



家庭网络多节点安全域建立方法

马智勇

(中国电信股份有限公司上海研究院 上海 200122)

摘要:针对家庭网络覆盖延伸中遇到的多节点组网流程复杂、用户难以自助完成的现状,对节点模块架构、安全域状态转移、节点交互、用户操作流程等提出了优化设计方案,经对比分析,本方案可降低多节点安全域建立的操作次数、操作时间、出错概率,降低服务成本。

关键词:家庭组网;安全网络;安全域

doi: 10.11959/j.issn.1000-0801.2015313

Method of Secure Domain Creation for Multiple Points in Home Networking

Ma Zhiyong

(Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China)

Abstract: To simplify the process of multiple-point connection in home networking, new designs for user operation process, end point structure, state machine, and system process were presented. Analysis shows that the method proposed needs less operations and less time, lowers the faulty probability, and cuts down the service costs as well.

Key words: home networking, secure network, secure domain

1 引言

近年来,全球宽带接入带宽高速增长,各国出巨资加速网络建设步伐。国内 20 Mbit/s 家庭接入带宽已不罕见,部分省市已在推进 100 Mbit/s 甚至 200 Mbit/s 家庭接入产品的部署。越来越高的接入带宽对用户家庭网络覆盖能力提出了新的要求。如何将高宽带接入从入户点无损地延伸到用户家庭的各个角落,防止家庭布线不充分成为宽带业务部署的瓶颈,已经逐步成为提升宽带服务价值的新关注点。

国内民用住宅以砖混结构为主,房型和面积也千差万别,基于传统 AP、无线路由器的单点无线网络覆盖在复杂

的用户环境中,将越来越难以胜任家庭高带宽全覆盖的重任。全以太网布线虽然可以满足需求但也仅适用于房屋初始装修阶段。相比之下,各种自组网辅助组网终端将在家庭网络中成为不可或缺的角色。这类终端组成的网络具有灵活的延展性,每增加一个节点即可实现网络在特定区域的覆盖延伸。位于不同房间的多个节点实现了用户家庭的高带宽全覆盖,如图 1 所示。近年来,国际上多个标准组织正开展家庭多节点辅助组网方面的标准化研究^[1,2]。

安全域(或安全网络),是这类家庭组网终端进行网络划分、确保信息安全的技术手段。不同安全域采用不同的加密密钥以确保数据安全。一个用户家庭中可以由一个或

收稿日期:2015-11-01;修回日期:2015-11-09

论文引用格式:马智勇.家庭网络多节点安全域建立方法.电信科学,2015313

Ma Z Y. Method of secure domain creation for multiple points in home networking. Telecommunications Science, 2015313

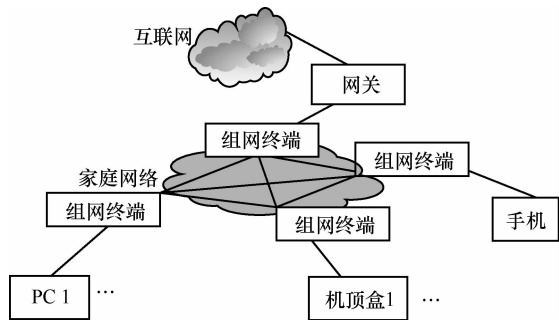


图1 家庭组网终端延伸网络覆盖

多个安全域承载多种业务和服务(如安防、照明、节能、影音娱乐等)。建立安全域是用户延伸网络覆盖无法规避的一个步骤。建立安全域的过程也直接影响着网络延伸的易用性和宽带服务的用户体验。事实上,该过程也确实遇到了多节点组网用户操作方面的问题。

本文对家庭组网产品安全域建立方法进行研究,重点针对多个节点组建安全域以及基于现有安全域构建新安全域的场景,尝试提出优化的安全域建立方法,并分析了新方法的操作效率、出错概率、服务成本、用户体验方面的优势。最后,对本文方法的应用进行了展望。

2 现有方法的问题

假设有两个组网节点(节点1、节点2)需要建立一个安全域,目前业界普遍采用的家庭多节点组网安全域架构中,所要进行的操作如下。

(1) 用户触发节点1的组网按键

- 若此前节点1没加入安全域,则寻找是否有表示“等待新节点注册”的消息。
- 若此前节点1加入了安全域,则发送“等待新节点注册”的消息,该消息中携带域名信息。

(2) 在规定的窗口内,用户触发节点2的组网按键

- 若此前节点1、2都没有加入安全域,则时间窗关闭后,节点1与节点2会随机生成新域名,建立新的安全域。
- 若此前节点1已加入了某个安全域,则节点2加入节点1所在的安全域中(此操作与先后顺序有关)。

以上方案的特点是:一次操作1对节点,逐步扩大节点数量,直至建立起多节点网络。其流程简单、容易理解也易于实现,但如果站在用户的角度会发现结果并不理想。根据上述操作流程,2个节点实现安全域组网,需要用户

在规定的窗口内通过2次操作分别触发两个组网节点; N 个节点组网时,需要用户进行 $2 \times (N-1)$ 次操作。若用户因为购买了多个新设备或者进行家庭网络的调整也经常会遇到在原安全域基础上建立新安全域的情况。例如,已有安全域1和安全域2两个安全域,其中安全域1包含 M 个节点,安全域2包含 N 个节点。当用户希望在这两个安全域基础上建立一个新的安全域时,按照现有方法,则需要至少 $2 \times (\min(M, N) - 1)$ 次操作。

上述操作需要次数繁多的按键触发,而且对时间窗口和操作的先后次序也有要求,这对于普通用户来说既繁琐又容易出错。特别是,如果用户家里的多个组网节点位于不同房间甚至内置在家用电器(如空调、冰箱、电视、吸顶灯等)中时,为了完成多节点组网,用户将不得不在各个房间里多次往返,这对于用户来说会变得难以理解和操作,并且几乎是无法完成的。向服务商投诉和寻求帮助将成为多数用户的唯一选择。

3 用户操作优化

为优化用户体验,本文针对多节点建立安全域从如下两方面着手。

(1) 通过智能设备显示屏将组网操作图形化

伴随着用户终端设备智能化水平不断提高,越来越多带屏的智能终端(如手机、平板电脑、智能电视等)接入家庭网络。这类终端可以提供图形界面,可方便地安装、运行各种应用软件。利用这些带屏智能终端支持包括网络设备查询、呈现节点清单,允许用户在清单中选择准入节点等功能。

例如,如图2、图3所示,智能电视机可内置组网模块或通过外接的辅助组网节点(即代理节点)连接到家庭网络中。用户通过智能电视屏幕选择组网配置功能,触发网络节点的查询,用户勾选后,将若干个新节点加入安全域网络中。

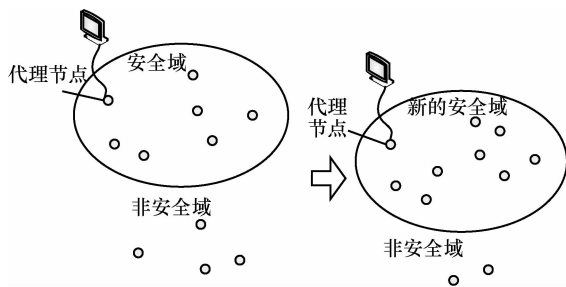


图2 带屏智能节点参与的安全域组网示例



图3 带屏智能节点呈现的组网节点清单与用户勾选示例

(2)基于现有安全域精简地建立新安全域

假设有两个不同的安全域，安全域1有 M 个节点，安全域2有 N 个节点，为了建立一个包含这 $M+N$ 个节点新的安全域，本文定义新的用户操作过程为：用户触发域1中节点1的组网按键；在规定的窗口内，用户触发域2中节点2的组网按键；两个域中的所有节点共同组建一个新的安全域，如图4所示。也就是说，用户仅需在特定的时间窗口内，先后触发两个域中各一个节点的组网按键，即可建立一个包含两个安全域所有节点的新安全域。

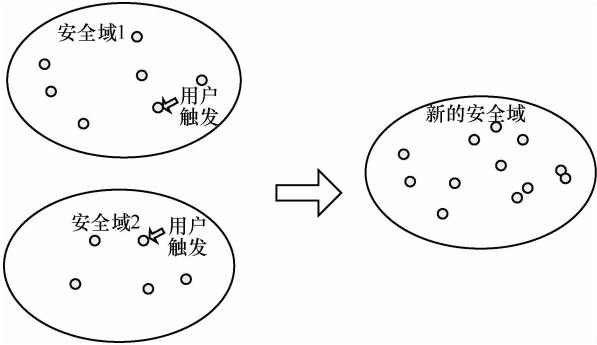


图4 基于两个既有安全域建立新的安全域

4 安全域子系统组成

为支持第3节描述的用户操作流程优化，辅助组网节点的域管理模块除控制节点状态转移外，还应具备代理管理功能，可以接收来自所连接的带屏智能终端的“节点查询”指令，搜索网络中的节点连接信息（含所在安全域内、安全域外的节点）。节点的“域管理侦听”模块能够区分并侦听加密通道和非加密通道侦听的域管理指令。节点架构如图5所示，图5中实线表示加密通道，虚线表示非加密通道。

节点通过非加密通道完成与外来域的域配置协商。当完成域配置协商后，节点通过加密通道向所在安全域中其他节点发送域配置更新指令。而安全域中的其他节点则在加密通道侦听所在安全域中节点的域配置更新指令，共同完成当前域的域配置更新。

域管理节点在收到“节点查询”指令时应在非加密通道广播“等待新节点注册”的指令。新节点加电后进入 ID0 状态。用户触发组网按键后，节点应开启时间窗口，在该时间窗口内，节点寻找是否有“等待新节点注册”的指令消息。如果接收到该指令且该消息中携带域名信息，则节点应启动准入流程^[1]。如果接收到该指令，但消息中未携带域名信息，则节点在非加密通道向域管理节点进行注册。根据管理节点的授权结果决定是否进入准入流程。完成准入流程后，新节点域名修改为所加入的域名，该节点进入 S0 状态。

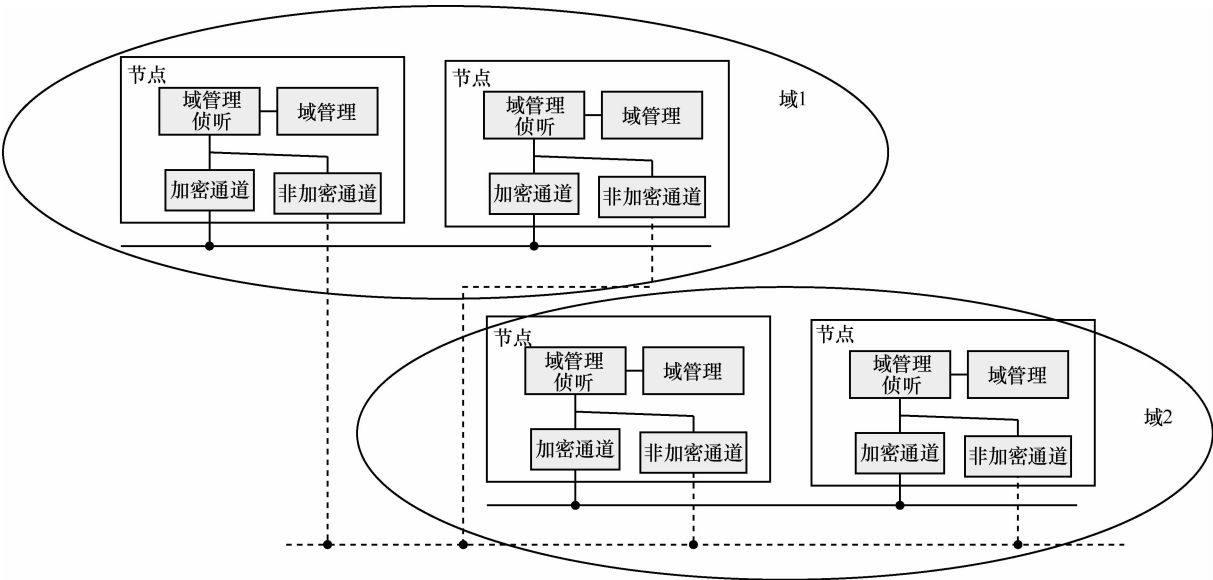


图5 安全域接入技术方案系统结构



5 节点交互优化

多节点安全域建立过程中如有带屏智能节点参与,可利用其图形界面,由用户启动安全域建立流程。与现有方法(参照第2节)不同之处在于,带屏设备连接的组网节点此时充当组网代理节点,向域管理节点发送“新节点查询”指令,而域管理节点在时间窗内等待所有新节点注册但不准入,只有用户通过带屏设备完成节点勾选后才允许相关节点接入安全域。被授权的新节点成功接入安全网络,节点更新为S0状态。详细过程不再赘述。以下着重讨论现有安全域基础上建立新安全域的场景下的节点交互。

5.1 节点状态转移

在基于已有的两个安全域建立新安全域的场景下,为简化用户操作,用户仅需要在特定的时间窗口内,先后触发两个域中各一个节点的组网按键,即可建立一个包含两个安全域中所有节点的新安全域,如图4所示。为达到在用户层面简化操作的目的,本文为组网节点定义了新的状态机。如第4节所述,已经加入安全域的节点处于S0状态。该节点的“域管理侦听”模块侦听并处理来自所在安全域中节点的“域配置更新”指令。用户触发安全域中的某个节点时,该节点通过3个状态转移(S0、S1、S2),完成新安全域的建立和域配置更新,其中:

- S0为节点的初始状态,节点在加密通道侦听网络中的安全域管理指令;
- S1状态,节点在非加密通道侦听并处理网络中的安全域管理指令;
- S2状态,节点在加密通道与所在安全域中节点交互安全域管理指令。

本文定义的节点状态机的状态转移过程如图6所示。用户通过触发节点的组网按键发出的域建立指令,将触发节点从S0到S1状态转移;S1状态下,节点将开启时间窗,在非加密通道内等待来自其他域的指令和配置协商;若时间窗超时,S1状态节点则回退到S0状态;在S1状态下,当节点与其他域完成配置协商后,将触发节点状态从S1状态转移到S2状态;在S2状态下,节点在加密通道上与当前安全域中的管理节点交互,进行当前域配置的更新;节点在S2状态下完成当前域配置更新后,将触发节点状态从S2状态转移到S0状态。

5.2 节点的交互流程

在基于已有的两个安全域建立新安全域的场景下,本

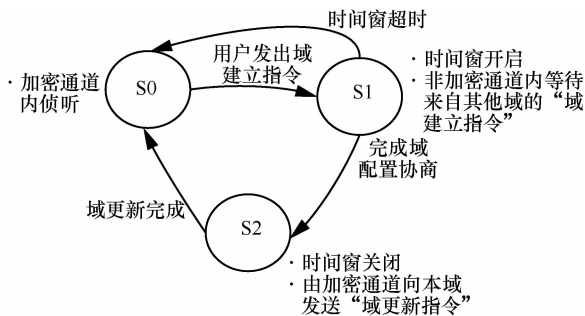


图6 基于既有安全域建立新安全域的状态转移

文设计的节点之间的交互流程如图7所示。假设有两个已有安全域(域1和域2),每个域中有多个节点,但为了简化说明的过程,图7中每个域只涉及了两个节点。

(1)用户向域1节点1发出域建立指令(通常是一次触发组网按键的操作),该节点向网络中发布域配置广播,并开启时间窗口,等待接收域配置反馈。

(2)同样的,用户向域2节点1发出域建立指令,该节点向网络中发布域配置广播,并开启时间窗口。

(3)域1节点1收到域2节点1的域配置广播信息后,向其发送域配置协商指令。

(4)域2节点1向域1节点1发域配置协商确认。

(5)域1节点1与域2节点1交互域配置信息,进行新安全域的参数协商,包括域名和加密信息等。

(6)域1节点1与域2节点1完成新域配置确认。

(7)域1节点1和域2节点1分别在各自域中发送域配置更新指令,该指令由各自的域管理节点处理,根据节点1发来的配置信息,进行本域域名、加密等配置的更新。

(8)域1和域2中的所有节点根据各自域管理节点的指令进行域配置的更新,并加入新安全域中。新的安全域中包含原来两个域中的所有组网节点。

6 优势分析与总结

辅助组网终端的多节点组网是延伸家庭网络覆盖的有效手段。本文通过允许带屏设备清单勾选和现有安全域精简操作建立新安全域两个方面来优化安全域操作。为了比较分析,不妨假设用户将2个节点组建成1个安全域所需要的时间平均为 t_0 ,用户可以成功完成本次操作的概率为 P ,并进一步假设多次操作之间彼此独立。

若有 N 个节点需建立安全域,则根据现有安全域建立方法(参加第2节),需要触发组网按键 $2 \times (N-1)$ 次,耗时 $t_0 \times (N-1)$,成功完成的概率为 P^{N-1} 。而使用本文带屏勾选终

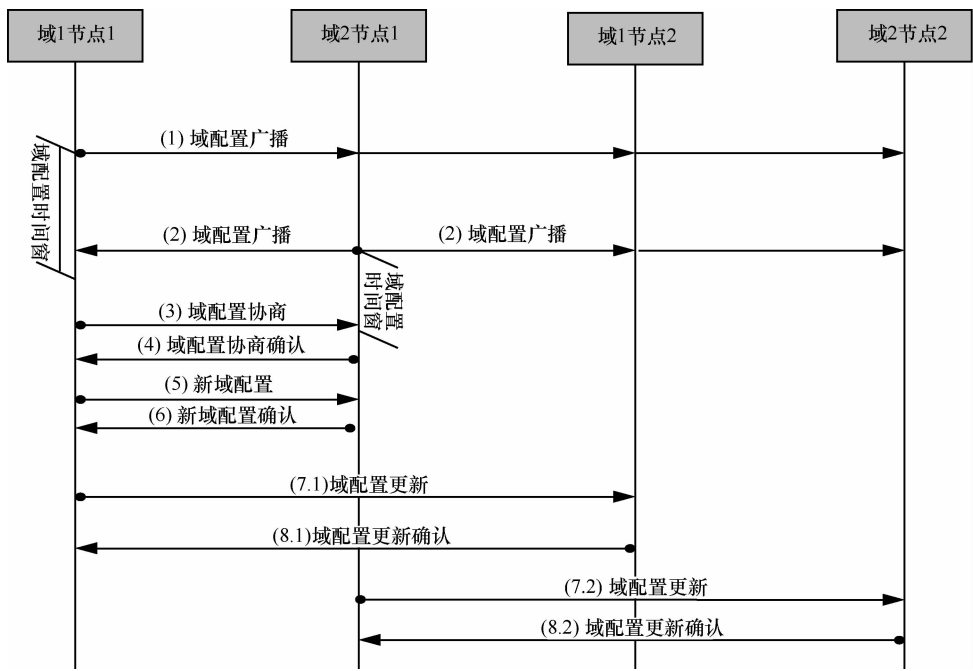


图 7 基于既有安全域建立新安全域节点交互流程

表 1 原方案与本文方案对比

方案	N 节点组建安全域			现有安全域组建新安全域 (M+N 个节点)		
	操作次数	耗时	成功概率	操作次数	耗时	成功概率
原方案	$2 \times (N-1)$	$t_0 \times (N-1)$	P^{N-1}	$2 \times (\min(M,N)-1)$	$t_0 \times (\min(M,N)-1)$	$P^{\min(M,N)-1}$
本文方案	N	t_0	P	2	t_0	P

端的方案需要触发组网按键 N 次,耗时 t_0 ,用户成功完成的概率为 P 。

若用户希望在两个已有安全域基础上建立一个新的安全域,其中安全域 1 包含 M 个节点,安全域 2 包含 N 个节点。根据现有安全域建立方法,则需要触发组网按键 $2 \times (\min(M,N)-1)$ 次,耗时 $t_0 \times (\min(M,N)-1)$,用户成功完成的概率为 $P^{\min(M,N)-1}$ 。而使用本文第 3.2 节的方案需要用户触发组网按键 2 次,耗时 t_0 ,用户成功完成的概率为 P 。

与原有方法相比,本文方法减少了用户操作次数和操作时间,降低了安全域操作的复杂度,见表 1。特别是,当用户家里存在多个组网节点(位于不同房间,内置于空调、电视、吸顶灯等家用电器)时,可以允许用户通过简单的操作完成组网,避免了用户在各个房间多次往返的困扰,从而提升了用户体验。此外通过表 1 中成功完成概率的比较,不难发现,本文方案提升了用户成功完成的概率,也相应降低了用户向运营商寻求帮助的概率,从而可以降低运营商的服务成本。

家庭辅助组网网络的建立与优化是国际标准组织近年关注的一个议题,本文的方法也将提交到相关标准组织作为起草新国际标准时的参考。

参考文献

1 ITU-T G.9961. Unified High-Speed Wire-Line Based Home Networking Transceivers-Data Link Layer Specification, 2015

2 IEEE P1905.1a. IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies Amendment 1: Support of New MAC/PHYs and Enhancements, 2014

[作者简介]



马智勇,男,中国电信股份有限公司上海研究院高级工程师,主要研究方向为家庭宽带网络、业务与接入终端、互联与组网技术,参与 ITU-T、Broadband Forum 国际标准化工作,在 ITU-T 担任标准编辑人。