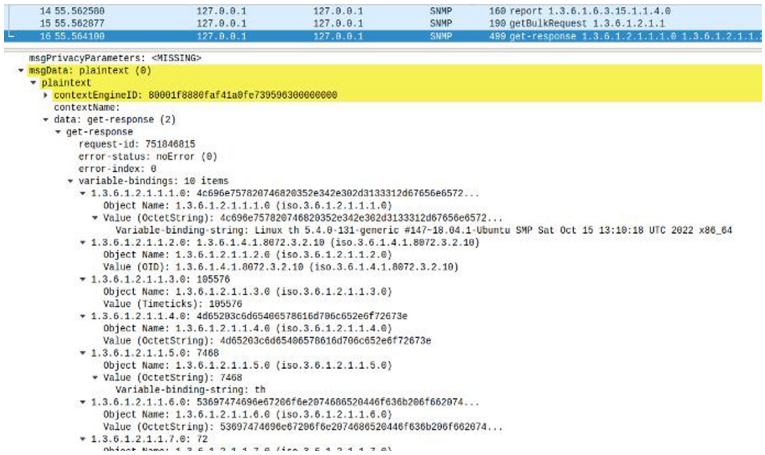
为防止实验过程中网络拥塞对实验结果的影响，保持实验结果的客观性，本次实验在本地进行。运行系统描述节点(system. sysDescr. 0 OID:. 1. 3. 6. 1. 2. 1. 1. 1. 0)是真实网络设备管理情境中查询次数较多的信息节点，本次实验将在不同模式下查询一万次运行系统描述节点，比较不同加密、认证协议下对该节点的查询效率。

实验环境如下：虚拟机系统为 Ubuntu18. 04 64 位，3 GB 运行内存。本次实验使用 Ubuntu 虚拟机访问本地管理信息库的 system. sysDescr. 0 节点，该节点存储内容为运行系统版本信息。

图 6(a)和图 6(b)给出了在只认证模式下，分别执行查询对本机运行系统描述节点执行查询操作和对系统信息子树(system OID:. 1. 3. 6. 2. 1. 1)执行块查询操作后，抓包软件捕获到的 SNMP 协议消息报文。如图 6(a)、图 6(b)所示，使用 HMAC-SM3-192 认证协议对 SNMP 消息进行身份认证后，认证参数字段长度为 24 字节。相比 HMAC-MD5-96 协议，出现碰撞的概率更低。查询结果以明文形式传输，可以明确看到 SNMP 消息的数据域内容、分析出查询节点以及查询方式。单一节点查询请求和块查询请求查询到本机运行系统为 Ubuntu18. 04 64 位版本，并且块查询操作还查询到了系统信息子树下系统名称、系统所在位置等节点信息。两种查询方式查询到的系统信息与实际情况一致，查询结果正确。



(a)只认证模式查询 sysDescr. 0 节点结果



(b)只认证模式块查询 system 节点结果

图 6 AUTHNOPRIV 模式下不同查询方式的返回结果

Fig. 6 Different query methods return results in AUTHNOPRIV mode

图 7(a)和图 7(b)给出了在认证加密模式下，分别执行查询对本机运行系统描述节点执行查询操作和对系统信息节点

(system OID:.1.3.6.2.1.1)执行块查询操作后，抓包软件捕获到的 SNMP 协议消息报文。使用 HMAC-SM3-192 协议和 PRIV-CBC-SM4 协议对 SNMP 消息进行认证加密后，认证参数字段长度是 24 字节消息认证码，加密参数字段填充了 8 字节随机数，数据部分进行了加密。如图 7(a)、图 7(b)所示，加密后无法从报文中直接获取数据信息，也无法分析出查询节点和查询方式。本文定义的 PRIV-CBC-SM4 协议能够很好地保证 SNMP 报文数据域的机密性，防止网络管理过程中泄露敏感信息。

(a)认证加密模式查询 sysDescr.0 节点结果

(b)认证加密模式块查询 system 节点结果

图 7　AUTHPRIV 模式下不同查询方式的返回结果

Fig. 7　Different query methods return results in AUTHPRIV mode

图 8 给出了不同模式下使用不同协议为 SNMP 提供安全服务时访问 1 万次 sysDescr.0 节点的平均单次访问时间。由图可知，虽然 HMAC-SM3-192 协议将消息认证码长度增加到 24 字节，但其平均单次查询耗时相比 HMAC-MD5-96 协议只增加了约 0.004%(约 0.1 ms)。在认证加密模式下使用 HMAC-SM3-192 认证协议、CBC-SM4 加密协议平均单次访问用时相比 HMAC-SM3-192 认证协议、CBC-DES 加密协议单次查询耗时增加了 0.009%，不到 0.5 ms 的时间，完全在用户可接受的响应时间之内。

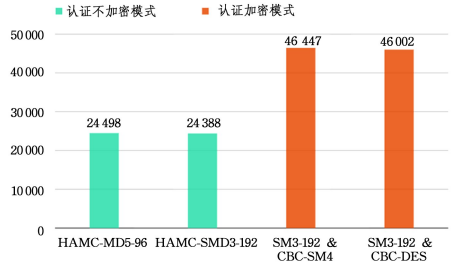


图 8　不同认证、加密协议下平均单次访问时间

Fig. 8　Average single access time under different authentication and encryption protocols

结束语　SNMP 协议作为公认的互联网设备管理标准，在网络管理领域发挥着重要作用。然而，SNMP 协议存在默认密码算法安全性不高、不支持国家密码标准算法等问题，因此提升 SNMP 协议的安全性对实现安全、高效的网络管理至关重要。本文分析了简单网络管理协议 v3 版本安全机制，将我国国家商密标准算法 SM3、SM4 算法嵌入 SNMP 协议，基于 SM3 杂凑算法和 SM4 对称加密算法为 SNMP 定义了新的认证协议和加密协议。在未明显增加响应时间的前提下，提升了 SNMP 消息传输过程中抵御伪装、信息篡改、信息泄露等安全威胁的能力，实现了 SNMP 协议在安全性方面的优化。

参 考 文 献

[1] YING W F, DUAN X D, SHEN J L. Analysis and com-parison of SNMPv1, SNMPv2 and SNMPv3 security protocols[J]. Computer Engineering, 2002, 28(10): 153-156.

[2] CHEN Y, LU Z X, FENG Y L. Analysis and Comparison of SNMPv1, SNMPv2c and SNMPv3 Protocol Structures[J]. Modern Computer, 2004(2): 59-64.

[3] PENG Z F, LI F, LUO C J. Research on the security scheme of network management system based on SNMP[J]. Computer Engineering and Design, 2010, 31(17): 3778-3780.

[4] LUO Y, YAO J L. Research on efficient algorithm of MIB construction tree based on SNMP[J]. Computer Engineering and Design, 2010, 31(15): 3386-3389.

[5] CHENG C L, ZHANG D Y. An improved SNMPv3 model supporting multicast[J]. Computer Science, 2012, 39(4): 89-93.

[6] ZHANG Y, HONG W J. Research on SNMPv3 optimization based on user security model[J]. Netinfo Security, 2012(2): 74-77.

[7] GUO X Q, XIE C W. Application of SNMP communication protocol in the database of ship communication network man-agement system[J]. Ship Science and Technology, 2021, 43(24): 130-132.

[8] ZHANG L L, ZHANG Y Q. Brute Force Attack on Block Cipher Al-gorithm Based on Distributed Computation[J]. Computer Engineering, 2008(13): 121-123.

[9] GUO H, DING G L, LIU C J, et al. Realization of DEMA for DES I mple mentation[J]. Microelectronics & Compute, 2009, 26(12): 34-37.

[10] WANG X, YU H. How to break MD5 and other hash functions [C]// Proc of the 24th Annual Int Conf on the Theory and Applications of Cryptographic Techniques. 2005: 19-35.

[11] WANG X Y, YU H B. Survey of Hash Function[J]. Journal of Information Security Research, 2015, 1(1): 19-30.

[12] HARRINGTON D, PRESUHN R, WIJNEN B. An architecture for describing simple network management protocol (SNMP) management frameworks[C]// RFC 3411. IETF, 2002.

[13] BLUMENTHAL U, WIJNEN B. User-based security model (USM) for version 3 of the simple network management protocol(SNMPv3)[C]// RFC 3414. IETF, 2002.

[14] WIJNEN B, PRESUHN R, MCCLOGHRIE K. RFC3415: View-based Access Control Model(VACM) for the Simple Network Management Protocol(SNMP)[C]// RFC 3415. IETF, 2002.

[15] HU J X, YANG Y, XIONG L, et al. SM Algorithm Analysis and Software Performance Research[J]. Netinfo Security, 2021, 21(10): 8-16.

[16] WANG X Y, YU H B. SM3 cryptographic hash algorithm[J]. Journal of Information Security Research, 2016, 2(11): 983-994.

TIAN Hao, born in 1999, postgraduate. His main research interests include network protocol security and information security.