

抗污染攻击的移动 P2P 数据安全分发系统

杨 柳, 钟 诚, 张 静, 伍世刚, 陈志朕, 陈绪伟, 马超金

(广西大学 计算机与电子信息学院, 广 西 南 宁 530004)

摘 要: 采用网络编码方法, 给出一个改进的抗污染攻击的安全签名机制, 使得签名的私钥能随着传输数据包的改变而改变, 运用该安全签名机制设计开发一个移动 P2P 数据分发原型系统 S-SymTorrent. S-SymTorrent 以抗污染攻击签名机制作为其数据传输的安全控制策略, 不仅获得了较高的传输率, 而且确保数据分发的安全性.

关键词: 安全数据分发; 移动 P2P 网络; 网络编码; 污染攻击; 签名机制

中图分类号: TP319

文献标识码: A

文章编号: 1000-7180(2012)09-0160-04

Secure Data Distribution System Against Pollution Attacks on Mobile Peer-to-Peer Network

YANG Liu, ZHONG Cheng, ZHANG Jing, WU Shi-gang,

CHEN Zhi-zhen, CHEN Xu-wei, MA Chao-jin

(School of Computer and Electronics and Information, Guangxi University, Nanning 530004, China)

Abstract: An efficient secure signature scheme against pollution attacks is improved by network coding, which the private key for its signature can be updated along with the change of transmission packet. A system prototype for secure data distribution on mobile peer to peer network, called S-SymTorrent, is designed and implemented by the given improved secure signature scheme. S-SymTorrent system can transform efficiently the data by the signature scheme against pollution attack, and it can guarantee reliable data distribution.

Key words: secure data distribution; mobile P2P network; network coding; pollution attack; signature scheme

1 引言

BitTorrent 是目前流行的 P2P^[1] 文件共享系统. BitTorrent 协议将文件分割成若干小部分, 然后在一个完全分布式计算环境下发送文件, 再通过定位来恢复文件^[2-3]. SymTorrent 是用于移动环境的 BitTorrent 客户端程序^[4], 它使用标准 BitTorrent 协议, 支持所有采用 Symbian 操作系统的手机, 支持多个用户同时上传和下载文件.

2 抗污染攻击的签名机制

所谓污染攻击^[3], 是指攻击者任意篡改正在传输的数据, 给这些数据加入假信息或错误信息. 在污

染攻击中, 攻击者的动机不仅是想截获发送方所发送的有用信息, 还千方百计想阻止发送方和接收方之间的正常通信^[6]. 本文改进一个抗污染攻击的安全签名机制, 该机制以基于同型哈希签名函数的网络编码签名算法为核心, 加大签名私钥的难度, 令攻击者无法伪造数据包, 以有效抵抗污染攻击.

2.1 网络模型

S-SymTorrent 原型系统将移动 P2P 网络看成由 N 个节点和 E 条边(链路)组成的有向图(N, E)^[4]. 网络中有 1 个或 $s \in N$ 个源节点要向其他 $t \in N$ 个接收节点发送信息. 源节点将要传输的文件 F 划分为 n 块, 每个文件块细分为 m 小块. 当接收节点收到 n 个线性独立的文件块时, 即可完整地还原

出原始文件:

$$F=(B_1, B_2, \dots, B_n)^T$$

$$B_i=(b_{i,1}, b_{i,2}, \dots, b_{i,m})$$

其中 $b_{i,j} \in Z_q (1 \leq i \leq n, 1 \leq j \leq m)$, q 为素数.

然后,源节点将 B_i 扩充成如下形式:

$$B_i=(B_i, U_i)$$

$$=(b_{i,1}, \dots, b_{i,m}, 0, \dots, 0, 1, 0, \dots, 0)$$

B_i 的第 $m+i$ 列到第 $m+n$ 列的元素中除了第 $m+i$ 列的元素值等于 1 外,其他列的元素值等于 0. 下面所涉及的 B_i 均指 B_i 的扩充形式.

令 $Out(v)$ 表示从节点 v 发出的边, $In(v)$ 表示进入节点 v 的边, $\bar{Y}(e)$ 表示在边 $e \in Out(v)$ 上传输的数据包, $\bar{Y}(e')$ 表示在边 $e \in In(v)$ 上传输的数据包,则 $\bar{Y}(e)$ 是 $\bar{Y}(e')$ 的线性组合,亦即在节点 v 处接收到的文件块(数据包) B_i 的线性组合. 用 W 表示 $\bar{Y}(e)$, W 即是中间节点或目标节点接收到的信息包. 则:

$$\begin{aligned} W = \bar{Y}(e) &= \sum_{e' \in In(v)} \beta_{e'}(e) \bar{Y}(e') = \sum_{i=1}^n g_i(e) B_i \\ &= \left(\sum_{i=1}^n g_i(e) b_{i,1}, \dots, \sum_{i=1}^n g_i(e) b_{i,m}, g_1(e), \dots, g_n(e) \right) \\ &= (y_1(e), \dots, y_m(e), g_1(e), \dots, g_n(e)) \end{aligned} \quad (1)$$

其中, $\beta_{e'}(e)$ 是随机数, $G(e) = (g_1(e), \dots, g_n(e))$ 是在 $e \in Out(v)$ 上的一个全局编码向量,由在 $e \in Out(v)$ 的本地编码向量 $\beta(e) = [\beta_{e' \in In(v)}(e)]$ 中递归计算而得. 即

$$G(e) = \sum_{e' \in In(v)} \beta_{e'}(e) G(e') \quad (2)$$

签名机制主要思想是:源节点计算出与 B_i 正交的向量 U ,再将 U 分解出来的一部分(与私钥有关)与 B_i 的乘积作为签名填充至 W 中. 接收节点收到 W 时利用公钥验证 W 的合法性.

2.2 签名机制

对于三阶段的签名机制,本文改进一个基于同型哈希签名函数的网络编码签名算法^[8],并作为抗污染攻击的安全签名机制的核心:

(1) 设置参数阶段

设置以下主要参数:

素数 p 和 q , $p < q$ 且 q 与 $p-1$ 互素, $g \in F_q$ 且满足 $O(g) = p$, 私钥 $K_S = \{\alpha_i, i=1 \sim m+n\}$, 公钥 $K_P = \{h_i = g^{\alpha_i}, i=1 \sim m+n\}$.

(2) 签名阶段

① 源节点计算与 B_i 的正交量

$$U=(u_1, u_2, \dots, u_{m+n}), U \in F_p^{m+n}$$

② 源节点计算

$$R=(u_1/\alpha_1, u_2/\alpha_2, \dots, u_{m+n}/\alpha_{m+n})$$

③ 将 B_i 与 R 的乘积作为签名填充至 W

发送节点对数据的正交向量计算可离线进行,不会对系统传输时间造成太大影响.

(3) 验证阶段

当接收节点收到 W 时,首先计算:

$$d = \prod_{i=1}^{m+n} h_i^{R_i W_i} \quad (3)$$

然后以 d 是否等于 1 判断 W 是否为合法的信息. 若 W 是合法的(即未被污染),则 $d=1$. 这是因为,若 W 是合法的,则有:

$$\begin{aligned} d &= \prod_{i=1}^{m+n} h_i^{R_i W_i} = \prod_{i=1}^{m+n} (g^{\alpha_i})^{U_i W_i / \alpha_i} \\ &= g^{\sum_{i=1}^{m+n} U_i W_i} = g^0 = 1 \end{aligned} \quad (4)$$

式(4)表明:若 $d=1$,表示收到的数据可用,否则不可用,应该放弃.

3 移动 P2P 安全数据分发原型系统 S-SymTorrent 的设计与实现

S-SymTorrent 原型系统运行在 Symbian 操作系统上,实现将数据从一个手机用户发送到另一个或多个手机用户的过程. S-SymTorrent 采用的安全控制策略是第 2 节提出的抗污染攻击的签名机制.

3.1 安全策略

S-SymTorrent 原型系统的数据传输机制采用了网络编码技术和抗污染攻击的安全签名机制. 发送者在发送前对文件块进行签名,接收者收到文件块时即可对该文件块的合法性进行验证. 检验工作不需在全部数据传输完成后才开始,以及时阻断非法数据的继续传播,节约传输带宽,提高数据的传输效率.

签名机制的签名算法在 CActive 类的成员方法 SDD_Write() 中实现;验证算法在 CActive 类的成员方法 SDD_Read() 中实现.

3.2 核心代码设计

S-SymTorrent 数据的分发与接收都是通过 Socket 实现,其中类 CSocketWriter 用来处理数据的分发,类 CSocketReader 用来处理数据的接收.

在数据分发之前,须先建立网络连接,然后监听节点的接入及其与跟踪服务器 Tracker 的连接,当有请求时开始发送/接收数据.

在 S-SymTorrent 中, CSocketBase 是抽象类, 它封装了节点异步读写 Socket 的请求, 读写 Socket 用 CSocketBase 的继承类 CSocketWriter 和 CSocketReader 实现。

CSocketWriter 类封装了节点的异步写请求, 其作用是通过已经建立好的 Socket 发送数据。数据发送前执行签名算法 SDD_Write(), 然后将可发送数据放入写缓冲区, 如果此时活动对象未激活则激活该对象, 如果对象已经处于激活状态, 则将数据发送出去。CSocketWriter 类 Write 方法描述如下:

```
void CSocketWriter::Write(const TDesC8& aBuf){
    iLongBuffer->Insert(iLongBuffer->Size(), aBuf);
    if (!IsActive()){
        if (SDD_Write())
            IssueWrite();}}}
```

当一个数据成功发送后, 系统检查发送缓冲区是否还有数据。如果该缓冲区还有数据, 则提交一个新的发送请求。如果发送请求失败, 则执行 HandleWriteError() 方法。

S-SymTorrent 系统中接收数据的处理过程与发送数据过程类似, 也是一个必须通过活动对象来实现的异步处理过程。节点接收数据时也要定义一个接收缓冲区, 接收到数据时要对数据进行验证, 即执行验证算法 SDD_Read(), 如果数据合法, 那么将数据放入缓冲区。这个过程用 CSocketReader 的 StartReading() 方法来实现:

```
void CSocketReader::StartReading(){
    if (!IsActive()){
        if (SDD_Read()){
            iSocket.RecvOneOrMore(iShortBuffer,
                0, iStatus, iLastRecvLength);
            SetActive();}}}}
```

S-SymTorrent 系统在运行过程中, 如果有某个或多个手机用户需要下载某个文件, 他们将发出请求, 拥有该文件的手机用户会响应这个请求, 将文件发送到这些需要这个文件的手机用户中。

3.3 系统运行结果

图 1 显示了 S-SymTorrent 原型系统文件发送和接收过程。图 1 只显示了一个源节点发送文件和一个目标节点接收文件的界面。事实上, 可以同时有多个节点发送和接收数据。

S-SymTorrent 原型系统的主要特色是将抗污染攻击的签名机制应用在数据分发过程中, 并在发送和接收过程中对数据进行签名和验证。该机制能及时发现并阻断非法数据包的继续传播, 攻击者很

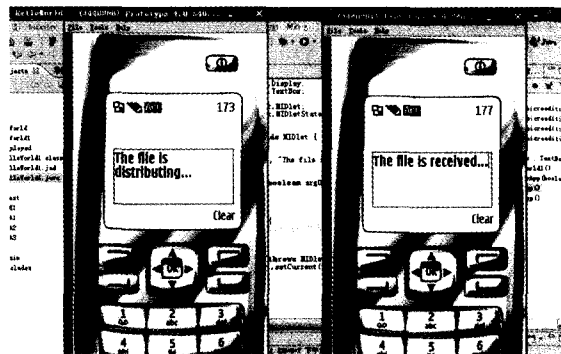


图 1 发送文件和接收文件的运行结果界面

难获得私钥, 因此能有效抵抗污染攻击。抗污染攻击的签名机制保证了 S-SymTorrent 原型系统数据传输的安全性。

4 结束语

本文采用网络编码方法, 改进抗污染攻击的安全签名机制, 使得签名的私钥能随着传输数据包的变化而改变; 进一步地, 在 SymTorrent 的基础上, 设计开发了一个具有安全控制的移动 P2P 数据分发原型系统 S-SymTorrent。该系统运行在 Symbian 操作系统下, 可以实现一个或多个手机源节点向其他手机节点发送数据。S-SymTorrent 系统将抗污染攻击的安全控制策略应用在数据分发过程中, 它能够有效降低和消除污染攻击的隐患, 确保 S-SymTorrent 数据的安全传输。

参考文献:

- [1] 杨柳, 钟诚, 陆向艳. 基于 P2P 网络的分布式聚类算法研究分析[J]. 微电子学与计算机, 2009, 26(8): 83-85.
- [2] Rafit Izhak-Ratzin. Collaboration in bittorrent systems [C] // Proceedings of NETWORKING 2009, LNCS, 2009, 55(5): 338-351.
- [3] Mohammed Hawa, Jamal S Rahhal, Dia I Abu-Al-Nadi. File size models for shared content over the BitTorrent Peer-to-Peer network[J]. Peer-to-Peer Networking and Applications, 2012, 5(3): 279-291.
- [4] Fitzek H P, Hassan Charaf. Mobile peer-to-peer (P2P) a tutorial guide[M]. Chennai, India: Laserwords Private Limited, 2009: 103-142.
- [5] Fragouli C, Boudec J Y L, Widmer J. Network coding: an instant primer[J]. SIGCOMM Computer Communication, 2006, 36(1): 63-68.
- [6] Shweta Agrawal, Dan Boneh, Xavier Boyen, et al. Preventing pollution attacks in multi-source network

coding[J]. Public Key Cryptography, LNCS, 2010, 56(6): 161-176.

- [7] Jiang Y, Fan Y, Shen A X, et al. A self-adaptive probabilistic packet filter scheme against entropy at-

tacks in network coding [J]. Computer Networks, 2009, 53(18): 3089-3101.

- [8] 杨铭熙, 严文杰. 一次一密的网络编码签名算法[J]. 武汉理工大学学报, 2009, 31(3): 73-76.

作者简介:



杨 柳 女, (1970—), 硕士, 讲师. 研究方向为网络信息安全、P2P 技术.



钟 诚 男, (1964—), 博士, 教授, 博士生导师. 研究方向为网络信息安全、并行分布计算.

(上接第 159 页)

进一步降低功耗. 可以从以下几方面进行改进: 采用动态功率管理机制, 根据网络链路状态动态改变芯片的发射功率; 嵌入操作系统, 对资源进行高效的利用和管理; 采用唤醒机制, 使节点可以从睡眠状态被动的进入唤醒状态.

参考文献:

- [1] 孙利明, 李建中, 陈渝, 等. 无线传感器网络[M]. 北京: 清华大学出版社, 2005.
- [2] 王殊, 阎毓杰. 无线传感器网络的理论及应用[M]. 北京: 北京航空航天大学出版社, 2007.
- [3] MSP430x13x, MSP430x14x, MSP430x14x1 Mixed Signal Microcontroller (Rev. F). [EB/OL]. [2012-02-05]. Available: <http://www.ti.com/product/msp430f149?>

247SEM.

- [4] nRF24L01+ Single Chip 2.4GHz Transceiver Product Specification v1.0. [EB/OL]. [2012-02-05]. Available: <http://www.nordicsemi.com/eng/Products/2.4GHz-RF>.
- [5] 李明明, 李伟. 低功耗无线传感器网络节点的设计技术[J]. 测控技术, 2010, 29(6): 8-11.
- [6] 段翠琴, 孙晶晶. WSN 中能量有效的分区聚簇多跳路由算法[J]. 计算机工程, 2010, 36(14): 87-89.

作者简介:

于 凯 男, (1987—), 硕士研究生. 研究方向为无线传感器网络.