维普资讯 http://www.cqvip.com

计算机科学2002Vol.29№.9

分组密码计数模式在ipsec中的应用及性能分析

Block Cipher Counter Mode's usage in Ipsec and Performance Analysis

许锡雷　叶澄清

（浙江大学计算机科学与工程系　杭州310027）

Abstract The article introduces counter mode and it's advantages, points out that counter mode is suitable for ipsec security gateway, and gives a complete solution applying counter mode in ipsec.

Keywords Counter mode, Ipsec, Sequence number, Message ID

一、分组密码计数模式简介

在分组密码中CBC模式是广为人知的，而计数模式(counter mode)则鲜为人知，其实早在1979年，就由Diffie和Hellman提出[1]。在计数模式下，设明文为M，密钥为K，加密函数为E，计数器为ctr，则密文C=M XOR E_K(ctr)|E_K(ctr+1)|E_K(ctr+2)|…。其中"|"表示连接运算，整个运算式共取|M|个比特。从另一个角度来看，也就是说，第i个密文块c_i和第i个明文块m_i的关系为$c_i=m_i$ XOR E_K(ctr+i)。(其中i=0,1,2,……)这与CBC模式的串行特性是不同的，也是计数模式许多优点的本质来源。从一般意义上来说，接收方得到C和ctr后，明文M=C XOR E_K(ctr)|E_K(ctr+1)|E_K(ctr+2)|……，即$m_i=c_i$ XOR E_K(ctr+i)。可见，加密与解密的区别仅在于C和M互换位置。

计数模式并没有规定ctr如何让接收方得知，这其实是计数模式如何应用的问题。ctr可以和C一起发送，也可以由双方事先约定的规范导出等等。计数模式的安全性在理论上是可以证明的，本质在于安全的分组加密函数具有伪随机变换的特性。

二、计数模式在ipsec中的适用性

ipsec是Internet网络层的安全标准，目前主要应用于VPN网关。作为网关应用，由于要为整个内部网转发数据包，所以性能是一个关键的问题，计数模式在提高性能方面是很有作为的。

在计数模式中，由于$c_i=m_i$ XOR E_K(ctr+i)，所以各个块的加密可以独立地进行，这在软件实现中，可以充分利用现代体系结构的并行性。如果用硬件实现加解密，可以设置多个功能单元，每个功能单元独立完成各个块的加解密，可以极大地提高性能。

计数模式的计算开销主要在E_K(ctr+i)上，由于每一个到来的数据包的ctr值是按一定原则分配的，所以该ctr值是可以预计的。因此，处理器有空闲时，可预先完成E_K(ctr)，E_K(ctr+1)，……等，以进一步提高性能。

由于解密操作不过是把加密操作中的C和M互换位置，这对简化实现是很有好处的，尤其是在硬件加密卡的实现上，可以减少近半的逻辑。

在CBC模式中，如果应用explicit IV，则密文包中还包含IV值，这加大了包的长度，即加大了安全网关的负载，而在计数模式中，则没有这个问题。

因此，计数模式在ipsec作为网关的实现中可以极大地提高性能。

三、计数模式在ipsec中的应用

在ipsec中，加密主要涉及到两个部分，一个是ESP，另一个是在SA的建立过程中，包括整个phase Ⅱ SA (ipsec SA)的建立过程，消息交换(informational exchange)和phase Ⅰ SA的最后步骤。

计数模式的具体应用主要是如何确定ctr的问题。一个重要的安全性原则是：对于一个密钥K，不能对同一个数值加密两次。设ctr值标识一个数据包，i标识包内的一个块，则(ctr,i)是唯一的。

在ESP中，由于协议头中有序列号(sequence number)字段占32比特，所以可用其标识数据包。假设加密函数块长度为64比特，则可取ctr=sequence number * 2∧32，而对包内的各个块依次以0,1,2……标识，即以sequence number为高32位值，块序号i为低32位值，构成加密函数所要求的64位值。

对于在SA的建立过程中涉及到的加密，一种选择是鉴于这些包比例很小，对总体性能影响不大，可以考虑采用现时ipsec标准的做法。但这样如果系统安装仅支持计数模式的加密卡，那么这些加密也只能采用软件实现。所以研究这些包的ctr的表示还是有意义的。

其实有一种合适的做法用于确定这些包的ctr值，在phase Ⅰ SA建立以后，每一次交换都有一个唯一的message ID，以明文形式出现在ISAKMP头中，占32位。因此，如果加密函数对块长度的要求为64位，则可让message ID占有高32位，在剩下的32位中，由于同一message ID的交换可能涉及来回几个包(因quick mode和informational exchange而异)，所以留出高两位用于标识同一个交换中的包次序(就目前的quick mode和informational exchange而言，两位是够用的)，剩下的30位标识包中的块序号。

由于message ID的合法值不包括0，所以对于phase Ⅰ SA建立过程中的最后两个要求加密的包(在main mode中)，就可以以0作为ctr的值，低32位的做法同上所述，包次序可分别以0和1标识。

至此，ipsec中所有要求加密的包都可以用计数模式了。

总结　在基于ipsec的VPN网关项目中，我们项目组成

(下转第38页)

许锡雷　硕士研究生，主要研究方向：网络新技术、网络安全。叶澄清　教授，博导，主要研究方向：图像处理、网络安全。

维普资讯 http://www.cqvip.com

测)修正,下面我们介绍该算法的基本思想。

4.1 基本定义

我们首先定义与数值型跟踪理论对应的符号型跟踪理论的几个概念。

定义 4 条件包括被跟踪目标在环境中的位置、速度等状态信息及类别信息,从而得到 Agent 符号化基本行为,如:变得更近、靠近等,并用预定义的谓词原子公式表示。

定义 5 计划原型,表示形成一个计划的最少活动序列,即 Agent 必要行为(necessary action)。计划方差:在该计划执行中可能匹配的行动序列,即可选行为(option action)。

定义 6 活动原型,核心行动,最少集合的条件和限制,它是能够用观测匹配识别一个行动的必要部分,如果满足,则该行动可以被实例化(该行动发生),即证实一个活动发生的最少条件。行动方差:指的是围绕核心行动的条件和限制,它有可能被观察所匹配。

定义 7 时刻 t_n 时状态是 S_n,表示计划库中的被标志的计划集合,被标志意味着执行该计划的 Agent 被跟踪,亦即多 Agent 正在执行的计划集合。状态 S_n 的演变由计划原型来确定,是 Agent 时序行为。

定义 8 状态噪声,由不属于计划原型中的 Agent 造成的不期望事件。

定义 9 观测噪声,当前状态的观测与实际观测的偏差,由传感器精度及情报信息的不确定性引起。

4.2 符号跟踪理论规划识别基本算法

初始情形下,用观测到的 Agent 行为建立初始计划集合,每一个计划相当一条航迹,即跟踪的开始;然后用该计划预测下一步发生的事件及态势情形(对下一个状态的预测和下一个观测的预测),对应于下一个计划步骤和实现该计划步骤的可观测行为(是一个集合,可观测范围内发生的 Agent 行为),这个步骤对应于目标跟踪中状态的预测和观测的预测。

在每一步,利用发生的事件来确定是否发生预测的观测,若发生,则该计划继续,若没发生,建立一条新的航迹(对应新的计划),同时降低原有计划的可信度。继续预测每个计划(航迹)的下一步(状态和观测范围),若原匹配的计划仍旧不匹配,则继续降低其信任度,新建立的计划若不匹配,同样降低其可信度,又建立新的计划,如原有计划信任度降到一定的门限,则去掉(跟踪消除),围绕新的计划(航迹)继续观测。若下一步的匹配在计划(航迹)的预测范围内,则认为该计划继续发生(航迹继续延续),同样,在这个过程中,由于状态噪声和观测噪声可能引起错误计划(误跟)和真实计划未识别(失跟),从而有可能产生虚警与漏报。

总之,该算法的主要步骤是:

· 预测过程:预测状态是 Agent 候选计划可到达的行为的集合,同时将预测状态投影到观测空间,从而得到下一步观测的焦点,这个步骤对应于卡尔曼滤波的状态方程和观测方程的功能。

· 修正过程:如果当前观测的行动和预测的活动原型一致,表明计划更新正常,最新状态在预测状态集合中;如果不一致,但是同预测活动原型一致,则该计划继续执行;同时根据多余行动的性质考虑是否引入新的计划;如果同预测活动原型不一致,则考虑一个新的计划。这个步骤对应于卡尔曼滤波中用增益和参差更新状态方程获得最优航迹的过程。

讨论 本文提出了战场态势估计的过程就是规划识别的过程,提出应用 Agent 符号卡尔曼滤波跟踪理论来建立态势规划识别模型,该算法能够在跟踪的过程中完成军事实体的计划识别,也就是一级融合和高级融合是同步进行的,符合融合的本质要求。另外,由于计划是与 Agent 相关联的,如何合并各个 Agent 的计划来形成更高级的计划,是一个需要解决的问题,我们打算用模板来聚合多 Agent 计划以形成更高抽象程度的战场态势描述。总之,多 Agent 符号卡尔曼滤波规划识别模型在解决高层数据融合中有广阔的应用前景。

参 考 文 献

1 Castel C. Dealing with Uncertainty in Situation Assessment: towards a symbolic Approach. In: 14th Conf. on UAI, USA, July 1998

2 Robert W. Knowledge Representation for Plan Recognition. In: Working Notes of the IJCAI-95 Workshop "The Next Generation of Plan Recognition Systems" Montreal, Canada

3 Devaney M, Ram A. Needles in a Haystack: Plan Recognition in Large Spatial Domains Involving Multiple Agents. National Conference on Artificial Intelligence (AAAI-98), Madison, Wisconsin. 1998

4 Kaminka G A, Pynadath D V, Tambe M. Monitoring Deployed Agent Teams. In: Proc. of the Fifth Intl. Conf. on Autonomous Agents (Agents-2001), Montreal, Canada

5 Kaminka G A, Wendler J, Ronen G. New Challenges in Mlti-Agent Intention Recognition: Extended Abstract. In: Proc. of the Fall Symposium on Intention Recognition for Collaborative Tasks. 2001

6 吴雾. 态势评估关键技术的研究:[西安电子科技大学博士论文]. 1996

7 何友,等. 多传感器信息融合及其应用. 电子工业出版社,2000

8 Hall D L. An Introduction to Multisensor Data Fusion. IEEE Proceedings, 1997, 85(1)

(上接第 112 页)

员深感性能问题将是项目成败的关键。计数模式可以极大地提高性能,在采用硬加密实现时尤其如此(不过要设计专用的计数模式加解密卡)。遗憾的是目前的 ipsec 标准尚不支持计数模式。本文提出了在 ipsec 中完整地应用计数模式的一个方案,并在我们的项目中实现为一个备选模块。我们期待着 IETF 标准化工作的进展。

参 考 文 献

1 Diffie W, Hellman M. Privacy and Authentication: An Introduction to Cryptography. Proceeding of the IEEE, 1979, 67: 397～427

2 Lipmaa H, et al. Comments to NIST Connecting AES Modes of Operations

3 Etienne J. The Counter-Mode and its Use with ESP, Internet-Draft, Work in progress

4 Kent S, Atkinson R. Security Architecture for the Internet Protocol, RFC2401

5 Kent S, Atkinson R. IP Encapsulating Security Payload (ESP), RFC2406

6 Maughan D, et al. Internet Security Association and Key Management Protocol (ISAKMP), RFC2408

7 Harkins D, Carrel D. The Internet Key Exchange (IKE), RFC2409