ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.17, Supplement, November 2006, pp.256−261

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于改进的串空间分析 Ad Hoc 路由协议安全性*

王继志+, 王英龙

(山东省计算中心,山东 济南 250014)

Security Analysis for Ad Hoc Routing Protocols Based on Improved Strand Space

WANG Ji-Zhi+, WANG Ying-Long

(Shandong Computer Science Center, Ji'nan 250014, China)

+ Corresponding author: Phn: +86-531-82605266, Fax: +86-531-82962004, E-mail: wangjzh@keylab.net

Wang JZ, Wang YL. Security analysis for ad hoc routing protocols based on improved strand space. *Journal of Software*, 2006,17(Suppl.):256−261. http://www.jos.org.cn/1000-9825/17/s256.htm

Abstract: Based on the characteristics of Ad Hoc mobile network, the paper redefines the consistency conditions for the normal operation of the protocol and at the same time adds intermediator credibility condition, thus adapts the strand space method to the security analysis for Ad Hoc routing protocols. The SRP protocol is taken as an example for the analysis of its security and the valuable results have been obtained.
Key words: strand space; secure protocol; consistency condition; intermediator credibility condition

摘 要: 根据 Ad Hoc 移动网络特点,重新定义了串空间中协议正常运行的一致性条件,在一致性条件中增加了中继可信条件,使串空间适用于 Ad Hoc 安全路由协议分析.以 SRP 协议为例进行协议分析,得出有价值的结果.
关键词: 串空间;安全协议;一致性条件;中继可信条件

目前,对 Ad Hoc 移动网络路由协议的安全性分析主要有两大类方法:一是非形式化的方法;一是形式化的方法.非形式化方法是目前分析的主要方法,该方法采用自然语言来描述路由协议中针对入侵者的攻击所采取的安全措施.具体来说,分析步骤如下:

1) 逐一列举目前已知的针对路由协议的攻击方法;
2) 阐述针对该种攻击,路由协议中所采取的安全措施;
3) 在某种假设的场景中,分析如果攻击发生后,路由协议是如何反应的,即路由协议是如何预防攻击的发生或如何阻止已发生攻击行为的进一步进行;
4) 得出结论,对于所列举的攻击行为,路由协议是安全的.

采用非形式化的方法分析路由协议,其优缺点是显而易见的.优点是方法简便,无须借助于任何工具,采用常用的推理方法,即可得出结论.而缺点是由于分析过程没有经过严格的数学证明,其结论显然是不严格的,有可能是模糊的或有歧义的.

形式化的方法主要是对协议进行形式化,采用严格的数学推理来分析协议的安全性.主要分析步骤如下:

1) 根据具体的形式化表示方法,如形式逻辑,串空间等,对协议进行形式化;

* Supported by the Natural Science Foundation of Shandong Province of China under Grant No.Q2005G02 (山东省自然科学基金)
Received 2006-03-30; Accepted 2006-10-08

2) 确定协议的安全目标和初始假设,并用相应的形式符号表示出来;

3) 根据推理规则和初始假设,对协议的各个消息进行推理、分析,若能满足安全目标,则协议在该方法下是安全的,否则,是不安全的;

4) 根据推理过程,分析协议的缺陷和冗余性.

该方法由于采用严格的数学工具,其结论是可信的.但目前该方法主要用于有线网络中通信协议的形式化,即该方法认为通信双方的连接是稳定的,静态的.然而由于 Ad Hoc 移动网络中节点的移动性,这就给协议的形式化带来了困难,无法直接将该方法应用于 Ad Hoc 移动网络路由协议的形式化,需要根据 Ad Hoc 移动网络的特点,对形式化方法改进,使其适用于 Ad Hoc 移动网络路由协议的分析.

1 串空间基本概念[1]

串空间是一个二元组(Σ,tr),其中Σ是一个串的集合,这里的串可以用来表示任何序列,tr 表示由Σ到 A(协议运行过程中参与者可能交换的信息的集合)中元素组成的序列的一个映射.下面给出串空间中的一些基本概念:

对于一个序列 A,其中的元素是协议要发送的消息,那么 A 中的元素称为项.

子项:$t_0 \subset t_1$ 表示 t_0 是 t_1 的子项.

定义 **1**. 对于二元组$\langle \sigma,\alpha\rangle$,其中$\alpha\in A$,$\sigma$为+或−,通常记为$+t$ 或$-t$,则$(\pm A)$是有符号项的有限序列.

定义 **2**. A 上的串空间定义为序列Σ,的迹,记为$\Sigma,\rightarrow(\pm A)$.

在串空间里,通常直接用串Σ来表示串空间,而不用迹来表示,只是在表示同一迹所产生的不同实例时,要将它们区分开来.

定义 **3**.

1) 一个节点 n 表示成一个二元对$\langle s,i\rangle$.其中 s 是Σ中的元素,i 表示该节点在这个串中的序号,每一个节点属于唯一一个串,节点的集合记为 N.

2) 如果 $n_1,n_2\in N$,定义 $n_1\rightarrow n_2$ 表示 $n_1=+a,n_2=-a$,也就是消息 a 从 n_1 发送到 n_2.

3) 如果 $n_1,n_2\in N$,定义 $n_1 \Rightarrow n_2$ 表示 n_1 和 n_2 是在同一串上,并且 n_2 是紧接着 n_1 的下一个节点.

4) 一个项 t 产生于节点 n,当且仅当节点 n 符号为正且 $t\subset term(n)$,并且对于任意的节点 n 之前的节点 n',$t\not\subset term(n')$.

5) 一个项 t 称作唯一产生于节点 n 当且仅当 t 产生于唯一的节点 n,例如随机数或时间戳.

6) 假设 I 是一个无符号项集,节点 $n\in N$ 是 I 的一个入口点当且仅当 $term(n)=+a,(t\in I)$,且对于任意 n 之前的节点 n_1,$term(n_1)\notin I$.

7) 一个项 t 结束于节点 n,当且仅当节点 n 的符号为负且 $t\sqsubseteq term(n)$,并且对于任意的节点 n 之后的节点 n',$t\not\sqsubset term(n')$.

定义 **4**. 假设$\rightarrow_c\subseteq\rightarrow$,$\Rightarrow_c\subseteq\Rightarrow$,且 $c=\langle N_c,(\rightarrow_c\cup\Rightarrow_c)\rangle$是$\langle N,(\rightarrow\cup\Rightarrow)\rangle$的子图,则 c 是丛,当

(1) c 是有限的.(2) 若 $n_2\in N_c$ 且 $term(n_2)$是负的,则存在唯一的 n_1 使得 $n_1\rightarrow_c n_2$.(3) 若 $n_2\in N_c$ 且 $n_1\Rightarrow n_2$,则 $n_1\Rightarrow_c n_2$.(4) c 是非循环的.

上述定义描述了如下性质:

一个串(或者说进程)可以发送或接收消息,但不能同时既发送又接收消息.

当一个串接收消息时,则存在一个唯一的节点发送该消息.

当一个串发送消息时,可以有许多串接收消息.

定义 **5**. 节点 n 在丛 $c=\langle N_c,(\rightarrow_c\cup\Rightarrow_c)\rangle$,记为 $n\in c$.串 s 在 c 中,则所有的节点都在 N_c 中.假如 c 是一个丛,则串 s 中的 c-height 是最大值 i 使得$\langle s,i\rangle\in c$,c-trace$(s)=\langle tr(s)(1),\ldots,tr(s)(m)\rangle$,其中 $m=c$-height(s).

2 攻击者能力

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由 k_p 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: $\langle +k\rangle$,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: $\langle -k^{-1}-\{h\}_k+h\rangle$,接受加密后的消息$\{h\}k$,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 协议正确性条件

在串空间中,协议的一致性属性有两个层次:

1) 强一致性条件:协议保证参与者 B(响应者)就某个数据项 X 达成一致,如果每次 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,确实存在惟一的一轮协议执行,其中 A 作为发起者也使用 X,并且认为它的响应者为 B.

2) 弱一致性条件: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.

二者区别是弱一致性条件不保证协议执行的惟一性,不能防止 A 执行了多轮与 B 对应的协议,而 B 只执行了一轮.类似地,对于发起者也存在同样的条件.

4 对串空间的改进

串空间中与一致性属性相对应地定义了两种角色,发起者和响应者.这种角色定义是与有线网络相适应的.然而由于 Ad Hoc 移动网络的特殊性[2,11,12],当我们把串空间应用到 Ad Hoc 移动网络路由协议安全性分析时[3],就会发现这种角色定义存在很大缺陷.

由于 Ad Hoc 是一种多跳的移动网络,发起者与响应者之间的通信必须通过中间节点的中继来实现.这就存在一种情况,发起者和响应者都是唯一的,但中继节点中存在恶意节点.这种情况在 Ad Hoc 移动网络路由协议的安全性分析中认为是不安全的,但如果用串空间来分析,这种情况是满足条件的.之所以出现这种情况,就是因为在 Ad Hoc 移动网络路由协议中,出现了一个新的角色,中继节点,我们把这一角色称为中继者.由于条件中没有考虑这一角色,导致分析结果与实际情况不符.

另一方面,在路由发现过程中,通常的做法是发起者采用泛洪的方式[4,11]进行广播,即发起者向所有的节点查询到目的节点的路径.由于发起者和响应者之间可能存在多条路径,导致对于发起者的一轮运行,响应者可能收到多个路由请求,对多个路由请求进行了响应,即运行了多轮,这就不满足强一致性.

因此针对 Ad Hoc 移动网络的特点,将串空间理论应用到路由协议安全性分析时,必须重新对条件进行描述.由于 Ad Hoc 移动网络路由协议的正常运行不满足强一致性条件,因此在条件中只保留弱一致性,同时针对新的角色—中继者,提出协议应满足中继者可信条件.详细描述如下:

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).

一致性条件保证了源和目的节点的合法性,而中继者可信条件则保证了中间节点的合法性.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.这两个条件与前文安全属性中的真实性是一致的,安全属性中的其他属性如何在串空间中表达,还需进一步的研究.

5 安全协议 SRP 分析

下面以安全路由协议 SRP[5−8]为例,采用串空间分析其安全性.

为简化分析过程,对于路由协议的路由发现阶段可按照如下形式进行形式化[9,10](在本节中重点分析路由发现阶段,忽略其他阶段):

$S\rightarrow R$: Message1

$R\rightarrow D$: Message2

$D\rightarrow R$: Message3

$R\rightarrow S$: Message4

其中,S 表示消息的发送节点,D 表示消息的接收节点,R 表示中继节点,Message 表示报文的消息项.消息项中用 N_a 表示随机数,K_a 表示公钥,K_a^{-1} 表示私钥,K_{ab} 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 K_h 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.虽然 Adhoc 移动网络中一次路由所经过的中继节点的个数是不确定的,但它们所发送的消息在形式上是一致的,因此没有必要把它们全部表示出来.考虑到一般性和分析的方便,用 R 来代表所有的中继节点.

举例来说,路由协议 SRP,具体形式化可表示如下:

$A\rightarrow R$: $A,N_a,\{N_a,K_{ab}\}K_h$

$R\rightarrow B$: $A,R,N_a,\{N_a,K_{ab}\}K_h$

$B\rightarrow R$: $A,R,B,N_b,\{A,R,B,N_b,K_{ab}\}K_h$

$R\rightarrow A$: $A,R,B,N_b,\{A,R,B,N_b,K_{ab}\}K_h$

其中,A 表示发起者,B 表示响应者,R 表示中继者.

5.1 形式化

根据上述方法,可以得出发起者串、响应者串和中继者串,如下:

发起者串:N_a,N_b,K_{ab},K_h,A,B,R

其迹为:$+A,N_a,\{N_a,K_{ab}\}K_h\ -A,R,B,N_b,\{A,R,B,N_b,K_{ab}\}K_h$

响应者串:N_a,N_b,K_{ab},K_h,A,B,R

其迹为:$-A,R,N_a,\{N_a,K_{ab}\}K_h\ +A,R,B,N_b,\{A,R,B,N_b,K_{ab}\}K_h$

中继者串:N_a,N_b,K_h,A,B,R

其迹为:$-A,N_a,\{N_a,K_{ab}\}K_h\ +A,R,N_a,\{N_a,K_{ab}\}K_h\ -A,R,B,N_b,\{A,R,B,N_b,K_{ab}\}K_h\ +A,R,B,N_b,\{A,R,B,N_b,K_{ab}\}K_h$

下面分别对一致性条件和中继者可信条件进行分析.对于这两个条件的证明可以采用反证法,即证明发起者串,响应者串和中继者串中的节点不可能源自攻击者串.

5.2 一致性条件分析

响应者保证:假设 Σ 是串空间,C 是丛,包含响应者串 $Resp[\,]$;K_{ab} 不属于 K_p;N_a 不等于 N_b,N_b 唯一源自 Σ,则 C 包含发起者串 $Init[\,]$.

证明:节点$\langle r,1\rangle$

M: 由于 K_{ab} 不属于 K_p,因此节点$\langle r,1\rangle$不可能源自 M 串.

F: 显然节点$\langle r,1\rangle$符号为正,不可能源自 F 串.

T: 显然节点⟨*r*,1⟩不是源自 *T* 串.

C: 则 $g=A,N_a,h=\{N_a,K_{ab}\}K_h$,由于 K_h 不存在解密密钥,攻击者无法更改 N_a,因此节点⟨*r*,1⟩不可能源自 *C* 串.

S: 显然节点⟨*r*,1⟩不是源自 *S* 串.

K: 显然节点⟨*r*,1⟩不是源自 *K* 串.

E: 由于 K_{ab} 不属于 K_p,因此节点⟨*r*,1⟩不可能源自 *E* 串.

D: 由于 K_h 不存在解密密钥,显然节点⟨*r*,1⟩不是源自 *D* 串.

同理,节点⟨*r*,2⟩

M: 由于 K_{ab} 不属于 K_p,因此节点⟨*r*,2⟩不可能源自 *M* 串.

F: 显然节点⟨*r*,2⟩不是源自 *F* 串.

T: 显然节点⟨*r*,2⟩不是源自 *T* 串.

C: 则 $g=A,R,B,N_b,h=\{A,R,B,N_b,K_{ab}\}K_h$,由于 N_b 唯一源自Σ,因此节点⟨*r*,2⟩不可能源自 *C* 串.

S: 显然节点⟨*r*,2⟩不是源自 *S* 串.

K: 显然节点⟨*r*,2⟩不是源自 *K* 串.

E: 由于 K_{ab} 不属于 K_p,因此节点⟨*r*,2⟩不可能源自 *E* 串.

D: 由于 K_h 不存在解密密钥,显然节点⟨*r*,2⟩不是源自 *D* 串.

因此,发起者串中的节点不可能源自攻击者串,发起者确实发起了一轮协议的运行,命题得证. □

类似地,可以证明协议也满足发起者保证.因此,该协议满足一致性条件.

5.3 中继者可信条件分析

对于中继者可信条件的分析,可以采用相同的方法,即对于中继者串,证明其节点不可能源自攻击者串.但对 SRP 进行分析时发现该协议无法满足中继者可信条件,因为中继者串中的节点⟨*r*,2⟩有可能源自攻击者串中的 *C* 串,具体分析如下:

对于节点⟨*r*,2⟩

M: 由于 K_{ab} 不属于 K_p,因此节点⟨*r*,2⟩不可能源自 *M* 串.

F: 显然节点⟨*r*,2⟩符号为正,不可能源自 *F* 串.

T: 显然节点⟨*r*,2⟩不是源自 *T* 串.

C: 则 $g=A,N_a,\{N_a,K_{ab}\}K_h,h=R,gh=A,R,N_a,\{N_a,K_{ab}\}K_h$,由此可以看出该节点有可能源自 *C* 串.

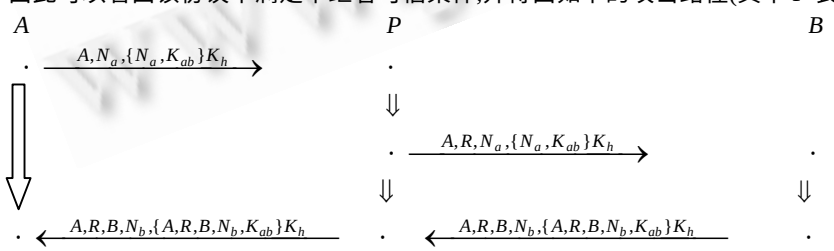
S: 显然节点⟨*r*,2⟩不是源自 *S* 串.

K: 显然节点⟨*r*,2⟩不是源自 *K* 串.

E: 由于 K_{ab} 不属于 K_p,因此节点⟨*r*,2⟩不可能源自 E 串.

D: 由于 K_h 不存在解密密钥,显然节点⟨*r*,2⟩不是源自 *D* 串.

由此可以看出该协议不满足中继者可信条件,并得出如下的攻击路径(其中 *P* 表示攻击者):



由此可以看到,攻击者可以冒充中继者完成一轮协议的运行.源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.这是由于 SRP 中没有针对中继节点的认证机制,导致该漏洞的产生.

结果与文献[6]中对 SRP 的分析结果是一致的.

6 小 结

从上述分析可以看出,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,该分析方法可以发现具体的攻击路径,明确指出协议存在哪些缺陷或漏洞,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,从而对协议进行改进.

然而正是由于该方法基于攻击者模型,最后的分析结果完全依赖于对于攻击者行为的描述.一方面这种攻击者模型是否能够完全表示所有的攻击行为,另一方面该方法并不能证明协议是安全的,也就是说如果该方法能够发现协议的缺陷,则协议是不安全的,如果不能发现协议的缺陷,则不能说该协议是安全的.

References:

[1] Fan H, Feng DG. Theory and Method of Secure Protocols. Beijing: Science Press, 2003 (in Chinese).

[2] Ying C, Shi ML. The architecture of the self-organized network. Journal of Communications, 1999,20(9):47−54 (in Chinese with English abstract).

[3] Qing SH. Twenty years development of security protocols research. Journal of Software, 2003,14(10):1740−1752 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/14/1740.htm

[4] Perkins CE, Royer EM. Ad Hoc on-demand distance vector routing. In: Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications. New Orleans, 1999. 90−100.

[5] Gong L, Needham R, Yahalom R. Reasoning about belief in cryptography protocols. In: Proc. of the 1990 IEEE Symp. on Research in Security and Privacy. Oakland, 1990. 234−248.

[6] Buttyan L, Vajda I. Towards provable security for Ad Hoc routing protocols. 2004. http://eprint.iacr.org/2004/159.pdf

[7] Papadimitratos P, Haas ZJ. Secure routing for mobile Ad Hoc networks. In: SCS Communication Networks and Distributed Systems (CNDS). San Antonio, 2002.

[8] Argyroudis PG, O'Mahony D. Secure routing for mobile Ad Hoc networks. http://www.ctvr.ie/docs/EN_Pubs/secure-adhoc-routing.pdf

[9] Song Z, Zhang Y, Li ZJ, Chen HW. Formalized description and analysis of secure protocols. Computer Sciences, 2003,30(8):24−27 (in Chinese with English abstract).

[10] Chen P, Liu DX, Bai YC. A study of analyzing security protocols formally. Computer Applications and Software, 2003,5:48−50 (in Chinese with English abstract).

[11] Johnson DB, Maltz DA, Hu YC. The dynamic source routing protocol for mobile Ad Hoc networks (DSR). IETF MANET Working Group. 2004. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt

[12] Saeed R, Khatun S. Ultra wide band (UWB) Ad Hoc networks: Review and trends. Journal of Computer Science, 2005,1(1):35−39.

附中文参考文献:

[1] 范红,冯登国.安全协议理论与方法.北京:科学出版社,2003.

[2] 英春,史美林.自组织网体系结构研究.通信学报,1999,20(9):47−54.

[3] 卿斯汉.安全协议 20 年研究进展.软件学报,2003,14(10):1740−1752. http://www.jos.org.cn/1000-9825/14/1740.htm

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

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

王继志(1976－),男,山东泰安人,助理研究员,主要研究领域为密码理论,信息安全.

王英龙(1965－),男,博士,研究员,主要研究领域为网络与信息安全.