邻居认证的 Mesh 网络安全多路径路由协议

张景东,吴振强
ZHANG Jing-dong,WU Zhen-qiang

陕西师范大学 计算机科学学院,西安 710062
College of Computer Science,Shaanxi Normal University,Xi'an 710062,China
E-mail:zjd0416@126.com

ZHANG Jing-dong,WU Zhen-qiang.Mesh secure multi-path routing protocol of neighbor authentication.Computer Engineering and Applications,2009,45(4):115-118.

Abstract: In Mesh networks,the mobility of node and the multi-hop of data transmission,the quality and safety of routing protocol became the critical factors in weighing the performance of Mesh network.It is necessary to find more efficacious and safer routing protocol instantly,and it can adapt the topology change on network.Because the actual routing protocol of Mesh network didn't consider the safety of the protocol itself.In this paper,a new scheme of secure multi-path routing protocol based on authentication is proposed.The safety mechanism is appended in the process of setting up the multi-path.The analysis shows that the routing algorithm can keep the safety of routing protocol on the base of supporting the balance of loading,enhancing the throughput in whole and increasing the ability of error tolerance.Beside,in this way,the node-disjoint between multi-paths can reduce the probability of path collapses and provide higher reliability for data transmission.

Key words: Mesh;routing protocol;multi-path;node-disjoint;authentication

摘 要:Mesh 网络节点的移动性和数据传输的多跳性,使得路由协议的质量以及安全性成为衡量 Mesh 网络性能的关键因素,迫切需要一种能适应网络拓扑变化,高效、安全的路由协议。而目前针对 Mesh 网络的路由协议很少考虑到协议本身的安全性问题。提出了一种基于认证的节点分离安全多路径路由协议,在多路径的建立过程中加入了安全机制。分析表明,该路由算法在提供负载平衡、提高整体吞吐量、增加容错性的基础上能够很好地保证路由协议的安全性,而且多路径之间节点分离能够降低链路断开的概率,为数据传输提供更高的可靠性。

关键词:Mesh;路由协议;多路径;节点分离;认证
DOI:10.3778/j.issn.1002-8331.2009.04.032 **文章编号**:1002-8331(2009)04-0115-04 **文献标识码**:A **中图分类号**:TP393.08

1 引言

无线 Mesh 网络(Wireless Mesh Network,WMN)是一种全新的无线网络技术。其核心是让网络中的每个节点都发送和接收信号,具有高速率、易组网、成本低、性能稳定等特点。无线 Mesh 网络最初是美国军方为了在战场上通信而研发的,近年来随着一些保密技术相继被公开并转化为民用,逐渐成为移动通信领域的研究热点[1]。

由于 Mesh 网络节点的移动性和拓扑结构的动态性,路由协议一直是 Mesh 网络研究的关键技术之一[2]。在 Ad hoc 网络中,路由协议分为两大类:表驱动(Table-driven,也叫先验式)路由协议(例如 ZRP[3])和按需驱动(On-demand,也叫反应式)路由协议(例如 DSR[4])。

根据一个路由请求所发现的路径的数量,路由协议又可以分为单路径(如文献[4-5])和多路径(如文献[6-7])。按照多路径间是否共享节点或链路,多路径又可以分为节点分离多路径(Node-disjoint Multi-path,NMP)和链路分离多路径(Link-disjoint Multi-path,LMP)[8]。

Mesh 网络中,节点的移动和拓扑结构的动态变化,很难维护一个持续的、稳定的、有效的端到端路由。而且随着人们需求的不断增长和 Mesh 网络与其他网络的融合,Mesh 网络除了传输一般的数据外,还会更多地用于传输多媒体数据等。而多媒体数据传输具有持续时间长、数据流量集中和实时性等特点,这对 Mesh 网络路由协议提出了更高的要求,持续长时间的数据传输要求路由协议能够在拓扑发生变化的情况下继续保持数据传输的畅通,在活动链路断开的情况下能够迅速切换到备用路径进行数据正常通信。数据流量的集中容易导致路由路径发生流量拥塞现象,需要对集中数据进行择路分流以实现负载平衡。实时性要求数据从源节点到目的节点的端到端传输过程中,时延降到最小。这些需求都是传统的路由协议(如 AODV 等)所无法满足的。而且 Mesh 网络拓扑结构的动态性和节点移

基金项目:国家自然科学基金重点项目(the National Natural Science Foundation of China under Grant No.60633020)。
作者简介:张景东(1983-),男,硕士生,主要研究方向为无线网络安全;吴振强(1968-),男,博士,副教授,硕士生导师,主要研究领域为无线网络安全,可信计算,匿名认证。
收稿日期:2008-01-08 **修回日期**:2008-03-31

动性对 Mesh 网络的安全性提出了严峻的考验,其中路由协议的安全性就是关键点之一。

近年来,很多研究人员针对无线 Ad hoc 网络的多路径路由做了大量的研究工作[9-12]。Lee 和 Gerla 提出了一种分离多路径路由算法(SMR)[9],用于建立一个最大的分离路径集;EDSR[10]路由算法用于发现节点分离路径;基于 AODV 的节点分离多路径路由协议 AODVM[11];SRP[12]协议采用了端对端的对称密码技术保护了路由发现过程的完整性,对于恶意节点的很多攻击起到了一定的抵抗作用。虽然多路径的提出解决了很多问题,也为 ad hoc 网络的发展做出了很多贡献。但是,仅仅靠多路径并不能保证安全问题,比如网内节点的伪装,未授权节点的访问,以及重放攻击等。

本文提出了一种基于邻节点认证的安全多路径路由协议 SMRPA(Secure Multi-path Routing Protocol Based on Authentication),该协议的基本思想是在路由建立发起之前先进行邻节点认证,以免在路由建立过程中有未授权节点加入到路由路径中,在路由建立过程中,通过加密和 hash 函数认证,确保收到的路由请求包的正确性和完整性,在目标节点选择路由过程中遵循相应数学原理合理选择路径数目并做出及时正确的路由响应。数据通过节点分离的多条路径传输时,能够有效地利用网络资源,减少网络拥塞,降低时延,提高错误容忍性,减低丢包率,达到稳定可靠的通信质量。

2 SMRPA 协议描述

SMRPA 协议在给定最大跳数限制的条件下,在源节点和目标节点之间找出了一个无环路的、节点分离的路径集,在这个路径集合中根据相应的选路规则选取其中最合理的 n(n 在下文给出)条路径作为源节点到目标节点的有效路径。SMRPA 协议的实现主要分为两个阶段。第一阶段为路由查询发起前的邻居节点认证阶段。第二阶段为路由建立阶段,路由的发现过程是在以下三种情况下发起的:路由初始化时、当前活动路径崩溃时(这种情况下,数据可以通过可选备用路径进行转发)或所有可达目标节点的已知路径全都不可用时[13]。而路由发现过程是在以下两种情况下停止的:已发现了足够数量的路径或所有可能的路径均已发现。具体分为三个环节,第一环节为源节点 S 发起路由请求包 *RREQ*,第二环节为中间节点接收并处理来自源节点的 *RREQ* 包,第三环节为 *RREQ* 到达目标节点后,目标节点进行路径集合的收集以及选出合理路径并发送 *RREP* 包给源节点,整个路由建立过程完成。

2.1 邻节点认证阶段

令 n_i 表示无线 Mesh 网络中的任意节点,假设每个 n_i 节点都分别拥有一对属于自己的公私钥对(PK_i,SK_i),每个 PK_i 由可信第三方授权机构 *CA* 分发的证书 $cert_i$ 来确定。Mesh 网络中的每个节点 n_i 都有一个 ID_i 号,作为节点在网络中的唯一标识。

在一定的时间间隔内,每个节点 n_i 广播一个带签名的消息给它的一跳邻居节点,消息包含内容为:$t_{current}$,ID_i,$sig(t_{current},ID_i)$,$cert_i$,$t_{current}$ 为节点 n_i 发出广播消息的当前时间,$sig(t_{current},ID_i)$是用来验证邻居节点的真实性的一个签名。在认证阶段完成以后,每个节点 n_i 分别拥有自己在时间 $t_{current}$ 的邻居表了,邻居表的表示用 N_i^t(这里的 t 就是 $t_{current}$)。

Mesh 节点在进行路由前,从接入网络到进行邻居认证的流程如图 1 所示。

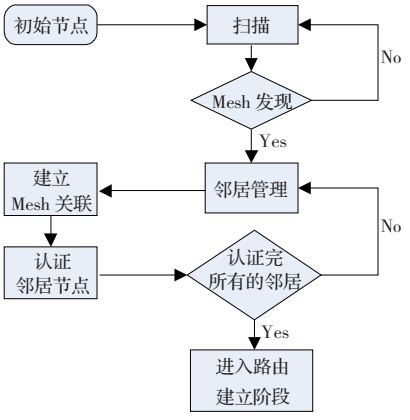

图 1 Mesh 节点邻居认证流程图

因为邻居表的认证部分是在本地邻居之间进行的,所以这些认证的过程都是在某几个局部范围内进行一跳认证,这个认证代价是可以容忍的,而且广播消息只限于一跳邻居,所以在整个网络来说不会形成网络风暴。

2.2 路由建立和维护阶段

路由建立和维护阶段又分三步完成:源节点发起 *RREQ* 包进行路由请求查询、中间节点收到 *RREQ* 包进行转发处理、*RREQ* 包到达目的节点,目的节点采用路径选择策略进行合理路径的选择,并发送 *RREP* 包给源节点。

2.2.1 路由请求查询

当源节点 S 想要和目的节点 T 进行通信时,S 首先检查是否有 T 的活动路径,如果有,则 S 与 T 直接通信,如果没有,S 将产生一个路由请求查询包 $RREQ_{S,T}$,$RREQ_{S,T}$ 中所包含的数据帧内容如下:

$$RREQ_{S,T}=(ID_S,ID_T,Q_{seq},T_{cnt},hop_{cnt},hop_{\max},E_{PKT}(K_{S,T}),RouteList,ExcludeList,NextHop,\text{hash}_{K_{S,T}}(ID_S,ID_T,Q_{seq},T_{cnt},hop_{\max}))$$

ID_S、ID_T 分别是源节点 S 和目的节点 T 的 ID 号,Q_{seq} 是一个序列号生成器,源节点 S 每一次发起的路由请求时 Q_{seq} 都会产生一个序列号,对每次查询请求来说 Q_{seq} 产生的序号都是唯一的,因此可以作为验证请求消息的正确性和重复性的一个依据。T_{cnt} 为发起请求时的时戳,hop_{cnt} 记录了 $RREQ_{S,T}$ 当前所经过的跳数,$hop_{\max}$ 为一个查询包所允许经过的最大跳数,可以综合当前网络规模和网络连通性分析给出,$K_{S,T}$ 是由源节点在路由发起时产生的一个随机数,作为 S 和 T 的共享密钥,用来协商确定 hash 函数 $\text{hash}_{K_{S,T}}$,$K_{S,T}$ 在传送过程中用目的节点 T 的公钥加密,以保证 $K_{S,T}$ 的安全,这一过程可以认为是安全信道。*RouteList* 是动态路由表,在路由查询过程中,通过分析,一些符合要求的中间节点可以加入到 *RouteList* 形成从 S 到 T 的路由路径。*ExcludeList* 也是一张动态节点登记表,记录一些由于特殊请求下被排除在外的节点的 ID,主要是防止在建立节点分离路径的过程中,由于某些节点的二次利用等而产生环路,*ExcludeList* 是生成节点分离路径的关键。*NextHop* 记录那些可以作为当前路由下一跳的节点。$\text{hash}_{K_{S,T}}(ID_S,ID_T,Q_{seq},T_{cnt},hop_{\max})$是由 S 和 T 的共享密钥 $K_{S,T}$ 产生的一个 hash 函数,用来验证 $RREQ_{S,T}$ 的正确性和完整性。

源节点 S 发起查询请求的算法流程如下:

(1)初始化:ID_S、ID_T 已知,Q_{seq} 根据历史记录产生,hop_{cnt}=0,

$hop_{max}=MAX$,$RouteList=S$,$ExcludeList=$Null,$NextHop=N_i^t$;

(2)S 选择随机数 $K_{S,T}$:确定 hash 函数 $\text{hash}_{K_{S,T}}()$,并计算 $E_{PKT}(K_{S,T})$和 $\text{hash}_{K_{S,T}}(ID_S,ID_T,Q_{seq},hop_{max})$;

(3)构造并广播 $RREQ_{S,T}$ 数据包。

2.2.2 中间节点处理环节

在每个节点内部都保存着一张记录表,表的内容为最近处理过的请求包的序列号 Q_{seq}。中间节点 n_i 在收到 $RREQ_{S,T}$ 后,通过判断其序列号是否包含在记录表中来判断 $RREQ_{S,T}$ 是否是重复接收,如果是,则直接丢弃。否则表明是第一次收到,把 Q_{seq} 加入到记录表,作为以后判断的依据。再进行第二次判断,此时,节点 n_i 检查自己是否属于 $RREQ_{S,T}$ 包的 $RouteList$ 中最后一个节点 n_j 的邻居表 N_j^t,如果 $ID_i\in N_j^t$,则表明 n_i 是 n_j 的一跳邻居,否则,收到的 $RREQ_{S,T}$ 包可能来自不安全节点,将其丢弃,这样就可以在中间节点之间进行双重认证,对于多重身份攻击(multiple identity attacks)可以起到有效防护作用。通过二次判断之后,可以验证 $RREQ_{S,T}$ 包的有效性。

本文给出的多路径路由是节点分离的,而且在查询过程中避免了环路现象,实现的关键技术就在于中间节点对 $ExcludeList$ 表的操作。假设节点 n_i 把它处理完的 $RREQ_{S,T}$ 包(用 $RREQ_{S,Ti}$ 表示)广播给它的邻居节点 n_j、n_k,则算法可以表示成:

$n_i\rightarrow RREQ_{S,Ti}$;

$RouteList=RouteList+ID_i$;

$ExcludeList=ExcludeList+N_{i-1}^t$;

$NextHop=\{n_j,n_k\}$;

$n_j\rightarrow RREQ_{S,Tj}$;

$RouteList=RouteList+ID_j$;

$ExcludeList=ExcludeList+N_i^t$;

$NextHop=N_j$;

节点 n_k 上的算法操作类似节点 n_j。

这一算法保证了 $RREQ_{S,T}$ 总是按从 $S\rightarrow T$ 的方向传送,中间出现回路情形时,由 $ExcludeList$ 阻止。

2.2.3 目标节点路由回复

当目标节点 T 收到 $RREQ_{S,T}$ 后,先解密获得 $K_{S,T}$,再通过函数 $\text{hash}_{K_{S,T}}()$对 $RREQ_{S,T}$ 包中的 ID_S、ID_T、Q_{seq}、T_{cnt}、hop_{max} 五项做 hash 运算得到值 $\text{hash}'_{K_{S,T}}(ID_S,ID_T,Q_{seq},T_{cnt},hop_{max})$,与 $RREQ_{S,T}$ 包中的 $\text{hash}_{K_{S,T}}(ID_S,ID_T,Q_{seq},T_{cnt},hop_{max})$做比较以验证 $RREQ_{S,T}$ 的完整性。如果两个 hash 值一致,则表明收到的 $RREQ_{S,T}$ 包被正确接收,放入缓存等待下一步处理,否则表明查询包在传播过程中出错,直接丢弃。在时间 T_{wait}(根据当前网络拓扑连通性以及 hop_{max} 综合考虑确定)内继续等待并验证从其他不同路径到达的同样的 $RREQ_{S,T}$,并放入缓存中,直到等待时间超过 T_{wait}。然后,目标节点 T 从收到的 m 个 $RREQ_{S,T}$ 中取出各自的 $RouteList$,构成一个在 hop_{max} 范围内的最大的节点分离路径集合 $P_{max}=\{P_1,P_2,\cdots,P_k\}$,$(1\leqslant k\leqslant m,P_i=(ID_S,ID_T,RouteList_i,1\leqslant i\leqslant k))$。然后进行最优路径选择。

发现多条可达路径并不意味着提高了路由的质量,如何获得多路径并不是路由设计的主要问题,路由设计的关键是如何从已发现的多条路径中选择出若干条最优路径,以便提高网络的路由质量。在相关多路径路由文献中,一般只是强调如何去寻找多条路径,但是对于路径的数目却没有明确的选择。Peter P 等人由数学模型证明了,有 2 条或 3 条路径的多路径路由协议的性能比较好[14]。文献[15]通过仿真和概率统计的方法进行了详细的研究分析,确定了在节点分离的多路径路由中有 3 条路径的路由协议是最优的。多路径路由的数目还同当前网络节点的分布密度有着很大的关系,基于以上研究结论作为参考,结合实际,在本文中,从效率和开销折中考虑选择 4 条路径作为最优路径,其中 2 条作为当前活动路径用于数据传输,其余 2 条作为备选路径。这样既符合最优路径数目选择,解决链路负载平衡,又有备选路径以防止活动路径崩溃后数据传输不中断。4 条路径的选择是以到达目标节点的时延为依据。因为算法所加的安全机制已经产生了时间延迟,所以在此算法中时延将是一个需要重点考虑的参数。而跳数跟实际网络节点分布密度和网络连通性有关,对于多路径的影响并不是很大,所以在此不作为考虑对象。定义路径代价为:

$$P_{cost}=T'-T_{cnt}$$

P_{cost} 为路径代价,T' 目标节点收到 $RREQ$ 包的当前时刻,T_{cnt} 为 $RREQ$ 包中时戳。然后选出 4 条 P_{cost} 值最小的路径作为有效路径。目标节点 T 针对每条有效路径构造并广播一个回复消息:$RREP_{T,Sj}=(ID_T,ID_S,seq,RouteList_j,\text{hash}_{K_{S,T}}(ID_T,ID_S,seq,RouteList_j))$

在回复消息中,T 作为消息源节点,S 作为消息目标节点。

每个中间节点 n_i 接到回复消息 $RREP_{T,Sj}$ 后,检测 n_i 是否属于 n_i,如果 $ID_j\notin RREP_{S,Tj}$,则丢弃 $RREP_{T,Sj}$,如果 $ID_j\in RREP_{T,Sj}$,则转发 $RREP_{T,Sj}$ 到下一跳。直到 $ID_i=ID_S$,则表明已经到达源节点 S,源节点通过验证 $\text{hash}_{K_{S,T}}(ID_T,ID_S,seq,RouteList_j)$的有效性来判断收到的回复消息是否有效。如果有效,$S$ 将存储路径 P_j 并通过 P_j 与节点 T 进行通信。

2.2.4 路由维护

由于网络拓扑结构动态变化,造成路由链路在(n_i,n_j)处断开时,节点 n_i 将对那些经过自己且因(n_i,n_j)断开而受到影响的当前活动路由广播一个经 n_i 签名的错误报告消息 $RRER$,收到 $RRER$ 的节点检查自己是否属于断开链路,如果是,则继续向其下一跳转发,知道源节点 S。否则,丢弃 $RRER$。

若不对 $RRER$ 进行签名,恶意节点可以用伪造的错误报告消息在网络内广播,而导致网络丧失通信能力。节点在收到错误报告消息后,检查其 ID 号是否属于此消息所包含的 $RouteList$,若包含,则对所在的断开链路做出标识并再次广播该消息给其他节点,直到接收到 S 或 T 节点告知的重新建立路由的消息。

3 性能分析

本文提出的是一种基于邻居节点认证的多路径路由,尽管这种多路径路由在设计和通信过程中比单路径路由复杂很多,但是其优势也是很明显。首先,由于 Mesh 网络节点的随机移动性和网络拓扑的频繁变化,链路断开的情况经常发生,提供多径路由,这对于 Mesh 网络路由的可靠性和容错性是有很好改良的;其次,此协议提供的是在源节点和目标节点之间相互独立的多条节点分离多路径,它们之间的实际带宽等于各条路径带宽的总和。这样就能够充分利用网络资源,从而改进通信性能,满足一定的 QoS 需求。由于本协议同时用两条路径进行数据传输,能够有效地把数据分组平均到两条路径当中,从而使网络中节点的负载趋于平衡。

3.1 安全性分析

源节点 S 利用目标节点 T 的公钥对随机数 K 进行加密，通过路由请求消息 $RREQ_{S,T}$ 发送到目标节点 T，从而实现了共享密钥的协商。目标节点 T 通过共享密钥 $K_{S,T}$ 协商的 hash 函数对 $RREQ_{S,T}$ 进行验证，实现了查询消息的端到端认证，保护了查询消息的完整性。在这一过程中只对随机数进行了一次加密和一次 hash 值的运算，因此运算代价是完全可以接受的。

本协议提供的邻居认证阶段，事实上对路由链路做了间接的认证。因为每个节点都在周期性地认证其邻居节点，每个节点都能够保证它自己参与的链路的前一跳和下一跳节点是合法的。在路由回复阶段也是如此，每个收到回复包 $RREQ_{S,T}$ 的节点 n_i 验证 $RouteList$ 中 ID_i 的上一跳和下一跳是否属于 n_i 的邻居表，这些验证对于没有加密的路由表来说是很有必要的。每个节点 n_i 只需要做的就是验证 ID_{i-1}、ID_{i+1} 是否属于 N_i^t，尽管每个中间节点可能会收到比较多的路由请求包和路由回复包，但是在这整个认证过程中，只需一次加密，因此效率比较高。

在路由回复阶段通过共享密钥 $K_{S,T}$ 所确定的 hash 函数 $\text{hash}_{K_{S,T}}(ID_T, ID_S, seq, RouteList_j)$ 能够验证路由回复消息是否被修改过，从而保护了回复消息的完整性，保证了源节点 S 能够使用正确无误的路由路径与目标节点 T 进行通信。而且在路由请求消息中通过序列号 seq 字段的唯一性和时戳 T_{cnt} 字段能够防止中间人攻击和重放攻击。

3.2 可靠性分析

从多条路径之间的关联关系可以把多路径分为链路分离多路径和节点分离多路径，如图 2、图 3 所示。

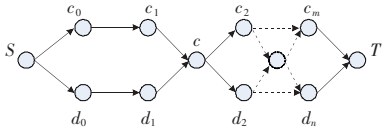

图 2 链路分离多路径 LMP

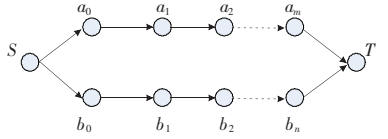

图 3 节点分离多路径 NMP

本文所提出的是一种节点分离多路径路由。在无线 Mesh 网络中，活动路径断开的主要原因是由于网络节点的频繁移动导致网络拓扑结构发生变化而引起的。下面从概率角度来分析在节点移动所引起的链路断开情况下，节点分离多路径相比链路分离多路径所体现出的优越性能。

假设图 2 的链路分离多路径 LMP 由路径 $P(S,c_0,c_1,c,c_2,\cdots,c_m)$ 和 $P(S,d_0,d_1,c,d_2,\cdots,d_n)$ 组成，图 3 的节点分离多路径 NMP 由路径 $P(S,a_0,a_1,a_2,\cdots,a_m)$ 和 $P(S,b_0,b_1,b_2,\cdots,b_n)$ 组成。下面就 LMP 和 NMP 两种多路径分别做稳定性分析并加以比较。

为了分析结果的通用性和分析的方便性，基于 Mesh 结构中各个节点之间的对等性做如下假设：

网络中每个节点在单位时间内移动的平均概率为 p，则对于一条由 k 个节点组成的路径 $P(n_0,n_1,n_2,\cdots,n_k)$，其路径断开出错的概率为：

$$P_{discon}=1-(1-p)^k \tag{1}$$

其路径正常连通的概率为：

$$P_{connet}=(1-p)^k \tag{2}$$

在一组多路径中，可以设两条路径之间的公共节点数为 i，因为可以把多路径表示成 MP_i，当 $i\geqslant 1$ 时，即为链路分离多路径，当 $i=0$ 时，即为节点分离多路径。下面分别就 i 取不同的值来分析图 2 和图 3 所示的多路径的可靠性。对多路径 MP_i 的可靠性，分析以下两种情况发生的概率：

(1)定义多路径 MP_i 包含的两条路径中有路径断开的概率为 $P_{part}(MP_i)$；

(2)定义多路径 MP_i 包含的两条路径都断开的概率为 $P_{all}(MP_i)$。

先对第一种情况进行分析：

当 $i=0$ 时，为图 3 的情形：

$$\begin{aligned}P_{part}(MP_0)&=p[P_{discon}(a_0,a_1,\cdots,a_m)\cup P_{discon}(b_0,b_1,\cdots,b_n)]=\\&1-p[P_{connet}(a_0,a_1,\cdots,a_m)\cap P_{connet}(b_0,b_1,\cdots,b_n)]=\\&1-(1-p)^{m+n}\end{aligned}$$

当 $i=k(1\leqslant k\leqslant m,n)$ 时，为图 2 的情形：

$$\begin{aligned}P_{part}(MP_k)&=p[P_{discon}(c_0,c_1,\cdots,c_m)\cup P_{discon}(d_0,d_1,\cdots,d_n)]=\\&1-p[P_{connet}(c_0,c_1,\cdots,c_m)\cap P_{connet}(d_0,d_1,\cdots,d_n)]=\\&1-(1-p)^{(m+n)-k}\end{aligned}$$

由此可以得到

$$P_{part}(MP_0)>P_{part}(MP_k) \tag{3}$$

即随着 i 值的增大，$P_{part}(MP_i)$ 值在减小。

下面对第二种情况进行分析：

当 $i=0$ 时，为图 3 的情形：

$$\begin{aligned}P_{all}(MP_0)&=p[P_{discon}(a_0,a_1,\cdots,a_m)\cap P_{discon}(b_0,b_1,\cdots,b_n)]=\\&[1-(1-p)^n][1-(1-p)^m]\end{aligned}$$

当 $i=k(1\leqslant k\leqslant m,n)$ 时，为图 2 的情形：

$$\begin{aligned}P_{all}(MP_k)&=p[P_{discon}(c_0,c_1,\cdots,c_m)\cap P_{discon}(d_0,d_1,\cdots,d_n)]=\\&[1-(1-p)^{n-k}][1-(1-p)^{m-k}]+kP\end{aligned}$$

通过以上计算推理得出

$$P_{all}(MP_k)\geqslant P_{all}(MP_{k-1})\geqslant\cdots\geqslant P_{all}(MP_0) \tag{4}$$

经过以上的理论分析，由式(3)和式(4)可以得出如下结论：

(1)在多路径路由中，各路径之间公共节点数越多，则有路径断开的概率就越小，而所有路径都断开的概率就越大；

(2)在多路径中，各路径之间的公共节点数目越少，则有路径断开的概率就越大，而所有路径都断开的概率就越小。

前面提到多路径路由发起策略是在当前活动路径都断开的情况下进行的，这和本文提出的节点分离多路径路由当前链路都断开的小概率性质是一致的。通过以上分析，可以得出使用节点分离的多路径路由要比链路相关的多路径路由的可靠性要高。

4 结束语

提出了一种基于认证的安全多路径路由协议 SMRPA。通过对多路径路由的安全性和可靠性的分析，SMRPA 能够实现源节点和目标节点的共享密钥的协商，验证中间节点身份的合法性，验证消息完整性。而且唯一的序列号和时戳能够阻止中间人攻击和重放攻击。当然 SMRPA 本身也存在着一些不足之处，比如认证和加解密所带来的时延问题，还有在效率和性能上还有待进一步提高的问题，这些将是以后需要研究和解决的。

(下转 133 页)