doi:10.3969/j.issn.1000-436x.2013.z1.015

SIM：应用于 MANET 的安全 IP 协议

李荣森[12]，窦文华[1]
（1. 国防科学技术大学 计算机学院，湖南 长沙 410073；2. 中国人民解放军第 72946 部队，山东 淄博 255000）

摘 要：参考 IP Sec 的核心思想，并结合 MANET 的具体实际，提出了一种安全的 IP 协议 SIM（secure IP protocol for manet）。通过在网络层和数据链路层之间添加一个无连接的安全层，对进出协议栈的数据报文进行安全处理。通过将 IP Sec 的安全协定 SA 简化为轻量级的适合 MANET 的 SSA，在保持 IP 安全性的同时降低了协议开销和部署复杂度。进行了基于 Linux 的协议栈设计和原型系统实现。

关键词：SIM；MANET；IP Sec；SA
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2013)Z1-0116-10

SIM: a secure IP protocol for MANET

LI Rong-sen[1,2], DOU Wen-hua[1]
(1. School of Computer Science, National University of Defense Technology, Changsha 410073, China;
2. 72946 Troops, People's Liberation Army, Zibo 255000, China)

Abstract: According to the core logic of IP Sec, a secure IP protocol was proposed for Mobile Ad Hoc network. Security deal to the packets in and out of the network protocol stack was done by adding a transparent secure layer between transport-layer and link-layer. By simplifying the complex security association to simple security association, SIM reduces the cost of initial IP protocol while keeping security. At last a prototype of the proposed protocol was also implemented.
Key words: secure IP protocol for manet; mobile ad hoc networks; IP security protocols; security association

1 引言

移动 ad hoc 网络（mobile ad-hoc network）简称 MANET，起源于 20 世纪 70 年代，具有不需要任何基础设施、无中心、无组织等特点。与传统的有线网和普通的无线网相比，MANET 具有如下特点[1]。1）快速变化的动态拓扑结构，在 MANET 中，用户和节点可以按照任何速度和任何方式随意地移动，所以节点间的相互关系也会相应地发生很大的变化。2）有限的带宽。MANET 采用无线传输技术作为其底层技术，所以带宽比传统的有线网络要小很多。3）能量受限。由于节点的移动特性，大部分节点会采用电池供电的形式，其总能量开销不可避免地受到很大限制。4）物理安全不可保证，与固定网络相比，MANET 的链路更容易被攻击和破坏，节点本身也很容易被捕获或摧毁，所以其安全隐患远大于传统的固定网络。因此，除了传统网络所受到的威胁，MANET 还面临一些特殊的威胁。所以，要保证 MANET 中数据传输的安全，除了传统的安全技术和措施外，还必须设计针对 MANET 的新的安全机制。

在深入研究 MANET 的安全特性的基础上，提出了一种应用于 MANET 的安全的 IP 协议 SIM（secure IP protocol for Manet）；分析了协议的安全性并描述了实现过程。

2 相关研究

刘永亮等[2]针对 AYDOS 等提出的密钥交换方案进行了分析，证明了该协议针对来自任何攻击者的中间人攻击都是脆弱的，并分析了这类协议易受到攻击

收稿日期：2013-07-30
基金项目：国防预先研究课题基金资助项目（405010202, 513160302）
Foundation Item: National Defense Pre-Research Foundation of China (405010202, 513160302)

的原因和其他一些安全缺陷。冯涛等[3]针对 Ad Hoc 网络提出了一种安全有效的分布式组密钥管理方案，实现了组密钥的前向保密与后向保密。李慧贤等[4]提出了一个无需安全信道的门限密钥管理方案。该方案中，可信中心的功能由局部注册中心和分布式密钥生成中心共同实现；通过门限技术，网络内部成员相互协作分布式地生成系统密钥；利用基于双线性对的公钥体制实现了用户和分布式密钥生成中心的双向认证；通过对用户私钥信息进行盲签名防止攻击者获取私钥信息。张串绒等[5]提出了一个基于身份的新签密算法，对其安全性和效率进行了分析及证明，并以 Ad Hoc 网络分布式门限密钥管理中各服务节点所拥有的系统密钥份额的更新为例，说明了将新签密算法用于 ad hoc 网络安全协议的方法及其意义。

AHMAD 等[6]针对 802.11w 协议的特性进行了研究，指出协议中的一些特性可能会被误用从而导致严重的冲突，并讨论了避免的方法。李小青等[7]基于 D-S 证据理论,设计了一个 MANET 信任评估模型，为路由建立提供安全的网络环境。协议根据信任评估结果选择可信节点建立路由，并提出在路由表中存储节点匿名身份的 Hash 路由登记表，保证 ARAN 协议认证安全，实现匿名安全和提高路由查找效率,同时协议在路由建立过程中，完成了会话密钥协商。付颖芳等[8]提出了无线 Mesh 网中一种基于端到端的虫洞攻击检测机制。

SHU 等[9]分析了无线 Ad Hoc 网络中的分组丢失究竟是由于链路差错还是恶意丢弃引起的，并提出了一种基于 HLA 的检测机制来检测不同原因引起的分组丢失。刘方斌等[10]将民主签名与无中心的秘密分享方案相结合，提出一种无可信中心的门限追踪 Ad Hoc 网络匿名认证方案。韩磊等[11]基于组合公钥思想，将 ElGamal 方案与预分配密钥方式相结合，提出一种基于身份的预分配非对称密钥管理方案(PAKMS)。通过私钥生成中心为节点预分配主密钥子集及基于时间获得节点密钥更新的方式，从方法上降低了移动 Ad Hoc 网络非对称密钥管理中的通信开销，弱化了基于身份密钥管理中存在的私钥托管问题对网络安全的影响。吴呈邑等[12]在可信平台模块 TPM(trusted platform module)的安全体系结构基础上，提出了一种基于动态第三方可信公平非抵赖协议,以取代固定 TTP，提高协议效率。

IPSec 是 IETF 下的 IPSEC 工作组，于 1994 年对 IP 安全协议（IPSP）和对应的 Internet 密钥管理协议(IKMP)进行标准化工作，其结果总体上由 4 部分组成：安全加密封装(ESP)[13]、报文认证(AH)[14]、安全协定(SA, security associations)和密钥管理[15]。IPSec 可提供如下安全服务：1) 数据源鉴别；2) 非连接 IP 信息机密性；3) IP 通信流量机密性；4) 非连接信息完整性；5) 强制存取控制或 IP 双向鉴别；6) 密钥分配。但 IPSec 也存在着一定的局限性，最重要的一点是其复杂性，要在无连接的 IP 层保持安全连接，需要记录较多的管理状态。其次的问题是如何为 IP 进行密钥分配特别是密钥交换。除了上述 2 个关键的问题外，IPSec 还有其他一些局限性，如需要已知范围的 IP 地址或固定范围的 IP 地址等。

借鉴 IP Sec 的核心思想，并引入新的安全机制，提出了应用于 MANET 的安全的 IP 协议 SIM。通过简化 IP Sec 的 SA 安全协定为 SSA(simplified security assciation)，并且在报文流入流出协议栈之前进行预处理，在保证安全性的前提下，大大降低了协议复杂度。与已有协议相比，SIM 的优势主要体现在：1) 基于 IP Sec 的核心安全机制，安全性较高；2) 新协议复杂度大大降低，便于实际实现和应用；3) 使用基于邻居表触发的 SSA 更新机制，使协议开销较小，并且密钥新鲜度高。下面将对提出的 SIM 协议进行详细介绍。

3　应用于 MANET 的安全 IP 协议栈 SIM

3.1　SIM 协议层次

论文设计的无连接网络层安全协议 SIM 基于 TCP/IP 协议栈，在网络层和数据链路层之间添加一个无连接的安全层，如图 1 所示。

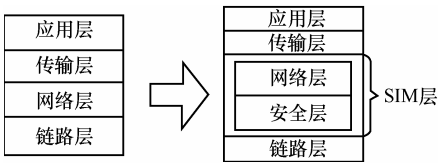


图 1　SIM 的协议层次

新的安全 IP 体系结构在原来的网络层次结构上插入了一个安全层，所有的数据发送和接收都要经过安全层。而新的安全层与原网络层一起构成新的 SIM 层，保证数据在每一步的无线传输过程中都有认证和加密保证。新的 SIM 安全协议将原 IPSec 的安全运算过程分布到了传输链路中的各个节点（在 MANET 模式中，中转节点和端节点是对等的），因而各个节点只需维护自己邻居节点的通信

安全协定 SA（security association），而不需要维护所有端到端的通信安全协定。新的 SIM 正是基于这个简化定义的通信安全协定 SSA 连接了数据链路层和网络层。

3.2 报文格式

定义新的 IP 层安全协议的功能为：一个透明的协议层在 IP 层与 MAC 层之间，以 SSA 为核心，对节点的无线接入进行认证，对 IP 报文的关键信息进行加密，提供对整个 IP 报文进行验证，同时提供防重放攻击的能力。简化的安全协定 SSA 主要包括对方 MAC 地址、密钥分组以及 Linux 内核相关的结构维护信息等。而 SIM 报文格式的具体定义则如图 2 所示。

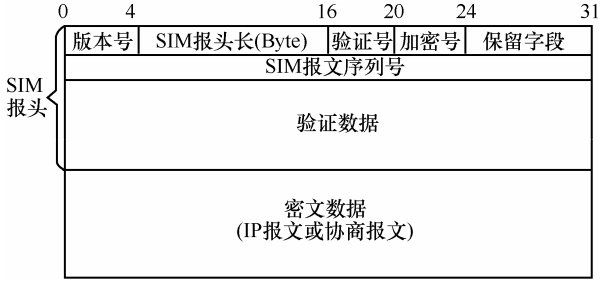


图 2 SIM 报文格式

版本号：用于区别不同的 SIM 版本，以支持后续设计和版本升级。

SIM 报头长：SIM 报头的长度（以字节为单位），SIM 报头之后的密文数据不计算在内。

验证号：指定 SIM 报文中生成验证数据的算法，验证号与验证算法的对应关系不在网络上传输，而是内定在各个参与通信的节点中。各个节点内部的对应关系严格一致，而且作为一种秘密信息不对外公开。

加密号：指定 SIM 报文中数据加密的算法，加密号与加密算法的对应关系不在网络上传输，而是内定在各个参与通信的节点中。各个节点内部的对应关系严格一致，而且作为一种秘密信息不对外公开。

保留字段：默认都置空，备后续版本扩展使用。

SIM 报文序列号：指示通信双方当前通信报文的报文序列号，用于防止重放攻击，同时用作通信双方同步通信密钥的索引。

验证数据：由验证算法生成的报文验证数据，数据验证范围包括 SIM 报头和紧跟其后的密文数据，生成验证数据时，SIM 报头中的验证数据全部填 0。

密文数据：受加密保护的 IP 层数据报文（出于效率考虑，这里只加密 IP 层的关键数据），或者 SIM 协议自身的 SSA 协商和管理报文（SIM 协商报文全部以密文的形式进行，初始的密钥基于 ECC 密码机制协商生成）。

3.3 报文处理过程

SIM 的协议交互和处理过程以 SSA 为核心。SSA 是 IPSec 中 SA 的精简定义，它把 IPSec 端到端的安全通信协定管理分散到通信路径中的各个节点，整个 SIM 数据报文通信过程的安全性是由安全的通信转发节点和安全的点到点通信链路一步一步保证的。SIM 可以看成是为 MAC 层提供点到点的安全通信服务，因而节点中的 SSA 表项只需管理和维护邻居节点的安全通信协定状态。

围绕节点 SSA 表项的维护和使用，SIM 的协议交互和处理过程可以分为 2 个大的方面：SSA 的生成与维护、根据 SSA 进行的 SIM 通信。

3.3.1 SSA 的生成与维护

1) SSA 的生成

由前述分析，节点中的 SSA 表项只保存相邻节点的安全通信协定，若节点收到的申请来自某个新节点（在当前的 SSA 表中未有该节点对应的表项），则启动协商生成新的 SSA 表项。初始的协商过程采用与 IP Sec IKEv2[16]类似的机制，使用 ECDH 密码机制来完成。现假定 A 在通信网络中（已通过无线接入认证），B 为新加入的节点，则 SSA 生成过程具体如下（设参与协商的双方分别用 A 和 B 表示），如图 3 所示。

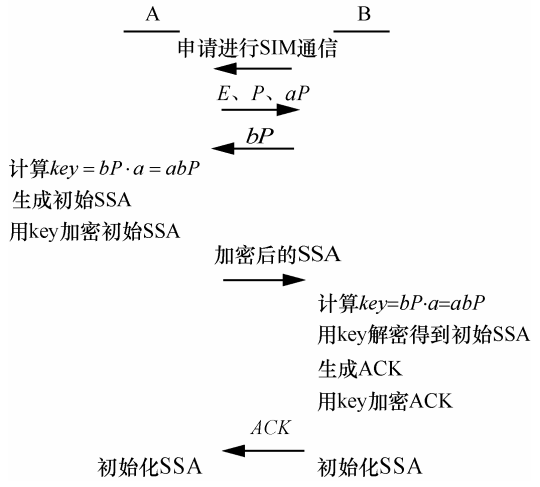


图 3 SSA 生成过程

(a) B 向 A 发出参与通信的申请，并给出有限域 Fq（其中 $q=p^r$，p 为素数）上自己支持的一组椭

圆曲线。

(b) A 从其中选定一条椭圆曲线 E，以及随机点 $P \in E$ （该点要保证能生成一个规模接近 E 的子群）。随后 A 选定一个随机数 $a \in \{1, 2, \cdots, q-1\}$，并计算出 aP，将 E、P、aP 一起反馈给 B。

(c) B 选定一个随机数 $b \in \{1,2,\cdots,q-1\}$，并计算出 bP 发送给 A。

(d) A 计算 $Key=bP \cdot a=abP$，并用计算出的 Key 加密 AB 之间的初始 SSA 信息，然后发给 B。

(e) B 计算 $Key=aP \cdot b=abP$，并用计算出的 Key 解密收到的初始 SSA 信息。然后初始化对应的 SSA 表项，并用 Key 加密一个确认信息，回复给 A 以确认 SSA 初始化完成。

2) SSA 的维护

由于节点 SSA 表中只保存了相邻节点对应的表项，这与 IP 协议栈中的 ARP 邻居表是相对应的，因而 SSA 邻居表项与 ARP 的邻居表项可以建立起一一对应的关系，从而 SSA 邻居表项的配置、生成、更新、删除等维护操作都由 ARP 邻居表的变化触发。这样做还可以带来额外的一个好处：ARP 动态邻居表项的更新时间周期为几分钟，正好自动使 SSA 表项同步进行更新，从而保证了 SSA 的新鲜性。

如果是更新周期到期或当前 SSA 密钥分组耗尽引起的 SSA 更新，则由当前节点直接生成一个新的 SSA，使用当前 SSA 生成通信密钥后，加密新 SSA 然后发送给对方，对方成功收到并解密后，发送一个回应信息。然后双方更新为新的 SSA 即可。

如果是新邻居节点加入或怀疑当前密钥泄露等其他网络故障引起的 SSA 更新，则按照初始 SSA 的生成过程执行新的 SSA 协商过程并生成新的 SSA。

3.3.2 SIM 通信过程

1) 通信密钥生成过程

如 3.2 节中所述，SSA 中有一个密钥分组字段。密钥分组中包含了一批可供当前通信加密使用的密钥。当需要对一个报文进行加密或解密操作时，首先根据目的节点 MAC 地址找到该报文对应的 SSA，然后从该报文中取出报文序列号，然后计算序列号的哈希值并对密钥分组中包含的密钥总数求余，以得到的余数作为密钥索引，从密钥分组中取出对应的密钥并用做通信密钥。如果取出的密钥已经被使用过，则顺序取出其后面的第一个未被使用过的密钥。如果密钥分组中密钥已耗尽，则启动一个 SSA 更新过程，然后用新的 SSA 生成通信密钥。

2) 发送过程

节点发送数据时，数据报文从协议栈的 IP 层进入 MAC 层的过程将被 SIM 的安全层截获，进入发送加密过程，具体步骤如下，如图 4(a)所示。

(a) SIM 根据数据报文要发往的下一跳节点在 SSA 邻居表中找到对应的 SSA 表项；

(b) 根据 SSA 的信息生成通信密钥流中的下一个加密密钥，同时记录报文对应的序列号；

(c) 根据 SSA 的信息选择报文的验证算法和加密算法；

(d) 加密上层报文的关键数据，用加密报文替换原来的报文；

(e) 添加 SIM 报头，将加密报文封装为 SIM 报文（其中的验证数据全填 0）；

(f) 计算整个 SIM 报文的验证数据，填入 SIM 报头的验证数据字段，形成完整的 SIM 报文格式；

(g) 将生成的新的 SIM 报文重新封装为 MAC 帧（修改帧长度和上层协议类型），然后将新的 MAC 报文交由 MAC 层进行发送处理。

3) 接收过程

节点接收数据是发送数据的逆过程，数据报文从协议栈的 MAC 层提交进入 IP 层的过程，提交函数根据 MAC 帧中关于上层协议类型的字段，将整个 MAC 帧提交到 SIM 安全层的接收函数，进入接收解密过程，具体步骤如下，如图 4(b)所示。

(a) SIM 根据 MAC 帧的源地址在 SSA 邻居表中找到对应的 SSA 表项；

(b) 根据报文的序列号进行防重放攻击判断；

(c) 根据报文的序列号和 SSA 信息生成通信密钥流中对应的解密密钥；

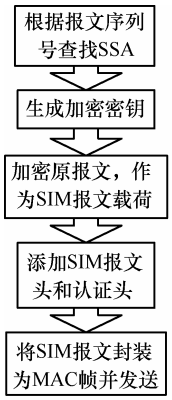
(d) 根据报文中的验证号、加密号和 SSA 的信息找到对应的验证算法和解密算法；

(e) 提取 SIM 报文中的验证数据，然后把 SIM 报文验证数据字段全部填 0；

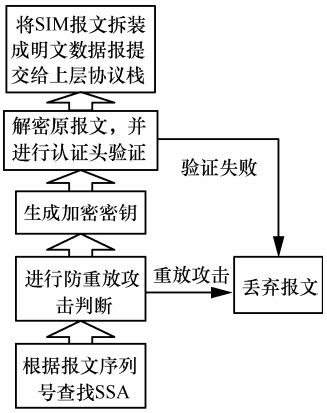
(f) 重新计算 SIM 报文的验证数据，与提取的验证数据进行比较验证；

(g) 解密 SIM 报文中的密文数据，得到上层协议报文的明文；

(h) 将上层协议报文的明文提交到网络层接收函数入口。



(a) 发送过程



(b) 接收过程

图 4 SIM 报文发送和接收过程

4 SIM 安全性讨论

4.1 SSA 生成与维护过程安全性

SIM 提供了网络层安全和 WLAN 安全相融合的安全服务，考虑到 IPSec 在 WLAN 中的适用性，精简 IPSec 中的 SA 为适用于 MANET 的 SSA；把原来 IPSec 复杂的端到端的安全通信协定(SA)的状态维护分布到了通信链路中的各个节点，形成了一个点到点的链路安全通信协定(SSA)。

4.1.1 SSA 生成过程的安全性

SIM 核心的安全技术基于 SSA 来完成，而 SSA 生成和维护的安全性则取决于协商生成初始 SSA 的过程。由于精简后的 SSA 的生成过程与 IPSec 中的 SA 的生成过程基本一样，所不同的只是参与协商的双方由端节点变成了链路中的 2 个相邻节点。所以提出的 SIM 协议中的 SSA 生成过程，其安全性与 IPSec 中 SA 的生成安全性是等价的。由 IPSec 协议 SA 生成过程的安全性可得 SIM 协议的 SSA 生成过程是安全的。

4.1.2 SSA 维护过程的安全性

SSA 维护主要分为正常的 SSA 更新和因网络拓扑变化或密钥泄露等引起的特殊更新 2 种。所以分 2 种情况进行讨论。

在正常更新情况下，新的 SSA 采用高强度密码算法加密后发送给对方，攻击者除密文外不能获得任何其他信息，在当前密钥安全的前提下，攻击新 SSA 的难度等同于破解基本的密码模块，所以此时新的 SSA 是安全的。

在密钥泄露等特殊情况下，新的 SSA 采用重新协商的方式进行更新。此时更新的过程与 SSA 生成过程基本一致，所不同的只是省去了选择椭圆曲线和生成元的操作，所以此种情况下 SSA 更新的安全性等价于 SSA 生成过程的安全性。由 4.1.1 节的结论可知此种情况下 SSA 更新过程也是安全的。

综合以上 2 种情况可知 SSA 维护过程是安全的。

4.2 SIM 通信过程安全性

SIM 协议采用了全新的网络报文格式，采用普通 IP 协议的节点无法进行协议的交互，更不能进行相互之间网络数据的传输，这堵绝了一大批攻击者，大大提高了系统安全性。

SIM 协议对每个报文进行认证，保证了数据报文的完整性和不可否认性。对原有载荷字段的全长度加密则保证了数据报文的机密性。通过对不同的报文动态地选择不同的密码算法和密钥，加强了实施攻击的难度。防重放攻击机制的设置，进一步增强了协议安全性。通信过程用到的密钥基于报文序列号和 SSA 生成，故其安全性由 SSA 保证，由 4.1 节的结论可知这些密钥是安全的。所以 SIM 通信过程是安全的。

综上所述，新设计的安全网络层协议 SIM 既能够提供类似于 IPSec 的安全服务，又能够很好适用于 MANET 的特殊无线通信环境，是无线网络中简单实用的网络层安全通信协议。

5 SIM 在嵌入式 Linux 平台的实现

安全网络层协议 SIM 基于开源的 linux 操作系统进行设计和实现，下面先分析 Linux 内核中网络协议栈，并设计 SIM 与 Linux 内核网络协议栈的联结关系，然后基于 HOOK 机制将 SIM 集成到 Linux 内核网络协议栈中，并简要描述内核代码中对应的修改点。

5.1 Linux 内核中网络协议栈

Linux 的 TCP/IP 协议栈大体流程如图 5 所示。

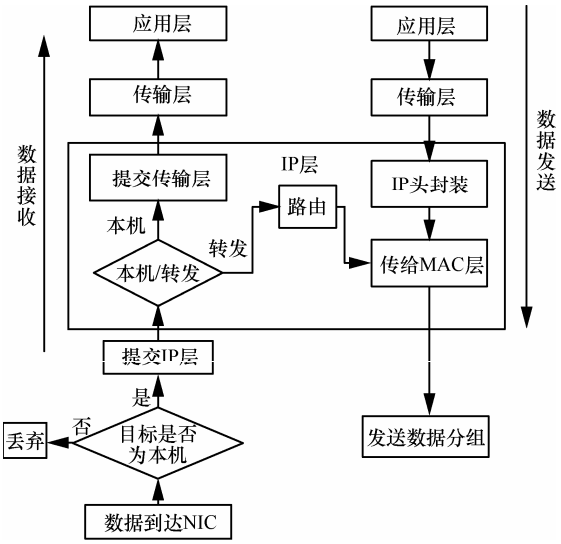


图 5　Linux 网络协议栈报文处理流程

Linux 网络协议栈中采用统一的缓冲区结构 sk_buff。底层从网络设备接收到数据帧后，分配一块内存，然后将数据整理成 sk_buff 的结构。在网络协议处理时，数据均以 sk_buff 的形式在各层之间传递、处理。一个个单独的 sk_buff 被组织成双向链表的形式。

sk_buff 的结构如图 6 所示，sk_buff 的强大功能在于它提供了众多指针，可以快速的定位协议头位置；它也同时保留了许多数据分组信息(如使用的网络设备等)，以便协议层根据需要灵活应用。

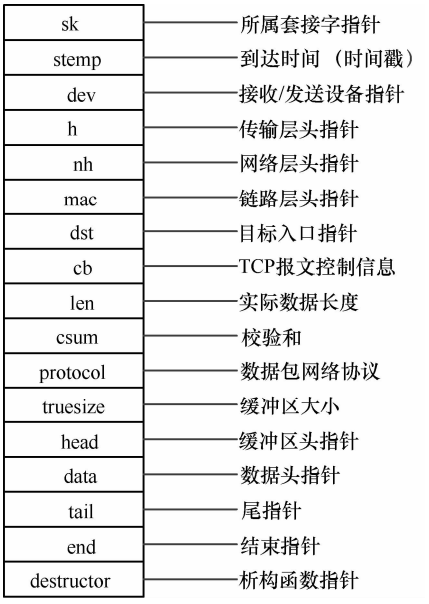


图 6　sk_buff 数据结构

控制 sk_buff 结构数据区的函数有多种，这些函数涉及的操作主要是指针运算，规律性很强，SIM 涉及到的主要有以下 4 个。

skb_put()：将数据添加到现有数据尾部。

skb_push()：将数据添加到现有数据头部。

skb_pull()：从数据区的头部删除数据。

skb_trim()：从数据区的尾部删除数据。

通过这些函数的操作，就可以方便的在数据分组头部添加、删除协议头，在数据分组尾部增加、删除数据。

Linux IP 层发送、接收、转发数据分组的函数则主要有以下几种。

ip_build_header()：此函数由各种不同的协议处理程序调用来根据套接字对象中包含的信息构建恰当的 IP 分组头部，并且把这个头部放入调用者传来的套接字数据缓冲区。IP 数据分组的头部就是由此函数构造。IPSec 构造新的 IP 报头也是利用这个函数来完成。

ip_build_xmit()：创建一个发送数据的套接字缓冲区。

ip_queue_xmit()：处理一个已经存在的套接字缓冲区，通过设备驱动程序发送一个 IP 分组。

ip_rcv()：这是一个非常重要的函数，它的功能就是从数据链路层那里接收数据分组。函数接收到一个 IP 数据分组后，首先检查这个分组是否有错误，即长度是否合法，版本是否正确，首部校验和是否正确，然后调用 skb_trim 函数将填充项去掉，得到真正的载荷，检查收到的分组是否分段，是否需要重组，之后，检查路由表，对数据分组路由，如果是发给本机的数据分组，最后，去掉 IP 报头，将数据分组提交到传输层协议那里(TCP 或 UDP)。如果不是发给本机的数据分组，调用 ip_forward。

ip_forward()：此函数将传送到本机，但目标主机又不是本机的数据分组转发出去。它常常由 ip_rcv 函数调用。

5.2　基于 Linux 的 SIM 设计

根据 SIM 协议在网络协议栈中的层次关系，结合 Linux 内核网络协议栈的结构，设计了 SIM 与原有 TCP/IP 之间的交互关系，如图 7 所示。

SSA 邻居表：SIM 的安全核心，记录通信双方的安全通信协定。

密钥流生成器：根据 SSA 中的信息生成通信双方的同步密钥流。

数据验证模块：实现 SIM 协议中的数据验证功能。

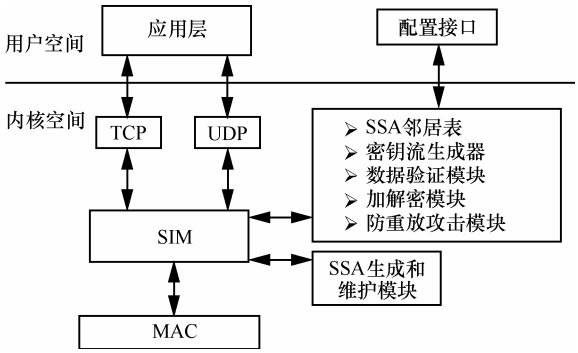


图 7　SIM 与 TCP/IP 交互关系

加解密模块：实现 SIM 协议中的数据加解密功能。

防重放攻击模块：实现 SIM 协议中根据报文序列号防止重放攻击的功能。

SSA 的生成和维护模块：基于椭圆曲线密码体制生成和维护 SSA 邻居表。

配置接口：为用户提供配置 SSA 的应用层接口。

5.2.1　SSA 的生成与维护

根据 SIM 的设计思想和采用的技术，在 SIM 协议与 Linux 内核中已有的 TCP/IP 协议栈之间，由 ARP 协议作为融合的桥梁，具体的实现方案如图 8 所示。

SIM 的 SSA 邻接表与 ARP 的邻居表相对应，SSA 表项的产生、维护、更新、删除等管理操作都由 arp_ibl 中对应表项的操作来触发，即 SIM 的 SSA 邻接表与 TCP/IP 协议族之间的交互融合由 ARP 协议代理完成。

当 SSA 邻接表被触发进行某项管理操作之后，SIM 将调用对应管理模块（如：节点加入、密钥更新、SSA 维护、节点退出）接收后发送 SIM 协商报文，完成对应的 SSA 管理操作。此过程是 SIM 内部定义的协商过程，不再与 ARP 协议相关。ARP 协议在 SIM 实现中的作用只是触发节点 SSA 表的管理操作，以实现 SIM 与 TCP/IP 协议族的融合。

5.2.2　SIM 通信过程

参考 Linux 中 Netfilter 的框架，SIM 安全层与 TCP/IP 协议栈之间的结合关系通过 HOOK 机制实现。因为 Netfilter 框架中预设的 5 个 HOOK 都是在 IP 层中实现的，因而不能基于已有的 HOOK 实现 SIM，因而论文在 Linux 中的 IP 层与 MAC 层之间专门为 SIM 添加了 2 个 HOOK，如图 9 所示。

SIM_INPUT_HOOK：是 SIM 截获进入本机的 IP 报文的钩子点，其对应于钩子函数 decrypt_SIM()。

decrypt_SIM()：SIM 的接收数据处理函数，该

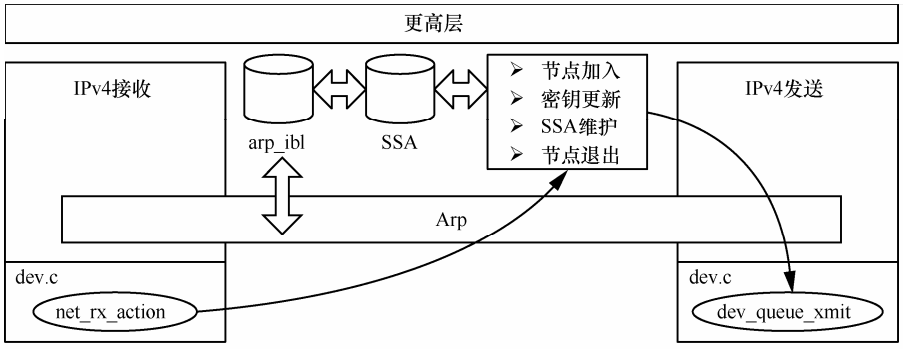


图 8　SIM 与 TCP/IP 的融合结构

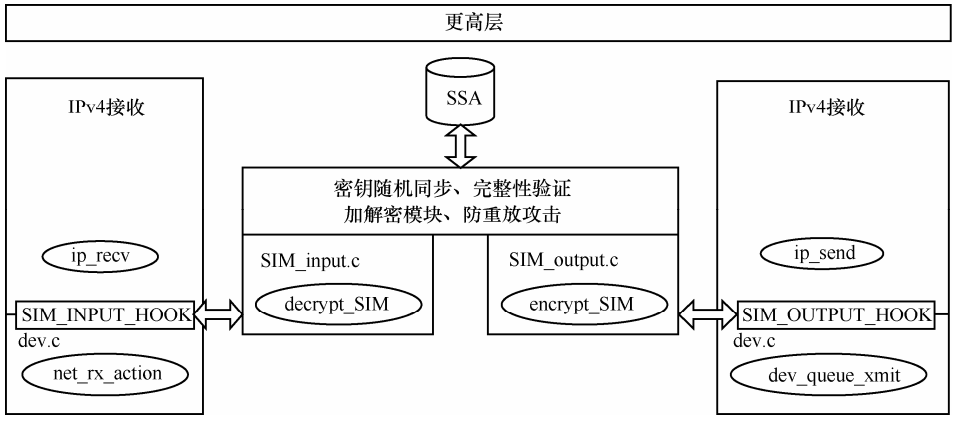


图 9　SIM 的 HOOK 实现机制

函数根据节点内部 SSA 表完成 SIM 接收数据的处理过程，然后再将处理后的数据分组提交给上层 IP 协议进行处理。

SIM_OUTPUT_HOOK：是 SIM 截获本机发送的 IP 报文的钩子点，其对应于钩子函数 encrypt_SIM()。

encrypt_SIM()：SIM 的发送数据处理函数，该函数根据节点内部 SSA 表完成 SIM 发送数据的处理过程，然后再将处理后的数据分组转交给下层 MAC 协议往外发送。

1) SIM 接收报文

net_rx_action()函数是网络数据从 MAC 层进入网络层的数据分组分发函数，它根据 MAC 帧中的协议类型字段将数据分组提交给对应的网络层处理函数（如：ip_rcv, arp_rcv 等）。SIM 安全协议的接收数据处理入口（SIM_INPUT_HOOK）将在该函数中实现。

net_rx_action()函数通过方法 skb_dequeue()从 CPU 输入队列中请求一个数据分组，作了相应的状态记录和更新之后，该数据分组被传递给在列表 ptype_all 中注册的所有协议（这些协议接收处理所有达到本机的数据分组），然后再根据 dev->protocol 指明的协议类型把数据分组提交给 ptype_base 中对应的协议处理函数（如：ip_rcv, arp_rcv 等）。

一般 Linux 内核协议栈中，列表 ptype_all 中没有注册任何协议，但是该接口特别适合于插入分析工具的使用（如：Linux 中透明网桥就是基于 ptype_all 实现的）。参考透明网桥的实现过程，SIM 报文接收过程的钩子点也在 net_rx_action()中实现，如图 10 所示。

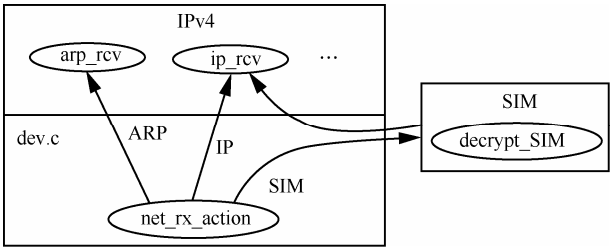


图 10　SIM_INPUT_HOOK 实现方案

net_rx_action()根据 MAC 层的协议类型字段判断到达的报文是不是 SIM 报文，若为 SIM 报文，则将该报文提交给 decrypt_SIM()进行处理。decryt_SIM()处理完成后，得到正常的 IP 报文，然后再提交给 ip_rcv()进行后续处理。

2) SIM 发送报文

类似于 SIM 接收报文的过程，SIM 的报文发送由 HOOK 机制在 dev_queue_xmit(skb)中实现。链路层以上的协议实例都使用 dev_queue_xmit(skb)并以套接字缓冲区 skb 的形式在网络设备上发送某一个数据分组。在 dev_queue_xmit(skb)中，套接字缓冲区 skb 被置于网络设备的输出队列中，然后触发对就绪状态的数据分组的进一步处理。

对 SIM_OUTPUT_HOOK，必须在 IP 数据分组进入网络设备输出队列之前转换为 SIM 的报文，并重新封装为 MAC 帧，然后才能添加到网络设备的输出队列中，如图 11 所示。

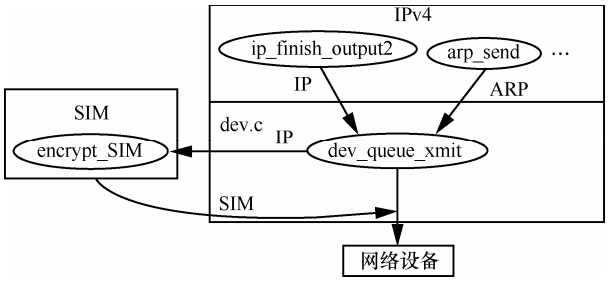


图 11　SIM_OUTPUT_HOOK 实现方案

dev_queue_xmit(skb)收到上层协议传来的报文后，判断是否为 IP 报文，若为 IP 报文，则将该报文转交给 encrypt_SIM()进行处理。encrypt_SIM()处理完成后得到对应的 SIM 报文，并将 SIM 报文重新封装为新的 MAC 帧，然后添加到网络设备的输出队列中。

6　实验结果

由于原型系统已上交有关部门，故本小节的实验结果为后期整理的结果。其中定性实验结论部分，是根据原型系统验收报告会时，验收测试报告中的记录整理而成。定量实验结论部分，是利用 NS3 网络模拟器编写模拟程序重新测试得到。

6.1　初始 SSA 建立时间

测量了初始 SSA 建立需要花费的时间，结果如图 12 所示。

从图 12 中可以看出，建立初始 SSA 所需要的时间基本在 350 ms 左右，相对于 AODV 路由协议网络发现过程大约需要十几秒来说，SSA 生成的时间开销是完全可以接受的，不会对网络性能造成任何可察觉到的影响。

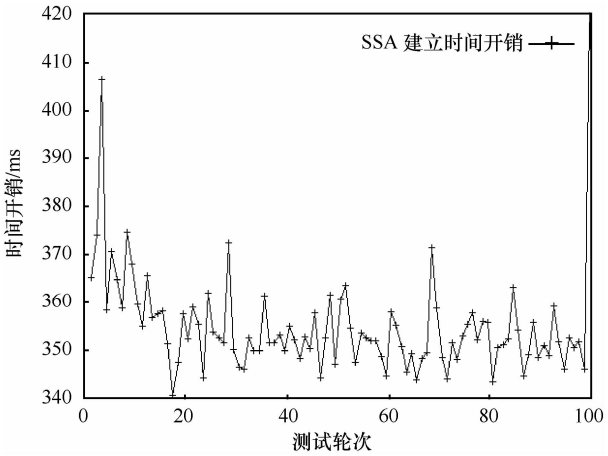


图 12　初始 SSA 建立时间

6.2　SSA 更新时间开销

测量了 SSA 更新所花费的时间，如图 13 所示。

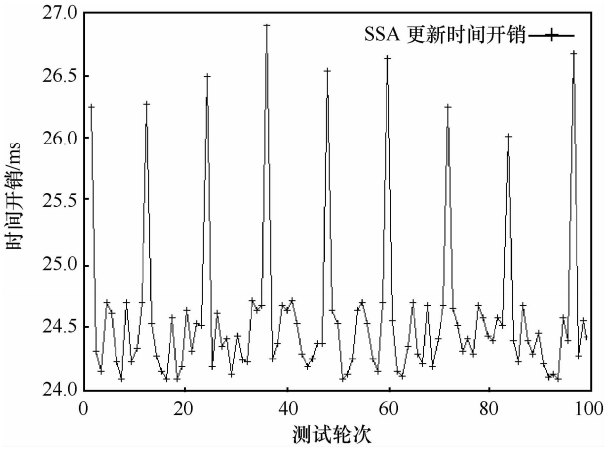


图 13　SSA 更新时间

SSA 更新的开销基本在 24.5 ms 左右，仅相当于数次报文传输时间，相对于大量的网络数据传输来说，这个 SSA 更新的时间开销是微不足道的。

6.3　报文收发额外时间开销

测量了 SIM 协议因对数据报文进行安全处理而带来的额外时间开销，结果如图 14 所示。

测试中分别设置了不同的报文长度，有效载荷部分的长度从 10 字节到 1 500 字节均匀变化。可以看出，随着报文载荷部分的增大，进行安全处理所需要的额外的时间也线性变化，处于可控范围内。而总的时间开销，最多的时候也没有超过 0.4 ms，平均在 0.2 ms 左右。这相对于 1 ms 以上的无线网 RTT 来说，是完全可以接受的。

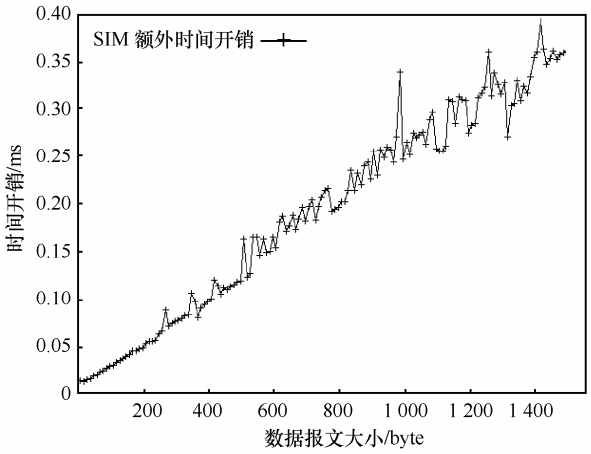


图 14　报文收发额外时间开销

6.4　抗重放攻击结果

进行了抗重放攻击的实验，实验网络拓扑如图 15 所示。其中 S 为服务提供者，提供 FTP、HTTP 等服务；C 为客户节点，向 S 申请服务；M 为攻击者，通过截获 C 的正常报文并重放，试图享受 S 提供的服务。测试的结果如表 1 所示。

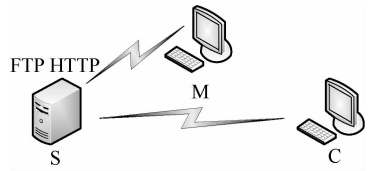


图 15　抗重放攻击实验网络拓扑

表 1　　抗重放攻击测试结果

攻击类型	攻击结果
FTP	成功检测并拦截
HTTP	成功检测并拦截
随机报文捕获与重放	检测拦截率 100%

原型系统成功检测出并拦截了全部的重放攻击报文。

6.5　抗 DOS 攻击结果

进行了抗 DOS 攻击实验，网络拓扑如图 16 所示。其中，S 为服务提供者，提供 FTP、HTTP、

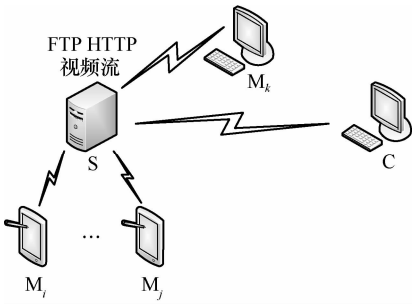


图 16　抗 DOS 攻击网络拓扑

视频点播等服务；C 为客户节点，向 S 申请服务；M_i、M_j、M_k 等为攻击者，对 S 发送大量恶意报文，并通过各种方式干扰 S 和 C 的通信，试图瘫痪 S 使其不能正常提供服务。测试的结果如表 2 所示。

表 2　　抗 DOS 攻击测试结果

服务类型	可用情况
FTP	可正常使用
HTTP	可正常使用
视频流比特率	基本不变

由于来自系统外部的攻击者的攻击报文不符合 SIM 报文格式要求，故被全部丢弃，根本没有进入到 MAC 层以上。从而攻击者的攻击除造成一定的无线电干扰效果外，对系统正常运行没有任何其他影响。

7　结束语

基于 5 节的设计方案，初步实现了 SIM 协议的原型系统，并编写了捕获数据分组进行重放攻击、DOS 攻击等测试程序，实验结果表明原型系统能抵抗此类攻击，并保持 MANET 的互联互通。但由于优化的不彻底，整体网络性能还不是很理想，仅能支持简单的视频传输应用，对于多路视频点播类应用尚不能提供很好的支持，下一步将有针对性地进行改进，并根据后续实验的结果，进一步对 SIM 协议性能进行优化。

参考文献：

[1] 胡华平,胡光明,董攀等.大规模移动自组网络安全技术综述[J].计算机研究与发展, 2007, 44(4): 545-552.
HU H P, HU G M, DONG P. Survey of security technology for large scale MANET[J]. Journal of Computer Research and Development, 2007, 44(4): 545-552.

[2] 刘永亮, 高文, 姚鸿勋等. Aydos 等基于椭圆曲线密码学无线认证协议的安全性[J]. 计算机研究与发展, 2006, 43(12):2076~2081.
LIU Y L, GAO W, YAO H, *et al*. Security on Aydos et al's elliptic curve cryptography based wireless authentication protocol[J]. Journal of Computer Research and Development, 2006, 43(12): 2076-2081.

[3] 冯涛, 王毅琳, 马建峰. 一种新的基于椭圆曲线密码体制的 Ad hoc 组密钥管理方案[J]. 电子学报, 2009, 37(5): 918-924.
FENG T, WANG Y, MA J. A new Ad Hoc group key agreement scheme based on ECC[J]. Acta Electronica Sinica, 2009, 37(5): 918-924.

[4] 李慧贤, 庞辽军, 王育民等. 适合 Ad Hoc 网络无需安全信道的密钥管理方案[J]. 通信学报, 2010, 31(1): 112-117.
LI H X, PANG L J, WANG Y M, *et al*. Key management scheme without secure channel for ad hoc networks[J]. Journal on Communications, 2010, 31(1): 112-117.

[5] 张串绒, 张玉清, 李发根等. 适于 Ad Hoc 网络安全通信的新签密算法[J]. 通信学报, 2010, 31(3): 19-24.
ZHANG C R, ZHANG Y Q, LI F G, *et al*. New signcryption algorithm for secure communication of ad hoc networks[J]. Journal on Communications, 2010, 31(3): 19-24.

[6] AHMAD M S, TADAKAMADLA S. Short paper: security evaluation of IEEE 802.11 w specification[A]. Proceedings of the Fourth ACM Conference on Wireless Network Security[C]. Hamburg, Germany, 2011. 53-58.

[7] 李小青, 李晖, 杨凯等. 一种基于 D-S 证据理论的 Ad Hoc 网络安全路由协议[J]. 计算机研究与发展, 2011, 48(8): 1406-1413.
LI X Q, LI H, YANG K, *et al*. A secure routing protocol based on D-S evidence theory in ad hoc networks[J]. Journal of Computer Research and Development, 2011, 48(8): 1406-1413.

[8] 付颖芳, 张兴, 张婷等. 无线 mesh 网络中的虫洞攻击检测研究[J]. 通信学报, 2011, 32(1): 59-65.
FU Y F, ZHANG X, ZHANG T, *et al*. Research on wormhole attacks in wireless mesh networks[J]. Journal on Communications, 2011, 32(1): 59-65.

[9] SHU T, KRUNZ M. Detection of malicious packet dropping in wireless ad hoc networks based on privacy-preserving public auditing[A]. Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks[C]. Tucson, Arizona, USA, 2012.87-98.

[10] 刘方斌, 张琨, 李海等. 无可信中心的门限追踪 Ad Hoc 网络匿名认证[J]. 通信学报, 2012, 33(8): 208-213.
LIU F B, ZHANG K, LI H, *et al*. Threshold traceability anonymous authentication scheme without trusted center for Ad Hoc network[J]. Journal on Communications, 2012, 33(8): 208-213.

[11] 韩磊, 刘吉强, 韩臻等. 移动 Ad Hoc 网络预分配非对称密钥管理方案[J]. 通信学报, 2012, 33(10): 26-34.
HAN L, LIU J Q, HAN Z, *et al*. Pre-distribution asymmetric key management scheme for mobile ad hoc networks[J]. Journal on Communications, 2012, 33(10): 26-34.

[12] 吴呈邑, 熊焰, 黄文超等. 移动自组网中基于动态第三方的可信公平非抵赖协议[J].电子学报, 2013, 41(2): 227-232.
WU C Y, XIONG Y, HUANG W C, *et al*. A trusted fair non-repudiation protocol based on dynamic third party in mobile Ad Hoc networks[J]. Acta Electronica Sinica, 2013, 41(2): 227-232.

[13] Kent S, Atkinson R. RFC2406: IP encapsulating security payload (EsP) [EB/OL]. http://www.rfc-editor.org/rfc/rfc2406.txt.

[14] Kent S, Atkinson R. RFC 2402: IP authentication header[EB/OL]. http://www.rfc-editor.org/rfc/rfc2402.txt.

[15] Harkins D, Carrel D. RFC 2409: The internet key exchange (IKE) [EB/OL]. http://www.rfc-editor.org/rfc/rfc2409.txt.

[16] Kaufman C. RFC 4306: internet key exchange (IKEv2) protocol[EB/OL]. http://www.rfc-editor.org/rfc/rfc4306.txt.

作者简介：

李荣森（1982-），男，河南舞阳人，国防科学技术大学博士生，主要研究方向为无线网络安全。

窦文华（1946-），男，山西运城人，国防科学技术大学教授、博士生导师，主要研究方向为计算机网络、信息安全。