学术论文

基于多跳双向认证的 802.16 Mesh 网络 SA 管理机制

王兴建，胡爱群，黄玉划
（东南大学信息安全研究中心，南京 210096）

[摘要] IEEE802.16－2004 无线城域网（wireless－MAN）标准支持的多跳（Mesh）网络是一种树状网络和 ad hoc 网络结合的新型网络。针对 Mesh 中使用的单跳单向认证 SA（安全关联）管理机制安全和效率上的缺陷，提出了一种和次优修正路由结合的多跳双向认证 SA 管理机制。与单跳单向机制相比，该机制是前向安全的，对中间节点的攻击具有强安全性，同时减少了系统开销和传输时延。在按需路由建立前使用修正路由传递管理信息可减少服务流建立时延。安全性分析证明了多跳双向机制的安全性，性能比较说明了在效率上的优势。

[关键词] IEEE802.16；Mesh；节点；多跳双向认证；修正路由
[中图分类号] TP915.08 [文献标识码] A [文章编号] 1009－1742（2006）09－0069－05

1 引言

无线局域网（WLAN）的设计特点不适用于室外的宽带无线接入（BWA），IEEE802.16 工作组相继制定了 802.16 和 802.16a 无线城域网标准。2004 年 10 月这 2 个标准融合增补成为统一的 802.16－2004 标准[1]。802.16－2004 标准同时在物理层解决室外射频传输和在 MAC 层实现 QoS，提供接入节点（SS/Node）和服务基站（BS）之间或节点（Node）间的宽带无线连接。802.16－2004 采用 2 种布网模式：PMP（点对多点）和 Mesh（多跳）网络。PMP 网络采用星形布局，各节点使用带宽调度直接与基站通信；Mesh 网络则是一种基于多跳路由、级联/对等并存的新型网络结构。Mesh 网络采用集中式和分布式调度并行的方式工作。集中式调度采用上限为 3 跳的调度树结构，调度树由 BS 定时在网内广播。各节点由父节点多跳中继，由 BS 统一转发。分布式调度采用 ad hoc 方式，各节点（包括 BS）关系对等，每个节点保持一个邻节点列表，形成自己的邻域。节点间通信按路由多跳转发[1]。集中式和分布式在带宽调度上隔离，为便于分析，将 Mesh 网络看作一个级联的树状网（见图 1）和一个 ad hoc 网（见图 2）的重合。

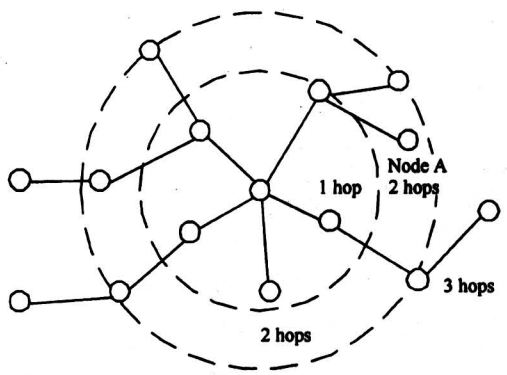

图 1 集中式级联树状网

Fig.1 Centralized concatenation tree network

2 Mesh 网络单跳单向认证 SA 管理机制和存在的缺陷

2.1 Mesh 网络单跳单向认证 SA 管理机制

Mesh 网络中节点入网后使用授权机制获得共

[收稿日期] 2005－05－25；修回日期 2005－07－22
[基金项目] “八六三”高技术研究发展计划资助项目（2003AA143040）；江苏省网络与信息安全实验室资助项目（BM2003201）
[作者简介] 王兴建（1978－），男，南京市人，东南大学博士生，研究方向无线网络安全和 QoS

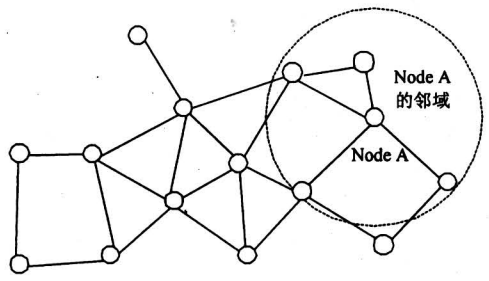

图2 分布式 ad hoc 网

Fig.2 Distributed ad hoc network

享秘密（OSS），OSS 为全网已授权节点共有并不断更新。节点使用 OSS 导出的 HMAC 摘要密钥（HMAC_KEY_S）互相验证。Mesh 安全管理采用单跳（直接相连）节点间的密钥管理协议（PKM），且只在单跳间实现。节点在自己的邻域内对每个邻节点的每个服务流建立和保持一一绑定的安全关联（SA），管理流加密密钥（TEK）的获取和更新。SA 由 SAID 标识和 TEK 参数构成，一个 SA 对应两套不断更新的 TEK 参数，TEK 参数由已加密的 TEK，TEK 剩余生命期，TEK 序列号，CBC 初始向量构成。TEK 用于加密 2 个单跳节点间的某个特定服务流数据，TEK 的管理是 SA 的核心，也是 Mesh 网络安全的关键。

SA 管理机制采用基于 ITU－T X.509 V3 证书[2]的单向认证方式获得 TEK。802.16 单跳单向认证的 TEK 分配机制如下式所示：

1）发起节点 Node_1→目标节点 Node_2：(KEY－REQ)，SEQ_{PKM} | SS $Cert_{Node\_1}$ | SAID | HMAC SHA－1 digest (with HMAC_KEY_S)；

2）Node_2→Node_1：(KEY－REPLY)，SEQ_{PKM} | SEQ_{OSS} | SAID | old TEKparam | new TEK param | HMAC SHA－1 digest (1)

"|"表示信息间串联。SEQ_{PKM}是一次 PKM 信息交互的标识以防重放。笔者提及的证书均为 X.509V3 证书[2]，KEY－REQ，KEY－REPLY 为 802.16 定义的管理信息。SS 证书由制造商 CA 签发，制造商 CA 证书则由节点软件支持。另外 802.16 使用的 SS 证书扩展数据域中包括了 MAC 地址[1]，因此 SS 证书是与 MAC 地址绑定的，即 Cert↔Macaddr。目标节点 Node_2 收到发起节点 Node_1 发来的 SS 证书后，用 Node_1 制造商 CA 证书内附的 RSA 公钥 CA RSA pub-key[3]验证 Node_1 SS 证书尾部的 CA 签名。证书和身份验证通过之后 Node_2 生成 TEK，用 Node_1 的 SS 证书内附的 RSA 公钥 SS RSA pub-key 加密 TEK 并发回 Node_1。

2.2 单跳单向认证 SA 管理机制的缺陷

文献[4]中指出，在 PMP 模式下使用单向认证是不安全的，并建议使用双向认证。另一方面，Mesh 采用单跳节点间 SA，使得每个节点只需管理与相邻节点间的 SA 的同时，也带来了不可避免的安全漏洞。一个节点 Node_*S* 与同网内的另一非邻节点 Node_*D*（BS 或其他节点）通信时，必须通过其他中间节点中继。因为 SA 只能在一跳内实现，所以 Node_*S* 的数据在各中继节点都要解密成明文，再用此中继节点向下一跳中继节点申请的 TEK 加密后传向下一跳（见图 3）。

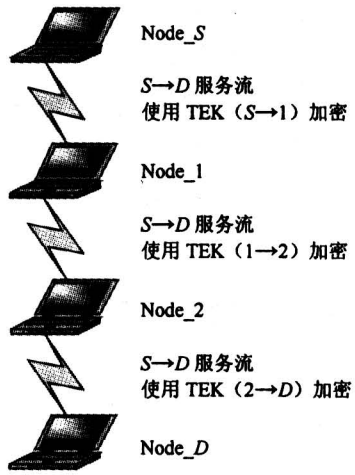

图3 单跳服务流中继示意图

Fig.3 One-hop service-flow relay sketch map

这样就带来 2 个问题：

1）中继的服务流数据安全无法保障。每个中间节点实际转发的是 Node_*S* 发送的明文，中间节点可以任意的修改，伪造和重放中继数据而不被发现。即使中间节点不作任何攻击，也可知道 Node_*S* 的隐私信息明文，这从数据的私密性来说是不可接受的。

2）服务流中继开销太大。为了建立一条数据通道需要建立和维护路由各节点间的多个 SA，Node_*S* 的数据在各中继节点都要解/加密各做一次，这需要使用很多带宽和系统资源并带来时延。另外，每次 TEK 分配都重复验证同样的证书也是不必要的。

3　与次优修正路由结合的多跳双向认证 SA 管理机制

针对 Mesh 单跳单向认证 SA 管理机制安全和性能的缺陷，提出了一种与次优修正路由结合的多跳节点间的双向认证 SA 管理机制。此机制仅在通信的 2 个节点间建立一个基于双向认证的 SA，而不是在每跳间实现一个 SA；TEK 分配机制在发起节点和目标节点间实现，由中间节点转发，具有前向安全性并对中间节点攻击有强安全性；在 SA 建立后中间节点只负责中继密文而无需加/解密，且无法解出明文。该机制与一种次优的修正路由结合，可将路由建立和初期 TEK 分配同时进行以减少服务流建立时延。

3.1　使用多跳双向认证的 TEK 分配机制

TEK 的分配是一个动态更新的过程。为了提高安全性和效率，将 TEK 分配分为初始化分配（第一次 TEK 分配）和一般分配（其余的 TEK 分配）。

1）初始化 TEK 分配：

发起节点 Node_ S→中间节点(0 ~ N 个)→目标节点 Node_ D:(KEY_REQ), SEQ_{PKM} | SS $Cert_{Node\_S}$ | SAID | HMAC digest | sig_{Node_S};

目标节点 Node_ D →中间节点→发起节点 Node_ S: (KEY - REPLY), SEQ_{PKM} | SEQ_{OSS} | SAID | old TEKparam | new TEK param | $MACaddr_{Node\_S}$ | SS $Cert_{Node\_D}$ | HMAC digest | sig_{Node_D}　　(2)

2）一般 TEK 分配：

发起节点 Node_ S→中间节点→目标节点 Node_ D: (KEY - REQ), SEQ_{PKM} | SAID | HMAC digest | Sig_{Node_S} Node_ D →中间节点→Node_ S: (KEY - REPLY), SEQ_{PKM} | SEQ_{OSS} | SAID | old TEKparam | new TEK param | $MACaddr_{Node\_S}$ | HMAC digest | Sig_{Node_D}　　(3)

Sig 是节点使用自己 SS 证书中 RSA 公钥对应的私钥对信息所做的签名，以保证信息内容不被修改。式（2）中如无中间节点时双方直接通信，否则发起节点 Node_ S 将 KEY - REQ 按路由转发给中间节点，中间节点以 UDP 隧道方式[1]多跳中继发往目标节点 Node_ D，Node_ D 验证 Node_ S 证书和签名后储存 Node_ S 的 RSA 公钥，将附有 TEK 参数的 KEY - REPLY 原文原路返回（不使用 UDP 隧道方式）。Node_ S 收到后验证 Node_ D 证书和签名并储存 Node_ D 的 RSA 公钥。在式（3）中节点证书不再使用，双方使用储存的对方公钥校验对方签名来鉴别对方身份。SA 建立后服务流中继传输见图 4，将 TEK 分配流程嵌入 802.16 的 SDL 流程图，见图 5 和图 6。

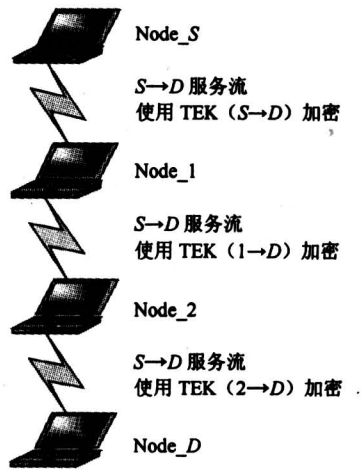

图 4　多跳服务流中继示意图

Fig.4　Multi-hops service-flow relay sketch map

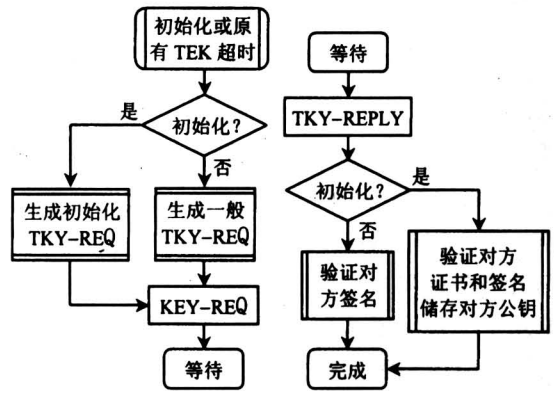

图 5　发起节点 TEK 分配 SDL 流程

Fig.5　Source-node TEK distribution SDL flow map

3.2　路由建立前 TEK 分配的修正路由方案

尽管 802.16 - 2004 标准尚未决定使用何种路由协议，但目前提出的 ad hoc 路由协议大多采用按需路由方式，最具有代表性的是 AODV 和 DSR。按需路由协议使用类似洪泛的方式以一定时延的代价获得路由。单跳单向认证 TEK 管理中各中间节点间 SA 的建立和初始化 TEK 分配由节点间服务流建立请求触发，必须在路由建立之后进行，建立路由和建立 SA 的时间相加会对服务流传输造成较大的时延。多跳双向认证机制只需在通信节点间建立

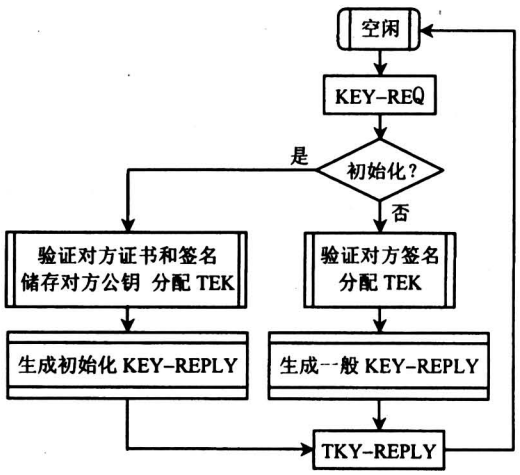

图6 目标节点 TEK 分配 SDL 流程

Fig.6 Destination node TEK distribution SDL flow map

SA，可将按需路由和开始的一个或多个 TEK 分配同时进行以减少时延。如将 TEK 分配和按需路由信息绑定实现，路由的洪泛方式会造成带宽浪费，一种解决方法是在寻找路由的同时使 TEK 管理信息沿一条次优的修正路由传输。

修正路由算法如下：TEK 分配开始时，路径上的每一节点（包括发起节点 Node_ S）先判断按需路由是否存在，存在则使用按需路由转发，否则先选中由 Mesh 网集中式调度树决定的与目标节点 Node_ D 之间的一条集中式路径作为基本的调度树路由，再将调度树路由中距自己大于一跳的节点与自己的邻节点列表比较，如找出有节点在列表内，则修正下一跳为调度树路由中跳数最大的邻节点，否则仍按调度树路由转发。下一跳节点收到后继续作同样判断以不断修正路由并按修正的路由转发（见图7）。

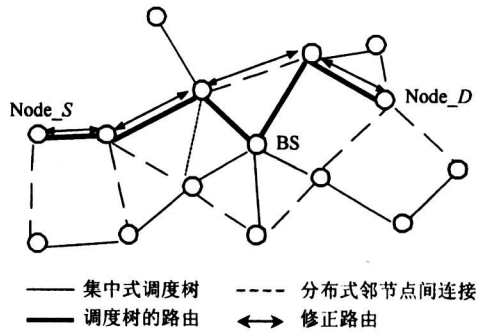

图7 无按需路由时 TEK 分配修正路由

Fig.7 TEK distribution corrected routingwithout on demand routings

此方案作为按需路由建立前的临时解决方案，在按需路由建立之后，TEK 分配仍旧按按需路由进行。值得注意的是，此方案也可用作 Mesh 网按需路由建立前少量数据传输的一个替代方案。

4 使用多跳双向认证的 TEK 分配机制安全性和性能分析

4.1 BAN 逻辑形式化证明

对安全性的讨论仅限于协议机制，可假设算法是安全的。多跳双向认证中将 TEK 分配过程分为式（2）初始化分配和式（3）一般分配2步。在式（3）中双方已验证过对方证书，并使用式（2）中储存的对方公钥对对方签名校验，因此式（3）是前向安全的，其安全性依赖于式（2）。这样安全的实现是基于式（2）中 Node_ S 收到的 KEY - REPLY 响应的可信性上。BAN 是由 Burrows，Abadi，Needham 于 1989 年提出的一种基于信念的模态逻辑[5]。这一逻辑的目的是在抽象层次上分析分布式网络的安全，使可信的参与者可以相信是在彼此（而不是入侵者）通信。证明的目的是双方建立一个可信任的 TEK，可表述为 $S \mid \equiv$ TEK 和 $S \mid \equiv D \mid \equiv$ TEK。协议可知有 $S \lhd \{\text{TEK}\}_{\text{Pub\_key}(S)}$。

从式（2）中 AUTH - REPLY 返回 $\text{Cert}_{\text{Node\_}D}$ 和 $\text{Sig}_{\text{Node\_}D}$，以及 $\text{Cert}_{\text{Node\_}D} \leftrightarrow \text{Macaddr}_{\text{Node\_}D}$，Node_ S 可确定 REPLY 信息及其中 TEK 确为 Node_ D 发出 $S \mid \equiv D \Rightarrow$ REPLY，$S \mid \equiv D \Rightarrow$ TEK。

根据 Node_ D 返回 $\text{MACaddr}_{\text{Node\_}S}$ 以及 $S \mid \equiv D \Rightarrow$ REPLY，Node_ S 可知 Node_ D 已收到 $\text{Cert}_{\text{Node\_}S}$ 和其中的 $\text{pub-key}(S)$：$S \mid \equiv D \xleftrightarrow{\text{pub-key}(S)} S$。

由于双方信息都使用了 SEQ_{PKM} 并签名，保证了信息的“新鲜”，得 $S \mid \equiv \#$（TEK）。

按消息含义规则[5]：

$$S \lhd \{\text{TEK}\}_{\text{Pub\_key}(S)},\ S \mid \equiv D \xleftrightarrow{\text{pub-key}(S)} S$$

$$S/S \mid \equiv D \mid \sim \text{TEK}。$$

按即时确认规则[5]：

$$S \mid \equiv D \mid \sim \text{TEK},\ S \mid \equiv \#(\text{TEK})/S \mid \equiv D \mid \equiv \text{TEK} \tag{4}$$

按信任控制规则[5]：

$$S \mid \equiv D \mid \equiv \text{TEK},\ S \mid \equiv D \Rightarrow \text{TEK}/\ S \mid \equiv \text{TEK} \tag{5}$$

由式（4）和式（5）可知双方建立了一个可信任的 TEK。

4.2 多跳双向认证的 TEK 分配机制性能分析

多跳双向认证的 TEK 分配使用单个 SA 取代多跳间的多个 SA，减少了大量服务流加解密的次数和 SA/TEK 管理的开销；在初次交换后不再发送证书，使用带宽和验证证书的开销也大为减少；使用修正路由和减少加解密的次数也减少了服务流建立和传输的时延。

表 1　TEK 分配机制性能比较

Table 1　TEK distribution characteristics comparison

	单跳单向认证	多跳双向认证
服务流建立时延	$T_R + 2NT_N + 2NT_p$	$\max(T_R, 2MT_N + 2MT_p)$
数据传输时延	$N(T_N + T_{en} + T_{den})$	$NT_N + T_{en} + T_{den}$
数据加/解密次数	N	1
使用 SA/TEK 数	N	1

T_R—按需路由建立时间，T_N—单跳节点间平均网络延时，T_p—节点建立 SA 延时，T_{en}—节点加密时延，T_{den}—节点解密时延，N—路由跳数，M—修正路由跳数（$M \geq N$）

5　结论

对 802.16 - 2004 Mesh 网络的单跳单向 SA 机制进行分析，指出了在安全和效率上存在的缺陷，并提出一种和修正路由结合的多跳双向 SA 机制以提高效率，实现对中间节点的强安全性，并是前向安全的。安全性分析证明了此机制的安全性，性能分析给出了此机制效率上的优势。多跳双向 SA 机制针对 802.16 - 2004 Mesh 网络提出，可简单的嵌入 802.16 协议，具有一定的实用价值。除此之外，对中间节点的强安全性使得 TEK 分配机制可使用在 ad hoc 网中以提供通过不可靠节点的通信，修正路由也可作为 Mesh 网在按需路由建立前一种次优的临时路由方式。

参考文献

[1] IEEE LAN/MAN Standard Committee. IEEE Std 802.16TM - 2004 IEEE Standard for Local and Metropolitan Area Networks Part 16 [S]. IEEE LAN/MAN Standard Committee, 2004

[2] Chokhani S, Ford W, Sabett R. Internet X.509 Public Key Infrastructure Certif-icate Policy and Certification Practices Framework, RFC3647 [EB/OL]. http:// www.rfc-editor.org, 2003

[3] RSA Laboratories RSA Cryptography Standard. RSA Public Key Cryptography Standard # 1 Vol 2.0 [DB/OL]. http:// www. rsasecurity. com/rsalabs/pkcs/pkcs-1/, Oct 1998

[4] Johnston D, Walker J. Overview of IEEE 802.16 security [J]. IEEE Security & Privacy Magazine, 2004, 2(3): 40 ~ 48

[5] Abadi M , Burrows M , Needham M. A logic of authentication [J]. ACM Transactions on Computer Systems, 1990, 8(1): 18 ~ 36

IEEE 802.16 Mesh Network SA Management Mechanism Based on Multi-hops Mutual Authentication

Wang Xingjian, Hu Aiqun, Huang Yuhua

(*Research Center of Information Security, Southeast University, Nanjing* 210096, *China*)

[**Abstract**] Mesh network supported by IEEE802.16-2004 wireless-MAN standard is a fresh network combining tree network and ad hoc network. Aimed at the weakness both in security and efficiency of one-hop one-way authentication SA (security association) mechanism employed by Mesh network, an multi-hops mutual authentication SA mechanism associated with hypo- optimal self-modified routing is proposed. Compared with the one-hop one-way mechanism, this one is of forward security and immune to middle attacks, which also lessens system cost and time delay in transmission. The employment of self-modified routing before routing establishment in management information transaction can also reduce the delay of service-flow creation. Subsequently, the security of multi-hops mutual mechanism is proved by security analysis, followed by the efficiency comparison which introduces the efficiency advantage of this mechanism.

[**Key words**] IEEE 802.16; mesh; node; multi-hops mutual authentication; self-modified routing