

订阅DeepL Pro以编辑此演示文稿。  
访问[www.DeepL.com/pro](https://www.deepl.com/pro?cta=edit-document)，了解更多信息。

多场景网络中移动设备域控制系统的设计

韩伟业、张玉阳、乔文轩、董萍

电子与信息工程学院， 北京交通大学，中国北京

21120056@bjtu.edu.cn, zhyy@bjtu.edu.cn, 19111033@bjtu.edu.cn, pdong@bjtu.edu.cn

**摘要--随着移动互联网的快速普及，各种应用场景对互联网的要求也逐渐提高。在移动网络下，移动互联网设备会在网络中产生大量的重要信息，这些信息可以用来分析整个网络的链路状态和运行性能。对这些远程设备进行安全有效的管理和控制，将有助于整个网络和技术的优化升级。然而，当前大多数网络架构都存在扩展性差、单点故障等问题。因此，为了对场景复杂的大规模网络设备进行分层按需管理和控制，我们提出了一种基于域的移动设备网络管理和控制系统。该系统根据应用场景将远程移动设备划分为域网络。同时，它可以通过隧道路由技术将不同域网络的远端连接起来，方便管理和控制。为了提高传输效率，提出了一种基于移动车辆的方法。在系统末端，进行了数据自适应调整的传输策略，同时对系统的安全保护和故障预防进行了详细的规划和分析。最终的测试结果表明，该系统可以充分利用网络资源，实现对远程移动设备的基于域的管理和控制。**

关键词--域网络管理；传输策略；移动网络；网络架构

# 导言

在移动互联网中，移动设备作为通信的主体，保留了大量的数据信息，可用于分析网络性能和提供各种服务。在目前流行的车联网中，Wi-Fi、蓝牙、蜂窝等无线通信方式大多用于车与车或车与人之间的数据交互和资源共享。卫星无线通信或移动蜂窝等无线通信技术用于实现与车辆的通信。互联网服务平台上的信息传输。近年来，随着互联网技术和网络服务的快速发展，可扩展、高效、智能的网络控制和管理已成为网络管理的 "必备 "功能。随着应用场景和设备数量的不断增加，设备之间的通信要求和所有设备的统一管理也变得越来越复杂。如何快速、可靠、安全、有效、便捷地管理如此众多的设备成为一个难题。[1].这已成为广大网络系统亟待解决的问题。为此，本文针对多场景、大规模网络中的移动设备提出了一种基于域的管理解决方案。它采用隧道技术，根据场景划分域网络，合理利用网络资源进行调度，并能在服务器出现故障时进行处理。自适应调整网络结构，提高网络的灵活性和可靠性。

本文的贡献可归纳如下。首先，提出了基于域的多场景移动设备管控系统，并对系统模块进行了描述。其次，从网络安全、传输资源分配、服务器故障防灾处理等方面进行了详细分析，并利用基于域的网络架构优势实现了网络资源的高效分配。最后，通过实际系统测试验证了系统的性能。

本文的结构如下。第Ⅱ节讨论网络管理与控制方面的现有相关工作。第Ⅲ节介绍基于域的网络管理与控制系统的体系结构。在第Ⅳ节中，我们详细介绍了该系统中更具特色的关键技术。在第五部分，我们通过实际系统测试证明我们的系统是有效和可靠的。

# 相关工作

在网络架构方面，虽然软件定义网络架构使网络控制和管理更加灵活，但在实际部署中仍存在一定问题。现有的多域系统大多基于 OpenFlow 协议，众所周知，该协议具有很强的协议依赖性，会影响网络的可扩展性。另一方面，多域场景处理还需要网络管理技术的支持，而 SNMP 作为事实上的网络管理协议标准之一，仍然存在很多缺陷。SNMP 依靠简单的轮询策略来获取网络管理信息[2]在大规模网络中，频繁的主动操作会带来严重的性能问题。其自我描述性差、交互性[3]和可扩展性给查询新的网络管理信息和设计分布式网络管理系统带来了困难。[4].

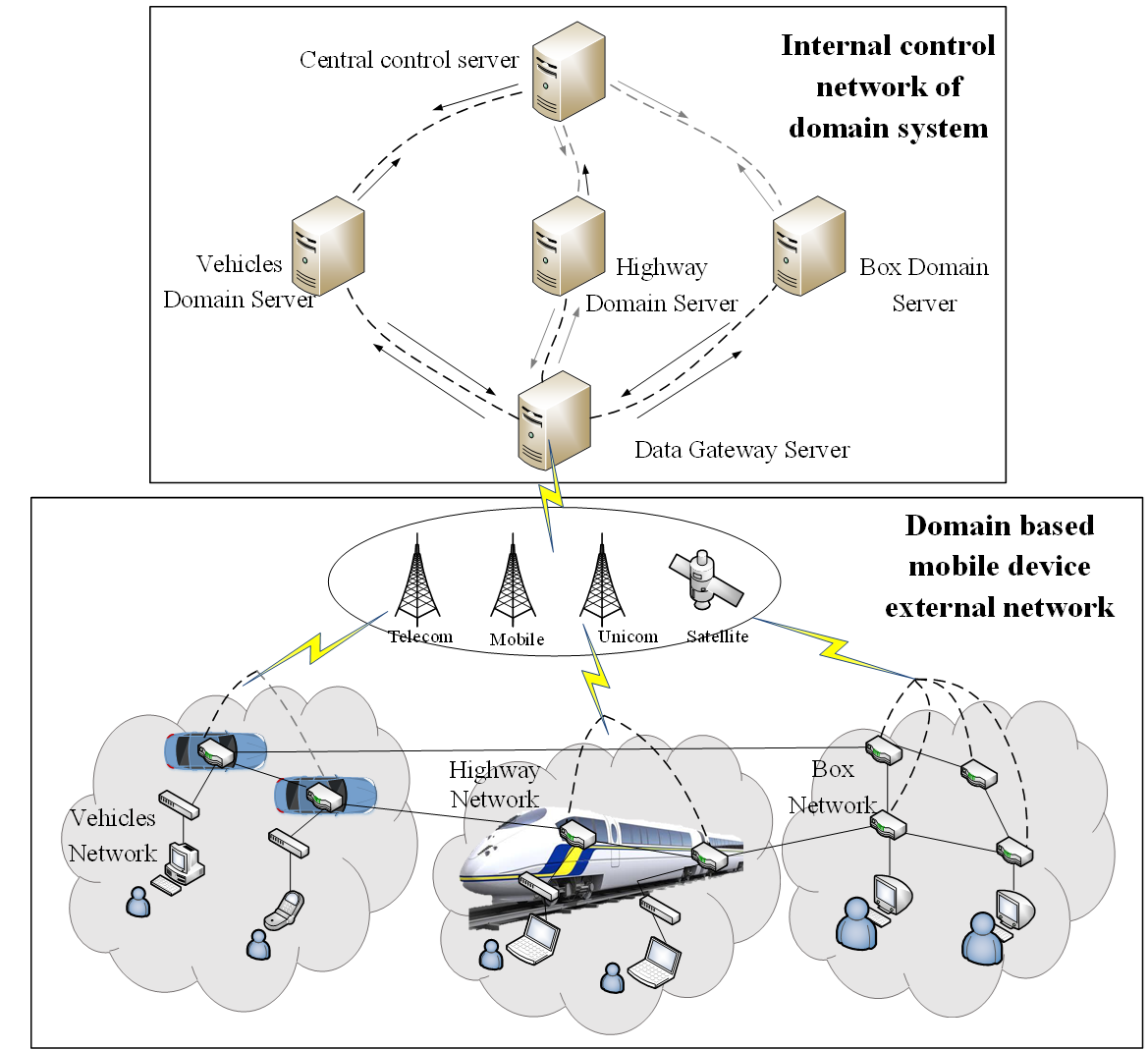
Araniti 等人[5]通过根据流量特征动态选择数据采集节点和采样，在满足数据处理和分析质量的同时，实现了经济地采集网络数据的效果。Chen 等人 [6]通过监测 QoS 参数来执行决策，并通过神经网络识别非法流量，提高了 SDN 的管理能力。在研究应急通信管理系统时 [7]中研究的应急通信管理系统应用于列车时，采用了多代理方案来减少一些网络管理信息流。Chen 等人 [8]分析了传统 SNMP 网络管理模型的不足，探讨了面向对象技术在网络管理中的潜在应用。

上述网络管理技术由于协议设计过于宽泛，不适合多场景移动网络规模扩大后的设备管理。有的针对一些特殊的网络场景或特殊的网络流，难以与不同领域的网络集成。同时，数据传输的安全性也难以保证。因此，本文提出了一个相对完善的基于域的网络管理与控制系统来解决这些问题。

# 引入领域管理和控制系统

本节将介绍多场景下基于域的网络管理与控制系统架构。本文提出了一个完整的高速铁路/定制通信车/便携式箱体域网络管理系统架构。该系统由移动智能网关、数据网关服务器、局域网服务器和中央管理与控制服务器四个实体组成。整个基于域的管理和控制的网络拓扑结构如图 1 所示。

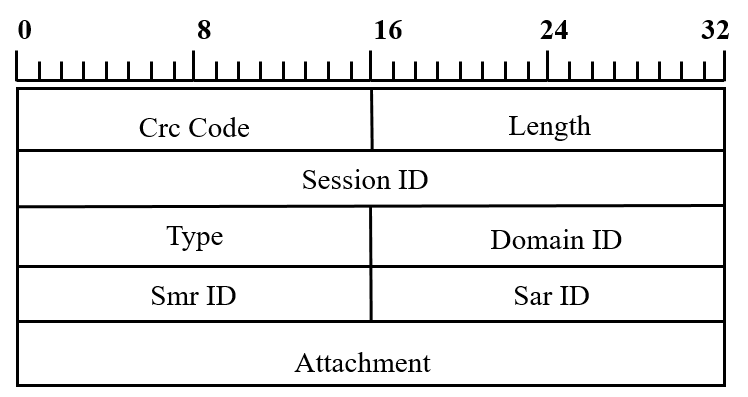
在整个域划分网络架构中，服务于同一场景的移动设备的另一端是本地服务器，属于一种域网络。这里所有域网络的集合就是域划分系统的外部网络。数据网关服务器和中心局服务器一般存放在机房内。远程移动设备和数据网关服务器通过隧道技术进行交互式通信。传输的数据包由数据网关服务器安全处理，然后转发到中央办公服务器进行存储。中心 管理和控制服务器通过分布式接口直观地显示收集到的信息，这些接口是基于域的管理和控制系统的内部网络。整个系统按功能可分为：域管理模块、信息传输模块、安全保护模块和数据存储模块。



1. 领域管理和控制系统的结构

## 网域管理模块

### 数据通信协议



1. 领域管理和控制系统模块划分

在分析现有网络管理协议和网络架构的基础上，采用自创的智能域控制协议（SDCP 协议）来进行网络中各节点之间的通信和交互。SDCP 协议的设计主要包括报文头设计、各报文类型的有效载荷设计、协议通信流程等。报文头设计如图 2 所示。

### 领域互动

通常情况下，远程设备是相互独立的，只需与相应的中心局服务器进行交互。此外，这种机制还能满足特殊情况下的通信需求，主要包括域内通信。实现方式是通过防火墙隔离和增删隧道路由。

### 请求更改域名

域名变更请求是指网络管理员根据各种需要在中央管理和控制可视化平台上执行的操作。域更改操作将从中央管理和控制服务器发送域更改请求，然后通过相应的本地服务器到达数据网关服务器。修改数据网关的域关系映射表即可完成操作。

### 适应性领域变化

自适应域变化用于处理中心局服务器突然故障和崩溃或某个中心局服务器超载的情况。数据网关服务器会向每个中心局服务器发送心跳传感信息。如果本地服务器出现异常，数据网关将触发自适应域变更机制，按照约定的算法对远程设备执行域变更操作，并对网络架构进行自适应调整。本文第四部分将介绍基于域架构下数据传输策略的具体研究。

## 信息传输模块

### 传输调度控制

中央服务器根据信息收集模块过去收集的设备状态信息（包括 CPU、内存使用情况等），评估远程移动设备的传输性能。通过修改配置文件中的相应参数，进行实时任务调度或频率调整。本文第四部分将介绍针对特定领域的传输调度策略的具体研究。同时，系统支持传输策略的定制。用户可以根据实际需要设计定制化的传输策略。

### 数据传输策略

模块根据调度结果实际传输数据。移动设备作为任务传输的发起方，中心局服务器作为任务接收方。整个传输过程是：移动设备在传输之前，首先会到数据网关服务器进行自身信息验证。通过数据网关后，根据设备发送的号码查询相应的中心局服务器号码、IP 地址和程序端口号，然后将数据信息转发给中心局服务器，中心局服务器接收后进行处理和存储。

## 安全保护模块

网络攻击手段层出不穷，包括：黑客恶意攻击、利用漏洞的恶意攻击、DDoS 攻击、欺骗和伪造攻击等。为了应对这些攻击，可以在 IP 层对数据包进行过滤，以阻止攻击，保护受攻击的系统。一方面为了尽可能提高网络系统的安全性，另一方面为了提高数据包过滤匹配算法的匹配效率和数据包的吞吐量，本文提出了一种两层的数据包过滤方法：一层是基于Linux内核的Netfilter，另一层是基于几何空间分割和哈希表的数据包过滤匹配，本文第四部分将介绍这部分的具体研究内容。

## 数据存储模块

### 分布式数据服务部署

位于中央管理控制服务器的可视化模块需要显示的信息需要从各个中心局服务器获取，中心局服务器提供信息接口供其调用。与传统的集中式部署不同，各域网中移动设备的数据信息会传输到与其域网相对应的中心局服务器，中心管理控制服务器会根据需要请求各中心局，即分布式部署应用。分布式部署可以有效解决单点故障问题。当中心服务器节点出现问题或负载过重导致程序无法正常运行时，不会影响其他服务器的正常运行。这样，即使发生故障，也不会对管理和控制网络的整体架构产生重大影响。

# 基于域的数据传输策略

本文设计的域网络管理与控制系统，主要面向带宽上下限较大的卫星无线通信或移动蜂窝应用环境。通过采用一定的数据传输策略，实现负载均衡、网络资源充分利用以及可靠性和安全性。在此前提下，利用基于域的网络架构优势，智能调整分布式存储的部分数据传输频率，自适应调整网络域结构，以应对各种故障突发情况。基于上述内容，本文将受控数据传输的具体实现内容分为以下几个部分：

## 认证机制

远程移动设备记录需要建立连接的中心局服务器地址。不过，在正式与服务器建立连接以传输控制数据之前，移动设备需要在数据网关服务器上验证其身份信息。数据网关通过自己的数据库进行记录。在数据传输前，数据网关会比对身份信息，接受或拒绝连接，完成身份验证机制，通过身份验证后，数据网关会将数据转发给中心局服务器。这种机制一方面便于对后续传输的数据或文件进行定向存储，另一方面也可以避免建立错误或恶意连接对整个网络造成的影响和破坏。

## 安全保护机制

本文提出了一种数据包双层过滤方法。该机制存在于数据网络管理服务器中，可以最大程度地拦截非法数据包。第一层是基于 Linux 服务器内核的 Netfilter 数据包过滤：它主要检查通过智能隧道到达的数据包各部分的长度，如检查数据包的长度和 IPv4 版本号。如果符合隧道规范，就可以放行。这种过滤功能嵌入在 Linux 内核中，因此效率相对较高。

第 2 层过滤主要检查内部协议头和传输的数据是否存在异常。使用的算法有：空间分割和哈希筛选。

规则集由按信息类型维度划分的规则组成。假设每个维度的规则数为 。传入数据包的每个部分需要检测的数据为 。通过哈希筛选获得匹配规则后，进行正则验证处理。

 (1)

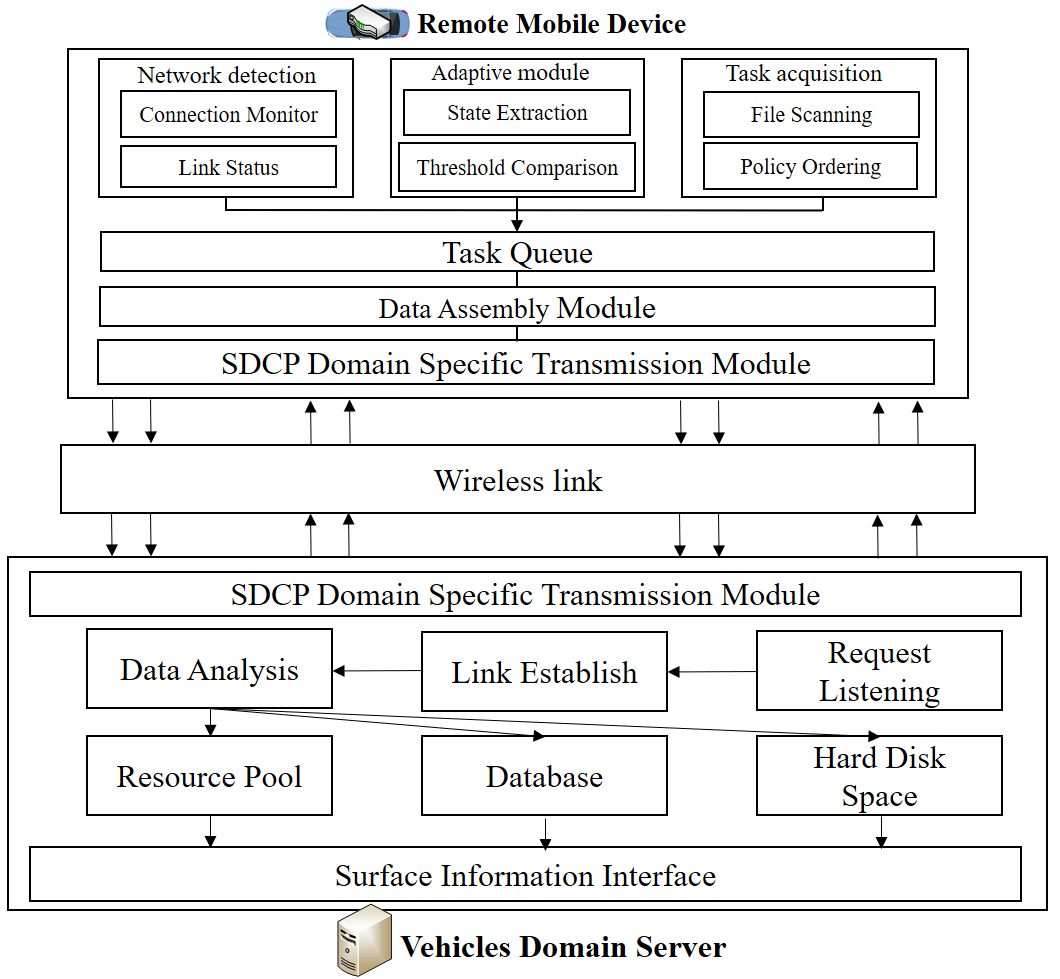
如果数据包是合法的，则下面的公式成立：

 (2)

是标题中附件的数量。如果不满足，则为非法。需要原子记录发送此数据包的 IP 地址，并计算记录数。超过一定阈值后，使用防火墙命令将此 IP 地址列入黑名单。

## 传输适应机制

为了在不影响传输链路主业务使用的前提下，尽可能实现特定网络移动环境下可用于网络性能分析等功能的文件顺畅传输，需要设计并采用特定的策略机制。总体调整策略如图 3 所示：



1. 领域架构下的传输策略

首先，CPU 使用率、内存使用率和网络延迟是大多数负载均衡算法需要引入计算的基本参数，分别用 、 和 表示。首先通过这三个参数确定移动设备 的负载值 ：

 (3)

 它综合考虑了 CPU、内存、网络延迟等常用参数指标，很好地体现了移动设备的负载状况。各指标的权重可根据经验设定为[0.47, 0.38, 0.15]。当移动设备的综合负载值超过设定的阈值时，将触发传输自适应调整，降低发送频率；当综合负载值降低时，将以一定的速率恢复到原来设定的发送频率。

## 自适应域切换机制

在实际网络环境中，服务器故障会引发很多问题。因此，在实际的网络拓扑结构中，必须针对此类问题进行充分的防灾设计。本文提出的基于域的网络架构可以在一定程度上解决这一问题。当服务器出现故障时，设备数据传输会出现故障并造成丢失。

在自适应域变更的设计过程中，需要选出一个新的中心局服务器来替换故障服务器。考虑到整个网络的负载平衡，有必要评估其余中心局的历史流量数据以预测未来。选择负载较轻的中心局作为选举对象。本文使用的算法是时空卷积网络预测算法（TCN）。

TCN 网络是因果网络（从未来到过去没有信息泄露），可以将任何序列映射到相同长度的输出序列。数据网关服务器将在第一阶段记录每个中心局服务器的历史数据包流量。对于某一历史流量输入，希望通过预测未来的输出来确定选择：

 (4)

 是输入数据， 是输出预测数据。每次迭代预测都要计算与真实值的差值，并尽可能减小差值，即损失函数最小化：

 (5)

利用扩张卷积，感受野可以呈指数级增长。对于一维输入序列 和卷积核 ，扩张卷积可表示为

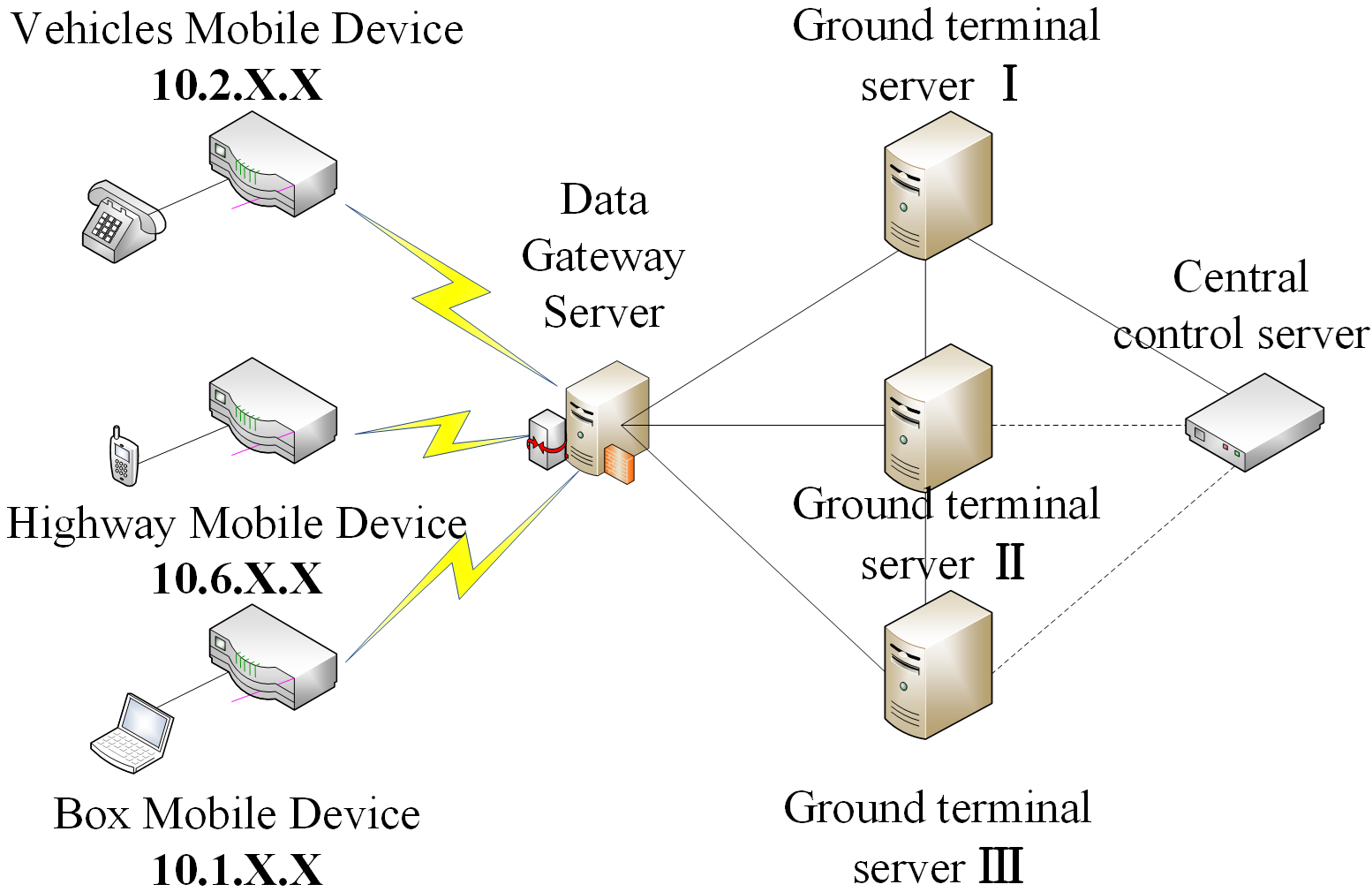
 (6)

远程移动设备向中心局服务器发送的业务数据包会经过数据网关服务器，因此数据网关可以原子式地记录每个中心局的数据包流量数据。当故障中心局的历史数据包流量输入 TCN 网络时，TCN 会通过一系列卷积层和残差连接操作对数据进行处理。每个卷积层对输入数据执行卷积操作和激活函数，并通过向下采样操作降低数据维度。同时，残差连接允许信息在整个网络中传输，以帮助更好地捕捉长期依赖关系。最终，TCN 网络将输出未来时间点数据包流量的预测结果，从而确定业务管理和控制数据包的流动方向。

数据流到中心局服务器后，这部分数据将被标记。故障排除后，将手动迁移数据，完成服务器故障的防灾处理。

# 系统测试

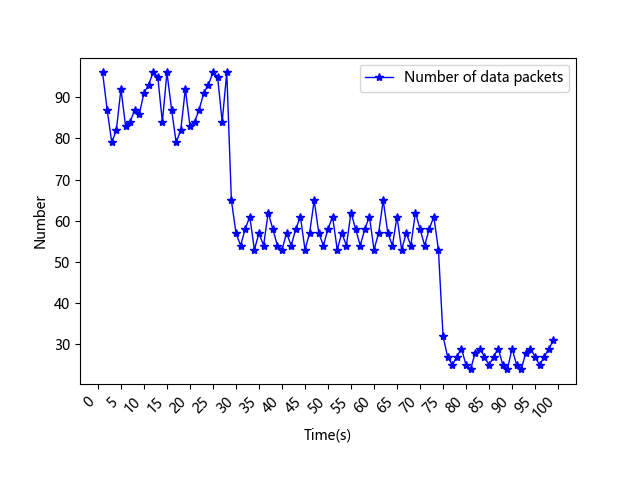
本文主要从安全保护、传输智能调整和自适应域变化三个方面测试和验证了这种域划分网络架构的可行性和有效性。根据实际应用环境和测试需要，构建了如下拓扑结构：外网有三台远程移动设备参与测试，分别属于通信车、高铁和便携箱域网。内网为一台数据网关服务器和三台域本地服务器。以及一台中央管理服务器，场景拓扑如图 4 所示：



1. 系统测试设备拓扑连接

## 安全保护测试：

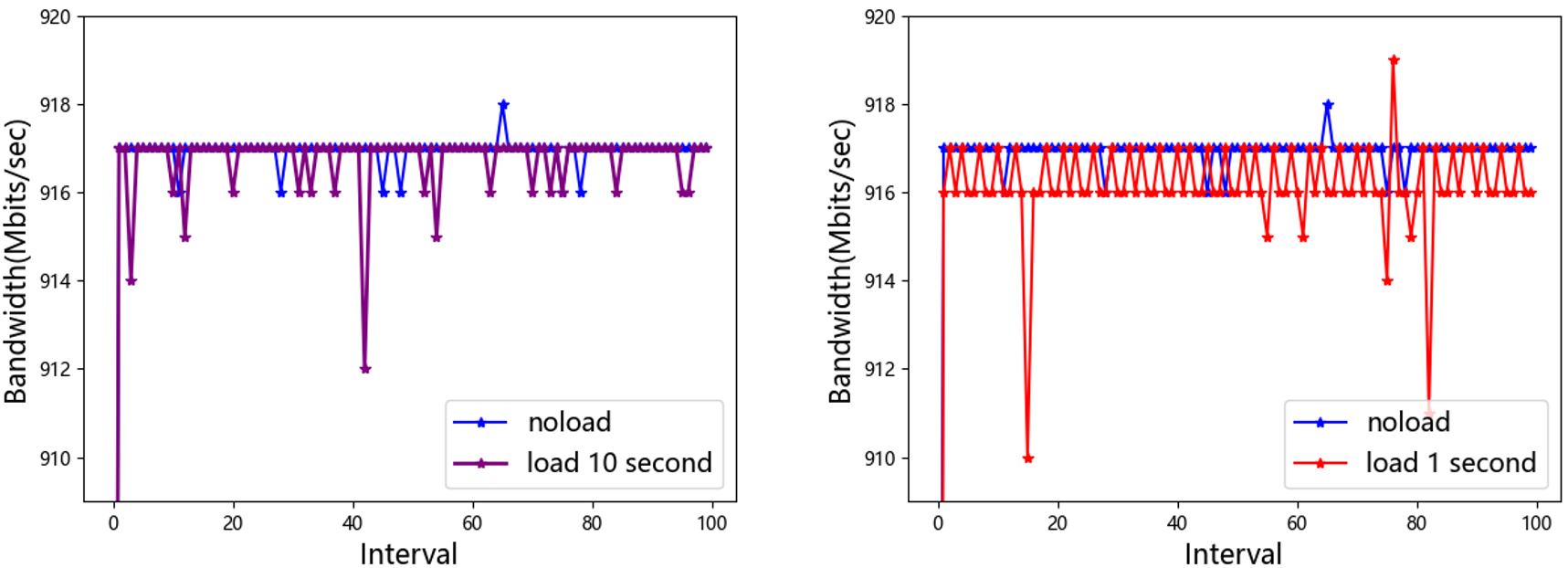
以下是测试结果显示。三台远程移动设备中，1 号正常，2 号随机发送异常数据包，3 号持续发送异常数据包。在数据网络管理部门，可以检测到异常数据包和相应的字段，并原子式地记录数据包流量的数量，便于自适应域变化。下侧为数据包流量记录曲线，结果如下：



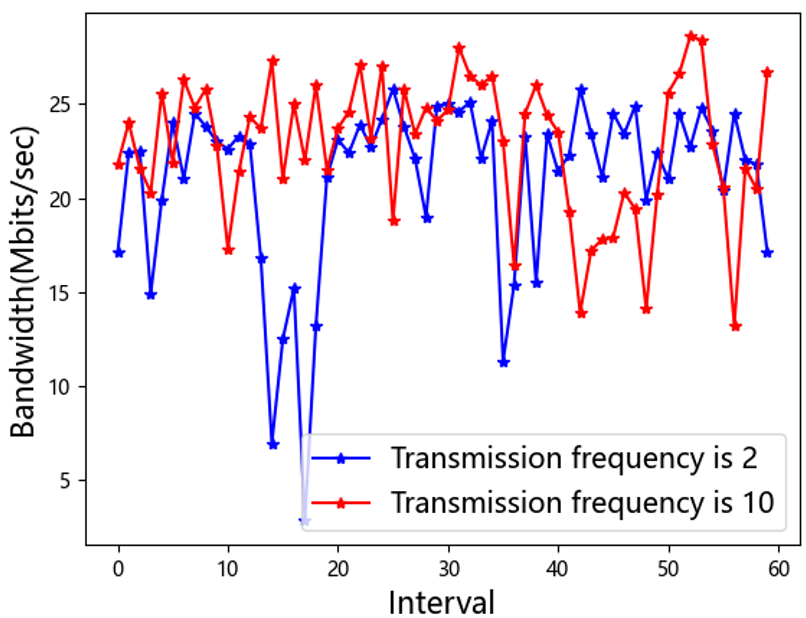
1. 安全保护数据包流量统计

## 智能调整传动测试

当主营业务运行，系统超负荷时，传输业务控制数据的程序不能影响主营业务。因此，需要对传输频率进行智能调整，并在两种情况下进行测试。一是有线链路，二是无线复合链路，对比分析服务器的带宽占用情况。



1. 有线链路下的传输带宽比较

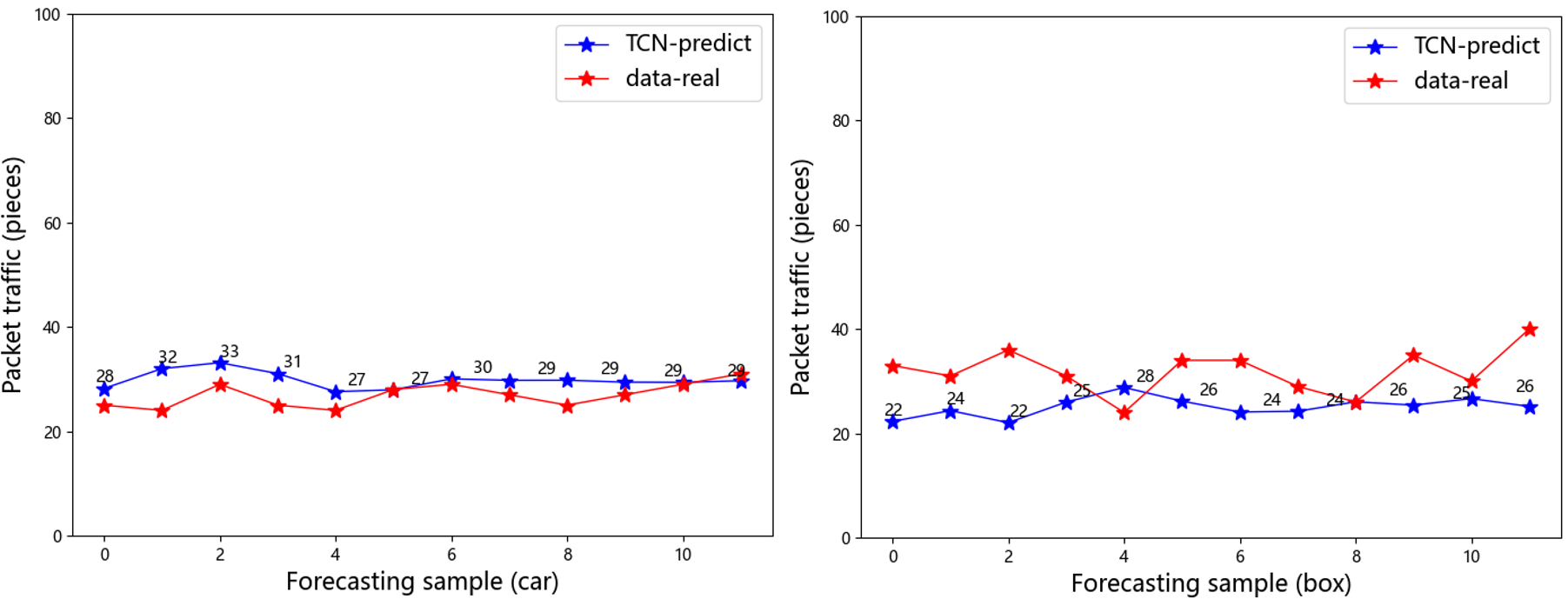


1. 无线链路下的传输带宽比较

由此可以发现，无论是在有线链路还是复杂的无线链路环境中，降低业务管理和控制数据传输的频率，都能在一定程度上提高系统的带宽和稳定性。

## 自适应域变化机制测试

假设高铁中心局服务器出现故障，需要将数据网关中其他中心局的数据包流量记录按 9:1 的比例分为训练数据和测试数据，并利用 TCN 网络对临时中心局进行训练和推荐。最终预测结果如下图所示：



1. TCN 数据预测结果比较

从图中可以看出，通信车中心局的数据包数量预测应该与实际数据比较吻合，数量低于便携箱中的中心局。它是基于负载均衡进行分配的。因此，建议将通信车中心局作为故障服务器。临时终端。

# 结论

大规模网络的发展趋势具有大规模、多域、异构等特点。面对这一发展趋势，新出现的网络需要利用自身的灵活性、开放性等优势，为大规模网络的域网管控提供解决方案。本文提出的多场景移动设备域网管控系统，为较大规模移动网络设备的管理提供了相对完善的域网管控解决方案，包括拓扑规划、安全防护、数据传输。策略和服务器防灾处理等方面，能够在一定程度上提高网络设备管理的便携性、安全性和可靠性，具有较强的现实意义。

##### 认可

本研究部分得到中国博士后科学基金（2021M690343）和中央高校基本科研业务费（2023JBGP005）的资助。

##### 引用

1. Nak-Jung Choi、Ji-In Kim 和 Seok-Joo Koh，"分布式移动性控制的基于域的标识符-定位器映射管理"，2017 年国际信息网络会议（ICOIN），越南岘港，2017 年，第 674-678 页，doi：10.1109/ICOIN.2017.7899579。
2. Q.Q. Ren, B.B. Sun, Y. Liu, Y.H. Guo, H. Jin, "A Circular Structure Based Information Collection Algorithm in Wireless Sensor Networks," Journal of Beijing University of Posts and Telecommunications, vol.39, no.1, pp.58-62, 2016.
3. H.Long, Sh.K. Zhang, Z. Zhang, "A File Scheduling And Data Transmission Algorithm In Vehicular Opportunistic Network," Computer Applications and Software, vol.37, no.4, pp.82-88, 2020.
4. Zh. Zhang, "Design of Reliable File Transmission based on Wireless Communication," Computer Applications and Software, vol. 38, no.Zhang，《基于无线通信的可靠文件传输设计》，《计算机应用与软件》，第 38 卷第 7 期，第 128-131 页，2021 年。
5. G. Araniti, C. Campolo, M. Condoluci, A. Iera, and A. Molinaro, "Lte for vehicular networking: a survey," IEEE communications magazine, vol. 51, no.5, pp.
6. S.Chen, J. Hu, Y. Shi, and L. Zhao, "Lte-v：基于 TD-LTE 的未来车载网络 v2x 解决方案》，《IEEE 物联网期刊》，第 3 卷，第 6 期，第 997-1005 页，2016 年。
7. 青藏铁路应急管理信息系统研究[M]. 2008.
8. 段晨月、赵琴、马艳：《面向对象的 IPV4/IPV6 分布式网络管理模式》，2010 年第三届 IEEE 宽带网络与多媒体技术国际会议（IC-BNMT），北京，2010 年，第 238-242 页，doi：10.1109/ICBNMT.2010.5705087。