第43卷第4期 南京航空航天大学学报 Vol. 43 No. 4
2011年8月 Journal of Nanjing University of Aeronautics & Astronautics Aug. 2011

基于直觉模糊理论的MANET主观信任模型

廖 俊[1,2] 张 宏[1] 蒋黎明[1] 姜海涛[1]

(1.南京理工大学计算机科学与技术学院,南京,210094;2.中国药科大学信息管理与信息系统系,南京,210009)

摘要:移动自组织网络缺乏可信第三方提供信任度量,节点可以依靠对其他节点特定行为进行主观判断以决定对其信任程度,而且行为特征还具有呈现与否的程度大小或者不知情的问题,为此,本文提出了一种基于直觉模糊理论的MANET主观信任模型,并给出了信任的直觉模糊表述和实现方法,用于量化和评估节点的可信程度。仿真实验表明本模型是适合移动自组网安全的信任模型,能够有效地抵御网络攻击和信任模型攻击。

关键词:移动无线自组网;信任模型;直觉模糊集;主观信任

中图分类号:TP393.08 **文献标识码**:A **文章编号**:1005-2615(2011)04-0538-06

Subjective Trust Model Based on Intuitionistic Fuzzy Set Theory for MANET

Liao Jun[1,2], *Zhang Hong*[1], *Jiang Liming*[1], *Jiang Haitao*[1]

(1. School of Computer Science and Technology, Nanjing University of Science and Technology, Nanjing, 210094, China;
2. Department of Information Management and Information Systems,
China Pharmaceutical University, Nanjing, 210009, China)

Abstract: The absence of trust valuation presented by certain trusted third party in mobile ad hoc network (MANET) may result in that a node's subjective trust in other nodes will only rely on their behavior, but the behavior may not present trust characteristics precisely. A subjective trust model based on intuitionistic fuzzy set theory (STMIFS) is proposed to quantify and evaluate the trust worthiness of nodes. Its intuitionistic fuzzy description and implementation are also given. The simulations show that STMIFS is suitable for MANET security and able to effectively defend against both ad hoc network attacks and trust model attacks.

Key words: mobile ad hoc network; trust model; intuitionistic fuzzy set; subjective trust

MANET中移动节点会受到诸如能量和计算能力等各种资源的限制,而且节点在缺乏稳定信任约束的合作中,容易在自身利益的驱动下表现出自私性、恶意洪泛、拒绝服务攻击等不端行为,严重影响系统的安全性。所以,信任成为了MANET安全研究的焦点之一。目前对信任的研究主要包含基于凭证和主观信任的两种信任关系。基于凭证的信任关系是对客体(如标识、证书等)的信任,所以可以精确地描述、推理和验证。由于MANET节点的运算资源、信道资源相对有限,并且节点具有匿名性和高度自治,使得无法部署复杂的安全协议和加密算法。因此在固定网络环境中常用的认证方法,依赖可信的第三方建立信任关系在MANET中已不再可行;黄刚等人[1]提出基于分簇的广播认证机制N-μTESLA提供信任,但认证问题研究还处于起步阶段。第二种信任是主体之间的信任,是对主体的特定特征或行为的特定级别的主观判断。本文使用Gambetta[2]给出的有关信任的定义,认为信任

基金项目:国家自然科学基金(90718021, 61003210, 60903027)资助项目;江苏省自然科学基金(BK2007593)资助项目。

收稿日期:2011-01-19;**修订日期**:2011-04-07

通讯作者:廖俊,男,博士研究生,讲师,1976年生,E-mail:liaojun@cpu.edu.cn。

是主体关于其他主体具有完成某一特定任务能力可能性的主观判断,其程度依赖于主体对于信任对象的直接经验和推荐信息。对主观信任进行研究,远比对客体之间的信任关系进行研究要复杂得多[3]。主观信任本质上是基于信念的,具有很强的主观性、模糊性,无法精确地加以描述和验证。本文旨在构造一种MANET环境下的基于直觉模糊理论的主观信任模型(Subjective trust model based on intuitionistic fuzzy set theory, STMIFS),研究信任的类型定义机制、定量描述机制、评价机制和推导机制。

1　相关研究

为了度量信任关系,Blaze等人[4]首次将信任管理的概念引入到网络安全领域,现有的安全技术都与信任相关,或者预先假定了某种信任前提,或者目的是为了获得或创建某种信任关系。Beth等人[5]提出一个基于经验和概率统计的信任模型,给出经验推荐所引出的信任度推导和综合计算公式,但是Beth模型对直接信任的定义比较严格,仅采用肯定经验对信任关系进行度量。Abdul-Rahman等人[6]认为信任是非理性的,为某一实体对其他实体实施某种行为可能性的主观度量,包括具体内容和程度划分两方面,提出分布式信任评估模型,将信任关系分为直接信任和推荐信任,采用离散数值度量信任关系。Jøsang等人[7]提出了事实空间和观念空间描述和度量信任关系,提供了主观逻辑算子用于信任度的推导和综合计算。使用了事实空间中的肯定事件和否定事件对信任关系进行度量,提供了推荐算子用于信任度的推导。上述研究工作中存在计算代价和通信代价高无法适应MANET资源受限的问题,同时无法支持推荐信任关系的自动形成与更新,对恶意推荐信息也缺乏抵御的能力。Whitby等人[8]通过递归过滤的方法减少恶意推荐的影响,评价者的信息超出合理范围被视为恶意推荐,将不参与信任值的计算。通过对合理范围的调节,该方法能够抵御恶意推荐。但同样使用了概率统计的假设检验思想对信任关系的度量进行解释,由于主观信任的主观性、不确定性与随机性表现为模糊性,使用概率统计的方法无法描述主观信任关系的真实情况。

模糊理论的提出将数学研究的对象扩大到质与量统一的对象和具有模糊性的概念。Tang等人[3]运用模糊集合理论对信任评估问题进行了数学建模,并给出了主体信任的一般评价机制和信任关系的推导规则。但没有提供推荐信任的评估方法以及信任评价尺度的具体含义。Song等人[9]提出的FuzzyTrust则采用模糊逻辑推理规则来计算节点的全局声誉。具有较高的恶意节点检测率,但其抵御的恶意行为仅为交易中的不诚实行为,而不能抵御各种针对信任机制的攻击。Luo等人[10]提出了基于模糊关系理论推荐信任的MANET信任模型,给出了具体的全局信任的模糊相似性推荐和判决方法,但信任度量属性仅考虑数据转发。上述研究中都使用了模糊理论来处理信任,但不能对信任的犹豫程度作出描述,缺乏抵御恶意推荐等针对信任模型攻击的能力。分析上述问题,本文利用Atanassov提出的直觉模糊集(IFS)[11]理论,其核心是增加了一个新的属性参数非隶属度函数,因而可描述非此非彼的模糊概念。该理论更细腻地刻画客观世界的模糊性本质,可以更好地针对信任中的犹豫程度作出信任决策。所以,本文将直觉模糊集合理论引入到MANET主观信任模型研究中,以解决MANET中具有模糊性的主观信任建模的问题。定义了关键属性作为评判因素,运用直觉模糊合成和变换给出了一个直接信任值计算模型,并提出了推荐信任关系的合成计算,构造了一个主观信任模型。仿真实验表明STMIFS在存在不端行为的MANET中较好地抵御了网络和信任模型攻击,验证了所提出的信任模型的有效性和可靠性。

2　主观信任模型

对MANET信任进行建模的关键在于如何对节点的信任度进行定义、评价和推导。所以信任研究的内容应当包括对目的节点信任的表述和度量、信任的推导和综合计算。如图1所示显示了MANET中的直接信任、推荐信任和间接信任。

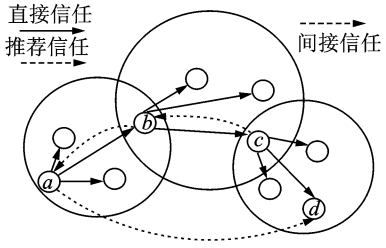

图1　直接信任、推荐信任和间接信任

定义1　直接信任是指相邻节点通过无线信道监测,彼此之间建立了一种直接信任关系,信任度来源于双方已定义的关键属性得出的直接经验。

定义2　推荐信任是指信任源、信任目的节点之间不相邻,但是可以通过请求其他对目的节点有直接信任的节点,由这些节点通过中间节点逐跳推

荐给源节点。

定义3 间接信任是源节点根据直接信任和推荐节点的推荐建立的一种信任关系，他们之间的信任度是由路径上所有节点评估得出的结果。

2.1 直接信任计算

直接信任度的计算采用直觉模糊综合评判的方法，使用已定义关键属性作为评判因素，确定权重矩阵和隶属矩阵，通过直觉模糊变换的方法计算节点的直接信任度。

定义4(直觉模糊集[11]) 给定论域X，X上的一个直觉模糊集A定义为$A=\{<x,\mu_A(x),\nu_A(x)>|x\in X\}$，其中$\mu_A(x):X\to[0,1]$和$\nu_A(x):X\to[0,1]$分别代表$A$的隶属函数$\mu_A(x)$和非隶属函数$\nu_A(x)$，且对于$A$上的所有$x\in X$，$0\leqslant\mu_A(x)+\nu_A(x)\leqslant 1$成立。

对于X上的每一个直觉模糊集，称$\pi_A(x)=1-\mu_A(x)-\nu_A(x)$为$x$的直觉指数，它表示$x$对$A$的犹豫度。

定义5(直觉模糊集算子) 设A和B是给定论域X上的直觉模糊子集，则

$$A*B=\{<x,\frac{\mu_A(x)+\mu_B(x)}{2(\mu_A(x)\mu_B(x)+1)},\frac{\nu_A(x)+\nu_B(x)}{2(\nu_A(x)\nu_B(x)+1)}>|\text{对一切 } x\in X\} \tag{1}$$

$$A\bigtriangledown\!\!\bigtriangleup B=\{<x,\frac{2\mu_A(x)\mu_B(x)}{\mu_A(x)+\mu_B(x)},\frac{2\nu_A(x)\nu_B(x)}{\nu_A(x)+\nu_B(x)}>|\text{对一切 } x\in X\} \tag{2}$$

设$U=\{u_1,\cdots,u_m\}$为前提论域，表示评判因素集，其中$u_1,\cdots,u_m$分别是MANET中的m个关键属性集函数。$E=\{e_1,\cdots,e_n\}$为结论论域，表示评语集。μ_A,ν_A为模糊集A的隶属函数和非隶属函数，本文采用三角直觉模糊隶属函数。

定义6 直觉模糊权重因素集$W=[w_1,\cdots,w_m]$，其中$w_1,\cdots,w_m$分别为因素$u_1,\cdots,u_m$的权重。表示各因素在评价中的相对重要性，用于刻划画关键属性对直接信任的影响程度。

定义7 信任向量$\boldsymbol{B}=[b_1,b_2\cdots,b_m]$，按照直觉模糊合成[12]和直觉模糊变换的原理，直接信任的直觉模糊综合评判就是进行如下的直觉模糊变换

$$\boldsymbol{B}=\boldsymbol{W}\circ\boldsymbol{R} \tag{3}$$

式中：$\boldsymbol{R}$为直觉模糊评价矩阵，其中$\mu_{i,j}(i=1,\cdots,m,j=1,\cdots,n)$为第$i$个因素$\mu_i$针对于第$j$个结论因素$e_j$根据隶属函数所得到的信任度，$\nu_{i,j}(i=1,\cdots,m,j=1,\cdots,n)$为第$i$个因素$\nu_i$针对于第$j$个结论因素$e_j$根据非隶属函数所得到的不信任度；$\boldsymbol{B}=\{b_1,\cdots,b_n\}$为得到的模糊综合评价集，使用定义5定义的$\bigtriangledown\!\!\bigtriangleup$，$*$算子进行运算，得出式(4)。

$$\boldsymbol{B}=\boldsymbol{W}\circ\boldsymbol{R}=\{w_1,\cdots,w_m\}\circ\begin{bmatrix}<\mu_{1,1},\nu_{1,1}>,\cdots,<\mu_{1,n},\nu_{1,n}>\\ \vdots\qquad\qquad\vdots\\ <\mu_{m,1},\nu_{m,1}>,\cdots,<\mu_{m,n},\nu_{m,n}>\end{bmatrix}=\{<\mu_{b_1},\nu_{b_1}>,\cdots,<\mu_{b_n},\nu_{b_n}>\} \tag{4}$$

直接信任T_{st}^D表示如下

$$T_{st}^D=Dt(x_s,x_t)=\max_{\mu}\{<\mu_{b_1},\nu_{b_1}>,\cdots,<\mu_{b_n},\nu_{b_n}>\} \tag{5}$$

2.2 推荐信任计算

当某个具有目的节点直接信任的节点接收到信任请求时，通过反向路径利用中间节点逐跳推荐给信任请求源节点。

$$T_{kt}^R=\mathrm{Re}(x_k,x_t)=\{\mu_{R_{kt}},\nu_{R_{kt}}\}$$

$$\mu_{R_{kt}}=\begin{cases}0.25+\dfrac{(4S_{s,k}^t-R_{sk})}{4H_r} & R_{sk}<H_r\\ \dfrac{\varepsilon\times S_{s,k}^t}{\varepsilon\times S_{s,k}^t+F_{s,k}^t} & R_{sk}>H_r,\varepsilon\geqslant 1\end{cases} \tag{6}$$

$$\nu_{R_{kt}}=\begin{cases}0.25+\dfrac{(4F_{s,k}^t-R_{sk})}{4H_r} & R_{sk}<H_r\\ \dfrac{\varphi\times F_{s,k}^t}{S_{s,k}^t+\varphi\times F_{s,k}^t} & R_{sk}>H_r,\varphi>\varepsilon\geqslant 1\end{cases} \tag{7}$$

式中：T_{kt}^R表示推荐信任；R_{sk}表示节点s向k请求推荐的总数；H_r为推荐次数的阈值；$S_{s,k}^t$表示节点k向s推荐t所提供服务的成功次数；$F_{s,k}^t$表示节点k向s推荐t所提供服务的失败次数；ε为对节点可信的奖励系数；φ为对节点的不端行为的惩罚系数，且$\varepsilon\ll\varphi$。某节点提供善意推荐时，推荐可信度值的增加比较缓慢，若提供恶意推荐，可信度值将快速降低。少量的攻击行为会导致信任急剧下降，可使叛徒攻击者为不端行为付出巨大的信任代价。

2.3 间接信任计算

间接信任是根据其他节点的推荐建立的一种信任关系，源和目的之间的信任度是由其他实体的推荐和源节点对推荐节点的直接信任模糊合成得出的结果。

(1)单路径信任推荐

根据图2所示，当源节点s需要与目的节点t的信任关系，但是s节点与t节点无直接信任，而s节

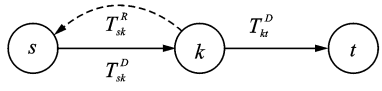

图2 两跳的单路径推荐

点与k 节点是直接信任,k 节点提供推荐信任。采用直觉模糊集合运算和直觉模糊合成可以计算间接信任

$$T_{st}^{I}=(Dt_{s,k}\circ \mathrm{Re}_{k,t})\circ Dt_{k,t}=\bowtie_{x_k\in X}(\triangleright\!\!\bowtie_{x_k\in X}(Dt(x_s,x_k)*\mathrm{Re}(x_k,x_t))*Dt(x_k,x_t)) \tag{8}$$

如果将问题推广,用一条路径上的n 个节点代替单个k 节点,其节点的序列为$\{k_1,k_2,\cdots,k_n\}$,得到

$$T_{st}^{I}=(Dt_{s,k_1}\circ \mathrm{Re}_{k_1,k2})\circ\cdots\circ(Dt_{k_{n-1},k_n}\circ \mathrm{Re}_{k_n,t})\circ Dt_{k_n,t}=(Dt\circ \mathrm{Re})^{n}\circ Dt_{k_n,t} \tag{9}$$

(2)多路径信任推荐

根据图3 所示,当源节点s 需要与目的节点t 的信任关系,但是s 节点与t 节点无直接信任,但存在节点的序列为$\{k_1,k_2,\cdots,k_n\}$,而s 节点与k_i 节点是直接信任,k_i 节点提供推荐信任。

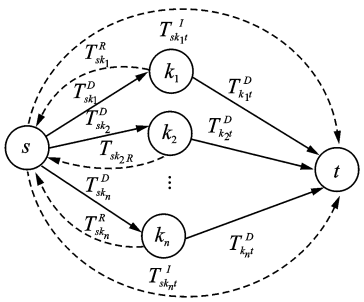

图 3　两跳的多路径推荐

$$T_{st}^{I}=(T_{sk_1t}^{I}\cup T_{sk_2t}^{I}\cdots\cup T_{sk_nt}^{I})=\bigcup_{i=1}^{n}(Dt_i\circ \mathrm{Re}_i)\circ Dt_t=\bigcup_{i=1}^{n}\bowtie_{x_{k_i}\in X}(\triangleright\!\!\bowtie_{x_{k_i}\in X}(Dt(x_s,x_{k_i})*\mathrm{Re}(x_{k_i},x_t))*Dt(x_{k_i},x_t)) \tag{10}$$

同样将问题推广,将每个两跳路径上单个k_i 节点变为路径上的m 个节点,得到

$$T_{st}^{I}=\bigcup_{i=1}^{n}(Dt\circ \mathrm{Re})^{m}\circ Dt_t \tag{11}$$

因此,MANET 网络端到端路径的信任值可以通过式(11)相应节点信任值的直觉模糊运算获得。

2.4　关键属性的选定

关键属性的选择首先要符合MANET 的结构特点,还需要满足可监测的要求以及体现客观性。对于MANET 节点信任评估,除了网络通信特性(如:转发指数)外还应该考虑该节点的自身物理属性,包括移动特性、无线信号特性以及空间特性等。为了提高信任模型的健壮性,对推荐信任的考察也放在关键属性中,做法是将节点做出的信任推荐结果反馈来参与直接信任的计算。

将MANET 信任评估的关键属性集定义为U =$\{$MAC 层指标,路由层指标,推荐信任指标,节点物理特性指标$\}$,MANET 中在计算资源很有限的情况下,关键属性可以采用表1 给出全集的一个子集。

表 1　信任模型关键属性指标

第一层指标	第二层指标			
MAC 层指标U_1	转发指数u_{11}	处理延迟u_{12}	数据传输率u_{13}	两跳邻居节点数u_{14}
路由层指标U_2	转发RREQ 指数u_{21}	转发RRER 指数u_{22}	转发RREP 指数u_{23}	处理RREP 延迟u_{24}
推荐信任指标U_3	推荐信任返回指数u_{31}	推荐服务成功指数u_{32}	推荐信任验证指数u_{33}	推荐信任准确度u_{34}
节点物理特性U_4	相对速度u_{41}	能量消耗u_{42}	信号强度u_{43}	信号变化率u_{44}

推荐信任指标U_3 的引入是为了抵御针对信任模型的拒绝推荐、恶意推荐、合谋攻击。节点推荐信任信息后将通过u_{31}体现,抑制拒绝推荐节点。u_{32},u_{33},u_{34}指数的反馈可以防御针对信任模型的恶意推荐攻击和合谋攻击。

3　仿真实验

MANET 网络攻击主要有不合作和数据修改、数据伪造,同时信任模型本身面临的攻击主要有拒绝推荐、恶意推荐、合谋推荐。仿真实验在网络模拟器ns-2 中采用 AOMDV[13]协议来对信任模型进行模拟并分析其性能。模拟使用50 设置了两种不同场景:单纯的MANET 网络攻击,以通过修改路由信息,可以导致网络数据流被丢弃的 Black hole 为对象。进而设置同时包括网络攻击和针对信任模型的恶意推荐、合谋推荐攻击。

3.1　网络攻击实验结果及分析

为了进行比较实验,使用 AOMDV[13],TME[14]和本文模型STMIFS 对路由开销比、分组投递率进行评价。

图4 为相对于恶意节点数路由开销比在不同模型下的比较结果分析图,本文路由开销比为产生的控制分组总数(除HELLO 和BEACON 包)和收到的数据包的总数之间的比例。随着恶意节点增

加，更多的路由被恶意节点获取，造成网络中恶意节点产生更多的路由控制数据包并且丢弃数据包，导致非常高的路由开销比。而在STMIFS中节点用监听的方式获取关键属性值，不产生额外的路由开销，并选择可信的路由屏蔽恶意节点发送的控制数据包，因此，STMIFS路由开销比显著下降。

图5为相对于恶意节点数分组投递率在不同模型下的比较结果分析图，从图中可以看出AOMDV在恶意节点数目增加时PDR急剧下降，因为AOMDV无法区分善意和恶意节点，因此，协议很容易选择被恶意修改的具有最短跳长或最高序列号的节点，因而导致数据流的中断。STMIFS模型利用直觉模糊的特性可以在节点信息不充分、与其他节点的存在关系不确定性时作出更好的信任决策，结果明显优于TME。

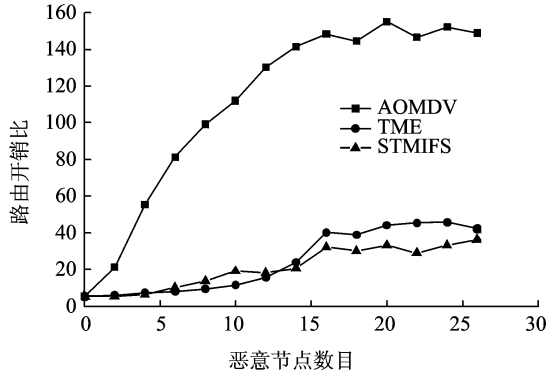

图4 相对于恶意节点数路由开销比在不同模型下的比较

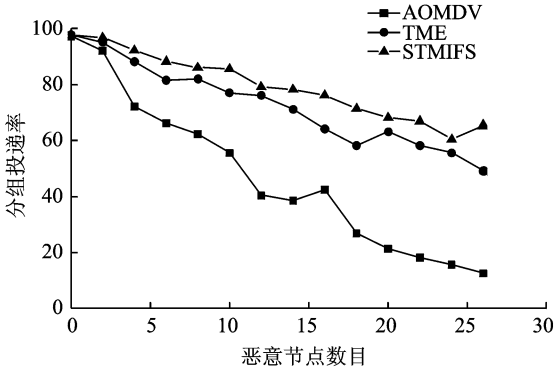

图5 相对于恶意节点数分组投递率在不同模型下的比较

3.2 信任模型攻击实验结果及分析

为了进行对信任模型的攻击比较实验，使用PureTrust[14]，TME[15]和本文模型STMIFS对路由开销比进行评价。

图6为在不同恶意推荐节点数影响下分组投递率的结果分析图，模拟恶意推荐，该类节点不仅进行恶意攻击，同时还会恶意抬高或降低其他节点的推荐信任度。PureTrust没有对信任模型攻击进行处理，使得节点的信任与真实情况偏离较大，TME模型较为有效地抑制了诋毁的影响。STMIFS在恶意节点所占比例超过30%后比TME有明显的提高，因为对推荐信任出现较大的摇摆时，进行推荐信任的相似度计算，验证推荐信任，并且对结果进行关键属性更新。

图7为在不同合谋推荐节点数影响下分组投递率的结果分析图，模拟合谋推荐，模型中的合谋恶意推荐节点其不仅进行恶意攻击，同时还会恶意抬高其他恶意节点的推荐信任度。STMIFS模型相比PureTrust和TME推荐夸大被明显抑制，由于采用了以下处理：采用节点作出的信任推荐结果反馈回直接信任的计算，并且多条路径的合成抑制了某几个节点合作对信任的影响。同时节点只有在收到推荐请求消息时才发送推荐信息，而没有收到请求消息就主动推荐的信息是不会被接收者采纳。这样使得多个合谋节点同时推荐不端节点的概率极低，从而破坏合谋攻击的条件。

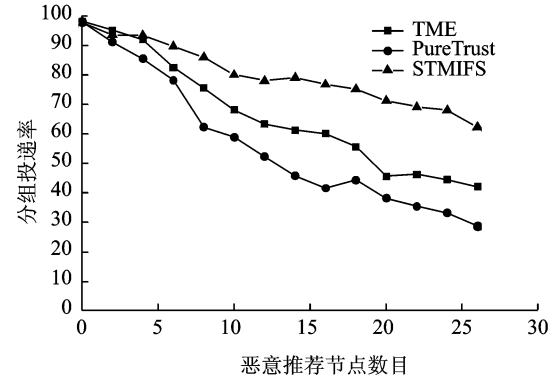

图6 相对于恶意推荐节点数分组投递率在不同模型下的比较

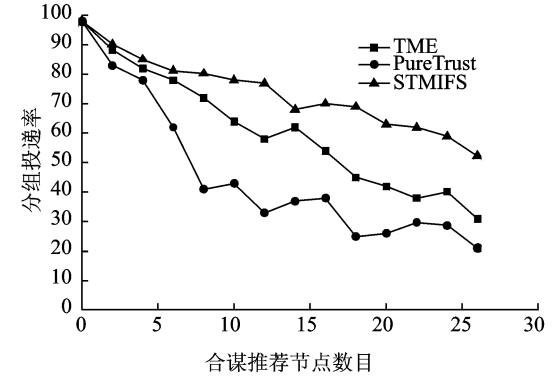

图7 相对于合谋推荐节点数分组投递率在不同模型下的比较

4　结束语

本文深入研究了MANET 网络环境中基于直观模糊集的节点主观信任及推荐信任的传递和合成问题,提出了一种 MANET 环境下的 STMIFS 模型。确定了MANET 信任模型的一个分层的关键属性集为信任的评估与处理服务,客观有效地体现网络行为特征。仿真实验中模拟了对MANET 网络的攻击和对信任模型攻击的不同情况,并分析了该模型的健壮性。验证了本文提出的使用直观模糊数据集方法处理信任中对主体特征和行为认知的主观性及不确定性的优越性。

参考文献:

[1] 黄刚,王汝传,许一帆. 无线传感器网络中基于分簇广播认证协议方案[J]. 南京航空航天大学学报,2010,42(1):72-76.

[2] Gambetta D. Trust:making and breaking cooperative relations [M]. Oxford: Basil Blackwell, 2000: 213-237.

[3] Tang Wen, Chen Zhong. Research on subjective trust management model based on fuzzy set theory [J]. Journal of Software, 2003, 14 (8): 1401-1408.

[4] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management [C]//Proceedings of the 17th Symposium on Security and Privacy. Oakland: IEEE Computer Society Press, 1996:164-173.

[5] Beth T, Borcherding M, Klein B. Valuation of trust in open network [C]//Proceedings of the European Symposium on Research in Security. Brighton: Springer-Verlag, 1994:3-18.

[6] Abdul-Rahman A, Hailes S. A distributed trust model[C]//Proceedings of Meeting on New Security Paradigms. Langdale UK: ACM,1998: 48-60.

[7] Jøsang A, Ismail R, Boyd C. A survey of trust and reputation systems for online service provision[J]. Decision Support Systems,2007,43(2):618-644.

[8] Whitby A, Jøsang A, Indulska J. Filtering out unfair ratings in Bayesian reputation systems[J]. The Icfain Journal of Management Research, 2005,4(2): 48-64.

[9] Song S S, Hwang K, Zhou R F, et al. Trusted P2P transactions with fuzzy reputation aggregation[J]. IEEE Internet Computing,2005,9(6):24-34.

[10] Luo Junhai, Liu Xue, Fan Mingyu. A trust model based on fuzzy recommendation for mobile ad-hoc networks[J]. Computer Networks, 2009,53(14): 2396-2407.

[11] Atanassov K. Intuitionistic fuzzy sets[J]. Fuzzy Sets and Systmes,1986,20(1):87-96.

[12] Deschrijver D, Kerre E E. On the composition of intuitionistic fuzzy relations[J]. Fuzzy Sets and Systems, 2003, 136(3):333-361.

[13] Marina M K, Das S R. On demand multi path distance vector routing in ad hoc networks[C]// Proceedings of 9th International Conference in Network Protocols. Los Alamitos: IEEE Computer Society Press,2001:14-23.

[14] Pirzada A A, Mcdonald C. Establishing trust in pure ad hoc networks[C]//Proceedings of the 27th Conference on Australasian Computer Science. Darlinghurst: Australian Computer Society, 2004: 47-54.

[15] Balakrishnan V, Varadharajan V, Tupakula U. Subjective logic based trust model for mobile ad hoc networks[C]//Proceedings of the 4th International Conference on Security and Privacy in Communication Networks. New York: ACM,2008: 1-11.