一种基于信任模型的安全度量及安全路由算法设计

张 静　胡捍英　童 珉　李庆荣
(信息工程大学信息工程学院　郑州　450002)

摘　要：针对网络路由的攻击普遍且后果严重。目前的研究大多是采用数字签名，消息验证和入侵检测等机制来提高路由控制信息的安全，基本没有考虑机密应用数据的路由安全问题。该文通过分析通信实体的安全机制和安全威胁来测量链路和节点的信任度，建立节点间的信任关系，并基于该信任模型定义和量化一种新的安全度量SM(Security Metric)，提出以SM为选路标准的安全路由算法SMRA(Security Metric based Routing Algorithm)。仿真表明，网络存在攻击时，SMRA算法比OSPF算法有更好的包传输率和路由安全性能。

关键词：路由安全；信任度；信任关系；安全度量
中图分类号：TP393　　**文献标识码**：A　　**文章编号**：1009-5896(2008)01-0010-06

A Security Metric and Related Security Routing Algorithm Design Based on Trust Model

Zhang Jing　Hu Han-ying　Tong Min　Li Qing-rong
(*Department of Communication Engineering*, *Information Engineering University*, *Zhengzhou* 450002, *China*)

Abstract: Network routing-based attacks have become more common and the attack consequence can be more serious than other traditional network attacks. Most schemes on improving routing data security are applied to current routing protocols, e.g. digital signature, message authentication and intrusion detection, etc. But very few design guidelines on how to select a secure path to forward confidential user packets. By analyzing the security mechanisms and security threats over network entities, trust degrees of communication links and routers are measured and trust relations are built among network routers. Based on the trust model, a novel SM (Security Metric) is further defined and quantified as the routing criterion used in the proposed security routing algorithm SMRA (Security Metric based Routing Algorithm). Simulation results show that SMRA gets better performance than OSPF in terms of packets delivery ratio and routing security in unsafe networks.

Key words: Routing security; Trust degree; Trust relation; Security Metric (SM)

1　引言

目前，针对网络路由的攻击越来越普遍且后果严重，网络的路由安全问题受到广泛关注。IETF专门成立“路由协议安全需求”工作组[1]，开展对路由协议安全的研究。Chakrabarti对路由攻击进行了分类，强调为保护Internet的底层结构进行体系结构，算法和协议的研究[2]，并开发了一种安全路由协议SLIP，有效检测恶意的LSA源[3]。Murphy等人提出用数字签名机制保证洪泛(flood)LSAs的完整性[4]；Cheung为链路状态路由设计了一种有效的消息验证机制[5]，还研究采用入侵检测机制来保护路由结构[6]。国内关于完善IOS配置来抵御网络攻击的讨论不胜枚举，范炜玮将物理网络划分为虚拟信任路由域VTRD，并设计了一种基于VTRD的安全路由协议框架[7]。这些方案的共同之处都是讨论如何增强路由结构的安全性，以保护路由协议数据免受攻击，如果把这些机制也用于应用数据的安全传输，将带来很高的CPU计算负载而难以实现。Gupta提出为0SPFv3[8]部署IPSec[9]，通过验证、重播检测和加密等手段提高应用数据的防攻击能力和验证其传输的完整性、正确性。但并不能保证在内部攻击的情况下路由协议还能正确运作，而且数据在网络传输过程中，不会躲避不安全的网络设备，从而丢包或被黑。总之，如何为安全敏感应用(如金融业务)选择一条有效的安全转发路径是值得研究的问题。

本文提出把网络的安全状态视为路由选择的度量之一。事实上，安全度量尚且是一个模糊的概念和不成熟的研究方向，业界尚未定义用于路由目的的安全度量和形成测量数据安全的统一标准，所以安全度量设计面临很多困难，最大挑战是如何在实际网络中测量该度量。本文通过分析通信链路和路由节点的安全机制和安全威胁，建立基于链路和节点信任度的信任模型，量化了一种新的安全度量 SM (Security Metric)，并提出基于 SM 的安全路由算法 SMRA(Security Metric based Routing Algorithm)，最后通过仿真测试了 SM 和 SMRA 算法的性能。

2006-05-29 收到，2007-01-26 改回
国家 863 计划重大课题(2005AA121210)和河南省杰出人才创新基金(0421000100)资助课题

2　信任模型和安全度量

信任网络是有向图 $G(R,E)$，其中 R 是路由节点集，E 是通信链路集。$e_{ij}\in E$ 表示链路 $e_{ij}=r_i\to r_j$，r_i 和 r_j 是共享链路 e_{ij} 的邻居节点。

2.1　信任度，信任关系和安全度量

通信链路和路由节点是两种关键的网络设备。节点 $r\in R$ 是否能安全地把数据包转发给其邻居依赖于两方面：一方面是与 r 相连的链路的可靠性，另一方面是 r 的邻居节点的可靠性。因此，本文提出在邻居节点(信任对)间建立信任关系，为源和目的间的通信建立一条安全的信息存储和包转发可信路径。在Huang的信任框架[10]中，假定链路是安全的且节点间只有两种信任关系，即trusted或untrusted。考虑到这种信任理论的简单性，本文对该信任模型进行改进，用信任度概念更精确地描述节点间的信任关系。

定义 1 信任度(Trust Degree, TD)　信任度概念包含通信链路信任度和路由节点信任度。t 时刻，令 $\mathrm{TD}_t(e_{ij})$ 表示 r_i 对连接其到邻居节点 r_j 的链路 e_{ij} 的信任程度；$\mathrm{TD}_t(r_{ij})$ 表示 r_i 对通过 e_{ij} 所连接的邻居节点 r_j 的信任程度。

定义 2 信任关系(Trust Relation, TR)　令 $\mathrm{TR}\{r_i\to r_j\}$ 表示 r_i 与邻居节点 r_j 的信任关系。影响 $\mathrm{TR}\{r_i\to r_j\}$ 的主要因素是 $\mathrm{TD}(e_{ij})$ 及 $\mathrm{TD}(r_{ij})$，所以 t 时刻的 $\mathrm{TR}_t\{r_i\to r_j\}$ 可形式化为

$$\mathrm{TR}_t\{r_i\to r_j\}=d_1\,\mathrm{TD}_t(e_{ij})+d_2\,\mathrm{TD}_t(r_{ij})$$
$$(d_1,d_2\in[0,1],\ \ d_1+d_2=1)$$

其中与 TD 无关的权值 d_1, d_2 表明链路 TD 和节点 TD 对于信任对间信任关系建立的重要程度。TR 是单向的：$\mathrm{TR}_t\{r_i\to r_j\}\neq\mathrm{TR}_t\{r_j\to r_i\}$，TR 随网络安全状态变化而动态更新：$\mathrm{TR}_{t_1}\{r_i\to r_j\}\neq\mathrm{TR}_{t_2}\{r_i\to r_j\}$，$t_1\neq t_2$。

定义 3　安全度量(Security Metric, SM)　对链路 $e_{ij}\in E$，定义其凹性的安全度量为 $\mathrm{SM}(e_{ij})$ 或 $\mathrm{SM}(r_i,r_j)$，表示从 r_i 转发数据到 r_j 的安全程度，SM 显然也是单向的。这样 G 中 h 跳路径 $p=(r_0,r_1,...,r_h)$ 的安全度量为

$$\begin{aligned}\mathrm{SM}(p)&=\min[\mathrm{SM}(r_0,r_1),\mathrm{SM}(r_1,r_2),...,\mathrm{SM}(r_{i-1},r_i)]\\&=\min[\mathrm{SM}(e_{i-1,i})],\quad 1\le i\le h\end{aligned}\tag{1}$$

邻居节点以及其间通信链路的可信度越高，节点间的信任关系就越可靠，数据传输的安全性就越高。安全路径其实就是沿信息传输路径建立一条信任关系链，因此不妨设链路 e_{ij} 在 t 时刻的安全度量为

$$\mathrm{SM}_t(e_{ij})=\mathrm{TR}_t\{r_i\to r_j\}=d_1\,\mathrm{TD}_t(e_{ij})+d_2\,\mathrm{TD}_t(r_{ij}),$$
$$d_1,d_2\in[0,1],\ \ d_1+d_2=1\tag{2}$$

在此，d_1, d_2 表明链路的安全状态对于链路 TD 和节点 TD 的敏感程度。可见 SM 是随网络安全状态变化而更新的动态变量，适用于路由计算。网络设备传输和转发数据时所面临的安全威胁和所采取的安全机制是关系到链路安全度量的两个主要因素，所以在量化链路 TD 和节点 TD 时应加以考虑。

2.2　通信链路信任度的量化

当前有许多作用于 OSI 模型中链路层的安全机制(表 1)，可带给 $\mathrm{TD}(e_{ij})$ 不同的信任度增加值 $\mathrm{IV}(e_{ij})$。令实施 $x(x\ge0)$ 种安全机制的链路 e_{ij} 的最大信任度为 $\mathrm{TD}^{\max}(e_{ij})=\sum_{x\ge0}\mathrm{IV}_{\mathrm{Label}(x)}(e_{ij})$，比如应用 C，A，T 安全机制的 $\mathrm{TD}^{\max}(e_{ij})=\mathrm{IV}_{\mathrm{C}}(e_{ij})+\mathrm{IV}_{\mathrm{A}}(e_{ij})+\mathrm{IV}_{\mathrm{T}}(e_{ij})$ =0.1+0.2+0.3=0.6。当然，无任何安全机制的链路信任度 $\mathrm{TD}^{\max}(e_{ij})$ =0，若动态增减 $x'(x'\ge0)$ 种链路安全机制，$\mathrm{TD}^{\max}(e_{ij})$ 也会随之增减相应的信任度：

$$\mathrm{TD}^{\max}(e_{ij})=\mathrm{TD}^{\max}(e_{ij})\pm\sum_{x'\ge0}\mathrm{IV}_{\mathrm{Label}(x')}(e_{ij})$$

另一方面，通信链路传输可能面临各种威胁(如MAC洪泛攻击，ARP攻击等)，有许多入侵/误用行为检测和反应技术[6]可发现攻击。在定长周期 Δt 内，若检测到 λ 次链路攻击，$\mathrm{TD}(e_{ij})$ 应该呈指数下降(信任度失去容易)：$\mathrm{TD}_t(e_{ij})=\mathrm{TD}_{t-\Delta t}(e_{ij})-2^{\lambda-1}\mathrm{DV}(e_{ij})$ $(\lambda\ge1)$，直到 $\mathrm{TD}(e_{ij})=0$ 为止；反之，若 Δt 内无链路攻击，曾遭到攻击而失去一些信任度的 $\mathrm{TD}(e_{ij})$ 则线性增加一个变化值 $\mathrm{CV}(e_{ij})$ (信任度获得难)：$\mathrm{TD}_t(e_{ij})=\mathrm{TD}_{t-\Delta t}(e_{ij})+\mathrm{CV}(e_{ij})$，同时重置攻击次数 $\lambda=0$，直到 $\mathrm{TD}(e_{ij})$ 恢复到 e_{ij} 被攻击前的最大信任度为止：$\mathrm{TD}(e_{ij})=\mathrm{TD}^{\max}(e_{ij})$。

表 1　通信链路的安全机制及 $\mathrm{IV}(e_{ij})$ 举例

安全机制	标识	协议举例	$\mathrm{IV}(e_{ij})$ 举例(可配置)
加密	C	DES、IDEA、RSA 等	0.1
认证	A	PAP、CHAP、数字签名、MIT Kerberos 等	0.2
隧道	T	PPTP、L2TP 等	0.3
⋮			

2.3　路由节点信任度的量化

r_j 不仅是 r_i 的邻居，也可能是网络中其它节点 $r_k\in R$ $(k\neq i\neq j,\ e_{kj}\in E)$ 的邻居。因此，路由节点信任度 $\mathrm{TD}(r_{ij})$ 的量化应包含两部分：一是 r_i 主动观测得到的对 r_j 的直接信任度 $\mathrm{DTD}(r_{ij})$，二是 r_i 通过路由信息交换，从其它节点 r_k 获得的对 r_j 的间接信任度 $\mathrm{ITD}(r_{kj})$，即

$$\mathrm{TD}_t(r_{ij})=w_1\,\mathrm{DTD}_t(r_{ij})+w_2\,\mathrm{ITD}_t(r_{kj})$$
$$(k\neq i\neq j,\ \ e_{ij},e_{kj}\in E,\ \ w_1,w_2\in[0,1],\ \ w_1+w_2=1)$$

其中权值 w_1, w_2 表示 DTD 和 ITD 在量化 $\mathrm{TD}(r_{ij})$ 时所占的比例，为防止敌人恶意诋毁，一般取 $w_1>w_2$。

(1)直接信任度测量　r_i 对 r_j 直接信任度 $\mathrm{DTD}(r_{ij})$ 的测量也是依据路由结构所面临的安全威胁及路由协议运行的安全机制。认证(authentication)和加密(confidentiality)是目前主要的两种路由信息安全机制(表2)，二者都可提供信息级(IL)或包级(PL)的安全服务[10]。r_j 采用不同的安全机制，可

带给 $\mathrm{DTD}(r_{ij})$ 不同的信任度增加值 $\mathrm{IV}(r_{ij})$。令 r_i 对实施 x ($x \geq 0$)种安全机制的节点 r_j 的最大直接信任度为

表2 路由节点的安全机制及 $\mathbf{IV}(r_{ij})$ 举例

安全机制		标识(Label)	协议举例	$\mathrm{IV}(r_{ij})$ 举例(可配置)
认证	包级	$\mathrm{APL_{P2P}}$	OSPFv2 和 OSPFv3	0.1
		$\mathrm{APL_{E2E}}$	N/A	0.2
	信息级	$\mathrm{AIL_{P2P}}$	N/A	0.3
		$\mathrm{AIL_{E2E}}$	带数字签名的 OSPF ([2])	0.4
加密	包级	CPL	OSPFv3	0.2
	信息级	CIL	N/A	0.4

P2P(point to point)：点到点。
E2E(end to end)：端到端，提供比P2P更强的保护。

$\mathrm{DTD}^{\max}(r_{ij}) = \sum_{x \geq 0} \mathrm{IV}_{\mathrm{Label}(x)}(r_{ij})$，比如应用 $\mathrm{APL_{P2P}}$ 和 CPL 安全机制的 $\mathrm{DTD}^{\max}(r_{ij}) = \mathrm{IV}_{\mathrm{APL_{P2P}}}(r_{ij}) + \mathrm{IV}_{\mathrm{CPL}}(r_{ij}) = 0.1 + 0.2 = 0.3$。如果 r_j 无任何安全机制，则 $\mathrm{DTD}^{\max}(r_{ij}) = 0$；如果 r_j 动态增减 $x'(x' \geq 0)$ 种安全机制，$\mathrm{DTD}^{\max}(r_{ij})$ 会随之增减：$\mathrm{DTD}^{\max}(r_{ij}) = \mathrm{DTD}^{\max}(r_{ij}) \pm \sum_{x' \geq 0} \mathrm{IV}_{\mathrm{Label}(x')}(r_{ij})$。

另一方面，网络路由攻击(包括外部攻击和内部攻击[10])普遍且后果严重。通过IDS(如Ji-Nao[11])等手段可以检测和隔离路由攻击。在定长周期 Δt 内，若检测到 λ 次对 r_j 的攻击，$\mathrm{DTD}(r_{ij})$ 呈指数下降：$\mathrm{DTD}_t(r_{ij}) = \mathrm{DTD}_{t-\Delta t}(r_{ij}) - 2^{\lambda-1}\mathrm{DV}(r_{ij})$ $(\lambda \geq 1)$，直到 $\mathrm{DTD}(r_{ij}) = 0$。若 Δt 内无路由攻击，曾失去一些信任度的 $\mathrm{DTD}(r_{ij})$ 则线性增加一个变化值 $\mathrm{CV}(r_{ij})$，同时重置攻击次数 $\lambda = 0$，直到 $\mathrm{DTD}(r_{ij})$ 恢复到 r_j 被攻击前的最大信任度为止：$\mathrm{DTD}(r_{ij}) = \mathrm{DTD}^{\max}(r_{ij})$。

(2) 间接信任度测量　r_i 对 r_j 间接信任度 $\mathrm{ITD}(r_{kj})$ 的测量是通过路由更新信息的洪泛。t 时刻，当 r_i 得到 r_k 发出的 $\mathrm{TD}_{t'}(r_{kj})$，$t' < t$，就更新其 $\mathrm{ITD}_t(r_{kj})$：

$$\mathrm{ITD}_t(r_{kj}) = \frac{\sum_{k=1,k\neq i\neq j}^{|R|} (\mathrm{TD}_{t'}(r_{kj}) - \mathrm{TD}_{t'}(r_{ij})) \times \mathrm{TD}_{t'}(r_{ik})}{|R|}, \quad t' < t$$

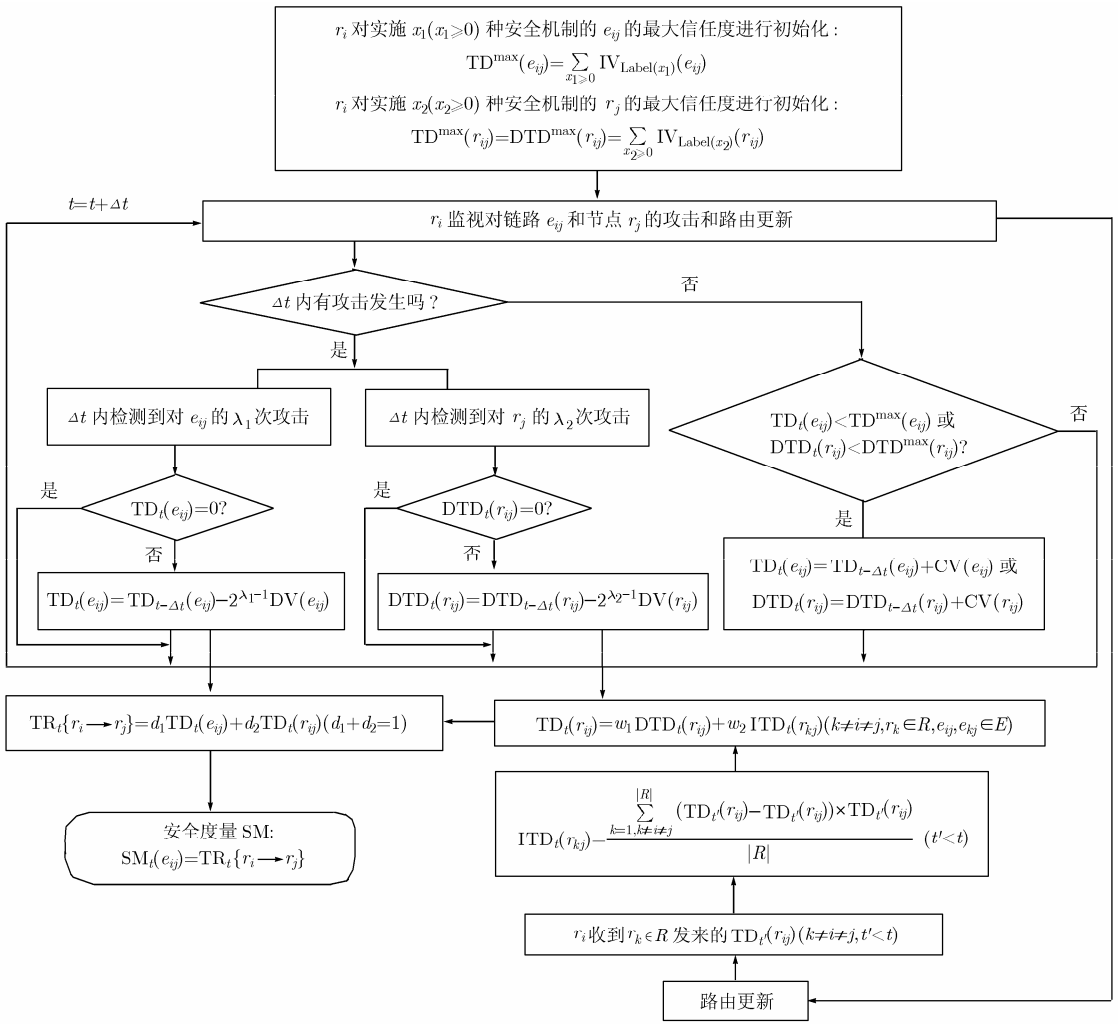

图1　信任模型及安全度量

其中 $|R|$ 是 G 中节点个数。显然，$\mathrm{ITD}(r_{kj})$ 与 r_i 对 r_k 的信任程度 $\mathrm{TD}(r_{ik})$ 有关，$\mathrm{TD}(r_{ik})$ 越高，$\mathrm{ITD}(r_{kj})$ 的更新程度越大，说明在量化 $\mathrm{TD}(r_{ij})$ 时，r_i 对其它节点观测意见的采纳程度，取决于 r_i 对这些节点的信任程度。

通过以上对通信链路和路由节点信任度的测量，为路由节点间建立了信任关系，得到一个量化的信任模型和链路 e_{ij} 在 t 时刻的安全度量 $\mathrm{SM}_t(e_{ij})$ (图1)。

3　SMRA 算法

安全度量SM可以和其它路由度量(如带宽、延时)共同应用于多约束的QoS路由机制(如QOSPF[12])。为方便讨论，本文改进原OSPF算法[13]，仅以SM为选路标准而得到SMRA安全路由算法(图2)：根据式(1)中路径安全度量的定义，SMRA定义比较函数FindSecureNode，输入是从源 s 到两个备选下一跳 v_1, v_2 的路径安全度量 $v_1\cdot\mathrm{sm}$ 和 $v_2\cdot\mathrm{sm}$，输出是从 v_1，v_2 中选出的较安全的下一跳。SMRA仍然基于Dijkstra's算法，由于FindSecureNode函数只是增加了一个常量因子，所以SMRA的计算复杂度与Dijkstra's算法相同，即 $O(|E|+|R|\log|R|)$。

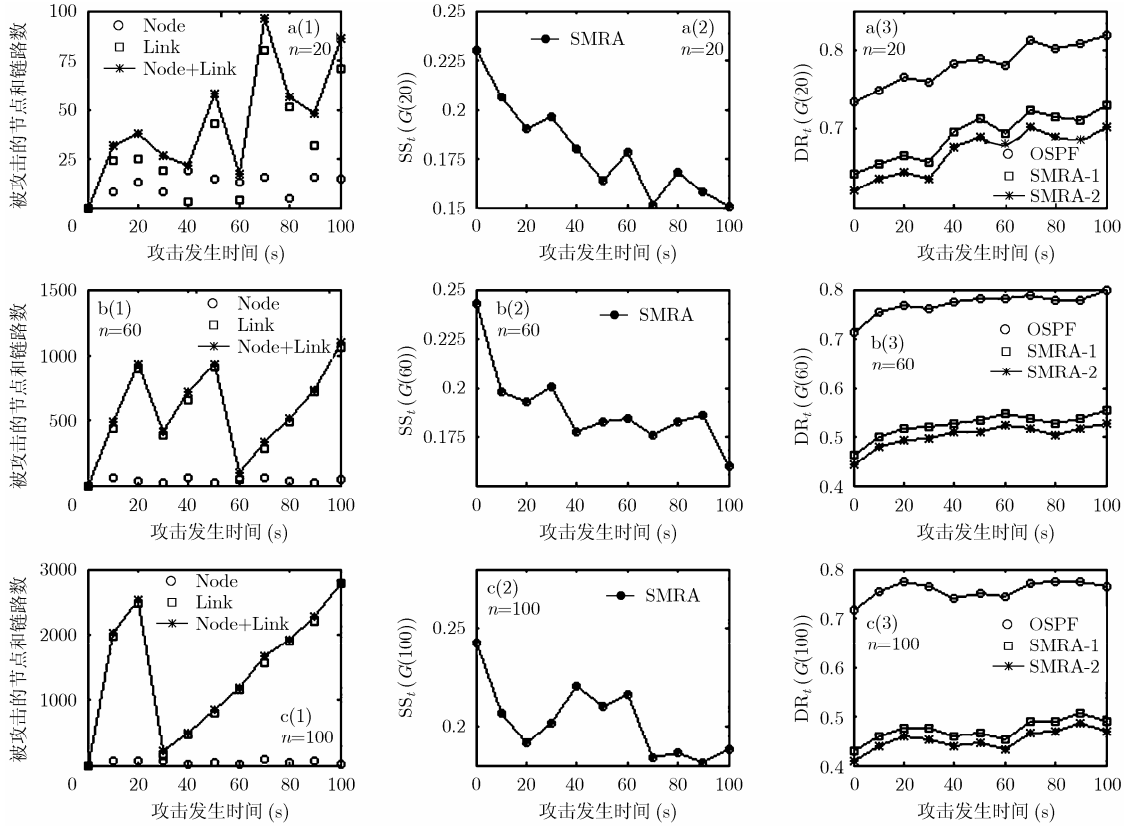

图 2　SMRA 算法伪码

4　仿真及性能分析

本节对应用SM的SMRA算法与传统OSPF算法进行了仿真和性能比较。令SMRA-1 和SMRA-2 分别表示不含和包含间接信任度测量部分。仿真以Waxman模型[14]随机生成拓扑网络 G：在矩形坐标区域内随机分布 n 个路由节点，任意节点对间有链路的概率为 $P(i,j)=\beta\exp\left(\dfrac{-d(i,j)}{\alpha d_{\max}}\right)$，

其中 $d(i,j)$ 是 r_i，r_j 之间的 Euclid 距离，$d_{\max}$ 是节点间可能的最大距离，α 控制长短边的比例，β 控制节点的度。G 中所有源和目的对间最多有 $\mathrm{PN}(n)=C_n^2$ 条路径。令初始时刻 $(t=0)$，$\mathrm{TD}_0(e_{ij})=\mathrm{TD}^{\max}(e_{ij})$ 和 $\mathrm{DTD}_0(r_{ij})=\mathrm{DTD}^{\max}\cdot(r_{ij})$ 在区间 [0,1] 内均匀分布，那么在 SMRA-1 中，$\mathrm{TD}_0(r_{ij})=\mathrm{DTD}_0(r_{ij})$；在 SMRA-2 中，令 $w_1=0.8$，$w_2=0.2$，$\mathrm{ITD}_0(r_{ij})=0$，则 $\mathrm{TD}_0(r_{ij})=0.8\times\mathrm{DTD}_0(r_{ij})+0.2\times\mathrm{ITD}_0(r_{ij})$ $=0.8\,\mathrm{DTD}_0(r_{ij})$。如果令式(2)中的权值 d_1, d_2 取相同值 0.5，即得到反映网络初始安全状态的在区间[0,1]内均匀分布的安全度量 $\mathrm{SM}_0(e_{ij})$。总仿真时间 $T=100$s，每隔 10s 同时触发一次链路攻击和节点攻击，随机选择攻击目标(一个目标可以被攻击多次)并更新 $\mathrm{TD}(e_{ij})$ 和 $\mathrm{TD}(r_{ij})$，选择下列参数来评价 SMRA 算法和 OSPF 算法的性能。

(1) 网络安全状态 $\mathrm{SS}_t(G(n))$　t 时刻 $(0\le t\le T)$，n 节点的 G 中所有链路的平均安全度量。$\mathrm{SS}_t(G(n))$ 随攻击的随机发生而动态变化。

$$\mathrm{SS}_t(G(n))=\left(\sum_{e_{ij}\in E(G)}\mathrm{SM}_t(e_{ij})\right)\Big/|E(G)|$$

$$=\left(\sum_{e_{ij}\in E(G)}(d_1\,\mathrm{TD}_t(e_{ij})+d_2\,\mathrm{TD}_t(r_{ij}))\right)\Big/|E(G)|$$

(2) 网络丢包率 $\mathrm{DR}_t(G(n))$　t 时刻$(0\le t\le T)$，n 节点的 G 中被攻击链路和节点的丢包数与网络传输数据包总量的比率。设任意路径 $p_k\in G(k\in[1,\mathrm{PN}(n)])$ 在 t 时刻的安全度量为 $\mathrm{SM}_t(p_k)$，所有路径的发包量均为 C，那么：

$$\mathrm{DR}_t(G(n))=1-\left(\sum_{k\in[1,\mathrm{PN}(n)]}(\mathrm{SM}_t(p_k)\times C)\right)/(\mathrm{PN}(n)\times C$$

$$=1-\left(\sum_{k\in[1,\mathrm{PN}(n)]}\mathrm{SM}_t(p_k)\right)\Big/\mathrm{PN}(n)$$

实验1　主要观察网络 G 的 $\mathrm{SS}_t(G(n))$ 动态变化情况。图3a(1)，3b(1)，3c(1)分别以“□”和“○”表示10次随机攻击的链路数和节点数。图3a(2)，3b(2)，3c(2)显示，随着被攻击目标(链路或节点)数量的增减，$\mathrm{SS}_t(G(n))$ 会随之伏起。这是因为被攻击目标的TD值呈指数下降，当被攻击目标数量增多时，涉及被攻击目标TD的链路SM随之减少，自然引起网络安全状态的迅速下降；相反，当被攻击目标数量减少时，曾被攻击过，而在本次攻击中幸免的目标TD值线性上升，涉及这些目标TD的链路SM也随之增加，因此网络安全状态会逐渐回升。总体来看，随着仿真的推移和网络不断面临攻击，网络的安全状态 $\mathrm{SS}_{100}(G(n))$ 比 $\mathrm{SS}_0(G(n))$ 明显下降约29%，说明路由攻击对网络安全性所造成的影响。

实验 2　主要比较在有攻击的网络 G 中，SMRA 和 OSPF 的丢包性能。图 3a(3)，3b(3)，3c(3)显示，OSPF 和 SMRA 的 $\mathrm{DR}_t(G(n))$ 都随着网络安全状态的伏起而升降，而且随着攻击次数的逐渐增加，总体都呈上升趋势，说明网络丢包率与网络的安全状态紧密相关。由于 OSPF 路由计算时并不考虑链路的安全度量，所以沿 OSPF 路径传输数据时不能主动绕开不良节点和攻陷链路。相反，SMRA 路由时尽量躲避被攻击目标，因此其网络丢包率明显低于 OSPF 网络。在仿真时间 T 内，定义 $\mathrm{DR}_{[0,T]}(G_{\mathrm{SMRA}}(n))$ 低于 $\mathrm{DR}_{[0,T]}(G_{\mathrm{OSPF}}(n))$ 的平均百分比为

$$\frac{1}{T}\sum_{0\le t\le T}\frac{(\mathrm{DR}_t(G_{\mathrm{OSPF}}(n))-\mathrm{DR}_t(G_{\mathrm{SMRA}}(n)))}{\mathrm{DR}_t(G_{\mathrm{OSPF}}(n))}\times 100\%\,,$$

图 3a(3)，3b(3)，3c(3)显示，$\mathrm{DR}_{[0,T]}(G_{\mathrm{SMRA}}(20))$ 低出 $\mathrm{DR}_{[0,T]}(G_{\mathrm{OSPF}}(20))$ 约 10%，$\mathrm{DR}_{[0,T]}(G_{\mathrm{SMRA}}(60))$ 低出 $\mathrm{DR}_{[0,T]}(G_{\mathrm{OSPF}}(60))$ 约 36%，$\mathrm{DR}_{[0,T]}(G_{\mathrm{SMRA}}(100))$ 低出 $\mathrm{DR}_{[0,T]}(G_{\mathrm{OSPF}}(100))$ 约 53%。可见网络规模越大，SMRA 比 OSPF 的丢包率性能更优，说明 SMRA 对于大型网络的适应性和可扩展性。

实验 3　主要比较 SMRA-1 和 SMRA-2 的网络丢包性能。图 3a(3)，3b(3)，3c(3)显示，SMRA-2 的丢包率低于 SMRA-1。可见对某路由节点的直接信任度测量有主观片面性，而参考其它节点观测意见的间接信任度测量可增加其客观性和准确度。

实验 4　任意时刻 t，令 $\mathrm{TD}_{\mathrm{ave}}(r(t))$ 表示平均一个被攻击节点的信任度，$\mathrm{UT}_{\mathrm{ave}}(r(t))$ 表示平均一个被攻击节点在所有路径中的使用次数，那么：

$$\mathrm{TD}_{\mathrm{ave}}(r(t))=\left(\sum_{r\in\mathrm{ATKset}(t)}\mathrm{TD}_t(r)\right)\Big/|\,\mathrm{ATKset}(t)\,|,\quad 0\le t\le T$$

$$\mathrm{UT}_{\mathrm{ave}}(r(t))=\left(\sum_{r\in\mathrm{ATKset}(t)}\sum_{k\in[1,\mathrm{PN}(n)]}\delta_{p_k}(r(t))\right)\Big/|\,\mathrm{ATKset}(t)\,|$$

$$0\le t\le T$$

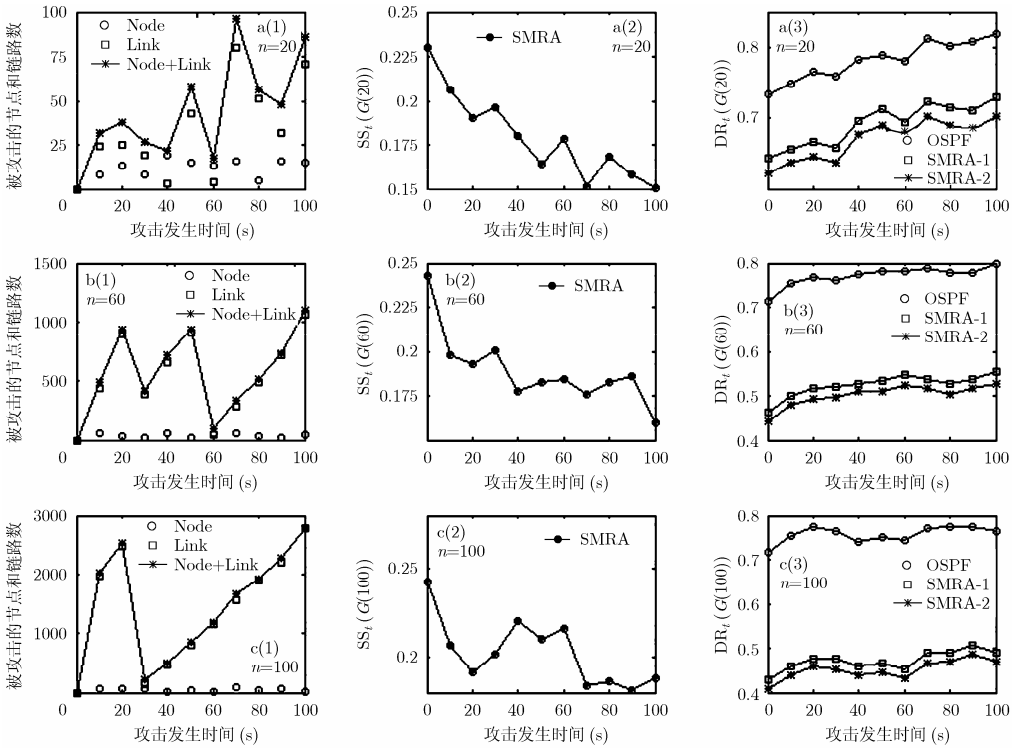

图 3 不同规模网络中，链路和节点被随机攻击的情况，网络安全状态的动态变化情况以及网络的丢包率趋势

其中 t 时刻，ATKset(t) 表示随机攻击的节点集合，$\mathrm{TD}_t(r)$ 表示攻击发生后节点 $r \in \mathrm{ATKset}(t)$ 的信任度，$\delta_{p_k}(r(t))$ 表示被攻击节点 $r \in \mathrm{ATKset}(t)$ 在路径 $p_k \in G(k \in [1,\mathrm{PN}(n)])$ 中的出现次数。采样 10 次(t =10s,20s,…,100s)节点和链路攻击，分别得到 $\mathrm{TD}_{\mathrm{ave}}(r(t))$ 和 $\mathrm{UT}_{\mathrm{ave}}(r(t))$ 的变化情况，以及 $\mathrm{TD}_{\mathrm{ave}}(e(t))$ 和 $\mathrm{UT}_{\mathrm{ave}}(e(t))$ 的变化情况。图 4(a) 显示，$\mathrm{UT}_{\mathrm{ave}}(r(t))$ 与 $\mathrm{TD}_{\mathrm{ave}}(r(t))$ 的变化趋势基本一致。说明当某个频受攻击的节点的信任度呈指数下降时，SMRA 网络对该节点的使用率会随之迅速降低，而经过一段安全周期，该节点的信任度开始恢复时，SMRA 网络对该节点的使用率也会随之递增。图 4(b)中关于通信链路的 $\mathrm{TD}_{\mathrm{ave}}(e(t))$，$\mathrm{UT}_{\mathrm{ave}}(e(t))$ 的情况也是类似的。这说明应用 SMRA 算法的网络提高了网络防御攻击，安全传输数据的能力。

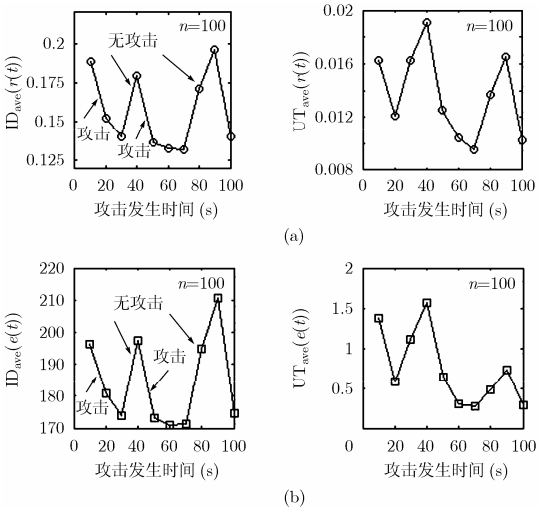

图 4 平均存在一个被攻击节点或链路时，其信任度和使用次数的变化情况

5 结束语

安全度量及安全路由是一个新的，有价值和挑战性的研究领域。在已有的安全度量研究中，大多是根据所采用加密算法的密钥长度[15]，或解密所耗费的时间和资源量来决定数据传输的安全级别[16]，没有精确量化的安全度量值，而且划分的安全等级也不能随网络安全状态动态变化，并不适用于路由决定。

本文以信任关系建立难，失去容易的思想，通过量化网络实体：通信链路和路由节点的信任度，在邻居节点间建立信任关系，基于该信任模型定义适用于路由选择过程，随网络安全状态变化而动态更新的安全度量 SM，并提出基于 SM 的安全路由算法 SMRA。仿真结果表明，SMRA 选路时尽量避开不安全节点和链路，提高了网络传输率，可扩展应用于大规模网络的安全路由，但是为机密应用绕道选择更安全路径时，可能会相应增加数据传输的路径跳数和延时等开销。

参 考 文 献

[1] IETF RPSecworking Group[DB/OL], http://www.ietf.org/html.charters rpsec-charter.html, 2003.

[2] Chakrabarti A and Manimaran G. Internet infrastructure security: A taxonomy. *IEEE Network*, 2002, 16(6): 13–21.

[3] Chakrabarti A and Manimaran G. A scalable method for router attack detection and location in link state routing. DCNL Tech. Report, 2002.

[4] Murphy S L and Badger M R. Digital signature protection of the OSPF routing protocol. In Internet Society Symposium on Network and Distributed Systems Security, San Diego, CA, USA, 1996: 93–102.

[5] Cheung S. An efficient message authentication scheme for link state routing. In 13th Annual. Computer Security Applications Conference, San Diego, CA, USA, 1997: 90–98.

[6] Cheung S and Levitt K N. Protecting routing infrastructure from denial of service using cooperative intrusion detection. In New Security Paradigms Workshop, Cumbria, UK, 1997: 23–26.

[7] 范炜玮，苏金树. 路由协议安全性分析与安全路由协议域研究. 武汉大学学报(理学版), 2004, 50(S1): 119–122.
Fan Wei-wei, and Su Jin-shu. The study of routing protocol security and secure routing protocol domain. *J. Wuhan Univ.* (Nat. Sci. Ed.), 2004, 50(S1): 119–122.

[8] Gupta M and Melam N. Authentication/confidentiality for OSPFv3. Internet draft, 2002.

[9] Kent S and Atkinson R. Security architecture for the internet protocol. RFC 2401, 1998.

[10] Huang Di-Jiang, Medhi Deep, and Beard Cory. Trust analysis of link state network routing. In Proceedings of the 2nd International Workshop on Trusted Internet (TIW), Hyderabad, India, 2003: 201–211.

[11] Wang Fei-yi, Gong F, and Wu F S. Intrusion detection for link state routing protocol through integrated network management. In Proceedings of the 8th International Conference on Computer Communications and Networks, Boston, MA, 1999: 634–639.

[12] Apostolopoulos G and Williams D. QoS routing mechanism and OSPF extensions. RFC 2676, 1999.

[13] Moy J. OSPF version 2. RFC 2328, IETF Network Working Group, 1998.

[14] Waxman B M. Routing of multipoint connections. *IEEE J. Select. Areas Commun.*, 1988, 6(9): 1617–1622.

[15] Almerhag I A and Woodward M E. Key length as a QoS routing metric. In Sixth Informatics Workshop, University of Bradford, 2005: 23–24.

[16] Nielsen F. Report about approaches to security metrics, Presented at CSSPAB Workshop on Approaches to Measuring Security, Washington, D.C., 2000: 13–14.

张　静：　女，1970年生，副教授，从事专业为通信与信息系统.
胡捍英：　男，1961年生，教授，从事专业为通信与信息系统.
童　珉：　男，1963年生，副教授，从事专业为通信与信息系统.
李庆荣：　男，1971 年生，副教授，从事专业为通信与信息系统.