编码感知多跳无线网络安全路由协议

郭显[1,3]，冯涛[1,2]，袁占亭[1]

(1. 兰州理工大学 计算机与通信学院, 甘肃 兰州 730050;
2. 西安电子科技大学 计算机网络与信息安全教育部重点实验室, 陕西 西安 710071;
3. 甘肃联合大学 电子信息工程学院, 甘肃 兰州 730010)

摘 要：分析了网络编码系统 DCAR“编码+路由”发现过程存在的安全问题，提出了适用于编码感知安全路由协议的安全目标，设计了基于 DCAR 的编码感知安全路由协议 DCASR，DCASR 协议利用密码学机制保证可信路由建立和正确编码机会发现。为建模多跳无线网络特征和分析路由协议安全性，引入线程位置和线程位置相邻概念扩展安全系统逻辑 LS2，提出了分析路由协议安全性的逻辑 LS2-RP。LS2-RP 用线程邻居集及邻居集的变化描述多跳无线网络的动态拓扑关系，用广播规则模型化多跳无线网络广播通信特征。最后，用 LS2-RP 协议编程语言描述了 DCASR 协议，用 LS2-RP 的谓词公式和模态公式描述 DCASR 协议的安全属性，用 LS2-RP 逻辑证明系统分析了 DCASR 协议的安全性，证明 DCASR 协议能够满足安全目标。

关键词：多跳无线网络；安全路由协议；DCAR；形式化方法；LS2 逻辑

中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2012)06-0133-10

Coding-aware secure routing for multi-hop wireless networks

GUO Xian[1,3]，FENG Tao[1,2]，YUAN Zhan-ting[1]

(1.School of Computer and Communication, Lanzhou University of Technology, Lanzhou 730050, China;
2. Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi’an 710071, China;
3. School of Electronic Information Engineering, Gansu Lianhe University, Lanzhou 730010, China)

Abstract: To address security issues of DCAR in “coding+routing” discovery, a new security destination was proposed and a distributed coding-aware secure routing (DCASR) was designed. DCASR guarantees discovery of correct coding opportunity and establishment of trusted routes by using cryptography. To analyze the properties of DCASR, LS2 (logic of security systems) was extended, and a new logic LS2-RP (LS2 for routing protocol) was proposed. In LS2-RP, the concepts of location and neighboring location of thread were introduced. The dynamic topology of multi-hop wireless networks was described by the set of neighbors for thread. The broadcast rule of neighboring location threads modeled the feature of wireless broadcast communication. Finally, DCASR was described by programming language of LS2-RP and security properties were defined by predicates and modal formulas of LS2-RP. Security of DCASR was analyzed by using the proof system of LS2-RP. DCASR can satisfy our secure destination.

Key words: multi-hop wireless network; secure routing; DCAR; formal method; LS2

收稿日期：2011-08-19；**修回日期**：2011-12-14

基金项目：国家自然科学基金资助项目(60972078)；甘肃省高等学校基本科研业务费基金资助项目(0914ZTB186)；兰州理工大学博士基金资助项目(BS14200901)；甘肃省自然科学基金资助项目(1014RJZA005)

Foundation Items: The National Natural Science Foundation of China(60972078); The Universities Basic Scientific Research Foundation of Gansu Province in China(0914ZTB186); The Lanzhou University of Technology Ph.D. Programs of China(BS14200901) ; The Natural Science Foundation of Gansu Province(1014RJZA005)

1 引言

局部编码协议 COPE[1]是第一个多跳无线网络网络编码系统，COPE 利用无线广播特征执行“机会监听(opportunistic overhearing)”和“编码广播(encoded broadcast)”，根据节点一跳邻居提供的监听分组信息，节点发送所有目标邻居节点都能解码的编码分组，从而减少所需分组传输次数。然而，编码机会发现和路径选择过程分离，致使 COPE 存在 2 个限制：执行网络编码的“编码机会”依赖于确定的通信模式；编码结构限制在 2 跳节点范围内。针对 COPE 存在的问题，文献[2]提出了“编码+路由(coding+routing)”发现的全局网络编码系统(DCAR, distributed coding-aware routing)，它是一种把编码机会发现过程和路径选择过程合并的基于网络编码的路由机制，在非恶意环境中，DCAR 能够找到传输路径上编码和解码的所有可能位置。

DCAR 由下面 3 个组件构成：整合编码机会发现的路由发现过程、分组编码和解码、分组转发。正确发现编码机会是利用网络编码的基础。DCAR 中，基于路由发现阶段建立的路径信息和收集的“谁能监听”信息，新发现路径上的节点独立地确定编码机会。DCAR 的路由发现过程类似动态源路由协议 DSR 的路由发现过程，针对 DSR 路由发现阶段的攻击[3]仍然能够攻陷 DCAR 协议的“编码+路由”发现过程[4]。另外，DCAR 的分组编码和编码分组传输过程同样会遭受污染攻击[4]。因此,在恶意网络环境中，DCAR 协议无法完成协议功能，设计编码感知的路由协议时需考虑安全问题。

传统基于 DSR 的安全路由协议[5~8]允许协议返回路径存在攻陷节点。但与传统路由的存储转发方式不同，在考虑网络编码的路由协议中，如果新建立路径上存在攻陷节点，该节点可能提供伪造的邻居集信息，导致错过编码机会发现或发现错误的编码机会。尤其在编码分组传输过程中，攻陷节点可能执行污染攻击。因此，传统路由协议的安全目标不适合于编码感知安全路由协议，需要设计新的安全目标。

多跳无线网络(如移动 ad hoc 网络，Mesh 网络等)是一种无基础设施的无线广播通信网络，网络节点既是主机又是路由器，编码感知安全路由协议只有依赖网络中所有可信节点协作才能获得正确的路由信息和“谁能监听”信息，而这种“依赖”需网络可信节点之间的实体身份认证和消息完整性认证来建立，传统用于验证认证，密钥协商等安全协议的形式化方法可用于安全路由协议的安全分析。

基于 Dolev-Yao 模型的符号化验证方法是目前安全协议形式化分析和自动化验证的主流方向[9]。LS2(logic of secure systems)[10]是基于协议组合逻辑(PCL, protocol composition logic) [11]的分析网络安全系统的逻辑，LS2 中引入了共享内存和存储保护等技术，试图建模和分析复杂安全系统，如操作系统、虚拟机监视器、Web 浏览器、可信计算系统等。LS2 继承了 PCL 的特征，LS2 的公理和规则保证该逻辑在无需明确推理攻击者行为的情况下验证协议安全属性。因此，该逻辑能够简化无线网络安全路由协议分析过程，提高路由协议安全分析的可信度。

本文所做的工作：分析了网络编码系统 DCAR 中存在的问题，提出了适合基于网络编码的路由协议的安全目标，设计了编码感知安全路由协议(DCASR, distributed coding-aware secure routing)；扩展 LS2 逻辑，提出了建模多跳无线网络特征和分析安全路由协议的逻辑(LS2-RP, LS2 for routing protocol)；在 LS2-RP 逻辑中，建模并分析了 DCASR 协议，证明 DCASR 协议能够满足安全目标。

2 DCAR 综述

COPE 有 2 个基本限制，1)“编码机会”依赖于确定通信模式。也就是说，当存在“确定编码结构”时，网络编码才是可能的。如图 1 所示，数据流 P_1 的目标节点 2 能够监听到节点 3 传输的数据 P_2，数据流 P_2 的目标节点 4 能够监听到节点 1 传输的数据 P_1，收到节点 2 和节点 4 的分组监听报告信息后，数据流 P_1 和 P_2 的中继节点 c 就可编码传输节点 2 和 4 都能够解码的编码分组 $P_1 \oplus P_2$，节点 2 和节点 4 分别执行相应的解码 $P_2 \oplus (P_1 \oplus P_2)$ 和 $P_1 \oplus (P_1 \oplus P_2)$ 获得分组 P_1 和 P_2。2)编码结构限制在 2 跳区域内。COPE 假设数据发送者(如节点 1 和节点 3)是编码节点 c 的一跳前驱，目标接收者是编码节点 c 的一跳后继，并且能够监听到相应数据分组。这些假设不必要地消除了无线网络中比 2 跳更长的路径上的编码机会。如考虑图 2 中的情况，2 条路径 1→2→3→4 和 5→3→6→7 在节点 3 相交。节点 3 能够编码来自这 2 条路径的分组并且广播编码分组给节点 4 和节点 6。尽管节点 6 不能执行解码所需的机会监听，但它能够转发编码分组给节点 7，

节点 7 能够监听节点 1 的数据发送并随后执行解码。这样，机会监听和解码节点是远离编码节点几跳之外的节点。如果这些普遍存在的编码机会都能被检测到，能够进一步提高带宽效率和吞吐量。

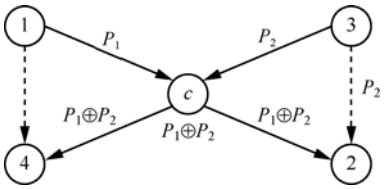

图 1　COPE 编码结构

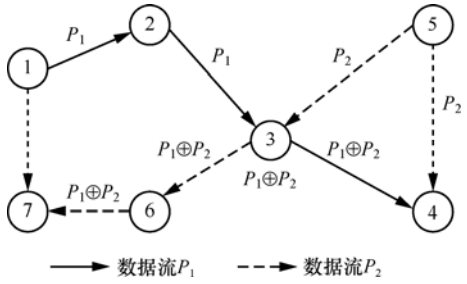

图 2　DCAR 协议实例

从以上分析可以看出，由于 COPE 协议把编码发现过程和路由发现过程“分离”以及仅仅基于节点一跳邻居的局部报告信息探测编码机会，导致协议无法发现如图 2 中存在的编码机会。针对这一问题，文献[2]提出了把编码机会发现过程与路由发现过程合并的编码感知路由机制 DCAR。

2.1　“编码+路由”发现过程

DCAR 协议中，当某节点要传输数据时，类似 DSR 协议，首先启动泛洪路由发现过程，查找与网络上现有数据流有潜在编码机会的传输路径，通过维护路由请求经过的路径上所有节点的邻居节点集合，每个节点跟踪网络中能够监听分组的其他节点。从而能在路由应答过程中，根据收集到的“谁能监听”信息和给定的编码条件，新发现路径上节点判断是否存在编码机会，并将存在编码机会的相应传输链路设置为编码可能(coding possible)路径，为后继的编码分组传输做准备。通过这种路径发现过程，DCAR 协议能够找到传输路径上的所有可能编码和解码位置。

2.2　编码条件

为发现具有潜在编码机会的路径，文献[2]提出了判断是否存在编码机会的充要条件。定义 1 定义了编码条件，其中，假设 a 表示网络中任意节点，$NE(a)$表示节点 a 的一跳邻居集合，F 表示数据流传输路径并且用 $a \in F$ 表示节点 a 在路径 F 上。用 $U(a, F)$表示路径 F 上节点 a 的所有上游节点集合，用 $D(a, F)$表示在路径 F 上节点 a 的所有下游节点集合。2 条路径 F_1 和 F_2 在某节点 c 上相交，当且仅当编码条件满足时，这 2 条路径上的数据分组能够在节点 c 上编码传输。

定义 1　2 条路径 F_1 和 F_2 的相交节点 c 上，能够执行分组编码的编码条件如下：

1) 存在 $d_1 \in D(c,F_1)$，以使得 $d_1 \in NE(s_1)$，$s_1 \in U(c,F_2)$ 或存在 $d_1 \in \mathrm{U}(c,F_2)$；

2) 存在 $d_2 \in D(c,F_2)$，以使得 $d_2 \in NE(s_2)$，$s_2 \in U(c,F_1)$ 或存在 $d_2 \in \mathrm{U}(c,F_1)$。

2.3　安全分析

图 2 中，假设节点 3 是攻陷节点，它可能在“编码+路由”发现过程中不按协议要求设置编码可能路径，导致节点 5 不用路径(3,6)传输数据而错过编码机会；或者节点 3 按协议要求设置编码可能路径，但在数据转发过程中能够启动污染攻击攻陷协议。另外，DCAR 协议路由发现过程类似 DSR 协议，针对 DSR 协议的攻击[3]对 DCAR 协议仍有效。因此，在恶意环境中，DCAR 协议不能完成其目标。然而，从路由发现过程和编码条件定义可以看出，DCAR 协议编码机会的判断依赖于“编码+路由”发现过程中建立的路径信息和收集的“谁能监听”信息，当每个节点有正确的路径信息和“谁能监听”信息时，它能够单独判断自己能否承担编码节点的角色。因此，只要保证路由发现过程能够建立可信路径(未攻陷节点构成的路径)并且收集到正确的“谁能监听”信息，就可保证正确编码机会发现。同样，可信路径的利用，能够排除污染攻击的可能。

3　DCASR 设计

3.1　安全目标

基于 DSR 的传统安全路由协议安全目标是：协议能否返回与网络拓扑一致的路径，这种路径上允许存在攻陷节点，通常称为存在路由(existent routes)[5,6]。文献[7]和文献[8]把网络上相邻攻陷节点合成单一节点构造攻陷网络拓扑模型，并把攻陷网络拓扑模型上的存在路由称为可模糊路由(plausible routes)。然而，如果允许发现路径上存在攻陷节点，节点共谋很容易构造错误路径，目前提出的基于这一安全目标的“安全”路由协议先后发现都存在安

全漏洞。如文献[7]提出的针对 SRP[5]，Ariadne[6]的攻击及文献[12]提出的针对 endairA[7]的攻击等。更重要的是，与传统路由的存储转发通信方式不同，在网络编码系统中，如果存在编码机会，传输路径上的节点将收到的分组编码后再转发。但如果建立的路径上存在攻陷节点，则可能不按协议要求编码传输而错过编码机会或启动污染攻击。

基于以上观察，本文提出的适合于编码感知的路由协议安全目标是：如果攻击者(内外部攻击者)无法阻止协议返回与网络拓扑一致的可信路径(trusted routes)，则称该协议是安全路由协议。这里的可信路径不允许包含攻陷节点。

因为泛洪路由请求能够通过多条路径到达目标节点，从源节点到目标节点，可能有多条存在编码机会的路径，现在的问题是目标节点如何识别可信路径?具体实现时，网络中可建立信任机制[13,14]，设置网络节点的信任级别，目标节点可根据节点的可信任等级选择可信路径，而不是传统的基于跳数选择路径，保证返回可信路径。信任机制的建立超出本文讨论范围，不作研究。

3.2 “编码+路由”发现过程

由于多跳无线广播通信特征，可信路径的建立和正确“谁能监听”信息的收集需要依赖网络中所有可信节点的协作，这种“依赖”可通过可信节点间的实体身份认证和消息完整性认证来建立。因此，DCASR 协议在路由应答消息中引入实体身份认证和消息完整性认证机制。假设网络中的每个节点维护一跳邻居表 $NE(a)$，该邻居信息可通过周期性地发送探测消息而获得，并假设新发现路径上的节点 c 有要转发的数据流。DCASR 协议具体过程如下。

1) 源节点 S 广播路由请求 RREQ 启动路由发现过程，该路由请求消息包含 S 的一跳邻居集 $NE(S)$。

2) 根据收到的 RREQ，中间节点 c 首先验证是否已经收到过该 RREQ，如果收到过该 RREQ，为防止出现环路，节点 c 取消 RREQ；否则节点 c 执行以下操作。

① 临时存储 RREQ，RREQ 包含对新路径的“谁能监听”信息。也就是说，节点 c 存储当上游节点传送数据时能够执行“机会监听”的监听节点集合。

② 更新“谁能监听”信息。节点 c 在 RREQ 的“谁能监听”表追加它的所有邻居，并广播新生成的 RREQ。

3) 当 RREQ 到达目标节点 T 时，T 用与源节点共享的密钥验证路由请求消息的可信性，验证成功，目标节点对收到的信息用与源节点共享的密钥加密并签名，生成路由应答消息，沿新发现路径的逆路径，目标节点 T 向源节点 S 转发路由应答消息 RREP，RREP 是包含路径信息和“谁能监听”信息的单播消息。

4) 根据收到的 RREP，中间节点 c 做如下操作。

① 验证自己的标识符是否在路由表中，验证自己的邻居集是否正确，验证转发 RREP 的节点是否是它的一跳邻居，验证转发 RREP 的节点的签名。如果这些验证失败，节点 c 删除该 RREP；否则，节点 c 根据编码条件判断是否存在编码机会。

② 比较包含在 RREP 路由表中的上游路径和它的临时存储 RREQ 中的路径，如果匹配，那么它已经获得了新路径和新路径上数据传输时的“谁能监听”信息。利用这些信息，节点 c 使用编码条件，能够验证新数据流和已存在数据流是否能编码，如果有编码机会，节点 c 在 RREP 中把相应链路标注为“编码可能”路径。

节点 c 对路由应答消息签名并单播路由应答消息给路由表中的下跳节点。

5) 当 RREP 到达源节点 S 时，除作类似中间节点的验证外，S 用与目标节点 T 共享的密钥验证路由应答消息的可信性，并验证路由表中节点签名，如果这些验证成功，接受该路径作为数据转发路径，否则，删除 RREP 等待 RREP 的其他副本。

由于“编码+路由”发现过程的中间节点操作方法类似，因此，为方便形式化验证，本文假设新数据流传输路径上仅有 2 个中间节点 R_1 和 R_2，DCASR“编码+路由”发现过程的协议消息如下：

$$M_1: S \to *: < RREQ, S, T, N_s, (), \{NE(S)\}, SYMENC_{K_{ST}}\{RREQ, S, T, N_s, (), \{NE(S)\}\} >$$

$$M_2: R_1 \to *: < RREQ, S, T, N_s, (R_1), \{NE(S), NE(R_1)\}, SYMENC_{K_{ST}}\{RREQ, S, T, N_s, (), \{NE(S)\}\} >$$

$$M_3: R_2 \to *: < RREQ, S, T, N_s, (R_1, R_2), \{NE(S), NE(R_1), NE(R_2)\}, SYMENC_{K_{ST}}\{RREQ, S, T, N_s, (), \{NE(S)\}\} >$$

$$M_4: T \to R_2 :< RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\},$$
$$SYMENC_{K_{S,T}}\{RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\}\},$$
$$SIGN_{K_T^{-1}}\{SYMENC_{K_{S,T}}\{RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\}\}\} >$$
$$M_5: R_2 \to R_1 :< RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\},$$
$$SYMENC_{K_{S,T}}\{RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\}\},$$
$$SIGN_{K_T^{-1}}\{SYMENC_{K_{S,T}}\{RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\}\}\},$$
$$SIGN_{K_{R_2}^{-1}}\{SYMENC_{K_{S,T}}\{RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\}\}\} >$$
$$M_6: R_1 \to S :< RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\}$$
$$SYMENC_{K_{S,T}}\{RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\}\},$$
$$SIGN_{K_T^{-1}}\{SYMENC_{K_{S,T}}\{RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\}\}\},$$
$$SIGN_{K_{R_2}^{-1}}\{SYMENC_{K_{S,T}}\{RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\}\}\},$$
$$SIGN_{K_{R_1}^{-1}}\{SYMENC_{K_{S,T}}\{RREP, S, T, N_s, (R_1, R_2),$$
$$\{NE(S), NE(R_1), NE(R_2)\}\}\} >$$

其中，M_1~M_3 表示广播消息，M_4~M_6 表示单播消息。$SYMENC_{K_{S,T}}\{|e|\}$ 表示用共享密钥 $K_{S,T}$ 加密的消息，$SIGN_{K_X^{-1}}\{|e|\}$ 表示用 X 签名密钥 K_X^{-1} 签名的消息。

4　LS2-RP 逻辑

4.1　协议编程语言

LS2-RP 逻辑中，把网络节点（协议参与方）模型化为某一位置（逻辑位置）上运行的线程，建模多跳无线网络为不同位置上线程的复合。用符号 ${}^{NE(I)}_{l}[P]_I$ 表示线程，其中，P 是位置 l 上线程 I 执行的行为序列，下标 I 是标识该线程的 5 元组$<\hat{I}, \eta, c, l, NE(I)>$，其中，$\hat{I}$ 是拥有该线程的协议参与方，η 是线程唯一会话标识符，c 是线程所在机器，l 是线程的逻辑位置。$NE(I)$是与线程 I 所在位置相邻位置上线程集合，“位置相邻”是指线程在相互通信范围内。所有线程邻居集的集合确定了当前网络拓扑结构，$NE(I)$会随网络节点的移动而发生变化，相反，$NE(I)$的变化模型化网络节点的移动和网络拓扑的动态变化过程。如果 $I_2 \in NE(I_1)$，则线程 ${}^{NE(I_1)}_{l}[P_1]_{I_1}$ 与线程 ${}^{NE(I_2)}_{m}[P_2]_{I_2}$ 在相互通信范围内，$I_1 \in NE(I_2)$ 也成立。

LS2-RP 中，把线程的内部计算、外部交互以及移动导致的网络进化过程称为网络迹（network trace），用 $\mathcal{N} = N_0 \xrightarrow{t_1} N_1 \ldots \xrightarrow{t_n} N_n$ 表示网络迹，N_i 表示网络状态，N_0 表示协议运行时的初始网络状态，N_n 表示协议运行完成时的网络状态。t_i 表示导致网络从状态 N_{i-1} 迁移到 N_i 的相应事件发生时间。

LS-RP 中，反应规则定义协议编程语言的操作语义，本文定义了建模多跳无线广播通信特征的广播规则：

$${}^{NE(I)}_{l}[send\ e; P]_I \mid {}^{NE(I_i)}_{m_i}[\prod\nolimits_{i\in n}(y_i := receive; Q_i)]_{I_i} \to$$
$${}^{NE(I)}_{l}[P]_I \mid {}^{NE(I_i)}_{m_i}[\prod\nolimits_{i\in n} Q_i\ (e/y_i)]_{I_i}$$

其中，线程 I 执行行为序列 send e;P 中的行为 send e，$I_i \in NE(I)\ (i = 1, 2, \cdots, n)$ 表示线程 I 的邻居 I_i 才能接收到线程 I 发送的消息，即与发送节点相邻的所有节点具有接收消息的能力。

4.2　语法

LS2-RP 逻辑用谓词公式和模态公式表达协议运行获得的网络迹 $\mathcal{N}$ 属性，谓词公式有行为谓词和普通谓词 2 类，对每个协议行为，有相应的行为谓词断言协议运行中出现了该行为，如 Send(X,e)表示线程 X 发送了表达式 e。普通谓词捕获没有指定确定行为的网络迹 $\mathcal{N}$ 属性，该类谓词的真假与网络迹 $\mathcal{N}$ 上状态迁移无直接关系，如 Honest($\hat{X}$)表示参与方 $\hat{X}$ 的线程严格遵循协议规范执行程序。

LS2-RP 逻辑用 2 类模态公式表达协议安全属性，它们是：${}^{NE(I)}_{l}[P]^{t_b,t_e}_{I}\phi$ 和 ${}^{NE(I)}_{l}[a]^{t_b,t_e}_{I,x}\phi$。模态公式 ${}^{NE(I)}_{l}[P]^{t_b,t_e}_{I}\phi$ 表示：任何时候位置 l 上线程 I 在半开区间$[t_b,t_e)$顺序执行了行为序列 P，那么公式 ϕ 满足，ϕ 通常表达协议基本程序序列 P 的安全属性。模态公式 ${}^{NE(I)}_{l}[a]^{t_b,t_e}_{I,x}\phi$ 的含义类似。

本文用到的符号，部分谓词公式的含义如下。

$\hat{X}$:表示拥有线程 X 的协议参与方。

$NE(X)$:与线程 X 相邻线程的集合。

$K_{X,Y}$：参与方 $\hat{X}$ 和 $\hat{Y}$ 的共享密钥。

K_X, K_X^{-1}：参与方 $\hat{X}$ 拥有的签名验证和签名密钥。

$SYMENC_K\{|e|\}$：用对称密钥 K 加密的表达式。

$SIGN_{K^{-1}}\{|e|\}$：用密钥 K^{-1} 签名的表达式。

symenc *e*,*K*：用对称密钥 *K* 对表达式 *e* 加密行为。

symdec *e*,*K*：用对称密钥 *K* 对表达式 *e* 解密行为。

sign *e*, K^{-1}：用密钥 K^{-1} 对表达式签名行为。

verify *e*, *K*：用密钥 *K* 验证签名表达式行为。

match *e*,*e*'：表达式 *e* 匹配表达式 *e*'行为。

append *e*,*e*'：表达式表 *e* 中追加表达式 *e*'。

lock/unlock *c*.*d*：机器 *c* 存储地址 *d* 加锁/解锁。

read/write *c*.*d*：读/写机器 *c* 存储地址 *d*。

Check *X* in *NE*(*Y*):验证线程 *X* 属于线程 *Y* 的邻居集。

Contains(e_1,e_2)：表示表达式 e_1 包含表达式 e_2。

Proj(*e*,*i*)：提取表达式表 *e* 中的第 *i* 个表达式。

Has(*X*,*e*)：协议参与方 $\hat{X}$ 的线程 *X* 拥有表达式 *e*。

Honest($\hat{X}$)：协议参与方 $\hat{X}$ 是诚实参与方。

Honest($\hat{X}$,$\vec{P}$)：诚实参与方 $\hat{X}$ 拥有的线程仅执行 $\vec{P}$ 中程序。

Send(*X*,*e*)|receive(*X*,*e*)|New(*X*,*e*)：发生了线程 *X* 发送、接收或生成表达式 *e* 的行为。

Sign(*X*,*e*)|Verify(*X*,*e*)|SymEnc(*X*,*e*,*K*)|SymDec(*X*,*e*,*K*)：发生了线程 *X* 签名、验证签名或对称加解密行为。

Read(*X*, *d*, *e*)/Write(*X*,*d*,*e*):发生了线程 *X* 读/写存储地址的行为。

IsLocked(*X*,*d*)/Unlock(*X* ,*d*)：线程 *X* 是否对存储地址加锁/解锁。

Mem(*d*,*e*)：存储地址 *d* 上有表达式 *e*。

4.3 语义

LS2-RP 在网络迹 $\mathcal{N}$ 上解释谓词公式的语义，语义命题 $\mathcal{N}\models^t \phi$ 表示网络迹 $\mathcal{N}$ 上的时间 *t*，公式 ϕ 满足。如：$\mathcal{N}\models^t$ Honest($\hat{X}$,$\vec{P}$)表示参与方 $\hat{X}$ 拥有的线程在网络迹 $\mathcal{N}$ 上执行了行为序列 $\vec{P}$。

LS2-RP 逻辑中，给出网络迹 $\mathcal{N}$ 与模态公式前缀 $^{NE(I)}_{l}[a]^{t_b,t_e}_{I,x}$ 和 $^{NE(I)}_{l}[P]^{t_b,t_e}_{I}$ 匹配(matching)概念定义 2 类模态公式语义，并给出了语义满足性定义。

定义 2 如果满足以下条件，则称网络迹 $\mathcal{N}=N_0\xrightarrow{t_1}N_1...\xrightarrow{t_n}N_n$ 与具有置换 θ 的前缀 $^{NE(I)}_{l}[a]^{t_b,t_e}_{I,x}$ 匹配，其中行为 *a* 返回值 *e*，记为 $\mathcal{N}\gg{}^{NE(I)}_{l}[a]^{t_b,t_e}_{I,e}\mid\theta$。

1) 时间 t_b，$\mathcal{N}$ 包含线程 $^{NE(I)}_{l}[\mathrm{a}\theta;\mathrm{p}\theta]_{\mathrm{I}}$；

2) 时间 t_e，逻辑位置 *l* 上线程 *I* 执行了行为 $\mathrm{a}\theta$ 并生成值 *e*。

定义 3 如果满足以下条件，则称网络迹 $\mathcal{N}=N_0\xrightarrow{t_1}N_1...\xrightarrow{t_n}N_n$ 与具有置换 θ 的前缀 $^{NE(I)}_{l}[P]^{t_b,t_e}_{I}$ (*P* 可能为空)匹配，记为 $\mathcal{N}\gg{}^{NE(I)}_{l}[P]^{t_b,t_e}_{I}\mid\theta$。

1) 对某行为序列 *Q* 和包含线程 $^{NE(I)}_{l}[(P;Q)\theta]_I$ 的状态 N_i，例如线程 *I* 运行程序 *P*;*Q* 的置换实例；

2) 对 $j\geqslant i$ $(i,j=1,2,\cdots,n)$及置换 ρ，N_j 包含 $^{NE(I)}_{m}[Q\rho]_I$；

3) 线程 *I* 运行行为序列 *P* 导致网络从 N_i 进化到 N_j，并且每个反应出现在半开时间区间$[t_b,t_e)$上。

定义 4 $^{NE(I)}_{l}[a]^{t_b,t_e}_{I,x}$ 和 $^{NE(I)}_{l}[P]^{t_b,t_e}_{I}$ 语义可满足性：

1) 任意置换 θ，如果对所有正常(ground)时间点 $t,t_b^{'}$ 和 $t_e^{'}$ 及任意正常表达式 *e*，$\mathcal{N}\gg{}^{NE(I)}_{l}[a]^{t_b^{'},t_e^{'}}_{I,e}\mid\theta$ 蕴含 $\mathcal{N}\models^t\phi\theta(t_b^{'}/t_b)(t_e^{'}/t_e)(e/x)$，则 $\mathcal{N}\models{}^{NE(I)}_{l}[a]^{t_b,t_e}_{I,x}\phi$ 满足；

2) 任意置换 θ，如果对所有正常(ground)时间点 $t,t_b^{'}$ 和 $t_e^{'}$，$\mathcal{N}\gg{}^{NE(I)}_{l}[P]^{t_b^{'},t_e^{'}}_{I}\mid\theta$ 蕴含 $\mathcal{N}\models^t\phi\theta(t_b^{'}/t_b)(t_e^{'}/t_e)$，则 $\mathcal{N}\models{}^{NE(I)}_{l}[P]^{t_b,t_e}_{I}\phi$ 满足。

4.4 证明系统

LS2-RP 逻辑中，用 $\succ\Phi$ 表示 Φ 是用证明系统中公理和规则可证明的公式，其中 Φ 可能是谓词公式、模态公式等。证明系统包括一系列公理和规则，也可以使用一阶逻辑中的所有公理。本文用到的重要公理如下：

ENC0 $\succ(\mathrm{SymEnc}(I,e,K)@t)\supset\exists t'.(t'<t)\wedge(\mathrm{Has}(I,K)@t')\wedge(\mathrm{Has}(I,e)@t')$

ENC1 $\succ(\mathrm{SymDec}(I,SYMENC_K\{|e|\},K)@t)\supset\exists I'.\exists t'.(t'<t)\wedge(\mathrm{SymEnc}(I',e,K)@t')$

Eq $\succ((e=e')\wedge\phi(e/x))\supset\phi(e'/x)$

Match $\succ(\mathrm{match}\,(I,e,e')@t)\supset e=e'$

Read $\succ(\mathrm{Read}(I,d,e)@t)\supset(\mathrm{Mem}(d,e)@t)$

VER $\succ((\mathrm{Verify}(I,e,K)@t)\wedge(\hat{I}\neq\hat{K})\wedge\mathrm{Honest}(\hat{K}))\supset(\exists I'.\exists t'.\exists e'.(t'<t)\wedge(\hat{I'}=\hat{K})\wedge\mathrm{Contains}(e',SIG_{K^{-1}}\{|e|\})\wedge(\mathrm{Send}(I',e')@t')\vee\exists d.\mathrm{Write}(I',d,e')@t'))$

New $\succ((\mathrm{New}(I,n)@t)\wedge(\mathrm{Receive}(I',e)@t')\wedge\mathrm{Contains}(e,n))\supset(t'>t)$

Write $\succ{}^{NE(I)}_{l}[\mathrm{write}\ d,e]^{t_b,t_e}_{I,x}\exists t.t\in[t_b,t_e]\wedge(\mathrm{Mem}(d,e)@t)\wedge(\forall e'.\neg\mathrm{Write}(I,d,e')\mathrm{on}(t,t_e))$

Mem = $\succ(\mathrm{Mem}(d,e)@t)\wedge(\mathrm{Mem}(d,e')@t))\supset(e=e')$

MemI $\succ(\mathrm{IsLocked}(d,I)\ \mathrm{on}\ [t_b,t_e)\wedge(\mathrm{Mem}(d,e)@t_b)\wedge(\forall e'.\neg\mathrm{Write}(I,d,e')\,\mathrm{on}\,[t_b,t_e))\supset(\mathrm{Mem}(d,e)\,\mathrm{on}\,[t_b,t_e))$

LockI $\succ(\mathrm{IsLocked}(d,I)@t)\wedge\neg\mathrm{Unlock}(I,d)\,\mathrm{on}\,[t,t'])\supset(\mathrm{IsLocked}(d,I)\,\mathrm{on}\,[t,t'])$

公理中“谓词@t”表示时间 t 该谓词为真，如 SymEnc(I,e,K)@t表示时间t线程I执行了加密操作。

本文用到的重要规则如下:

Seq $$\frac{\succ {}^{NE(I)}_{l}[a]^{t_b,t_m}_{l,x}\phi \qquad \succ {}^{NE(I)}_{l}[P]^{t_m,t_e}_{I}\psi \quad (t_m\ fresh)}{\succ {}^{NE(I)}_{l}[x:=a;P]^{t_b,t_e}_{I}\exists t_{\mathrm{m}}.\exists x.((t_{\mathrm{b}}<t_{\mathrm{m}}<t_{\mathrm{e}})\wedge\phi\wedge\psi)}$$

Hon $$\frac{\forall Q\in IS(\vec{P}).\ \succ {}^{NE(I)}_{l}[Q]^{t_b,t_e}_{I}\phi}{\succ \mathrm{Honest}(\hat{I},\vec{P})\supset\forall t_e.\phi(-\infty/t_b)}$$

5　DCASR 协议安全分析

5.1　形式化描述

LS2-RP 协议编程语言描述 DCASR 协议如下：

$S(d,\hat{R}_1,\hat{R}_2,\hat{T},K_T,K_{R_1},K_{R_2})$ {

/* *generates and broadcasts the route request* */

lock $d.pk_1$, $d.pk_2$, $d.pk_3$;

write $d.pk_1$, K_T ; write $d.pk_2$, K_{R_2} ; write $d.pk_3$, K_{R_1} ;

new N_s;

c:=symenc $(RREQ,\hat{S},\hat{T},N_s,(),\{NE(S)\})$,$K_{S,T}$;

send $(RREQ,\hat{S},\hat{T},N_s,(),\{NE(S)\},c)$;

/**receives the route reply* */

(m,c,a_1,a_2,a_3):=receive ;

/**verifies whether the forwarder is its neighbor* */

X:=proj(proj(m,5),1);Check$X$ in $NE(S)$;

/**verifies whether its neighbor set in RREQ is modified during route discovery process.* */

match proj(proj(m,6),1), $NE(S)$;

m_1:=symdec c, $K_{S,T}$; match m_1,m;

pk_1:=read $d.pk_1$; s_1:= verify a_1, pk_1;

m_2:=symdec s_1, $K_{S,T}$; match m_2, m;

pk_2:=read $d.pk_2$; s_2:= verify a_2, pk_2;

m_3:=symdec s_2, $K_{S,T}$; match m_3, m;

pk_3:=read $d.pk_3$; s_3:= verify a_3, pk_3;

m_4:=symdec s_3, $K_{S,T}$; match m_4, m;

unlock $d.pk_1$, $d.pk_2$, $d.pk_3$;}

T (){

/* *receives the route request* */

(m, c):=receive;

m_1:=symdec c, $K_{S,T}$; match m_1,m;

/**generates and sends the route reply*/

m:=(*RREP*,proj (m,2), proj (m,3), proj (m,4), proj (m,5), proj (m,6));

c:=symenc m, $K_{S,T}$; a:=sign c, K_T^{-1} ; send (m,c,a);}

$R_1(d_1,\hat{R}_2,K_{R_2})$ {

lock $d_1.pk$;write $d.pk$, K_{R_2} ;

/**receives the route request*/

m:=receive;

rl:=proj (m,5); append rl,R_1;

ne:=proj(m,6); append ne,$N(R_1)$;

m:=(*RREQ*,proj (m,2), proj (m,3), proj (m,4),rl,ne);

send m;

/**receives the route reply*/

(m,c,a_1,a_2):=receive;

/* *verifies it's identifier in route list* */

X:= proj(proj (m,5),1); match X,R_1;

/* *verifies whether its neighbor set in RREQ is modified during route discovery process.*/

ne:=proj(proj(m,6),2) ;match ne,$NE(R_1)$;

s:= verify a_2, K_{R_2} ;

a_3:=sign c, $K_{R_1}^{-1}$; send (m,c,a_1, a_2, a_3);

unlock $d_1.pk$;}

$R_2(d_2,\hat{T},K_T)$ {

lock $d_2.pk$; write $d_2.pk$, K_T ;

/**receives the route request*/

m:=receive;

rl:=proj (m,5); append rl,R_2;

ne:=proj(m,6); append ne,$NE(R_2)$;

m:=(*RREQ*,proj (m,2), proj (m,3), proj (m,4),rl,ne);

send m;

/**receives the route reply*/

(m,c,a_1):=receive;

/* *verifies it's identifier in route list* */

X:=proj(proj (m,5),2); match X,R_2;

/* *verifies whether its neighbor set in RREQ is modified during route discovery process.*/

ne:=proj(proj(m,6),3) ;match ne, $NE(R_2)$;

s:= verify a_1, K_T ;a_2:=sign c, $K_{R_2}^{-1}$; send (m,c,a_1, a_2);

unlock $d_2.pk$;}

5.2　协议环境假设

本文假设用某种密钥分发机制给网络中的节

点预分配了所需公私钥对，网络中每个节点知道其他节点的签名验证密钥，并分配了源与目标节点间的共享密钥 $K_{S,T}$。

$\Gamma_{DCASR}=\varphi_1\wedge\varphi_2\wedge\varphi_3$ 表示 DCASR 协议环境假设：

$$\varphi_1\equiv \mathrm{Honest}(\hat{S},S(d,\hat{R_1},\hat{R_2},\hat{T},K_T,K_{R_1},K_{R_2}))\wedge\mathrm{Honest}(\hat{T},T())\wedge \mathrm{Honest}(\hat{R_1},R_1(d_1,\hat{R_2},K_{R_2}))\wedge\mathrm{Honest}(\hat{R_2},R_2(d_2,\hat{T},K_T))$$

$$\varphi_2\equiv \mathrm{Honest}(\hat{X})\wedge\mathrm{Has}(\hat{X},K_X^{-1})\wedge\neg\exists\hat{Y}((\hat{Y}\neq\hat{X})\wedge\mathrm{Has}(\hat{Y},K_X^{-1}))$$

$$\varphi_3\equiv \forall X.\mathrm{Honest}(\hat{S},\hat{T})\wedge\mathrm{Has}(X,K_{S,T})\wedge(\hat{X}=\hat{S})\vee(\hat{X}=\hat{T})$$

φ_1 表示参与方 $\hat{S},\hat{R_1},\hat{R_2},\hat{T}$ 是诚实参与方，并且它们诚实遵循它们的协议规范。φ_2 表示参与方 $\hat{S},\hat{R_1},\hat{R_2},\hat{T}$ 不会泄露各自的私钥信息，而 φ_3 表示仅源节点 S 与目标节点 T 知道共享密钥 $K_{S,T}$。

5.3 安全属性

非形式化描述 DCASR 协议的安全目标如下。

1) 目标节点 T 收到路由请求消息时，T 能够证明源节点 S 发送了路由请求消息。

2) 当中间节点 R_2 收到包含可信路径 (R_1,R_2) 及邻居集为 $\{NE(S),NE(R_1),NE(R_2)\}$ 的路由应答消息 RREP 时，R_2 能够证明节点 T 转发了该路由应答消息。

3) 当中间节点 R_1 收到包含可信路径 (R_1,R_2) 及邻居集为 $\{NE(S),NE(R_1),NE(R_2)\}$ 的路由应答消息 RREP 时，R_1 能够证明邻居节点 R_2 转发了该应答消息。

4) 源节点 S 收到包含可信路径 (R_1,R_2) 及邻居集为 $\{NE(S),NE(R_1),NE(R_2)\}$ 的路由应答消息 RREP 时，源节点 S 能够证明目标节点 T 生成并发送了路由应答消息 RREP；并且能够证明中间节点 R_1,R_2 签名并转发了该路由应答消息。

假设源节点 S 成功执行了程序 $S()$，那么 T，R_1 和 R_2 的线程肯定成功执行了相应程序 $T()$，$R_1()$和 $R_2()$，可用如下模态公式 M_1，M_2，M_3 和 M_4 形式化描述 DCASR 协议的安全目标：

$$J_T=\overset{NE(T)}{l_T}[T()]_{I,-}^{t_b,t_e}\exists I.\exists t_1'.\exists t_1''.(t_1'<t_1'')\wedge(\hat{I}=\hat{S})\wedge (\mathrm{New}(I,N_S)@t_1')\wedge(\mathrm{symenc}(I,m',K_{S,T})@t_1'') \quad (M_1)$$

$$J_{R_2}=\overset{NE(R_2)}{l_{R_2}}[R_2(d_2,\hat{T},K_T)]_{I,-}^{t_b,t_e}\exists I.\exists t_1'.\exists t_1''.(t_1'<t_1'')\wedge (\hat{I}=\hat{T})\wedge(\mathrm{New}(I,SYMENC_{K_{S,T}}\{|m|\}@t_1')\vee (\mathrm{Receive}(I,SYMENC_{K_{S,T}}\{|m|\})@t_1'))\wedge (\mathrm{Sign}(I,SYMENC_{K_{S,T}}\{|m|\},K_T^{-1})@t_1'') \quad (M_2)$$

$$J_{R_1}=\overset{NE(R_1)}{l_{R_1}}[R_1(d_1,\hat{K_{R_2}},K_{R_2})]_{I,-}^{t_b,t_e}\exists I.\exists t_1'.\exists t_1''.(t_1'<t_1'')\wedge (\hat{I}=\hat{K_{R_2}})\wedge(\mathrm{New}(I,SYMENC_{K_{S,T}}\{|m|\}@t_1')\vee (\mathrm{Receive}(I,SYMENC_{K_{S,T}}\{|m|\})@t_1'))\wedge (\mathrm{Sign}(I,SYMENC_{K_{S,T}}\{|m|\},K_{R_2}^{-1})@t_1'') \quad (M_3)$$

$$\begin{aligned}J_S=&\overset{NE(I)}{l_S}[S(d,\hat{R_1},\hat{R_2},\hat{T},K_T,K_{R_1},K_{R_2})]_{I,-}^{t_b,t_e}\\&\exists I_1.\exists I_2.\exists I_3.\exists t_1'.\exists t_1''.\exists t_1'''.\exists t_2'.\exists t_2''.\exists t_3'.\exists t_3''.\\&(t_b<t_1'<t_1''<t_1'''<t_2'<t_2''<t_3'<t_3''<t_e)\wedge\\&(\hat{I_1}=\hat{K_T})\wedge(\hat{I_2}=\hat{K_{R_2}})\wedge(\hat{I_3}=\hat{K_{R_1}})\wedge\\&(\mathrm{Receive}(I_1,m)@t_1')\wedge(\mathrm{symenc}(I_1,m,K_{S,T})@t_1'')\wedge\\&(\mathrm{Sign}(I_1,SYMENC_{K_{S,T}}\{|m|\},K_T^{-1})@t_1''')\wedge\\&(\mathrm{Receive}(I_2,(m,SYMENC_{K_{S,T}}\{|m|\},\\&SIGN_{K_T^{-1}}\{|SYMENC_{K_{S,T}}\{|m|\}|\})@t_2')\wedge\\&(\mathrm{Sign}(I_2,SYMENC_{K_{S,T}}\{|m|\},K_{R_2}^{-1})@t_2'')\\&(\mathrm{Receive}(I_3,(m,SYMENC_{K_{S,T}}\{|m|\},\\&SIGN_{K_T^{-1}}\{|SYMENC_{K_{S,T}}\{|m|\}|\},\\&SIGN_{K_{R_2}^{-1}}\{|SYMENC_{K_{S,T}}\{|m|\}|\}))@t_3')\wedge\\&(\mathrm{Sign}(I_2,SYMENC_{K_{S,T}}\{|m|\},K_{R_1}^{-1})@t_3'')\end{aligned} \quad (M_4)$$

以上模态公式中 m，m'的值如下：

$$m=(RREP,\hat{S},\hat{T},N_S,(R_1,R_2),\{NE(S),NE(R_1),NE(R_2)\})$$

$$m'=(RREQ,\hat{S},\hat{T},N_S,(),\{NE(S)\}).$$

5.4 安全证明

定理 1 (安全性) 对协议环境假设 Γ_{DCASR} 和协议安全属性 J_S、J_{R_1}、J_{R_2}、J_T，使用 LS2-RP 证明系统中的公理和推理规则能够证明 $\Gamma_{DCASR}\succ J_S,J_{R_1},J_{R_2},J_T$。

证明 这里给出主要证明思路。首先证明 $\Gamma_{DCASR}\succ J_S$，假设源节点 S 完整执行了程序 $S(d,\hat{R_1},\hat{R_2},\hat{T},K_T,K_{R_1},K_{R_2})$，从分析源节点 S 处理路由应答消息 RREP 的单个行为开始，合并执行这些行为获得的属性，得出模态公式 M_4 描述的安全属性。

1) 源节点 S 的线程 I 在 I 所在机器存储地址 $d.pk_1$，$d.pk_2$, $d.pk_3$ 上拥有独占写锁。根据公理 Lock,Write 以及不变式公理 MemI 和 LockI，公钥 K_T,K_{R_1},K_{R_2} 在协议分析期间保持完整性。

2) 源节点 S 用共享密钥 $K_{S,T}$ 成功解密了路由应答消息中的加密消息，根据公理 ENC1，存在线程 X 用共享密钥 $K_{S,T}$ 对路由应答消息中的相应部分做

了加密操作，而根据公理 ENC0，线程 X 必须拥有共享密钥 $K_{S,T}$。根据假设 Γ_{DCASR}，仅源节点 S 和目标节点 T 拥有共享密钥 $K_{S,T}$，那么由假设：

$$Honest(\hat{S},S(d,\hat{R}_1,\hat{R}_2,\hat{T},K_T,K_{R_1},K_{R_2}))\wedge Honest(\hat{T},T())$$

必定是目标节点 T 的线程用共享密钥 $K_{S,T}$ 加密了路由应答消息中的相应部分。

3) 源节点 S 用私钥 K_T^{-1} 成功验证了路由应答消息中的签名消息。根据假设 Γ_{DCASR}，仅目标节点 T 的线程知道私钥 K_T^{-1}，再根据公理 VER 得出结论，必定是目标节点 T 的线程用私钥 K_T^{-1} 对路由应答消息中的相应部分作了签名操作。

4) 源节点 S 成功验证目标节点 T 的签名后，源节点 S 再用共享密钥 $K_{S,T}$ 成功解密了目标节点 T 作签名的消息。

5) 综合 2)，3)和 4)，目标节点 T 加密并签名转发了路由应答消息中的相应部分。

6) 源节点 S 分别用私钥 $K_{R_1}^{-1}$，$K_{R_2}^{-1}$ 成功验证了路由应答消息中的相应签名消息。根据假设 Γ_{DCASR}，仅中间节点 R_1 和 R_2 的线程知道它们各自的私钥 $K_{R_1}^{-1}$，$K_{R_2}^{-1}$，再根据公理 VER 得出结论，分别是中间节点 R_1 和 R_2 的线程用私钥 $K_{R_1}^{-1}$，$K_{R_2}^{-1}$ 对路由应答消息中的相应部分作了签名操作。

7) 源节点 S 成功验证中间节点 R_1 和 R_2 的签名消息后，源节点 S 用共享密钥 $K_{S,T}$ 成功解密了中间节点 R_1 和 R_2 作签名的消息。

8) 综合 2)，6)和 7)，说明中间节点 R_1 和 R_2 签名转发了来自目标节点 T 的路由应答消息。

综合 5)和 8)，源节点 S 收到包含可信路径(R_1,R_2)及邻居集为 $(NE(S),NE(R_1),NE(R_2))$ 的路由应答消息 RREP 时，源节点 S 证明目标节点 T 生成并发送了路由应答消息 RREP，并且中间节点 R_1，R_2 签名并转发了该路由应答消息。

至此证明了 $\Gamma_{\text{DCASR}} \succ J_S$。类似 2)能够证明 $\Gamma_{\text{DCASR}} \succ J_T$，类似 3)能够证明 $\Gamma_{\text{DCASR}} \succ J_{R_1},J_{R_2}$。

6　相关协议方案比较

本文从安全目标、安全分析方法、安全性、路由请求和路由应答中密码运算次数几个方面，对 DCASR 协议与基于 DSR 的经典“安全”路由协议 SRP[5]，Ariadne[6]，endairA[7]做了比较分析。这里假设 n 是网络节点的个数，k 是协议返回路径上节点个数，并假设各种密码学操作的复杂性相同，比较结果如表 1 所示。

表 1　　相关协议方案比较

协议	安全目标	分析方法	安全	密码学操作次数	
				路由请求	路由应答
SRP	存在路由	BAN 逻辑	否	2	2
Ariadne	存在路由	非形式化	否	2+2n+2k	4+3k
endairA	模糊路由	摸拟方法	否	0	1+3k
DCASR	可信路由	LS2-RP	是	2	3+3k

7　结束语

DCAR 协议没有考虑安全问题，在恶意环境中，DCAR 协议可能无法完成协议目标。传统基于 DSR 的安全路由协议安全目标不适用于编码感知的安全路由协议，本文提出了新的安全目标，设计了基于 DCAR 的安全路由协议 DCASR。DCASR 协议可与信任机制结合，仅在路由应答消息中引入安全机制，在源与目标节点间建立安全关联，保证路由应答消息传播过程中攻击者不可能删除、篡改和伪造路由消息，保证可信路径的建立和发现正确的编码机会，并且与传统安全路由相比能够减少密码学操作次数。扩展了安全系统逻辑 LS2,提出了建模多跳无线网络和分析安全路由协议的逻辑 LS2-RP，并在 LS2-RP 逻辑中建模并分析了 DCASR 协议安全性。协议安全分析中，LS2-RP 逻辑的公理和规则保证不需明确推理攻击者的行为，简化了路由协议安全分析的复杂性，提高了协议分析的可信度。

研究适合于多跳无线网络环境的信任机制并与本文设计的路由协议相结合是以后的主要工作，通过仿真方法研究编码感知路由协议效率问题是以后另一主要工作。

参考文献：

[1] KATTI S, RAHUL H, HU W. XORs in the air: practical wireless network coding[J]. IEEE/ACM Transactions on Networking, 2008, 16(3):497-510.

[2] LE J L, JOHN LUI C S, CHIU D M. DCAR: dsitributed coding-aware routing in wireless networks[J]. IEEE Transactions on Mobile Computing, 2010, 9(4): 596-608.

[3] KANNHAVONG B, NAKAYAMA H, NEMOTO Y. A survey of routing attacks in mobile ad hoc networks[J]. Wireless Communication, 2007, 14(5): 85-91.

[4] DONG J, REZA C, CRISTINA N R. Secure network coding for wireless mesh networks: threats, challenges, and directions[J]. Computer Communications, 2009, 32(17):1790-1801.

[5] PAPADIMITRATOS P, HAAS Z. Secure routing for mobile ad hoc networks[A]. The Communication Networks and Distributed System Modeling and Simulation Conference [C]. San Antonio, 2002. 27-31.

[6] HU Y C, PERRIG A, JOHNSON D B. Ariadne: a secure on-demand routing protocol for ad hoc networks [J]. Wireless Networks, 2005, 11(1-2):21-38.

[7] ACS G, BUTTYAN L, VAJDA I. Provably secure on-demand source routing in mobile ad hoc networks[J]. IEEE Transactions on Mobile Computing, 2006, 5(11):1533-1546.

[8] 冯涛,郭显,马建峰.可证明安全的节点不相交多路径源路由协议[J].软件学报,2010,21(7):1717-1731.
FENG T, GUO X, MA J F. Provably secure approach for multiple node-disjoint paths source routing protocol[J]. Journal of Software, 2010, 21(7):1717-1731.

[9] 韩继红,郭渊博,王亚弟.安全协议形式化分析方法[J].信息工程大学学报,2008,9(3):272-276.
HAN J H, Guo Y B, WANG Y D. On methods and techniques for formal analysis of security protocols[J]. Journal of Information Engineering University, 2008, 9(3):272-276.

[10] DATTA A, JASON F, DEEPAK G. A logic of secure systems and its application to trusted computing [A]. 2009 30th IEEE Symposium on Security and Privacy [C]. Washington, DC, USA, 2009. 221-236.

[11] DATTA A, DEREK A, MITCHELL J C, *et al*. Protocol composition logic (PCL) [J]. Electronic Notes in Theoretical Computer Science, 2007, 172(1):311–358.

[12] BURMESTER M, MEDEIROS B D. On the security of discovery in MANETs[J]. IEEE Transactions on Mobile Computing, 2007, 8(9): 1180-1188.

[13] PENG S C, JIA W J, WANG G J. Trusted routing based on dynamic trust mechanism in mobile ad hoc networks[J]. IEICE Transactions on Information and Systems, 2010, E93.D(3):510-517.

[14] GHOSH T, PISSINOU N, MAKKI K. Towards designing a trusted routing solution in mobile ad hoc networks[J]. Mobile Networks and Applications, 2005, 10(6):985-995.

作者简介：

郭显（1971-），男，甘肃定西人，博士，甘肃联合大学副教授，主要研究方向为无线网络安全，安全协议形式化分析。

冯涛（1970-），男，甘肃临洮人，博士，兰州理工大学计算机与通信学院副院长、研究员，主要研究方向为可证明安全协议理论、无线和移动网络安全。

袁占亭（1961-），男，陕西扶凤人，硕士，兰州理工大学教授、博士生导师，主要研究方向为无线网络安全、计算机软件与理论。