面向命名数据网络的安全通信机制及其优化

苏令华[1]，李水芳[2]✉，张　茜[1]
(1.空军工程大学信息与导航学院，西安，710077；2.安徽省合肥市公安局网安支队，合肥，230000)

摘要　NDN 网络架构的安全机制构建在信息本身，因此 NDN 中对传输的数据必须采取有效的签名和加密措施，否则攻击者可以随意获取数据或发送虚假内容，这将成为 NDN 网络的最大安全隐患。文中针对 NDN 的安全隐患，设计出一种轻量级加密算法来解决 NDN 网络架构的安全问题，详细分析了该算法每个步骤的含义和目的，以及它在各种攻击方式下的安全性，同时对算法进行了优化，提高了算法的运行效率。并且在 ndnSIM 下嵌入该算法进行仿真，验证了数据从发布者开始是以密文方式进行传输，具有机密性；收到数据后能正确地验证发布者的身份，具有认证性；并正确地解出明文和验证数据是否有改动，具有完整性；再分别对攻击方式中的数据内容篡改和身份伪装进行了仿真，验证了对传统网络攻击防范的有效性。

关键词　NDN；NS-3；ndnSIM；轻量级
DOI　10.3969/j.issn.1009-3516.2019.05.016
中图分类号　TP393.08；TN919.2　　**文献标志码**　A　　**文章编号**　1009-3516(2019)05-0097-08

Research on Security Communication Mechanism and Optimization of Named Data Network

SU Linghua[1], LI Shuifang[2] ✉, ZHANG Qian
(1. Information and Navigation College, Air Force Engineering University, Xi'an 710077, China;
2. Hefei Public Security Bureau Network Security Detachment, Hefei 230000, China)

Abstract: NDN security mechanism lies in the information itself, and the effective signature and encryption must be given to the data transmitted in NDN , otherwise the attacker can get data or send them at will. In view of this security problem, a lightweight encryption algorithm is designed. The meaning and purpose of the each step of the algorithm and security under various attack modes are analyzed in detail. The algorithm is optimized to improve its efficiency and is embedded in ndnSIM for simulation. The verified data are transmitted in encrypted way from the publisher and the identity of the publisher can be verified correctly after receiving the data, and the change of plaintext and the verification data can be correctly solved. The effect of the algorithm on confidentiality, authentication , integrity and efficiency are verified.
Key words: NDN; NS-3; ndnSIM; lightweight

由于目前 TCP/IP 网络所暴露出来的不安全　　性、可靠性差、移动性差以及灵活性差等问题，

收稿日期：2019-02-27
基金项目：陕西省自然科学基础研究计划(2016JM4008)
作者简介：苏令华(1979—)，男，山东枣庄人，副教授，博士，主要从事网络空间安全和遥感图像处理研究。E-mail：sulinghua79@sina.com
通信作者：李水芳(1978—)，女，山东枣庄人，副教授，主要从事信息网络安全研究。E-mail：lisf1978@126.com

引用格式：苏令华，李水芳. 面向命名数据网络的安全通信机制及其优化[J]. 空军工程大学学报(自然科学版)，2019，20(5)：97-104. SU Linghua，LI Shuifang，ZHANG Qian. Research on Security Communication Mechanism and Optimization of Named Data Network[J]. Journal of Air Force Engineering University (Natural Science Edition)，2019，20(5)：97-104.

TCP/IP 网络架构已经越来越难以满足人们的需求。目前国际上有很多研究机构进行未来的网络的设计研究,如美国 DONA[1]、TRIAD[2]、CCN[3]和 NDN[4],欧洲 PSIRP[5]、4WARD[6]、PURSUIT[7]和 SAIL[8],NDN(Named Data Networking,命名数据网络)是在 2010 年获得美国国家自然基金 800 万美元投资,专门为未来互联网体系架构研究的一个基础信息中心网络项目,已经取得实质性进展,正在成为未来体系架构的主流。NDN 架构的设计反映了对目前互联网的优势和局限性的理解[9],其核心思想就是把网络中所有的东西都看成信息,把信息作为核心对象,其通信模型是以信息为中心,取代了 TCP/IP 网络中的以地址为中心的方式,通信模式从主机到主机进化为主机到网络,转发机制由存储转发进化为缓存转发,传输模式由"推"变为"拉",增强了主机移动性,解决了海量数据传输的难题。在 NDN 网络架构中,安全机制建立在信息本身,用户只需发出某个请求,不需要提供位置信息(IP、域名),就可以享有其他用户请求的内容,攻击者无法对用户系统进行直接攻击,NDN 网络的安全防护集中到数据层面,如果 NDN 中对传输的数据不采取有效的签名和加密措施,攻击者可以随意获取数据或随意发送虚假内容,这将成为 NDN 网络的最大安全隐患,如何对内容数据包签名加密来实现信息传输的机密性、认证性和完整性,是 NDN 安全机制的研究重点。

文中首先介绍了 NDN 网络的工作模式,针对 NDN 的安全隐患,提出一种轻量级加密算法来解决 NDN 网络架构的安全问题,详细分析了该算法每个步骤的含义和目的,并说明它在各种攻击方式下的安全性,同时对算法进行了优化,提高算法的运行效率。最后,在 ndnSIM 下嵌入该算法进行仿真,验证了数据从发布者开始是以密文方式进行传输,具有机密性;收到数据后能正确地验证发布者的身份,具有认证性;并正确地解出明文和验证数据是否有改动,具有完整性;再分别对攻击方式中的数据内容篡改和身份伪装进行了仿真,验证了对传统网络攻击防范的有效性。

1 NDN 技术概述

1.1 NDN 的安全机制

NDN 针对 TCP/IP 在设计上的缺陷和不足,提出从框架设计上根本解决的观点。该架构保留了 TCP/IP 网络架构的细腰沙漏模型,保证了路由策略配置灵活多样,网络中传递和储存的数据包都是包括数据名称和数据内容的,以数据内容作为互联,通过数据的名称标识所有的信息单元,安全机制基于数据内容的,是直接建立在信息上而非主机,对网络层基本透明,再由应用程序进行处理。

NDN 的安全机制的大概分为以下 3 个步骤:①所有数据都需要签名,包括数据内容,路由信息等;②通过多路径路由的方式减轻前缀劫持的影响;③NDN 的消息只可以跟相关应答数据交互。这种机制的优点是成功实现网络传输和数据安全的分离,更具灵活性和方便性,也真正符合了数据请求的自然处理方式。

1.2 NDN 的路由方式和转发机制

NDN 中有 2 种类型的包,分别是请求包(Interest)和数据包(Data),它们通过数据包上的命名进行匹配[10]。NDN 采取请求方驱动的通信模式,由请求方广播 Interest 包,以数据上的命名为联系,通过"拉"方法获得 data 包。在通信开始阶段,请求者首先发送一个 Interest 包到网络中的路由节点,这些收到包的路由节点,如果本地没有符合要求的数据,会根据包的名称和设定好的路由策略转发包到相邻的节点,直到该 Interest 包到达正确的发送者或者被丢弃为止。在交互的过程中,data 包的粒度比较高,故较大的数据对象一般被划分为较小的数据块。

表 1 NDN/CCN 节点工作模型

CS		PIT		FIB	
Name	Data	Name	Face	Name	Face
/SJTU/welcome1	1100	/SJTU/map/lake	1	/SJTU	0
/DM/paris.mpg	1110	/DM/foot.avi	1,2	/DM	2,1
				/SJTU/map	3,1

由表 1 可知,NDN 路由机制中维护着 3 张表,分别是转发路由表(Forwarding Interest Base,FIB),待处理请求表(Pending Interest Table,PIT)和数据包缓存(Content Store,CS)数据结构。表 1 给出了 NDN 节点的工作模块,其中是用 FIB 寻找合适的转发接口,CS 用来进行内容数据包的缓存,并采用 LRU 缓存算法。PIT 保存收取的 Interest 包,当这个包中数据的名称和收到的 data 包名称匹配时,将会根据相应的 face 接口传递回去,同时信息的转发方式采用最长前缀匹配。

NDN 数据包具有独立性,与它的来源和终点无关,不依赖 TCP 那样的连接控制,也不需要储存状态信息。NDN 路由节点会将 Interest 包缓存于 PIT 表中,而 Data 包缓存于 CS 表中,从而等待交互应答。如果对应于相同的 Data,有多个 Interest,节点会先消去重复的部分,然后把到达的接口存储在 PIT 中,并只会转发最先到达的 Interest。而 Data 包到达时,节点会寻找与 Data 包中数据名称相符的 PIT 条目,根据 PIT 表中该数据对应的 Face 接口将

其发送回去，之后 PIT 删除相应的条目，CS 表就会增加一项该数据，CS 在这里就充当了 Data 包的缓冲存储器了。

在数据传输的过程中，Interest 包和 Data 包在传输顺序上是前者在前，后者在后，而在传播路径上，两者是恰好相反的。Interest 包在经过每一个路由节点时都有得到需要的 Data 包的可能，因此实现了逐跳式流平衡。NDN 路由可支持多种路由协议，包括多播组播[11]、内容分发、移动性和延迟容错网络，而传统的 IP 路由只采用最佳路径防止循环。

在原理上，NDN 防止了网络冲突和拥塞，实现了多链路路由，同时基于网络内缓存实现了就近获取、负载均衡和容断能力，从而提升了内容分发的性能、效率和可靠性。在安全性上，NDN 的加密保护是基于数据包本身的，而 TCP/IP 是依靠传输端点和通道的保护，这样路由安全性上，NDN 更胜一筹。首先，所有数据和路由信息都需要签名，例如使用 SHA1 或 MD5 产生哈希摘要，这样可以保障数据的完整性，防止攻击者伪造篡改；其次，通过多路径路由来减轻前缀劫持，因为路由器可以检测由前缀造成的异常劫持，并尝试其他路径检索数据；另外，NDN 消息未必发送到主机，这令到恶意数据包很难定位到特定主机。这种机制实现了数据安全与网络传输的分离，降低了实现的难度，但也因此导致 NDN 机制中无法得知数据源，所以认证性无法保证。

2　通信安全加密算法设计与分析

2.1　设计原则

信息安全的 5 个要素是机密性、完整性、可靠性、可用性和认证性。其中，对于可用性的保护，主要依赖 NDN 本身数据通信的特点，NDN 对于防范 DDos 攻击有着天然的优势，而这种攻击在 IP 网络是难以防御的。对于可靠性的保护，主要依靠硬件设备的安全可靠，这可以通过备份等方式提高。

本文提出的算法主要提高数据的机密性、完整性、和认证性。另外，在算法的加解密效率上也要有所兼顾。对于机密性的保护，本文采用加解密的思路进行，加解密的算法弃用传统方式改用异或的方式，这样会提高算法的效率。对于完整性的保护，采用的是加密消息摘要的方式进行，并且分析比较了对消息摘要进行哈希加密的时间效率。对于认证性的保护，是通过数据中附带用户 ID 来进行的，通过附带用户 ID，路由节点就可以通过信任列表得到该 ID 是否受信任的信息。

2.2　算法设计与分析

2.2.1　算法描述

算法建立在网络模型的传输过程中，首先假设需要发送数据的节点为 A，接收数据的节点为 B。算法具体描述如下：

1. 初始化
2. $\forall u \in N_i$，令 $K_N^i = \mathrm{hash}(ID_i + x)$
3. 令 $h = \mathrm{hash}(ID_i + K_N^i)$
4. 令 $H\mathrm{mac} = \mathrm{hash}(\mathrm{information})$
5. 令 $C = \mathrm{information} \oplus h$
6. 向路由传送 $<C, H\mathrm{mac}, ID_i>$ 信息对
7. NDO 接收信息对
8. 令 $h = \mathrm{hash}(ID_i + K_N^i)$
9. 令 $\mathrm{information}' = C \oplus h$
10. 令 $H\mathrm{mac}' = \mathrm{hash}(\mathrm{information}')$
11. 如果（$H\mathrm{mac} = H\mathrm{mac}'$），则完成信息传输
12. 否则退出

算法具体描述如下：

步骤 1　各路由节点初始化；

步骤 2　x 代表各节点自己的私钥，ID_i 代表第 i 个节点的 ID 号。该步骤表示各节点通过直接连接自己的 ID 号和私钥，生成 hash 值为 K_N^i，这个 K_N^i 通过秘密方式共享给拓扑中受信任的所有节点。各路由节点中的签名方式由第 3 方签名，群体签名[12-13]，环签名[14-15]或者临时身份进行。

步骤 3　各节点直接连接自己的 ID 号和**步骤** 2 生成的 K_N^i，生成 hash 值，记作 h。

步骤 4　A 节点生成需要发送的 information 的 hash 值，记作 $H\mathrm{mac}$。值得注意的是，这里的 information 其实不单指数据内容本身，还包括路由信息、节点信息等具体内容。

步骤 5　A 节点对 information 和 h 做一次异或，记作 C。异或的具体方式就是把字符二进制化之后，再按位异或，之后生成新字符，假设采用 SHA1 算法时，则 h 是定长 20 byte，当 information 的长度 length 小于等于 20 byte 时，按位异或 information 与 h 的前 length 字节。当 information 的长度 length 大于 20 byte 时，超出的位数每 20 位再异或一次 h，直到剩余的位数小于等于 20 byte，然后按照前一种情况进行处理。

步骤 6　A 节点向相邻的所有路由节点广播 C，$H\mathrm{mac}$ 和 A 的 ID 号，三者放在一同一个数据块中同时传输。

步骤 7　B 节点接收数据块。

步骤 8　B 节点根据数据块中的 ID 号从路由表中找出该 ID 号对应的私钥 K_N^i，若无，则丢弃数据块。若有，则根据 B 节点直接连接数据中的 ID 号与 K_N^i，生成 hash 值，记作 h。

步骤 9 B 节点对 C 和 h 做一次异或,记作 information′。这一步中,每个路由节点都需要维护一张信任节点表(ID,Key,TRUST),ID 是拓扑结构中全部节点的 ID 号,Key 是该节点 ID 对应的公开密钥 K_N^i,TRUST 表示该 ID 是否受信任,若否,则丢弃它发过来的信息。

步骤 10 B 节点计算出 information′的 hash 值,记作 $H\text{mac}'$。

步骤 11~12 B 节点把 $H\text{mac}'$ 与数据块中的 $H\text{mac}$ 进行比较。若完全相等,则验证了信息的完整性和信息的来源的确来自该 ID,保障了信息的可认证性,从而接收信息;否则,则可认为数据遭到损失或攻击者的篡改,从而丢弃信息退出。

2.2.2 算法攻击防范策略的理论分析

1)攻击方式 1。对算法第 4 步得到的数据,进行穷举异或攻击,直到得到有意义的数据为止。

防范策略:算法第 4 步要进行 $H\text{mac}$ 位数的循环异或,而不单独异或 hash 的某一位,这样是为了增大密文的复杂度,防止攻击者截取信息后使用穷举破解的方法。下面根据算法复杂度的分析,假设明文的长度为 N,对其加密分别采用 hash 第 0 位,和循环哈希值。

a. 当密文 $p[i]=\text{info}[i]\oplus h[0]$时,加密时的复杂度为 n。攻击者解密时穷举所有 $h[0]$可能的情况,对 info[i]分别进行异或运算,总共 $2^8-1=255$ 种可能,就可以破译出有意义的内容,所以最大破译时间为 $O(255n)=O(n)$的复杂度,线性时间的复杂度非常低,即便在数据量不大的情况下也是很快被破解的,极其不安全。

b. 当密文 $p[i]=\text{info}[i]\oplus h[i\%20]$时,加密时的复杂度也为 n。攻击者解密时穷举所有 $h[i\%20]$可能的情况,对 info[i]分别进行异或运算,总共 $(2^8-1)20=255^{20}$约为 10^{48}种可能,就可以破译出有意义的内容,所以最大破译时间为 $O(255^{20}n)$的复杂度。假设攻击者的攻击效率为 100 亿次/s,$10^{48}n/10^{10}=1\ 038n$ 显然超出了破解密码有意义的时间,故目前而言可以看作是不可计算的。

根据以上的理论分析,可以认为该算法在加密效率上是比较高的,而在保障数据的机密性方面是具有可行性的。

2)攻击方式 2。在数据传输的过程中,攻击者中途截取了数据对,篡改其中的 ID 号、$H\text{mac}$ 或者数据内容。

防范策略:只要接收者最终不接收该数据,就是防范成功了,分为以下 3 种情况:

a. 攻击者篡改了 ID 号(假设把 ID 改成了 ID′),该 ID′号可能是受信任的,也可能是不受信任的。如果是不受信任的节点,那就直接丢弃;如果是受信任的,接收者会从信任列表里找出 ID′号的密钥,但是当且仅当 ID′和 ID 密钥完全相同的情况下,异或所得的 information′才与原 information 相等,但是这个概率极低。否则,就会计算出错误的 h(假设为 h'),C 异或 h'得到的 information′就会与 information 不相等,那 $H\text{mac}$ 显然也不相等,完整性认证失败,接收者会丢弃该信息。

b. 攻击者篡改了数据内容(假设把 C 改为 C')。由于 ID 没变,接收者能够从信任列表中得到正确的密钥以及计算出正确的 h 值。但由于 C 已经发生变化,所以 C'异或 h 得到的 information′与 information 不相等,Hmac 显然也不相等,完整性认证失败,接收者会丢弃该信息。

c. 攻击者篡改了摘要内容(假设把 $H\text{mac}$ 改为 $H\text{mac}'$)。接收者能根据 ID 找到正确的密钥,能计算出正确的 h,也能解密出正确的 information 和计算出正确的 $H\text{mac}$。然而数据自带的 $H\text{mac}$ 已经遭到篡改,显然与计算所得不等,故完整性认证失败,接收者会丢弃该信息。

3)攻击方式 3。由于 ID 是公开的,攻击者如果盗用了某个接收者信任的 ID 号(假设为 ID),然后它想伪装成 ID 跟接收者发送信息。于是他自己做了一个数据包,把消息名称做成与 Interest 包相同,里面加入自己的消息内容,首先计算出 $H\text{mac}$,并采用自己的秘钥计算出 h,生成出 C,然后把数据发送给接收者。

防范策略:接收者接受了数据后,会根据 ID 的公开密钥计算出 $h'=\text{hash}(ID+K_n)$,

但是由于 K_n 和攻击者的秘钥不相同,得到的 h'和 h 显然不同,所以解密出的 information′也和 information 不相同,生成的 Hmac 也不相同,故完整性认证失败,接收者会丢弃该信息。

综上所述,该算法对于保障完整性方面也是具有可行性的。

2.2.3 算法效率的优化

根据以上对算法的描述,算法计算复杂度主要集中在异或和哈希算法中。发包前,算法耗时的地方在于第 2~5 步。其中步骤 2 需要 hash 的字符串只是 ID 和密钥的长度和,步骤 3 只是 ID 和摘要的长度和。由于 ID 密钥和摘要的长度都很短,所以复杂度在常数时间内,本文用 t_b 表示这 2 步的耗时,属于次要耗时。则:

$$t_b=b \tag{1}$$

式中:b 表示一个较小的常数,单位为 μs。

主要耗时在于第 4 步和第 5 步，步骤 4 是用 hash 算法加密不定长的信息内容，根据对 MD5、SHA1、SHA256、SHA384、SHA512 等 5 种哈希函数在同一软件和硬件系统中对 0～1 500 000 byte 的数据进行仿真分析，步骤时间为 t_h，则：

$$t_h = k_h L \tag{2}$$

式中：L 表示数据长度，单位为 byte；t_h 单位为 μs；k_h 的大小跟选取的 hash 算法有关。其中：

$$k_h = \begin{cases} 0.002\ 3(\text{hash}=\text{MD5}) \\ 0.002\ 4(\text{hash}=\text{SHA1}) \\ 0.006\ 1(\text{hash}=\text{SHA256}) \\ 0.006\ 2(\text{hash}=\text{SHA384}) \\ 0.006\ 5(\text{hash}=\text{SHA512}) \end{cases}$$

因此，第 4 步的效率仅跟字符串长度和 hash 算法的选取类型相关，算法优化主要在于第 5 步的异或算法。如果采取直接异或的方式，所得到的图像见图 1：

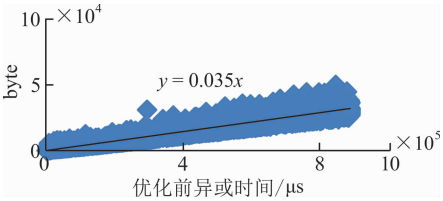

图 1　优化前异或时间与数据长度的关系

但是这个耗时比 hash 算法高出几倍乃至十几倍，可以采用如下方式（图 2）进行优化：

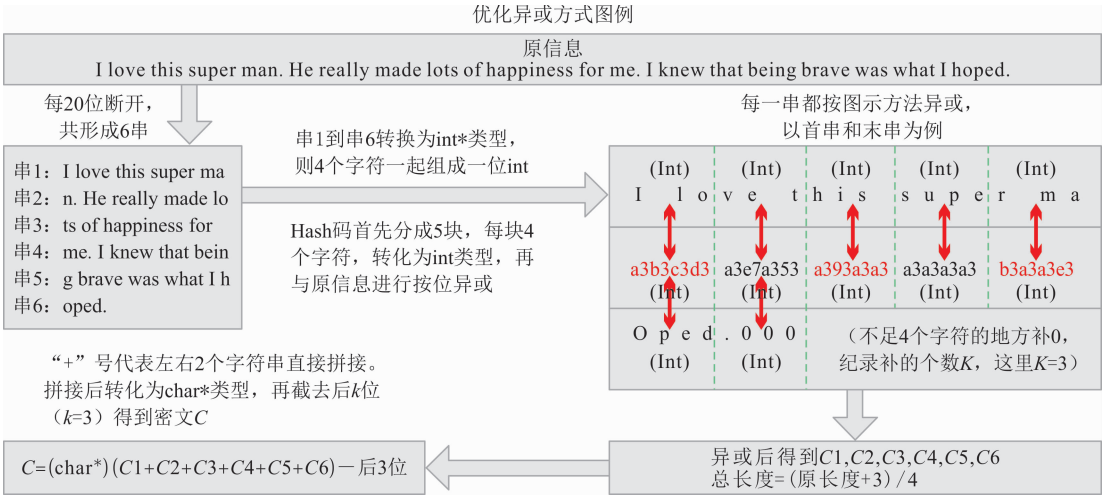

图 2　优化异或方式图例

由于 CPU 可以使用 32 位数据类型来处理程序，而未优化的算法采用的是直接单字符异或，即 8 位异或，显然效率无法达到最佳。因此把 8 位的 char 类型变量转换为 32 位的 int 类型变量，即把原文和 hash 码每 4 个字符转换成 int 类型再进行异或，异或次数变为原来的 1/4，而优化前后算法的二进制过程是完全一致的，只是运算的类型不同而已，因此理论上可以把异或算法的复杂度由 $O(n)$ 降低为 $O(n/4)$，下面证明其正确性：

例如：假设“abcd”^“efgh”

原算法是：

a⊕e＝01100001⊕01100101＝00000100

b⊕f＝01100010⊕01100110＝00000100

c⊕g＝01100011⊕01100111＝00000100

d⊕h＝01100100⊕01101000＝00001100

最终结果为：00000100 00000100 00000100 00001100

优化算法为：

(int)“abcd”→01100001 01100010 01100011 01100100

(int)“efgh”→01100101 01100110 01100111 01101000

(int)“abcd”⊕(int)“efgh”＝00000100 00000100 00000100 00001100

优化前后结果相等。实质上优化前后算法的二进制过程是完全一致的，只是运算的类型不同而已，这足以证明优化算法的正确性。在 Visual Stdio2012 下运行优化异或算法得到如下图像（图 3）：

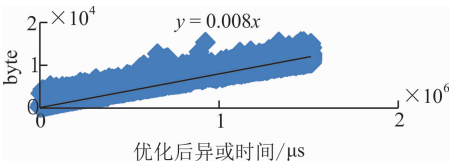

图 3　优化后异或时间与数据长度的关系

可以把异或算法所耗时间记作 t_y，则：

$$t_y = k_y L \tag{3}$$

式中：$k_y = \begin{cases} 0.035\ 5(\text{算法优化前}) \\ 0.008(\text{算法优化后}) \end{cases}$；$L$ 表示数据长度，单位为 byte；t_y 单位为 μs。

综上，设算法的加密步骤 2～5 所耗总时间为

t_{alg},则根据式(1)～(3)得:

$$t_{alg}=t_b+t_h+t_y=(k_h+k_y)L+b \tag{4}$$

对比优化前的图 1,可以看到效率有了明显地提升,时间系数由 0.035 降到 0.008。

3 通信安全加密算法仿真与验证

3.1 基于 NS-3 的 ndnSIM 仿真软件

NS-3 是一个离散事件的网络仿真器,仿真的核心支持基于 IP 和非 IP 网络,是开源免费的软件,研究、开发和利用都是公开可用的,目前获得了 GNU GPLv2 的许可。

NDN 相比 IP 网络最基本的改变就是网络通信设计的广泛和多元化。然而 NDN 实现和测试平台部署的成本比较高,使得针对它的实验设计和大范围测试评估难以实现。于是在这样的前提下,NDN 模拟器——ndnSIM 便应运而生了。ndnSIM 设计具有以下特点[16]:

1)代码完全开源,研究者可以根据需要改变 NDNSIM 中的代码,编写自己的路由策略,协议代码等等,并在公共的仿真平台下做实验。

2)它保持了 CCNx 实现分组级别的互操作性,使 ndnSIM 和 CCNx 之间实现了数据分析工具和流量测量的共享,CCNX 的流量驱动 ndnSIM 的仿真实验,从而支持大范围的实验。

3)它完全遵从 NDN 的框架,作为全新的网络协议模型实行,可以在任意的链路层协议,如 WIRELESS,CSMA 等,和传输层协议,如 TCP、UDP 等,模型上承载,灵活性大大提高,使得 NDNSIM 能仿真多样化的部署场景,如 NDN-only,NDN-over-ip 等。同时,它支持网络层实验与路由、数据缓存、数据包转发和拥塞管理,并使用模块化的方式实现,模块化结构由于遵循了"高内聚,低耦合"的架构设计原则,使得任何组件修改和更换对于其他组件影响非常小。

3.2 仿真实验环境搭建

本次实验运行环境为 Vmware 10 下的 Ubuntu14.04 系统,需要安装的软件为 NS-3,ndnSIM 2.1,Netanim,RGUI。ndnSIM 的安装与配置过程在官网上有详细的步骤,这里不详细叙述。

在 ndnSIM 内部,data 是以块的格式通过 producer 类传递给 consumer 类的,原始的类没有添加任何的安全算法,producer 直接得到数据包,并根据 interest 包中相匹配的数据名向网络中路由节点发送数据包。如果攻击者劫持了某个路由节点,就能很轻易地知道信息的全部内容,数据的完整性,机密性以及可认证性都没能得到保护。所以,算法必须加在 producer 类和 consumer 类中,即在 producer 发送数据前加密数据,在 consumer 类接收数据后解密和验证数据,从而提高安全性。

验证安全性采用以下拓扑结构,见图 4。

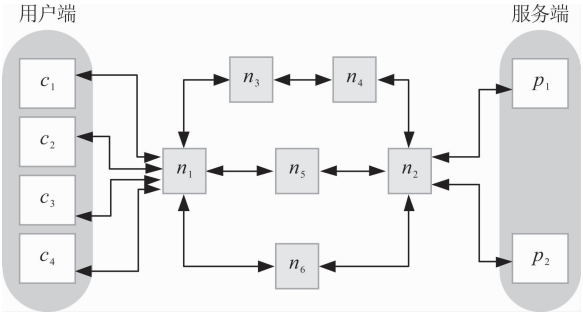

图 4 自定义 12 节点模型

以下是配置文件(表 2):

表 2 配置参数

x	y	速率/Mbps	OSPF	延迟/ms	最大包个数
c_1	n_1	10	1	50	200
c_2	n_1	10	1	10	200
c_3	n_1	10	1	100	200
c_4	n_1	10	1	1	200
n_1	n_3	1	136	20	20
n_3	n_4	1	176	20	20
n_4	n_2	1	176	20	20
n_1	n_5	1	587	1	20
n_5	n_2	1	446	1	20
n_1	n_6	1	587	1	20
n_6	n_2	1	846	1	20
n_2	p_1	10	260	1	200
n_2	p_2	10	700	1	200

采用的路由策略为最佳路由策略。

3.3 算法在 ndnSIM 下安全性仿真验证

3.3.1 算法机密性、完整性和认证性的仿真验证

在 ndnSIM 下按照以上配置搭好上述拓扑后,开始对拓扑进行仿真,见图 5。

如图 5 所示,仿真开始后,前 3 行显示的是 consumer 的发包过程,第 4 行 p_2 节点收到某个 consumer 发来的 Interest,第 5 行 p_2 在信任列表中找出自己的私钥 ,并对数据进行本文的加密。第 6 和第 7 行表示 p_2 已经把数据加密完成并发往路由,可以看到数据名称是公开的,但是数据内容是加密过的,无法被截获者理解,验证了机密性。

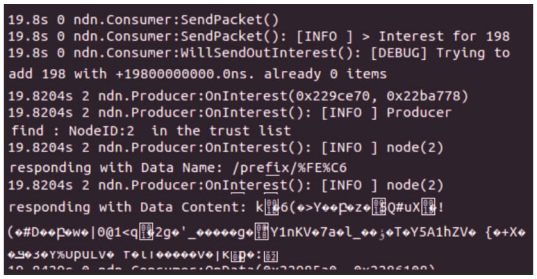

图 5　producer 加密数据过程图

如图 6，第 1 行到第 3 行表示，某个 consumer 收到了 data 发回的加密过的信息。第 4 行表示，consumer 根据 data 包中附带的 ID 号检查信任列表，这里发现 p_2 在列表中，验证了认证性，所以开始检查数据完整性。第 5 行表示 consumer 根据密钥解密出了信息，这里信息为“This program is designed for Named Data Networking with smart grid in my Graduate Design. This Data is sent by NodeID:2”。但是是否完整无法得知，所以第 6 行，consumer 计算出信息的摘要并与 data 包中附带的摘要进行比较，然后发现 hash 值相等，所以接收数据，验证了完整性。

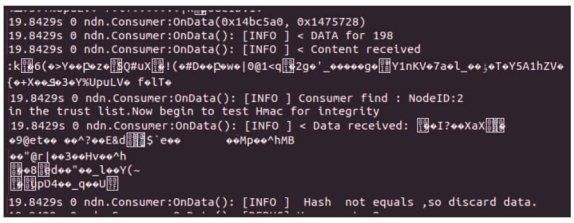

图 6　consumer 解密数据及认证过程图

把 p_2 从 consumer 的信任列表中去掉，如图 7 第 4 行，那 consumer 就会认为 p_2 发送的数据不受信任，不会接收，后面的步骤不会进行。

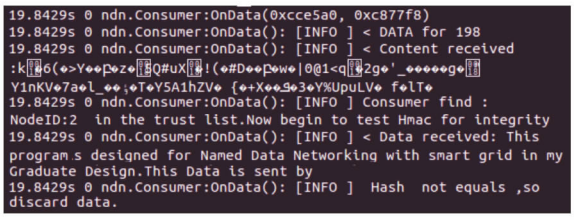

图 7　p_2 不受信任后消费者验证过程

综上，算法仿真的过程验证了数据的机密性、完整性及认证性。

3.3.2　攻击方式模拟仿真验证

1）攻击者篡改数据内容。

如果数据中途发生变更，例如 C（密文）被攻击者截去或者丢失了末尾的 nodeID，变为：“ This program is designed for Named Data Networking with smart grid in my Graduate Design. This Data is sent by ”，如图 8 所示。

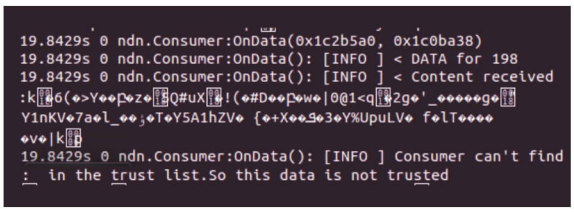

图 8　数据内容受篡改后的防范策略

consumer 尽管不知道数据是否完整，但是可以从信任列表中找出密钥，解密出信息，验证摘要时发现不相等，于是完整性验证失败，不予接收数据。

2）攻击者伪造成另外的 ID。

如果攻击者伪造受信任的 ID（在这里假设 ID 为 Node:2），向消费者发送自己的 Hmac 和 C，以及受信任的 ID，则如图 9 所示。

图中，consumer 接收数据后在信任列表里找到了 Node:2，于是利用 p_2 的密钥对数据内容做了异或解密，但是由于攻击者和 p_2 的密钥不相等，无法解出正确的信息，完整性也验证失败，不予接收数据。

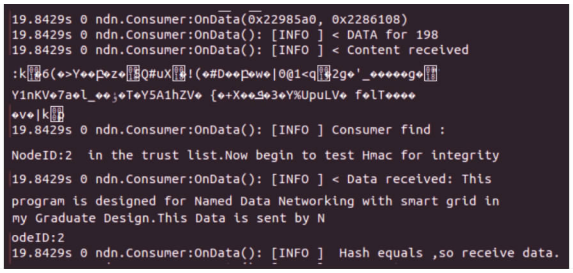

图 9　ID 被伪装后的防范策略

综上所述，算法的安全性以及在各攻击方式前的防范策略，都在仿真中得到了验证。

4　结语

本文的设计目标是实现一种适合 NDN 网络拓扑的数据加解密算法，保障互联网异构网络下通信安全，并通过 ndnSIM 仿真器进行验证。算法共为 13 个步骤，第 1～6 步为发送方数据加密和发送过程，第 7～13 步为接收方数据解密和验证的过程。此算法提高了数据的机密性、完整性、和认证性，同时优化了异或算法提高了算法效率，并对遭受的各种网络攻击方式，包括穷举攻击、数据内容篡改和身份伪装等，有相应的防范策略，具有良好的解决效果。此算法的仿真验证是采用 ns-3 的 ndnSIM 仿真软件，完全遵从 NDN 的框架的模块化方式。为了验证算法的安全性，在 ndnSIM 下自定义一个 12 节点的拓扑结构，采用最佳路由策略，模拟完整的通信过程，证明了数据从发布者开始是以密文方式进

行传输,具有机密性;收到数据后能正确地验证发布者的身份,具有认证性,并正确地解出明文和验证数据是否有改动,具有完整性。然后分别对攻击方式中的数据内容篡改和身份伪装进行了仿真,验证了对网络攻击防范的有效性。

参考文献(References):

[1] KOPONEN T, CHAWLA M, CHUN B G. A Data-Oriented (and Beyond) Network Architecture[J]. ACM SIGCOMM Computer Communication Review, 2007,37(4):181-192

[2] CHERITON D R, GRITTER M. TRIAD: A New Next-Generation Internet Architecture[ROL]. Technical Report, Stanford: Computer Science Department, Stanford University, 2000.

[3] JACOBSON V, SMETTERS D K, THORNTON J D, et al. Networking Named Content[J]. Communications of the ACM,2012,55(1):117-124.

[4] ZHANG L, AFANASYEV A, BRUKE J, et al. Named Data Networking[J]. ACM SIGCOMM Computer Communication Review,2014,44(3):66-73.

[5] LAGUTIN D, VISALA K, TARKOMA S. Publish/Subscribe for Internet: PSIRP Perspective[M]. Amsterdam: IOS Press. 2010:75- 84.

[6] NIWVWER N, BAUCKE S, EI-KHAYAT I, et al. The Way 4WARD to the Creation of a Future Internet [C]//IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications. Cannes, France:IEEE,2008:1-10.

[7] FOTIOU N, NIKANDER P, TROSSEN D, et al. Developing Information Networking Further: from PSIRP to PURSUIT[C]// Broadband Communications, Networks, and Systems. Berlin Heidelberg: Springer, 2012:1-13.

[8] SAIL Project. Scalable and Adaptive Internet Solutions (SAIL)[EB/OL]. [2013-01-01][2018-07-01]. http://www.sail-project.eu.

[9] 杨柳,马少武,王晓湘.以内容为中心的互联网体系架构研究[J].信息通信技术,2011,5(6):66-70.
YANG L, MA S W, WANG X X. Research on Content Centric Internet Architecture[J]. Information And Communications Technologies 2011,5(6):66-70. (in Chinese)

[10] 雷凯.信息中心网络与命名中心网络[M].北京:北京大学出版社,2015.
LEI K. Information Center Network and Named Center Network[M]. Beijing: Beijing University Press, 2015. (in Chinese)

[11] 孔媛媛,杨震,吕斌,等. 一种基于信道生成密钥的安全网络编码系统[J].南京邮电大学学报(自然科学版),2018,38(3):7-13.
KONG Y Y, YANG Z, LYU B, et al. Secure Network Coding System Based on Channel Generation Key [J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2018, 38(3):7-13(in Chinese)

[12] SALAH H, WULFHEIDE J, STRUFE T, et al. Coordination Supports Security: A New Defence Mechanism Against Interest Flooding in NDN[C]//The 40th Annual IEEE Conference on Local Computer Networks. Clearwater Beach, FL, USA: IEEE, 2015: 73-81.

[13] CHAUM D, VAN HEYST E. Group Signatures [C]//EUROCRYPT'91. Berlin: Springer, 1991: 257-265.

[14] RENY J, HARNZ L. How to Leak a Secret from Multiple Sources[C]// Military Communications Conference. SAN Diego, CA,USA: IEEE,2008.

[15] DASH S, SAHU B J R, SAXENA N, et al. Flooding Control in Named Data Networking[J]. IETE Technical Review, 2018, 35(3):266-274.

[16] MASTORAKIS S, SAHU A A, ZHANG L X. On the Evolution of ndnSIM[J]. ACM SIGCOMM Computer Communication Review,2017,47(3):19-33.

(编辑:徐楠楠)