引用格式：漆骏锋, 潘文伦, 冷恣杰. 面向多类型节点的混合多级 μTESLA 协议 [J]. 电子科技大学学报, 2025, 54(2): 233-241.
QI J F, PAN W L, LENG M J. Hybrid multi-level μTESLA protocol for multi-type nodes[J]. Journal of University of Electronic Science and Technology of China, 2025, 54(2): 233-241.

面向多类型节点的混合多级 μTESLA 协议

漆骏锋[1*]，潘文伦[2]，冷恣杰[3]

（1. 电子科技大学 计算机科学与工程学院，成都 611731；2. 北京海泰方圆科技股份有限公司 密码技术融合创新中心，北京 100085；
3. 中国人民大学 信息资源管理学院，北京 100872）

摘要：随着5G技术的广泛应用和6G网络技术的前瞻性研究，物联网设备已广泛应用于各种实际场景中，无线通信网络也日益复杂。在这样复杂的无线通信环境中，确保数据安全和通信效率尤为关键。广播鉴别协议作为主要解决方案之一，已应用于多种场景，但在面对多类型、大规模节点的安全广播需求时，现有协议仍存在局限性。针对这一问题，提出了一种创新性的广播鉴别协议：混合多级μTESLA 协议。该协议融合并优化了现有 TESLA 协议及其变体的优点，特别针对多类型节点环境进行了创新性改进。协议采用了双层密钥链设计，其中高级密钥链具有较长的时间间隔，用于生成和管理低级密钥链；低级密钥链则直接应用于消息鉴别。这种设计不仅提升了鉴别效率，还显著减轻了广播节点在密钥使用和存储方面的负担。此外，低级密钥链被分为多组，每组专门用于向特定类型的节点群广播消息，实现了针对不同类型节点群的分类广播与资源的动态优化。

关键词：连续鉴别；分类广播；低开销；可扩展性；TESLA 协议
中图分类号：TP393.08 **文献标志码：**A DOI: 10.12178/1001-0548.2024039

Hybrid multi-level μTESLA protocol for multi-type nodes

QI Junfeng[1*], PAN Wenlun[2], and LENG Minjie[3]

(1. School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China;
2. Cryptographic Technology Integration and Innovation Center, Beijing Haitai Fangyuan Technologies Co., Ltd., Beijing 100085, China;
3. School of Information Resource Management, Renmin University of China, Beijing 100872, China)

Abstract: With the widespread applications of 5G technology and the forward-looking researches on 6G network technology, IoT devices have been extensively used in various practical scenarios, leading to an increasingly complex wireless communication network. In such a complex wireless communication environment, ensuring data security and communication efficiency has become particularly crucial. Broadcast authentication protocols, as one of the main solutions, have been applied in multiple scenarios. However, when facing secure broadcasts to multi-type and large-scale nodes, existing protocols still have limitations. To address this issue, an innovative broadcast authentication protocol is proposed, named the hybrid multi-level μTESLA protocol. This protocol integrates and optimizes the advantages of the existing TESLA protocol and its variants, with innovative improvements specifically for environments with multiple types of nodes. The protocol employs a dual-layer key chain design, where the high-level key chain has longer time intervals for generating and managing the low-level key chains; the low-level key chains are directly used for message authentication. This design not only enhances authentication efficiency but also significantly reduces the burden on broadcast nodes in terms of key usage and storage. Moreover, the low-level key chains are divided into multiple groups, each dedicated to broadcasting messages to a specific type of node group, achieving classified broadcasting and dynamic optimization of resources for different types of node groups.

Key words: continuous authentication; categorized broadcasting; low overhead; scalability; TESLA protocol

收稿日期：2024−02−26
基金项目：国家重点研发计划（2021QY2334）
作者简介：漆骏锋，博士生，高级工程师，主要从事密码应用、移动安全通信、物联网安全等方面的研究。
*通信作者 E-mail: 14455418@qq.com

随着5G技术的广泛应用和对6G技术的研究深入[1]，网络容量和连接密度显著提升，这使得物联网设备间的通信更加高效，为大规模的 IoT 部署奠定了基础。然而，网络规模和复杂性的增加也带来了更大的安全挑战，包括外部攻击（如网络钓鱼和 DDoS 攻击）和网络内部的威胁（如节点间的恶意数据传输或者节点的伪造）。物联网设备的能源和通信带宽限制加剧了这些安全问题，凸显了对更轻量级、更高效安全解决方案的需求[2]。

轻量级密码学协议广泛应用于资源受限的物联网设备[3]，其中，一个关键的轻量级广播鉴别协议是时间高效流丢失容忍鉴别（timed efficient stream loss-tolerant authentication, TESLA）协议。TESLA 协议采用密码技术，在受限设备中保持低通信和计算开销的同时实现了完整性和用户鉴别[4-6]。TESLA 协议及其变种主要依赖对称密码学，包括用于鉴别广播数据包的对称密钥以及生成消息鉴别码（MAC）值以验证数据包的完整性[7]。

尽管 TESLA 协议有着显著的优势，但它在适应5G和6G技术下物联网网络的环境时也面临若干局限性：可扩展性的不足，在日益增长的物联网设备数量和网络复杂度面前，TESLA 协议在支持大规模网络可扩展性方面存在挑战；实时性的局限，TESLA 协议在处理发送者和接收者之间的实时鉴别方面存在局限，这可能影响对实时数据和动态网络环境的响应；脆弱性问题，尽管 TESLA 提供了基本的安全保护，但它可能对某些类型的攻击，如拒绝服务（DoS）攻击和暴力破解攻击仍然脆弱。鉴于这些挑战，对 TESLA 协议的进一步改进和优化是必要的，以便更好地适应5G和6G技术下物联网网络的需求。

为了解决原始 TESLA 协议的局限性，研究人员提出了多种改进方案，如无限 TESLA（Inf-TESLA）协议[8]、增强型 Inf-TESLA 协议[9]、μTESLA 协议[10-11] 及其相关改进多级μTESLA 协议[12-13]，以及综合并最大化这些协议的优点，并在网络中保持可接受的计算和通信需求的混合 TLI-μTESLA（hybrid two-level TESLA）协议[14]。这些改进着重于提高网络的可扩展性、实时性，以及增强对复杂网络攻击的抵抗力，从而确保物联网设备间的实时监控和数据传输的安全，以及保持网络对周围环境的实时响应和更新。

本文对文献 [14] 中的方案进行了深入改进，提出了一种新型混合广播鉴别协议，称为混合多级 μTESLA（hybrid multi-level μTESLA）协议。该协议专为应对大规模物联网中向众多不同类型节点进行分类广播的挑战而设计。该协议通过独立向不同类型的节点进行广播，降低了接收节点的计算负担，简化了数据处理流程，并优化了广播节点中高级密钥链的使用，实现了更高效、更安全的广播机制。该协议平衡了物联网中安全性和效率的双重需求，为下一代物联网应用提供了一个全面的解决方案，在不断发展的5G和6G技术背景下，该协议具有重要应用价值。

1 TESLA 相关协议介绍

本节简要介绍 TESLA、Inf-TESLA 与增强型 Inf-TESLA、μTESLA 与多级μTESLA 协议，以及混合 TLI-μTESLA 协议等。由于 TESLA 系列协议均使用密钥延迟披露的方式使接收者获取密钥信息，实现对之前接收到的消息的鉴别，而当接收者与发送者具有共同密钥后，可以使用成熟的对称密码技术实现对消息的鉴别，如文献 [15-17] 中的系列方法，因此，本文只考虑上述协议的密钥生成与披露过程，而略去密钥的使用方法。

1.1 TESLA 协议

TESLA 协议是一种专为无线和其他资源受限网络环境设计的数据认证协议。它提供了一种有效的方式来确保数据的完整性和来源的真实性，具有对称密码的效率，同时具有较低的能源和带宽的限制。

TESLA 协议基于对称密钥加密和时间同步的概念，使用一系列相关的密钥（密钥链），其中每个密钥都是通过对前一个密钥进行杂凑运算得到的。这种设计确保了即使某个密钥被泄露，也不会影响到之前的密钥。TESLA 协议的基本原理如下。

1）密钥链：在协议开始时，发送方选择随机数K_n，并使用单向函数F生成密钥链：

$$K_0, K_1, \cdots, K_n$$

式中，$K_i = F(K_{i+1})$。$i = 0, 1, \cdots, n-1$。而在使用密钥时，从K_0开始依次使用，如在时刻t使用密钥K_t，在时刻$t+1$使用密钥 K_{t+1}。

2）时间同步：要求发送方和接收方之间有一定程度的时间同步，协议依赖于时间信息来确定密钥的有效性。如接收方在时刻t收到的消息，可以确认是发送方在时刻$t-\delta$发送的，其中δ为允许的最大时间误差。

3）延迟密钥披露：发送方在发送消息时使用当前密钥生成消息鉴别码，但不立即公布该密钥。

密钥会在一定时间后才被公布，确保了即使攻击者截获了密钥，也无法在有效期内利用它伪造消息。

4）消息鉴别：接收方在收到密钥公布后，可以使用该密钥验证先前接收的消息的真实性。

TESLA 协议具有前向安全性，由于密钥链的单向性，当前密钥披露后，并不影响后续密钥的安全。同时，由于每个密钥只在特定时间内有效，重放的旧消息将无法通过鉴别，即具有抗重放攻击能力。由于使用对称密码技术实现消息鉴别，TESLA 协议更高效、节能。

基本的 TESLA 协议由于需要一定程度的时间同步，这在某些网络环境中可能难以实现。接收方需要等待发送方披露密钥后才能验证消息，这导致该协议可能不适用于所有实时应用。这些缺陷限制了 TESLA 协议的应用。

1.2　Inf-TESLA 和增强型 Inf-TESLA

在原始 TESLA 协议中，一旦密钥链使用最后一个密钥，系统就需要重新建立发送者和接收者之间的同步，类似于建立一个新的连接。这种重建同步的过程可能会导致计算需求和能源消耗的增加。为了解决这一问题，Inf-TESLA（infinite timed efficient stream loss-tolerant authentication）协议[8] 引入一种新的机制，即两个错位对齐的并行密钥链。这种设计确保了当一个密钥链用尽时，另一个密钥链仍然能够维持发送者和接收者之间的同步。这两个密钥链可以采用双密钥模式或交替模式运作。

1）双密钥模式：在这种模式下，每个数据包中都包含两个密钥，分别来自两个不同的密钥链。这样即使一个密钥链结束，另一个密钥链仍可用于维持认证过程。

2）交替模式：在交替模式中，两个密钥链的密钥交替出现在数据包中。具体来说，一个密钥链负责奇数时间间隔的密钥，而另一个负责偶数时间间隔的密钥。这种方法不仅提高了密钥使用的灵活性，还增强了系统的安全性。

通过这种并行密钥链的设计，Inf-TESLA 协议有效地解决了原始 TESLA 协议中密钥链结束时重新同步的问题，减少了因重新同步导致的计算和能源开销，同时提高了协议的可靠性和效率。这一改进使得 Inf-TESLA 协议特别适合于长期运行的无线传感器网络和其他需要持续认证的应用场景。

Inf-TESLA 协议的设计者声称可以保证发送者和接收者在网络整个生命周期内的持续同步，然而，文献 [9] 研究发现 Inf-TESLA 协议的持续性仅限于前两个密钥链的长度。换句话说，一旦这两个密钥链到期，发送者应重新与同一接收者建立同步，这会导致能量、内存空间和时间的显著浪费。因此，文献 [9] 提出了增强型 Inf-TESLA 协议，以改进 Inf-TESLA 协议。增强型 Inf-TESLA 协议允许在通信时间窗口内重建新的偏移密钥链，无须终止连接和确定新的同步，从而实现发送者和接收者之间的持续通信和鉴别。增强型 Inf-TESLA 协议保留了 Inf-TESLA 的基本框架，同时引入一些关键的改进。

1）改进的密钥链机制：增强型 Inf-TESLA 协议采用了更高效的密钥链生成和管理机制，以减少密钥更新的开销，并提高密钥的安全性。

2）动态时间同步：该协议引入更灵活的时间同步机制，以适应网络延迟和节点之间的时间偏差，从而提高协议在动态网络环境中的鲁棒性。

3）优化的密钥分发：协议优化了密钥的分发过程，以减少通信开销，并提高密钥分发的安全性和可靠性。

增强型 Inf-TESLA 协议特别适用于需要长期运行、网络条件动态变化的无线广播环境，如无线传感器网络、物联网设备网络等。增强型 Inf-TESLA 协议通过优化密钥链机制和密钥分发过程，提高了协议的效率和安全性，所采用的动态时间同步机制使得协议能够更好地适应网络延迟和时间偏差，更适应于动态网络环境。

增强型 Inf-TESLA 协议由于引入的新特性增加了协议的实现复杂性，尽管有所优化，但因为结构与原始 TESLA 协议类似，时间同步的要求仍然存在，可能在某些环境中难以实现。

1.3　μTESLA 和多级μTESLA 协议

μTESLA（micro timed-efficient stream loss-tolerant authentication）协议[10-11] 是原始 TESLA 协议的一种简化和改进版本，旨在通过向单个接收者发送数据包来提高性能和效率。与原始 TESLA 协议在每个数据包中附加已公开的密钥不同，μTESLA 协议选择在特定时间间隔内单独发送密钥公开信息，且这些信息与广播的数据包是独立的。这种设计显著降低了接收者的计算需求，并减少了由不必要的数据包引起的通信带宽占用。μTESLA 协议的一个限制是它对合法接收者的数量有所限制，这意味着接收者的内存中不会存储完整的单向密钥链。虽然这种方法减少了内存需求，但它也限制了系统的可扩展性。

为了解决这个问题，研究者们提出了多种改进

μTESLA 协议的策略，其中最显著的是多级μTESLA（multilevel micro timed-efficient stream loss-tolerant authentication）协议[12-13]。多级μTESLA 协议的主要优势在于它能够减少发送者和接收者之间的认证时间延迟，这对于需要快速响应的应用场景尤为重要。此外，该协议还降低了拒绝服务（DoS）攻击的风险。在多级μTESLA 协议中，通过使用多个密钥链和分层的认证机制，可以更有效地管理密钥和分发过程，从而提高整体的网络性能和安全性。多级μTESLA 协议生成两级密钥链，其中高级密钥链直接与发送者连接，而低级密钥链负责鉴别发送者和接收者之间传输的数据包。高级密钥链具有较长的时间间隔，覆盖接收者的整个生命周期，从而无须频繁建立新的密钥链，减少了网络的计算复杂性。高级密钥链中的每个时间间隔进一步划分为相应的低级密钥链，其具有显著缩短的时间间隔。这种短时间间隔减少了接收和鉴别数据包所需的时间，从而进一步降低了发生DoS攻击的可能性。

多级μTESLA 协议还引入了一种额外的鉴别消息，称为承诺分发消息（commitment distribution message, CDM），用于发送在高级密钥链的时间间隔中应生成的低级密钥链的承诺密钥。 CDM数据包的构造允许在未来的时间间隔中预先生成低级密钥链的承诺密钥，确保接收者有足够的时间在接收相应数据包之前缓冲和鉴别重要信息。多级μTESLA 协议（以两级为例）基本原理如下。

1）高级密钥链：在协议开始时，发送方选择随机数K_n，并使用单向函数F_0生成密钥链：

$$K_0, K_1, \cdots, K_n$$

式中，$K_i = F_0(K_{i+1})$。$i = 0, 1, \cdots, n-1$。

2）低级密钥链：根据每个高级密钥链生成低级密钥链，过程如下。

（A）使用单向函数F_{01}根据高级密钥K_i依次生成密钥：

$$K_{0,m}, K_{1,m}, \cdots, K_{n-1,m}$$

式中，$K_{i,m} = F_{01}(K_{i+1})$。$i = 0, 1, \cdots, n-1$。

（B）使用单向函数F_1扩展上述密钥得低级密钥链：

$$K_{0,0}, \cdots, K_{0,m}, \cdots, K_{n-1,0}, \cdots, K_{n-1,m}$$

式中，$K_{i,j} = F_1\left(K_{i,j+1}\right)$。$i = 0, 1, \cdots, n-1$；$j = 0, 1, \cdots, m-1$。

3）承诺分发消息 CDM：

$$\mathrm{CDM}_i = i \,\|\, K_{i+2,0} \,\|\, \mathrm{MAC}_{K_i}(i \,\|\, K_{i+2,0}) \,\|\, K_{i-1}$$

式中，CDM_i是发送方在第i时间段广播的承诺分发消息；$K_{i+2,0}$是第$i+2$时间段使用的低级密钥链中的承诺密钥；MAC_{K_i}表示使用密钥K_i生成消息鉴别码，用于保护承诺密钥$K_{i+2,0}$，K_{i-1}为披露的第$i-1$时间段所使用的高级密钥。

需要注意的是，CDM 数据包通常会发送与未来两个时间间隔相关的低级密钥链的承诺密钥，以确保接收者有足够的时间在接收相应数据包之前缓冲和鉴别重要信息。同时，为了避免由 CDM 数据包发送的重要信息的丢失，发送者在第i个时间段内应随机发送几份CDM_i数据包副本，确保接收者能收到数据包。

多级μTESLA 协议通过其创新的多级密钥链设计，提供了一种在大规模和动态无线网络环境中实现高效、安全数据鉴别的解决方案。然而，这种方法在提高安全性和效率的同时，也增加了一定的实现复杂性。

1.4 *TLI*$-\mu$TESLA 协议与混合*TLI*$-\mu$TESLA 协议

两级μTESLA（two-level and inf$-\mu$TESLA, TLI-μTESLA）协议通过结合多级μTESLA 协议和 Inf-TESLA 协议来实现较低的计算开销和连续鉴别。由于 Inf-TESLA 被证明仅限于前两个密钥链长度，研究人员将 TLI-μTESLA 协议中的 Inf-TESLA 协议替换为增强型 Inf-TESLA 协议，提出混合 TLI-μTESLA 协议[14]。

混合 TLI-μTESLA 协议最大化了相关 TESLA 协议变体的优势，支持可扩展性和多级μTESLA 协议的即时鉴别，以及增强 Inf-TESLA 协议的连续鉴别和最小计算开销等。混合 TLI-μTESLA 协议原理如下。

1）高级密钥链：在协议开始时，发送方选择随机数K_n，并使用单向函数F_0生成密钥链：

$$K_0, K_1, \cdots, K_n$$

式中，$K_i = F_0(K_{i+1})$。$i = 0, 1, \cdots, n-1$。

2）低级密钥链：根据每个高级密钥链生成低级密钥链，过程如下。

（A）使用单向函数F_{01}根据高级密钥K_i依次生成密钥：

$$K_{1,m}^1, K_{2,m}^1, \cdots, K_{n,m}^1$$

$$K_{1,m}^2, K_{2,m}^2, \cdots, K_{n,m}^2$$

式中，$K_{i,m}^1 = F_{01}(s_1 \| K_{i+1})$；$K_{i,m}^2 = F_{01}(s_2 \| K_{i+1})$。$i = 0,1,\cdots,n$。$s_1, s_2$为两个不同的盐值，由发送方与接收方预先约定。

（B）使用单向函数F_1扩展上述密钥得低级密钥链：

$$K_{1,0}^1,\cdots,K_{1,m}^1,\cdots,K_{n,0}^1,\cdots,K_{n,m}^1$$

$$K_{1,0}^2,\cdots,K_{2,m}^2,\cdots,K_{n,0}^2,\cdots,K_{n,m}^2$$

式中，$K_{i,j}^k = F_1\left(K_{i,j+1}\right)$。$i = 1,2,\cdots,n$；$j = 0,1,\cdots,m-1$；$k = 1,2$。在第$i$时间段，以增强型 Inf-$\mu$TESLA 协议类似的方式使用上述两条低级密钥链，如对奇数序号消息使用密钥$K_{i,j}^1$，对偶数序号消息使用密钥$K_{i,j}^2$。

3）承诺分发消息 CDM：

$$\mathrm{CDM}_i = i \| K_{i+2,0}^1 \| K_{i+2,0}^2 \| \mathrm{MAC}_{K_i}$$

$$\left(i \| K_{i+2,0}^1 \| K_{i+2,0}^2\right) \| K_{i-1}$$

式中，CDM_i是发送方在第i时间段广播的承诺分发消息；$K_{i+2,0}^1, K_{i+2,0}^2$是第$i+2$时间段使用的两条低级密钥链中的承诺密钥；MAC_{K_i}表示使用密钥K_i生成消息鉴别码，用于保护承诺密钥$K_{i+2,0}^1$与$K_{i+2,0}^2$，K_{i-1}为披露的第$i-1$时间段所使用的高级密钥。

类似地，为了避免由 CDM 数据包发送的重要信息丢失，发送者在第i个时间段内应随机发送几份 CDM_i数据包副本，确保接收者能收到数据包。

混合 TLI-μTESLA 协议可以无缝实现物联网设备的可扩展性，几乎实现即时和连续鉴别，并通过包含 3 种不同的密钥链，同时保持可接受的计算和通信需求水平，增强网络安全性。

混合 TLI-μTESLA 协议综合了现有 TESLA 相关协议的多种优点，然而，该协议仍难以满足具有海量不同类型的接收者的应用场景需求。如智能城市的广泛监控网络，在这样的网络中，不同类型的节点执行不同的功能，一部分节点专注于交通监控，而另一部分则负责环境监测。在这种情况下，特定的数据可能仅对某一类节点有用，如交通数据对于环境监测节点可能无关紧要。面对此类场景，若使用混合 TLI-μTESLA 协议向所有节点广播数据，会导致所有节点都需要处理接收到所有数据，这不仅增加了节点的处理负担，还可能导致网络拥塞和能源浪费。另一方面，如果为每一类节点单独实施一个混合 TLI-μTESLA 协议，虽然能够解决数据过载问题，但这将给发送者带来巨大的存储和管理负担。

为了解决这些问题，本文基于混合 TLI-μTESLA 协议提出了面向多类型节点的混合多级μTESLA 协议。该协议允许发送者根据节点类型进行数据广播，即只有特定类型的节点需要并能够鉴别这些数据的来源。这样，其他类型的节点可以有效地过滤掉与它们不相关的数据，从而减少了无用数据的处理和存储需求。此外，该协议还支持动态调整广播策略，以适应网络中节点类型和功能的变化，进一步提高了网络的灵活性和可扩展性。通过这种方式，面向多类型节点的混合多级μTESLA 协议不仅提高了数据传输的效率和安全性，还降低了网络的整体资源消耗。它特别适用于那些需要处理大量异构数据的复杂网络环境，如智能城市、工业物联网、健康监测系统等。

2　面向多类型节点的混合多级μTESLA 协议

本节具体介绍面向多类型节点的混合多级μTESLA 协议。

设应用场景中有t类节点，每类节点分别具有标识$l_1, l_2, \cdots, l_t$，节点的标识信息与消息发送者共享。具体地，标识可以根据节点功能、位置、分组标签或其他属性等多种因素来定义。面向多类型节点的混合多级μTESLA 协议如图 1 所示，具体原理如下。

1）高级密钥链：在协议开始时，发送方选择随机数K_n，并使用单向函数F_0生成密钥链：

$$K_0, K_1, \cdots, K_n$$

式中，$K_i = F_0(K_{i+1})$。$i = 0,1,\cdots,n-1$。

2）低级密钥链：根据每个高级密钥链生成低级密钥链，过程如下。

（A）使用单向函数F_{01}, F_l根据高级密钥K_i依次生成密钥:

$$K_{1,m_{1,1}}^{1,1}, K_{2,m_{1,2}}^{1,1}, \cdots, K_{n,m_{1,n}}^{1,1}$$

$$K_{1,m_{1,1}}^{1,2}, K_{2,m_{1,2}}^{1,2}, \cdots, K_{n,m_{1,n}}^{1,2}$$

$$\vdots$$

$$K_{1,m_{t,1}}^{t,1}, K_{2,m_{t,2}}^{t,1}, \cdots, K_{n,m_{t,n}}^{t,1}$$

$$K_{1,m_{t,1}}^{t,2}, K_{2,m_{t,2}}^{t,2}, \cdots, K_{n,m_{t,n}}^{t,2}$$

式中，$K_{i,m_{j,i}}^{j,1} = F_{01}\left(F_l\left(1 \| l_j\right) \| K_i\right)$；$K_{i,m_{j,i}}^{j,2} = F_{01}(F_l(2 \| l_j) \| K_i)$。$i = 1,2,\cdots,n$；$j = 1,2,\cdots,t$。

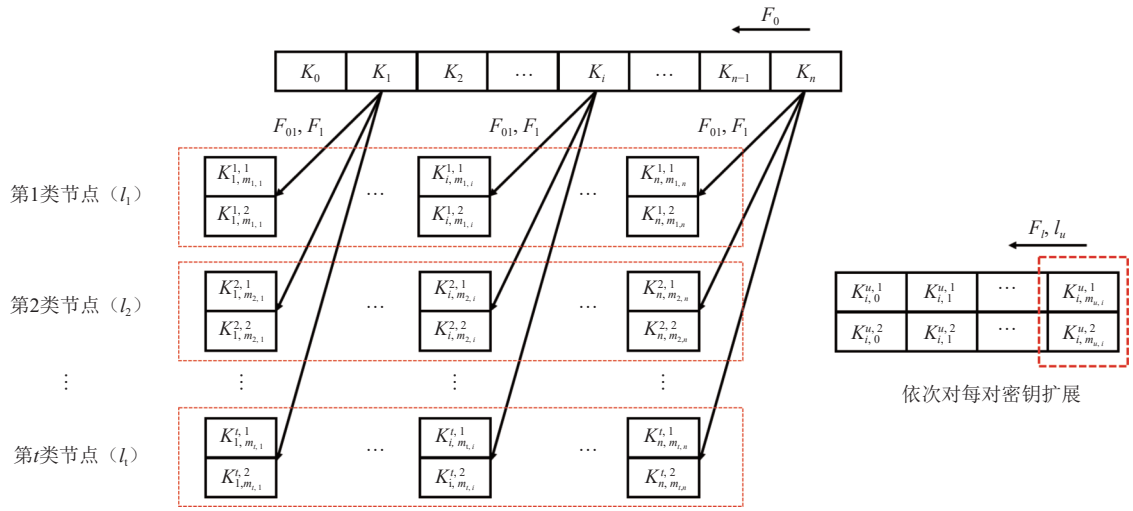

图 1 混合多级μTESLA 协议示意图

（B）使用单向函数 F_1 扩展上述密钥得低级密钥链:

$$K_{1,0}^{1,1},\cdots,K_{1,m_{1,1}}^{1,1},\cdots,K_{n,0}^{1,1},\cdots,K_{n,m_{1,n}}^{1,1}$$

$$K_{1,0}^{1,2},\cdots,K_{2,m_{1,1}}^{1,2},\cdots,K_{n,0}^{1,2},\cdots,K_{n,m_{1,n}}^{1,2}$$

$$\vdots$$

$$K_{1,0}^{t,1},\cdots,K_{1,m_{t,1}}^{t,1},\cdots,K_{n,0}^{t,1},\cdots,K_{n,m_{t,n}}^{t,1}$$

$$K_{1,0}^{t,2},\cdots,K_{2,m_{t,1}}^{t,2},\cdots,K_{n,0}^{t,2},\cdots,K_{n,m_{t,n}}^{t,2}$$

式中，$K_{i,j}^{\mu,k}=F_1\left(l_u \| K_{i,j+1}^{u,k}\right)$。$i=1,2,\cdots,n$；$j=0,1,\cdots,m_{u,i}-1$；$k=1,2$；$u=1,2,\cdots,t$。在第 i 时间段，发给标识为 $l\mu$的节点群的消息使用增强型 Inf-μTESLA 协议类似的方式使用相关的两条低级密钥链，如对奇数序号消息使用密钥$K_{i,j}^{\mu,1}$，对偶数序号消息使用密钥$K_{i,j}^{\mu,2}$。

3）承诺分发消息 CDM：

$$\mathrm{CDM}_i^u=i \| F_l(3 \| l_u) \| K_{i+2,0}^{u,1} \| K_{i+2,0}^{u,2} \| \mathrm{MAC}_{K_i}$$

$$\left(i \| l_u \| K_{i+2,0}^{u,1} \| K_{i+2,0}^{u,2}\right) \| K_{i-1}$$

式中，CDM_i^u是发送方在第i时间段面向标识为l_u的节点群广播的承诺分发消息；$K_{i+2,0}^{u,1}, K_{i+2,0}^{u,2}$是第$i+2$时间段使用的两条低级密钥链中的承诺密钥；$\mathrm{MAC}_{K_i}$表示使用密钥$K_i$生成消息鉴别码，用于保护承诺密钥$K_{i+2,0}^{u,1}$与$K_{i+2,0}^{u,1}$；$K_{i-1}$为披露的第$i-1$时间段所使用的高级密钥；$\mathrm{MAC}_{K_i}$是使用密钥$K_i$生成的MAC值，用于保护承诺密钥 $K_{i+2,0}^{u,1}$与$K_{i+2,0}^{u,2}$。CDM数据中标签l_u的杂凑值字段$F_l(3 \| l_u)$用于节点筛选CDM 数据包，而字段$\mathrm{MAC}_{K_i}\left(i \| l_u \| K_{i+2,0}^{u,1} \| K_{i+2,0}^{u,2}\right)$中使用的是标签$l_u$，用于确保只有拥有标签$l_u$的节点才能鉴别其中的密钥 $K_{i+2,0}^{u,1}, K_{i+2,0}^{u,2}$。

类似地，为了避免由 CDM 数据包发送的重要信息丢失，发送者在第i个时间段内应随机发送几份CDM_i^u数据包副本，确保接收者能收到数据包。

混合多级μTESLA 协议的核心贡献在于其创新性的密钥管理和数据传输策略。该协议是对文献 [14] 提出的混合 TLI-μTESLA 协议的进一步发展，采用了一个统一的高级密钥链，同时通过对低级密钥链进行特定的节点群标识划分，实现了对不同节点群在相同时间段内广播不同消息的能力。这种方法的主要优势如下。

1）目标化广播：协议允许发送者根据接收者的类型或群体进行定制化广播，确保信息的相关性和有效性。

2）高效的信息过滤：每个节点群能够自动过滤掉非目标信息，仅对发送给自己的信息进行处理和鉴别，大大减少了无关数据的处理负担。

3）资源优化：这种方法减少了网络中的数据传输量，从而降低了能源消耗和网络拥塞，特别适用于资源受限的环境。

4）安全性增强：通过使用不同的密钥链对不同的节点群进行加密，协议增强了数据的安全性，使得即使某一密钥被破解，也不会影响到其他节点群的安全。

5）动态适应性：协议支持动态调整密钥链和广播策略，以适应网络中节点群的变化，提高了网络的灵活性和可扩展性。

6）易于管理：通过统一的高级密钥链管理，

简化了密钥分发和更新的过程，降低了管理的复杂性。

7）适用于多种场景：该协议特别适用于需要处理大量异构数据的复杂网络环境，如智能城市、工业物联网、应急响应系统等。

混合多级μTESLA 协议提高了数据传输的效率和安全性，优化了网络的资源使用，更适用于大规模和多类型节点网络中的消息广播鉴别。

3　协议分析

3.1　异常数据处理

在上一节，本文给出了混合多级μTESLA 协议的密钥生成与披露方式。前两组承诺分发消息如下：

$$\mathrm{CDM}_0^u = 0 \,\|\, F_l(3 \,\|\, l_u) \,\|\, K_{2,0}^{u,1} \,\|\, K_{2,0}^{u,2} \,\|$$

$$\mathrm{MAC}_{K_0}\left(0 \,\|\, l_u \,\|\, K_{2,0}^{u,1} \,\|\, K_{2,0}^{u,2}\right) \,\|\, K_{-1}$$

$$\mathrm{CDM}_1^u = 1 \,\|\, F_l(3 \,\|\, l_u) \,\|\, K_{3,0}^{u,1} \,\|\, K_{3,0}^{u,2} \,\|$$

$$\mathrm{MAC}_{K_0}\left(0 \,\|\, l_u \,\|\, K_{3,0}^{u,1} \,\|\, K_{3,0}^{u,2}\right) \,\|\, K_0$$

式中，CDM_0^u中的K_{-1}并不存在，而CDM_1^u中披露的高级密钥K_0为高级密钥的承诺密钥，其为所有节点所共享的密钥，因此，并不需要广播CDM_0^u，而广播的CDM_1^u可修改成：

$$\mathrm{MOD\_CDM}_1^u = 1 \,\|\, F_l(3 \,\|\, l_u) \,\|\, K_{3,0}^{u,1} \,\|\, K_{3,0}^{u,2} \,\|$$

$$\mathrm{MAC}_{K_0}\left(0 \,\|\, l_u \,\|\, K_{3,0}^{u,1} \,\|\, K_{3,0}^{u,2}\right)$$

对于最后两组承诺分发信息：

$$\mathrm{MOD\_CDM}_{n-1} = (n-1) \,\|\, K_{n-2}$$

$$\mathrm{MOD\_CDM}_n = n \,\|\, K_{n-1}$$

由于低级密钥链并不使用 $K_{n+1,0}^{u,1}, K_{n+1,0}^{u,2}, K_{n+2,0}^{u,1}, K_{n+2,0}^{u,2}$，因此可将其修改为：

$$\mathrm{MOD\_CDM}_{n-1} = (n-1) \,\|\, K_{n-2}$$

$$\mathrm{MOD\_CDM}_n = n \,\|\, K_{n-1}$$

分别用于在第$(n-1), n$时间段披露高级密钥K_{n-2}, K_{n-1}，以及在第$(n+1)$时间段使用：

$$\mathrm{MOD\_CDM}_{n+1} = (n+1) \,\|\, K_n$$

披露最后一个高级密钥K_n。

至此，任意一类节点在收到 CDM 数据时，均可通过数据包中的数据字段$F_l(3 \,\|\, l_u)$筛选出发送者发送给这类节点的数据，从中找到密钥$K_{i+2,0}^{u,1}$，$K_{i+2,0}^{u,2}$，并鉴别之前的密钥。

类似地，在使用密钥$K_{i,j}^{u,k}$对发送给具有标识l_u消息数据msg生成鉴别信息P时，可在数据包中附上标签的杂凑值，用于接收节点筛选数据包。优选地，可以采用带关联数据的可鉴别加密方式生成数据包P，以实现对消息数据msg机密性、完整性、真实性保护，同时鉴别数据包中的标签杂凑值等公开传输字段的真实性，具体方法可参考文献 [17]。

3.2　参数选择

本节探讨发送方的计算与存储开销。协议中的单向函数可以使用密码杂凑算法 SM3[18]，其输出的杂凑值长度为 256 bits，消息鉴别算法可以采用基于 SM4 分组密码算法[19] 的消息鉴别工作模式[15] 或可鉴别加密工作模式[16]，输入的密钥长度为 128 bits，MAC 长度不超过 128 bits 不少于 32 bits。

本协议可通过存储关键密钥节点，显著减少了存储需求，同时保持了密钥链的完整性和可访问性； 利用 SM3 算法的高效性，实现了在需求时快速生成密钥的能力，减少了预先计算和存储的负担；低级密钥链的按需生成机制提供了高度的灵活性，适应不同的使用频率和需求，并能够根据不同节点群的需求和时间变化，动态调整密钥生成规模，优化资源使用。

1）高级密钥链的生成与存储优化。发送方需预先生成高级密钥链：

$$K_0, K_1, \cdots, K_n$$

此过程从随机生成的K_n开始，通过连续执行n次杂凑函数得到。鉴于高级密钥链使用的较长时间间隔和 SM3 算法的高效性，采用时间与存储的权衡策略。具体来说，只存储部分密钥，其余在使用时再生成，以减少存储需求。如存储以下密钥：

$$K_0, K_1, K_p, K_{2p}, \cdots, K_{\lfloor n/p \rfloor}, K_n$$

则存储高级密钥的所需存储空间由$128\times(n+1)$bits 降低到约$128\times(\lfloor n/p \rfloor+2)$ bits。在实际使用中，只需在下一个时间段之前，根据存储的中间密钥进行至多p次杂凑运算即可。

2）低级密钥链的灵活生成。低级密钥链使用频率较高，在给定高级密钥K_i后，可快速扩展生成相应的低级密钥链。这些低级密钥链根据需求生成，仅需临时存储。

3）密钥链的动态调整。不同类型的节点群广播的数据量可能有所不同，相应的密钥需求量也会有差异。同一类型的节点在不同时间段所需密钥量也可能不同。本协议设计允许根据不同类型的节点或不同时间段的需求，调整参数$m_{i,j}$的大小，从而在不同时间段根据不同节点需求生成相应规模的密钥数量。

3.3 性能与安全性分析

本协议在接收方节点仅包含单一类型时，其基本运作机制与文献 [14] 中描述的混合 TLI-μTESLA 协议相似。关键的不同之处在于，本协议中 CDM 数据包增加了特定的标签相关字段，这一改进旨在提高消息筛选的效率和精确度。因此，尽管本协议在鲁棒性和抗攻击能力方面与混合混合 TLI-μTESLA 协议相当，但在处理消息的速度和资源消耗方面展现出显著的优势。

在全局广播模式下，尽管广播消息被发送到网络中的所有节点，本协议允许每类接收节点通过分析收到的广播数据包P和 CDM，利用标签杂凑值字段迅速筛选出对其而言重要的信息。这种方法显著提高了接收节点处理消息的速度，同时减少了资源消耗。

在定向广播模式下，特定消息仅被发送给网络中的特定一组节点。在这种情况下，本协议的接收节点所需处理的数据量及资源消耗与文献 [14] 中的方案相似。

无论采用全局广播还是定向广播，广播节点所需广播的消息数据量与文献 [14] 持平。本协议的显著优势在于，通过采用同一高级密钥链为不同类型的节点生成所需的密钥，大幅降低了广播节点所需生成的密钥量。

在涉及多类型节点的复杂网络环境中，本协议通过为每类节点分配不同的杂凑函数来生成低级密钥，不仅保证了不同节点间密钥的独立性，还增强了整个系统的安全性。这意味着，即使某一类型节点的密钥被破解，其他类型节点的安全性不会受到影响。此外，这种方法提高了协议的灵活性和可扩展性，使其能够适应网络环境的变化，如新增节点类型或调整现有节点的功能，而无须重新设计整个协议。

3.4 复杂度分析

本协议基于文献 [14] 进行了扩展和改进，旨在优化大规模多类型节点环境中的消息广播鉴别问题。由于本协议所需广播消息数量与文献 [14] 一致，所需生成的低级密钥数量也相同。

在应用场景中存在t类节点时，本协议所需的高级密钥量保持不变。相比之下，文献 [14] 的方案无论是采用全局广播还是对各类节点进行定向广播，所需的高级密钥量均约为本协议所需高级密钥量的t倍。此外，采用本协议时，每类节点可以快速筛选出所需处理的消息，这大幅降低了接收节点的计算量和能源消耗，从而在大规模多类型节点的网络环境中提供了更高的效率和可扩展性。

4 结束语

本文详细介绍了面向多类型节点的混合多级 μTESLA 协议，这是一种为复杂网络环境设计的高效安全广播鉴别协议。通过对协议的分析和讨论，展示了其在多种应用场景中的适用性和优势。首先，本协议的核心在于其对多类型节点环境的高度适应性。通过为不同类型的节点分配不同的杂凑函数来生成低级密钥，协议不仅确保了密钥的独立性，还增强了整个系统的安全性。这种设计使得即使某一类型节点的密钥被破解，也不会影响到其他类型节点的安全性。其次，本协议在保持与传统混合 TLI-μTESLA协议相似的处理效率和资源消耗的同时，通过引入标签杂凑值字段，进一步优化了数据处理流程。这一改进使得接收方能够更加高效地处理信息，特别是在资源受限的环境中。此外，本协议的设计充分考虑了易用性和灵活性。它支持动态调整密钥生成规模，以适应不同节点群的需求和时间变化，从而为用户提供了更加灵活的密钥管理解决方案。面向多类型节点的混合多级μTESLA 协议不仅提高了在多类型节点环境中的通信安全性，还保持了高效的数据处理能力。这些特点使得本协议更适用于各种复杂网络环境，特别是动态和不确定的网络中。

参 考 文 献

[1] MAHDI M N, AHMAD A R, QASSIM Q S, et al. From 5G to 6G technology: Meets energy, Internet-of-things and machine learning: A survey[J]. Applied Sciences, 2021, 11(17): 8117.

[2] PEREIRA F, CORREIA R, PINHO P, et al. Challenges in resource-constrained IoT devices: Energy and communication as critical success factors for future IoT deployment[J]. Sensors, 2020, 20(22): 6420.

[3] MOHAMAD AL-ABOOSI A M, KAMIL S, SHEIKH ABDULLAH S N H, et al. Lightweight cryptography for resource constraint devices: Challenges and recommendation

[C]//Proceedings of the 3rd International Cyber Resilience Conference. New York: IEEE, 2021: 1-6.

[4] PERRIG A, TYGAR J D. Secure broadcast communication [M]. Boston: Springer, 2003: 29-53.

[5] PERRIG A, SONG D, CANETTI R, et al. RFC4082: Timed efficient stream loss-tolerant authentication (TESLA): Multicast source authentication transform introduction [EB/OL]. [2024-02-02]. https://www.rfc-editor.org/rfc/rfc4082.

[6] GROVER K, LIM A. A survey of broadcast authentication schemes for wireless networks[J]. Ad Hoc Networks, 2015, 24: 288-316.

[7] KRISHNAKUMAR S, SRINIVASAN R. Securing TESLA broadcast protocol with Diffie-Hellman key exchange[J]. International Journal of Computer Engineering and Technology, 2013(4): 152-170.

[8] CÂMARA S, ANAND D, PILLITTERI V, et al. Multicast delayed authentication for streaming synchrophasor data in the smart grid[EB/OL]. [2024-02-02]. https://hal.inria.fr/hal-01369539.

[9] ELEDLEBI K, ALZUBAIDI A A, YEUN C Y, et al. Enhanced inf-TESLA protocol: A continuous connectivity and low overhead authentication protocol via IoT devices[J]. IEEE Access, 2022, 10: 54912-54921.

[10] PERRIG A, SZEWCZYK R, TYGAR J D, et al. SPINS: Security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5): 521-534.

[11] LIU D G, NING P. Multilevel μTESLA: Broadcast authentication for distributed sensor networks[J]. ACM Transactions on Embedded Computing Systems, 2004, 3(4): 800-836.

[12] AL D A, YEUN C Y, DAMIANI E. New two-level μTESLA protocol for IoT environments[C]//Proceedings of the IEEE World Congress on Services. New York: IEEE, 2019: 84-91.

[13] LI X, RUAN N, WU F, et al. Efficient and enhanced broadcast authentication protocols based on multilevel μTESLA[C]//Proceedings of the IEEE 33rd International Performance Computing and Communications Conference. New York: IEEE, 2014: 1-8.

[14] ELEDLEBI K, ALZUBAIDI A A, YEUN C Y, et al. Simulation analysis and comparison of new hybrid TLI-μTESLA and variant TESLA protocols using SHA-2 and SHA-3 hash functions[J]. Sensors, 2022, 22(23): 9063.

[15] GB/T 15852.1-2020 信息技术安全技术消息鉴别码第 1 部分: 采用分组密码的机制[EB/OL]. (2020-12-14)[2024-01-08]. https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=2C2CF7FD11D1AA8C666C0E49A2186CBE.
GB/T 15852.1-2020 Information technology-Security techniques-Message authentication codes-Part 1: Mechanisms using a block cipher[EB/OL]. (2020-12-14) [2024-01-08]. https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=2C2CF7FD11D1AA8C666C0E49A2186CBE.

[16] GB/T 36624-2018 信息技术 安全技术 可鉴别的加密机制 [EB/OL]. (2018-09-17). [2024-01-08]. https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=7DF46F1692B9F774F53E0BEF094379C3.
GB/T 36624-2018 Information technology-security techniques-authenticated encryption[EB/OL]. (2018-09-17) [2024-01-08]. https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=7DF46F1692B9F774F53E0BEF094379C3.

[17] NIST special publication 800-38D recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC[EB/OL]. (2023-08-23) [2024-01-08]. https://csrc.nist.gov/pubs/sp/800/38/d/find.

[18] GB/T 32905-2016 信息安全技术 SM3 密码杂凑算法[EB/OL]. (2016-08-29)[2024-01-08]. https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=45B1A67F20F3BF339211C391E9278F5E.
GB/T 32905-2016 Information security techniques-SM3 cryptographic hash algorithm[EB/OL]. (2016-08-29) [2024-01-08]. https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=45B1A67F20F3BF339211C391E9278F5E.

[19] GB/T 32907-2016 信息安全技术 SM4 分组密码算法 [EB/OL]. (2016-08-29) [2024-01-08]. https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=7803DE42D3BC5E80B0C3E5D8E873D56A.
GB/T 32907-2016 Information security technology-SM4 block cipher algorthm[EB/OL]. (2016-08-29)[2024-01-08]. https://openstd.samr.gov.cn/bzgk/gb/newGbInfo?hcno=7803DE42D3BC5E80B0C3E5D8E873D56A.

编　辑　张　莉