

MANET 主机安全自配置协议研究

薛 咏^{1,2}, 冯博琴¹

(1 西安交通大学 电子与信息工程学院, 陕西 西安 710049;

2 西南科技大学 信息工程学院, 四川 绵阳 621010)

摘 要: 提出一种基于 IPv6 的安全地址自配置方案 SMAAC(Security MANET Address Auto-Configuration), 新节点以口令方式通过节点验证服务器的验证后, 由该服务器发放节点授权票据, 由邻居节点进行授权票据检验并根据相关硬件信息产生 IPv6 地址, 并完成地址冲突检测, 保证网络内节点身份合法性. 最后对该方案进行了安全及性能分析与仿真.

关键词: 移动自组网; 地址自配置; 授权票据

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2010)05-0031-04

A Secure Hosts Autoconfiguration Protocol for MANET

XUE Yong^{1,2}, FENG Bo-qin¹

(1 School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China;

2 School of Information Engineering, Southwest University of Science and Technology, Mianyang 621010, China)

Abstract: A novel security address autoconfiguration SMAAC scheme is presented that based on IPv6, after a new node passed the identifying of the authorization server by the way of password and admitted to join the net, the server broadcasts a permitting ticket for the node, the neighbors of the node check the tickets and produce the IPv6 address according to the hardware information of the new node, and finish the duplicate address detection, the whole process ensures the validity of the new nodes. The security and performance of the protocol are analyzed and simulated at the end.

Key words: MANET; address autoconfiguration; ticket granting

1 引言

由于移动自组网网络的拓扑结构不断动态变化, 采用动态编址技术可适应移动自组网的移动性和自组织性. 主机地址自配置(Address Autoconfiguration), 是在节点加入网络时, 为节点动态地选择、分配和配置一个全网唯一的网络地址供其路由协议使用; 节点离开网络时又可以回收该地址, 以保证地址的重复利用; 其主要作用是有效地管理移动自组网网络的地址资源^[1-2].

在节点地址安全配置的基础上 MANET 的移动性为其带来如下问题^[3-4]:

(1) 孤立节点初始化; (2) 一群节点同时初始化; (3) 新节点加入网络; (4) 节点离开网络; (5) 网络分

割和再合并; (6) 独立网络的合并^[5].

目前, MANET 的安全问题研究主要集中在网络层以上, 研究节点密钥管理分配、链路认证与加密、服务发现等问题, 对于地址资源配置层的恶意节点入侵研究相对较少, 文献[6]中提出基于 Authentication Service(MAE)的 MANET 节点认证模型, 保证网络节点入网安全性. 文献[7]中提出一种给邻居节点建立可信任模型的方法来控制节点行为, 通过定义节点行为模式抵御资源占用攻击、拒绝服务攻击. 文献[8]中采用挑战应答机制, 由网络节点对待验证节点发送经过已知节点私钥加密的一个随机数(nonce), 如果验证节点能够通过私钥解密并发回该随机数的自加值, 则通过验证, 该方法能抵御通过重放进行的各种入侵攻击.

现有方法在新节点入网认证和地址篡改攻击方面缺乏防御能力,对于新节点的认证证书如何发放网络各节点没有详细的解决方案,在防范篡改地址攻击是假设节点会在协议的控制下自动发送地址冲突检测信息,这不符合网络攻击的基本情况.文中提出的 SMAAC 协议,以网络一次一密入网口令为基础,使验证过程具有较强可操作性,同时保证网络节点资源配置的安全性,将地址配置过程分为节点认证和地址配置两个阶段,兼顾集中管理与分布式处理的优势,针对地址配置阶段的各种攻击均有防御能力.

2 基于安全认证的主机配置方案

2.1 孤立节点初始化

对于一个没有发现任何邻居节点的孤立节点,需要进行初始化工作组成一个单节点网络,需要至少一个节点作为 AS(Authentication Server)认证服务器,以便完成新加入节点的安全认证,同时通过记录相关硬件信息抵制资源占用型攻击,考虑到服务器负荷问题,该节点只负责口令式节点接入认证与硬件信息登记.孤立初始节点充当 AS 服务器并完成自配置需要完成以下步骤的初始化:

(1) 初始化网络节点登记表.为了抵御资源占用型攻击行为,同时保证在节点离开后能够回收网络资源,设计一个网络节点的登记表,如表 1 所示.

表 1 网络节点配置登记表

字段名	NUM	ID _c	HD _c	Lifetime	Leasetime	Sign
字段长度/bit	16	32	48	16	32	1

NUM 为网络中节点的序列号, ID_c 为节点标识符, HD_c 为节点硬件标识符, Lifetime 指向一个计时器, Leasetime 表明一个 IP 地址的租用有效期,以便对节点突发离开时进行资源回收, Sign 纪录该节点是否或拥有一个 IP 地址.

在每个新加入节点通过了网络口令认证以后,将节点对应信息填入表中,如果节点在 Lifetime 时间内获得了一个合法的 IP 地址则完成了地址配置阶段.孤立节点初始化还需要生成一个对称密码 q_A , 用来在邻居节点之间进行地址验证,防止篡改地址攻击.

(2) 生成 IP 地址.文中协议采用 IPv6 地址格式,在 IPv6 地址分类中链路本地地址的网络地址为 FE80::/10, 站点本地地址为 FEC0::/10, 本文方案中新节点加入时需要在一跳邻居内交换信息, 本方案使用 FE80::HD/10 为节点初始化一跳地址,

其中 HD 为节点硬件地址.在为节点分配永久全局有效地址时把节点的地址分为网络前缀(Network Prefix)和接口标识符(Interface Identifier)两部分,其中网络前缀固定为 FEC0::NP 共 64 位,其中 NP 是一个由初始化节点产生的 16 位的随机数,则网络内节点地址为网络前缀地址与 64 位本地地址的拼接.

初始化节点本地地址由一个哈希函数 $H(\cdot)$ 生成,文中使用 MD5 算法,在第一次本地网络地址生成表达式为 $H(NP \parallel HD)$, 其中 NP 为一个 16 位的随机数, $\parallel$ 为拼接符号,经过与网络前缀拼接后形成全局地址.

2.2 群结点初始化

如果有多个节点同时建立网络,可能会出现多个节点建立 AS 服务器的场景,本协议中利用 AS 固定周期发送 HOLD 信息到各个节点,以表明该 AS 服务器的存在,不但可以解决网络分割时的 AS 重新组织的问题,也可以解决群结点初始化的问题.如果在这个 HOLD 信息发送周期内有 Ticket 发出则该周期无需再发送 HOLD 信息, Ticket 为一个新节点通过认证后 AS 给全局服务器洪泛一个的地址配置授权票据.在这种策略下,如果群初始化的时候出现了多个 AS 服务器,因为它们必须周期性地广播 Ticket 或者是 HOLD 数据,这样同一网络内其他的 AS 服务器都可以得知这种多服务器冲突,这时地址较大的服务器可以清除自己的配置登记表,按照新节点加入的程序获得一个新地址.

2.3 新节点加入

一个节点要加入当前网络,首先需要获得一个准入口令,在此基础上发出 ASREP(Authourization Server Request) 信息,请求通过 AS 的准入验证,过程描述为

$$N \rightarrow AS: ID_c \parallel HD_c \parallel K_p^c \parallel Password,$$

式中, N 表示新节点, (K_p^c, K_s^c) 为该节点产生的一对非对称密钥,其中将公钥 K_p^c 与硬件地址 HD_c、节点标识符 ID_c、网络入口命令连接并通过 1 跳邻居转发 ASREP 信息到 AS 服务器,同时新节点设置时钟作为本次请求回应有效时间.上述过程中口令是明文传输的,有被恶意节点窃听并利用的可能,所以在口令使用中可以通过一次一密的方式予以避免.

邻居节点在收到新节点的 ASREP 信息后将其发送到 AS 服务器进行验证,在通过验证后,首先需要在 AS 服务器的登记列表中查询是否该节点已经存在,如果没有则录入相关信息,否则进一步查看其

Sign 域标识确定是否已经为其分配了 IP 地址. 节点只有在节点配置登记表进行了登记而且没有得到一个 IP 地址的基础上, AS 通过广播的方式发送该节点的验证响应, 一个 TG(Ticket Granting) 信息. 否则需要查看租用时间, 如果距离上次申请时间小于设定值 $T_{threshold}$, 则视本次入网申请为恶意占用资源类攻击并不予响应. 通过验证的 TG 信息结构和 AS 行为描述为

$$AS \rightarrow * : Ticket \parallel E\{q_A\}_{K_p^c} \parallel HD_c.$$

对于 TG 信息, $E\{q_A\}_{K_p^c}$ 表示以 K_p^c 为密钥对 q_A 进行加密, Ticket 部分为 AS 服务器对网络内节点的广播信息, 意在通知各节点将有新节点其标识符为 ID_c 、硬件地址为 HD_c 、公钥为 K_p^c 的节点将可能 Lifetime 时间内向邻居节点请求全局网络地址, 票据的组成方式为

$$Ticket = E\{ID_c \parallel HD_c \parallel K_p^c \parallel Lifetime\}_{q_A}$$

新节点通过 HD_c 确定该消息是否应该由自己处理, 这个消息由 TG 服务器通过洪泛方式发送, 确保能到达尚未获得合法 IP 的新节点.

新节点在收到 TG 信息并获得本网密钥 q_A 后, 向邻居节点发出 AREP 信息, 由收到该 ID_c 入网票据的邻居节点予以回应, 新节点选择其中一个作为代理邻居, 负责进行其后的地址分配与冲突检测.

一个已配置节点在充当代理邻居后, 首先要对新节点进行身份确定, 防止恶意节点冒充正常节点, 这里使用了挑战应答机制. 节点认证信息格式为

$$P \rightarrow N : E\{nonce \parallel t_p\}_{K_p^c}$$

Nonce 是由邻居节点随即产生的一个 16 位数字, t_p 为节点 P 产生的一个时间戳. 代理邻居将该随机数用新节点的公钥加密后发送, 新节点收到该 CM(Challenge Message) 信息后, 用私钥进行解密后对随机数加 1, 然后与时间戳一起用 q_A 加密发回给邻居节点. 该应答信息 PM(Challenge Message) 形式为

$$N \rightarrow P : E\{nonce + 1 \parallel t_p\}_{q_A}.$$

如果新节点通过了挑战验证, 则进入 IP 地址产生阶段, 由邻居节点执行函数 $H(nonce \parallel HD)$, HD 为新节点 MAC 地址, 哈希函数 $H(\cdot)$ 与前面相同, 经过运算后产生两个 64 位, 这两个 64 位作为 2 个本地地址分别装入两个 DAP 信息进行全网地址冲突检测, 代理邻居在收到回复后经过对比如果发现节点对这两个 DAP 信息都回复 ACN(Address Conflict Notice) 地址冲突信息, 则可以肯定这是一个假地址冲突恶意节点(False Address Conflict Attack), 此时

可以选取一个本地地址与网络地址拼接, 并将这个网络地址作为新节点的全局地址经过节点私钥加密后分配给新节点. 如果两个 DAP 分别被拒绝, 对应地址都被网络占用, 此时代理邻居需要重新生成 nonce 并通过哈希函数计算新的本地地址.

邻居节点在 Lifetime 时间内完成上述步骤后, 新节点地址分配过程完成, 最后向 AS 发送 AC(address configured) 信息, AS 在节点配置登记表中分别填写 Sign 与 Leasetime 项.

2.4 节点离开

对于正常节点的离开, 只需要发送 NA(Node Apart) 信息到 AS 服务器, 服务器在节点配置登记表中删除该节点相关信息, 完成资源回收.

对于节点由于未知原因在没有发送 NA 信息并突发性离开网络时, AS 服务器是无法感知节点离开, 资源可能不能得到及时的回收, 但这时的资源仅限于对 AS 服务器内存的占用, 直到节点在 Lease-time 时间内没有发送延时租用请求, 资源将被自动回收.

2.5 网络切割

一个运行中的 MANET 因为移动或者节点失效可能导致网络分割, 这时只可能只有一个网络有 AS 服务器能够正常运行, 而被分割网络中节点会因为周期内没有收到 TG 消息或者 HOLD 信息而发现网络分割问题. 此时网络自动转入群节点初始化过程, 但是与初始节点不同的是, 最终的 AS 节点会保留自身网络地址不变, 以便于在网络再合并过程中作为标识, 但是密钥 q_A 必须重新选择.

2.6 网络再合并

对于分割后的网络在一段时间后稳定, 拥有自己的 AS 服务器并能够进行节点配置, 在此过程中如果有节点检测到其他网络地址, 但是持有不同密钥则可以做出再合并判断, 则表示这两个网络以前是同一个网络分割的. 由节点给本网 AS 服务器发送 MNR(Merge Network Request) 信息后, 双方 AS 服务器进入网络再合并阶段, 由网络地址较小的节点将本网的节点配置表发送给另一个网络服务器, 同时对本网节点广播发出 UAS(Update Authentication Server) 信息, 通知新的 AS 服务器地址以及新的网络密钥.

2.7 防御 IP 地址篡改攻击

MANET 恶意节点通过暴力篡改 IP 地址的方法, 进入网络并窃听或重放所有经过本节点的信息, 有可能造成严重破坏或者通信路由黑洞, 所以必须有

有效的方法进行发现,可以利用路由发现 HELLO 信息及时发现邻居节点的情况,如果有新邻居节点加入,可以通过验证网络密钥的方法进行节点认证。

3 协议仿真分析

本方案在 NS2 平台下进行了仿真,无线传输范围 200m,移动速度为 1~10m/s 之间变化,仿真时间为 300s。仿真模拟了 20 到 100 节点的地址初始化过程,考察了初始化时间和网络开销情况,并分别在 10s 时投入了地址篡改、拒绝服务以及资源耗尽性恶意节点,通过仿真程序运行记录查看协议的防御能力。

为了验证 SMAAC 协议的性能和防御能力,本文同文献[6]基于 Buddy 技术的安全地址配置方案进行了仿真比较。图 1 为不同仿真场景下网络内主机初始化时间,地址篡改、拒绝服务和资源消耗恶意节点发现时间的比较,仿真结果表明两种方案的初始化时间随着节点的增加而增大,时间开销基本一致。但是 Buddy 方案对于新加入节点没有授权验证过程,仅保证网内节点不能够被假冒,不能发现已验证节点的恶意行为。本方案中新节点在获得地址后连续发送两个地址进行 DAD,所以能以最快时间发现拒绝服务型攻击,同样由于 AS 服务器的作用能够迅速发现资源号耗尽型攻击。

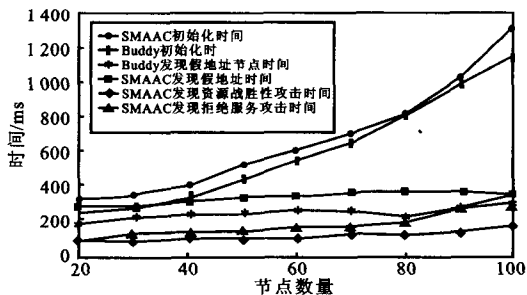


图1 协议初始化及发现各种不安全节点时间比较

图 2 给出了不同仿真场景网络的负荷,网络内节点每秒向随机发送两个长度为 512 字节的数据

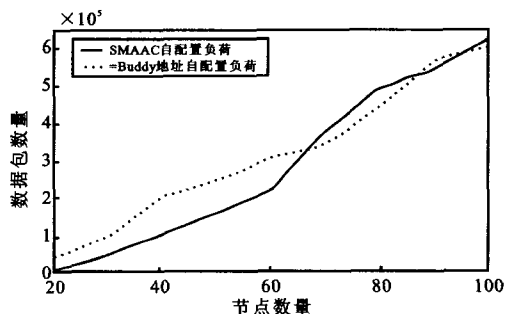


图2 协议负荷比较

报,网络层使用了 OLSR 路由协议。本方案由于采用了 IPv6 的地址格式、中心节点要进行一次洪泛通知,使得网络负荷相对较大,但是由于 Buddy 方案需要多邻居验证同样带来较大网络负荷,因为在 200m 的通信半径下邻居节点非常多,而对于本方案采用的洪泛方法却非常有利,所以在节点较多的情况下本方案反而有较小的网络开销。

4 结束语

针对 MANET 的主机地址安全配置问题,文中将节点验证与地址配置过程统筹考虑,提出 A-MAAC 协议使之能够有效地抵御无线网络中地址配置阶段的四种节点入侵方式,保证了网络内节点的合法身份,同时解决了网络的分割与合并的问题。相对已有方案防御能力最强,但是如何进一步减小网络开销需要进一步研究。

参考文献:

- [1] 解争龙. 基于无线 AdHoc 网络的入侵检测系统体系结构研究[J]. 微电子学与计算机, 2007, 24(5): 103 - 105.
- [2] 谭运宝, 钟诚. 一种基于邻居合作监测的移动 Ad hoc 网络信任模型[J]. 微电子学与计算机, 2008, 25(10): 227 - 230.
- [3] Wang Chiungying, Li Chengying. Global connectivity for mobile IPv6 - based Ad Hoc networks[J]. AINA, 2005: 807 - 812.
- [4] Ilkyun Park, Younghun Kim, Sangsan Lee. IPv6 address allocation in hybrid mobile Ad - Hoc networks[C]// WST-FEUS. Vienna, 2004: 58 - 62.
- [5] WildmanJeffrey, Hamel David. Performance and scaling of wireless Ad hoc IPv6 stateless address[C]// MILCOM. Orlando, 2007: 1 - 9.
- [6] Fabio Buiati, Ricardo Puttini. A secure autoconfiguration protocol for MANET nodes, lecture notes in computer science[M]. Berlin/Heidelberg: Springer, 2004: 108 - 121.
- [7] Shenglan Hu, Chris J Mitchell. Improving IP address auto-configuration security in MANETs using trust modeling [M]. Barlin: Springer, 2005: 83 - 92.
- [8] Ana Cavalli, Jean - Marie Orset. Secure hosts autoconfiguration in mobile Ad hoc networks[C]// ICDCSW. Tokyo, 2004: 809 - 814.

作者简介:

薛咏男, (1978 -), 博士. 研究方向为网络安全、语义网。
冯博琴男, 教授, 博士生导师. 研究方向为智能网络。