doi:10.3969/j.issn.1000-436x.2013.z1.008

基于 CSP 方法的移动自组织网络认证协议 TAM 的分析与改进

刘礼才[1,2]，殷丽华[2]，郭云川[2]，孙燕[1,2]
(1. 北京邮电大学 计算机学院，北京 100876；2. 中国科学院 信息工程研究所，北京 100195)

摘 要：针对移动自组织网络认证协议应对安全威胁、满足安全目标的有效性问题，提出了采用基于通信顺序进程（CSP, communicating sequential process）和模型检测的协议分析方法，对移动自组织网络的代表性认证协议 TAM 进行分析、建模、检验并改进。首先采用 CSP 方法对 TAM 中参与者的通信行为建立模型、给出了安全目标的安全规范；然后利用模型检测工具 FDR 验证了 TAM 的 CSP 进程，结果表明 TAM 不满足认证性和机密性安全规范；最后对 TAM 进行了改进并检验，结果表明改进后的 TAM 满足安全目标，实验表明与 TAM 相比，改进的 TAM 在合理的簇规模情况下增加可接受的额外开销。

关键词：移动自组织网络；认证协议；安全协议分析；通信顺序进程；TAM
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0058-09

Analysis and improvement for authentication protocols of mobile ad hoc network with CSP approach

LIU Li-cai[1,2], YIN Li-hua[2], GUO Yun-chuan[2], SUN Yan[1,2]
(1. School of Computer Science, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100195, China)

Abstract: Authentication protocols are often adopted to reduce the security threats in mobile ad hoc network(MANET). However, a vulnerable protocol might bring more serious threats to MANET. As a result, formal verifications of security protocols become more important. An approach based on the communicating sequential process (CSP) and Model Checking tool FDR was proposed to model and verify a typical authentication protocol of MANET, callced TAM. First, the communication behaviors of all participants in TAM and its security (authentication and confidentiality) specifications were formally modeled using CSP. Second, based on these models, the participants' behaviors were verified by FDR and the verification result indicates that the original TAM could not guarantee authentication and confidentiality. Finally, an improvement was proposed and the experiment result shows that the improved TAM satisfies security goals and increases an acceptable consumption in the case of a reasonable size of clusters compared with the original TAM.

Key words: MANET; authentication protocols; security protocol analysis; communicating sequential process; TAM

1 引言

移动自组织网络(MANET, mobile ad hoc network)是由一组带有无线收发装置的移动节点组成的自组织、多跳的无线自治网络系统[1]，它不依赖于任何固定的基础设备和管理中心，而是通过资源有限的移动节点间的相互协作和自组织来维持网络连接和实现数据传递[2]。移动自组织网络已被应用到众多重要领域，如国防军事、情报预警、环境监测、智能交通、医疗健康、居家智能、制造业等，已成为研究热点[3]。与传统网络相比，移动自组织网络具有无中心、多跳、自组织、有限资源(能源、带宽、存储空间)和弱能力(计算能力、通信能力)等特点[4]。

由于自身特点和开放的应用环境，使得移动自组织网络具有易攻击、节点易被捕获、拓扑动态变

收稿日期：2013-07-31
基金项目：国家自然科学基金资助项目(61100181, 61070186, 61100186)
Foundation Item: The National Natural Science Foundation of China (61100181, 61070186, 61100186)

化、安全策略简单等安全弱点[4~6]。为应对移动自组织网络的安全威胁，使其提供可靠服务，研究者提出了很多有意义的认证解决方案和协议，如 TESLA[7]、TESLA++[8]、LHAP[9]、TSVC[10]、Structural Results[11]、JATC[12]和 TAM[2]等。TESLA[7]是一种采用单向散列链进行消息认证的广播认证协议，由于具有高效、低开销等特点，因此被广泛使用，但是不适用于大规模的动态网络中。TESLA++[8]是基于 TESLA 改进而得的一种面向车载自组网的消息认证协议，它通过建立单向散列链来认证对称密钥，减少认证过程中的计算量和资源消耗，能够抵御 DoS 攻击和提供不可抵赖性。LIN 等基于 TESLA 提出了一种高效安全的认证方案 TSVC[10]，该方案中节点首先向邻居广播散列链，邻居通过验证由散列链元素生成的 MAC 来验证消息的真实性，具有极短的延迟和很小的通信开销等优点，但是在快速变化的大规模动态网络拓扑中，时间同步和顽健性不够理想。BU[11]提出了一种持续用户认证和入侵检测相结合的分布式解决方案 structural result，解决了安全性和资源冲突的问题。为了提高吞吐量，GUAN[12]提出了一种针对移动自组织网络合作通信的结合消息认证和拓扑控制方案 JATC。YOUNIS [2]提出了一种适用于大规模密集自组织网络的分层多播认证方案 TAM，利用时间不对称性和密钥不对称性来进行消息认证，被认为具有低开销、低延迟，高可扩展性和适用性等优点。TAM 协议继承了著名的无线网络认证协议 TESLA 的优点，且克服了其缺点，是 MANET 认证协议的典型代表，对其进行协议分析具有重要的意义。

认证协议通过协调和规范移动自组织网络中节点的通信行为，使得节点能够在高度未知、充满敌意的环境中顺利完成通信服务。为了提供安全、高效、可信的通信服务，认证协议必须满足特定的安全目标[13,14]：1)机密性，保证机密信息、路由信息不泄露给未经授权的用户；2)可用性，保证网络在需要时可靠地提供有效服务；3)认证性，保证信息和节点身份不被伪造、假冒、篡改，包括确保其抗抵赖性、完整性和真实性。

协议的形式化分析方法是采用标准的方法对协议进行分析和建模，以检查协议是否满足特定安全目标的行之有效的手段，能够准确地描述协议的边界、行为和特性，验证安全规范。目前，协议的形式化方法主要有推理逻辑方法(如 BAN 逻辑[15])、定理证明方法(如串空间[16])、模型检测方法(如基于 CSP 的 FDR[17~19])、互模拟等价方法(如 SPI 演算[20])、混合方法(如 NRL 协议分析器[21])等。CSP 是专为描述并发系统中实体的通信行为而设计的抽象语言，良好的语义使其对协议的描述极为接近协议的本义[17]。基于 CSP 的模型检测方法是将协议的安全性问题归结为协议的 CSP 进程是否满足安全规范的问题，验证协议是否满足安全属性[18]。因此，CSP 方法是分析移动自组织网络认证协议的有效方法。

本文提出了采用基于 CSP 的模型检测方法对移动自组织网络认证协议 TAM 进行分析、建模、检验并改进。首先采用 CSP 方法对 TAM 中参与者的通信行为建立模型，给出了认证性和机密性等安全目标的安全规范；然后利用模型检测工具 FDR 验证了 TAM 的 CSP 模型，结果表明 TAM 不满足认证性和机密性安全规范；最后对 TAM 进行了改进，模型检测结果表明改进 TAM 协议满足安全目标。通过模拟实验表明：在合理的簇大小情况下，改进 TAM 协议增加的开销在可接受的范围之内。

2　预备知识

2.1　CSP 概述

CSP 是著名计算机科学家 Hoare C A R 于 1978 年为解决并发现象而提出的代数理论，是一种描述并发系统中通信实体交互行为的分布式抽象语言[17]。CSP 具有进程代数的特点，擅长描述事件并发和进程交互，具有较为完整的代数演算能力，因此，CSP 广泛用于描述通过传递消息进行通信、组成构件间相互影响的并行代理系统，如通信协议、分布式系统等。

2.2　CSP 基本算子

在 CSP 中，一个或一系列动作组成一个事件；而进程通过它能执行的通信事件来定义，是一系列动作集合。进程间通过通信进行交互，通信表现为可见事件和动作。不可见动作 τ 与可见动作组成所有动作集合 $\sum$。CSP 定义了完整的运算符和规则来描述并发系统[22]，其基本运算符和规则如表 1 所示。

表 1 中，*Stop* 表示停止进程，*Skip* 表示进程成功终止执行。进程 P_1 表示先后执行事件 x 和 y 之后成功终止。进程 P_2 表示循环执行 x 和 y 事件的递归定义。进程 P_1 和 P_2 描述如式(1)所示。

$$\begin{aligned} P_1 &= x \to y \to Skip \\ P_2 &= y \to x \to P_2 \end{aligned} \tag{1}$$

表 1 CSP 基本规则

规则	语义	规则	语义
Stop	停止进程	*Skip*	进程成功终止
P,Q	顺序组合	$\mu p.F(p)$	递归进程
$a \to b$	事件前缀	$a \to P$	进程事件前缀
$?x:A \to P(x)$	事件前缀选择	$c?x:A \to P(x)$	输入前缀选择
$\Box x:S$	集合外部选择	$P \Box Q$	进程间的选择
$P \prod Q$	非确定选择	$P \parallel Q$	紧接并行
$P \underset{x}{\parallel_Y} Q$	同步并行	$P \underset{Y}{\parallel} Q$	接口并行
$\lvert\lvert\lvert S$	普通穿插	$P \setminus X$	事件隐藏
$P[\![R]\!]$	进程重命名	$P = F(P)$	递归定义

进程 P_3 是根据外部环境选择执行进程 P_1 或 P_2，如果外部选择事件是 x，则执行进程 P_1；反之，则执行 P_2。进程 P_4 表示进程 P_1 和 P_2 都可能执行。进程 P_3 和 P_4 描述如式(2)所示。

$$\begin{aligned} P_3 &= P_1 \Box P_2 \\ P_4 &= P_1 \prod P_2 \end{aligned} \tag{2}$$

协议中的参与者(通信实体)通过信道传递消息进行通信。CSP 定义了几类信道：信道 *Receive* 和 *Send* 代表诚实实体间的标准通信，其中，*Receive* 表示接收消息，*Send* 表示发送消息；信道 *Hear* 和 *Say* 代表入侵者收到或发送消息；信道 *Leak* 表示消息可能被泄漏。

2.3 基于 CSP 的模型检测方法

使用进程代数 CSP 和模型检测工具 FDR 分析认证协议的方法是当前分析认证协议的最著名的形式化分析方法之一。Lowe[18,19]首先提出采用 CSP 方法和模型检测技术对 Needham-Schroeder[23]公开密钥协议进行形式化分析，发现并改进了协议的缺陷。CSP 方法将安全协议是否满足安全目标的问题归结为安全协议的 CSP 进程是否满足相应安全规范的问题。

如图 1 所示，CSP 方法的主要过程为：1)对协议进行 CSP 建模，对协议中参与者和入侵者的通信行为用 CSP 进程表示；2)将协议要满足的安全目标用 CSP 表示为安全规范；3)将协议模型和安全规范输入模型检测工具 FDR，FDR 搜索状态空间，检测协议模型中是否存在不满足安全规范的行为；4)如果存在，则协议不满足安全目标，FDR 给出攻击路径；如果不存在，则协议满足安全目标。在建模时，安全协议分析编译器 Casper(complier for the analysis of security protocols)[24]简化了生成协议的 CSP 描述的复杂过程。

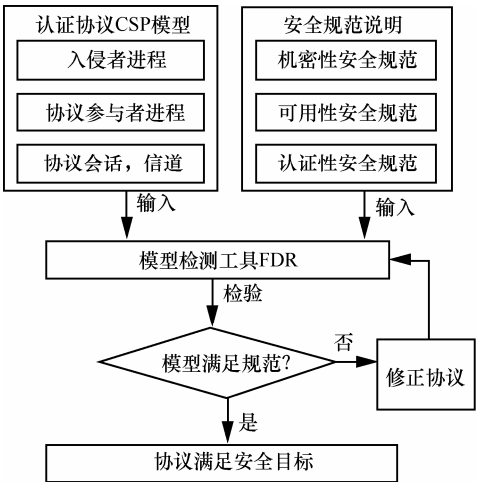

图 1 CSP 方法的协议分析过程

3 认证协议 TAM 的形式化分析

3.1 认证协议 TAM 简介

移动自组织网络认证协议 TAM 是 Younis 提出的针对大规模 ad hoc 网络的多播分层认证协议[2]，通过将节点分簇来管理网络，每个簇由一个可以到达所有簇内节点的簇头管理，能够到达其他簇的节点充当网关，其余节点为普通成员，图 2 是一个移动自组织网络分簇结构的示例。TAM 利用单向散列函数串和消息认证码[25](MAC, message authentication codes)进行簇内和簇间的消息认证。

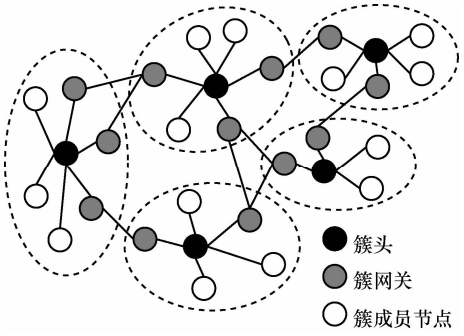

图 2 移动自组织网络分簇结构示例

如图 3 所示，TAM 认证机制可归纳为如下步骤。

1) 发送者 S 生成密钥池 M，并将密钥安全地分配给含有接收者的簇头，$K_j^{inter,s}$ 表示 S 生成的第 j 个密钥，假设该密钥分配给簇头 CH_a；簇头选择密钥 $K_0^{intra,r}$，并用单向散列函数以 $K_0^{intra,r}$ 递归生成一次性的密钥串，其中，有 $K_i^{intra,r}=H(K_{i-1}^{intra,r})=H^i(K_0^{intra,r})$，与接收者共享最后一个密钥 $K_l^{intra,r}$。

2) 建立时间同步，使得发送者与接收者有相同的时间参考。

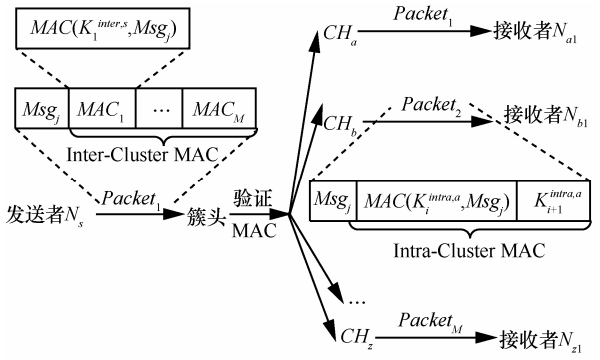

图 3　TAM 认证机制

3) 发送者用分配给其簇头的密钥 $K_j^{inter,s}$ 生成 $MAC(K_j^{inter,s}, Msg)$，然后广播添加 *MAC* 的消息。

4) 簇头接收消息后，用分配的密钥验证 *MAC*，如果验证不通过，则终止；如果验证通过，则用密钥 $K_i^{intra,r}$ 生成 $MAC(K_i^{intra,r}, Msg)$，将 *MAC* 和前一个 *MAC* 的密钥 $K_{i+1}^{intra,r}$ 添加到消息中，然后在簇内广播消息。

5) 簇内接收者在接到下一个消息时验证上一个消息，因为密钥有 $K_{i+1}^{intra,a}=H(K_i^{intra,a})$，可用 $K_i^{intra,a}$ 来验证 $K_{i+1}^{intra,a}$ 和 $MAC(K_i^{intra,a}, Msg)$。

TAM 的认证机制可以用如下消息表示，其中，K_{rs} 为发送者和接收者之间共享的密钥。K_{chs} 为发送者和簇头之间共享的密钥。

Message 1: $R\rightarrow S$: N_r

Message 2: $S\rightarrow R$: $\{N_r|T_s|T_i|T_{int}\}K_{rs}$

Message 3: $S\rightarrow CH$: $N_s|\{K_i^{inter,s}\}K_{chs}$

Message 4: $S\rightarrow CH$: $Msg|MAC(K_1^{inter,s},Msg)$, $MAC(K_2^{inter,s}, Msg),\cdots, MAC(K_m^{inter,s}, Msg)$

Message 5: $CH\rightarrow R$: $Msg \mid MAC(K_i^{intra,r}, Msg)|K_{i+1}^{intra,r}$

3.2　认证协议 TAM 建模

CSP 方法将安全协议描述为并发进程的交互过程，并对协议中的所有参与者进行建模。认证协议 TAM 中有 3 个参与者：发送者(initiator) *S*、簇头 CH (cluster head)和接收者 *R*(responder)，它们通过含有入侵者 *Intruder* 的不可信媒介通信，因此 TAM 有 4 个 CSP 进程。

发送者 *S* 与簇头 *CH* 和接收者 *R* 进行通信。首先，*S* 与 *R* 建立时间同步，使得发送者与接收者有相同的时间参考。如果 *S* 认同与 *R* 的通信细节，则发出信号 *signal.Commit*1*_Initiator.S.R*，该信号与信号 *signal.Running_Responder.R.S* 相对应。然后，*S* 用分配给其簇头的密钥生成 *MAC*，将 *MAC* 添加到消息中，然后广播消息。如果能够保证机密信息只被诚实实体所知，则发出信号 *signal_Claim_Secrect*。*S* 的进程描述如式(3)所示。

$$
\begin{aligned}
&Initiator(S)\triangleq\\
&\Box R: Agent, Nr\in Nonce, K_i^{intra,r}\in SharedKey,\\
&\quad Krs\in SessionKey\cdot env.S.R\rightarrow\\
&\quad receive.R.S.Nr\rightarrow\\
&\quad send.S.R.(\{Nr.Ts.Ti.Tint\}Krs)\rightarrow\\
&\quad signal.Commit1\_Initiator.S.R.Nr\rightarrow\\
&\Box CH: Agent, K_i^{inter,s}, Kchs\in SharedKey,\\
&\quad send.S.CH.(\{Ns.K_i^{inter,s}\}Kchs)\rightarrow\\
&\quad send.S.CH.(Msg.MAC(K_i^{inter,s}, Msg))\rightarrow\\
&\quad signal.Running2\_Initiator.S.CH.K_i^{inter,s}\rightarrow\\
&\quad signal.Running3\_Initiator.S.R.Nr\rightarrow\\
&\quad \text{if } CH\in Honest\\
&\qquad \text{then } signal.Claim\_Secret.S.K_i^{inter,s}.\{CH\}\\
&\qquad\quad \rightarrow SKIP\\
&\quad \text{else } SKIP
\end{aligned}
\tag{3}
$$

ClusterHead CH 表示簇头节点，与发送者 *S* 和接收者 *R* 进行通信，*CH* 接收并验证 *S* 发来的消息，然后转发给 *R*，其进程描述如式(4)所示。

$$
\begin{aligned}
&ClusterHead(CH)\triangleq\\
&\Box S: Agent, K_i^{inter,s}, Kchs\in SharedKey,\\
&receive.S.CH.(\{Ns.K_i^{inter,s}\}Kchs)\rightarrow\\
&receive.S.CH.(Msg.MAC(K_i^{inter,s}, Msg))\rightarrow\\
&\text{if } (Verify(MAC(K_i^{inter,s}, Msg)))\\
&\left\{\begin{array}{l}
signal.Commit2\_ClusterHead.CH.S.K_i^{inter,s}\rightarrow\\
\Box R: Agent, K_i^{intra,r}\in SharedKey\\
\quad send.CH.R.(Msg.MAC(K_i^{intra,r}.Msg).K_{i+1}^{intra,r})\rightarrow\\
\quad signal.Running4\_ClusterHead.CH.R.K_i^{intra,r}\rightarrow\\
\quad \text{if } R\in Honest\\
\qquad \text{then } signal.Claim\_Secret.CH.K_i^{intra,r}.\{R\}\\
\qquad\quad \rightarrow SKIP\\
\quad \text{else } SKIP\\
SKIP
\end{array}\right.\\
&\text{else } SKIP
\end{aligned}
\tag{4}
$$

Responder R 表示消息接收节点，与簇头 *CH* 和发送者 *S* 进行通信，*R* 向 *S* 发送请求并建立时间同

步，然后接收并验证 *CH* 发来的消息，其进程描述如式(5)所示。

$$
\begin{aligned}
&Responder(R,Nr)\triangleq\\
&\Box S:Agent,Nr\in Nonce,K_i^{intra,r}\in SharedKey,\\
&\quad Krs\in SessionKey\cdot env.R.S\rightarrow\\
&send.R.S.Nr\rightarrow\\
&signal.Running1\_Responder.R.S.Nr\rightarrow\\
&receive.S.R.(\{Nr.Ts.Ti.Tint\}Krs)\rightarrow\\
&signal.Claim\_Secret.R.Krs.\{S\}\rightarrow\\
&\Box CH:Agent,K_i^{intra,r}\in SharedKey\\
&receive.CH.R.\left(Msg.MAC\left(K_i^{intra,r}.Msg\right).K_{i+1}^{intra,r}\right)\rightarrow\\
&\text{if}\left(K_{i+1}^{intra,r}==H\left(K_i^{intra,r}\right)\right)\\
&\text{then if}\left(Verify\left(MAC\left(K_i^{intra,r}.Msg\right)\right)\right)\\
&\text{then}\begin{cases}signal.Commit4\_Responder.R.CH.K_i^{intra,r}\\ \rightarrow signal.Commit3\_Responder.R.S.Nr\\ \rightarrow SKIP\end{cases}\\
&\text{else } SKIP\\
&\text{else } SKIP
\end{aligned}
\tag{5}
$$

CSP 入侵者模型基于标准 Delov-Yao 模型[26]。入侵者可以冒充其他实体监听消息(*learn.m*)和发送伪造消息(*say.m*)。入侵者进程的初始知识 *IK* 包括所有实体的身份标识，自身的身份标识、密钥、*Nonce* 值。入侵者通过对初始知识和获得的消息进行推理，得到机密消息。入侵者进程描述如式(6)所示。

$$
\begin{aligned}
&Intruder(X)=\\
&\quad learn?m:messages\rightarrow\\
&\quad Intruder\left(include\left(X\cup\{m\}\right)\right)\\
&\quad \Box say?m:X\cap messages\rightarrow Intruder(X)
\end{aligned}
\tag{6}
$$

3.3 认证协议 TAM 的安全规范

在验证协议安全性之前，需要明确协议的安全需求并将其描述为安全规范。在分析协议的过程中，所有参与者满足安全规范，并且入侵者使用任何方式都不能破坏安全需求，则认为协议是安全的。

在本文中，主要讨论认证性安全规范和机密性安全规范。认证性安全规范要求协议保证参与者之间的协议会话存在一一对应关系，并且保证参与者对会话中的所有细节和数据认可，确保消息的一致性。认证性安全规范描述如式(7)所示。

$$
\begin{aligned}
&Auth\_Spec\triangleq Init\_Auth\_Spec\,|||\\
&\quad Resp\_Auth\_Spec\,|||\,Clus\_Auth\_Spec\\
&Init\_Auth\_Spec_0(S,R,Nr)\triangleq\\
&\quad signal.Running3\_Initiator.S.R.Nr\rightarrow\\
&\quad signal.Commit3\_Responder.R.S.Nr\rightarrow STOP\\
&Resp\_Auth\_Spec_0(R,S,Nr)\triangleq\\
&\quad signal.Running1\_Responder.R.S.Nr\rightarrow\\
&\quad signal.Commit1\_Initiator.S.R.Nr\rightarrow S\\
&Init\_Auth\_Spec_1\left(S,CH,K_i^{inter,s}\right)\triangleq\\
&\quad signal.Running2\_Initiator.S.CH.K_i^{inter,s}\rightarrow\\
&\quad signal.Commit2\_ClusterHead.CH.S.K_i^{inter,s}\rightarrow\\
&\quad STOP\\
&Clus\_Auth\_Spec_0\left(CH,R,K_i^{intra,r}\right)\triangleq\\
&\quad signal.Running4\_ClusterHead.CH.R.K_i^{intra,r}\rightarrow\\
&\quad signal.Commit4\_Responder.R.CH.K_i^{intra,r}\rightarrow\\
&\quad STOP
\end{aligned}
\tag{7}
$$

机密性安全规范要求协议保证机密信息只为诚实实体所知，入侵者通过已有知识和推导方法不能得到机密信息。机密性安全规范描述如式(8)所示。

$$
\begin{aligned}
&Secret\_Spec\triangleq|||_{s:ALL\_SECRETS}\ Secret\_Spec_0(s)\\
&Secret\_Spec_0(s)\triangleq\\
&\quad signal.Claim\_Secret?S!s?R\rightarrow\\
&\quad\begin{cases}\text{if } R\notin Honest\\ \quad\text{then } Secret\_Spec_0(s)\\ \text{else } Secret\_Spec_1(s)\end{cases}\\
&\quad\Box leak.s\rightarrow Secret\_Spec_0(s)\\
&Secret\_Spec_1(s)\triangleq\\
&\quad signal.Claim\_Secret?S!s?R\rightarrow\\
&\quad Secret\_Spec_1(s)
\end{aligned}
\tag{8}
$$

如果 TAM 协议中参与者的进程能够满足以上认证性和机密性的安全规范，则认为 TAM 协议能够保证认证性和机密性，满足安全目标。

3.4 认证协议 TAM 的模型检测与改进

使用进程代数 CSP 和模型检测器 FDR 分析安全协议被认为是有效的方法[19, 24]，但是只有熟练掌握 CSP 的人才能生成协议的 CSP 描述。安全协议分析编译器 Casper 简化了复杂的生成协议 CSP 描述过程。Casper 编译器为协议生成 CSP 描述，建立 CSP 模型；然后将协议的 CSP 模型和安全规范输入 FDR，FDR 通过搜索状态空间检验协议参与者的

CSP 进程的执行是否满足安全规范。

通过进程代数 CSP 和模型检测工具 FDR 对移动自组织网络认证协议 TAM 进行分析和模型检验，结果表明 TAM 只满足部分安全规范，如图 4 所示。

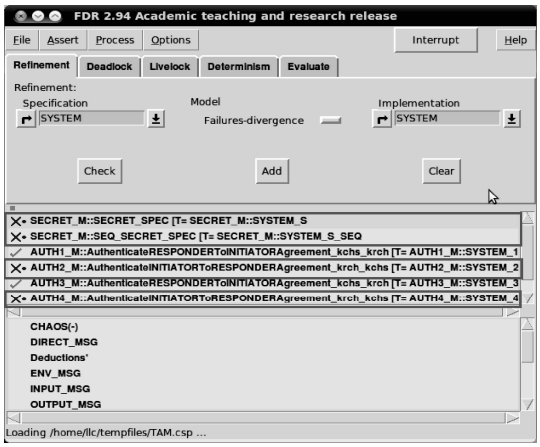

图 4　TAM 协议的 FDR 2.94 检测结果

首先，TAM 不能满足消息互认证，如 *ClusterHead* 无法认证 *Source*，*Receiver* 无法认证 *ClusterHead*，这可能造成恶意节点(被攻陷的节点)冒充 *Source* 要求 *ClusterHead* 对虚假消息进行验证，或者冒充 *ClusterHead* 要求 *Receiver* 对虚假消息进行验证。下面的消息给出一个违反认证性的反例。

Message 1: $I\_S \rightarrow CH$: $N_s|\{K_i^{inter,s}\}K_{ch}$

Message 2: $CH \rightarrow I\_S$: $N_{ch}|\{N_s\}K_{chs}$

Message 3: $I\_S \rightarrow CH$: $N_{ch}|\{K_i^{inter,s}\}K_{ch}$

Message 4: $CH \rightarrow I\_S$: $N_{ch}2|\{N_{ch}\}K_{chs}$

Message 5: $I\_S \rightarrow CH$: $\{N_{ch}\}K_{chs}$

该反例表明入侵者可以伪装成发送者参与到合法的发送者和簇头之间的通信中，而簇头仍然认为在和合法发送者完成协议的运行，不能正确验证发送者的身份，违反了协议的互认证性。

其次，TAM 不能满足机密性安全规范。入侵者假装合法实体与 *S*、*CH* 和 *R* 通信，可获得机密消息。下面的消息给出一个违反机密性的反例。

Message 1: $S \rightarrow I\_CH$: $N_s|\{K_j^{inter,s}\}K_{ch}$

Message 1: $I\_S \rightarrow CH$: $N_s|\{K_j^{inter,s}\}K_{ch}$

Message 2: $S \rightarrow I\_CH$: $Msg|MAC(K_1^{inter,s}, Msg)$, $MAC(K_2^{inter,s}, Msg),\cdots,MAC(K_m^{inter,s}, Msg)$

Message 2: $I\_CH \rightarrow I\_R$: $Msg|MAC(K_i^{intra,r}, Msg)|K_{i+1}^{intra,r}$

该反例表明入侵者可以伪装成发送者和簇头参与到合法的发送者和簇头之间的通信中。建立通信后，假冒簇头可以接收到发送者的消息，并将消息发送给其簇内的假冒接收者，从而使得假冒接收者获得机密消息，违反了协议的机密性。

本文提出了改进的 TAM 协议，弥补原协议的缺陷，采取了有效措施使得 TAM 协议满足认证性和机密性的安全目标。首先，为了达到消息互认证的目的，在 *ClusterHead* 和 *Source* 的通信中增加认证会话(如下面的消息 Message 4 和 Message 5)，在 *Receiver* 和 *ClusterHead* 的通信中增加认证会话(如下面的消息 Message 8 和 Message 9)。其次，为了防止入侵者获得机密信息，将数据分组中传输的消息进行加密处理。改进 TAM 协议可用如下消息表示。

Message 1: $R \rightarrow S$: N_r

Message 2: $S \rightarrow R$: $\{N_r|T_s|T_i|T_{int}\}K_{rs}$

Message 3: $S \rightarrow CH$: $\{N_s|K_1^{inter,s}\}K_{chs}$

Message 4: $CH \rightarrow S$: $N_{ch}|\{N_s\}K_i^{inter,s}$

Message 5: $S \rightarrow CH$: $\{N_{ch}\}K_i^{inter,s}$

Message 6: $S \rightarrow CH$: $\{Msg\}K_{chs}|MAC(K_1^{inter,s}, Msg), MAC(K_2^{inter,s}, Msg),\cdots, MAC(K_m^{inter,s}, Msg)$

Message 7: $CH \rightarrow R$: $\{Msg\}K_{rch}|MAC(K_i^{intra,r}, Msg)|K_{i+1}^{intra,r}$

Message 8: $R \rightarrow CH$: $N_r|\{N_{ch}\}K_{i+2}^{intra,r}$

Message 9: $CH \rightarrow R$: $\{N_r\}K_{i+2}^{intra,r}$

利用 CSP 对改进 TAM 协议重新进行分析和建模，对协议中的 3 个参与者：发送者 *S*、簇头 *CH* 和接收者 *R* 重新描述其 CSP 进程。改进 TAM 协议增加了 *S* 和 *CH* 之间的会话，使得 *CH* 能够验证 *S* 的身份。改进 TAM 协议的 *S* 进程描述如式(9)所示。

$$
\begin{aligned}
&Initiator(S) \triangleq \\
&\Box R: Agent, Nr \in Nonce, K_i^{intra,r} \in SharedKey, \\
&\quad Krs \in SessionKey \cdot env.S.R \rightarrow \\
&\quad receive.R.S.Nr \rightarrow \\
&\quad send.S.R.(\{Nr.Ts.Ti.Tint\}Krs) \rightarrow \\
&\quad signal.Commit1\_Initiator.S.R.Nr \rightarrow \\
&\Box CH: Agent, K_i^{inter,s}, Kchs \in SharedKey, \\
&\quad send.S.CH.(\{Ns.K_i^{inter,s}\}Kchs) \rightarrow \\
&\quad signal.Running2\_Initiator.S.CH.K_i^{inter,s} \rightarrow \\
&\quad receive.CH.S.(Nch.\{Ns\}K_i^{inter,s}) \rightarrow \\
&\quad send.S.CH.(\{Nch\}K_i^{inter,s}) \rightarrow
\end{aligned}
\tag{9}
$$

$$
\begin{aligned}
&send.S.CH.\left(\{Msg\}Kchs.MAC\left(K_i^{inter,s},Msg\right)\right)\rightarrow\\
&signal.Running3\_Initiator.S.R.Nr\rightarrow\\
&\text{if } CH\in Honest\\
&\text{then}\begin{cases}signal.Claim\_Secret.S.K_i^{inter,s}.\{CH\}\\ \rightarrow SKIP\end{cases}\\
&\text{else } SKIP
\end{aligned}
$$

改进的 TAM 增加了 CH 和 R 间的会话，使得 R 能够验证 CH 的身份。改进 TAM 的 CH 进程如式(10)所示。

$$
\begin{aligned}
&ClusterHead(CH)\triangleq\\
&\square S:Agent,K_i^{inter,s}\in SharedKey,\\
&receive.S.CH.\left(\left\{Ns.K_i^{inter,s}\right\}Kchs\right)\rightarrow\\
&send.CH.S.\left(Nch.\{Ns\}K_i^{inter,s}\right)\rightarrow\\
&receive.S.CH.\left(\{Nch\}K_i^{inter,s}\right)\rightarrow\\
&receive.S.CH.\left(Msg.MAC\left(K_i^{inter,s},Msg\right)\right)\rightarrow\\
&\text{if}\left(Verify\left(MAC(K_i^{inter,s},Msg)\right)\right)\\
&\begin{cases}
signal.Commit2\_ClusterHead.CH.S.K_i^{inter,s}\rightarrow\\
\square R:Agent,K_i^{intra,r}\in SharedKey\\
send.CH.R.\left(Msg.MAC\left(K_i^{intra,r}.Msg\right).K_{i+1}^{intra,r}\right)\rightarrow\\
signal.Running4\_ClusterHead.CH.R.K_i^{intra,r}\rightarrow\\
receive.R.CH.\left(Nr.\{Nch\}K_i^{intra,r}\right)\rightarrow\\
send.CH.R.\left(\{Nr\}K_i^{intra,r}\right)\rightarrow\\
\text{if } R\in Honest\\
\quad\text{then}\begin{cases}signal.Claim\_Secret.CH.K_i^{intra,r}.\{R\}\rightarrow\\ SKIP\end{cases}\\
\text{else } SKIP\\
SKIP
\end{cases}\\
&\text{else } SKIP
\end{aligned}
\tag{10}
$$

改进 TAM 协议的 R 的进程描述如式(11)所示。

$$
\begin{aligned}
&Responder(R,Nr)\triangleq\\
&\square S:Agent,Nr\in Nonce,K_i^{intra,r}\in SharedKey,\\
&\quad Krs\in SessionKey\cdot env.R.S\rightarrow\\
&send.R.S.Nr\rightarrow\\
&signal.Running1\_Responder.R.S.Nr\rightarrow\\
&receive.S.R.\left(\{Nr.Ts.Ti.Tint\}Krs\right)\rightarrow\\
&signal.Claim\_Secret.R.Krs.\{S\}\rightarrow\\
&\square CH:Agent,K_i^{intra,r}\in SharedKey\\
&receive.CH.R.\left(Msg.MAC\left(K_i^{intra,r}.Msg\right).K_{i+1}^{intra,r}\right)\rightarrow\\
&\text{if}\left(K_{i+1}^{intra,r}==H\left(K_i^{intra,r}\right)\right)\\
&\text{then if}\left(Verify\left(MAC\left(K_i^{intra,r}.Msg\right)\right)\right)\\
&\text{then}\begin{cases}
send.R.CH.\left(Nr.\{Nch\}K_i^{intra,r}\right)\rightarrow\\
receive.CH.R.\left(\{Nr\}K_i^{intra,r}\right)\rightarrow\\
signal.Commit4\_Responder.R.CH.K_i^{intra,r}\rightarrow\\
signal.Commit3\_Responder.R.S.Nr\rightarrow\\
SKIP
\end{cases}\\
&\text{else } SKIP\\
&\text{else } SKIP
\end{aligned}
\tag{11}
$$

利用 FDR 对改进 TAM 协议的 CSP 模型进行模型检测，检测结果表明改进 TAM 协议中所有参与者的进程满足认证性安全规范和机密性安全规范。即改进 TAM 协议满足认证性和机密性安全目标，如图 5 所示。

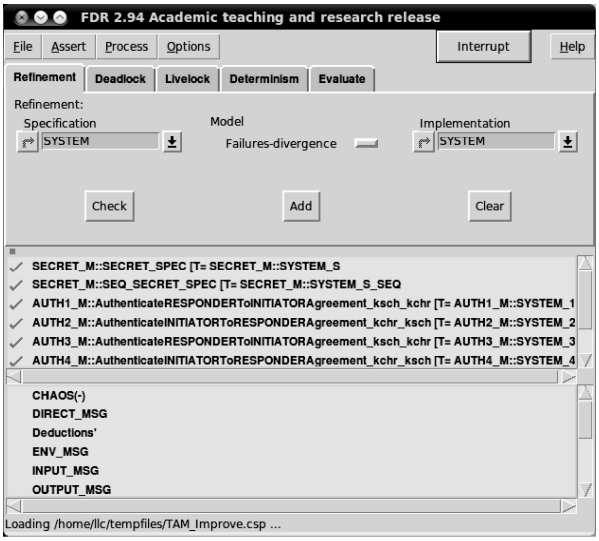

图 5　改进 TAM 协议的 FDR 2.94 检测结果

由于改进 TAM 协议增加了会话，势必增加一些代价。假设移动自组织网络中有 400 个节点，均匀分布在 200 m×200 m 的区域内。网络中节点分成 40 个簇，每个簇有 10 个节点，其中一个节点为簇头节点，可与相邻簇通信的节点充当簇网关节点，其余节点为簇成员节点，节点之间通信可达，无孤立节点。假设节点发送的消息平均 10 跳可达。通过仿真实验模拟评估改进 TAM 协议比原协议增加的开销与簇大小(簇内节点数量)的关系如图 6 所示。改进 TAM 协议增加开销百分比随着簇大小增加而增加，当网络的簇有 5、10 个节点时，开销分别增加 5.57%、9.52%；当有 20 个节点时，开销增加

22.48%，将严重影响网络通信服务质量。在 TAM[2] 中指出以 2~3 跳的簇半径形成簇较为合理，可知在本实验中簇大小约为 12，改进 TAM 增加约 11.63% 的开销，属可接受范围。由此可知，在规模合理的分簇大小情况下，改进 TAM 协议通过付出可接受的代价来保证协议的认证性和机密性。

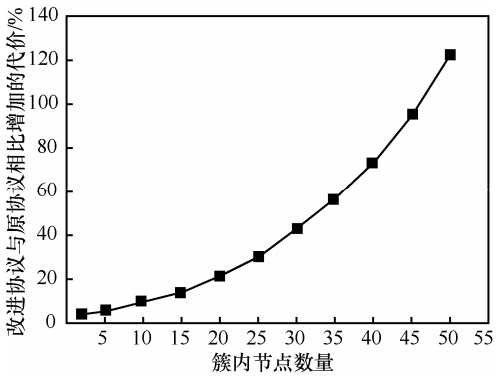

图 6　改进 TAM 协议的簇内节点数量与增加代价的关系

4　结束语

在移动自组织网络的应用中面临着各种各样的安全漏洞和安全威胁，认证协议是应对移动自组织网络的安全威胁，保证安全目标的有效途径。这些认证协议声称能够保证网络的认证性和机密性，但协议需要经过分析和检验以验证其保证安全目标的有效性。本文提出了采用基于 CSP 的模型检测方法对移动自组织网络的认证协议 TAM 进行分析、建模、检验并改进。首先，利用 CSP 对 TAM 进行建模，描述协议所有参与者和入侵者的 CSP 进程；其次，提出协议需要满足的安全需求和安全规范（认证性安全规范和机密性安全规范），并用 CSP 描述安全规范；然后，将 TAM 协议的 CSP 模型和安全规范输入模型检测工具 FDR 中进行检验，检验结果表明：TAM 协议不满足安全规范；最后，提出了一种改进的 TAM 协议，利用 CSP 和 FDR 对改进的 TAM 协议进行分析、建模、检验，检验结果表明：改进的 TAM 协议满足安全规范，能够达到认证性和机密性的安全目标。通过模拟实验表明：在合理的簇大小情况下，改进 TAM 协议增加的开销在可接受的范围之内。

参考文献：

[1] LOU W J, FANG Y G. A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions[M]. New York: Kluwer Academic Publishers, 2004.

[2] YOUNIS M, FARRAG O, ALTHOUSE B. TAM: a tiered authentication of multicast protocol for ad-hoc networks[J]. IEEE Transactions on Network and Service Management, 2012, 9(1):100-113.

[3] PERKINS C E. Ad Hoc Networking[M]. NewYork: Addison-Wesley Professional, 2008.

[4] YANG H, LUO H Y, YE F, *et al*. Security in mobile ad hoc networks: challenges and solutions[J]. IEEE Wireless Communications, 2004, 11(1):38-47.

[5] LUO J H, YE D X, XUE L, *et al*. A survey of multicast routing protocols for mobile ad-hoc networks[J]. IEEE Communications Surveys & Tutorials, 2009, 11(1):78-91.

[6] ISLAM N, SHAIKH Z A. Security Issues in Mobile Ad Hoc Network[M]. Berlin: Springer Berlin Heidelberg, 2013. 49-80.

[7] PERRIG A, CANNETI R, SONG D, *et al*. The TESLA broadcast authentication protocol[J]. RSA Cryptobytes, 2002, 5(2):2-13.

[8] STUDER A, BAI F, BELLUR B, *et al*. Flexible, extensible, and efficient VANET authentication[J]. Journal of Communications and Networks, 2009, 11(6):574-588.

[9] ZHU S C, XU S H, SETIA S, *et al*. LHAP: a lightweight hop-by-hop authentication protocol for ad-hoc networks[J]. Ad Hoc Networks, 2006, 4(5):567-585.

[10] LIN X D, SUN X T, WANG X Y, *et al*. TSVC: timed efficient and secure vehicular communications with privacy preserving[J]. IEEE Transactions on Wireless Communications, 2008, 7(12):4987-4998.

[11] BU S R, YU F R, LIU X P, *et al*. Structural results for combined continuous user authentication and intrusion detection in high security mobile ad-hoc networks[J]. IEEE Transactions on Wireless Communications, 2011, 10(9):3064-3073.

[12] GUAN Q, YU F, JIANG S, *et al*. Joint topology control and authentication design in mobile ad hoc networks with cooperative communications[J]. IEEE Transactions on Vehicular Technology, 2012, 61(6): 2674-2685.

[13] GIRUKA V C, SINGHAL M, ROYALTY J, *et al*. Security in wireless sensor networks[J]. Wirel Commun Mob Comput, 2008, 8(1):1-24.

[14] CAYIRCI E, RONG C M. Security in Wireless Ad Hoc and Sensor Networks[M]. Hoboken: John Wiley & Sons, 2009.

[15] BURROWS M, ABADI M, NEEDHAM R M. A logic of authentication[A]. Proceedings of the Royal Society of London Series A Mathematical and Physical Sciences[C]. 1989,426(1871):233-271.

[16] FABREGA F J T, HERZOG J C, GUTTMAN J D. Strand spaces: why is a security protocol correct?[A]. Proceedings of the 1998 IEEE Symposium on Security and Privacy[C]. Oakland, CA, USA, 1998. 160-171.

[17] HOARE C A R. Communicating sequential processes[J]. Commun ACM, 1978, 21(8):666-677.

[18] LOWE G. Breaking and Fixing the Needham-Schroeder Public-Key Protocol Using FDR[M]. Berlin, Heidelberg: Springer, 1996. 147-166.

[19] LOWE G, ROSCOE B. Using CSP to detect errors in the TMN protocol[J]. IEEE Transactions on Software Engineering, 1997, 23(10):659-669.

[20] ABADI M, GORDON A D. A calculus for cryptographic protocols: the spi calculus[A]. Proceedings of the 4th ACM Conference on Computer and Communications Security[C]. Zurich, Switzerland,

1997. 36-47.

[21] MEADOWS C. The NRL protocol analyzer: an overview[J]. The Journal of Logic Programming, 1996, 26(2):113-131.

[22] ROSCOE A W. The Theory and Practice of Concurrency[M]. Upper Saddle River, USA: Prentice-Hall, 2010.

[23] NEEDHAM R M, SCHROEDER M D. Using encryption for authentication in large networks of computers[J]. Commun ACM, 1978, 21(12):993-999.

[24] LOWE G. Casper: a compiler for the analysis of security protocols[J]. Journal of Computer Security, 1998, 6(1):53-84.

[25] YACINE C, HATEM B, ABDELMADJID B. A taxonomy of multicast data origin authentication: issues and solutions[J]. IEEE Communications Surveys & Tutorials, 2004, 6(3):34-57.

[26] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2):198-208.

作者简介：

刘礼才（1986-），男，江西赣州人，北京邮电大学博士生，主要研究方向为信息安全、安全属性、认证协议分析。

殷丽华（1973-），女，辽宁朝阳人，博士，中国科学院副研究员，主要研究方向为信息内容安全、安全属性计算。

郭云川（1979-），男，四川营山人，博士，中国科学院博士后，主要研究方向为信息安全、形式化方法。

孙燕（1982-），女，山东德州人，北京邮电大学博士生，主要研究方向为物联网安全与隐私保护。