动态 Ad hoc 网络环境下组播源认证研究*

赵安军[1,2]，徐邦海[2]，郭　雷[2]
(1. 西安建筑科技大学 信息与控制工程学院，陕西 西安 710055；2. 西北工业大学 自动化学院，陕西 西安 710072)

摘　要：就 Ad hoc 网络环境下基于消息认证码的源认证技术进行了研究和分析,针对 TESLA 源认证方案给出了一个新的源认证引导方案,并采用间接引导方式来适应 Ad hoc 网络。实验数据表明,新的引导方案可以在较大程度上减轻系统的负担,从而提高认证的效率。

关键词：自组网；组播源认证；TESLA；消息认证码；无线自组网
中图法分类号：TP309　　**文献标识码**：A　　**文章编号**：1001-3695(2007)01-0291-03

Source Authentication for Multicast in Mobile Ad hoc Networks

ZHAO An-jun[1,2], XU Bang-hai[2], GUO Lei[2]
(1. *College of Information & Control Engineering, Xi'an University of Architecture & Technology, Xi'an Shanxi* 710055, *China*; 2. *College of Automatic Control, Northwestern Polytechnical University, Xi'an Shanxi* 710072, *China*)

Abstract: This paper aims to improve TESLA so that our selected authentication scheme is well suited for a mobile Ad hoc network. A main improvement is that new architecture for bootstrapping is adopted to improve the efficiency of bootstrapping and reduce burden for sender. Experimental results show that by amortizing overhead of bootstrap over bootstrapping tree, the new scheme modifies the way of bootstrap in Tesla and improves the efficiency of source authentication on great degree.
Key words: Ad hoc; Multicast Source Authentication; TESLA(Timed Efficient Stream Loss-tolerant Authentication); MAC(Message Authentication Code); MANET(Mobile Ad hoc Network)

无线自组网[1~3](Mobile Ad hoc Network, MANET)是一个由几十到上百个节点组成,采用无线的通信方式,动态组网的多跳的移动性对等网络。其目的是通过动态路由和移动管理技术来传输具有服务质量要求的多媒体或信息流。

MANET 使用了无线通信技术来传输数据,因此它具有无线通信系统信道质量低、带宽有限、节点通信距离有限和能量有限等特点[3,4]。为了充分利用有限的带宽和计算资源,节点均以组播的通信方式来执行某项任务,因此组播在 MANET 中就显得非常重要。目前,国外已经提出了几种针对 MANET 的组播路由算法和协议[4~6]。由于 MANET 大都用于军事或灾后重建等,现有的点对点通信模式中的数据源认证技术已不能满足组播传输的要求。安全问题,尤其是对数据源认证的问题就非常重要。因为在组播通信中,如果发送方和所有接收方共享一个密钥,每一个接收方均可以使用共享密钥去欺骗其他接收者,因此使用数字签名的方案既可以达到对数据源认证的目的,还提供数据源的非否认性。然而,数字签名在运算及网络通信流量方面的巨大开销阻碍了该方案的实施,这在 MANET 中是不允许的[3,7]。

最近,IETF 提出了一种新的组播源认证技术——TESLA[8]。它是基于消息认证码的认证技术,具有计算量小、带宽要求低等特点,非常适合 MANET。通过改进 TESLA 的引导方式,以可靠组播修复树的思想为基础,提出了一种基于引导树的数据源认证引导方式,即将由引导所带来的计算与其他开销分摊在引导树上,以便最大限度地提高引导效率并减轻数据源认证中发送方的负担,从而提高认证效率。

收稿日期：2005-10-20；**修返日期**：2006-03-27
基金项目：国家自然科学基金资助项目(60175001)

1　TESLA 工作原理及其使用的引导方式

TESLA 用于组播源认证的核心思想是,在一定的时间间隔后(即公开延迟时间间隔 d),公开先前发送的数据包 P_j 中用来计算消息认证码的密钥 K_i,发送方数据包的构成如下所示:P_j:{M_j|MAC(K'_i,M_j)|K_{i-d}},其中 M_j 为发送方发送的消息,MAC(K'_i,M_j)为消息 M_j 的消息认证码,K_{i-d}为公开密钥,且 $K'_i = F(K_i)$,$F(\cdot)$为某一单向函数。当接收方获得含有密钥 K_i 的数据包时,便可以对相应的缓存数据包进行验证。TESLA 的安全条件保证,如果消息 M_j 不是由发送者所发送,那么接收者永远不会接收它。

对于每个新加入的成员来说,必须用一个经过数字签名的数据包对其进行引导。这个签名的数据包主要包含以下关于时间间隔和密钥链信息:一个特定的时间间隔 T_j 开始时间以及时间间隔的标记 I_j;时间间隔的持续时间 T_{int};密钥的公开延迟时间间隔 d(单位时间间隔);一个密钥链中密钥 K_i($i < j - d$, j 表示当前的时间间隔索引)。由加入成员和发送方进行的引导方式称为简单或直接引导(Direct Bootstrap,DB)。然而,在大多数组播通信中,发送方资源属于整个组播系统的瓶颈资源。用户大量的加入对于发送方来说,引导过程将给其带来巨大的负担。文献[9,10]已经提出了不同的方法来解决这类问题,但是从实际应用来看并没有较好的效果。

2　间接引导方式

由于 MANET 所固有的特点,就必须尽可能地减少由认证

带来的计算和带宽开销。本文使用了类似可靠组播修复树[11]的方式来进行新加入成员的引导,称其为引导树,这种方式也称为间接引导(Indirect Bootstrap,IDB)。也就是,在整个移动节点组成的组播树中,选择某些节点来作为辅助的引导节点(Bootstrap Node,BN),功能与发送方的引导相同。具体过程如下:发送方使用数字签名方案发送相应的引导数据给有引导请求的引导节点。引导节点验证发送方的数据,然后同样使用数字签名方案在其所维护的分组中广播引导数据,分组中的成员验证数据从而完成引导,具体过程如下:

(1)发送方(Sender)通过安全的方式,将引导数据发送给引导节点(BN)。

(2)BN 解密引导数据并进行验证。

(3)BN 计算引导数据包以及散列值,并使用私钥对其进行签名,然后广播引导数据和签名。

(4)BN 所管辖的分组新加入的成员得到引导数据并进行验证,从而完成对其源认证的引导过程。

解决问题的关键是如何构建引导树。在组播的初始阶段,随着成员的加入,发送者根据通信组的规模以及网络分布选择网络条件和位置比较好的多个主机作为辅助的引导节点。在组播树完成后,发送者通过组播相应的信息来触发引导树的构建。这些信息包含了引导广播间隔(Bootstrap Advertisement Interval, BAI),BAI 确定了在引导节点发送引导广播(BA)的速率。通信组中的辅助成员也就是引导节点接收到这些消息后,开始按照它所给出的发送速率周期性地发送引导广播,这个发送包括发送者本身。在通信群组不再允许新成员加入时,包括发送者,所有的引导节点将停止广播 BA。当一个非引导节点成员接收到 BAI 后,它等待一个 BA 侦听间隔(Listen Interval,BALI)接收 BA 信息。BALI 由 BALI = min((3 × BAI),60s)决定。在 BALI 结束时,假如还没有接收到 BA 消息,那么接收者继续侦听下一个 BALI;当接收者获得一个或者多个 BA 消息后,整个侦听过程结束。在这多个 BA 消息中,接收者应该选择最适合自己的引导节点。选择的标准是从接收成员到引导节点,TTL 距离最小,并且拥有最多的成员数量。一旦选择了引导节点,接收者发送给所选择 BN 一个单播引导绑定(Bootstrap Bind, BB)消息。在接收到 BB 后,引导节点通过单播的方式发送接收或者拒绝该成员的消息。拒绝消息的发送是因为引导节点不再接收成员或者它要放弃自己的引导责任。在发送了绑定消息后,接收方等待一定的时间间隔来接收引导节点的响应,如果收到拒绝消息后,它将从 BA 消息中选择其他的引导节点并发送 BB,或者重新侦听已发现更好的引导节点。如果收到接收消息,则可以进行引导过程。

由于引导节点状态的变化,对于引导树可靠有效的管理非常重要。在管理过程中,有以下几种消息被用到:

(1)Hello。它是一个在整个通信组中广播的消息,由发送者发送,且 TTL 被限定在可到达最远引导节点。

(2)Hello-Unicast。发送者发送给特定引导节点的单播 Hello 消息。

(3)ACK。引导节点向发送者发送的单播控制消息。

发送者周期性地向通信组组播 Hello 消息。Hello 消息的作用是告诉引导节点,发送者依然可以接收新的成员。假如在一两个 Hello 消息周期后,引导节点没有接收到 Hello 消息,那么引导节点在其下一个 ACK 消息中设置标志以表示其未收到 Hello 消息,如果两个如此的 ACK 消息没有响应,这个引导节点将不再进行新加入成员源认证的引导。如果发送者接收到了包含有标志(没有接收到 Hello)的 ACK 消息,它将立即发送一个 Hello-Unicast 消息告诉引导节点,还可以接收新的成员。同时,发送者也使用下列机制来监控引导节点。在每个确认周期内,每个引导节点必须至少发送一个 ACK 消息。如果发送者在一个确认周期后,仍然没有接收到某个引导节点的 ACK 消息。引导节点将把这个成员增加到一个列表中,在下一个 Hello 消息的构建中将列表加入。引导节点发现它自己在列表中,将立即向引导节点发送 ACK 消息。如果如此的上述 Hello 消息超过两次,发送者还没有接收到引导消息的 ACK 消息,它将重新选择一个新的引导节点。

在引导节点的管理中,为了节省带宽,发送者应该以较小的 TTL 值来组播引导树控制消息。然而,为了能够使所有引导节点接收到管理信息,TTL 值又要相对较大。因此,选择一个合适的 TTL 对于引导的效率有很大的影响。在初始阶段,每个引导节点根据接收到的发送方信息得到 TTL 值,并将其 ACK 消息发给发送者。发送者使用最大的 TTL 值作为管理消息的 TTL。在引导节点与发送者路径发生变化后,相应的 TTL 值也应当变化。下面给出了调整 TTL 值的机制:

(1)当发送者管理消息 TTL 值不够时,某些引导节点将不能接收到 Hello 消息。这些引导节点将通过 ACK 来汇报相应的情况。

(2)发送者将通过单播 Hello-Unicast 来响应这些 ACK 消息,以告知引导节点其状态。然后在下一个广播 Hello 消息中增加 TTL 值。

这两个步骤连续执行直到所有的引导节点在其发送的 ACK 消息中不再包含 TTL 值过小的标志。另外,在引导节点的 ACK 消息中,如果发送者发现目前所使用的 TTL 值偏大,它将减少 TTL 值以节省带宽。

通过使用新的引导机制,能够在很大程度上降低由于对新加入成员源认证引导在发送方所带来的负担,这一点可以在实验结果中得以验证,从而提高组播系统瓶颈资源的利用效率。

3 试验环境和性能评价指标

在 TESLA 源认证试验中,使用了基于离散事件的 NS-2[12]网络模拟器,并且使用了 CMU 大学的无线扩展模块;使用了 IEEE 802.11 分布式协调功能作为 NS-2 的介质访问控制协议;每个节点的最远传输距离为 150m,带宽为 1.5Mbps;通信组的大小为 100;试验使用 MAODV(Multicast Ad hoc On-Demand Distance Vector)协议[4]作为 MANET 组播路由协议。

每次试验根据所使用的时间同步方式的不同分为两种引导方式,即直接引导方式和间接引导方式。对于直接引导来说,当成员发送请求数据包后,它设置一个计数器以监视引导过程,如果在计数器溢出后成员依然没有获得响应数据包,那么它将重新发出请求数据包并且复位计数器,试验中将计数器设为 0.5s。成员请求数据包最多发送次数为 10 次。对于间接时间同步,相当于对于接收方间接的引导。假设成员加入后已经获得了引导信息,仅需要的就是一个时间的同步信息,这可

以根据不同的第三方时间服务器而采用不同的方法。

数据载荷的认证头主要包含了密钥公开位、间隔 ID、序列号以及数据包头和数据内容的 MAC 值。直接时间同步的请求数据包头包含源地址和 Nonce。响应数据包包含了源地址和目的地址、发送的时间、响应序列号以及签名。图 1 给出了接收方源认证缓存区的数据结构。

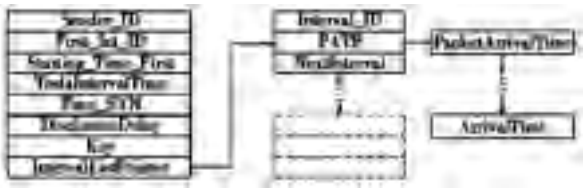

图 1　接收方源认证缓存区的数据结构

我们定义了以下几个主要的性能评价指标来评估 TESLA 和改进型组播源认证方案的性能:

(1)缓冲比(Buffered/Received)。它被定义为成员所缓存的数据包与接收到的数据包的比值。缓冲比所反映的其实就是在所有接收到的数据包中,满足 Tesla 源认证安全条件数据包的比重。这个主要是由网络延迟和初始的一些引导信息所决定的。

(2)认证比(Authenticated/Received)。它被定义为成员进行源认证并且提交给应用的数据包与所接收到的数据包的比值。实质上,认证比也就是在成员所接收到的数据包中通过源认证并提交给应用的数据包的比重。

(3)丢弃比(Droped/Received)。它被定义为成员所丢弃的数据包与其所接收的数据包的比值,丢弃比等于 1 减去认证比。

4　实验结果及其分析

首先描述一下实验具体参数的设置。实验网络包含了 100 个成员和 1 个发送者的通信组;发送数据包的大小为 64Bytes;发送方以固定速率 10 Packets/s 发送数据包。当发送者想要发送数据时,它通知路由算法对所使用的组播地址建立路由关系。每次模拟执行 300s。在模拟中使用了不同的模拟间隔时间 T_{int},分别为 0.1s,0.2s,0.5s,并且对于密钥的公开,也使用了不同的延迟间隔 d,分别为 1,2,3,4。每次根据不同的引导方式分为两次执行。图 2 中 DB 表示直接引导方式,IDB 表示间接引导方式。

图 2 给出了在发送速率为每秒十个数据包、一个发送者的情况下,在不同时间同步方式下的认证比、丢弃比以及缓冲比。由图 2 可知,间隔时间越大,认证所花费的时间越长,并且缓存时间和认证延迟越大。同时,接收数据包满足 TESLA 安全条件的可能性就越高。在间接引导方式中,比较合适的密钥公开延迟间隔在 10 Packets/s 的值应该为 2。图 2 中的数据也表明,间接的引导方式的源认证对比与直接引导方式来说,在三个性能指标方面均取得了较好的性能。前者相比较于平均的性能来说,提高了大约百分之二十左右。在当前的发送速率下,所有被缓冲的数据包几乎均得到了认证,从而表明所有通信组的成员几乎都接收到了大多数携带公开密钥的数据包。

5　结束语

本文详细地讨论和分析了无线自组网的组播源认证的问题,并描述了 TESLA 源认证的基本原理还介绍了它所采用的引导方式。以可靠组播修复树的思想为基础,提出了一种基于引导树的数据源认证引导方式,将引导所带来的计算和其他开销分摊在整个 MANET 所形成的引导树上。实验数据表明,新的组播源认证引导方式在动态的 Ad hoc 网络环境下,比 TESLA 所采用的直接引导方式,不论是引导效率、还是认证效率均有较大程度的提高。

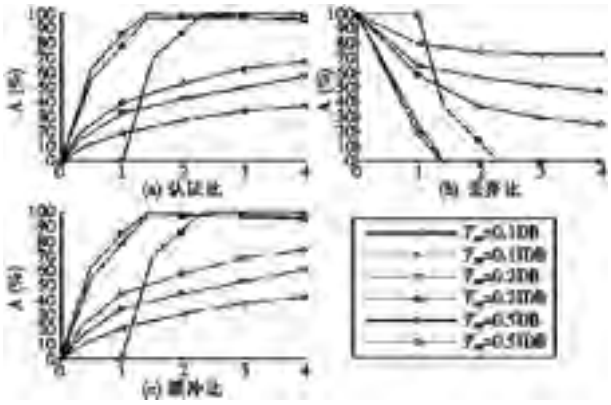

图 2　在发送速率为 10 Packets/s 下的三种性能指标的实验结果

参考文献:

[1] L Zhou, Z J Haas. Securing Ad hoc Networks[J]. IEEE Network Magazine,1999,13(6):24-30.

[2] S Jacobs, M S Corson. MANET Authentication Architecture[R]. IETF,1998.

[3] J-P Hubaux, L Buttyan, S Capkun. The Quest for Security in Mobile Ad hoc Networks[C]. Proceedings of ACM Symposium on Mobile Ad hoc Networking and Computing (MOBIHOC), 2001.

[4] E Royer, C E Perkins. Multicast Operation of Ad hoc On-Demand Distance Vector Routing Protocol[C]. Seattle, WA: Proceedings of ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom), 1999.201-218.

[5] S-J Lee, W Su, M Gerla. On Demand Multicast Routing Protocol (ODMRP) for Ad hoc Networks[R]. Draft-ietf-manet-odmrp-01.txt,1999-06.

[6] P Sinha, R Sivakumar, V Bharghavan. MCEDAR: Multicast Core Extraction Distributed Ad hoc Routing[C]. Proceedings of the Wireless Communications and Networking Conference, 1999.

[7] Kruus P. A Survey of Multicast Security Issues and Architectures [C]. VA: The 21st National Information Systems Security Conf. Rlington, 1998.

[8] Perrig A, Canetti R, Briscoe B. TESLA: Multicast Source Authentication Transform[EB/OL]. http://www.securemulticast.org/ msec-bof-5-Perrig-tesla-ietf-bof.PDF, 2000.

[9] A Perrig, R Canetti, D Tygar, *et al*. The TESLA Broadcast Authentication Protocol[J]. RSA CryptoBytes, 2002, 5(2):2-13.

[10] A Perrig, R Canetti, J D Tygar, *et al*. Efficient Authentication and Signing of Multicast Streams over Lossy Channels[C]. IEEE Symposium on Security and Privacy, 2000.

[11] Maihofer C, Rothermel K. Optimal Branching Factor for Tree-based Reliable Multicast Protocols[J]. Computer Communications, 2002, 25(11):1018-1027.

[12] Network Simulator, ns version 2[EB/OL]. http://ns2.netlab.cse.yzu.edu.tw/,2003-12.

作者简介:

赵安军(1975-),男,陕西大荔人,讲师,博士后,主要研究方向为网络安全和分布式网络计算;徐邦海(1974-),男,重庆壁山人,博士研究生,主要研究方向为 Ad hoc 网络安全以及组播安全;郭雷(1954-),男,山东人,教授,博导,博士,主要研究方向为图像处理和信息安全。