无线 Mesh 网络中安全路由协议的研究

宋志贤,喻继燊,肖明波*
(厦门大学信息科学与技术学院,福建 厦门 361005)

摘要: 无线 Mesh 网作为一种新型的无线通信网络,能在更大的覆盖范围内提供高的速率. 本文旨在提出一种高效、安全的 Mesh 网路由机制,保证网络正常工作. 首先介绍其安全需求,随后分析了一种无线 Ad hoc 网络中的 ARAN 鉴别路由协议,最后提出了一种全新的基于 ARAN 协议鉴别思想并且适用于无线 Mesh 网络的 ARWMN 安全路由协议,并对其安全性能进行了分析,其安全性与收敛速度能较好地满足网络需求.

关键词: WMN;无线 Ad hoc 网络;安全路由;ARAN 协议
中图分类号: TP 393.04 **文献标识码**: A **文章编号**: 0438-0479(2008)06-0823-05

无线 Mesh 网络(Wireless Mesh network, WMN)[1],作为一种新型的无线通信网络,有着自组织性、自愈性、频谱效率高、覆盖范围大、可扩展性强、可靠性强等众多优势,能在更大的覆盖范围内提供高的速率,成为下一代无线通信网络研究的热点之一. 但是 WMN 容易受到安全攻击,比如受到窃听、伪造、拒绝服务等,其安全目标与传统有线网络中的安全目标是一致的:可用性、机密性、完整性、安全认证和抗抵赖性. Mesh 路由协议基本沿用 Ad hoc 网络路由协议,但需要针对 WMN 的特点设计专门适用于 WMN 的安全、高效路由协议. 本文对 Ad hoc 网络的鉴别路由 ARAN (Authenticated routing for Ad hoc networks)[2]协议进行简单的阐述. 根据 ARAN 的鉴别思想,提出在一个 WMN 下可实现的基于对称密钥体制的鉴别安全路由协议 ——ARWMN (Authenticated routing for wireless Mesh network)[3],对 ARWMN 进行了安全的理论分析,然后对 DSR[3]、ARAN 和 ARWMN 三种路由协议进行了仿真比较.

1 WMN 网络安全

1.1 安全挑战

WMN 与传统意义上的移动 Ad hoc 网络结构有一定的差异. 一般来说,WMN 有客户节点、路由节点和网关节点组成. 根据网络的具体配置的不同,WMN 不一定包含以上所有类型节点. WMN 具有自愈性、多跳、非视距连接、组网方便、支持多种网络接入等特点[3]. 正是由于这些特性使得它面临许多挑战[4]:

(1) 用无线信道导致自组网容易受到诸如被动窃听、主动入侵、信息阻塞、信息假冒等方式的攻击.

(2) 由于节点的 CPU 的计算能力较低,无法实现复杂的加密算法,这增加了被窃密的可能性.

(3) 当路由节点放在室外时,由于缺乏足够的保护,很有可能被占领. 因此,恶意的攻击不仅来自自组网之外,而且可能从网内产生.

(4) 由于 WMN 的扩展性,自组网的拓扑结构和成员处于动态变化中. 节点间的信任关系也不断变化. 只具有静态配置的安全方案在自组网中是不可行的.

1.2 安全目标

WMN 的安全目标与传统有线网络中的安全目标是一致的,它们包括:可用性、机密性、完整性、安全认证和抗抵赖性[5].

可用性指受到攻击如拒绝服务攻击,节点仍然能够提供有效的服务. 对于终端节点,可用性还涉及到电源问题. 设计时,通常让主机在空闲时处于睡眠状态,必要时将其唤醒. 攻击者可以通过合法方式与节点交互,目的就是为了消耗节点的有限电池能源.

机密性是保证特定的信息不会泄露给未经授权的个体. 路由信息在有些情况下也必须保密,因为这些信息可能被敌方所利用.

可用性保证信息在发送过程中不会被中断. 如果没有完整性,在网络中的恶意攻击或无线信道干扰都可能使信息发送中断.

安全认证使每个节点能够确认与之通信的节点身份. 如果没有认证,敌方将很容易冒充某一节点,从而得以获取重要的资源和信息,并干扰其他节点.

抗抵赖性确保每条信息的发出节点不能否认已经

收稿日期:2008-03-21
基金项目:福建省自然科学基金(A0710022)资助
*通讯作者:mingbo @xmu.edu.cn

发出该信息.

2 一种全新的 WMN 安全路由协议

2.1 ARAN 鉴别路由协议

ARAN 协议为 Ad hoc 网络提供了身份鉴别、信息完整性和不可抵赖性等安全保证. 该协议通过可信任认证服务器,为所有有效节点颁发证书,将节点地址与其公钥及证书有效期绑定. ARAN 协议的特点在于:路由包信息中无路由跳数计数或源路由信息,它包括证书申请、路由查找、路由维护及证书吊销等.

ARAN 在无线 Ad hoc 网络中使用中有如下的问题:发起点必须在路由请求包中添加当前时间标记 t,对网络中的时钟同步有较高要求;不能有效地阻止内部恶意节点的攻击;ARAN 增加了对节点存储量的要求;算法复杂度高;需有一台证书服务器.

2.2 ARWMN 安全路由协议

ARAN 没有为 WMN 的路由特性进行优化. 对于 WMN,节点的 CPU、内存和带宽等资源相对比较短缺,公钥加密技术并不理想. 本文提出了一种专门针对 WMN 的安全路由协议 ARWMN,它借鉴 ARAN 鉴别路由的设计思想,使用能够快速计算的对称密码体制作为其核心安全算法,避免了算法复杂度问题. 不但能实现路由信息的鉴别、消息完整性以及不可抵赖性,也可以有效地实现 WMN 路由安全需求:即路由信令不能被欺骗;伪造的路由消息不能被注入网络;路由消息在传输过程中不能改变,除非是根据路由协议的正常功能进行的;不能因恶意行为导致路由环路;不能因恶意行为形成最短路径使路由重定向;非授权的节点应被排除在路由计算和查找之外.

2.2.1 使用环境与条件假设

WMN 中,我们关心的是如何为终端用户提供 Internet 网的接入服务,所以在 ARWMN 协议中,只讨论在 WMN 的骨干网中如何建立无线 Mesh 路由器(Wireless Mesh route,WMR)到因特网网关的安全路由通道. 假设唯一网关服务器 T 已经与每个 WMR 节点 A、B ··都各自拥有共同的对称密钥:K_A,K_B,…,而 WMR 节点相互不知道彼此密钥. 所有的路由节点和网关 T 都拥有共同的密钥 K_P,用来加密公共消息,防止外来节点探听 WMN 的内部路由信息.

2.2.2 路由查找

(1) 初始路由查找

假设 A →T 途径的节点中都不包含到网关 T 的路由信息,则路由查找过程为:节点 A 开始查找至网关 T 的路由,向它的近邻广播一条路由查找分组 RREQ,定义如下:

$$A \rightarrow broadcast: [REQ, IV_A, t, IP_A, [REQ, IV_A, t, IP_A]_{K_A}]_{K_P}$$

路由查找分组 RREQ 包括分组类型标识 REQ、路由查找标识值 IV_A,时戳 t,源节点 A 的 IP 标识 IP_A 以及利用源节点 A 的密钥 K_A 计算的 RREQ 的签名.

其中称"REQ, IV_A, t, IP_A"为 IP 链;称"$[REQ, IV_A, t, IP_A]_{K_A}$"为 RREQ 签名包.

每次源节点 A 执行路由查找时,均单调增加该路由查找标识值,以标识路由查找的新鲜性,而其他节点需为该节点存储最新的路由查找标识和时戳. 若在两个不同时戳的有效分组中,出现了相同的路由查找标识,则表示该标识值溢出后出现翻转.

一个节点接收到 RREQ 消息后,记录其上游节点建立至源的反向路径,以便收到应答消息能转发回源. 该节点利用 K_P 解开加密包,验证是否存在自身 IP 信息,若存在则丢弃该 RREQ,否则再验证(IV_A, IP_A)对的新鲜性. 若该节点以前处理过此数据对,则丢弃该 RREQ,否则,该节点附加自己的 IP 标识到 IP 链后面,再对 RREQ 签名包加上自己的 IP 标识并进行签名,使用 K_P 加密后广播转发给它的近邻.

假设 B 为收到 A 的 RREQ 广播的近邻节点,则 B 转发的广播如下:

$$B \rightarrow broadcast: [REQ, IV_A, t, IP_A, IP_B, [[REQ, IV_A, t, IP_A]_{K_A}, IP_B]_{K_B}]_{K_P}$$

以此类推,假设 C 收到 B 的广播信息,则:

$$C \rightarrow broadcast: [REQ, IV_A, t, IP_A, IP_B, IP_C, [[[REQ, IV_A, t, IP_A]_{K_A}, IP_B]_{K_B}, IP_C]_{K_C}]_{K_P}$$

即,路径上的每个节点重复此步骤:

●验证是否存在自身 IP 信息,若存在则丢弃该消息;

●验证(IV_A, IP_A)对的新鲜性,若存在则丢弃该消息;

●使用 K_P 对上游节点的 RREQ 包解密;

●加入自身的 IP 标识到 IP 链后面;

●使用自身的密钥对 RREQ 签名包和自身的 IP 标识进行签名;

●记录上游节点的 IP 地址;

●使用 K_P 加密;

●继而转发广播此消息;

●直至到达网关 T 为止.

(2) 网关的路由应答

网关 T 收到 RREQ 消息时,进行如下操作:

●验证(IV_A, IP_A)对的新鲜性;

●根据 IP 链,对 RREQ 签名包进行逐级解密,并

验证其 IP 标识是否相同;

●若某个 IP 标识信息错误,则记录下其 IP 标识并进入纠错程序,否则下一步;

●若逐级解密都完成后,获得的 与 IP 链的头文件不符,则记录下最初的 IP 标识并进入到纠错程序,否则进入下一步;

●记录下 IP 链;

●向 IP 链的最末 IP 发送 RREP 消息.

假设 T 收到了一个 A →B →C →T 的 RREQ 消息,并通过了校验,则单播给节点 C 一个的 RREP 消息,其内容为:

$T \rightarrow C: [REP, IV_A, t, RA_A [[[REP, IV_A, t, IP_B]_{K_A}, IP_C]_{K_B}, IP_T]_{K_C}]_{K_P}$

其中路由授权 $RA_A = [IV_A]_{K_T}$ 是对应路由查找标识为 IV_A 的 IP 链信息的授权标识,是用来进行路由信息授权时使用的. RA_A 只是用来标识路由的有效性,若有效路由链外节点伪造 RA_A,并未能起到攻击作用,路由链各节点已知其前向转发节点. 若有效路由内节点伪造 RA_A,将导致路由失效.

(3) 应答消息的处理

当一个节点接收到 RREP 消息后,记录其上游节点以便验证 RREP 消息的真伪. 该节点利用 K_P 解开加密包,验证是否之前处理过该 IV_A 的 RREQ 消息,若不存在此 IV_A,则丢弃该 RREP 消息;否则,该节点利用自身的密钥解密时戳 t 后面的 RREP 签名包,验证解密出来的 IP 数据是否为之前记录的前趋节点的 IP,若不是则丢弃该消息;否则认为该信息有效.

确认一个有效信息后,根据时戳 t 将之前记录的上游节点 IP 更新为到网关 T 的路由信息并记录下其路由授权 RA_A. 随后将解密出来的下一级 RREP 签名包加上 RREP 的头信息"REP, IV_A, t, RA_A"并使用 K_P 加密后单播给它之前记录的相应 IV_A 的上游节点.

例如当节点 C 收到 T 单播给自己的 RREP 消息,确认了其有效性后,记录下到网关的路由信息,然后单播给上游节点 B 一个 RREP 消息,其内容为:

$C \rightarrow B: [REP, IV_A, t, RA_A, [[REP, IV_A, t, IP_B]_{K_A}, IP_C]_{K_B}]_{K_P}$

以此类推,直到最终节点 A 收到了 RREP 消息,验证了其 IV_A 和前趋节点 IP_B,将其前趋节点 IP_B 根据时戳 t 更新到自己的路由信息里.

(4) 已有路由信息下的查找

上面论述的路由查找是建立在初期各个节点均无路由信息的情况下,当建立起一定的路由信息表后,后来的节点可以利用已经建立好的路由表,加快自身的路由表的建立. 由于各个节点之间并没有相互信任的机制,已有路由信息的节点想要将自身的路由信息共享给别的节点,需要到网关服务器上下载相应的授权.

一个已建立路由表的节点 S 收到 RREQ 消息,内容为:

$RREQ_{A,B} = [REQ, IV_A, t, IP_A, IP_B, [[REQ, IV_A, t, IP_A]_{K_A}, IP_B]_{K_B}]_{K_P}$

首先 S 先验证自身到网关 T 的下一跳 IP 是否在 IP 链内,若存在,则丢弃这条消息,否则由于节点 S 已经拥有了到网关 T 的路由授权 RA_S,所以 S 可以根据路由信息直接发送一个路由信息授权请求 RIAR (Route information accredited request):

$S \rightarrow T: RIAR_{S|A,B} = [RIAR, IV_A, t, IP_S, RA_S, [RREQ_{A,B}, IP_S]_{K_S}]_{K_P}$

当网关 T 收到 RIAR 消息的时候,检验 IP_S 是否在 RA_S 对应的 IP 链内,若不存在则丢弃该消息,否则使用 K_S 将 $RREQ_{A,B}$ 解密出来,然后进行如下操作:

●验证(IV_A, IP_A)对的新鲜性;

●根据 IP 链,对 RREQ 签名包进行逐级解密,并验证其 IP 标识是否相同;

●若某个 IP 标识信息错误,则记录下其 IP 标识并进入纠错程序,否则进入下一步;

●若逐级解密都完成后,获得的 与 IP 链的头文件不符,则记录下最初的 IP 标识并进入到纠错程序,否则进入下一步;

●根据 RA_S,找出 S →T 的路由信息;

●记录下 IP 链,并向此 IP 链后添加 S →T 的路由信息;

●检查此 IP 链是否有重复 IP,若没有,则进入下一步,否则向 S 发送授权路由冗余信息 REDU:

$T \rightarrow S: [REDU, IV_A, t, IP_S, [REDU, IV_A, t]_{K_S}]_{K_P}$

●向 S 发送 RREP 授权消息,消息为:

$T \rightarrow S: [RAP, IV_A, t, IP_S, [[REP, IV_A, t, RA_A, [[REP, IV_A, t, IP_B]_{K_A}, IP_S]_{K_B}]_{K_P}, RA_S]_{K_S}]_{K_P}$

当 S 收到 RREP 授权消息时,解密出:

$[REP, IV_A, t, RA_A, [[REP, IV_A, t, IP_B]_{K_A}, IP_S]_{K_B}]_{K_P}, RA_S$

验证 RA_S 是否正确,然后直接发给节点 B:

$S \rightarrow B: [REP, IV_A, t, RA_A, [[REP, IV_A, t, IP_B]_{K_A}, IP_S]_{K_B}]_{K_P}$

(5) RIAR 消息的处理

若某节点接收到一个 RIAR 消息,自身拥有到网关 T 的路由信息且未处理过此 IV 的消息,则向下一跳节点转发该消息,否则丢弃该消息.

(6) 授权失败的处理

当节点 S 发出的 RIAR 消息在相应的时间周期

(TTL)未获得响应,则 S 删除掉自身的路由信息,使用当前收到的 RREQ 消息进行新的路由查找过程:

$S \rightarrow broadcast: [REQ, IV_A, t, IP_A, IP_B, IP_S, [[[REQ, IV_A, t, IP_A]_{K_A}, IP_B]_{K_B}, IP_S]_{K_S}]_{K_P}$

2.2.3 路由维护

通过设定合理的纠错机制可以检测出恶意节点造成的附近节点的异常行为,通过广播去呼叫相应的节点,检查是否真的节点出现故障.

当网关 T 的纠错程序判断某个节点 E 可能出现故障时,可以发起节点的呼叫广播 CFB,内容为:

$T \rightarrow broadcast: [CALL, IV_T, [CALL, IV_T, t]_{K_E}, [IV_T, t]_{K_A}, [IV_T, t]_{K_B}, [IV_T, t]_{K_C}, \cdots]_{K_P}$

在 CFB 消息内包含了除 K_E 所有的密钥 K_A, K_B …加密过的 IV_T, t,而用 K_E 特别去加密 CALL, IV_T, t,以示区分.

当某个节点接收到一个 CFB 消息时,首先判断是否处理过此 IV_T 的消息,然后再使用自身密钥去解密时戳后面的签证分组,若解密出来的分组中包含 IV_T, t 字串,则原样转发此 CFB 消息.

当节点 E 接收到 CFB 消息时,通过验证出 CALL, IV_T, t 字串而得知网关 T 正在呼叫自己,则发起一次路由查找以注销掉网关 T 对自己的故障判断.

若网关 T 发出 CFB 消息后,在一定的时间内无法获得节点 E 的任何消息,正式认为节点 E 发生故障,通过认证中心广播其证书吊销信息,来隔离其功能.

为了使得恶意节点无法更改 IV_T,而在 CFB 消息内加入了所有节点的签证包,造成了 CFB 消息过于冗长,但是由于在 WMN 中节点故障发生的概率较低,所以 CFB 机制还是可以接收.

3 ARWMN 协议的安全性能分析与仿真

3.1 安全性能分析

ARWMN 采用对称密码技术,在本文假设存在各种攻击的前提下,评估协议的鲁棒性来分析其安全性能.接下来分析该协议如何抵抗常见的攻击.

(1)欺骗路由信令:由于只有源节点可以用它的密钥进行加密,则在路由查找中攻击者不可能更改加密过的路由信令;同样,在网关的路由应答过程中,路过的节点只能解密相对应的包,无法更改其信令,这避免了源节点或目的节点被欺骗的攻击.

(2)伪造路由消息:一旦公共密钥被恶意节点获知,恶意节点既可任意发出伪造路由消息,但是伪造的路由消息需要网关的授权才能被其他节点接收,所以 ARWMN 对伪造消息具有一定的威慑力.

(3)改变路由消息:在 ARWMN 中,虽然一旦 RREQ 消息的 IP 链被篡改,沿途 Mesh 路由节点无法对收到的伪造路由消息进行判别,而造成伪造信息将在 WMN 内广播,浪费网络网络资源.但是当网关收到此更改过的消息,而且对其解密失败后可转入相应的纠错程序,所以可以保证 RREQ 路由信息正确性.而对于 RREP 消息,采取的是只有收件人才可拆信的制度,所以 RREP 路由消息也是无法更改的.

(4)保护最短路径:由于隧道攻击还可出现在 ARWMN 协议中,因此根据跳数,ARWMN 无法确保最短路径,但是根据物理度量如路由消息中的时戳,它可选择一条最快路径使数据到达目的节点.

(5)重放攻击:路由消息中包含路由查找标识和时戳阻止了重放攻击.

(6)网络拓扑攻击:由于 RREQ 消息中 IP 链的存在,网络拓扑只是使用了公共密钥加密,易被恶意节点获知,但是由于 WMN 主要应用在民用领域,所以网络拓扑的安全重要性不高.

ARWMN 协议采用网关统一鉴别方式,WMN 中需有一台数据库服务器用来存放密钥和 IP 链,增加了网络铺设的成本;只支持到网关的安全路由通道的建立;协议每个 RREQ 消息的长度沿途是逐级变大的,在一个大型网络中势必会增加路由包的处理时间而造成的延迟,相同的 RREP 消息的平均长度也是非常大的;对称密钥方式的安全性能有所降低.

虽然 ARWMN 存在一些缺点,但它能有效地抗击大部分的恶意攻击,在几乎不增加设备成本的情况下提供较高的安全保障,保护网络的正常运行. ARWMN 协议为一种有效的按需路由安全协议,较好地满足在民用领域中对 WMN 上层路由的安全需求.

3.2 仿真环境

ARWMN 的主要优点是相对于 DSR 提高了安全性,相对于 ARAN 降低了路由消息处理延迟和 Mesh 路由节点的设备成本.仿真实验中,主要是对 3 种路由协议在不同的网络复杂度即不同的路由跳数下,接收到第一个分组的时刻做比较.路由收敛速度是衡量路由协议性能的一个重要标志.采用 QualNet 网络仿真器进行仿真,选择表 1 所示的仿真场景进行实验.

对于 ARWMN 协议的策略为:每个节点收到 RREQ 包后,在确认可以发包后,在原包基础上添加 256 bit;服务器在收到第一个 RREQ 包后,回复相同长度 RREP 包;每个节点收到 RREP 包后,在确认可以发包后,在原包基础上减少 256 bit;源节点收到 RREP 包后,确认路由的建立,开始发送数据.

表 1　仿真环境设置

Tab. 1　Simulation condition

场地面积	600 m ×1800 m
节点数目	2 ,3 ,4 ,5 ,6 ,7 ,8 ,9
物理层	802. 11b
节点位置	成一条直线均匀摆放,间隔 200 m
业务流量	1 条 CBR 流量,512 Bytes/ Packet,发送间隔(0. 1 s),由头节点指向末尾节点(网关服务器)
节点移动模型	静止状态
路径损失	双径模型
信道衰落	理想无衰落信道
MAC 层	802. 11b
路由协议	DSR、ARAN 和 ARWMN

3.3　仿真结果

利用 QualNet 的结果导出机制,将仿真实验结果在 Excel 中进行处理,得到如下一系列网络性能参数的比较图,每一个数据点都是对应的路由协议和路由跳数下各自的 30 次仿真结果的算术平均值(图 1).

从图 1 可以看出,3 种路由协议在接收到第一分组时刻都是随跳数的增大而增大. ARAN 收敛速度最慢,而且随着路由复杂性的增加,接收到第一分组时刻呈现加速上升趋势,这是由于其使用的公钥加密算法的复杂性所决定的;ARWMN 的路由表收敛速度慢于 DSR 的,但是与其非常接近,产生延迟的主要原因在于发送的消息长度的平均值较大. 使用对称密码体制的 ARWMN 的路由表收敛速度明显优于 ARAN. 可见,使用 ARWMN 来增强 WMN 的路由协议安全性是可行的.

4　结　论

本文提出 ARWMN 协议,描述了其工作原理,并对安全性能进行分析,通过仿真对路由效率进行了验证. 该协议增强了 WMN 网络安全性能并提高其路由收敛速度,能抵御一些常见的工具,具有一定的实用性. 今后的工作将对 ARWMN 协议的分析和实现都存在着一些不足做更深入的研究,以实现在更复杂网络中提供更安全更有效的数据传送.

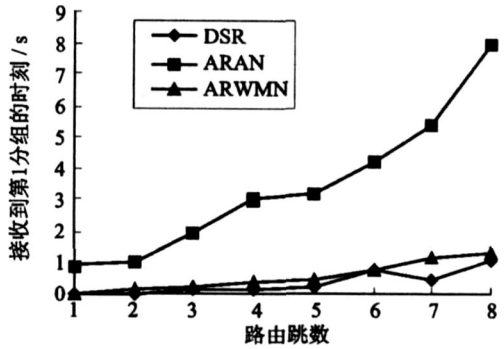

图 1　第一分组达到时间-路由跳数

Fig. 1　Time of first received packet-router-hops

参考文献:

[1] 樊自甫,万晓榆. 新一代宽带无线网络结构 ——Wireless Mesh[J]. 通讯世界,2003(9) :42.

[2] Kimaya Sanzgiri ,Bridget Dahill ,Brian Neil Levine ,et al. A secure routing protocol for ad hoc networks[C]//Proceedings of 2002 IEEE International Conference on Network Protocols (ICNP). Paris , France: IEEE ,2002 :78 - 86.

[3] 马婉秋. 无线 Mesh 网络的路由算法研究[D]. 成都:电子科技大学,2005.

[4] 方旭明. 下一代无线因特网技术:无线 Mesh 网络[M]. 北京:人民邮电出版社,2006.

[5] 于宏毅. 无线移动自组网[M]. 北京:人民邮电出版社,2004.

Research of Secure Routing Protocol in Wireless Mesh Network

SONG Zhi-xian , YU Ji-shen , XIAO Ming-bo *

(School of Information Science and Technology , Xiamen University , Xiamen 361005 , China)

Abstract: As a newly developed wireless network , WMN can provide wider wireless coverage with higher data rate . Our work features have an effective and secure routing mechanism to ensure successful operation of WMN. In this work , we mainly study the scure routing of WMN. The feature and security of WMN are introduced first. By analyzing the possible threats and characteristic of WMN , we propose ARWMN , an improved secure routing of WMN based on the authenticated routing of Ad hoc network (ARAN). Its performance is evaluated to prove that it can work well on WMN.

Key words: WMN ; Ad hoc ; secure routing ; ARAN