干扰环境下面向延迟的骨干节点路由方法

张立冬[1,2] 覃光成[1] 尹 浩[2] 陈 强[2]
(解放军理工大学通信工程学院 南京 210007)[1] (总参第61研究所 北京 100141)[2]

摘 要 由于参与节点多、移动性强,武器协同数据链一般采用分层的网络结构。战场环境下,己方通信经常会受到敌方干扰,而这将对武器协同数据链网络的一个很重要的性能指标——时延产生明显影响。另外,传统的只考虑下一跳延迟的路由方法并不能保证端到端延迟最小。针对这两个问题,提出了一种干扰环境下面向延迟的骨干节点路由方法和实现模型。该方法通过信息反馈、跨层的方法感知,利用临近节点的干扰信息和目的节点的端到端延迟信息,来为当前节点决定下一跳路由,实现最小端到端时延。仿真和数值结果表明,与几种典型路由协议相比,该方法具有更好的性能。

关键词 数据链,路由,干扰,时延
中图法分类号 TN915.851 **文献标识码** A

Delay-oriented Routing Approach for Backbones with the Interference

ZHANG Li-dong[1,2] QIN Guang-cheng[1] YIN Hao[2] CHEN Qiang[2]
(ICE, PLAUST, Nanjing 210007, China)[1] (PLA's 61st Research Center, Beijing 100141, China)[2]

Abstract The weapon cooperation data link adopts hierarchical methodology generally, as the nodes in it are numerous and moving rapidly. In the battlefield, the interference often occurs, and it will impact the delay seriously, which is an important parameter of the network. Moreover, the general approaches that only care about the delay of next hop can't always obtain the minim end-to-end delay. A delay oriented routing approach with implementing model was proposed for backbones. The SINR to the neighboring nodes and the end-to-end delay to the destination could be obtained to be used for deciding upon the next hop adopting the idea of feedback and cross-layer. The results provide important insights that the approach can get better performance than other several typical routing protocols.

Keywords Data link, Routing, Interference, Delay

1 引言

数据链是现代高技术战争中必需的一种装备,被誉为"现代战争的神经网络",信息化战争离不开数据链。作为数据链体系的重要组成部分,武器协同数据链是一种将空间内多种传感器、武器平台有机地联合起来,快速收集、传输、处理、分发各种战场信息,从而形成传感器-传感器、传感器-武器平台之间的高速、大容量网络通信能力的特殊数据链。所提供的作战能力主要包括:在高速动态的飞行环境下可实现作战成员快速组网;协同探测、决策并快速摧毁正在逼近的威胁性目标;平台间实现跨平台武器投放和控制功能,共享武器资源;平台对制导武器进行接力引导和控制,实现跨平台武器制导;对多目标攻击的空战态势进行综合评估及辅助决策,保证作战决策的正确性。作为移动 Ad hoc 网络(MANET, Mobile Ad hoc Network)的新应用,武器协同数据链具有一般 MANET 特点,无中心基站、易于配置、自组织等。由于武器协同数据链网络在运行过程中,参与节点多、机动性强、用户密集,加之网络资源有限,应用需求严格,因此相对于大部分采用扁平式组网模式来说,武器协同数据链大多采用分层结构,这样的结构能够提高网络的可扩展性,提高网络容量,减少网络开销。

目前,针对分层结构 MANET 路由协议主要可以分为两类:一类认为网络中所有节点的通信能力是相同的;另一类则认为骨干节点具有较强的通信能力(如信号发送距离、传输带宽等)。在第一类路由协议中,基于簇分层的自适应路由协议(ARCH, The Adaptive Routing using Cluster Hierarchies)、SAFARI 协议、群首网关交换路由(CGSR, Clusterhead Gateway Switch Routing)、分层状态路由(HSR, Hierarchical State Routing)是早期提出的基于分层 MANET 的路由协议;第二类路由协议中,比较有代表性的是 H-LANMAR 路由协议。

ARCH 协议[1]中,移动节点同临近节点周期地交互 Hello 信息来建立一个簇的分层,协议的自适应特性使得层的级别可以随着网络条件的变化而实时调整。当网络规模变大时,层的级别提高,反之则降低。文献中给出了仿真结论,在 50~

到稿日期:2009-03-14 返修日期:2009-05-14 本文受"十一五"预研项目资助。
张立冬(1978—),男,博士研究生,主要研究方向为武器协同数据链相关技术,E-mail:zld_cn@163.com;覃光成(1985—),男,博士研究生,主要研究方向为战术信息分发技术;尹 浩(1959—),男,研究员,博士生导师,主要研究方向为通信网总体规划与设计;陈 强(1972—),男,高级工程师,主要研究方向为数据链总体规划与建设。

750 个节点的网络规模条件下，只有少于 2%的节点既不是首节点，也不是网关节点，并且大多数的一般节点能够同多个首节点通信，这种特性使得网络具有较好的鲁棒性能。

SAFARI[2]是另外一种分层路由协议，协议主要考虑提供大规模移动无线网络链接以及基本的网络服务，主要包括 3 个基本协议：自组织、可扩展路由和分布式的地址决定。

自组织协议主要作用是在移动的环境下建立和维持一个分层的网络结构，主要有 3 种机制：信标协议、桶级别选择算法以及成员关系算法。移动节点自动地、自选性地形成一个个的子集，称为桶，桶的唯一功能就是产生信标。信标的内容包括序列号、信标级别、坐标以及跳数，所有的节点将接收到的信标储存在缓存中，形成 DART(Drum Ad hoc Routing Table)，作为网络的自组织和路由之用。

CGSR 协议[4]是对基本 DSDV 路由协议的扩展，是一种基于分群的层次路由协议。它使用 LCC (Least Cluster Change) 群首选举算法来维护分群结构的稳定性，通过交替使用群首-网关序列来高效地传递数据分组，是一种可扩展的先应式自组网路由协议。由于限定分组的传输必须经过群首网关序列，可能产生非最优路径。

HSR 协议[5]是一种层次化的链路状态路由协议，它将动态、分布式分群思想与有效的位置/成员管理结合起来，维护节点物理的层次拓扑和逻辑上的子网。HSR 协议使用物理层次拓扑解决分组的转发路径问题，而使用逻辑子网结构解决节点移动过程中的位置管理问题。HSR 协议虽然具有一定的可扩展性，但协议比较复杂，得到的路径可能是非最优路径，当网络节点移动速度较高时，路由开销也较大。

H-LANMAR[3]是另一种多级分层路由协议，所不同的是，协议中承认一些特殊的节点。这些节点除了一般的电台等装备外，还配备了几个大功率无线电(或具有远距离通信能力设备)，称这样的节点为骨干节点，在骨干节点间建立的网络称为骨干网络。采用这样的配备能够减少长距离通信时过多的跳数。

采用 GloMoSim 对 1000 个移动节点在 3200m×3200m 范围进行了仿真实验，结果证明，H-LANMAR 协议在分发成功率、吞吐量以及时延性能上均优于 AODV 协议。当节点移动速度增加时，协议 AODV 的开销迅速增加，而对协议 H-LANMAR，则所受影响不大。

2 问题描述

从武器协同数据链的应用需求角度分析，低时延信息需求占据了网络业务中的绝大部分，因此在协议栈的下层包括路由层需要提供相应的保证。如前所述，大多数情况下，武器协同数据链更加适合于采用分层的网络结构，相对于一般节点来说，骨干节点之间的通信保证需要引起更多的注意。例如，战术环境下某些节点或者链路遭受敌方干扰，传输路径遭到破坏，战术信息不能得到实时准确传输。在这种情况下，一般节点间通信的解决方法相对简单，更多的是通过增加发射功率或者提高己方的抗干扰能力来争取信息交互的权利。然而对于骨干节点间的信息交互，除了以上两种最基本的方式外，还可以通过改变路由的方式来解决。图 1 所示为两级分层网络中的骨干节点 A 和 B 在进行通信，当传输路径遭受敌方干扰时，节点 A 或者中间节点应该具有实时的根据链路的受干扰情况进行相应的改变传输路径的能力，以保证信息的实时交互。

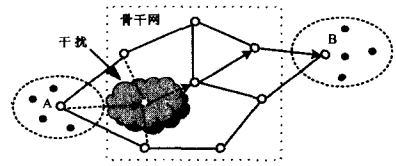

图 1 受干扰的两级分层网络拓扑

从已见文献可知，在讨论和解决分层 MANET 路由问题的过程中，都没有充分考虑、分析和解决战场环境下干扰对骨干网络路由时延的影响问题。在已有的面向延迟的路由协议中，都是基于每跳最优，然而这样并不能确保端到端的时延最小。本文针对武器协同数据链网络中的低时延需求信息，在考虑实战过程中遭受敌方干扰的环境下，提出一种面向延迟的骨干节点路由方法(I-DOBR, Interference-Delay Oriented Backbones Routing)，不失一般性，本文在以下的讨论和分析过程中仍采用两级分层的网络拓扑结构。

3 方法及模型

多跳网络中，端到端时延为信息从源节点产生至目的节点的应用处理中所有传输和处理时间之和，包括节点延迟和链路延迟。其中链路延迟为信号在节点间无线链路的传输时间，一般很小，可以忽略，因此本文主要考虑路由方法的节点延迟。沿用图 1 所示的网络拓扑，则信息由节点 A 至节点 B 所带来的时延可以表示为

$$Delay(P_{AB})=Delay(P_{Ai})+Delay(P_{im})+\cdots+Delay(P_{jB}) \tag{1}$$

其中，i,m,j 均为路径 P 上的中继节点。设每一跳的备选节点集中均有 M 个节点，则对于路径上的任一中继节点 k，从最小端到端时延的角度来选择下一跳中继节点 $m(1\leqslant k,m\leqslant M)$，需要满足

$$Delay(P_{kB})=\min(Delay(P_{km})+Delay(P_{mB})) \tag{2}$$

式(2)表达了节点 k 所选择的下一跳节点 m 必须使得由节点 k 至节点 m 的时延加上节点 m 至目的节点 B 的端到端时延最小。为避免事件的偶然性，对式(2)取平均，即

$$E(Delay(P_{kB}))=\min(E(Delay(P_{km}))+E(Delay(P_{mB}))) \tag{3}$$

式(3)右边第一项可以近似理解为当前节点时延，第二项为下一跳节点至目的节点的端到端时延，更多的情况下第二项决定着式(3)。$E(Delay(P))$从一个侧面反映了两节点间的链路质量和传输能力，是路由选择参数、链路有效吞吐量以及数据排队等待时间的函数，式(3)可以进一步表示为

$$E(Delay(P_{kB}))=\min(E(Delay(T_{km}^{good},W_{km}))+\sum_{n=1}^{M}\beta_{mn}\cdot E(Delay(P_{nB}))) \tag{4}$$

其中，T_{km}^{good} 为当前节点到下一跳节点的有效吞吐量，W_{km} 为数据排队等待时间，β 为路由选择因子。等式右边的第一项可以近似表示为

$$E(Delay(T_{km}^{good},W_{km}))=\frac{L}{T_{km}^{good}}+W_{km} \tag{5}$$

其中，L 为统一包长，若设 k 节点和 m 节点间的信干噪比为 $SINR_{km}$，误比特率为 BER_{km}，则两节点间的误包率可以表示为

$$p_{km}=1-(1-BER_{km})^{L} \tag{6}$$

使用 Sigmoid 函数[7]，式(6)可以统一地近似表示为

$$p_{km}=\frac{1}{1+e^{\zeta(SINR_{km}-\delta)}} \tag{7}$$

其中，ζ,δ 是常数，在确定的包长的情况下，由具体的调制、编码方式决定。例如当采用 BPSK 调制方式，没有任何编码措施、包长设为 20 的情况下，相应的 $\zeta=1.2,\delta=3.1$。则有效吞吐量可以表示为

$$T_{km}^{good}=1-T_{km}\cdot p_{km}=\frac{T_{km}}{1+e^{-\zeta(SINR_{km}-\delta)}} \tag{8}$$

参数 T^{good} 将通过跨层的方式由 MAC/物理层传递给路由层，通过式(4)、式(5)得到选择某个中继节点而造成的端到端时延，进而决定路由。由文献[8]中的带有止步和中途退出的排队系统模型可以得到路由选择因子的表达式

$$\beta_{km}=\frac{C}{1+\kappa E[Dela\,y_{kmB}]^{\varphi}} \tag{9}$$

其中，κ 和 φ 为常数，κ 的值取决于数据到达速率，φ 作为平均延迟的加权，使得路径选择满足端到端时延的最小化。参数 β 是一个路由选择的概率，对于任意节点 k,m 满足

$$0\leqslant\beta_{km}\leqslant 1 \tag{10}$$

$$\sum_{m=1}^{M}\beta_{km}=1 \tag{11}$$

当临近节点 m 没有信息反馈，或者节点不可达时，$\beta_{km}=0$；当 m 为目标节点时，$\beta_{km}=1$。C 为标准化系数，以保证式(11)得以满足

$$C=(\sum_{m=1}^{M}\frac{1}{1+\kappa E[Dela\,y_{kmB}]^{\varphi}})^{-1} \tag{12}$$

由以上分析可知，通过下一跳节点反馈的端到端延迟、信干噪比信息，当前节点能够得到多个临近节点的路由选择因子，并依据这个参数进行路由选择，方法的模型框图如图 2 所示。

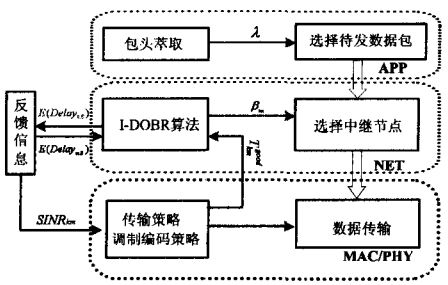

图 2　I-DOBR 实现模型

模型中的应用层根据信息的优先级别 λ，选择待发信息数据，路由层根据上述描述的算法确定每个数据包的下一跳；MAC 层和物理层根据相应的设置进行数据的发送。算法的输入部分为临近节点到目的节点的端到端延迟反馈 $E(Delay)$，MAC/物理层的有效吞吐量为 T^{good}，输出为决定中继节点的路由选择因子 β，以及反馈到临近节点的到达可达节点的平均延迟。路由选择因子用于本地数据选择下一跳节点，反馈到临近节点的延迟信息用于临近节点决定路由。由图 2 以及 I-DOBR 算法可知，这种路由方法考虑了外界干扰对网络延迟所造成的影响，以最小端到端延迟为目标选择中继节点，解决了战场环境中在受干扰的情况下网络骨干节点的面向延迟路由问题，从这个层面上为武器协同数据链网络中的低时延信息需求提供了保证。

4　可实现性分析

对于分层网络拓扑结构，骨干节点数目相对较少，一般为所有节点数目的几十分之一至几百分之一。由第 3 节的方法模型可知，算法的实现需要每两个可达节点之间周期性地反馈端到端延迟和信干噪比信息，这属于 NP 完全问题[11]，具有较大的网络开销，不适合于扁平结构的网络。但对于上层相对较少的骨干节点，则不会占用太多的网络资源，网络开销可以接受。

在组成武器协同数据链网络的成员中，绝大部分是以集群或编队的形式出现，因此以组移动模型考虑武器协同数据链网络较为合适，网络子集的运动并非随机、杂乱无章的。在短时间内，骨干节点相对位置变化不大，因此节点间反馈的延迟和信干噪比信息能够有效地反映当前网络的链路质量，骨干路径过时的可能性不大。

5　仿真与数值结果

使用 Qualnet 仿真工具，实验仿真环境为在 4km×4km 区域内分别放置 16 个节点作为骨干节点，忽略一般节点。通过限制节点间的距离和节点的移动速度来实现以一般 MANET 网络拓扑代替骨干网络的方式进行仿真，节点采用随机游走模型，运动速度为 5m/s。设置每个节点的传输范围一样，均为 2.5km，采用 BPSK 调制方式，不采用编码措施。设干扰为单频样式，每个暂停时间内以等概率方式干扰如图 1 所示的链路之一，干扰强度在 0～20dB 均匀分布。

为了说明问题，将提出的 I-DOBR 路由方法同经典的 DSDV，OLSR 路由协议进行了比较。图 3 和图 4 所示分别为网络延迟性能以及数据交付率性能的比较，由图可知，同两种经典先应式路由协议相比，I-DOBR 路由方法在这两方面均具有明显的优势。在延迟性能方面，I-DOBR 路由方法好于 OLSR 路由协议 0.2～0.5 个单位时间，好于 DSDV 路由协议最大达到近 1 个单位时间。在数据交付率性能方面，I-DOBR 路由方法在存在干扰的情况下，一直维持在 80%左右，而 DSDV，OLSR 路由协议则分别在 50%，65%上下。

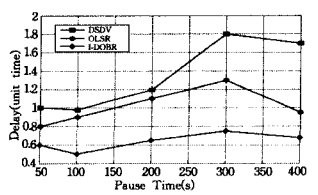

图 3　网络延迟性能比较

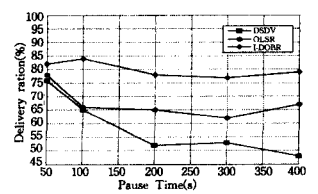

图 4　数据交付率性能比较

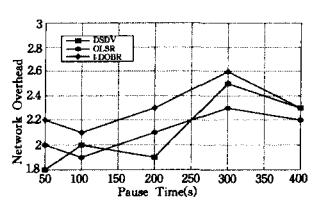

图 5　网络开销性能比较

图 5 所示为网络开销性能比较，由图可知，DSDV 和 OLSR 开销相差不大，而 I-DOBR 路由方法较之两者显得稍大一些，主要原因在于 I-DOBR 路由方法反馈了大量的端到端延迟信息和链路干扰信息。由骨干节点组成的网络中，节点数目不大，密集度不高，I-DOBR 路由方法的网络开销可以承

受，且不会对网络性能产生明显影响。

结束语 本文针对干扰环境中武器协同数据链网络骨干节点的路由问题，提出了一种面向延迟的路由方法，并给出了实现模型。该方法通过信息反馈、跨层手段感知、充分利用了链路端到端时延信息以及干扰状况，来为当前节点选择路由，实现了信息的最小端到端时延，满足了武器协同数据链网络中低时延业务的需求。仿真表明，同传统的 DSDV，OLSR 协议相比，I-DOBR 路由方法除开销稍大以外，其他主要性能指标均好于两者。

参 考 文 献

[1] Belding-Royer E M. Multi-level Hierarchies for Scalable Ad hoc Routing[C]// Santa Barbara. Wireless Networking (WINET). California: Department of Computer Science. University of California, 2003: 461-478

[2] Saha A K, Johnson D B. Self - Organizing Hierarchical Routing for Scalable Ad hoc Networking[R]. Houston, Texas: Rice University Department of Computer Science, 2000

[3] Xu K, Hong X, Gerla M. Landmark Routing in Ad hoc Networks with Mobile Backbones[M]. Orlando: Academic Press, INC., *2003: 110-122*

[4] Chiang C C, Wu H K, Liu W, et al. Routing in Clustered Multihop, Mobile Wireless Networks with Fading Channel[C]// IEEE Singapore International Conference on Networks. Guangzhou, *1997: 197-211*

[5] Westcott J, Lauer G. Hierarchical routing for very large net - works[C]// IEEE MILCOM'84. Los Angeles, 1984: 214-218

[6] Shiang Hsien-po, van der Schaar M. Multi - User Video Streaming over Multi-Hop Wireless Networks: a Distributed, Cross-Layer Approach Based on Priority Queuing[J]. IEEE Journal Selected Areas in Communications, 2007, 25(4): 770-785

[7] Krishnaswamy D. Network-Assisted Link Adaptation with Power Control and Channel Reassignment in Wireless Networks[C]// 3G Wireless Conf. New York, 2002: 165-170

[8] Kleinrock L. Queuing Systems Volume I: Theory [M]. New York: Wiley-Interscience Publication, 1975: 320-322

[9] Srivastava V, Motani M. Cross-Layer Design: A Survey and the Road Ahead[J]. IEEE Comm. Magazine, 2005, 43(12): 112-119

[10] van der Schaar M, Turaga D S. Cross-Layer Packetization and Retransmission Strategies for Delay-Sensitive Wireless Multimedia Transmission[J]. IEEE Trans. Multimedia, 2007, 9(1): 185-197

[11] Xiao Wendong, Boon Hee Soong, Choi Look Law. QoS Routing Protocol for Ad hoc Networks with Mobile Backbones[C]// IEEE ICNSC. Singapore, 2004: 1212-1217

(上接第 92 页)

(3)移动 Agent 只含有私有代码和公共数据，不产生结果数据。如图 4(c)所示，这时代码逐渐减少，数据不变；

(4)移动 Agent 只含有公共代码和数据以及私有数据，主要用于收集管理信息。如图 4(d)所示，这时代码不变，数据逐渐增多；

(5)移动 Agent 只含有公共代码和公共数据以及私有数据，主要用于设置管理参数。如图 4(e)所示，这时代码不变，数据逐渐减少；

(6)移动 Agent 只含有公共代码和公共数据，不产生结果数据。如图 4(f)所示，这时代码不变，数据也不变。

(1)－(3)含有私有代码而不含有公共代码，而(4)－(6)含有公共代码而不含有私有代码，因为移动 Agent 中属于某个被管理节点的私有代码被篡改和伪造只影响这个节点安全的网络管理，而移动 Agent 中公共代码被篡改和伪造将影响要访问的所有被管理节点安全的网络管理，所以在(4)－(6)网络管理过程中，MANMSM 能够提供比(1)－(3)更加安全的保护。可见，在 MANMSM 中，我们能够基于不同的安全要求，灵活地选择和装配不同的移动 Agent 进行具体的网络管理。

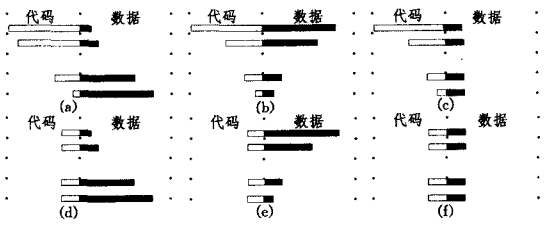

图 4 安全管理过程移动 Agent 典型的代码和数据变化实例

结束语 面向移动 Agent 网络管理的安全模型 MANMSM 利用 Java 卡和加密技术对基于移动 Agent 的网络管理过程实施硬件和软件的保护，较好地解决了网络管理站、被管理节点和移动 Agent 的安全保护问题。但该模型并不能保证网络管理过程绝对安全，因为 MANMSM 安全性的高低还要取决于安全保护措施(例如网络管理站、Java 卡)自身的保护程度，所以在 MANMSM 中，安全的网络管理站和 Java 卡能够给 MANMSM 网络管理过程带来高度的安全性。

参 考 文 献

[1] 张云勇，刘锦德. 移动 agent 技术[M]. 北京：清华大学出版，2003

[2] Braun P, Rossak W. Mobile Agents : Basic Concepts , Mobility Models, and the Tracy Toolkit[M]. Morgan Kaufmann Publishers, 2004

[3] 王汝传，徐小龙，黄海平. 智能 Agent 及其在信息网络中的应用[M]. 北京：北京邮电大学出版社，2006

[4] Autran G, Li Xining. Large Scale Deployment a Mobile Agent Approach to Network Management[C]// Proceedings of 2008 Seventh International Conference on Networking (ICN 2008). April 2008: 614-619

[5] Nilchi A R N, Vafaei A, Hamidi H. Evaluation of security and fault tolerance in mobile agents[C]// Proceedings of 2008 5th IFIP International Conference on Wireless and Optical Communications Networks (WOCN'08). May 2008: 1-5

[6] Ketel M. Applications of mobile agents and related security issues[C] // Proceedings of IEEE SoutheastCon 2007. March 2007: 23-28

[7] 陈志，王汝传. 移动代理网络管理模型的安全性研究[J]. 南京邮电学院学报，2004, 24(2): 70-75

[8] Koliousis A, Sventek J. A Trustworthy Mobile Agent Infrastructure for Network Management[C]// Proceedings of 2007 10th IFIP/IEEE International Symposium on Integrated Network Management (IM'07). 2007: 383-390

[9] Mayes K, Markantonakis K. Smart Cards, Tokens, Security and Applications[M]. Berlin: Springer, 2008