软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(9):2829−2843 [doi: 10.13328/j.cnki.jos.005273]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于信任机制的机会网络安全路由决策方法*

李 峰[1], 司亚利[2,3], 陈 真[3], 鲁 宁[1], 申利民[3]

[1](东北大学 秦皇岛分校计算机与通信工程学院,河北 秦皇岛 066004)

[2](燕山大学 里仁学院,河北 秦皇岛 066004)

[3](燕山大学 信息科学与工程学院,河北 秦皇岛 066004)

通讯作者: 李峰, 申利民, E-mail: lifeng@neuq.edu.cn, shenllmm@ysu.edu.cn

摘 要: 提出一种基于信任机制的机会网络安全路由决策方法 TOR,该方法在节点中引入信任向量的数据结构,记录节点携带消息能力的信任度.采用层状硬币模型和数字签名机制,在消息传递过程中将节点签名的转发证据动态捆绑到消息包上,依靠消息携带方式实现证据链的采集.周期性地将具有签名和时间戳的信任向量表通过洪泛方式反馈到网络中,在每个节点,迭代形成一个由多维行向量集组成的只读可信路由表 TRT,作为选择下一跳节点和副本分割策略的决策依据.在节点相遇时,选择信任度比自身大的作为下一跳转发节点,消息沿着信任梯度递增的方向传递.实验结果表明:与现有路由算法相比,TOR 算法能够有效抑制恶意节点和自私节点的破坏行为,且具有较高的消息传递成功率和较低的消息转发平均时延,对缓存空间和计算能力要求较低.

关键词: 机会网络;信任机制;可信路由表;信任度;消息副本

中图法分类号: TP393

中文引用格式: 李峰,司亚利,陈真,鲁宁,申利民.基于信任机制的机会网络安全路由决策方法.软件学报,2018,29(9):2829−2843. http://www.jos.org.cn/1000-9825/5273.htm

英文引用格式: Li F, Si YL, Chen Z, Lu N, Shen LM. Trust-Based security routing decision method for opportunistic networks. Ruan Jian Xue Bao/Journal of Software, 2018,29(9):2829−2843 (in Chinese). http://www.jos.org.cn/1000-9825/5273.htm

Trust-Based Security Routing Decision Method for Opportunistic Networks

LI Feng[1], SI Ya-Li[2,3], CHEN Zhen[3], LU Ning[1], SHEN Li-Min[3]

[1](Computer and Communication Engineering College, Northeastern University at Qinhuangdao, Qinhuangdao 066004, China)

[2](LiRen College, Yanshan University, Qinhuangdao 066004, China)

[3](Information Science and Engineering College, Yanshan University, Qinhuangdao 066004, China)

Abstract: This paper proposes a security opportunistic routing decision method based on trust mechanism (TOR). In this scheme, every node locally maintains a trust vector to record trust degree of other nodes, which indicates their ability of carry and forward messages. Using layered coin model and digital signature mechanism, the forwarding evidences of relay node signature are bound dynamically on message packet during the relay process, and the message carries evidence chain to the destination node. The node broadcasts periodically the trust vector with signature and time-stamp to network by flooding. Through multi-iteration, the read-only trust routing table (TRT) with multidimensional row vectors is built on every node, which will become the key-player of selecting the next-hop relay node and dividing copy number. The node with greater trust degree is taken as the next-hop relay node. Therefore, the message can be delivered to the destination along the direction of trust gradient increment. Simulation results show that compared with existing algorithms, TOR

* 基金项目: 国家自然科学基金(61300193, 61272125, 61601107); 河北省自然科学基金(F2015501105, F2017203307, F2015501122); 中央高校基本科研业务费专项基金(N120323012)

Foundation item: National Natural Science Foundation of China (61300193, 61272125, 61601107); Natural Science Foundation of Hebei Province (F2015501105, F2017203307, F2015501122); Fundamental Research Funds for the Central Universities (N120323012)

收稿时间: 2015-09-21; 修改时间: 2016-05-11, 2016-08-29; 采用时间: 2017-02-15; jos 在线出版时间: 2017-03-31

CNKI 网络优先出版: 2017-03-31 21:54:43, http://kns.cnki.net/kcms/detail/11.2560.TP.20170331.2154.007.html

algorithm can resist the network destruction behavior of malicious nodes and selfish nodes with higher probability of delivery and lower average delivery delay, and it only needs very small buffer and computing ability of node.

Key words: opportunistic networks; trust mechanism; trust degree; message copy

近年来,机会网络作为一种新型自组织网络受到了国内外研究者的关注,在野外动物追踪、车载网络等领域得到了广泛应用.机会网络节点具有典型的移动性、开放性和稀疏性的特征,节点的相遇率较低缺乏固定和有保障的连通链路,一般采用“存储-携带-转发”机制,依靠节点移动带来的机会实现路由[1,2],这种模式需要所有节点都自愿协作转发其他节点的路由消息.然而,在开放的机会网络中存在某些自私节点不愿意参与网络协作,甚至有一些恶意节点利用恶意丢包、篡改包或产生垃圾消息包等黑洞攻击形式破坏网络的路由机制[3],导致整个网络消息包的转发成功率和转发效率降低,增加了网络的平均消息转发延迟时间.如何有效地解决节点的自私问题及抵御恶意攻击,提高消息转发性能,成为设计安全高效的机会网络路由协议的关键问题.

现有的传染转发(epidemic)、PROPHET、SAW、MaxProp 以及相遇预测等路由技术,只考虑网络转发成功率和时延等性能问题,比较适用于安全稳定的网络环境,而在具有自私节点和恶意节点的环境其性能将会导致急剧下降.对于节点自私和恶意行为的检测,传统 P2P 网络和 MANET 网络一般采用信任或声誉等激励机制来解决,通过监视狗或反馈机制收集邻居节点的信任证据,利用信任或声誉评估算法动态计算邻居节点的信任度,信任度大小反映节点行为的优劣;还有研究基于虚拟货币的经济学合作模型激励网络中的自私节点主动合作,每个节点通过为邻居节点提供转发服务赚取虚拟货币,而通过支付虚拟货币来让其他节点协助转发数据包,从而激励网络节点自愿提供转发服务.然而,由于机会网络中节点的能量、计算能力、网络带宽和缓存空间的限制,以及节点连接的不稳定性和不确定性,使得已有信任建模方案很难直接应用到机会网络,问题如下.

(1) 难以准确及时地收集直接信任证据.由于节点具有动态性,有可能将消息传递到下一跳节点之后就离开连通域,因此无法采用邻居节点监视的方式收集是否成功转发的证据;

(2) 缺乏可信的授权中心.节点连接的多跳性和间断性,导致无法存在可信授权中心来验证下一跳节点的合法性,因为假设存在集中认证授权中心,当通过多跳路由获取验证信息之后,下一跳转发节点可能离开了连通范围,致使验证信息失效错失转发机会;

(3) 节点的计算能力和缓存空间受限.已有的信任建模方案在信任证据获取、信任关系维护和评估以及存储空间等方面需要花费较大的代价,但是资源受限的机会网络中节点需要付出尽可能小的代价实现信任管理,而以较多的资源实现“存储-携带-转发”的路由任务.

针对上述问题,提出了一种基于信任机制的机会网络安全路由方法 TOR(trust-based opportunity routing),TOR 采用捆绑携带机制,在消息包转发过程中动态捆绑中间节点转发证据;目的节点接收到消息包后,依据其携带的转发证据,对本次参与消息转发的中间节点进行信任度评估形成或更新信任路由表信息,利用信任广播方式周期性地将最新信任路由表反馈给网络中的节点,使每个节点都维护到目的节点的信任路由表,简化了传统信任关系评估和传播的复杂性,节点只付出较小的存储和计算代价维护信任路由表.在消息转发过程中,TOR 采用沿着信任度递增的梯度转发,若当前节点与目的节点位于同一连通域,则直接转发;否则,转发给当前连通域内到达目的节点可信度最高的节点.该转发方法易发现到达目的节点的最佳路径,提高了整个网络的消息转发成功率,降低了网络平均消息转发时延,并且利用信任路由表可以有效抵御节点的自私行为和黑洞攻击等恶意行为.

1 相关工作

2014 年,Zhu 通过建立有效的信任机制实现了一种概率化的恶意行为检测方案 iTrust[4],在网络中引入可信授权节点 TA 来收集网络路由证据,基于收集的证据 TA,周期性检测节点的行为,从而以较小的代价保障机会路由的安全性.2013 年,李云提出了一种基于买卖模型的节点激励策略 BIP[5],BIP 策略采用货币支付模式,综合考虑节点自身资源、拥有的虚拟货币以及消息属性对消息进行定价,从而激励自私节点合作.2010 年,Lu 提出了一种有效的激励协议 Pi[6],Pi 协议在 Bundle 消息转发过程中通过附加一些激励信息,激励自私节点自愿公平的转

发其他节点的 Bundle 消息,利用可信授权中心为中间转发的声誉和信用进行奖励,采用层状硬币模型和双线性加密签名技术实现可靠授权和转发信息的完整性保护机制.2012 年,Erman 提出了基于迭代算法的信任和声誉机制 ITRM[7],ITRM 利用有向图描述节点的信任关系,通过迭代算法评价节点的信任度和检测节点的恶意行为,并将恶意节点加入“黑名单”隔离.ITRM 是一种纯分布式的不需要集中授权中心,具有较好的健壮性;但 ITRM 的建立和维护算法复杂,对节点资源的消耗较大.2009 年,Nelson 提出了一种基于相遇预测的路由转发机制 ERB[8],网络中每个节点维护一个与其他节点相遇概率的列表,采用基于定量的多副本转发策略,消息转发的副本数由相遇概率智能决策,节点能耗开销较小,消息副本分割规则简单,但没有解决自私问题和共谋问题. 2013 年,Chen 提出了一种应用于容延网络安全路由的动态信任管理协议[9],该协议从 QoS 和社会信任两方面,采用传统的直接信任和推荐信任相结合的方法评估网络节点的信任度,每个节点内有一个朋友列表,节点相遇时互换和共享列表中的信息(只互换共有朋友信息),利用相遇矩阵描述节点间的连通性和计算相遇概率,但节点信任评价开销较大,证据获取延迟较高.2012 年,Li 提出了一种分布式的消息包恶意丢弃行为检测方案[10],该方案中,每个节点维护一个具有签名的接触记录表,当两个节点相遇时互换历史接触记录表,依据历史接触信息判断节点是否有恶意丢包行为;对于恶意节点,通过共谋伪造接触记录表的情况,利用随机证人行为一致性检测方法实现共谋行为的识别.2009 年,Li 提出了一种基于相遇票据的证据安全保障方法[11],该方法利用可信 PKI 两个节点相遇时互相用各自的私钥对票据进行数字签名,有效防止了恶意节点对票据的篡改;并且采用 D-S 证据理论推断相遇节点的转发能力,提高了下一跳转发节点预测的准确性.2010 年,Chen 针对容延网络设计了一个基于信誉的激励系统 MobiCent[12],该系统采用激励机制对节点的转发行为进行奖励和惩罚,保证了路由协议能够发现有效的转发路径.2007 年,Burgess 为了验证恶意攻击对 DTN 网络的影响,设计了 UMass DieselNet 和 Haggle 两个网络系统[13],通过长期跟踪网络的连通性,分析恶意行为对路由攻击的有效性.实验表明:多副本路由是抑制恶意节点攻击的最有效方式,尤其是抑制恶意丢包和篡改数据包攻击最有效.2013 年,Zhao 提出了一种适用于周期性移动 AdHoc 网络的信任管理方案 CTrust[14],该方案在信任建模过程中不仅仅考虑邻居间的信任关系,而且将节点的移动位置和时间因素引入到了信任关系中,利用有向信任图表示信任关系,有效提高了节点间信任建立的准确性和效率.2013 年,王博提出了一种基于信任度和最小成本机会路由的转发算法 MCOR[15],该算法能够抵制恶意节点加入到信任邻居转发列表,以及剔除恶意链路参与到信任机会路由的建立过程,并且在吞吐量、端到端时延、期望转发次数和成本开销等方面都有很大的性能提高.2014 年,张三峰提出了一种基于最优停止理论的路由决策方法 OSDR[16],该方法将每个时隙上所遇节点和目标节点的平均相遇时间作为一个随机变量,根据该随机变量的统计特性得到一个停止观察、复制消息的规则,实现了数学期望意义上的最小消息投递延迟.

2 系统模型

采用与文献[4,6,9,10]类似的系统模型,网络中不存在集中的可信授权中心,每个节点具有一定的射频范围,只有当两个相遇节点进入射频范围时才允许互相建立连接和通信,源节点与目的节点的通信采用多跳协作转发实现.网络节点数为 n,每个节点有唯一的 iD 标识 N_i 以及对应的公私密钥对,节点初次进入网络时分配,公钥证书在节点第一次相遇时互相传播.每个节点分别有两个独立的缓存空间 B_oB_m,B_o 用来存储路由信任表,B_m 用来存储携带转发的消息包和节点自身产生的消息包.每个消息包都有唯一的 iD 标识 M_j、产生的时间戳 t、生存周期 TTL 和最大副本数 Nc,所有节点时钟同步;当消息包生存时间结束或收到消息包到达目的节点的确认消息 ACK 后,节点自动从缓存 B_m 中将其删除;当产生一个新消息或接收其他节点转发的消息时,首先检测剩余缓存空间是否满足新消息的存储要求,如果 B_m 已满或剩余缓存空间太小,则删除剩余生存时间最小的消息包.

3 基于信任策略的安全路由方法

3.1 基本思想

机会网络中节点具有周期性移动规律,如果某节点成功将消息携带到了目的节点,则将来某个时刻与此目

的节点相遇概率则很高.因此,目的节点利用以往成功携带消息的历史记录,可以较准确地预测将来哪些节点能够成功携带消息达到.基于此原则,提出基于信任机制的机会网络安全路由方法 TOR,每个节点维护一个可信路由表 TRT(trust routing table)的数据结构,TRT 采用 $n\times n$ 二维矩阵表示如公式(1):

$$TRT=\begin{bmatrix} T_{11} & T_{12} & T_{13} & \cdots & T_{1n} \\ T_{21} & T_{22} & T_{23} & \cdots & T_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ T_{n1} & T_{n2} & T_{n3} & \cdots & T_{nn} \end{bmatrix} \tag{1}$$

其中,T_{ji} 表示目的节点 N_j 对转发节点 N_i 的信任程度,反映节点 N_i 将消息携带到目的节点 N_j 的能力.TRT 中的行向量 $T_j=(T_{j1},T_{j2},T_{j3},\ldots,T_{jn})$表示目的节点 N_j 对网络中各个转发节点的信任度,该向量数据由节点 N_j 维护和更新,并周期性的反馈到网络,当节点收到 N_j 新反馈的信任信息后对 TRT 表中的行向量 T_j 数据进行更新.列向量 $T_{*i}=(T_{1i},T_{2i},T_{3i},\ldots,T_{ni})^T$ 表示各个目的节点分别对转发节点 N_i 的信任度.

在数据转发过程中,利用行向量构成决策知识判断相遇节点携带消息到达目的节点的能力,依据路由决策方法决定是否将携带的消息转发给下一跳节点,而利用列向量构成决策知识判断源节点产生消息的可靠性,防止垃圾消息包的转发.消息转发过程如图 1 所示,节点 N_1 携带到节点 N_6 的消息 m,当节点 N_1 遇到节点 N_2 时,首先查找可信路由表 TRT 获取 T_{61},T_{62},如果 $T_{62}>T_{61}$,表明节点 N_2 携带消息 m 到达节点 N_6 的能力大于节点 N_1,是合适的下一跳转发节点,N_1 将消息 m 转发给 N_2;否则,N_1 将继续携带消息 m,直到遇到 N_6 或下一跳更可信的转发节点.

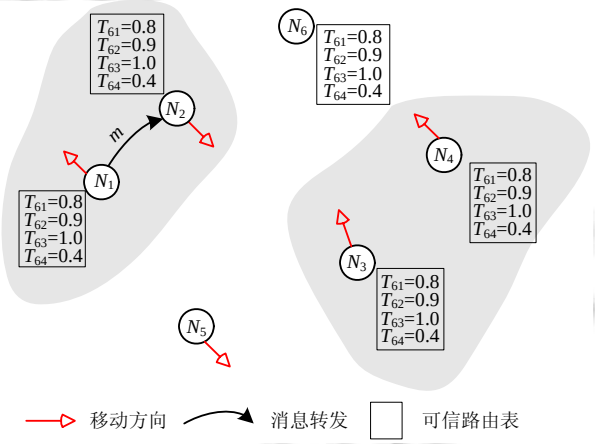


Fig.1 Message forwarding process based on trust

图 1 基于信任的消息转发过程

3.2 转发证据采集

消息从源节点传递到目的节点需要经过多个中间节点,如图 2 所示,源节点 N_0 将消息传递到目的节点 N_k,需要经过传输链 $Path$:$N_0\rightarrow N_1\rightarrow N_2\rightarrow N_3\rightarrow N_k$,为了让目的节点及时可靠地采集到中间节点 N_1,N_2,N_3 转发消息和相遇的证据,采用捆绑携带 Captive-Carry 机制,在消息传递过程中,将节点转发证据动态捆绑到消息中,由消息携带到目的节点.目的节点收到消息后,同时获得参与消息转发节点的证据,从而能够对这些转发节点进行信任评价.

采用文献[6]中的层状硬币模型实现捆绑携带机制,典型层状硬币模型由基础层和扩展层组成,基础层由源节点在产生消息时按照指定格式生成,多个扩展层由携带消息的节点在遇到下一跳转发节点时动态生成,作为将消息成功转发到下一跳节点的证据,如图 3 给出了一个基于层状硬币模型的消息格式.消息的基础层包括消息头、消息内容和源节点生成的扩展信息,消息头字段 mid,N_0,N_k,t,TTL,nc 分别表示消息 id、源节点 id、目的节

点 id、消息生成时间戳、消息的生存周期和消息的副本数,消息内容 C 由源节点利用目的节点的公钥加密生成 $E_{pk_k}(H(N_0|t|N_k|C))$,$H(*)$是消息属性和内容的哈希函数,用于对消息进行验证.当源节点 N_0 在移动过程中遇到节点 N_1,依据路由算法判定节点 N_1 是否是合适的下一跳转发节点,如果节点 N_1 被选择作为下一跳转发节点,则源节点生成扩展层,$sig_0=SIG_0(N_0|mid)$表示源节点对消息的签名,扩展层字段记录源节点 N_0 将消息转发给节点 N_1 的证据消息,ts_0 表示源节点发送消息到下一跳节点的时间戳,$sig_1=SIG_1(H'(N_0|ts_0|N_1))$是节点 N_1 的签名,$H'(*)$是生成转发证据摘要的哈希函数,作为源节点 N_0 和节点 N_1 的相遇证据和接收证据,表示节点 N_1 接收了上一跳节点转发的消息.在转发过程中,如果在 ts_i 时刻携带消息的节点 N_i 遇到下一跳转发节点 N_k 时,则动态生成扩展层描述节点 N_i 将消息转发给节点 N_k 的证据,以及节点 N_k 接收消息的签名,在每次转发过程中,都按照上述步骤执行,直到消息到达目的节点为止.

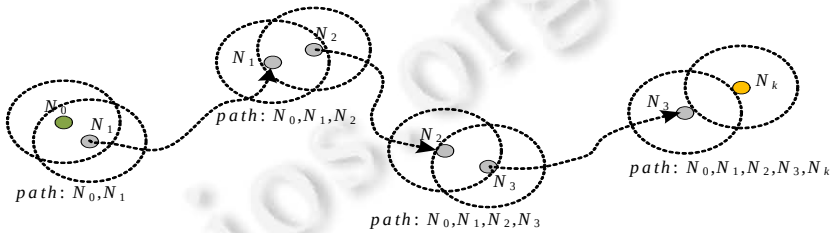


Fig.2 Data transmission link

图 2 数据传输链路

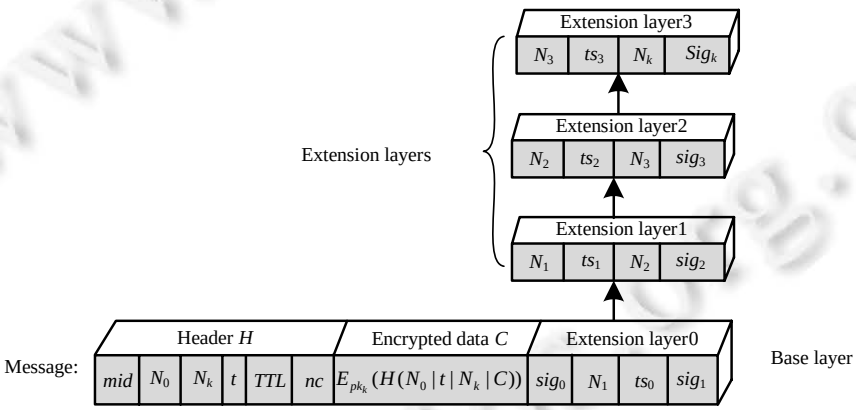


Fig.3 Message format based on layered coin model

图 3 基于层状硬币模型的消息格式

由于消息在转发过程中附加了多层证据信息,基于层状硬币模型的消息开销相对于基本消息开销稍大一些,假设消息 id、节点 id 和时间戳等固定字段占 8 个字节,消息头中 6 个字段共占有 48 个字节,基础层中源节点生成的扩展信息包括两个基本字段和两个签名字段共占有 16+2×|sig|个字节,转发节点生成的扩展信息包括 3 个基本字段和一个签名字段共占有 24+|sig|个字节,那么一个具有 k 个扩展层的消息大小 $Length_k(m)$为:

$$Length_k(m)=48+|E_{pk_k}(H(N_0|t|N_k|C))|+16+2\times|sig|+(k-1)\times(24+|sig|)\text{字节}$$
$$=40+|E_{pk_k}(H(N_0|t|N_k|C))|+24k+|sig|(k+1)\text{字节},$$

其中,$|E_{pk_k}(H(N_0|t|N_k|C))|$表示消息内容加密后的长度,|$sig$|表示节点签名信息的长度.因此,消息长度主要由消息内容和附加信息构成.一般情况下,|sig|大概需要 20 个字节,附加的证据信息长度为 L=24k+20(k+1)=44k+20 字节,当 k=20 时,L≈0.89KB,对网络的带宽和节点的存储只付出较小的代价.

3.3 可信路由表的构建

目的节点 N_j 收到消息 m 后,从 m 中提取转发节点的证据链:

$$path: N_0 \xrightarrow{ts_0} N_1 \xrightarrow{ts_1} N_2 \xrightarrow{ts_2} \ldots \rightarrow N_i \xrightarrow{ts_i} \ldots \xrightarrow{ts_k} N_j.$$

对各节点的数字签名信息进行验证作为信任评价证据,如果签名验证正确,则对参与消息转发的节点进行信任奖励.为了体现信任评价的公平性和激励性,在奖励时需满足可靠性和延时性原则.

(1) 转发节点在证据链中的位置 $path(N_i)$越接近目的节点,信任度奖励应越高.$path(N_i)$越大,节点携带消息到达目的节点的可靠性越高;

(2) 对于链路长度相同的消息,消息延时时间$\Delta t=ts_k-t$ 越小,节点信任度奖励应越高.Δt 越小,说明这条链中的节点将消息转发到目的节点的延时性越小.

定义 1(信任奖励度). 设 $T_{ji}^{(m)}$ 表示目的节点 N_j 对节点 N_i 在消息 m 转发过程中的信任奖励度,令

$$T_{ji}^{(m)}=\frac{1}{2}\left(e^{-\lambda\times\frac{\Delta t}{TTL}}+\varphi+(1-\varphi)\times\left(\frac{path(N_i)}{|path(m)|}\right)^2\right) \tag{2}$$

其中,$|path(m)|$表示消息 m 转发路径的长度,$\rho(x)=e^{-\lambda x}$,$0\leqslant x\leqslant 1$ 表示证据链延时性奖励函数.该策略具有指数递减性,Δt 越小,延时性信任奖励越高,取值范围为 $e^{-\lambda}\leqslant\rho(x)<1$,$\lambda>0$ 为延时性奖励最小值的调节因子,该奖励函数根据网络延时性要求设置调节因子λ.$path(N_i)$表示节点 N_i 在证据链中的位置,其取值为 $1\leqslant path(N_i)\leqslant|path(m)|$. $f(y)=\varphi+(1-\varphi)y^2$,$0<y\leqslant 1$ 为转发节点可靠性奖励函数.该策略具有递增性,$path(N_i)$越大,可靠性信任奖励越高,取值范围 $f(y)\in(\varphi,1]$,$0\leqslant\varphi<1$ 为可靠度奖励最小值的调节因子,能够根据网络对可靠性的要求设置调节因子φ.分析可知,$T_{ji}^{(m)}$ 取值范围为 $(e^{-\lambda}+\varphi)/2<T_{ji}^{(m)}<1$.该奖励策略可以根据不同网络场景对延时性和可靠性的要求进行设置,并且保证了信任奖励的最大值为 1.

定义 2(信任度). 设 T_{ji} 表示目的节点 N_j 对节点 N_i 携带消息到达能力的信任度,令

$$T_{ji}=\begin{cases}T'_{ji}\times\zeta(t_n,t_o), & \text{if } t_n-t_o>Tw \ \&\& \ N_i\notin\mathfrak{N}\\ T'_{ji}+(1-T'_{ji})\times T_{ji}^{(m)}, & \text{other}\end{cases} \tag{3}$$

其中,T'_{ji} 表示节点 N_j 对 N_i 的历史信任度;Tw 表示信任度更新窗口的长度;$\mathfrak{N}$为当前窗口内所有携带消息到达 N_j 的节点集合,即当前窗口内收到的所有消息证据链中节点组成的集合.如果在窗口 Tw 内收到了节点 N_i 携带的消息,则对节点 N_i 的信任度进行奖励操作,增加其信任度;否则进行衰减运算,降低节点 N_i 的信任度.如果多个更新窗口不携带消息到达,其信任度将不断衰减直到 0 为止.衰减性反映了信任度是一个长期不间断积累的过程,只有不断的携带消息才能维持高信任度,从而抑制恶意节点和作弊节点.

函数$\zeta(t_n,t_o)\in(1-\gamma,1)$为时间衰减因子,$t_n$,$t_o$ 分别表示当前时刻和最后更新时刻,如公式(4)所示:

$$\zeta(t_n,t_o)=1-\frac{(t_n-t_o)\gamma}{t_n} \tag{4}$$

其中,$0<\gamma\leqslant 1$ 是衰减速度调节因子,其值越大,信任度衰减速度越快;反之,衰减速度越慢.如果在一个安全稳定的网络环境,γ可以取较小值;如果网络中存在大量的恶意节点和自私节点,则γ可以取较大值,从而防止这类节点通过有选择性的转发消息积累信任度.同时,该衰减策略能够根据网络的运行时间自动调整衰减速度,当信任度更新间隔 t_n-t_o 相等时,当前时刻 t_n 越大,信任度衰减越慢.因为随着网络的长期运行,节点的信任度逐渐收敛到了一个稳定状态.

利用公式(1)和公式(2),目的节点 N_j 经过多个周期的网络运行形成信任向量表 $T_j=(T_{j1},T_{j2},T_{j3},\ldots,T_{jn})$,并依据节点携带消息的证据,周期性地维护和更新向量表中节点的信任度.可信路由表 TRT 由网络中各节点的行向量组成,其构建依靠节点移动相遇时互换信任向量表迭代完成,如图 4 所示:当节点 N_i 与节点 N_j 相遇时,互相交换各自携带的信任向量表,迭代形成新的可信路由表.为防止转发过程中向量表中节点信任度被恶意篡改,在传递过程采用数字签名和时间戳机制,具有签名的信任向量 $T_{sig_j}=SIG_j(H''(T_j\,|\,TwID))$,$H''(*)$为信任向量表和更新窗口 $TwID$ 的哈希函数.如果两个节点包含同一节点的信任向量表 T_k 时,则依据窗口 $TwID$ 判断最新的 T_k 进行更新.

由于可信路由表是多次迭代构建,在网络初始阶段存在冷启动问题,为此,在初始阶段采用 epidemic 路由协议实现消息转发.

$$TRT_i=\begin{bmatrix}T_{11} & T_{12} & T_{13} & \cdots & T_{1n}\\ T_{21} & T_{22} & T_{23} & \cdots & T_{2n}\\ T_{i1} & T_{i2} & T_{i3} & \cdots & T_{in}\end{bmatrix} \longleftrightarrow \begin{bmatrix}T_{31} & T_{32} & T_{33} & \cdots & T_{3n}\\ T_{j1} & T_{j2} & T_{j3} & \cdots & T_{jn}\end{bmatrix}=TRT_j$$

$$\Downarrow$$

$$TRT_i=\begin{bmatrix}T_{11} & T_{12} & T_{13} & \cdots & T_{1n}\\ T_{21} & T_{22} & T_{23} & \cdots & T_{2n}\\ T_{31} & T_{32} & T_{33} & \cdots & T_{3n}\\ T_{i1} & T_{i2} & T_{i3} & \cdots & T_{in}\\ T_{j1} & T_{j2} & T_{j3} & \cdots & T_{jn}\end{bmatrix}=TRT_j$$

Fig.4 Iterative procedure of trust routing table (TRT)

图 4 可信路由表 TRT 的迭代过程

算法 1. 可信路由表构建算法.

初始化:设置 $TTL,Tw,\lambda,\varphi,\gamma$参数值;

$\mathcal{N}=\phi$;

IF N_j 接收到消息 m && $m.target==N_j$ THEN

提取信任证据链 $m.path$;

IF $m.path$ 中节点数字签名验证通过 THEN

提取消息创建时间 $m.timeCreated$;

提取消息接收时间 $m.timeReceived$;

计算消息延时时间$\Delta t=m.timeReceived-m.timeCreated$;

FOR (i=1; $i\leqslant|path(m)|$; i++) DO //对信任链中各节点进行信任奖励

$\mathcal{N}=\mathcal{N}\cup\{N_i\}$;

利用公式(1)计算信任链中第 i 个节点 N_i 的信任奖励度 $T_{ji}^{(m)}$;

利用公式(2)奖励操作更新信任向量表中第 i 个节点 N_i 的信任度 T_{ji};

endFOR

endIF

endIF

IF $t_n-t_o\geqslant Tw$ THEN

利用式(2)衰减运算更新信任向量表中节点 $N_k\notin\mathcal{N}$的信任度 T_{jk};

$\mathcal{N}=\phi$;

$TwID$++; //增加更新窗口

endIF

IF N_j 与 N_i 建立了链接 THEN

$TRT_j\rightarrow N_j$;

$TRT_j\rightarrow N_i$;

WHILE $\forall T_k\in TRT_i\cap TRT_j$ DO

IF $N_i(T_k).TwID>N_j(T_k).TwID$ THEN

$N_j(T_k)=N_i(T_k)$; //N_j update 可信路由表 TRT 中向量 T_k

endIF

endWHILE

WHILE $\forall T_x \in TRT_i$ && $T_x \notin TRT_j$ DO

N_j update 可信路由表 $TRT_j=TRT_j \cup T_k$;

endIF

endWHILE

endIF

该算法相对于文献[6,7,9]具有较好的及时性和便捷性,仅需要目的节点在收到消息之后提取信任证据对转发节点进行信任评估,形成信任评估向量,不需要额外代价收集信任证据.该算法利用泛洪机制将目的节点的最新信任向量广播到网络中,形成或更新可信路由表 TRT,设网络中有 n 个节点,则每个目的节点中信任行向量最多有 n 条记录,每条信任记录占 2 字节,信任行向量最大占 $2n$ 字节,可信路由表 TRT 最大为 $2n^2$ 字节.假设节点在相遇时有 p%的行向量需要更新,则更新可信路由表所需流量为 $2n^2 \times p$%字节.可见,节点缓存 B_o 大小和维护可信路由表消耗的流量均与网络节点数有关.当 n=1000 时,只需大概 2MB 的缓存;当 p=20 时,即每次更新 200 条行向量,只需要大概 0.4MB 流量.因此,该算法对于中小型网络在空间复杂度和网络性能方面有明显优势.

3.4 基于信任的安全路由算法

TOR 采用有限消息副本转发策略,依据目的节点对转发节点的信任度实现转发决策和分割消息副本数,当节点 N_i 遇到节点 N_k,首先查找缓存 B_m 是否有携带要转发的消息,如果存在转发消息集 M,则循环检测每条消息 $m \in M$,获取消息的目的节点 N_j,然后查找 TRT 表获取节点 N_i,N_k 的信任度 T_{ji},T_{jk},按照如下策略转发.

- 如果 $T_{jk}>T_{ji}$,则 N_i 分割消息 m 的副本数 Nc_i,将副本数为 Nc_k 的消息 m 转发给 N_k,更新 $Nc_i \leftarrow Nc_i - Nc_k$;否则,当 $T_{jk} \leqslant T_{ji}$,则 N_i 继续携带消息直到遇到信任度更大的节点.消息副本数分割计算如公式(5):

$$Nc_k \leftarrow \left\lceil \frac{T_{jk}}{T_{ji}+T_{jk}} \cdot Nc_i \right\rceil \tag{5}$$

- 在初始阶段,如果 T_{jk},T_{ji} 都不存在,则利用其他节点对 N_i,N_k 的综合信任度 $\frac{1}{n}\sum_{p=1}^{n} T_{pi}$,$\frac{1}{n}\sum_{p=1}^{n} T_{pk}$ 作为消息转发的决策依据,即:如果 $\frac{1}{n}\sum_{p=1}^{n} T_{pk} > \frac{1}{n}\sum_{p=1}^{n} T_{pi}$,则 N_i 将副本数为 Nc_k 的消息 m 转发给 N_k,更新 $Nc_i \leftarrow Nc_i - Nc_k$;否则,继续携带消息.这种情况下,消息副本数分割计算如公式(6):

$$Nc_k \leftarrow \left\lceil \frac{\frac{1}{n}\sum_{p=1}^{n} T_{pk}}{\frac{1}{n}\sum_{p=1}^{n} T_{pk}+\frac{1}{n}\sum_{p=1}^{n} T_{pi}} \cdot Nc_i \right\rceil \tag{6}$$

- 当 $\frac{1}{n}\sum_{p=1}^{n} T_{pi} = \frac{1}{n}\sum_{p=1}^{n} T_{pk} = 0$,说明网络在冷启动阶段.此时,采用 epidemic 算法实现消息转发,N_i 将消息 m 转发给 N_k,不分割副本数 Nc_i.

算法 2. 基于信任的安全路由算法.

IF N_i 在移动过程中与 N_k 建立链接 THEN

IF $B_m \neq \phi$ THEN

将需要转发的消息添加到集合 M 中;

endIF

FOR $\forall m \in M$ DO

从 $m.target$ 得到消息的目的节点 N_j;

查找可信路由表 TRT 的行向量 $T_j=(T_{j1},T_{j2},T_{j3},\ldots,T_{jn})$,得到 N_i,N_k 的信任度 T_{ji},T_{jk};

IF T_{ji} and T_{jk} 都不存在 THEN

对可信路由表 TRT 的列向量 $T_{*i}=(T_{1i},T_{2i},T_{3i},\ldots,T_{ni})^T$ 进行计算 $\frac{1}{n}\sum_{p=1}^{n}T_{pi}$;

对可信路由表 TRT 的列向量 $T_{*k}=(T_{1k},T_{2k},T_{3k},\ldots,T_{nk})^T$ 进行计算 $\frac{1}{n}\sum_{p=1}^{n}T_{pk}$;

IF $\frac{1}{n}\sum_{p=1}^{n}T_{pk}>\frac{1}{n}\sum_{p=1}^{n}T_{pi}$ THEN

利用公式(6)计算分割的消息副本数 Nc_k;

N_i 将副本数为 Nc_k 的消息 m 副本转发给节点 N_k;

更新消息副本数 $Nc_i \leftarrow Nc_i - Nc_k$;

ELSE

IF $\frac{1}{n}\sum_{p=1}^{n}T_{pi}=\frac{1}{n}\sum_{p=1}^{n}T_{pk}=0$ THEN

N_i 采用 epidemic 算法将消息 m 的副本转发给节点 N_k;

endIF

endIF

ELSE

IF $T_{jk}>T_{ji}$ THEN

利用公式(5)计算分割的消息副本数 Nc_k;

N_i 将副本数为 Nc_k 的消息 m 副本转发给节点 N_k;

更新消息副本数 $Nc_i \leftarrow Nc_i - Nc_k$;

endIF

endIF

endFOR

endIF

该算法的节点只需要查找本地可信路由表 TRT,其时间复杂度最大为 $O(|M|\times n)$.消息沿着信任梯度递增的方向传递,只有 $T_{jk}>T_{ji}$ 时转发消息,使得消息到达目的节点的概率越来越高,有效提高了消息传递的成功率.由于恶意或自私节点不参与协作,导致其信任度很低,则利用信任关系可以剔除这类节点,提高了网络的安全性和可靠性.

4 实验结果分析

利用 ONE 模拟器实现了 TOR 路由算法,并对其性能和有效性进行了验证.ONE 模拟器是专门为 DTN 网络和机会网络开发的网络仿真平台,该平台提供了多种节点移动模型和一些比较典型的路由算法,如 Epidemic, SAW,Prophet 及 MaxProp 等.为了验证 TOR 路由算法的优势,本文与经典的路由算法进行了对比分析.

4.1 实验环境设置及性能指标

采用 ONE 模拟器自带的地图作为仿真场景,网络区域设置为 4500m×4500m,节点个数为 200.将节点分为正常节点、自私节点和恶意节点,自私节点只转发熟悉节点的消息,而恶意节点接收到消息包后直接丢弃形成黑洞.实验模拟节点 24 小时内的移动和相遇场景,节点采用基于最短路径移动模型,其中,正常节点移动速度为 0.5m/s~1.5m/s.为体现恶意节点的破坏能力,设置其移动速度为 2.7m/s~13.9m/s,消息产生周期 25s~35s,产生 2 900 条消息,每条消息大小 512KB,消息生存周期为 30~240 分钟,节点缓存 B_m 设置为 5~60MB,具体参数设置见表 1.

Table 1 Parameters for simulation environment

表 1 仿真环境参数设置

参数	取值
节点数	200 个
网络区域	4500m×4500m
消息生成周期	30 分钟~240 分钟
交付/接收消息速度	250KB/s
节点缓存空间	5 MB~60MB
节点到达目的节点后停留时间	0s~120s
数据分组大小	512KB
初始更新信任表周期	60s
节点产生消息周期	25s~35s

性能评价指标包括消息传递成功率、消息平均转发延迟时间、网络交付代价和平均跳数.

- 消息传递成功率 *d_prob* 为成功传递的消息数 Num_d 与网络中产生的总消息数 Num_c 的比值;
- 平均转发延迟时间 *l_avg* 为消息从源节点转发到目的节点的平均消耗时间,单位为秒,该指标评估路由算法的延迟性,时间越小,表示性能越优.设整个网络成功传递的消息集合为 M_d,消息 *i* 传递消耗的时间为 lT_i,则 *l_avg* 为

$$l\_avg = \frac{1}{Num_d}\sum_{i\in M_d} lT_i \tag{7}$$

- 网络交付代价 *o_ratio* 为网络中所有消息副本数 Num_r 减去成功传递的消息数 Num_d 与成功传递的消息数的比值,该指标评估网络的开销情况,交付代价越小,表示网络性能越优;
- 平均跳数 *h_avg* 为消息从源节点到目的节点所传递的节点数,该指标评估转发节点选择的准确性.平均跳数越小,表示转发节点选择的准确性越高.设消息 *i* 传递的节点数为 hc_i,则 *h_avg* 为

$$h\_avg = \frac{1}{Num_d}\sum_{i\in M_d} hc_i \tag{8}$$

4.2 仿真结果与分析

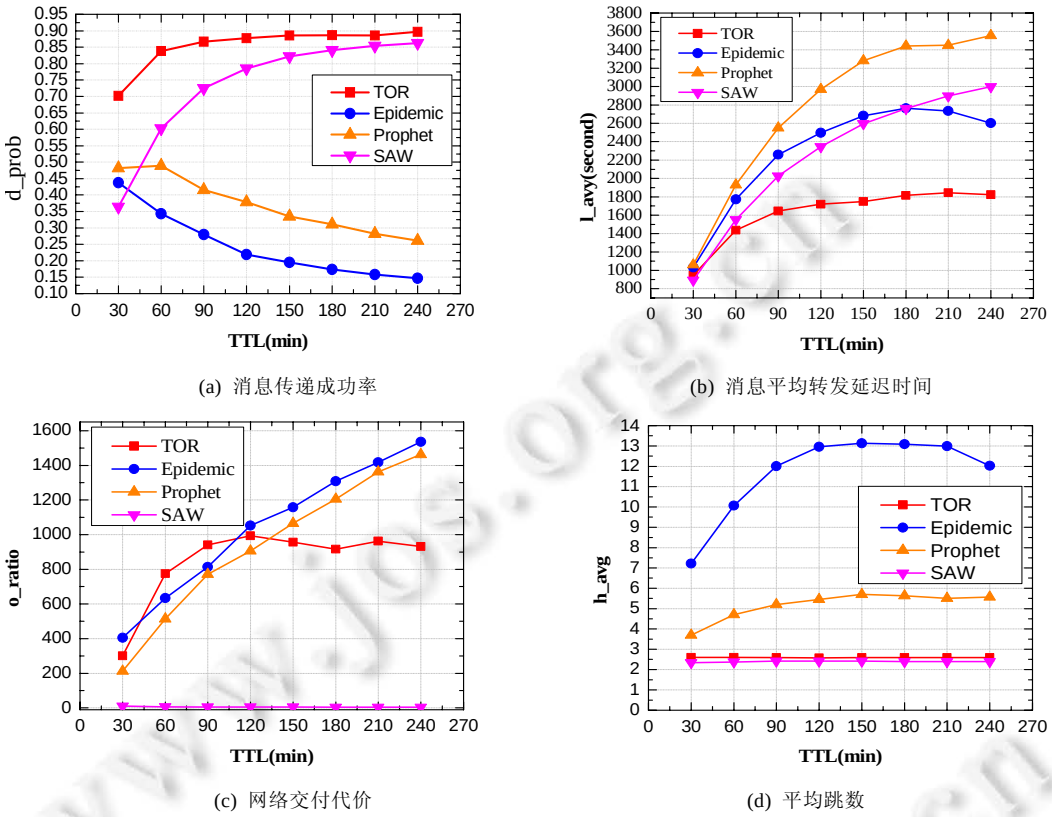
实验过程中,通过调整消息生存周期 *TTL*、节点缓存大小以及网络中恶意节点的数量等参数值,来分析 TOR 路由算法与其他路由的性能对比情况.

实验 1:消息生存周期的大小对路由协议性能的影响.

每个节点缓存设置为 5M,考察消息生存周期的变化对路由协议性能的影响.图 5 给出了 4 种路由算法随着消息生存周期的增加其性能指标的变化情况.

由图 5(a)和图 5(b)可以看出:TOR 算法在转发成功率和转发延时方面优势明显,受 *TTL* 变化影响较小,即使 *TTL* 为 30min 时,其成功率仍达到了 70%;在 *TTL* 为 120min 时,其成功率达到 88.5%,趋于稳定状态.这是因为 TOR 采用了可信节点选择和有限副本转发策略提高了转发成功率,而 Epidemic 和 Prophet 算法采用了无限副本转发策略,由于 *TTL* 较大随着网络的运行产生了大量消息包,导致节点缓存中没有及时转发的消息被删除从而降低了成功率.虽然 SAW 算法随着生存周期 *TTL* 的增加,消息转发成功率趋近于 TOR 算法,但是在消息平均转发延时方面,TOR 算法有优势,而其他 3 种算法随着 *TTL* 的增加有明显增长趋势,说明 TOR 算法采用信任机制在转发消息时能够找到一条延时较短的可信转发路径.

由图 5(c)和图 5(d)可以看出:在交付代价和平均跳数方面,SAW 算法效果明显.这是因为 SAW 算法产生的消息副本数较少所致,而 TOR 算法在 *TTL* 小于 110min 时,相对于其他算法网络交付代价稍高.在平均跳数方面,TOR 算法与 SAW 算法比较接近.这是由于 TOR 算法采用了基于信任度递增的方式传递消息,使得每条信任链需要较少的节点即可将消息携带到目的节点.



(a) 消息传递成功率 (b) 消息平均转发延迟时间

(c) 网络交付代价 (d) 平均跳数

Fig.5 Performance comparison of TOR with different TTL

图 5 不同生存周期 TOR 路由的性能对比

实验 2:考察缓存大小的变化对路由协议性能的影响.

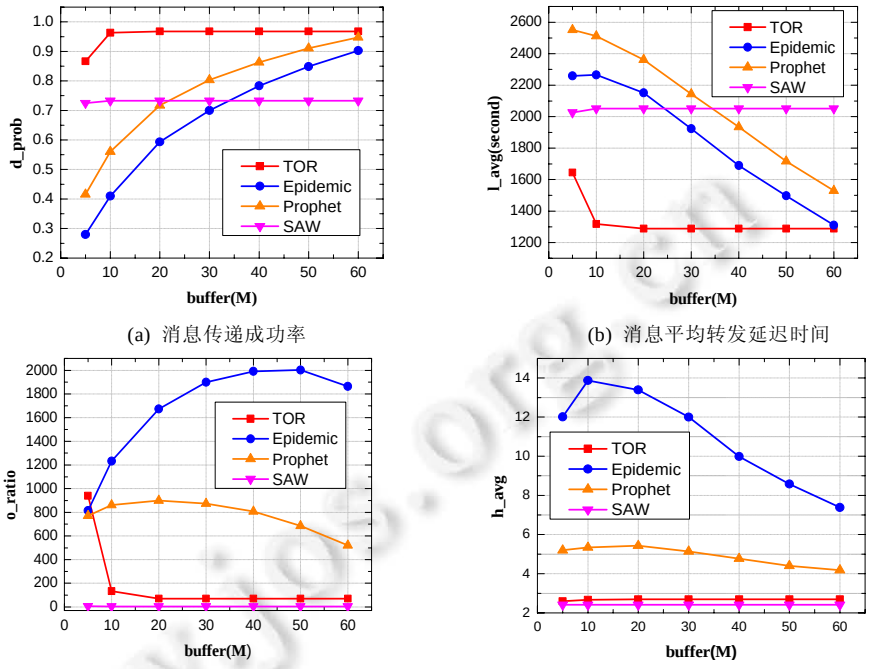
设置 *TTL* 为 90min,通过调整缓存大小考察路由算法性能指标的变化情况.图 6 给出了 4 种路由算法在不同缓存情况下的性能指标.

由图 6(a)和图 6(b)可以看出,TOR 算法只需要较小的缓存就可以在消息传递成功率和平均转发时延方面有较好的性能.当缓存为 10M 时,TOR 算法就趋于一个稳定状态,成功率达到了 96.3%,平均延迟降低为 1 300s.说明 TOR 算法对缓存空间要求较低,比较适合于缓存有限的机会网络.而 Epidemic 和 Prophet 算法随着缓存空间的增大其转发成功率逐步递增、平均转发延时呈递减趋势.这是由于缓存的增大使得节点有足够空间存储未及时转发的消息副本,提供了更多的转发机会,说明这两种算法对缓存大小的依赖性较强,对于计算能力和缓存空间有限的机会网络效率较低.SAW 算法由于只采用了有限消息副本策略而缺乏转发节点的判断机制,使得该算法对缓存空间要求虽然较小但其效率大大低于 TOR 算法.

图 6(c)和图 6(d)可以看出:随着缓存空间的增加,TOR 算法的网络交付代价大大降低.在缓存为 10M 时,其交付代价降低到了 100 左右,与 SAW 算法比较接近且趋于稳定状态.而 Epidemic 和 Prophet 算法虽然呈现先上升后下降的趋势,但其交付代价仍然较高.在平均跳数方面,TOR 算法和 SAW 算法仍然保持良好的性能.

实验 3:考查恶意节点对路由协议性能的影响.

设置 *TTL* 为 60min,缓存大小为 20M,将网络中 40 个比较活跃的正常节点变为恶意节点来考察网络性能变化情况.图 7 给出了存在不同数量恶意节点时算法的性能对比情况.

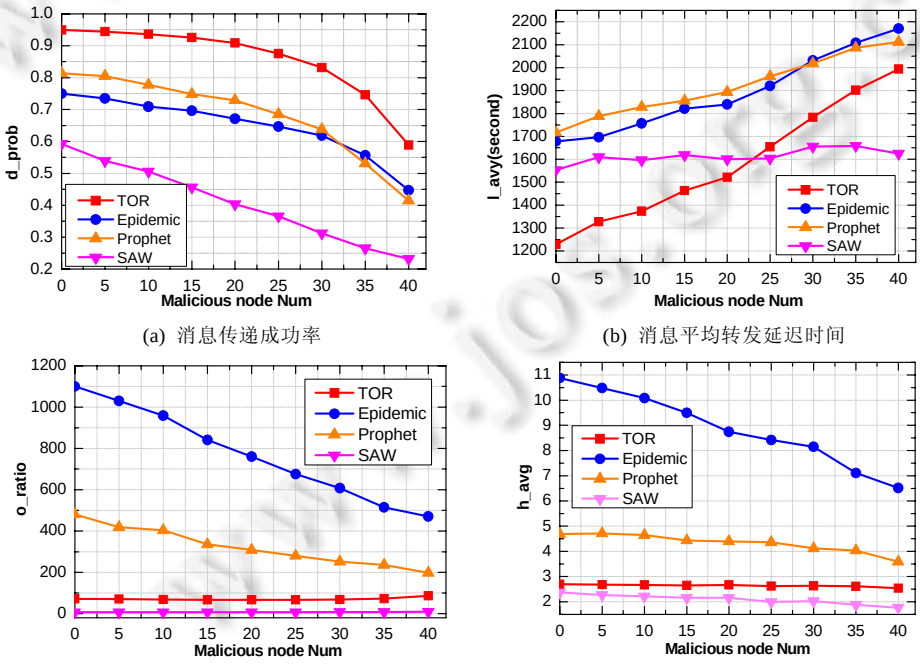


(a) 消息传递成功率 (b) 消息平均转发延迟时间

(c) 网络交付代价 (d) 平均跳数

Fig.6 Performance comparison of TOR with different buffer

图 6 不同缓存大小 TOR 路由的性能对比



(a) 消息传递成功率 (b) 消息平均转发延迟时间

(c) 网络交付代价 (d) 平均跳数

Fig.7 Performance comparison of TOR with different malicious node number

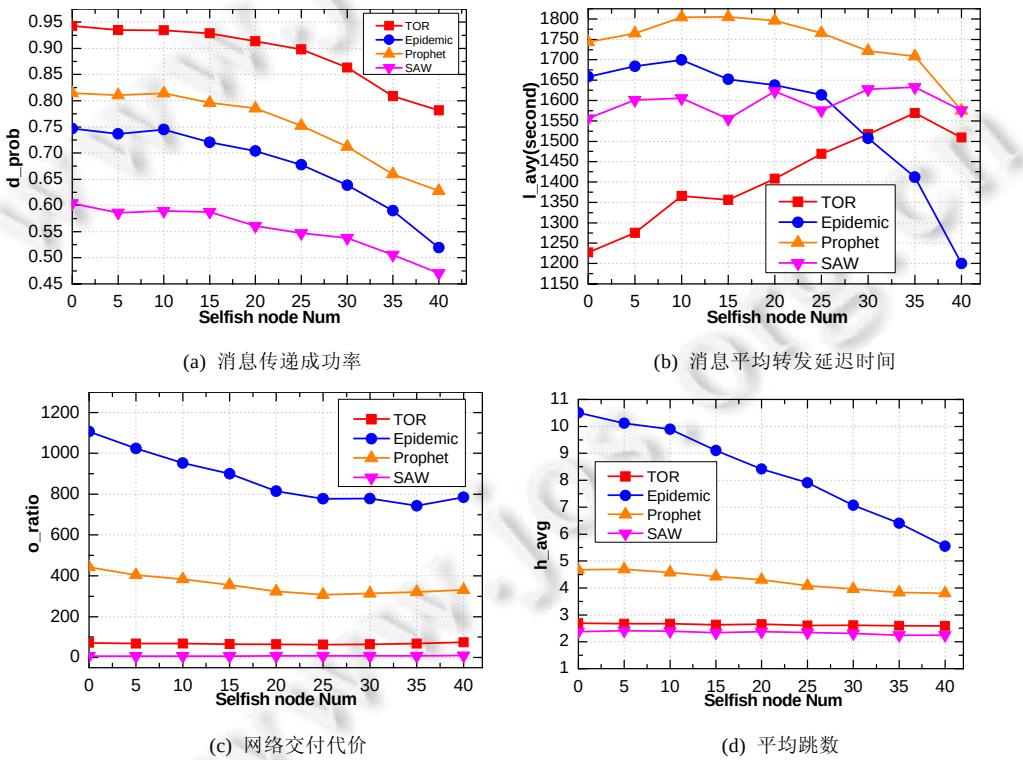
图 7 不同恶意节点数 TOR 路由的性能对比

由图 7(a)和图 7(b)可以看出:随着恶意节点数量的增多,4 种路由算法的消息传递成功率都呈下降趋势,平均转发延时呈上升趋势.而 TOR 算法在恶意环境下,相对于其他 3 种算法仍然具有较高的成功率,当恶意节点数达到 30 时,其消息转发成功率为 84%.即使网络中 40 个活跃节点都变为了恶意节点,其消息转发成功率仍保持在 60%左右.说明 TOR 算法采用的信任转发策略对恶意行为具有较好的抵御作用.之所以消息转发成功率降低和平均转发延时升高,是因为网络中起主要传递作用的活跃节点变为了恶意节点后,网络中正常节点稀疏导致的.SAW 算法的消息传递成功率呈线性下降趋势,说明有限副本转发策略受恶意行为的影响较大.而 Epidemic 和 Prophet 算法在恶意节点数较少时消息转发成功率下降比较缓慢,这是因为无限冗余转发策略本身就具有一定的安全性,可以简单地抵御恶意攻击行为.

由图 7(c)和图 7(d)可以看出:在恶意环境下,TOR 算法仍具有较好的网络交付代价和平均跳数.这是由于 TOR 算法采用的有限副本和信任转发策略既可以有效识别恶意节点,同时又能够保证选择信任度较高的节点转发消息的缘故.Epidemic 和 Prophet 算法随着恶意节点数的增多,其网络交付代价和平均跳数呈下降趋势,这是因为正常节点稀疏之后,整个网络的消息副本数减少的缘故.而 SAW 算法由于采用有限副本转发和平均副本分割策略,使得该算法的网络交付代价和平均跳数仍保持较高的效率.

- 实验 4:考察自私节点对网络协议性能的影响

设置 *TTL* 为 60min,缓存大小为 20M,将 40 个活跃度较高的正常节点变为自私节点考察对网络性能的影响.图 8 给出了不同数量自私节点各算法的性能对比情况.



(a) 消息传递成功率 (b) 消息平均转发延迟时间

(c) 网络交付代价 (d) 平均跳数

Fig.8 Performance comparison of TOR with different selfish node number

图 8 不同自私节点数 TOR 路由的性能对比

由图 8(a)和图 8(b)可以看出:随着自私节点的增加,4 种路由算法的消息传递成功率都呈下降趋势;在转发延时方面,TOR 算法呈上升趋势,Epidemic 算法和 Prophet 算法呈现先升后降的趋势,TOR 算法较其他算法优势明显,尤其是当自私节点小于 20 时,保持 91%以上的传递成功率,即使自私节点达到 40 时,其传递成功率仍然在

80%左右,说明 TOR 算法采用的信任机制对自私行为具有较好的抑制作用.TOR 算法平均转发延时升高是因为当自私节点增多时,正常节点需要花费更长的时间才能遇到下一跳可信的转发节点.而 Epidemic 算法和 Prophet 算法由于对自私行为没有抑制,很多消息在转发过程中生存时间超时被丢弃,成功转发的消息数量减少,致使两种算法在自私节点数超过 10 时,传递成功率和平均转发延时降低比较明显.SAW 算法由于采用两跳转发策略直接将消息传递给目的节点,使得在转发延迟方面受自私行为影响较小.

由图 8(c)和图 8(d)看出,TOR 算法在网络交付代价和平均跳数方面有优势.这是因为 TOR 算法采用基于信任梯度递增的消息传递策略,只有遇到信任度更高的转发节点时才传递消息,所以不受自私行为影响.Epidemic 和 Prophet 算法随着自私节点规模的增大,其网络交付代价和平均跳数呈下降趋势,这是由于自私节点不参与消息转发,使得网络中消息副本总数减少所致.而 SAW 算法性能表现最优,是因为该算法产生的消息副本数最少的缘故.

5 结束语

提出了一种基于信任机制的机会网络安全路由决策算法 TOR,该算法根据目的节点采集到的信任证据链和消息延时时间计算转发节点的信任度,存储在信任向量表中.信任证据采集利用层状硬币模型和数字签名机制,在传递过程中将节点转发证据动态捆绑到消息包上,由消息携带到目的节点.该方法具有较好的及时性和安全性,付出的额外代价较小.节点周期性地将具有签名和最新的信任向量表利用泛洪方式反馈到网络中,在各个节点迭代形成由多维行向量集组成的只读可信路由表 TRT,作为下一跳转发节点选择和消息副本数分割的决策依据,利用签名和时间戳机制防止信任向量表在反馈过程中被恶意节点篡改,有效保证了路由表的安全性和可靠性.消息沿着信任梯度递增的方向传递,不仅有效抑制恶意行为,而且大大提高了消息投递的成功率,降低了消息投递延时.

References:

[1] Xiong YP, Sun LM, Niu JW, Liu Y. Opportunistic networks. Ruan Jian Xue Bao/Journal of Software, 2009,20(1):124−137 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3467.htm

[2] Su JS, Hu QL, Zhao BK, Peng W. Routing techniques on delay/disruption tolerant networks. Ruan Jian Xue Bao/Journal of Software, 2010,21(1):119−132 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3689.htm [doi: doi: 10.3724/SP.J.1001.2010.03689]

[3] Wu Y, Li JH, Lin C. Survey of security and trust in opportunistic networks. Journal of Computer Research & Development, 2013, 50(2):278−290 (in Chinese with English abstract).

[4] Zhu H, Du S, Gao Z, Dong M, Cao Z. A probabilistic misbehavior detection scheme toward efficient trust establishment in delay tolerant networks. IEEE Trans. on Parallel & Distributed Systems, 2014,25(1):22−32.

[5] Li Y, Yu JH, You XH. An incentive protocol for opportunistic networks with resources constraint. Chinese Journal of Computers, 2013,36(5):947−956 (in Chinese with English abstract).

[6] Lu R, Lin X, Zhu H, Shen X, Preiss B. Pi: A practical incentive protocol for delay tolerant networks. IEEE Trans. on Wireless Communications, 2010,9(4):1483−1493.

[7] Ayday E, Fekri F. An iterative algorithm for trust management and adversary detection for delay-tolerant networks. IEEE Trans. on Mobile Computing, 2012,11(9):1514−1531.

[8] Nelson SC, Bakht M, Kravets R. Encounter-Based routing in DTNs. In: Proc. of the 28th Int'l Conf. on Computer Communications (INFOCOM 2009). Piscataway: IEEE, 2009. 846−854. [doi: 10.1109/INFCOM.2009.5061994]

[9] Chen IR, Bao F, Chang MJ, Cho JH. Dynamic trust management for delay tolerant networks and its application to secure routing. IEEE Trans. on Parallel & Distributed Systems, 2014,25(5):1200−1210.

[10] Li Q, Cao G. Mitigating routing misbehavior in disruption tolerant networks. IEEE Trans. on Information Forensics & Security, 2012,7(2):664−675.

[11] Li F, Wu J, Srinivasan A. Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets. In: Proc. of the 28th Int'l Conf. on Computer Communications (INFOCOM 2009). Piscataway: IEEE, 2009. 2428−2436. [doi: 10.1109/INFCOM.2009.5062170]

[12] Chen BB, Chan MC. MobiCent: A credit-based incentive system for disruption tolerant network. In: Proc. of the 29th Int'l Conf. on Computer Communications (INFOCOM 2010). Piscataway: IEEE, 2010. 1−9. [doi: 10.1109/INFCOM.2010.5462136]

[13] Burgess J, Bissias GD, Corner MD, Levine BN. Surviving attacks on disruption-tolerant networks without authentication. In: Proc. of the 8th ACM Int'l Symp. on Mobile Ad Hoc Networking and Computing (MobiHoc 2007). New York: ACM Press, 2007. 61−70. [doi: 10.1145/1288107.1288116]

[14] Zhao H, Yang X, Li X. cTrust: Trust management in cyclic mobile ad hoc networks. IEEE Trans. on Vehicular Technology, 2013, 62(6):2792−2806.

[15] Wang B, Chen XX. Opportunistic routing algorithm based on trust model for ad hoc network ad hoc. Journal on Communications, 2013,34(9):92−104 (in Chinese with English abstract).

[16] Zhang SF, Huang D, Chen Z, Wu GX. Optimal stopping decision method for routing of opportunistic networks. Ruan Jian Xue Bao/Journal of Software, 2014,25(6):1291−1300 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4434.htm [doi: 10.13328/j.cnki.jos.004434]

附中文参考文献:

[1] 熊永平,孙利民,牛建伟,刘燕.机会网络.软件学报,2009,20(1):124−137. http://www.jos.org.cn/1000-9825/3467.htm

[2] 苏金树,胡乔林,赵宝康,彭伟.容延容断网络路由技术.软件学报,2010,21(1):119−132. http://www.jos.org.cn/1000-9825/3689.htm [doi: doi: 10.3724/SP.J.1001.2010.03689]

[3] 吴越,李建华,林闯.机会网络中的安全与信任技术研究进展.计算机研究与发展,2013,50(2):278−290.

[5] 李云,季弘,尤肖虎.资源受限的机会网络节点激励策略研究.计算机学报,2013,36(5):947−956.

[15] 王博,陈训逊.Ad Hoc 网络中一种基于信任模型的机会路由算法.通信学报,2013,34(9):92−104.

[16] 张三峰,黄迪,陈州,吴国新.一种面向机会网络路由的最优停止决策方法.软件学报,2014,25(6):1291−1300. http://www.jos.org.cn/1000-9825/4434.htm [doi: 10.13328/j.cnki.jos.004434]

李峰(1978－),男,山东德州人,博士,讲师,CCF 专业会员,主要研究领域为机会网络,信任管理.

司亚利(1981－),女,副教授,CCF 学生会员,主要研究领域为移动推荐,信任管理.

陈真(1987－),男,博士,CCF 学生会员,主要研究领域为信任管理,服务计算.

鲁宁(1984－),男,博士,讲师,主要研究领域为网络安全.

申利民(1962－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为柔性软件,协同计算.