WSN和计算机网的融合模型研究

吴作顺
(中国电子系统工程研究所 北京 100141)

摘 要 针对无线传感器网与计算机网融合的基础性结构问题,在综合分析无线传感器网络和计算机网络特点的基础上,提出了互联网络、隧道网络和异构网络3种融合网络结构模型,深入研究了异构网络结构模型中采用模糊逻辑的节点移动性管理技术,并重点讨论了异构网络融合的路由模型与协议框架,最后对基于异构网络融合模型的关键技术研究进行了实验分析。

关键词 异构网络融合,网络结构模型,移动性管理,路由协议模型
中图法分类号 TP371 **文献标识码** A

Network Model for Convergence of WSN and Computer Network

WU Zuo-shun
(Institute of China Electronic System Engineering, Beijing 100141, China)

Abstract As the basic architecture for convergence of WSN and computer network, Interconnected model, Tunneled model and Heterogeneous model were presented and compared with analysis of WSN and computer networks. Node mobility management based fuzzy-logic in heterogeneous network model was specially focused. Routing model and protocol frame were also detailed for Heterogeneous integrated network of WSN and Computer network. Key technologies based on heterogeneous network model were examined in the end.

Keywords Heterogeneous integrated network, Network architecture model, Mobility management, Route protocol model

异构网络融合是将多种类型的网络融合起来,在一个通用的网络平台上提供多种业务,是未来网络技术发展的必然趋势。为了充分利用不同网络技术的优点来满足移动用户对QoS的需求,出现了很多异构网络的融合方案,如3GPP制定了3G/UMTS-WLAN融合计划书,并提供了一个有弹性的双网融合方案[1]。不同技术的网络在服务类型、网络条件等方面存在较大差异,异构网络融合面临的主要挑战是如何提供通用的、无缝的网络结构基础模型。

大型化、综合化、扁平化的计算机网和小型化、多样化、移动化的无线传感器网(WSN)代表未来通信网络发展的两大主流方向,其融合是异构网络融合的典型模式。应进行如下工作:通过异构网络的相互协作和对资源的有效管理及合理分配,有效地提高网络吞吐量,降低无线传感设备的能量消耗,减少异构网络间切换的延迟;扩大网络的覆盖范围,使得网络具有更强的可扩展性;向不同用户提供各种不同服务,更好地满足未来网络用户多样性的需求;有效提高网络的可靠性等。异构网络的融合面临着高延迟、高消耗、低速率等诸多方面的"瓶颈",面临一系列新的基础性问题,如网络基础架构、信任控制和行为监测控制等。本文着重对无线传感器网与计算机网融合的结构模型进行研究。

1 相关工作

国内很多大学和研究机构,如中科院传感器技术国家重点实验室、清华大学计算机与科学系等已相继开展了无线传感器网络和异构网络融合的相关研究[2,3]。但相关研究成果尚未达到完全实用阶段,大部分工作仍处在仿真和实验阶段。

异构融合网络结构的研究主要集中在无线传感器网络路由协议[4,5]。虽然出现了一系列特定应用模式下的改进型路由协议,但仍存在不足之处,无法用作异构网络融合的基础网络结构模型。如TinyOS信标协议容易受到伪造路由信息、选择性转发、Sinkhole、Sybil、Wormholes、Flood攻击;Flood协议存在着消息的"内爆"(implosion)和"重叠"(overlap)等固有缺陷,在网络规模扩大时,端到端的传输延时偏大;SPIN是以数据为中心的自适应路由协议,通过协商机制来解决Flood算法中的"内爆"和"重叠"问题,但SPIN协议的扩展性差,功耗在所有节点之间分布不均衡;LEACH协议是为无线传感器网络设计的低能耗自适应簇类路由算法,但该协议容易受到选择性转发攻击和Flood攻击;定向扩散协议逐级扩散路由请求,最终遍历全网,该协议存在容易受到伪造路由信息、Flood攻击等缺点;GEAR&GPSR是基于位置的路由协议,节点依据源和目的位置来选择路径,两个协议需要在节点间交换能量和位置信息,因此容易受到选择性转发和Sybil攻击。

本文研究面向无线传感器网和计算机网融合的网络结构模型,目的是在使可信传感器网络在保障传感器节点信息可用性的同时,融合计算机网实现网络拓扑的广域拓展和快速

到稿日期:2009-03-17 返修日期:2009-05-25 本文受国家863项目(2009AA01Z204),国家973项目(2007CB310800)资助。
吴作顺(1974-),男,博士后,高级工程师,主要研究方向为通信网络与信息安全等,E-mail:wuzuoshun@163.com。

收敛，并能保障关键服务的高效存活性，以及网络系统的可信性和鲁棒性等，重点突破路由控制、资源管理、信任控制和行为监控技术，形成核心关键技术研究的闭环，为无线传感器异构网络的广域拓展、随遇接入、业务敏捷等提供关键技术支持。

2 无线传感器网和计算机网融合的网络模型

无线传感器网络综合了传感器技术、嵌入式计算机技术、分布式信息处理技术和无线通信技术，能够协作地实时监测、感知和采集网络分布区域内的各种环境或监测对象的信息，并对这些数据进行处理，获得详尽而准确的信息，将其传送到需要这些信息的用户。它由部署在监测区域内大量的传感器节点组成，通过无线通信方式形成一个多跳的、自组织的网络系统。无线传感器网络可以在高度移动的环境中通过优化路由和资源管理策略使带宽利用率最大化，同时为用户提供一定的服务质量保证。另外，其通信比较隐蔽，避免了长距离的无线通信易受外界噪声干扰的影响，因此具有巨大的应用价值，已经引起了很多国家的工业、军事等部门的极大关注。

计算机网络是指通过传输介质将地理位置不同的多台计算机互联起来，实现资源共享和信息传输的信息系统。其典型代表是 Internet，它采用开放式标准化 TCP/IP 协议将全球范围的计算机连接起来，得到了广泛的应用。在研究无线传感器网络和计算机网络融合互联模型时，需要综合考虑无线传感器网络和计算机网络的特点，提出能够适应多种网络信道、多种网络应用和多种组网方式的基础网络结构模型。

2.1 互联融合模型

无线传感器网和计算机网互联融合，可以有多种融合方式，如图 1 所示。图中模型(a)、(b)和(c)分别是互联网络(Interconnected Networks)、隧道网络(Tunneled Networks)和异构网络(Heterogeneous Networks)模型。

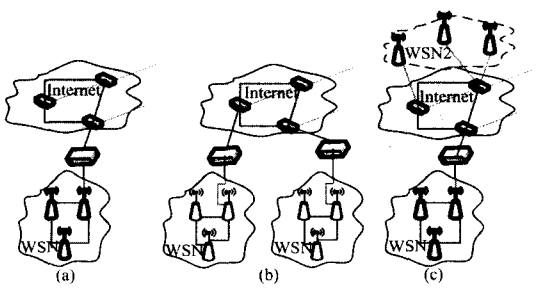

图 1 无线传感器网和计算机网的互联融合模型

在互联网络模型中，无线传感器网络和计算机网络是分离的、对等的和互联的，两个网络在物理结构上独立，仅通过网关互联，传送传感数据。从计算机网络的角度来看，无线传感器网络可视为其连接的另一个局域网。

在隧道网络模型中，无线传感器网通过计算机网互通数据，计算机网构建隧道网络，为无线传感器网提供传输通信链路。两个网络的融合更进一层，但各自仍然维持网络层以下的独立完整性。

异构网络模型是 3 种模型中最紧密的融合形式，无线传感器节点就近接入计算机网，在计算机网上构建虚拟的 Overlay 网，和无线传感器网络的其他子网共同组成一个完整的网络。无线传感器网可以更大程度地共享计算机网络 IP 层以上部分及公共核心网。异构网络模型是目前异构网络体系结构研究的主要模型，也是本文的重点研究对象。

2.2 无线传感器节点的移动性管理

在异构融合网络中，用户接入将有更多的选择。在处于多个网络同时可以接入的场景中，对于一个多模终端用户来说，在综合考虑用户业务要求、网络资源的有效利用等各种因素的条件下，如何自动选择、切换到一个更适合的网络服务，是异构网络移动性管理中一项重要的研究内容，也是异构网融合的关键特征和核心技术。

网络层移动性管理包括域间移动性管理和域内移动性管理[6]。前者习惯上亦称为宏移动(Macro-mobility)管理，指移动节点在不同域之间移动时的管理；后者习惯上称为微移动(Micro-mobility)管理，指移动节点在一个域内移动时的管理。宏移动和微移动如图 2 所示。

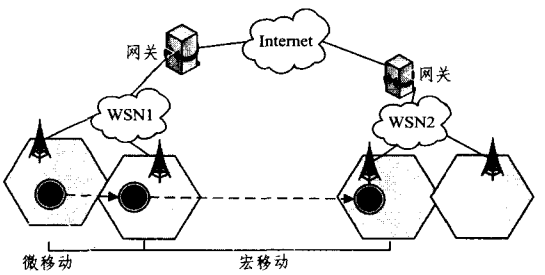

图 2 宏移动和微移动示意图

异构网络移动性管理由两部分组成：位置管理和切换管理。二者是移动性管理的两个不同但相关的方面：前者关心如何定位一个移动节点，跟踪其移动性，更新位置信息，主要研究问题包括寻址方法、数据库结构、位置更新时间以及寻呼机制等。后者重点在于数据传输时控制移动接入点的改变，在数据传输过程中保持移动节点与网络的连接，涉及的操作包括切换触发、连接重建和分组路由等。本课题重点研究切换管理技术。

在切换判决过程中，涉及到通信系统中的多个实体，如用户、网络、终端和服务，需要综合考虑系统中多个实体的属性参数。在切换初始阶段，系统收集切换算法所需要的输入参数即属性参数，这些系统提供的属性参数一般分为静态参数和动态参数。静态参数是指实体固有的特征属性，在时间上是常数或只是偶然发生变化；动态参数是通过系统实际测量获得和变更的。

通常考虑的属性参数可以分为下面 4 个方面：

1)服务属性的静态参数指用户定购的服务类型、服务的特征参数、服务的优先级等；动态参数指服务质量等。

2)用户属性静态参数通常指特定场景的用户参数和成本参数等。用户参数指用户的当前时间、位置和环境；成本参数指情报用户情愿付出高成本来换取高质量的服务，而在空闲时间则期望有较低的成本；动态参数指用户参与位置、状态等信息的获知和更新等。

3)终端属性静态参数指终端的 CPU 类型与性能、存储空间容量、电池能量等；动态参数指终端工作状态中资源利用状况等。

4)网络属性静态参数指网络所用频段信息以及特定 RAT 有特定的 QoS 承载服务等，动态参数指网络负载信息等。

传统切换方法仅仅考虑了上述一种或两种标准，发展多

目标综合判决算法以满足异构性的需要是一种趋势。异构网络切换判决必须应用多因素、多标准综合判决的切换机制或算法。将切换的目标网络选择问题归结为一个多目标评判问题，采用了多种标准判决切换。基于模糊逻辑研究多目标判决模型原理图如图 3 所示。

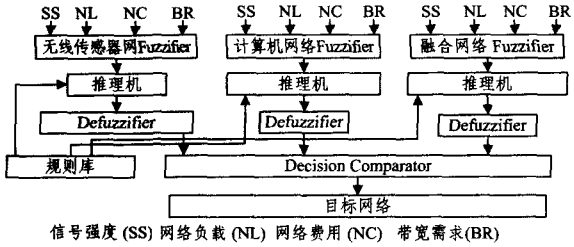

图 3 基于模糊逻辑的网络选择原理图

模糊系统的多准则输入包括信号接收强度(SS)、网络负载(NL)、网络成本(NC)和业务所需带宽(BR)。用于接入网络选择的 MCDM 模糊控制可以分为 3 个阶段。

阶段 1：在该阶段 4 种参数的测量数据被输入一个模糊器，实时测量数据被转化为模糊序列，序列中有不同级别的成员：低(L)、中(M)、高(H)。如网络负载可以分为低负载(L)、中负载(M)、高负载(H)。4 个模糊变量和 3 个模糊序列构成总共 81 个规则。如规则 1 表示接收信号强度“低”、网络负载“高”、成本“高”和所需带宽“高”；规则 81 表示接收信号强度“高”、网络负载“低”、成本“低”和所需带宽“低”，因此所有的标准都赞成选择网络。

阶段 2：该阶段把模糊序列输入到推理机。81 个规则分为 7 个级别，每一级别按照 4 种可能的判决结果(YES, PROBABLY YES, PROBABLY NO, NO)来判决是否选择网络。如第一级别是“YES”，对应于选择网络；第 7 级别是“NO”，对应于不选择网络。上述规则 1 中所有的标准都不赞成选择网络，因此属于级别 7，判决结果是“NO”，即“不选择网络”；而规则 81 则属于级别 1，判决结果是“YES”，即“选择网络”。

阶段 3：解模糊。使用某种解模糊方法将得到的模糊判决序列转换为精确的量，方便排序做判决。

3 无线传感器网和计算机网融合的路由协议模型

在异构网络模型中，大量传感器节点随机地部署在目标区域内部或附近，以自组织方式构成网络。传感器节点数据沿着其它节点逐跳进行传输，其传输过程可能经过多个节点处理，经过多跳后到达汇集(Sink)节点，最后通过收发器接入计算机网。用户通过管理节点对传感器网络进行配置和管理，发布检测任务以及收集检测数据[7]。异构网络模型对其路由协议提出了如下特殊要求：

(1)由于传感器节点在能量、计算、存储和通信上的能力有限，难以获取实时、详尽、准确的网络信息，难以对传感节点进行参数预配置，很多网络参数、密钥等都是传感节点在部署后进行协商形成的。

(2)由于节点能量状态不稳定和节点运动，引起异构融合网络的拓扑结构频繁变化，基于固定拓扑结构的路由算法难以应用于异构融合网络。

传感器网络与计算机网互联融合的路由模型如图 4 所示。

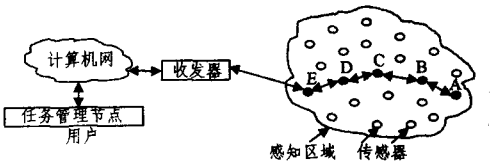

图 4 传感器网络与计算机网互联融合的路由模型

在路由地址配置协议中，每个传感器节点都会进行一定的数据收发，节点根据自己当前所处状态和所收到的数据包的不同，进行相应的处理[8]。每个刚加入网络的传感器节点都被设定为新节点，经过一系列处理后，将会成为老节点或转变为代理节点，之后节点就一直维持这个状态不变。图 5 是 3 种状态转换的示意图。

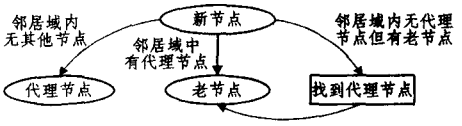

图 5 融合网络节点状态转换示意图

新节点首先发送地址请求包，寻找代理节点。若在指定时间内未收到任何应答，说明一跳范围不存在其他节点，该节点将从新节点状态转变成代理节点状态，自己为自己分配合法地址，之后承担起为其他新节点分配地址的任务。如在指定时间内收到代理节点应答，或通过老节点找到代理节点，新节点将会被分配地址，并转变为老节点状态。

当 WSN 和计算机网通过网关互通时，网间可信路由互通主要考虑在网关处进行可信路由协议消息映射和协议参数的转换，包括传感器网内的区域-局部地址与计算机网可路由 IP 地址之间的相互转换、数据包格式之间的相互转换以及可信路由机制的无缝传递。可信路由传递可采用消息认证和加密机制实现，如使用数字签名来认证路由消息，或使用 Hash 链加密跳数信息防止虚假路由信息。

通过对两种网络进行整体设计，构建异构网络间统一的安全路由协议框架，用综合的方法来适应异构网络的动态性，对网络结构的变化和其他网络信息做出合理反应，两网之间能够互相提供和利用有用信息，对网络特性参数协调融合，使得协议栈能够以全局的方式适应特定应用所需的 QoS 保证和网络状况的变化，并实现对网络资源的有效分配和综合优化。异构网络融合路由协议框架如图 6 所示。

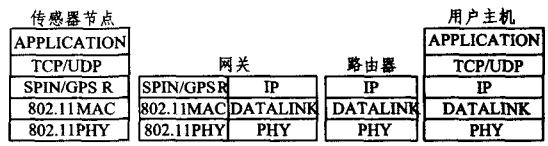

图 6 融合网络统一协议栈结构图

4 实验与分析

以融合网络模型的信任评估为例，采用不同的计算方法来计算信任值，能更准确地评估不同模型中网络实体之间的信任关系。本文假设融合网络有 100 个实体，其中有 20 个恶意实体且恶意实体的信任值各不相同。这些实体完成的都是同一类型交易，并且处于同一上下文中。用融合值表征异构网络融合。当融合组网结束后，实体信任值的更新情况如表

(下转第 109 页)

进展的基础上，设计实现了基于自适应控制的 DTN Web 服务器。通过新增连接管理模块，实现了 DTN Web 服务器上的 PDD 服务。试验结果表明，即使在动态变化的负载条件和不同分布的负载下，闭环系统中的 DTN Web 服务器仍然能较好地为不同优先级的 Web 客户提供 PDD 服务。较固定参数的 PI 控制器而言，自适应控制器使得控制指标在动态负载下波动更小。而且，自适应闭环控制系统可适应系统参考输入的变化，实现面向两个服务类别的 PDD 服务。

在进一步的工作中，将着重研究面向多个服务类别的 PDD 服务在 DTN Web 服务器上的实现。同时，考虑到仿真的复杂度，只检验了 DTN 参考实现 DTN2 下的 PDD 服务，在未来的工作中，将结合 DTN 网络的高延时、高中断率等特征开展深入研究。

参 考 文 献

[1] 单志广，林闯，肖人毅，等. Web QoS 控制研究综述[J]. 计算机学报，2004(2)

[2] Cerf V, et al. Delay-tolerant Network Architecture [S]. IETF RFC 4838. informational, April 2007

[3] Wood L, Holliday P. Using HTTP for delivery in Delay/Disruption-Tolerant Networks[EB/OL]. Internet-Draft, 2008

[4] Ott J, Kutscher D. Bundling the Web: HTTP over DTN[C]// WNEPT 2006 Workshop on Networking in Public Transport, QShine Conference. 2006

[5] Dovrolis C, Stiliadis D, et al. Proportional Differentiated Services: Delay Differentiation and Packet Scheduling[C]// Proceedings of the ACM SIGCOMM. 1999

[6] Abdelzaher T F, Stankovic J A, Lu Chengyang, et al. Feedback Performance Control in Software Services [J]. IEEE Control Systems, 2003, 23(3)

[7] Lu Chengyang, Abdelzaher T F, Stankovic J A, et al. A Feedback Control Approach for Guaranteeing Relative Delays in Web Servers[C]// Proceedings of IEEE Real-time Technology and Applications Symposium. Taiwan, June 2001

[8] Wei Jian-bin, Xu Cheng-zhong. Design and Implementation of a Feedback Controller for Slowdown Differentiation on Internet Servers[C]// WWW 2005. Chiba, Japan, 2005

[9] Lu Y, Abdelzaher T F, Saxena A. Design, implementation, and evaluation of differentiated caching services[J]. IEEE Transactions on Parallel and Distributed Systems, 2004, 15(5): 440-452

[10] Harchol-balter M, Schroeder B, Bansal N, et al. Size - based Scheduling to Improve Web Performance[J]. ACM Transactions on Computer Systems, 2003, 21(2), 207-233

[11] The Apache Software Foundation [J/OL]. http:// www. apache. org

[12] Peltola L. Enabling DTN-based Web Access : the Server Side [D]. Department of Communications and Networking, Helsinki University of Technology, April 2008

[13] 韩曾. 自适应控制[M]. 北京：清华大学出版社，1995

[14] 谢新民，丁锋. 自适应控制系统[M]. 北京：清华大学出版社，2004

[15] Barford P, Crovella M E. Generating Representative Web Workloads for Network and Server Performance Evaluation [J]. Measurement and Modeling of Computer Systems, 1998: 151-160

[16] Crovella M E, Bestavros A. Self-similarity in World Wide Web Traffic: Evidence and Possible Causes[J]. IEEE/ACM Transactions on Networking, 1997, 5(6): 835-846

(上接第 96 页)

1 所列。

表 1 融合网络中恶意实体的信任变化统计表

信任值=0.5		会话的失败次数						
融合值	实体数	1	3	4	5	6	7	8
0.2	3	0.1632	−0.0150					
0.3	4	0.2632	0.0850	−0.0115				
0.4	5	0.3632	0.1850	0.0885	−0.0094			
0.5	5	0.4632	0.2850	0.1885	0.0906	−0.1068		
0.6	2	0.5632	0.3850	0.2885	0.1906	0.0921	−0.0068	
0.7	1	0.6632	0.4850	0.3885	0.2906	0.1921	0.0932	−0.0069
恶意实体数		0	3	7	12	17	19	20

本文的网络信任域是对称的。当更新后的信任值小于零时，该信任模型认为该实体为恶意实体。由表 1 可知，在异构融合模式中，假设信任值度为 0.5，当实体的初始融合值较低(0.2～0.4)时，通过较少的交易行为就可以判断出实体是否存在恶意实体；当实体的初始融合值较高(0.5～0.7)时，需要通过更多的交易行为来判断实体是否为恶意实体。该信任模型对于实体的行为能够迅速准确地反映在信任值上，因此这种判断方法能够保证将恶意实体所带来的损失降到最低。

结束语 无线传感器网络和计算机网络融合是异构网络融合的典型代表，网络结构模型是异构网络互联融合的关键。本文在综合考虑计算机网络和无线传感器网络特点的基础上，提出并分析了互联、隧道和异构网络等 3 种融合模型，并重点研究了第 3 种模型的移动性管理和路由协议架构。

下一步计划在异构网络融合结构模型的基础上，重点开展可信路由控制、资源管理与访问控制、信任管理以及行为检测控制等关键技术研究，并进行仿真验证，通过关键技术研究进一步促进异构网络模型的完善。

参 考 文 献

[1] 3GPP TS 23.234 V6.0.0. 3GPP System to Wireless Local Area Network (WLAN) interworking: system description (Release 6) [S]. 2004

[2] 刘侠，蒋铃鸽，何晨. 一种无线异构网络的垂直切换算法[J]. 上海交通大学学报，2006，40(5)：742-746

[3] 崔莉，鞠海玲，苗勇，等. 无线传感器网络研究进展[J]. 计算机研究与发展，2005，42(1)：163-174

[4] Patwardhan A, Parker J, Iorga M, et al. Secure Routing and Intrusion Detection in Ad Hoc Networks[C]// Proceedings of the 3rd IEEE Int'l Conf. on Pervasive Computing and Communications (PerCom 2005). 2005

[5] Jiang Yuan-xi, Zhao Bao-hua. A Secure Routing Protocol with Malicious Nodes Detecting and Diagnosing Mechanism for Wireless Sensor Networks[C]// IEEE Asia-Pacific Services Computing Conference. 2007

[6] Guo C, Guo Z, Zhang Q, et al. A Seamless and Proactive End-to-End Mobility Solution for Roaming Across Heterogeneous Wireless Networks[J]. IEEE Journal on Selected Areas in Communications, 2004, 22: 834-848

[7] Song Qingyang, Jamalipour A. A Network Selection Mechanism for Next Generation Networks[C]// IEEE ICC. 2005: 1418-1422

[8] Jiang Yuan-xi, Zhao Bao-hua. A Secure Routing Protocol with Malicious Nodes Detecting and Diagnosing Mechanism for Wireless Sensor Networks[C]// IEEE Asia-Pacific Services Computing Conference. 2007