



一种在无状态地址自动配置中 DAD 攻击的防御方法^{*}

宋广佳¹, 季振洲¹, 王 晖²

(1. 哈尔滨工业大学计算机科学与技术学院 哈尔滨 150001;

2. 国家计算机网络应急技术处理与协调中心 北京 100029)

摘 要:在无状态地址自动配置中,新 IP 地址在使用前需要进行重复地址检测。在检测过程中,一旦有攻击节点声称解析地址已经被占用,将导致节点地址配置失败,从而形成重复地址检测攻击。针对这种情况,提出使用 WAY 机制作为防御手段,WAY 机制使用逆向地址确认、自我声明及 WAY-table 检查的方法,对欺骗报文进行过滤,使欺骗节点攻击成本增加且无法进行二次欺骗。仿真实验表明,WAY 机制弥补了邻居发现协议安全性的不足,可大幅提升无状态地址自动配置的成功率。

关键词:网络安全;地址解析;IPv6;无状态地址自动配置;重复地址检测

doi: 10.3969/j.issn.1000-0801.2014.04.008

A Defense Approach of DAD Attack in Stateless Auto Configuration

Song Guangjia¹, Ji Zhenzhou¹, Wang Hui²

(1.School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China;

2.National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100029, China)

Abstract: In stateless address auto configuration, node needs to carry out duplicate address detection before using a new IP address. In the detection process, once a malicious node claims that the resolve IP address is occupied, the node's address configuration will fail. For this case, WAY (who are you) mechanism as a defensive approach was proposed. WAY mechanism uses reverse address confirmation, self-declaration and WAY-table inspection to filter the spoofing packets, which make attackers' cost increase and cannot carry out secondary attack. The experiments show that WAY mechanism can effectively compensate the security flaws of neighbor discovery protocol, significantly increase the success rate of stateless address auto configuration.

Key words: network security, address resolution, IPv6, stateless address auto configuration, duplicate address detection

1 引言

在 IPv4 中,使用地址解析协议(address resolution protocol, ARP)进行地址解析,而针对 ARP 进行的攻击是局域网安全的主要威胁。在 IPv6 中,不再使用 ARP,而是

使用邻居发现协议(neighbor discovery protocol, NDP)进行地址解析,由于 IPv4 与 IPv6 在设计时都假设网络中的节点是可信的^[1,2],而现实的网络环境却不是这样,因此地址解析过程中的欺骗攻击一直存在,同时也是局域网的主要安全威胁^[3-5]。

^{*} 国家自然科学基金资助项目(No.61173024)

IPv6 中的地址配置主要有两种方式:一种是无状态地址自动配置(stateless address auto configuration,SLAAC),另一种是利用 DHCP 服务器进行地址配置。无状态地址自动配置是指接口在接入网络后可以根据自己的 MAC 地址按照 EUI64 规则生成链路本地地址,或者根据路由器公告信息生成其他类型地址,这些地址在使用前需要进行重复地址检测(duplicate address detection,DAD)^[2,6]。以链路本地地址为例,地址配置过程如下。

比如,局域网中有两台主机 A 与 C,MAC 地址分别是:AA:AA:AA:AA:AA:AA 与 CC:CC:CC:CC:CC:CC。当主机或者接口刚接入网络时,接口可以根据自己的 MAC 地址,按照 EUI64 规则生成链路本地地址,如 A 生成的链路本地地址是 FE80::A8AA:AAFF:FEAA:AAAA,同样,接口也可以根据路由器公告(router advertisement,RA)信息中的前缀生成全球唯一单播地址,无论是链路本地地址还是全球单播地址,在使用之前,都需要进行重复地址检测,在这一过程中,攻击节点可以不断声称该地址已经被占用(实际情况是并未被占用),则主机将无法获取可用 IP 地址。

2 相关工作

在 IPv6 中,DAD 主要使用邻居发现(neighbor discovery,ND)协议中的邻居请求(neighbor solicitation,NS)报文与邻居公告(neighbor advertisement,NA)报文进行信息交换,ND 报文主要由 3 部分构成:Ethernet 部分、IPv6 头部与 ICMPv6 部分,主要字段如图 1 所示。NS 报文没有“RSO”字段,NS 报文的“type”字段为 135,NA 报文的“type”字段为 136。“RSO”字段只在 NA 中使用,“target address”字段一般写入地址解析的目的地址,“option”字段在不同类型的 ICMPv6 消息中用法各不相同,在 ND 协议中一般给出发送该报文的节点的 MAC 地址。

Ethernet部分	Dest MAC SRC MAC type
IPv6头部	SRC IP DST IP next header
ICMPv6部分	RSO(only for NA) type target address option

图 1 ND 报文的主要字段

A 生成临时地址之后会以广播方式发送如图 2 所示的邻居请求报文进行 DAD,在等待一段时间后如果没有

收到 NA,则说明该地址没有冲突,可以使用;如果收到了 NA,说明该地址已经被占用,如图 3 所示,说明网络上已经有接口使用该地址,地址自动配置失败,需要手动配置地址。

Ethernet部分	33:33:FF:AA:AA:AA AA:AA:AA:AA:AA:AA 0x0806
IPv6头部	:: FF02::1:FFAA:AA:AA 0x3A
ICMPv6部分	135 FE80:A8AA:AAFF:FEAA:AAAA AA:AA:AA:AA:AA:AA

图 2 NS 报文

Ethernet部分	33:33:00:00:00:1 BB:BB:BB:BB:BB:BB 0x0806
IPv6头部	FE80:B9BB:BBFF:FEBB:BBBB FF02::1 0x3A
ICMPv6部分	136 O=1 FE80:A8AA:AAFF:FEAA:AAAA BB:BB:BB:BB:BB:BB

图 3 NA 报文

一种常见的攻击方式就是对 DAD 过程中的 NS 消息进行回答,声称该 IP 地址已经被使用,则该节点或接口将无法获得可用的 IP 地址^[7]。虽然 IPv6 中使用 IPSec 协议对网络通信进行保障,但 IPSec 协议只对端到端的通信进行加密,无法抵御 DAD 攻击^[8]。

为了增加 ND 协议的安全性,IETF 小组提出了安全邻居发现(security neighbor discovery,SEND)协议,它使用加密地址生成(cryptographically generated addresses,CGA)、数字签名等技术对通信进行加密,有效防止 IP 地址被盗用^[9,10]。但一方面,CGA 过程需要大量集中计算,而且 CGA 产生的地址仍然需要进行重复地址检测,一旦发现冲突,就需提高安全等级,然后重新进行 CGA 计算,而重新计算需要的时间是上次计算所需时间的 65 534 倍^[11]。当 Sec=3 时,时间将以年为单位,这是无法忍受的。因此,如何缩短 CGA 的计算时间是 SEND 亟待解决的问题,许多研究人员对此进行了探索,如采用并行化计算方法^[12]以及更快速的加密算法^[13,14],或者根据给定时间条件确定 Sec 值的大小^[15]等。另一方面,SEND 协议也无法有效解决 DAD 攻击问题^[16]。这些原因导致 SEND 协议虽然安全性很高,但很难被实现,或者只是部分实现^[17]。同时,SEND 与 ND 的并存还会带来新的路由问题^[18]。

因此,如何抵御 DAD 攻击成为 ND 协议中亟待解决



的问题。本文使用 WAY(who are you)机制抵御 DAD 攻击, 为了实现 WAY 机制, 增加了两种新的分组格式, 采用逆向地址确认的方法对 DAD 过程中发生冲突的 NA 消息进行过滤, 对返回的 WAY-reply 分组进行检测, 以确定是否存在欺骗, 同时对发生冲突的地址进行 WAY-table 登记, 防止二次欺骗。

3 加入 WAY 机制的 DAD 过程

WAY 机制是一种节点自我声明的机制, 它基于下面两个原理。

- 由于交换机是根据自身的<MAC, 端口>映射表对报文进行转发与交付, 如果节点使用虚假的 MAC 地址对主机进行欺骗, 在逆向单播确认时, 会出现报文丢失, 即目的不可达(注: 即使欺骗节点使用虚假 MAC 地址欺骗交换机从而收到了单播确认, 但在后续的二次欺骗中也会被发现并被写入 WAY-table)。
- 在 IPv6 的无状态地址自动配置中, 由于接口的 MAC 地址具有唯一性, 因此对于基于 EUI-64 规则自动生成的链路本地地址, 理论上不会出现地址冲突, 更不会出现多次(包括二次)地址冲突。

为了实现 WAY 机制, 在 ND 协议中增加了两种新的报文: WAY-request 与 WAY-reply。这两种报文的格式与 ND 协议报文格式基本相同, 区别之处在于: 在 WAY-request 中, “target”字段不再写入重复地址检测的地址, 而是使用临时地址“::”代替。在 WAY-reply 中, “target”字段填写自己的链路本地地址。为了避免与已有 ICMPv6 报文类型发生冲突, WAY-request 与 WAY-reply 的类型(“type”字段)分别设置为 152 与 153。同时在 WAY 机制中增加 WAY-table, 用于存储在 DAD 过程中与之发生冲突的接口的<MAC, IP>以及信任信息; 地址自动配置过程如果发生冲突, 则会将冲突接口的 MAC 地址与 IP 地址信息写入 WAY-table, 并将信任标记为 T, 意思是目前可信, 如果二次地址配置过程中依然与该地址发生冲突, 则将该地址标记为 F, 即不可信。如果认为接口存在欺骗行为, 则将该接口的 MAC 地址与 IP 地址信息写入 WAY-table, 并且直接标记为 F, 即该节点不可信。

加入 WAY 机制后的 DAD 过程如下: 当节点进行重复地址检测时, 如果收到 NA 回复, 声明地址已经被使用, 则节点首先等待一个随机时间, 然后使用 WAY-request 对发

生冲突的 NA 进行逆向确认, 采用单播方式发送到冲突的接口, 同时要求对方使用 WAY-reply 回复自己 MAC 地址及链路本地地址, 即进行自我声明, 这样主机就可以对 WAY-reply 中的信息与前面收到的 NA 进行核对, 以确定是否存在欺骗。如果没有收到 WAY-reply, 说明对方使用虚假的 MAC 地址, 前面的 NA 为伪造的, 并没有发生地址冲突, 地址可用。如果收到了 NA, 则根据待检测的地址进行判断, 如果待检测的是一个链路本地地址, 则需要满足下面两个条件才会被认为真正发生了地址冲突。

- 条件 1: WAY-reply 中的源 IP 地址与待检测 IP 地址相同, 而且源 MAC 地址与前面收到的 NA 中的源 MAC 地址相同。
- 条件 2: WAY-table 中如果有 WAY-reply 的源 MAC 地址对应的信息, 则该信息的字段必须是 T。

如果条件 1 和条件 2 不能同时满足, 则认为待检测地址(链路本地地址)可用, 没有发生冲突。

如果待检测的地址为非链路本地地址, 而是节点根据路由器公告的前缀信息生成的其他类型地址, 则判断条件如下。

- 条件 1: WAY-reply 中的源 MAC 地址与前面收到的 NA 报文中的源 MAC 地址相同。
- 条件 2: WAY-table 中如果有 WAY-reply 中源 MAC 地址对应的信息, 则该信息的字段必须是 T。

如果条件 1 和条件 2 不能同时满足, 则认为没有发生地址冲突, 前面收到的 NA 是伪造的。

加入 WAY 机制后的 DAD 过程如图 4 所示。

假设 C 是一个欺骗节点, 一直存在于网络上, C 的欺骗策略是只要收到 DAD 过程中发出的 NS 报文, 就发送 NA 进行回复。以链路本地重复地址检测为例, 当节点 A 刚加入网络时, 根据 MAC 地址生成临时地址 FE80::A8AA:AAFF:FEAA:AAAA, 然后进行 NS 多播, 报文如图 1 所示, 如果没有收到 NA, 则认为该地址可以使用。因为 C 是欺骗节点, A 会收到 C 发送的 NA, 如图 2 所示, 为了辨别 NA 报文的真假, A 在等待一个随机时间后, 会单播 WAY-request 报文进行逆向测试, 如果没有收到 WAY-reply, 说明收到的 NA 是伪造的并且使用了假的 MAC 地址, 则 A 产生的临时地址是可用的, 如果收到 WAY-reply, 则需要对 WAY 检查, 方法如下。

假设 WAY-reply 中的 MAC 地址为 MAC_x , 链路本地地址为 IP_x 。首先, 检查 WAY-reply 中的 MAC 地址与 NA 中的 MAC 地址是否相同, 如果不同则存在欺骗, 将 $\langle MAC_x, IP_x \rangle$,

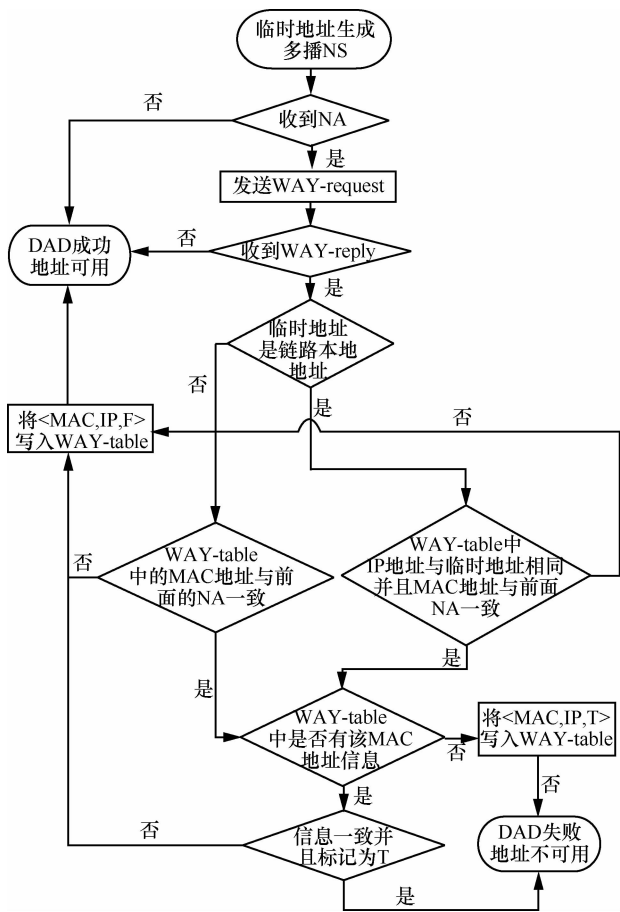


图 4 WAY 机制流程

F>写入 WAY-table, 如果相同则继续比较 IP_x 与临时地址是否相同, 如果不同, 则存在 NA 欺骗, 临时地址可用, 并且将 NA 中的 $\langle IP_x, MAC_x, F \rangle$ 存入 WAY-table, 如果相同, 则检查 WAY-table 是否存在 MAC_x 的信息, 如果存在, 看信任标记, 如果是 F, 则存在欺骗, DAD 成功, 如果标记为 T, 则比较 IP 地址是否一致, 一致则 DAD 失败, 不一致则存在欺骗, DAD 成功, 将标记改为 F; 如果 WAY-table 中不存在 MAC_x 的信息, 则 DAD 失败, 将 $\langle IP_x, MAC_x, T \rangle$ 写入 WAY-table。

如果 C 在收到如图 5 所示的 WAY-request 分组后回复的 WAY-reply 如图 6 所示, 则 A 检查发现 IP 地址与临时地址不同, 则认为存在欺骗, 将 $\langle CC:CC:CC:CC:CC:CC, FE80:CECC:CCFF:FECC:CCCC, F \rangle$ 写入 WAY-table, DAD 成功, 则 A 产生的临时地址可用, WAY-table 见表 1。

4 实验与分析

4.1 仿真实验

实验使用的仿真软件为 OPNET。实验采用模拟局域

Ethernet 部分	CC:CC:CC:CC:CC:CC AA:AA:AA:AA:AA:AA 0x0806
IPv6 头部	:: FF02::1:FFAA:AA:AA 0x3A
ICMPv6 部分	152 :: AA:AA:AA:AA:AA:AA

图 5 WAY-request

Ethernet 部分	AA:AA:AA:AA:AA:AA CC:CC:CC:CC:CC:CC 0x0806
IPv6 头部	FE80:CECC:CCFF:FECC:CCCC FF02::1 0x3A
ICMPv6 部分	O=1 153 :: CC:CC:CC:CC:CC:CC

图 6 WAY-reply

表 1 WAY-table

MAC 地址	IP 地址	T 或 F
CC:CC:CC:CC:CC:CC	FE80:CECC:CCFF:FECC:CCCC	F

网方式, 网络中包含 1 个交换节点, 即 8 个外围节点, 其中 1 个为正常节点, 7 个为欺骗节点。欺骗节点的攻击方式为只要收到 DAD 检测报文就进行虚假 NA 回复, 声称该地址已经被占用。正常节点中包含一个分组发送源, 用于产生随机地址的 DAD 检测报文, 分组发送间隔服从泊松分布, 平均值为 1。如果首次地址配置失败则进行二次地址配置, 最多配置 3 次^[2]。背景流量采用黑龙江中医药大学综合楼 30 天平均流量统计, 数据采集软件为 Solar Winds Orion, 数据如图 7 所示。实验分两个场景进行, 分别模拟正常的 DAD 过程与 WAY 机制下的 DAD 过程, 统计量为首次地址配制成功率与二次地址配置成功率。

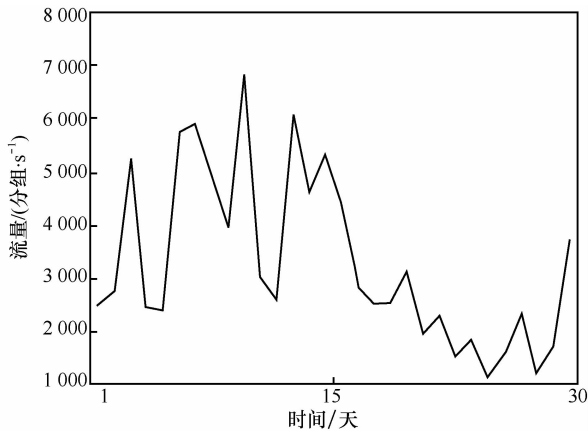


图 7 背景业务负载



欺骗节点采取的策略有以下 4 种。

- 策略 1: 在 NA 分组中使用假的 MAC 地址。
- 策略 2: 在 WAY-reply 分组中回答自己的真实 IP 地址与 MAC 地址。
- 策略 3: 在 WAY-reply 分组中, 回答自己的 MAC 地址与根据 WAY-request 中 A 的 MAC 地址生成的链路本地地址。
- 策略 4: 在 WAY-reply 分组中, 使用虚假 MAC 地址与根据 WAY-request 中 A 的 MAC 地址生成的链路本地地址。

在 WAY 机制中, 策略 1 由于使用虚假的 MAC 地址, 无法收到 WAY-request 报文, 因此无法进行 WAY-reply, 不能造成 DAD 失败。策略 4 由于在 WAY-reply 中使用假 MAC 地址, 无法通过 WAY 测试, 也无法造成 DAD 失败。策略 2 与策略 3 则可能造成地址检测失败, 以链路本地地址配置为例, 策略 2 与策略 3 的仿真结果如图 8~图 10 所示, 仿真统计量为 DAD 失败率与 WAY-table 真实度。其中, DAD 失败率为 DAD 失败次数与 DAD 总次数的比值, WAY-table 真实度为 WAY-table 中信息为真的条目数与总条目数的比值。

由图 8 与图 9 可见, 在实验过程初期, 当发生 DAD 冲突时, 由于此时 WAY-table 为空白, 因此无法对发生冲突的 MAC 地址进行查证, 此时会导致节点 A 的 DAD 失败(一般为首次地址配置), 随着时间的增加, 节点在进行二次地址配置及后续地址配置时, 如果欺骗节点 C 继续进行攻击, A 节点会通过检查 WAY-table 发现 C 在说谎, 并将 C 标记为不可信。随着时间继续增加, 所有欺骗节点都将被记入 WAY-table, 并且标记为不可信。因此, 经历了初期的 DAD 失败高峰之后, DAD 失败率将逐渐降低, 趋向于 0。

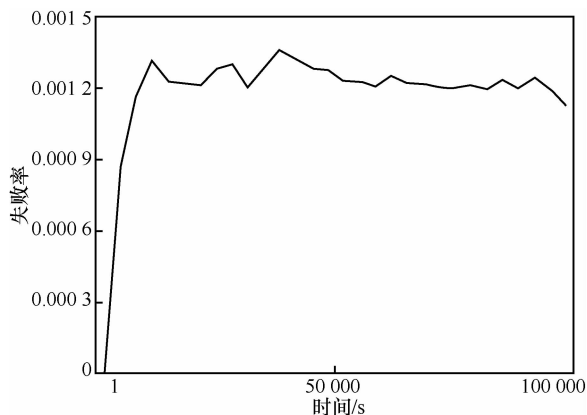


图 8 地址配置失败率(策略 2)

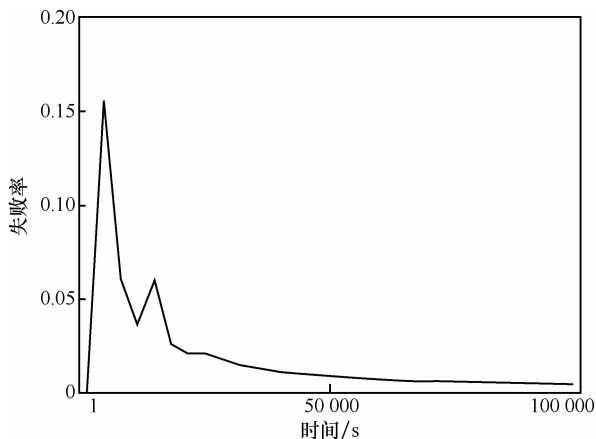


图 9 地址配置失败率(策略 3)

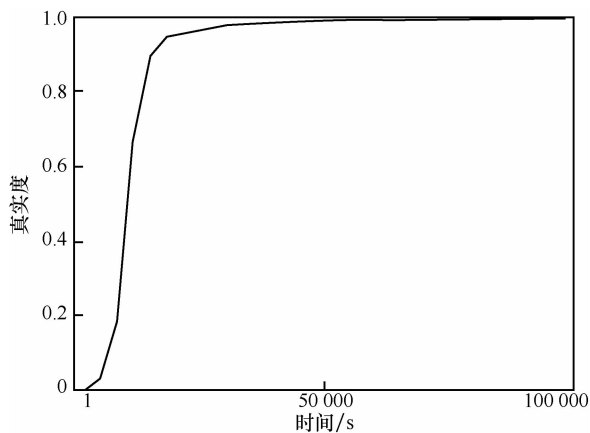


图 10 WAY-table 真实度

由于策略不同, 图 8 与图 9 的高峰期有所区别, 表现为当 A 进行首次地址配置时, 如果 C 采用策略 3, 则 C 有较大概率可以通过 WAY 测试, 因此 DAD 失败率会大大增加, 但同样随着时间的增加, 在后续的 DAD 过程中, 所有欺骗节点都将被 WAY-table 所记录, 从而无法进行重复欺骗, 因此 DAD 失败率也逐渐趋向于 0。在 WAY-table 真实性方面, 初期 WAY-table 中真实条目较少, 但随着检测到的欺骗行为不断增加, 程序逐渐对 WAY-table 中的条目进行修正, WAY-table 的真实性逐渐趋向于 100%。

4.2 对比与安全性

参考文献[19,20]都建议使用 ICMP 对收到的地址解析报文进行逆向地址确认, 以应对地址解析过程中出现的各种攻击, 也包括 ARP 中的重复地址检测冲突。该过程或者由主机自身完成, 或者由第三方完成。利用 ICMP 检测的基本假设如下。

- 接口(网卡)只接收目的 MAC 地址与自己的硬件地址相符的数据分组、广播数据分组和特定的多播分组, 而对于其他类型的分组则全部丢弃。

- 攻击节点无法阻止正常节点对 ARP 请求与 ICMP 请求的应答,正常节点不会对目的 IP 地址与自身 IP 地址不符的 ICMP echo request 数据分组进行转发。

将参考文献[19,20]中的方法进行整合,扩展其功能。描述如下:在收到 ARP 报文之后,节点并不直接相信,而是首先对报文中的以太网头部的 IP、MAC 源地址与 ARP 头部的 IP、MAC 源地址进行比对,如果二者不符则认为存在欺骗,如果符合则发送 ICMP echo request 报文进行逆向探测,然后根据探测结果进行判断。比如,如果没有收到返回分组,则认为之前收到的 ARP 报文是伪造的;如果收到了返回分组,但其中的源 IP、MAC 地址与之前收到 ARP 报文中的源 IP、MAC 地址不符合,则也认为存在欺骗行为;如果目标返回的报文是正确的,但目标对两条具有不同目的 IP 地址的 echo request 都回答,则同样认为节点存在欺骗。与这种方法相比,在有攻击节点的情况下,WAY 机制的优势表现为以下 3 点。

(1)参考文献[19]中使用数据库记录 IP 地址与 MAC 地址的映射关系,并且要保证不会出现多个 IP 地址对应同一个 MAC 地址。但这样的方法在 IPv6 中不再有效,因为在 IPv6 体系中,一个接口可以同时具有多个不同类型的 IP 地址,即使是同一类型 IP 地址,也可以具有多个,而非 IPv4 中一个接口一般只对应一个 IP 地址。而 WAY 机制则以 MAC 地址为最终依据,对 DAD 过程中收到的 NA 进行逆向单播确认,如果欺骗 NA 使用假的 MAC 地址,则无法收到 WAY-request,也就无法进行回复,这就使得 MAC 欺骗变得不可能。如果节点想要欺骗,则必须在 NA 中使用真实的 MAC 地址,而一旦使用真实 MAC 地址进行欺骗攻击,无论成功与否,MAC 地址都会被对方记入 WAY-table,同时由于在网络中正常节点占大多数,具有欺骗行为的节点占少数,所以 WAY-table 中的记录数要远小于数据记录方式下的 IP 地址与 MAC 地址映射数。

(2)参考文献[20]中对具有强欺骗能力的节点只能发现,但无法防止其后续的欺骗行为,而 WAY 机制使用对冲突的地址进行记录,防止二次欺骗。由于对发生冲突的节点信息进行了记录,如果在二次 IP 地址配置中仍然发生冲突则认为存在欺骗,因为在 SLAAC 中,接口首选的 IPv6 地址,无论是链路本地地址还是根据 RA 生成的全球单播地址,理论上只有一个。

(3)参考文献[20]中具有强欺骗能力的节点可以针对

性地回答 ICMP echo request 报文,但在 WAY 机制中,欺骗节点在进行 WAY-reply 回答时很难做出正确回答,因为欺骗节点不知道发送 WAY-request 分组的接口正在进行链路本地地址 DAD 还是全球单播地址检测,无论是链路本地地址的 WAY 检测还是全球单播地址的 WAY 检测,发出的 WAY-request 都是一样的,并且 WAY-request 中几乎不包含任何 IP 地址信息,使欺骗节点无法根据“target address”字段进行欺骗,同时,欺骗节点在一段时间内会收到很多 WAY-request 检测分组,如何对其中的一个进行成功欺骗,是一个很难的问题。

当然,WAY 机制也存在一些需要完善的地方。首先,WAY 机制由于采用逆向地址确认,会导致网络中单播的地址解析报文数量增加;其次,如果欺骗节点采用虚假的 MAC 地址,则在逆向地址确认过程中交换机为了查找这个不存在的 MAC 地址会进行泛洪,会在一定程度上导致网络中的广播报文增多。

5 结束语

地址解析过程的安全性是网络通信的前提保障,随着 IPv6 网络的推广与使用,无状态地址自动配置由于其自身的方便与快捷,必将成为 IPv6 中地址配置的主要方式,但由于缺少安全机制,无状态地址配置过程中容易受到重复地址检测攻击。本文通过对邻居发现协议安全性的分析,提出了一种无状态地址自动配置中可抵御 DAD 攻击的安全机制,由于该机制对 NA 消息采用逆向确认与自我声明,一旦欺骗节点使用虚假 MAC 地址将无法收到确认分组,而且由于确认分组中隐藏了“target-address”字段,即使欺骗节点收到了确认分组也无法根据该字段伪造应答,同时 WAY 检测以及 WAY-table 登记使欺骗节点一旦欺骗成功,则将<IP,MAC>等地址信息记录到 WAY-table 中,无法进行二次欺骗,从而降低了欺骗成功率。仿真实验表明,WAY 机制使无状态地址自动配置首次地址配置成功率及二次地址配置成功率显著提高,同时由于 WAY 机制的认证过程采用单播方式,并且没有采用非对称加密等复杂算法,相对于整体网络,占用的带宽与通信量都是非常低的。

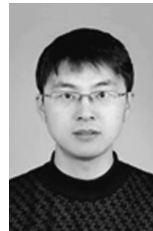
参考文献

- 1 Plummer D C. An ethernet address resolution protocol. <http://tools.ietf.org/html/rfc826>,1982
- 2 Narten T, Nordmark E, Simpson W, et al. Neighbor discovery for IP version 6(IPv6).<http://tools.IETF.org/html/rfc4861>, 2007



- 3 Gao J H, Xia K J. ARP spoofing detection algorithm using ICMP protocol. Proceedings of the IEEE International Conference on Computer Communication and Informatics, Coimbatore, India, 2013:1~6
- 4 Wang X L, Zhou G. Defence design for ARP spoofing based on NDIS intermediate driver. Proceedings of the IEEE International Conference on Computer Distributed Control and Intelligent Environmental Monitoring, Changsha, China, 2012:218~220
- 5 Pandey P. Prevention of ARP spoofing: a probe packet based technique. Proceedings of the IEEE International Advance Computing Conference, Ghaziabad, India, 2013:147~153
- 6 Thomson S, Narten T, Jinmei T. IPv6 stateless address auto configuration. <http://tools.IETF.org/html/rfc4862>, 2007
- 7 Nikander P, Kempf J, Nordmark E. IPv6 neighbor discovery (ND) trust models and threats. <http://tools.IETF.org/html/rfc3756>, 2004
- 8 Liu C H, Dai Q G. Design of security neighbor discovery protocol. Proceedings of the IEEE International Conference on Communication Systems and Network Technologies, Gwalior, India, 2013:538~541
- 9 Arkko J, Kempf J, Zill B, *et al.* Secure neighbor discovery (SEND). <http://tools.IETF.org/html/rfc3971>, 2005
- 10 Aura T. Cryptographically generated addresses (CGA). <http://tools.IETF.org/html/rfc3972>, 2005
- 11 AlSa'deh A, Meinel C. Secure neighbor discovery: review, challenges, perspectives, and recommendations. IEEE Security & Privacy, 2012, 10(4): 26~34
- 12 Rafiee H, AlSa'deh A, Meinel C. Multicore-based auto-scaling secure neighbor discovery for windows operating systems. Proceedings of the IEEE International Conference on Information Networking, Bali, 2012: 269~274
- 13 Alsa'deh A, Feng C, Meinel C. CS-CGA: compact and more secure CGA. Proceedings of the IEEE International Conference on Networks, Singapore, 2011:299~304
- 14 Siddiqi Q S, Anwar M U. A study of CGA- (cryptographically generated address) signature based authentication of binding update messages in low-end MIPv6 node. Proceedings of the IEEE International Conference on Computer and Communication Engineering, Kuala Lumpur, Malaysia, 2012:510~514
- 15 AlSa'deh A, Rafiee H, Meinel C. Stopping time condition for practical IPv6 cryptographically generated addresses. Proceedings of the IEEE International Conference on Information Networking, Bali, 2012: 257~262
- 16 Su G X, Wang W D, Gong X Y. A quick CGA generation method. Proceedings of the IEEE International Conference on Future Computer and Communication, Wuhan, China, 2010: 769~773
- 17 Rafiee H, AlSa'deh A, Meinel C. Winsend: windows secure neighbor discovery. Proceedings of the ACM International Conference on Security of Information and Networks, Sydney, Australia, 2011: 243~246
- 18 Hou Y, Wang Z X, Wang Y, *et al.* Routing attack in the ND and SEND mixed environment. Proceedings of the IEEE International Conference on Multimedia Information Networking and Security, Nanjing, China, 2012:959~962
- 19 Jinhua G, Kejian X. ARP spoofing detection algorithm using ICMP protocol. Proceedings of 2013 International Conference on Computer Communication and Informatics (ICCCI), Paris, France, 2013:1~6
- 20 Pandey P. Prevention of ARP spoofing: a probe packet based technique. Proceedings of Advance Computing Conference (IACC), 2013 IEEE 3rd International, Los Angeles, USA, 2013: 147~153

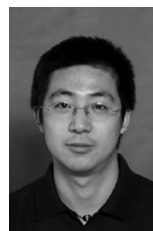
[作者简介]



宋广佳,男,哈尔滨工业大学博士生、讲师,主要研究方向为 IPv6 网络、网络安全、学术信誉度评价。



季振洲,男,博士,哈尔滨工业大学教授,主要研究方向为高级计算机体系结构、并行计算技术、计算机网络安全和 QoS 体系。



王晖,男,博士,现就职于国家计算机网络应急技术处理与协调中心,主要研究方向为网络建模和卫星宽带网络拥塞控制。

(收稿日期:2014-03-10)