



基于终端可信度的路由策略设计与实现

殷安生, 张顺颐

(南京邮电大学, 江苏 南京 210003)

摘要:可信路由随着可信网络的发展而兴起,目前的研究主要集中在轻量化网络的路由策略方面,存在的问题主要有路由算法开销大、应用范围小,且主要以 IPv4 为基础。提出了一种基于 IPv6 流标签定制的可信路由方案,在终端的可信评估基础上,通过流识别和流标记实现可信路由策略。利用前驱 ARP 代理机制设计了一种基于代理的虚拟链路协议,并设计了原型系统。实验证明,该协议实现了 IPv6 的流标记路由,提高了信息传输的安全性和效率。

关键词:可信路由;IPv6;流标签;前驱 ARP 代理

中图分类号:TP393

文献标识码:A

doi: 10.11959/j.issn.1000-0801.2016084

Design and implementation of routing strategy based on terminal trust

YIN Ansheng, ZHANG Shunyi

Nanjing University of Posts and Telecommunications, Nanjing 210003, China

Abstract: With the development of trusted networks, trusted routing emerges. Currently, the research focuses on the routing strategies of lightweight network. The routing algorithm has the large overhead and small applications, which is mainly based on IPv4. A trusted routing scheme was presented based on the flow label of IPv6, which was achieved by adding a flow identification module to TNC(trusted network connection)module. Drawing on previous proxy ARP, a proxy-based virtual link protocol and prototype system was designed. Experiments show that this protocol can achieve IPv6 routing based on flow label and improve the security and efficiency of information transmission.

Key words: trusted routing, IPv6, flow label, previous proxy ARP

1 引言

常规的路由协议都是假设网络中所有的终端皆为可信终端,然而诸如 DoS 攻击、自私性攻击、修改序列号攻

击、修改路由跳数攻击、黑洞攻击^[1]等攻击越来越频繁。可信路由是随着可信网络的发展而兴起的研究方向,主要是指路由协议能够实现流的可信转发。现有研究利用密码学机制提出了基于动态源路由协议的 ARIADNE^[2]、基于 AODV

收稿日期:2015-09-09;修回日期:2016-02-28

基金项目:国家自然科学基金资助项目(No. 61003237);江苏省科技成果转化专项资金资助项目(No.BA2012047);南京邮电大学校科研基金资助项目(No. NYS213026, No.JG00915JX95)

Foundation Items: The National Natural Science Foundation of China(No. 61003237), Special Fund for the Transformation of Scientific and Technological Achievements of Jiangsu Province(No.BA2012047), Science Foundation of NUPT(No.NYS213026, No.JG00915JX95)



的 SAODV^[3]等;参考文献[4]将可信度的机制融入 TORA 路由协议;参考文献[5]提出了基于模糊理论的 FTSODV 可信路由协议、基于信息论框架^[6]的可信路由的方案等。然而基于密码学的路由算法开销太大,基于目前特定结构的路由算法应用范围太小,基于信誉度的路由协议多聚焦在路由器本身的属性,因此这些路由协议都有一定的局限性。另外由于目前主流的 IP 地址协议为 IPv4,因而目前的路由协议基本都以 IPv4 为基础。

本文提出了一种基于 IPv6 流标签定制的可信路由策略。首先计算终端可信度,将计算结果根据安全策略映射到 IPv6 的流标签上,路由器在接收到流后,查看流的标记,选择合适的转发路径并根据事先设定的策略有区别的对这些流进行存储转发。

2 基于 IPv6 的流标记方法

在 IPv6 下实现网络流量识别的主要问题在于 IPv6 对 IP 数据报格式和 IP 地址表示方式与 IPv4 不同。由于采用分析数据报头的方法可以实现对流量的识别与控制,本文将 对 IPv6 报头中的有关字段进行设计,从而实现 IPv6 下的流识别。

在 IPv4 网络中,流的识别和标记可以通过五元组<源地址,目的地址,源端口号,目的端口号,传输协议>来标识,但是在 IPv6 网络中,由于存在分片和加密等行为,使用报头来定位一个流变得不可行。但是通过定义流标签,可以通过源地址域、目的地址域与流标签域来标识一个 IPv6 流。

使用 20 bit 流标签来标识流,考虑到安全和服务质量,需要使用聚合流,所以使用 2~14 bit 为聚合流标识;14~20 bit 为单流标识(与源目地址一起标识一个流),流标签的生命期仍然为 120 s。

流标签格式如图 1 所示,共分为 4 个功能部分:0~2 bit 为标识位;2~8 bit 为终端可信参数;9~14 bit 为服务质量参数;15~20 bit 为单流标识。

使用前两位为标识位,00 表示尽力而为;01 表示所有路由器都要遵循的标准值;10 为自定义(只在本地有意义);11 为保留,未使用。

2~8 bit 为可信网络参数,其中,2~4 bit 为传输路径可

信度,5~8 bit 为终端可信度,可以有 64 种分级策略,基本满足可信度评估的需要。

实验证明^[8],QoS 最重要的参数为传输时延、抖动、分组丢失率,这 3 个参数基本能够表述 QoS 的状态。可以有 64 种分级策略,能够满足区分服务的要求。

3 基于流标记的可信路由

本文提出的可信路由指的是利用得到的终端和链路可信度,通过流标记策略对每个流赋予一个可信度。可信路由就是在路由器端通过检查流的标识,然后根据设定的策略执行相应的转发策略,根据不同的安全等级选择不同的转发路径。在安全性要求高的网络中按照可信度来确定路由策略,对于可信等级高的流,设定其优先级比可信度低的流的优先级高,在路由器中,优先转发可信等级高的流,如果发生了阻塞,则优先丢弃可信度低的流。

3.1 可信流控策略

整个系统分为两个模块:流标记与管理及基于流识别的可信路由。系统首先按照可信网络的实际需求制定安全策略,根据终端可信度的判决结果划分流类别,设定相应的流标签值,赋予各安全策略的流相应类别的等级。然后按策略管理器提供的分类策略对流进行实时、精确的分类和处理。基于可信度的路由器流控模型如图 2 所示。

在执行转发策略时,根据 IPv6 协议中标识的网络流类别信息值,综合选择不同的队列管理方法、分组调度方法和策略选路。如采用基于可信等级的加权随机早期丢弃,实现报文按优先级丢弃,防止链路早期拥塞;采用加权循环调度算法实现多种业务安全等级按策略合理分配带宽,让权重与依据安全等级分配的带宽成比例,从而提供不同服务类型的调度转发服务。

路由器在转发时根据业务类的安全/QoS 要求,选择合适的备选路径进行转发。对于高安全需求的流量,路由器会根据流标签值选择保密性强、安全性高、可靠性高的路径进行转发;对于视频流,就可以选择低时延特性的路径进行转发;而消耗大量带宽的 P2P 业务则选择尽力而为的路径进行转发。路径选择策略可借鉴最高/最低信任法^[9],首先剔除路径中链路信任值低于最低信任阈值的路径,再从备选路径中选择综合信任值最高的路径。



图 1 流标签格式

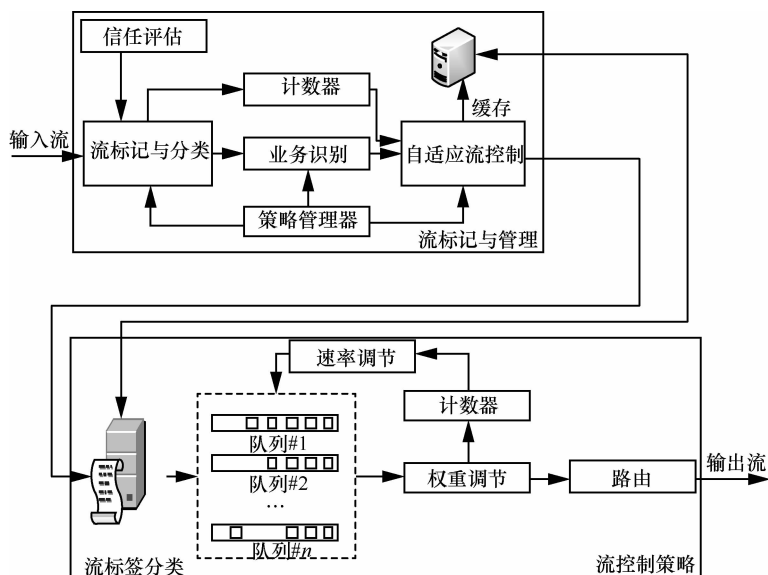


图2 可信策略流控模型

3.2 选路算法

选路算法就是根据业务的安全或者 QoS 需求选择相应的路径。业务的 QoS 需求主要考虑链路的带宽、时延、抖动、差错率、误码率等,在路由算法上已有很多成熟的模型或应用,不再赘述。本文提出了基于终端可信度的路由策略,主要针对业务的安全需求,就是为有安全要求的业务提供一条安全的转发链路。本文设计了一种最大最小值(max-min)法实现相应的路由策略,该方法的设计思想是在路由拓扑中选择一条综合考虑可信度与链路长度的路径,也就是尽可能地选择可信度大的节点和链路来转发数据,同时又不显著增加链路的长度,这里假设链路长度和分组传输时间成正比。

假设路由拓扑如图3所示,其中所有链路和终端(在这里承担路由功能)的可信度已知。S为发送节点,R为接收节点,从图3中可知,节点的可信度为0.7,发送节点S到 N_1 的链路可信度为0.81。

所有链路都是双向的,也就是说链路可信度体现的是这条链路上双向通信用可信度的程度。在运行路由算法之前要对路由拓扑进行剪枝,剔除不符合安全要求的终端和链路,再在剩下的路由拓扑中选择合适的链路。在这里通过设置终端可信度和链路可信度的阈值来实现,可信度的阈值参考流标签中的可信网络参数来确定。本文设置链路和终端的可信度阈值为0.6,如图4所示,删除阈值低于0.6的链路和终端。

由于采用的是全局信任模型,因此发送节点了解整个网络中各转发节点的可信度和链路可信度。在选择转发路径时,从发送节点出发,首先选择一条最可信的第一步转发链路,选择时考虑的要点有两个:终端可信度和链路可信度的和最大;终端可信度和链路可信度的差值最小。由于所处网络环境的不同,在计算终端可信度和链路可信度的和时,链路可信度和终端可信度的重要性可以通过分配不同的权值来体现,在本文中,为便于理解,将终端可信度

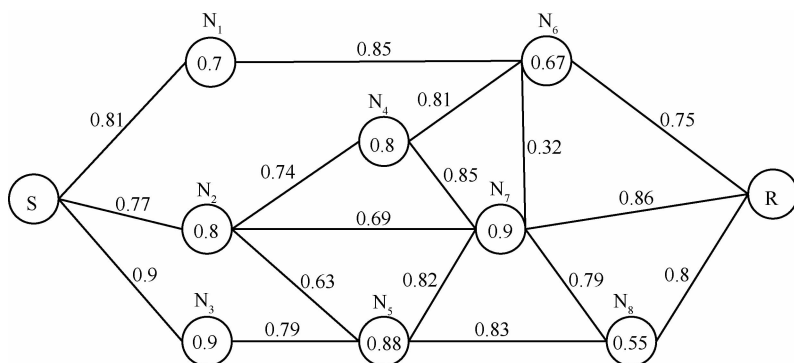


图3 路由拓扑

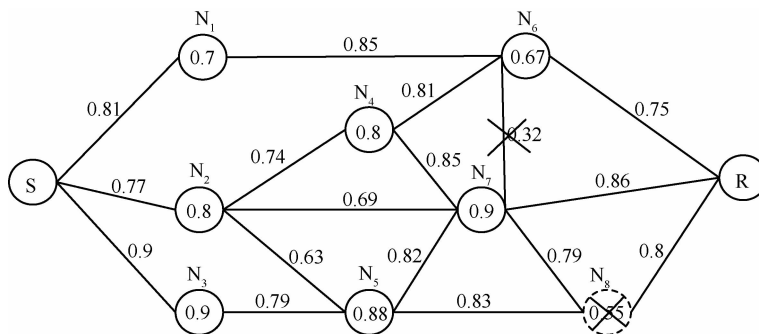


图4 路由拓扑剪枝

和链路可信度的权值设置为相同值。

设终端可信度为 t_n , 链路可信度为 t_l , 发送节点 S 和接收节点 R 的可信度在计算时设置为 1。

由节点 S 出发, 假设每一条链路和其链接的一端组成了一条路径, 那么该路径的可信度为 $\frac{t_n - t_l}{t_n + t_l}$ 。寻找 S 和 R 之

间的可信路径, 就是从 S 出发, 首先计算出与 S 相邻的所有路径的可信度, 从中选择一条可信度最高的路径作为 S 的第一步转发路径, 然后再从这条路径出发计算与此条路径相邻的其他路径的可信度, 再选择一条可信度最高的路径, 依此类推直到达到节点 R。在寻路过程中, 如果发现待计算的路径中的终端在已计算的路径中出现过, 那么此条路径不再考虑。经过计算, 在图 5 中 S 到 R 的可信转发路径为 $S \rightarrow N_3 \rightarrow N_5 \rightarrow N_7 \rightarrow R$ 。

假设每两个相邻终端之间的路径长度取值为 1, 在图 5 中转发路径长度为 4。在得到转发路径后, 需要判断路径长度是否超过规定的阈值。设路径长度阈值为 L_1 , 其取值是根据网络的规模来确定的。如果最终选择的路径长度超过 L_1 , 那么需要重新选择路径, 此时将已选择好的路径从节点 R 开始向发送节点的方向后退, 根据路径可信度依次选择次优的路径。例如在图 5 中, 从节点开始寻找次优链路, 为 $N_7 \rightarrow N_4$, 再从 N_4 开始寻找到节点 R 的最优路径, 找到

$N_4 \rightarrow N_6$ 的链路, 再从出发点利用路径可信度寻找到 R 的最优路径, 最后找到的路径为 $N_4 \rightarrow N_6 \rightarrow R$, 如果链路长度小于阈值, 则达到要求, 如仍然超过阈值则从出发寻找次优路径, 以此类推, 直到最终找到一条满足条件的路径, 其可信度局部最优且路径长度满足要求。

网络的路由根据心跳算法定时刷新。假设网络上的终端或链路可信度发生改变, 如果可信度提高则路由暂不更新, 等刷新时间到再重新选路; 如果发现有不安全的终端或链路产生, 也就是某段链路或者终端的可信度低于阈值, 则需要立即重新选路。

3.3 路由协议实现

目前, 可信路由研究主要集中在轻量化网络的路由策略研究方面^[9-12], 因此本文设计实现了一种轻量化的路由协议, 主要应用于无线网络领域, 如 Ad Hoc 网络等。

设计了一种基于前驱 ARP 代理的虚拟链路(virtual link based on previous proxy ARP, VLPPA)协议。运行 VLPPA 协议的每个终端首先主动向其邻近节点发送路由维护报文, 使各个终端能够同步网络拓扑信息并主动维护各自的拓扑表。在某个终端发起一个路由请求时, 它和目的终端通过路由探测报文和路由可达报文来设置从源终端到目的终端的一条转发路径上的代理, 从而形成一条虚拟链路, 供源终端与目的终端进行通信。VLPPA 的工作原理如图 6 所示。

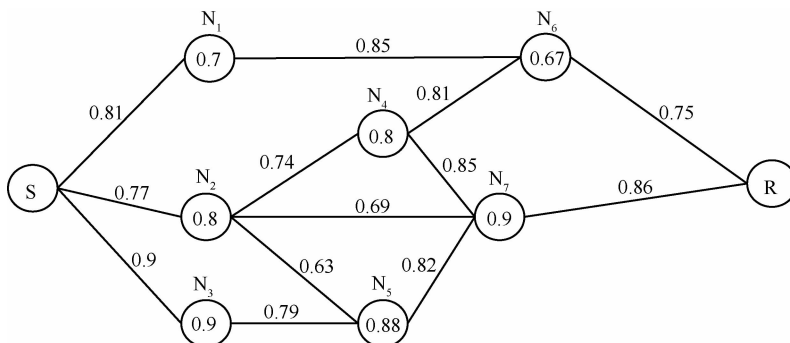


图5 转发路径

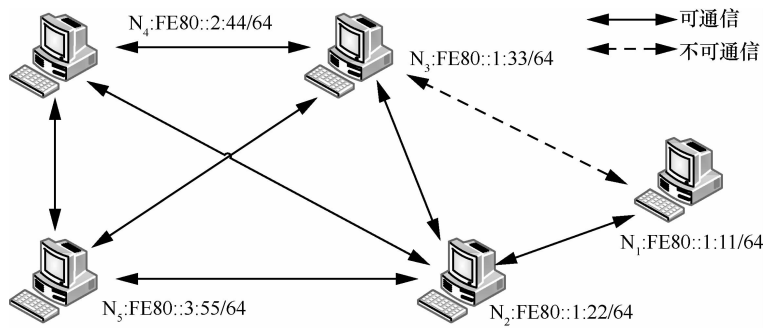


图6 VLPPA 的工作原理

如图6所示,由于终端 N_1 与终端 N_3 不能直接进行通信,所以当终端 N_1 想发送一个数据分组 $packet_{13}$ 给终端 N_3 时,只要将 $packet_{13}$ 首先发送到终端 N_2 ,此后再由终端 N_2 转发到终端 N_3 就可以了。由于 $packet_{13}$ 在局域网内部首先会打包成MAC帧,目的MAC地址决定了MAC帧的发送方向,因此,应当把 $packet_{13}$ 所在的MAC帧的目的MAC地址设为终端 N_3 的MAC地址,将 $packet_{13}$ 的目的IP地址设为终端 N_3 的IP地址。这样,终端 N_2 将收到 $packet_{13}$ 之后,终端 N_2 判断此分组的目的MAC地址是终端 N_2 本身,而目的IP地址是其他主机,因此 $packet_{13}$ 需要路由转发,终端 N_2 将按照相应的路由协议找到 $packet_{13}$ 报文的下一跳。由于终端 N_3 与终端 N_2 直连,因此终端 N_2 将 $packet_{13}$ 报文封装成新的MAC帧,其目的MAC地址设为终端 N_3 的MAC地址,这样, $packet_{13}$ 将被转发往终端 N_3 。上述流程完成之后, $packet_{13}$ 就能发送到终端 N_3 。目前主要的难点在于

如何让终端 N_1 得知哪一个下一跳节点能够将 $packet_{13}$ 转发到终端 N_3 。

不同于一般的ARP代理机制,本文提出了一种前驱ARP代理机制。终端 N_1 可以通过路由协议率先获知通往 N_3 终端的最短路径上的下一跳节点是 N_2 ,从而直接将发往终端 N_3 的 $packet_{13}$ 打包成目的MAC地址是终端 N_2 的MAC地址的MAC帧,于是不必收到终端 N_2 发回的用于伪装代理的ArpReply报文, $packet_{13}$ 就被直接发送到终端 N_2 。之后再由 N_2 转发往终端 N_3 。这种不需收到ARP应答报文即可先行设定ARP代理的方式称为前驱ARP代理。终端 N_2 就是终端 N_1 的一个代理终端。

3.4 系统架构

本节实现了一个基于VLPPA协议的软件路由器来组建多跳IP无线网络,构建了一个网络实验平台加以验证,系统框架结构如图7所示。

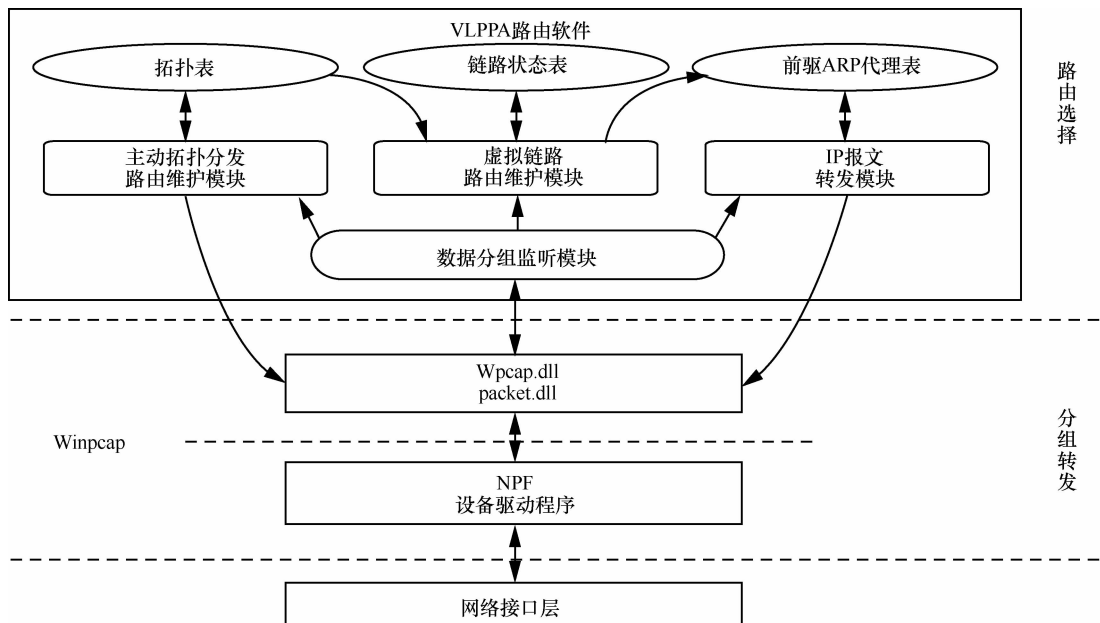


图7 系统框架结构



VLPPA 路由软件运行于用户级,通过调用底层的 Winpcap 提供的各种接口函数来完成对物理层网卡的各种控制操作。

VLPPA 路由软件主要包括三大模块以及 3 张表:数据分组监听模块、VLPPA 路由维护模块和 IP 报文转发模块;拓朴表、链路状态表和前驱 ARP 代理表。数据分组监听模块利用 Winpcap 驱动接口函数,实时捕获所有经过网卡端口的数据分组,并对其进行分析。适配器获取数据分组之后,数据分组监听模块将启动,并判断其是否为 ARP 分组,然后提交给 ARPPacketProc 函数进行处理,该函数主要判断该数据分组是否为路由请求。然后判断是否为 IP 数据分组,如果是,则提交给 IP 报文转发模块进行相应的处理;如果不是,再判断该分组是否为路由控制报文。如果是,则将其提交给路由控制模块进行处理;否则,将其提交给超时处理模块或异常处理模块。

4 实验结果分析

本文设计了一种无线网络中的实验环境,假设网络中存在善意终端和恶意终端,恶意终端可能会发起灰洞、DDoS、诽谤攻击等。设定实验环境中共有 100 个终端,以参考文献[10]中汇总的实验参数作为默认的参数。

选择经典的路由协议 GPSR^[13]以及一个轻量化的路由协议 TSRF^[10]进行比较。TSRF 协议是一个轻量化的抵御各种恶意攻击的路由框架,基于信任值实现,路由建立的过程主要包括获取信任及传统的路由发现机制。由于 GPSR 协议没有获取信任值,所以其路由建立时间很短,但如果加入信誉值广播的过程,则需要极大时间来建立路由。TSRF 协议基于半环理论寻找最优路径,节省了重复计算的时间。而 VLPPA 协议使用前驱 ARP 代理协议,由于前驱 ARP 代理机制选取代理节点时不是通过代理节点本身返回 ARP 应答报文来设定,而是相应的路由协议在源节点端设定,省去了 ARP 应答过程带来的开销,节省了路由建立时间。根据最大最小法来选择链接,节省了全局广播的过程和时间。从图 8 可以看出,在和 GPSR+TSRF 协议比较时,当平均路由长度达到 8 时,VLPPA 协议能节省 45% 的路由建立时间。从图 9 可以看出,当平均邻居节点数量达到 14 时,VLPPA 协议能够节省 32.2% 的路由建立时间。VLPPA 协议通过流标签来建立路由,所以相对 TSRF 协议来说其收敛速度更快。

为了验证 VLPPA 协议的安全性,假设恶意终端会发

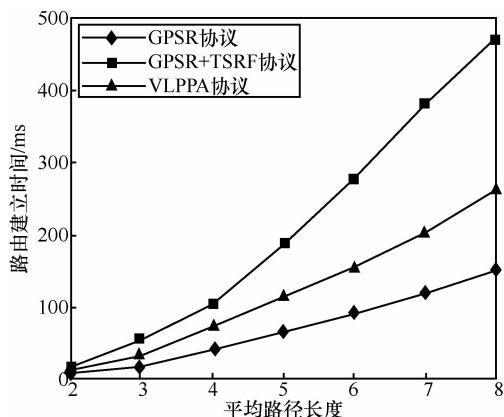


图 8 路由建立时间 (平均路径长度)

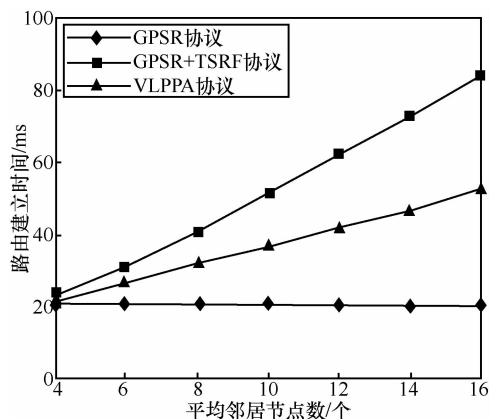


图 9 路由建立时间 (平均邻居节点数)

起灰洞、DDoS、诽谤攻击等,各类攻击占比相同。在图 10 中,比较以不同速率发起恶意攻击时路由的恢复时间,为便于计算,假设终端一旦发生恶意攻击行为即被系统发现。从图 10 可以看出,在短时间内恶意节点发起攻击并被检测到的数量越多,路由恢复时间越长,这是由于单位时间内恶意终端不断产生,导致路由由不断重选路,这样平均选路时间就会不断增加,极端情况甚至会产生路由震荡。同时随着时间的增加,恶意终端越来越多,路由拓扑越来越简单,路由恢复的时间又越来越短。与 TSRF 相比,随着恶意节点的增多,VLPPA 能较早摆脱恶意行为的影响,最终减小了路由选路的时间。

假设到第 2 s 时,恶意终端发起攻击(包括灰洞、DDoS、诽谤攻击等),各类攻击占比相同。以恶意终端成功丢弃一个路由数据分组或成功进行了垃圾数据分组的发送为攻击成功,验证了不同攻击速率下,本路由协议对恶意行为的抑制效果,结果如图 11 所示。

从图 11 可以看出,随着路由策略的执行,不断剔除有恶意行为的终端,其对网络恶意行为的抑制效果明显。在

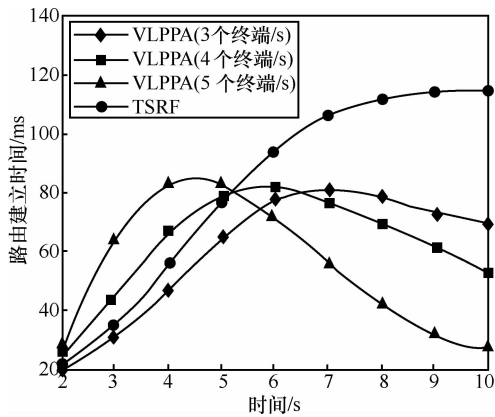


图 10 不同攻击速率下的重路由时间

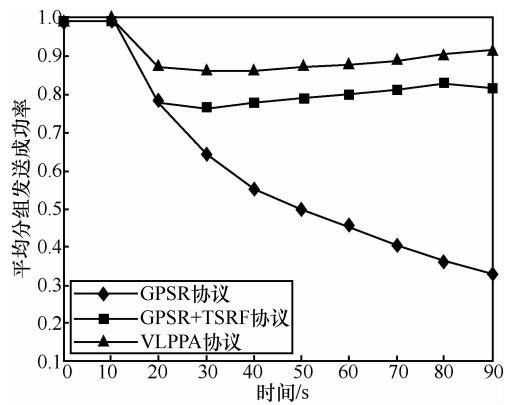


图 12 平均分组发送成功率

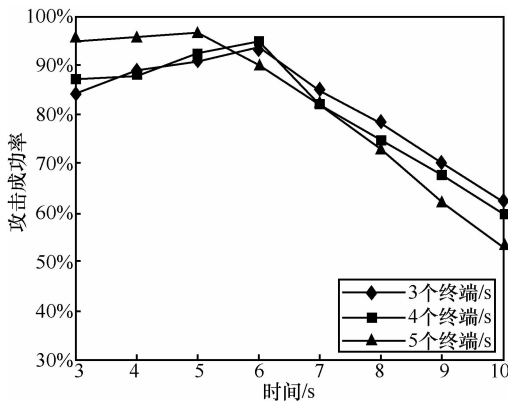


图 11 VLPPA 协议对恶意行为的抑制效果

本文设置的可信度阈值为 0.6, 如果增加可信度阈值, 那么可以增强对恶意攻击行为的抑制, 但同时带来的是对路由路径的破坏和路由转发时间的提高。

利用分组发送成功率来检验算法的应用效果, 以分组平均转发成功率为指标, 假设恶意终端占比为 50%, 如图 12 所示, 到第 10 s 时, 恶意终端发起攻击, 从图 12 可以看出, VLPPA 协议能够有效地确保数据分组的传送。

如图 12 所示, 随着时间增加, 不考虑终端信誉值的 GPSR 协议的安全性急剧下降, 而 TSRF 协议在发现恶意终端时能快速发起一个路由更新以发现一个可信路径, 然而 TSRF 协议只是寻找一个局部最优解, 所以和使用 max-min 法的 VLPPA 协议相比, 其分组丢失率要更高。

5 结束语

本文提出一种基于 IPv6 和流标记的可信路由策略, 对不同终端在网络中的流, 根据其可信度的差别制定不同的策略。通过和其他无线路由协议的比较, 证明 VLPPA 协议切实可行, 且在效率和安全性上都有提高。

下一步的工作主要集中在提高路由在大规模网络中的适应性。

参考文献:

- [1] 崔莹. 基于信任度模型的 Ad Hoc 网络安全路由[D]. 南京: 南京航空航天大学, 2007.
CUI Y. Secure routing algorithm based on trust model for Ad Hoc network[D]. Nanjing: Nanjing University of Aeronautics and Astronautics, 2007.
- [2] HU Y C, PERRIG A, JOHNSON D B. Ariadne: a secure on-demand routing protocol for ad hoc Networks [J]. Wireless Networks, 2002, 11(1-2): 21-38.
- [3] ZAPATA M G. Secure ad hoc on-demand distance vector routing [J]. ACM Mobile Computing and Communications Review, 2006, 6(3): 106-107.
- [4] PIRZADA A A, DATTA A, MCDONALD C. Propagating trust in ad-hoc networks for reliable routing [C]//2004 International Workshop on Wireless Ad-Hoc Networks, May 31-June 3, 2004, Oulu, Finland. New Jersey: IEEE Press, 2004: 58-62.
- [5] MANICKAM J M L, SHANMUGAVEL S. Fuzzy based trusted Ad hoc on-demand distance vector routing protocol for MANET[C]// Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, October 8-10, 2007, White Plains, NY, USA. New Jersey: IEEE Press, 2007: 39.
- [6] LINDSAY S Y, WEI Y, ZHU H, et al. Information theoretic framework of trust modeling and evaluation for ad hoc networks[J]. Selected Areas in Communications, 2006(24): 305-317.
- [7] CHEN Y X, BU T M, ZHANG M, et al. Max-minimum algorithm for trust transitivity in trustworthy networks[C]//IEEE/WIC/ACM International Joint Conferences on Web Intelligence and Intelligent Agent Technologies, September 15-18, 2009, Milan, Italy. New Jersey: IEEE Press, 2009: 62-64.



- [8] LEMESHKO O V, YEVSEYEVA O Y, GARKUSHA S V. A tensor model of multipath routing based on multiple QoS metrics [C]//International Siberian Conference on Control and Communications (SIBCON), September 12-13, 2013, Tomsk, Russia. New Jersey: IEEE Press, 2013: 1-4.
- [9] XIA H, JIA Z, LI X, et al. Trust prediction and trust-based source routing in mobile ad hoc networks[J]. Ad Hoc Networks, 2013, 11(7): 2096-2114.
- [10] DUAN J Q, YANG D, ZHU H Q, et al. TSRF: a trust-aware secure routing framework in wireless sensor networks [J]. International Journal of Distributed Sensor Networks, 2014(1): 1-14.
- [11] ABUSALAH L, KHOKHAR A, GUIZANI M. Trust aware routing in mobile ad hoc networks [C]//The IEEE Telecommunications Conference(GLOBECOM'06), November 27- December 1, 2006, San Francisco, USA. New Jersey: IEEE Press, 2006: 1-5.
- [12] PARIS S, NITA-ROTARU C, MARTIGNON C, et al. EFW: a cross-layer metric for reliable routing in wireless mesh networks with selfish participant [C]//The IEEE INFOCOM 2011, April 10-15, 2011, Shanghai, China. New Jersey: IEEE Press, 2011: 576-580.
- [13] SUN Y L, YU W, HAN Z. Information theoretic framework of trust modeling and evaluation for ad hoc networks [J]. IEEE Journal on Selected Areas in Communications, 2006, 24 (2): 305-315.

[作者简介]



殷安生(1982-),男,博士,南京邮电大学讲师,主要研究方向为可信网络。



张顺颐(1944-),男,博士,南京邮电大学教授、博士生导师、原副校长,中国通信学会学士、理事,IP应用与增值电信技术委员会主任,中国电子学会通信学分会副主任,主要研究方向为计算机通信网络和电信业务及其管理。多次承担国家和省部级科研项目,12次获得省部级科技进步奖。目前的研究方向是计算机通信网络、电信业务和信息系统建设。