论 文

一种基于多维 DHT 空间映射的 P2P 安全拓扑方案

孙知信^{①②*}, 骆冰清^①, 陈亚当^①, 卜凯^①

^① 南京邮电大学宽带无线通信与传感网技术教育部重点实验室, 南京 210003

^② 南京大学计算机软件新技术国家重点实验室, 南京 210093

* 通信作者. E-mail: sunzx@njupt.edu.cn

收稿日期: 2011-10-11; 接受日期: 2012-12-09

国家自然科学基金 (批准号: 60973140, 61170276) 和江苏省高校自然科学研究重大项目 (批准号: 12KJA520003) 资助

摘要 基于 DHT (distributed Hash table) 的分布式检索和路由算法凭借其良好的分布性、自组织性、可扩展性等优点, 正成为国际上结构化 P2P(peer-to-peer) 网络研究和应用的热点. 但相对于传统的 C/S (client/server) 网络, P2P 网络的非中心化特点以及网络中节点较强的自治性和动态性, 使得节点实施恶意行为的可能性大大增加, 这令 DHT 对节点安全性的要求很难得到满足. 本文提出了一种基于多维映射机制的安全 DHT 协议, 该机制通过对标识符进行按组划分, 将 P2P 网络中的节点映射到一个多维空间, 并通过设计合理的路由算法, 使安全工作定位到相对简单的节点区域内进行. 理论分析和实验结果表明, 本机制能够简化现有 DHT 安全机制, 有效抑制恶意路由行为, 提高资源搜索成功率.

关键词 多维映射 分布式 Hash 表 结构化 P2P 网络 路由攻击 安全

1 引言

DHT (distributed Hash table, 分布式 Hash 表)^[1] 是研究和实现结构化 P2P (peer-to-peer, 点对点) 网络的关键技术, 它使用分布式 Hash 算法来解决结构化的分布式存储问题. 在采用 DHT 技术的 P2P 网络中, 节点 (peer) 和资源分别通过 Hash 计算得到, 相对于其他节点与资源唯一的标识符 (identifier), 其最突出的特点是节点并不需要记录整个网络的信息, 而是仅存储与自身标识符有特定关系的节点以及资源信息, 并根据相应的特定关系实现资源搜索, 从而取消了非结构化 P2P 网络中的泛洪算法, 提高了路由效率并降低了路由带来的网络开销. 基于 DHT 的分布式检索和路由算法, 凭借其良好的分布性、自组织性、可扩展性等优点, DHT 技术正成为国际上结构化 P2P 网络研究和应用的热点. 目前, 基于 DHT 的结构化 P2P 网络研究领域中具有代表性的研究项目主要包括 MIT (Massachusetts Institute of Technology, 麻省理工学院) 的 Chord, 微软研究院的 Pastry, 以及 UC Berkeley (University of California, Berkeley, 加州大学伯克利分校) 的 CAN, Tapestry 等.

但是, DHT 机制正确运行的前提是系统中的节点是可信任的, 即对节点的安全性有较高的要求.

引用格式: 孙知信, 骆冰清, 陈亚当, 等. 一种基于多维 DHT 空间映射的 P2P 安全拓扑方案. 中国科学: 信息科学, 2013, 43: 343–360

而相对于传统的 C/S (client/server) 网络, P2P 网络的非中心化特点以及网络中节点较强的自治性和动态性, 使得节点实施恶意行为 (malicious behaviour) 的可能性大大增加, 这令 DHT 对节点安全性的要求很难得到满足. 文献 [2,3] 总结了结构化 P2P 网络中节点可能实施的恶意行为, 包括恶意节点 (malicious node) 可能通过不正确的路由转发或不正确的路由更新发动路由攻击导致受攻击节点不能正常享受 P2P 网络服务; 恶意节点也可能在正确执行查找协议之后否认自己保存该数据, 或宣称自己保存这些数据, 但却拒绝提供这些数据; 恶意节点可能对网络中不同的节点表现不一致的行为 (对一部分节点进行攻击, 同时对一部分节点表现正常状态) 来躲避节点安全审查机制等.

本文针对 DHT 所存在的主要安全问题, 提出了一种基于多维空间映射机制 (multidimensional mapping mechanism) 的安全 DHT 协议. 该机制通过对节点标识符 (nodeId) 进行按组划分, 将 P2P 网络中的节点映射到一个多维空间, 并通过设计合理的路由算法, 使安全工作定位到相对简单的节点区域内进行, 简化现有 DHT 安全机制, 有效抑制恶意路由行为, 以实现高成功率的资源搜索.

2 安全 DHT 相关研究

结构化 P2P 技术出现以来, 大多数的研究工作都致力于如何提高系统的稳定性与搜索效率, 但是, 没有采取严密的攻击防御措施的系统可能会受到恶意攻击行为的威胁, P2P 网络也不例外 [3]. 目前国内针对结构化 P2P 的 DHT 安全问题的研究主要集中在以下几个方向.

2.1 冗余路由机制

文献 [4] 在总结分析结构化 P2P 路由安全问题时提出了为一次资源搜索过程发起多条查询路径的思想, 如果恶意节点未参与到所有的查询路径中, 则可认为本次资源搜索操作没有被恶意路由行为干扰.

文献 [5] 提出了两种方法来通过冗余路由机制实现安全路由, 其中递归 Hash 函数法 (recursive Hash function) 通过在多个节点上复制与查询信息对应的查询发起节点 (lookup originator), 所查询资源的标识符 (lookup key) 以及相应的路由表来为针对被复制的资源标识符的查询信息提供多条不同的查询路径; 而查询委托法 (lookup delegation) 则要求查询信息发起节点同时将查询信息发送至多个邻居节点, 然后由这些邻居节点分别发起查询信息的路由操作.

文献 [6] 则通过对覆盖网络拓扑结构进行改进使得任意两个节点之间都有多条独立, 不交叉的路径, 以此支持查询信息的冗余路由. 文献 [7] 所提出的冗余路由方法中, 参与到路由路径中的每个节点都选择多个合适的节点作为下一跳节点, 同时在下一跳节点的选择过程中也引入了一定的筛选机制排除已被其他节点反馈为不可信任的节点.

文献 [8] 为每个节点增加一个存储部分邻居节点信息的表格, 并引入宽路径 (wide path) 查询机制, 在路由过程中结合所存储的邻居节点信息构建多条路径, 仅当多条路径中同一级节点失效时导致查询失败, 提高了系统对恶意节点的免疫能力, 但是该方案要求节点与个其他节点的链接, 同时将查询消息的复杂度也提高到了 $\Omega(\log^2 N)$.

文献 [9] 在冗余路由的基础上采用了加密信息消息的方法, 其为每条路由分配一个密钥 key, 由发送端和目的端进行保护, 甚至某些中间可信节点也可以参与, 并且结合了某节点的需求和自身行为进行评判, 评判规则依然类似于依赖邻居节点的局部信任度评价方法.

2.2 节点认证机制

节点认证机制的主要思想是将传统网络中的认证中心 (certificate authority, 简称 CA) 技术应用到 P2P 网络中的节点安全管理, 通过一定的认证措施确保节点之间通信安全性。

文献 [10] 所提出 Myrmic 协议在离线 CA (off-line CA) 的基础上, 引入了新的在线 (on-line) 认证中心 NA (neighborhood authority, 邻居授权), 在节点加入或退出时, NA 通过给一些相关节点发布邻居证书 (neighborhood certificate) 的方式参与 DHT 的网络管理. Myrmic 允许执行查询操作的节点根据查询结果的邻居节点所储存的该节点的邻居证书副本, 对查询结果进行检验, 防止恶意节点的不正确路由操作, 但这却为每次查询操作引入了 2l 条 (邻居证书副本总数) 验证消息的通信开销. 对于 NA 失效问题, 系统规定在 NA 离线时, 新的节点可以暂时通过系统中已获得邻居证书的节点进行资源搜索, 但不能加入该网络, 这将进一步增加全局路由更新的延迟, 而 CA, NA 的引入也在一定程度上影响了 P2P 网络的分布性和非中心性。

文献 [11,12] 提出的基于分布式 CA 的认证方案在联合的恶意节点数目过多时会导致整个系统陷入信任危机, 而且这些认证方案同样存在着证书获取与撤销等难题, 因此不适用于节点认证这一类对安全性有较严格需求的应用场景. 文献 [13] 则提出利用单向累积函数实现分布式网络的认证, 借助单向累积函数的特性, 节点间可直接实现相互认证, 但是该协议仍存在与文献 [11,12] 类似的缺点, 且新加入的节点成为中心计算节点 CCA (central computing authority) 的策略使得单个恶意节点便可严重危害网络安全. 文献 [14] 在文献 [15,16] 的基础上提出了安全动态累积函数的概念。

文献 [17] 针对无线网络的低安全性以及网络中节点易被攻击的特性, 提出了一种基于公共基础键值 (PKI) 的方式去弥补节点过于灵活, 难于管理等问题, 文章建立了基于 PKI 架构的模型, 在认证节点上只需很少的系统资源就可对 public key 进行编码, 使更多不同分布网络下的不同主机进行安全通信. 其最大优点是在于认证节点不需要存储所有节点的原始信誉度, 从而一定程度上节省了自己内存, 但其架构与传统认证节点机制并无太大变化, 造成过于中心化。

文献 [18] 基于安全动态累积函数提出了一种称为 CIADA (central identity-code assignment and distributed authentication, 身份认证码统一发放和分布式认证) 的安全认证方案, CIADA 弥补了上述文献中的不足, 有效地实现了节点间的交互认证, 节点的动态加入与删除, 并且支持域间认证以及域的合并, 但其引入认证中心的实质同样有悖于 P2P 技术有别于传统网络模式的非中心化特点。

2.3 信誉度机制

Douceur 在文献 [19] 中定义并阐述了 Sybil 攻击的概念, 当 P2P 网络中潜伏着大量恶意节点并且网络中没有验证节点身份的认证中心时, 系统便容易遭受 Sybil 攻击. 文献 [20] 提出信誉度机制对 Sybil 等路由攻击进行防御, 信誉度机制又称信任度机制, 它通过采取一定的措施为网络中的节点维护相应的信誉度 (或可信度), 并以节点信誉度作为路由操作过程中路由转发, 路由安全验证的主要依据。

文献 [21,22] 对常见的基于 P2P 环境的信任模型进行归纳并分析, 参考人际网络中的基于推荐的信任关系建立方法是比较合理的研究手段, 全局可信度模型就是基于这个思想, 通过邻居节点间相互满意度的迭代来获取节点的全局可信度。

文献 [23] 提出了基于分布式信任管理的信誉度模型并在此基础之上引入了时间域的概念去描述节点交互经历与评价的时间特性. 其中长期时段信誉度以及较短时段信誉度都将作为节点的最终信誉评价依据. 其优点在于应对具有多样性, 易变性的恶意路由行为. 但是这种方法的负面问题在于把时间域作为它的描述因素, 难以达到最佳效果。

文献 [24] 根据节点上载文件的历史记录为其分配一个唯一的全局信誉度 (global reputation value), 当节点 i 需要了解任意节点 k 的全局信誉度时, 首先从与 k 发生过交易的节点处获知节点 k 的信誉度信息, 然后根据这些交易伙伴自身的信誉度综合计算出 k 的全局信誉度. 但该模型对造成服务失败的节点没有设置相应的惩罚机制, 这意味着节点实施恶意行为后其全局信誉度短期内并不会明显下降, 导致这段时期内该模型不能真实反映节点可信任的程度. 另外, 每次交易所引起的全网范围内的迭代, 也势必对网络性能带来一定的影响.

上述 3 种典型安全路由技术中, 存在一些缺点:

- 冗余路由机制通过发起多条搜索路径来防御恶意路由攻击是以牺牲路由开销为代价的, 查询路径数目越多, 对网络带宽资源的负担就越重. 而且冗余路由机制提高结构化 P2P 路由安全性能的一个关键因素就是确保能够在多条查询路径所得返回信息中选择正确结果, 即要求为最终查询结果的确定引入严密有效的检验机制, 这进一步加大了有效控制冗余路由机制对路由效率产生影响的难度.

- 节点认证机制则过于中心化, 一旦认证节点被攻击或者瘫痪, 则造成的后果不堪设想. 虽然目前已有许多减轻认证节点负担和动态化认证节点的思想, 但其对于复杂的动态化网络环境来看, 适应度并不大. 这将进一步增加全局路由更新的延迟, 而在一定程度上影响了 P2P 网络的分布性和非中心性.

- 基于信誉度机制的结构化 P2P 路由安全机制除了存在实现开销较大, 信任模型不易建立等局限 [25] 之外, 在信任模型中引入的报告机制 (或反馈机制) 也为恶意节点进行故意提供较低的评价值诋毁正常节点信誉度, 或提供较高的评价值提升与其联合的其他恶意节点的信誉度等恶意行为提供了可能.

除上述缺点以外, 现有路由安全研究方案同时还在一些方面表现出一定的局限性.

首先, 现有路由安全机制一般仅针对某一类 DHT 协议, 缺少适用于多种 DHT 协议的一般性. 所采用的拓扑结构不同, DHT 协议所设计的路由算法也具有较大差别, 例如路由表的结构, 路由转发规则等都因拓扑结构的不同而异. 一般的针对结构化 P2P 路由安全问题的研究方案仅仅适用于特定的 DHT 协议, 且大多以 Chord 或 Pastry 为研究重点, 缺少与 DHT 协议所采用拓扑结构独立的, 能够适用于多种 DHT 协议的安全机制.

其次, 现有研究方案中针对标识符不均匀分布 (non-uniformly distributed) 的 DHT 协议所提出的安全机制比较缺乏. 对于传统的基于对数形式的结构化 P2P, 节点在执行路由操作时根据路由表记录的对应自个节点区域内的节点信息将查询信息转发至与所查询资源的标识符最为接近的节点, 但是, 对于一些面向数据的 (data-oriented) P2P 应用, 资源标识符之间的排序或接近度等语义关系对信息检索等复杂的语义数据处理操作的支持则更为关键.

本文所提出的基于多维 DHT 的结构化 P2P 路由安全机制可解决目前典型研究方案中存在的一些缺陷, 同时旨在改善路由安全机制的一般性及可扩展性, 通过设计与具体拓扑结构无关, 可直接供路由算法调用, 与整个路由过程相关的一整套安全机制来提高结构化 P2P 的路由安全性能.

3 多维映射机制

本节首先对典型的恶意节点行为进行举例分析, 然后在此基础上引出多维映射机制及其提高 DHT 安全性的具体原理及相关措施.

3.1 恶意路由例析

为了满足结构化 P2P 网络对可扩展性 (scalability)、可维护性 (maintainability) 以及发现算法效

图 1 DHT 恶意路由攻击示例

Figure 1 The example of attack from DHT Malicious routing

率的要求, DHT 协议规定每个节点仅存储网络中少数节点的信息, 这导致了节点因网络全局信息的匮乏而易于受到恶意路由攻击。

图 1 列举了几种可能的路由攻击方式, 其中节点 Q 发出搜索 key 为 k 的查询信息 (Search k), 节点 B 负责存储 k 的相关信息, 节点 A 为当前网络状态下该查询信息的正确路由路径中节点 B 的直接前驱节点。当节点 A 将查询信息正确路由至节点 B , 如果节点 B 属于恶意节点, 它可能 ① 否认自己存储 k 相关信息, 丢弃该查询信息并返回查找失败信息; ② 否认自己存储 k 相关信息并继续将查询信息路由至下一节点 C , 由 C 或其后继节点返回查找失败信息。如果节点 A 本身就属于恶意节点, 则可能 ③ A 丢弃该查询信息并返回查找失败信息; ④ A 将该查询信息错误路由至正确目标节点范围之外的节点, 最终由收到该查询信息的节点返回查找失败信息。

对上述几种可能的路由攻击进行分析, 不难发现其根本原因是每个节点仅存储少数节点信息而导致节点之间信息透明性非常有限。如果节点 Q, A, C 能够获得节点 B 所存储的 keys 相关信息, 则 B 便不能成功实施诸如 ①, ② 的恶意行为; 如果 Q, C 能够获得节点 A 所存储的 keys 相关信息, 那么诸如 ③, ④ 的路由攻击也不能得以成功进行。但 P2P 网络中节点数目众多, 加入和退出操作频繁使得大范围内节点信息共享难以实现, 本文提出的多维映射机制, 将节点信息共享问题归化到相对较小的节点区域内, 使 DHT 安全机制得以简化。

实际上, 根据上面所述, 空间映射机制将路由操作逐渐转化到相对较小的节点空间内进行, 这样能够使得路由效率和安全性得以改善, 其根本原因是通过缩小节点空间范围而提高节点之间的信息透明度 (peers information transparency)。所谓节点信息透明度是指一个节点对于相同节点空间中节点信息了解的程度, DHT 主要通过令节点保存路由表 (routing table) 来实现对节点空间中部分节点信息的共享, 这样通过本文的某些检验与定位机制算法, 在发现路由过程中检测路由的正确性, 节点的安全性。

后续内容将详细阐述所提出的多维映射机制。这里先对多维映射机制做个简单概述, 当空间转换条件满足时, 原节点空间 S_1 (节点标识符 $p_{1i} \in \{p_{10}, p_{11}, \dots, p_{1(n-1)}\}$, 其中 n 为该节点空间所能容纳的最大节点个数) 中与剩余路由操作相关的部分节点 $p_{1i} \in \{p_{1a}, p_{1(a+1)}, \dots, p_{1b}\}$ 映射到一个相对较小的独立节点空间, 其节点标识符 $P_{2i} \in \{P_{20}, P_{21}, P_{22}, \dots, P_{2(m-1)}\}$, 其中 m 为所能容纳的最大节点个数且 $m = 2^{\lceil \log_2(b-a+1) \rceil}$ 。

如图 2 所示, 原节点空间 S_1 中节点 Q_1 发出资源查找请求 (lookup message), 该请求被转发至节点 P_1 时, 空间转换条件满足, P_1 启动空间转换机制, 将自己连同与剩余路由操作相关的一部分节点

图 2 多维映射机制原理

Figure 2 The principle of multidimensional maps mechanism

重新规划并映射成一个相对较小的独立节点空间 S_2 , 节点 P_1 继续在空间 S_2 中路由该资源查找请求. 当节点 P_3 收到该请求时由于空间转换条件满足再次启动空间转换机制并在新的空间 S_3 中完成本次资源搜索操作. 从图 2 可以形象的看出每一次空间转换机制的成功执行都将剩余路由操作转换到一个相对较小的节点空间内继续进行, 其中 S_4 是另一条由节点 Q_2 发起的路由路径中节点 P_2 运行空间转换机制所得到的节点空间. 从而, 多维映射机制能够简化现有 DHT 网络, 实现之前所述的安全 DHT 所需要的理想状态.

3.2 多维空间划分

结构化 P2P 网络中, 节点 (资源) 均被赋予相应的标识符, 这些标识符是通过一定的 Hash 函数计算得到的整数, 长度相等并且每个节点 (资源) 对应的标识符具有全局唯一性, 即同一结构化 P2P 网络中的节点 (资源) 标识符互不相同. 资源标识符为 key 的资源在网络中的分布信息由节点标识符与 key 相等或最为接近的节点负责存储, 而成功的搜索是指网络中存在搜索资源时, 查询信息能够正确路由到负责存储该资源的相关节点, 并由该节点返回其相关信息. 本文通过对节点 (资源) 标识符进行分组 (规则 1), 并提出相应的映射机制实现多维空间的划分 (规则 2).

规则 1 标识符分组: 设标识符长度为 n bits, 将其划分成 m 组, 每组对应的长度为 p_i bits, 其中 $i \in [1, m]$, 即满足公式 $\sum_{i=1}^m p_i = n, (1 \leq i \leq m)$.

规则 2 多维空间映射: 第 i 维空间对应标识符组 $[p_i, \dots, p_m]$, 即第 i 维空间所包含节点个数 $s_i \leq 2^{n - \sum_{j=1}^{i-1} p_j}, (1 \leq i \leq m)$ 或 $s_i \leq 2^{\sum_{j=i}^m p_j}, (1 \leq i \leq j \leq m)$.

下面结合图 3 对规则 1 和规则 2 进行解释.

为了将节点映射至相对较小的区域, 进而简化 DHT 安全机制, 我们首先对标识符进行分组操作, 令第 i 组对应的长度为 p_i bits, 其中 $i \in [1, m]$, m 为对标识符划分所得到的总组数. 然后按照映射空间对应的节点范围逐渐缩小的原则, 为映射空间分配个数递减的标识符组, 第 i 维空间对应标识符长

图 3 多维映射机制原理

Figure 3 The principle of multidimensional maps mechanism

度为 $n - \sum_{j=1}^{i-1} p_j (1 \leq i \leq m)$ 或 $\sum_{j=i}^m p_j (1 \leq i \leq j \leq m)$, 进而第 i 维空间对应的 nodeId 范围为 $(\text{currentId}, \text{currentId} + 2^{n - \sum_{j=1}^{i-1} p_j}) (1 \leq i \leq m)$ 或 $(\text{currentId}, \text{currentId} + 2^{\sum_{j=i}^m p_j}) (1 \leq i \leq j \leq m)$ (currentId 为启用空间映射机制的节点的 nodeId). 另外, 第 1 维空间 ($i=1$) 对应完整的标识符, 即初始 P2P 拓扑空间. 第 m 维空间也称为最终维度空间, 当 $m=1$ 时, 代表未对标识符进行分组操作, 此时 P2P 拓扑结构相当于传统 DHT.

3.3 快速定位及初始安全路由检验机制

为了有效控制多维映射机制引入的路由开销, 即降低查询信息路由过程中相对于传统 DHT 所增加的步数 (hop count), 第 1 维空间内仍采用传统 DHT 路由机制. 如采用 Chord 路由算法, 则第 1 维空间中节点的路由表将第 1 维空间所对应的一维圆环分割成 n 个区域, n 即标识符的长度, 与 P2P 网络在线节点个数 N 应满足关系式 $n = \text{floor}(\log N)$ (floor 为上取整函数). 其中第 i 个区域所对应的标识符范围为 $[(\text{nodeId} + 2^{i-1}) \bmod 2^n, (\text{nodeId} + 2^i) \bmod 2^n) (1 \leq i \leq n)$, 并选取该范围内第一个在线节点做为路由至该区域中查询信息的下一跳 (next hop) 节点. 资源标识符为 key 的共享资源在网络中的分配信息由第一个满足 $\text{nodeId} \geq \text{key}$ 的节点负责存储.

在此基础上, 我们提出了初始安全路由检验机制 (initial secure routing inspection mechanism) 以避免传统 DHT 路由过程中存在的安全问题. 节点利用初始安全路由检验机制对所接收到的查询信息进行路由正确性验证并将其作为判断路由该查询信息的前一跳节点安全性的依据, 传统 DHT 协议中, 当节点接收到上一跳节点转发的资源查询信息时, 如果自身的标识符仍处在当前路由算法下发起资源查询的节点对应的标识符与所查询资源对应的标识符范围之间, 则按照上一跳节点所采用的下一跳节点选择方法将资源查询信息继续向后路由. 而如果节点目前已经落在上述标识符对应的节点区域之外, 则视本次资源搜索失败, 并向发起资源搜索操作的节点返回查询失败信息. 由此不难看出, 传统 DHT 协议所设计的路由算法为了满足结构化 P2P 对大型动态网络环境下路由效率的要求, 却忽略了一些对路由正确性必要的检查, 使得传统 DHT 协议的路由操作易于受到恶意节点实施的路由攻击.

图 4 列举了一种简单的错误路由现象, 节点 A 发出对资源 key 的查询信息, 并将该查询信息转发至节点 B. 当前网络环境下, 资源 key 在网络中的分布信息由节点 C 负责存储, 如果节点 B 在路由表已按当前网络状态进行过更新操作, 却把该查询信息路由转发至节点 D, 导致节点 D 返回给 A 查询失败信息, 则可说明节点 B 在此步路由操作中实施了恶意路由攻击. 此处值得注意的是, 仅根据节点 B 至节点 D 这步错误路由操作并不能简单的将节点 B 判断为恶意节点, 如前所述, 节点未正确选择下一跳节点 C 可能是由于其未及时将节点 C 的状态更新至其路由表中. 这也是本文在 DHT 安全路由问题解决方法的研究过程中没有引入报告机制的主要原因. 而且, 引入报告机制必须同时给出严密有效的报告检验机制, 否则就会存在恶意节点通过发送虚假的报告诬陷正常节点的隐患. 本文首先

图 4 错误路由示例

Figure 4 The example of wrong routing

图 5 初始路由安全检验机制

Figure 5 Security check mechanism of initial routing

引入初始路由安全检验机制用以节点对所接收到的查询信息进行正确性的验证。

规则 3 初始路由安全检验机制, 如图 5 所示: 令 Q, C, K 分别表示最初发起资源搜索操作的节点 (querier), 当前接收到上一跳节点 P (previous node) 转发来的查询信息并进行路由安全性检验的节点以及当前网络状态下负责存储所搜索资源 key 分布信息的节点, 则节点 C 对 P 所进行的路由操作进行如下安全检验及处理:

- 1) 节点 C 首先检查自己是否存储 Q 所查询资源 key 对应的信息, 如果是, 则向 Q 返回资源信息, 并结束本次路由搜索操作, 否则, 至 2);
- 2) 根据当前 DHT 协议的路由算法, 如果当前维度空间内 (即节点 C 尚未满足空间转换判决条件) 节点 C 处于节点 P 与节点 K 所构成的路由路径范围内, 则 C 继续该查询信息的路由转发操作, 并令下一跳节点 N (next hop node) 正式成为 C 至 1); 否则, 至 3);
- 3) 节点 C 根据自身路由表检查在 K 与 C 所构成路由路径范围内, 是否有合适的目标节点 D (destination), 如有则至 4), 否则至 5);
- 4) 节点 C 将查询信息转发至 D , 如在规定时间内能够成功收到节点 D 返回的响应信息, 则 D 正式成为下一个当前节点 C , 并至 1) 进行同样的路由安全检验操作; 否则, 至 5);
- 5) 节点 C 根据自身路由表检查在 P 与 K 所构成的路由路径范围内, 是否有合适的“上一跳节点” P' , 如有则至 6), 否则至 7);
- 6) 节点 C 将查询信息转发至 P' , 如在规定时间内能够成功收到节点 P' 返回的响应信息, 则 P' 正式成为下一个当前节点 C , 并至步骤 1) 进行同样的路由安全检验操作, 否则至 7);
- 7) 节点 C 判断空间转换条件是否满足, 并根据判断结果决定是否转化到另一维度空间中进行剩余路由操作.

3.4 空间转换机制

令启动空间转换机制的节点对应节点标识符为 ID_1 , 且其通过空间转换判断规则 (规则 5) 所确定的转换空间另一界限相关节点的标识符为 ID_2 , 则由转换机制所得到的节点空间维度 i 遵守规则 4.

规则 4 空间转换机制: $\sum_{j=i+1}^m p_j \leq \lceil \log_2((ID_2 + N_1 - ID_1 + 1) \bmod N_1) \rceil \leq \sum_{j=i}^m p_j$, ($1 \leq i \leq m$), 其中 N_1 为启动空间转换机制前所对应的节点空间规模, i 就为所转换到的空间维数.

此处之所以称 ID_2 为界限相关节点, 是因为 ID_2 是节点 ID_1 在运行基于多维映射机制的 DHT 安全路由算法且当空间转换条件满足时, 根据查询信息对应的资源标识符 key 以及自身路由表中所维护的其他节点信息而选取的与根据标识符分组方法以及空间转换规则确定的新节点空间的规模相关的节点. 也就是说, 新节点空间规模 N_2 必须满足 $N_2 \geq (ID_2 + N_1 - ID_1 + 1) \bmod N_1$ 才能确保将负责保存资源 key 在 P2P 网络中分布信息的节点包括到所转换的节点空间内, 以保证剩余路由操作能够实现正确的查找, 而 ID_2 是否恰好与新节点空间的另一界限节点标识符相等则与 ID_1 及所转换至的空间维度 i 有关. 能够容纳 $(ID_2 + N_1 - ID_1 + 1) \bmod N_1$ 个节点的节点空间所对应的标识符长度 l 应满足 $l \geq \lceil \log_2((ID_2 + N_1 - ID_2 + 1) \bmod N_1) \rceil$ bits, 则根据标识符分组规则, 与 l 最符合的标识符组集合 $\{p_i, p_{i+1}, \dots, p_m\}$ 应满足 $\sum_{j=i+1}^m p_j \leq l \leq \sum_{j=i}^m p_j$, ($1 \leq i \leq m$), 而 i 即这部分标识符组根据空间映射规则 (规则 2) 所对应的空间维度. 可见, 只有当 $((ID_2 + N_1 - ID_1 + 1) \bmod N_1) \bmod 2 = 0$ 时, ID_2 本身才恰好属于新节点空间的另一界限节点.

规则 5 空间转换判断规则: 当处于第 i 维空间内的节点 C, K 之间的拓扑距离 $D(C, K)$ 已经符合第 $i+1$ 维或更高维节点空间的规模, 便启动空间转换机制, 将剩余部分路由操作转化至相对较小的高维度空间中进行, 在节点之间信息透明度较高的网络环境下结合一定的路由安全机制使资源查询操作的正确性得到保障. 即满足公式 $D(C, K) \leq N(i+1)$, $1 \leq i \leq m-1$.

其中 C, K 所代表的意义与规则 3 中相同, $D(C, K)$ 表示当前所处维度空间内根据所采用的 DHT 协议的拓扑结构及其路由算法由节点 C, K 所构成的路由路径区域上两节点之间的拓扑距离, 也即相当于当前维度节点空间中可以最多落在二者之间的节点个数. $N(i)$ 则代表第 i 维节点空间的规模, 由

于对于映射至第 m 维空间的路由操作不再需要进一步的空间转换, 所以 i 的限定范围为 $[1, m-1]$.

3.5 最终维度空间路由

根据前面的阐述, 本文依次给出了基于多维映射机制的 DHT 在资源查询信息的路由过程中采用的一些安全机制, 相对于传统 DHT 的路由算法, 本文所采用的路由机制因对路由正确性的检验及纠正措施延后了资源搜索失败信息的返回, 本小节主要介绍采用多维映射机制的结构化 P2P 网络中如何确定资源查询的最终结果.

对于本文所采用的安全路由机制, 一般情况下资源的查询结果由映射至最终维度空间内路由操作确定. 根据多维空间划分及映射方法, 相对于其他维度空间, 最终维度空间所对应的节点区域范围最小, 而 DHT 协议路由算法为满足结构化 P2P 网络的可扩展性以及资源搜索的高效性所具备的一个特点就是节点的路由表中与该节点具有相对较近拓扑距离的节点信息占有较大比重, 这样, 便可以结合最终维度空间的规模引入一定的辅助手段实现最终维度空间内节点信息的全部共享, 进而达到一步路由操作确定资源查询结果的目的.

规则 6 最终维度空间全局信息共享机制: 最终维度节点空间中, 节点根据最终维度空间规模 N_2 , 路由表中对应最终维度空间内节点集 S_1 , 邻居节点集中对应最终维度空间内节点信息 S_2 实现对节点之间信息透明度的最大化.

为了维护 P2P 网络的稳定性 (stability), DHT 路由算法设计过程中, 除了在节点的路由表中保存利于路由算法选择下一跳节点的部分节点信息之外, 还要保存一个包含一定数量邻居节点的信息集 S . 当节点探测到路由表中的某个邻居节点 P 失效时, 便从 S 中选择合适的节点更新失效邻居节点 P' 对应的路由表项, 继而完成全局路由更新操作, 即利用 P' 替换整个 P2P 网络中节点路由表中节点 P 对应的路由表项. 根据规则 6, 本文基于多维映射机制的 DHT 在最终维度空间内的路由操作也同时将邻居节点信息集 S 等效成另一张路由表供节点在路由查询信息时直接使用, 这样, 参与到最终维度空间内路由操作的节点在全局信息的基础之上, 便可根据规则 7 经过一步路由将查询信息转发至初始目标节点.

规则 7 一步路由机制: 最终维度节点空间中, 节点根据所采用 DHT 协议资源分布信息的存储规定, 将资源查询信息直接转发至最符合该规定的节点, 并将其作为初始目标节点.

规则 7 之所以把一步路由机制所选择的节点暂时作为初始目标节点, 而不是作为本次资源搜索的最终结果, 仍然是为了保证查询结果的正确性所提出的进一步保障措施. 下面首先通过规则 8 给出相关的安全检验机制, 然后在最终路由安全检验机制解释的过程中介绍最终查询结果的确定方法.

规则 8 最终路由安全检验机制: 最终维度节点空间中, 节点根据一步路由机制选择初始目标节点 init-resultID 时, 同时在全局信息中挑选同维度空间中另一节点 assistantID , 且 assistantID 一步路由操作的结果为 $\text{init-resultID}'$. 发起资源查询信息的节点最终在 init-resultID 与 $\text{init-resultID}'$ 所返回的信息中确定查询结果.

考虑到恶意路由攻击以及前面讨论过的节点之间路由表更新不同步的问题, 规则 8 在最终资源查询结果的确定过程中特别引入一个辅助节点 assistantID 也同时执行最终维度空间一步路由操作, 由 assistantID 的查询结果 $\text{init-resultID}'$ 与初始目标节点 init-resultID 构成双重保证, 发起查询信息的节点根据 init-resultID 与 $\text{init-resultID}'$ 对应的返回信息来决定本次资源查询操作的最终结果. 为了更进一步保证路由查找的正确性, 发起资源搜索的节点在接收到 init-resultID 和 $\text{init-resultID}'$ 返回的查询结果时可以与最终维度空间中负责选择初始目标节点以及辅助节点的那个节点进行一定的联合检验

机制, 进而提高在两个返回结果中选择符合当前网络状态结果的效率, 这一问题也是本文在将来后续研究工作中主要分析的要点之一.

另外, 当查询过程中没有节点实施恶意路由行为, 且所查询的资源确实不存在于当前网络空间中时, 传统 DHT 路由算法在这种情况下负责返回查询消息的节点与资源标识符 key 等值节点, 本文所提机制负责开启最终维度空间一步路由机制的节点具有相对较近的拓扑距离, 且都被映射至最终维度空间拓扑范围之内, 也就是说, 在正常查询失败的情况下, 基于多维 DHT 的安全型 P2P 拓扑结构中的路由操作比传统结构化 P2P 中基于传统 DHT 的路由操作在路由路径长度上增加了一步的跳数.

4 实验对比与分析

为了对比测试传统 DHT 与加载本文的基于安全路由的多维映射机制, 简称 3MSR 机制 (multidimensional mapping mechanism based secure routing) 的 DHT 平均查找成功率的差别, 本节先将所提方法应用到传统 chord 协议, 然后与现有典型安全方法进行对比, 具体选取冗余路由机制及信誉度机制. 因为节点认证机制的实现不符合 P2P 网络的分布性, 所以本节对比试验时不考虑该方法.

4.1 与传统 chord 协议对比分析

为了验证 3MSR 对资源查找正确性的保障效果, 本节进行加载 3MSR 机制的 DHT 与传统 DHT 之间资源搜索操作平均查询正确率的对比实验. 所谓查询正确率包含两个方面, 即对于当所查询资源确实存在于当前 P2P 网络中且查询结果成功返回该资源对应信息, 以及所查询资源在当前网络状态下不存在且查询失败的情况都是正确的.

首先, 引入 20 组各含 50 次共 1000 次模拟资源查询实验, 对于每一次实验, 首先将一个随机生成的资源 key 及其对应信息存储到适合的节点, 然后再随机选择节点 querierID 发起对 key 的查询信息, 也就是说, 当所有节点均不实施恶意路由行为时 (即节点在参与路由过程中实施恶意路由攻击行为的概率 $p = 0$, 这里 4 种恶意路由行为在恶意节点中都以等概率出现), 平均查询正确率应该基本维持在 100%. 图 6 给出了 $p = 0.2$ 时, Chord 协议在加载与未加载 3MSR 机制的情况下进行上述实验所得到的平均查询正确率对比图, 此处每组实验对应的平均查询正确率由该组实验中成功返回资源信息的次数与每组实验总次数 50 的比值计算而得.

实验过程中, 加载 3MSR 机制的 Chord 在每组 50 次的模拟资源搜索操作中, 都保证了 40 次以上的查询结果能够成功返回所搜索资源 key 对应的信息, 图 6 中其对应的平均查询正确率维持在 85% 以上. 相比之下, 未加载 3MSR 机制的传统 Chord 在参与路由的节点以概率 $p = 0.2$ 实施错误路由对正常的资源搜索进行干扰时, 平均查询正确率较预期有明显的下降, 大部分组别的平均查询正确率已经低于 80%. 从图 6 可以明显的看出, 传统 DHT 协议加载了 3MSR 机制之后, 对恶意路由攻击的防御能力有显著提高, 因此在相同的节点实施恶意路由行为的概率下, 加载 3MSR 机制的 Chord 协议相比传统 Chord 协议具有较高的平均查询正确率.

然后, 仍然选用 Chord 协议检验当节点实施恶意路由行为的概率 p 逐渐增大时, DHT 平均查询正确率所受影响的程度. 为此, 我们设计了如下实验: 对 $p \in \{0.1, 0.2, 0.3, 0.4, 0.5, 0.6, 0.7, 0.8, 0.9\}$, 为每种节点恶意实施恶意路由行为的可能分别进行 100 次模拟资源查询实验, 每次实验仍然采取上述的条件, 即对于每一次模拟实验, 随机选择一个节点 querierID 发起对已存储资源 key 的查询信息, 理论上, 如果在模拟的资源搜索过程中, 参与到查找信息路由操作的节点如果不故意进行错误的转发, 则预期

图 6 Chord 平均查询正确率对比

Figure 6 The comparison of Chord mean inquire correct rate

的平均查询正确率应该达到 100%. 为了更具体的反映平均查询正确率在节点恶意路由概率的影响下的波动情况, 对于具体概率 p 的 100 次实验, 我们将其平均分为 10 组进行, 根据每组 10 次查询实验中查询成功的次数计算得到本组实验的平均查询成功率 a_i , 恶意路由概率 p 对应的平均查询成功率则按 $A_j = 1/10 \sum_{i=1}^{10} a_i (j \in [1, 9])$ 计, 同时记录 10 组实验中 a_i 的最大值 $A_{\max j}$ 与最小值 $A_{\min j}$.

图 7(a) 根据上述 $A_j, A_{\max j}, A_{\min j}$ 给出了不同恶意路由概率 p 对应的网络环境下 Chord 加载安全机制 API 前后平均查询正确率的对比情况, 随着恶意路由概率 p 的增加, 两组实验所得到的平均查询正确率都呈下降趋势, 但相比加载了 3MSR 机制的安全 Chord, 传统 Chord 协议模拟资源搜索实验受网络环境的影响更大, 网络环境的恶化导致其平均查询正确率大幅度下降. 加载了 3MSR 机制后, 平均查询正确率受恶意路由概率增大影响的程度得到了减缓, 而且也使平均查询正确率得到提高.

同时, 随着 p 的增大, 根据 Chord 路由算法^[8]的特点, 实施恶意路由行为的节点因直接将资源查询信息转发至目标节点范围之外而导致查询失败的概率也随之增大, 而且对应的路由开销也会比正常网络环境下有所减少. 而本文中安全检验机制会增加额外的路由开销, 假设节点在参与路由操作过程中以概率 p 实施恶意路由行为, 则初始路由安全检验机制增加的路由步数平均为 $p * O(\log_2 N)$, 对于空间转换机制引起的较传统 DHT 增加的路由步数, 通过前面的讨论可知, 空间转换机制后的新节点空间一般是包括节点 key (即与查询资源具有相等标识符的节点) 且以拓扑分布在 key 两侧且具有相对最近拓扑距离的两个节点作为界限相关节点的较小区域, 即一次完整的资源查询过程中空间转换机制执行的次数非常少, 所以空间转换机制带来的额外路由开销也非常小. 如图 7(b) 所示, 当 Chord 协议在模拟实验过程中加载了本文所述 3MSR 机制之后, 随着节点实施恶意路由行为概率 p 的不断增大, 安全机制纠正错误路由而带来的较传统 Chord 额外的路由转发步数也有所上升. 虽然路由开销稍有增加, 但是提高了查找成功率、安全性. 这也是关于成功效率与消耗性能的权衡问题, 是不可避免的. 可以根据系统实际需求对其选择取舍, 其具体权衡分析工作将在今后继续深入研究.

本节首先对典型 DHT 协议加载 3MSR 机制前后进行了恶意路由防御效率的对比实验, 实验结果表明, 本文所给出的 DHT 安全路由机制能够在对路由效率产生有限影响的情况下, 提高 DHT 协议对

图 7 不同网络环境下 Chord 平均查询率对比实验

Figure 7 The comparison of Chord mean inquire rate in different network. (a) The comparison experiment of the mean right rate of inquire; (b) the comparison experiment of the mean routing overhead

资源搜索过程中节点恶意路由行为的防御能力。

4.2 与冗余路由机制的对比

本文采用如下方法模拟冗余路由机制: 为了确保将冗余机制对路由效率的影响相对降到最低, 模拟实验过程中仅设置两条查询路径, 根据文献 [5] 中委托查询方法的思想, 发起资源搜索的节点 Querier 在路由表中选取两个与自己具有最近拓扑距离的邻居节点 N_1 , N_2 , 然后将查询信息分别发送至 N_1 与 N_2 , 并由 N_1 , N_2 按照路由算法的规定完成查询信息的路由过程. 对于最终查询结果的确定采用的判断方法为: 如两条查询路径返回的查询结果 R_1 , R_2 均查找成功, 则首先对其中最符合路由算法的返回结果中对应节点实施初始路由安全检验机制 (规则 3), 如果确定其在线则以其做为最终查询结果, 否则继续对另一返回结果对应的节点执行相同操作; 如果仅有一条路由路径查找成功, 则根据其所对应节点的探测结果确定是否以该结果作为最终查询结果; 若两条查询路径均返回查询失败信息, 则直接视本次资源查询失败。

此处选取 Chord 协议为实验对象, 模拟节点空间规模为 $N = 10^5$. 正常情况下, 即节点实施恶意路由行为的概率 $p = 0$, 对模拟冗余路由机制及加载 3MSR 机制的 Chord 分别平均分 10 组进行 1000 次模拟路由实验. 图 8 为实验过程中平均查找成功率及平均路由开销的统计结果. 如图 8 所示, 当模拟网络中没有节点实施恶意路由行为时, 两者的平均查找成功率均接近理论值 0.5, 但由于冗余路由机制采用两条路由路径进行资源搜索, 故其平均路由开销维持在传统 Chord 协议平均路由开销的 2 倍

图 8 多维 DHT 安全机制与冗余路由机制对比实验 1

Figure 8 The 1st comparison between multidimensional DHT security mechanism and redundancy routing mechanism

图 9 多维 DHT 安全机制与冗余路由机制对比实验 2

Figure 9 The 2nd comparison between multidimensional DHT security mechanism and redundancy routing mechanism

左右, 而本文 3MSR 机制因增加了一些必要的安全检验措施而较传统 DHT 平均路由开销略有提高.

图 9 所描述的则是当节点实施恶意路由行为概率 $p = 0.3$ 时二者对比实验的结果, 此部分对比实

验目的是对比 3MSR 机制与冗余路由机制的路由攻击防御效果及对路由效率的影响, 所选恶意路由概率 $p = 0.3$ 仅是所述实验结果对应的实验参数, 并无特殊含义。

如图 9 所示, 当参与路由过程中的节点以概率 $p = 0.3$ 实施恶意路由行为时, 冗余路由机制会因两条查询路径受到路由攻击概率增大而导致最终查询成功的概率减小, 而本文的 3MSR 机制由于对整个路由过程都设有严格的安全检验及校正措施使得加载该安全机制的 Chord 协议较正常情况下的平均查找成功率并未表现出大幅的下降。而对于每次资源搜索操作所对应的平均路由开销, 如同与传统 DHT 的对比实验结果, 冗余路由机制的平均路由开销由于恶意节点错误路由转发直接导致的查询失败而较正常情况有所降低, 3MSR 机制则因实施对错误路由的检验及纠正措施增加了少数的路由步数。

上述对比实验结果表明了本文所提出的 3MSR 机制对恶意路由攻击不仅具有略优于传统基于冗余路由机制研究方案的防御效果, 而且更加有效地控制了安全保障措施对路由效率所带来的影响。下部分将与另一典型的路由安全方案信誉度机制进行类似的对比实验。

4.3 与信誉度机制的对比

为模拟 P2P 环境下的信任模型^[20~22], 我们对每个节点引入信任度 $r \in [0, 1]$, r 的数值越大表示节点在路由过程中可信任的程度越高。在进行具体的性能对比实验之前, 首先通过以下方法得到一个比较平稳的信任环境:

每个节点所分配的初始信任度 $r = 0.5$, 即与节点平均可信程度的理论值相等, 令节点实施恶意路由行为的概率 $p = 0.3$ (同上, 所选恶意路由概率 $p = 0.3$ 仅是所述实验结果对应的实验参数, 并无特殊含义), 在模拟资源搜索过程中调用本文安全机制对应的路由安全检验 API 判断节点所进行路由转发的正确性, 同时将判断的结果发送给所判断节点的一部分邻居节点, 接收到判断结果的节点对消息所对应节点的信任度记录进行更新操作: 如该节点进行错误路由, 则对其信任度 r 执行 $r - 0.02$ 操作, 否则执行 $r + 0.01$ 操作, 此处对执行正确路由与错误路由的节点执行不同的更新程度是为了保证信任度能够更加真实清晰地反映出节点在参与路由过程中的表现, 由于实验过程中并未不存在恶意节点诬陷正常节点的情况, 所以此处不用考虑这种情况对信任度更新的影响。另外, 信誉度机制模拟过程中调用本文所提出的路由正确性检验 API 目的是为了判断路由操作对应节点的安全性, 为信任度计算提供依据, 所以并不调用与错误路由纠正措施相关的 API。

在 3MSR 机制与信誉度机制的对比实验的过程中, 仍调用 3MSR 机制中检验路由正确性的 API 为信任度计算提供依据, 图 10 即为针对 Chord 协议平均分 10 组进行的 1000 组实验对应的实验结果, 实验所取节点实施恶意路由概率 $p = 0.3$ 。同样的实验条件下, 信誉度机制与本文 3MSR 机制具有相近的平均查询正确率, 但由于信誉度机制实现过程中引入了用以反馈节点信任度相关信息的报告机制, 节点除了发送与传统 DHT 路由算法有关的信息之外, 还要增加大量的信任度查询, 信任度报告等信息, 导致节点的通信压力也随之增加。如图 10 所示, 模拟信誉度机制的实验网络中平均每个节点每秒钟发送的消息数目多大 130 条左右, 而加载 3MSR 机制的模拟实验中此数值仅为 50 左右。

以上部分分别选取了 Chord 路由机制与信誉度机制进行与本文 3MSR 机制的对比实验, 实验结果表明, 相对于这两种典型的现有安全机制研究方案, 本文所述 3MSR 机制在对恶意路由攻击表现出良好防御效果的同时, 对路由效率影响的控制明显优于两种对比方案。

图 10 多维 DHT 安全机制与信誉度机制对比实验

Figure 10 The comparison between multidimensional DHT security mechanism and creditworthiness mechanism

5 结论与展望

本文提出了一种基于多维映射机制的新型安全 DHT, 该机制通过对标识符进行按组划分, 引入多维空间划分机制将 P2P 网络中的节点映射到一个多维空间, 并通过设计合理的路由算法, 使安全工作定位到相对简单的节点区域内进行. 实验结果表明, 本机制能够简化现有 DHT 安全机制, 在传统 DHT 基础上引入少量额外开销的情况下, 通过对恶意路由行为的有效抑制以达到提高资源搜索成功率的效果.

进一步的研究工作包括改进最终维度空间信息共享方式以减少路由表存储开销, 引入对查询信息的跟踪机制以及对反馈信息的检验机制增强对恶意节点直接丢弃查询信息的路由攻击的防御能力, 恶意路由概率的增加所产生的平均路由开销与查询的正确率之间做权衡性分析等. 其中, 跟踪机制确保跟踪记录查询信息所转发至的节点相关信息, 当发起资源搜索的节点收到查询失败的信息后, 利用跟踪机制所提供的返回查询失败信息的节点信息对失败信息的有效性进行检验, 进而检验返回失败信息的节点的安全性.

参考文献

- 1 Eric R. Introduction to distributed Hash tables. IETF-65 Technical Plenary. 2006
- 2 Sit E, Morris R. Security considerations for peer-to-peer distributed Hash tables. In: Druschel P, Kaashoek F, Rowstron A, eds. Peer-to-peer Systems. Berlin: Springer-Verlag, 2002. 261-269

- 3 Wallach D S. A survey of peer-to-peer security issues. In: Okada M, Pierce B, Scedrov A, et al., eds. *Software Security-Theories and Systems*. Berlin: Springer-Verlag, 2002. 42–57
- 4 Castro M, Druschel P, Ganesh A, et al. Secure routing for structured peer-to-peer overlay networks. In: *Proceedings of the 5th Symposium on Operating Systems Design and Implementation*, Boston, 2002
- 5 Hyeokchan K, Sunkee K, Jaehoon N, et al. The secure routing mechanism for DHT-based overlay network. In: *Proceedings of the 10th International Conference on Advanced Communication Technology*. Gangwon-Do: IEEE Press, 2008. 1300–1303
- 6 Artigas M S, Lopez P G, Skarmeta A F G. A novel methodology for constructing secure multipath overlays. *IEEE Internet Comput*, 2005, 9: 50–57
- 7 Sanchez-Artigas M, Lopez P G, Skarmeta A F G. Bypass: Providing secure DHT routing through bypassing malicious peers. In: *Proceedings of IEEE Symposium on Computers and Communication*. Marrakech: IEEE Press, 2008. 934–941
- 8 Hildrum K, Kubiawicz J. Asymptotically efficient approaches to fault-tolerance in peer-to-peer networks. *Lecture Notes in Computer Science*, 2003, 2848: 321–336
- 9 Yu M, Zhou M C, Su W. A secure routing protocol against Byzantine attacks for MANETs in adversarial environments. In: *Proceedings of IEEE Vehicular Technology Society*. Florida State Univ: IEEE Press, 2009. 449–460
- 10 Peng W, Nicholas H, Ivan O, et al. Myrmic: Secure and Robust DHT Routing. DTC Research Report 2006/20, 2006
- 11 Luo H, Lu S. Ubiquitous and Robust Authentication Services for Ad Hoc Wireless Networks. Technical Report UCLACSD-TR-200030. Los Angeles: University of California, 2000
- 12 Seongil H, Yongjae J, Seunghye Y, et al. A self-organized authentication architecture in mobile Ad-hoc networks. In: *Proceedings of International Conference on Information Networking*. Jeju Island: Springer, 2005. 689–696
- 13 Narasimha M, Tsudik G, Yi J H. On the utility of distributed cryptography in P2P and MANETs: the case of membership control. In: *Proceedings of 11th IEEE International Conference on Network Protocols*. Atlanta: IEEE Press, 2003. 336–345
- 14 Gokhale S, Dasgupta P. Distributed authentication for peer-to-peer networks. In: *Proceedings of 2003 Symposium on Applications and the Internet Workshops*. Orlando: IEEE Press, 2003. 347–357
- 15 Camenisch J, Lysyanskaya A. Dynamic accumulators and application to efficient revocation of anonymous credentials. *Lecture Notes in Computer Science*, 2002, 2442: 101–120
- 16 Benaloh J, Automaton G. One-way accumulators: a decentralized alternative to digital signatures. *Lecture Notes in Computer Science*, 1994, 765: 274–285
- 17 Holohan E, Schukat M. Authentication using virtual certificate authorities: a new security paradigm for wireless sensor networks. In: *Proceedings of IEEE Network Computing and Applications (NCA)*. Cambridge: IEEE Press, 2010. 92–99
- 18 Zhou Z, Huang Y F, Li X. Framework for secure authentication of nodes in peer-to-peer network. *J Southeast Univ (Nat Sci Ed)*, 2007, 37: 100–104 [周洲, 黄永峰, 李星. P2P 网络的节点安全认证. *东南大学学报 (自然科学版)*, 2007, 37: 100–104]
- 19 Douceur J R. The sybil attack. In: Druschel P, ed. *Proceedings of the 1st International Workshop on Peer-to-Peer Systems*. Cambridge: Springer-Verlag, 2002. 251–260
- 20 Dingledine R, Freedman M J, Molnar D. Accountability measures for peer-to-peer systems. In: *Peer-to-Peer: Harnessing the Power of Disruptive Technologies*. Sebastopol: O'Reilly and Associates Inc., 2001
- 21 Marti S, Ganesan P, Garcia-Molina H. DHT routing using social links. *Lecture Notes in Computer Science*, 2005, 3279: 100–111
- 22 Yu Z H. Analysis of malicious behaviors in peer-to-peer trust model. *Comput Eng Appl*, 2007, 43: 18–21
- 23 Hu J L, Li X H, Zhou B, et al. A reputation based attack resistant distributed trust management model in P2P networks. In: *Proceedings of IEEE Electronic Commerce and Security (ISECS)*, Guangzhou, 2010. 237–241
- 24 Kamvar S D, Schlosser M T, Garcia-Molina H. EigenRep: reputation management in P2P networks. In: Lawrence S, ed. *Proceedings of the 12th International World Wide Web Conference*. Budapest: ACM Press, 2003. 123–134
- 25 Despotovic Z, Aberer K. A probabilistic approach to predict peers' performance in P2P networks. *Lecture Notes in Computer Science*, 2004, 3191: 62–76

Secure P2P topology based on a multidimensional DHT space mapping

SUN ZhiXin^{1,2*}, LUO BingQing¹, CHEN YaDang¹ & BU Kai¹

1 Key Laboratory of Broadband Wireless Communication and Sensor Network Technology (Nanjing University of Posts and Telecommunications), Ministry of Education, Nanjing 210003, China;

2 State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China

*E-mail: sunzx@njupt.edu.cn

Abstract Distributed search and routing algorithms based on the DHT (distributed Hash table) protocol have attracted considerable attention in structured P2P (peer-to-peer) research as a result of favorable properties such as distribution, self-organization, and high scalability. Compared with a traditional C/S (client/server) network, the probability of peers initiating malicious behavior increases dramatically because of their self-governing and dynamic characteristics, which also make it harder to satisfy the peers' security required by DHT. In this paper, we propose a new secure DHT protocol based on a multidimensional mapping mechanism. This mechanism maps peers to a multidimensional space by dividing the identifiers into groups. Moreover, a series of secure methods and routing algorithms are provided to achieve secure DHT in smaller spaces. Compared with state-of-the-art approaches, the theoretical analysis and experimental results show that the multidimensional mapping mechanism can effectively improve the average success rate of a resource search by inhibiting malicious behavior.

Keywords multidimensional mapping, DHT (distributed Hash table), structured P2P (peer-to-peer) network, routing attack, security

SUN ZhiXin was born in 1964. He received the Ph.D. degree in Nanjing University of Aeronautics and Astronautics. Currently, he is a Doctoral Supervisor at Nanjing University of Posts and Telecommunications. His research interests include computer application and network safety, multimedia communications and Internet of Things.

LUO BingQing was born in 1987. Currently, she is a doctoral student at Nanjing University of Posts and Telecommunications. Her research interests include information network, multimedia communications and Internet of Things.