Ad-hoc路由协议的串空间安全性扩展

董学文[1,2] 牛文生[3] 马建峰[1,2] 盛立杰[1]
(西安电子科技大学计算机学院 西安 710071)[1]
(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 西安 710071)[2]
(中国航空计算技术研究所 西安 710068)[3]

摘 要 根据Ad-hoc移动网络特点,深入分析了串空间模型的一致性条件,提出路由五段式模型,将中继者可信条件修改为任意中继者可信条件,使串空间适用于Ad-hoc安全路由协议分析。然后以一个攻击实例验证路由五段式模型的正确性和优越性。

关键词 串空间,安全协议,一致性条件,任意中继者可信条件
中图法分类号 TP393 **文献标识码** A

Security Extension on Strand Space Model for Ad-hoc Routing Protocols

DONG Xue-wen[1,2] NIU Wen-sheng[3] MA Jian-feng[1,2] SHENG Li-jie[1]
(School of Computer Science & Technology, Xidian University, Xi'an 710071, China)[1]
(Key Laboratory of Computer Networks & Information Security of Ministry of Education, Xidian University, Xi'an 710071, China)[2]
(China Aeronautics Computing Technique Research Institute, Xi'an 710068, China)[3]

Abstract Abstract based on the characteristics of Ad-hoc mobile network and detail analysis of the consistency condition in strand space model, a concept of five routing segments model was brought up and intermediator credibility condition was changed into the arbitrary intermediator credibility condition, thus the strand space model was adapted to the security analysis for Ad-hoc routing protocols. Then an attack was brought to verify the correctness and superiority of the five routing segments model.

Keywords Sstrand space model, Security protocol, Consistency condition, Arbitrary intermediator credibility condition

1 引言

移动Ad-hoc网络(MANET mobile Ad hoc networks)是一种不依赖于固定基础设施的无线网络,因其自组织特性,在救灾保障、会务通信、作战指挥、实施远距离或危险环境中的监控等场合具有广阔的应用前景,但同时导致了更多的安全问题,已得到广泛关注和研究。安全路由协议的设计与分析即是其中之一。

目前大部分安全路由协议分析都是基于非形式化方法,例如主观分析、模拟仿真等。其分析过程不精确、不严格,缺乏有力的分析证明,导致很多原来声称"安全"的路由协议后来都被发现存在安全漏洞[1,2]。近年来,形式化分析方法开始应用于安全路由协议的分析研究上,例如ban逻辑[3]、串空间等等。

串空间最初被设计用于分析静态的、参与主体较少的协议,例如认证协议。文献[4]对串空间进行扩展并应用于动态的、参与主体相对较多的Ad-hoc路由协议,但认为对串空间存在不甚确切的地方,应对其进一步扩展完善。

本文第2节简单介绍串空间模型;第3节介绍Ad-hoc路由协议的一致性条件、中继者可信条件;第4节深入分析其中继者可信条件,指出其不合理的地方,并进行扩展、完善,提出路由五段式模型和任意中继者可信条件;第5节以一个攻击实例验证路由五段式模型的正确性和优越性;最后为结束语。

2 串空间

Strand空间模型[5,6](Strand space model, SSM)是Thayer Fàbrega, Herzog和Guttman等人在1998年提出的安全协议分析模型,它借助图论的方法描述协议的执行过程。协议主体行为序列构成Strand,而所有Strand的集合构成Strand空间;不同协议主体的Strand之间通过消息数据的收发相互关联,从而形成丛(bundle)或称为线束。在线束的基础上,不同节点之间的偏序关系使得存在极小元,从而又产生了一种类似于归纳法[7]的协议安全性证明方法。

为了简化描述,除了串空间理论中的攻击者能力部分,本

到稿日期:2010-08-24 返修日期:2010-11-12 本文受国家自然科学基金重点项目(60633020),国家高技术研究发展计划(863)(2007AA01Z429),国家科技重大专项(2009ZX03004-003),国家自然科学基金项目(60573036,60702059,60503012,60872041),中央高校基本科研业务费专项资金(JY10000903006,JY10000903012)资助。

董学文(1981-),男,博士生,讲师,主要研究方向为无线网络安全、安全协议设计与分析,E-mail:xddongxuewen@gmail.com;牛文生(1967-),男,博士,研究员,博士生导师,主要研究方向为航空电子系统安全;马建峰(1963-),男,博士,教授,博士生导师,主要研究方向为密码学、网络安全;盛立杰(1976-),男,博士,讲师,主要研究方向为计算机网络。

文直接引用 Strand 空间模型的一些概念，它们的基本定义可以参阅文献[5,6]，认证测试定理参阅文献[8,9]。

串空间理论建立了攻击者行为模型，对于攻击者的一些基本攻击进行了形式化描述。攻击者的能力主要由两方面因素来描述：一是攻击者所掌握的密钥集，二是攻击者由它所接受的消息产生新消息的能力。其中攻击者所掌握的密钥集用 Kp 表示，攻击者的基本行为由下面攻击者的迹的集合来描述：

M：$\langle +t \rangle$，发送消息。

F：$\langle -t \rangle$，接收消息。

T：$\langle -g+g+g \rangle$，接收到消息后，重复转发该消息。

C：$\langle -g-h+gh \rangle$，分别接收消息 g，h 后，发送消息 gh。

S：$\langle -gh+g+h \rangle$，接收消息 gh 后，分别发送消息 g 和 h。

K：$\langle +k \rangle$，发送密钥 k。

E：$\langle -k-h+\{h\}k \rangle$，接收消息 h 后，用密钥 k 加密，并发送加密后的消息。

D：$\langle -k^{-1}-\{h\}k+h \rangle$，接收加密后的消息 $\{h\}k$，用私钥解密，并发送消息 h。

对于一个协议的攻击可以看作是这些基本行为的组合。这些攻击者的迹给出了对于攻击者能力的形式化描述并保证了由攻击者发出的消息对于自由信息空间上的运算是封闭的。

3 一致性条件和中继者可信条件

文献[4]中，将串空间中协议的一致性扩展应用到 Ad-hoc 路由协议上。扩展的主要原因表现在两个方面：①基于路由协议的中继节点的存在，增加了中继者角色的定义；②基于路由发现过程中，发起者通常采用泛洪的方式[10,11]进行广播，因而 Ad-hoc 路由协议一致性不满足强一致性定义。文献[4]中具体 Ad-hoc 路由协议的一致性表现如下。

一致性条件：每次 B 作为响应者使用数据 X 与它所认为的 A（发起者）完成一轮协议执行时，确实存在一轮协议执行，其中 A 作为发起者也使用 X，并且认为它的响应者为 B（称为响应者保证）。

相应地，每次 A 作为发起者使用数据 X 与它所认为的 B（响应者）完成一轮协议执行时，确实存在一轮协议执行，其中 B 作为响应者也使用 X，并且认为它的发起者为 A（称为发起者保证）。

中继者可信条件：每次发起者 A 和响应者 B 使用数据 X 完成一轮协议执行时，中继者确实转发过数据 X，并且认为数据 X 的源和目的节点分别为发起者 A 和响应者 B（称为中继者保证）。

重点分析路由发现阶段，忽略其他阶段，文献[4]将 SRP 路由协议的发现阶段按照如下形式进行形式化[12,13]：

$S \rightarrow R$：Message1

$R \rightarrow D$：Message2

$D \rightarrow R$：Message3

$R \rightarrow S$：Message4

即将网络结构划分为 3 个部分：发起者 S、响应者 D、中继者 R。路由协议消息过程如图 1 所示。下面将这种形式化方法简称为路由三段式，相应的一致性条件也称为路由三段式一致性条件。

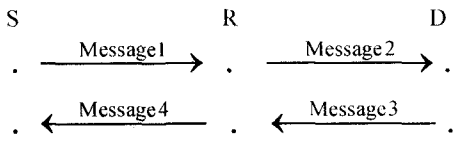

图 1 路由三段式

文献[4]以 SRP 协议为例，协议经过路由三段式形式化表现如下：

$A \rightarrow R$(Message1)：$A, Na, \{Na, Kab\}Kh$

$R \rightarrow B$(Message2)：$A, R, Na, \{Na, Kab\}Kh$

$B \rightarrow R$(Message3)：$A, R, B, Nb, \{A, R, B, Nb, Kab\}Kh$

$R \rightarrow A$(Message4)：$A, R, B, Nb, \{A, R, B, Nb, Kab\}Kh$

其中，A 表示发起者，B 表示响应者，R 表示任意中继者。消息项中用 Na 表示随机数，Ka 表示公钥，Ka^{-1} 表示私钥，Kab 表示两个节点的共享密钥，其中小写字母表示产生该项的节点。特别地，单向散列函数用 Kh 表示（这里的小写字母不表示节点），且它只有加密密钥，没有相应的解密密钥。

笔者在下节将重点分析路由三段式中不完善之处，并提出路由五段式分析模型和任意中继者可信条件。

4 任意中继者可信条件

路由三段式的模型结构存在下面几点不足之处：

①从整体方面，路由三段式将所有的中继节点形式化成一个中继者角色 R，掩盖了各个中继节点消息的差异性。在不同的协议中，各个中继节点传输的消息一般来说是不一样的，例如不同的消息积累路由或者签名。而仅用一个中继者角色代表所有中继节点，却忽略了上述情况。假定 SRP 协议中继者 R 由 $R0$，$R1$，$R2$ 3 个节点组成，路由请求阶段中 $R0$ 接收到的消息 Message1_$R0$ 为 $A, Na, \{Na, Kab\}Kh$，路由请求阶段中 $R1$ 接收到的消息 Message1_$R1$ 为 $A, R0, Na, \{Na, Kab\}Kh$，显然这两种消息不同。推广可得：协议的整个运行过程中，中继者 R 的不同节点接收、发送消息的差异性在路由三段式中未能体现出来。

②从细节方面，路由三段式中，与 R 有关的操作只有接收 message1、发送 message2、接收 message3、发送 message4。其中接收 message1 的实际行为主体应该是所有中继节点中的第一个节点，发送 message2 的实际行为主体应该是所有中继节点中的最后一个节点，message3、message4 类似。这样 R 的操作仅反映部分节点的部分操作。例如当中继节点数多于一个时，所有中继节点中的第一个节点 A 先接收到 message1，然后 A 会发送另一个消息 msg（msg 不一定与 message1 消息相同），但 msg 在路由三段式里面没有反映出来。假定 SRP 协议中继者 R 由 $R0$，$R1$，$R2$ 3 个节点组成，路由请求阶段 $R0$ 接收到消息 Message1_$R0$ 后，发送消息 msg=A，$R0, Na, \{Na, Kab\}Kh$，消息 msg 在路由三段式中未被体现出来。

③从特殊情况方面，假如路由路径上两端的中继节点转发了数据 X，而中间部分中继节点未转发数据 X，这种情况是否满足中继者可信条件呢？很明显应该不满足。但对于 S，D 来说，中继者角色 R 这个整体确实转发了数据 X。路由三段式中继者可信条件不能清楚辨别这一点。文献[1]给出的攻击实例中即为这种情况（详见 5.2 节）。

基于上述原因，笔者在路由三段式基础上设计出路由五段式的分析模型，模型将任意中继节点 N 抽象出来，并增加前段路由 Ra、后段路由 Rb。路由协议的发现阶段按照如图 2

所示形式进行形式化。

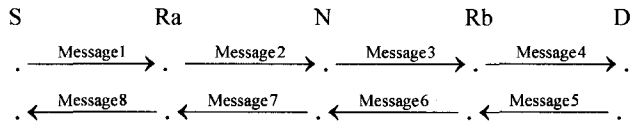

图 2　路由五段式

根据以上分析，保留一致性属性中两种角色（发起者和响应者），中继者角色更改为任意中继者角色，并增加前段路由 Ra 角色和后段路由 Rb 角色。将 Ad-hoc 路由协议的中继者可信条件更改为任意中继者可信条件，详细描述如下。

任意中继者可信条件：每次发起者 A 和响应者 B 使用数据 X 完成一轮协议执行时，任意中继者确实转发过数据 X，并且认为数据 X 的源和目的节点分别为前段路由 Ra 和后段路由 Rb（称为任意中继者保证）。

路由五段式串空间性质：路由五段式中不必考虑前段路由 Ra、后段路由 Rb 的串。

理由：路由五段式中任意中继者角色可代表路由中的任意一个中继节点，而 Ra、Rb 角色的合法性可以由任意中继节点通过递归法来保证。假如 Ra 或 Rb 中存在某节点不满足合法性即受到攻击，则可认为任意中继者角色代表该节点，重新定义 Ra、Rb，这样可得出任意中继者 N 不满足合法性的结论。因此只要满足任意中继者的合法性，即可得出 Ra、Rb 的合法性。这样，仅分析任意中继者角色串便可代表对所有中继节点行为串进行分析。

任意中继者可信条件保证了所有中间节点的合法性，一致性条件保证源和目的节点的合法性，因此这两个条件保证了参与路由协议运行的所有节点的合法性。

5　安全协议 SRP 分析

举例来说，路由协议 SRP 经过路由五段式模型分析，形式化可表示如下：

$A \rightarrow Ra$(Message1)：$A, Na, \{Na, Kab\}Kh$

$Ra \rightarrow N$(Message2)：$A, Ra, Na, \{Na, Kab\}Kh$

$N \rightarrow Rb$(Message3)：$A, (Ra, N), Na, \{Na, Kab\}Kh$

$Rb \rightarrow B$(Message4)：$A, (Ra, N, Rb), Na, \{Na, Kab\}Kh$

$B \rightarrow Rb$(Message5)：$A, (Ra, N, Rb), B, Nb, \{A, (Ra, N, Rb), B, Nb, Kab\}Kh$

$Rb \rightarrow N$(Message6)：$A, (Ra, N, Rb), B, Nb, \{A, (Ra, N, Rb), B, Nb, Kab\}Kh$

$N \rightarrow Ra$(Message7)：$A, (Ra, N, Rb), B, Nb, \{A, (Ra, N, Rb), B, Nb, Kab\}Kh$

$Ra \rightarrow A$(Message8)：$A, (Ra, N, Rb), B, Nb, \{A, (Ra, N, Rb), B, Nb, Kab\}Kh$

其中，A 表示发起者，B 表示响应者，N 表示任意中继者，Ra、Rb 分别为前段路由、后段路由。消息项中用 Na 表示随机数，Ka 表示公钥，Ka^{-1} 表示私钥，Kab 表示两个节点的共享密钥，其中下标表示产生该项的节点。特别地，单向散列函数用 Kh 表示（这里的下标不表示节点），它只有加密密钥，没有相应的解密密钥。

5.1　形式化

根据上述方法，可以得出如下发起者串、响应者串和任意中继者串。

发起者串：Init$[Na, Nb, Kab, Kh, A, B, R]$

其迹为

$+A, Na, \{Na, Kab\}Kh$

$-A, R, B, Nb, \{A, R, B, Nb, Kab\}Kh$；

响应者串：Resp$[Na, Nb, Kab, Kh, A, B, R]$

其迹为

$-A, R, Na, \{Na, Kab\}Kh+$

$A, R, B, Nb, \{A, R, B, Nb, Kab\}Kh$；

任意中继者串：Intermediate$[Na, Nb, Kh, Kab, A, B, Ra, N, R]$

其迹为

$-A, Ra, Na, \{Na, Kab\}Kh$

$+A, (Ra, N), Na, \{Na, Kab\}Kh$

$-A, R, B, Nb, \{A, R, B, Nb, Kab\}Kh$

$+A, R, B, Nb, \{A, R, B, Nb, Kab\}Kh$

其中，$R=(Ra, N, Rb)$。

对于 Ad-hoc 路由协议来说，一般只分析发起者节点、响应者节点均为可信节点的路由安全性。

定义 1　一个被渗透的串空间(Σ, P)是一个 SRP 空间，Σ由下列 4 类串构成：

攻击者串 $s \in P$；

路由发现发起者串 $s \in$ Init$[Na, Nb, Kab, Kh, A, B, R]$；

路由发现响应者串 $s \in$ Resp$[Na, Nb, Kab, Kh, A, B, R]$；

路由发现任意中继者串 $s \in$ Intermediate$[Na, Nb, Kh, A, B, Ra, N, R]$。

网络中节点包括可信节点和敌手节点，节点具有对称的双向通信能力。敌手模型为 active-1-1[1]，敌手节点通信能力与可信节点相同。

单个可信节点的消息串只能为源节点串、响应者串、任意中继者串中的一种，而敌手节点的攻击者串则是不确定的。

下节给出攻击实例，以验证路由五段式分析模型相对于路由三段式的优越性。

5.2　攻击实例分析

图 3 示出网络拓扑结构，P 为敌手节点，其他为可信节点。节点 A 试图与节点 B 建立一条路由，攻击实例中协议运行返回一条不存在路由。

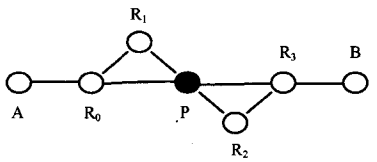

图 3　网络拓扑图

详细攻击过程如下：

①A 首先广播消息 $msg1=A, Na, \{Na, Kab\}Kh$；

②$R0$ 接收到 $msg1$ 后广播消息 $msg2=A, (R0), Na, \{Na, Kab\}Kh$；

③P 接收到 $msg2$ 后，以 $R2$ 身份广播消息 $msg3=A, (R0, R1, C, R2), Na, \{Na, Kab\}Kh$，其中 C 为任意标识，且与 $R1$，$R2$ 不相邻；

④$R3$ 接收到 $msg3$ 后发送给 B，B 验证通过并发送返回消息 $msg4$ 给 $R3$，$msg4=A, (R0, R1, C, R2, R3), B, Nb, \{A, (R0, R1, C, R2, R3), B, Nb, Kab\}Kh$；

⑤$R3$ 接收 $msg4$ 后将其转发给节点 $R2$，敌手节点 P 截获该消息，并以 $R1$ 身份将 $msg4$ 发送给 $R0$，然后 $R0$ 将其发送给 A，验证通过。

协议运行完毕，接受一条不存在路由$(A, R0, R1, C, R2,$

$R3,B$)，攻击成功。

整个攻击过程路由($R0,R1,C,R2,R3$)两端的中继节点 $R0,R3$ 均转发了路由请求数据 X，而中间部分中继节点未转发数据 X，但对于 A,B 来说，中继者角色 $R=(R0,R1,C,R2,R3)$这个整体转发了数据 X。路由三段式中将所有中继节点抽象为一个角色，不能清晰合理地辨别这种情况，因而有必要将所有中继节点分为多个角色，继而推导出路由五段式抽象模型和任意中继者可信条件。

定理 1 上述攻击实例不满足任意中继者可信条件。

证明：任意中继者可信条件定义为任意中间路由节点均转发路由请求数据 X，并且数据 X 的源和目的节点分别为前段路由 Ra 和后段路由 Rb。

上述攻击实例中继者角色 $R=(R0,R1,C,R2,R3)$，对于中间路由节点 $R1$ 来说，前段路由 $Ra=(R0)$，后段路由 $Rb=(C,R2,R3)$，显然路由请求阶段 $R1$ 未在前段路由 $Ra=(R0)$、后段路由 $Rb=(C,R2,R3)$间转发请求数据 X。同理，中间路由节点 $C,R2$ 均未在该节点的前段路由、后段路由间转发数据 X，因此定理 1 成立。

定理 1 证明了：因路由三段式分析模型对中继者角色的抽象不甚合理和描述不够精确，上述攻击实例存在满足中继者可信条件的可能，但仍然不满足路由五段式分析模型中的任意中继者可信条件。

从另一角度分析，上述攻击实例能攻击成功，说明了在源节点、目的节点均为可信节点的 SRP 协议中，任意中继者串中的节点可能源自攻击者串，由此可得定理 2。

5.3 任意中继者可信条件分析

定理 2 源节点、目的节点均为可信节点的 SRP 协议中，任意中继者串中的节点可能源自攻击者串。

文献[4]证明了路由三段式下中继者串中的节点$\langle r,2\rangle$有可能源自攻击者串中的 C 串。同理，路由五段式下任意中继者串中的$\langle r,2\rangle$也可能源自攻击者串中的 C 串。

下面证明任意中继者串 $Intermediate[]$的$\langle r,3\rangle\langle r,4\rangle$也容易受到攻击。

对于 $Intermediate[]$的$\langle r,3\rangle$：$-A,R,B,Nb,\{A,R,B,Nb,Kab\}Kh$。

M：由于 Kab 不属于 Kp，因此节点$\langle r,3\rangle$不可能源自 M 串。

F：显然节点$\langle r,3\rangle$不是源自 F 串。

T：显然节点$\langle r,3\rangle$不是源自 T 串。

C：则 $g=A,B,Nb,\{A,R,B,Nb,Kab\}Kh,h=R,gh=A,R,B,Nb,\{A,R,B,Nb,Kab\}Kh$，由此可以看出该节点有可能源自 C 串。

S：显然节点$\langle r,3\rangle$不是源自 S 串。

K：显然节点$\langle r,3\rangle$不是源自 K 串。

E：由于 Kab 不属于 Kp，因此节点$\langle r,3\rangle$不可能源自 E 串。

D：由于 Kh 不存在解密密钥，显然节点$\langle r,3\rangle$不是源自 D 串。

同理，对于 $Intermediate[]$的$\langle r,4\rangle$可能受到攻击者串中的 C 串攻击。从而定理 2 得证。

由此可以看到，文献[4]证明了源节点、目的节点均为可信节点的 SRP 协议满足发起者保证、响应者保证，但定理 2 证明其不满足任意中继者可信条件。攻击者可以冒充中继者完成一轮协议的运行。源节点和目的节点将通过包含有攻击节点的路径进行通信，这将导致信息泄漏或恶意丢包，并可能返回不存在路由，即不满足路由安全定义 plausible routing[14]。这是由于 SRP 协议没有对中继节点进行认证，导致该漏洞的产生。

结束语 本文针对路由三段式中中继者角色的局限性，提出路由五段式模型，并重新完善了串空间下 Ad-hoc 路由协议的一致性和任意中继者可信条件的定义。然后以一个返回不存在路由的攻击为例，证明发送者、接收者皆为可信节点的 SRP 协议亦不满足任意中继者可信条件，以验证路由五段式模型的正确性和优越性。

从分析过程可以看出，串空间基于攻击者模型，对攻击者的基本行为进行了刻画，因此从攻击者的角度出发，明确指出协议存在哪些缺陷或漏洞，即可能存在攻击者串中的何种类型攻击，为协议设计人员提供明确的指导方向，使协议设计人员了解协议缺陷的原因，从而进行改进。

然而串空间仅对协议的消息序列进行形式化，没有对节点验证进行分析，因此仅仅根据串空间分析结果不能有效找到 Ad-hoc 路由协议的攻击实例。后续工作将重点解决如何将节点验证和串空间分析结合起来，以便简单有效地获得协议可能的攻击实例。

参 考 文 献

[1] Buttyan L, Vajda I. Towards provable security for Ad-hoc routing protocols[C]// Proc of SASN'04. Washington DC, USA, 2004:94-105

[2] 毛立强，马建峰. 可证明安全的 MANET 按需距离矢量路由协议分析[J]. 西安电子科技大学学报：自然科学版，2008，35(6)：1063-1068

[3] Burrows M, Abadi M, Needham R. A logic of authentication[J]. ACM Transactions in Computer Systems, 1990, 8(1):18-36

[4] Wang Ying-long, Wang Ji-zhi. The Security Analysis for Ad-hoc Routing Protocols Based on Improved Strand Space [C]// SPCA06: 1st International Symposium on Pervasive Computing and Applications. 2006(1):585-588

[5] Fàbrega F J T, Herzog J C, Guttman J D. Strand spaces: Why is a security protocol correct? [C]// Proc. of the 1998 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 1998:160-171

[6] Fàbrega F J T, Herzog J C, Guttman J D. Strand spaces: Proving security protocols correct [J]. Journal of Computer Security, 1999, 7(2/3):191-230

[7] Paulson L C. The inductive approach to verifying cryptographic protocols[J]. Journal of Computer Security, 1998, 6(1):85-128

[8] Guttman J D, Fàbrega F J T. Authentication tests[C]// Proc. of the 2000 IEEE Symp. on Security and Privacy. Los Alamitos: IEEE Computer Society Press, 2000:96-109

[9] Guttman J D, Fàbrega F J T. Authentication tests and the structure of bundles [J]. Theoretical Computer Science, 2002, 283(2):333-380

[10] Perkins C E, Royer E M. Ad-hoc on-demand distance vector routing[C]// Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications. New Orleans, 1999:90-100

[11] Johnson D B, Maltz D A, Hu Y C. The dynamic source routing protocol for mobile Ad-hoc networks (DSR) [EB/OL]. IETF MANET Working Group. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt, 2004

[12] 宋震，张艳，李舟军，等. 安全协议的形式化描述和分析[J]. 计算机科学，2003，30(8)：24-27

[13] 陈平，刘东喜，白英彩. 安全协议的形式化分析方法研究[J]. 计算机应用与软件，2003，5：48-50

[14] Acs G, Buttyan L, Vajda I. Provable Security of On-demand Distance Vector Routing in Ad-hoc Networks [C]// Proc of ESAS2005, LCNS3813. Berlin: Springer, 2005:113-127