基于信任度计算的三阈值控制 Ad Hoc 网络节点撤销机制

郭 萍[1,2],周 未[3],成亚萍[1,2]
(1.南京信息工程大学江苏省网络监控中心,江苏南京 210044; 2.南京信息工程大学计算机与软件学院,江苏南京 210044;
3.南京理工大学计算机科学与工程学院,江苏南京 210094)

摘 要: 为解决在资源受限且拓扑结构多变的 Ad Hoc 网络中对节点状态的量化控制,提出一种准确计算节点信任度值、三阈值控制的节点撤销机制.基于投诉机制的阈值用于快速将可疑节点挂起;基于信任度计算的阈值用于最终将恶意节点撤销;基于预警的阈值用于防止恶意节点短期内发起对某合法节点的连续错误投诉.分析及仿真表明:所提方案避免根据投诉数目而撤销节点的武断性,三阈值的采用保证了对潜在恶意节点的快速反应、信任度可量化及准确撤销,且能防止恶意节点对合法节点合谋投诉而造成的误撤销.

关键词: Ad Hoc 网络; 信任度计算; 三阈值控制; 节点撤销
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2015)08-1589-09
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.08.018

Trust Calculation-Based Triple Thresholds Controlling Node Revocation in Ad Hoc Networks

GUO Ping[1,2], ZHOU Wei[3], CHENG Ya-ping[1,2]
(1. *Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing, Jiangsu* 210044, *China*;
2. *School of Computer & Software, Nanjing University of Information Science & Technology, Nanjing, Jiangsu* 210044, *China*;
3. *College of Computer Science & Engineering, Nanjing University of Science & Technology, Nanjing, Jiangsu* 210094, *China*)

Abstract: In order to solve the problem of how to evaluate the trusted degree of the nodes in the resource-constrained and topology-changed Ad Hoc networks, a scheme for evaluation of Ad Hoc nodes based on trust degree calculation and triple thresholds control has been put forward, improving the previous literature on the node trust evaluation mechanism. The accusation-based threshold is adopted to hang on a suspect node rapidly. The trust degree calculation-based threshold is used to revoke a node only when its trust value has reached the threshold value preseted according to safety requirements. The warning-based threshold is set to limit a potentially suspect node to launch a series of continuous malicious accusations to a legitimate node. Analysis and simulations show that the proposed scheme overcomes node revocation arbitrarily in the previous schemes in which node revocation is based on the number of accusations. Triple thresholds ensure a rapid response to malicious nodes, quantification of node trust and more accurate revocation of malicious nodes; moreover, it prevents illegal nodes from accusing legitimate nodes in collusion and then avoids a wrong revocation.

Key words: Ad Hoc networks; trust degree calculation; triple thresholds control; node revocation

1 引言

目前,越来越多的公钥密码技术被应用来保障 Ad Hoc 网络安全,通常对 Ad Hoc 网络节点授予证书的形式来证明其合法性,这就涉及到当证书过期或节点被攻陷,如何撤销证书的问题,对证书的撤销归根到底是对节点的撤销.本文主要侧重对 Ad Hoc 节点的分布式撤销机制研究[1~7].文献[1]采用门限机制来消除 CA(Certificate Authority)集中的特性,由一组节点承担分发密钥及撤销节点的任务,然而这种机制控制复杂,各个认证服务器间需要更多的协同工作,在无线环境中,很难取得理想效果.文献[2]采用基于公钥密码算法无中心非

收稿日期:2013-02-28;修回日期:2014-09-25;责任编辑:梅志强
基金项目:国家自然科学基金(No.61272421);中国气象局(No.[2014]MC16);江苏高校优势学科建设工程资助

门限机制的节点撤销方案,节点的撤销依赖于节点间的相互投诉,如果对某个节点的投诉数目超过系统预先设定的阈值,则这个节点变得不可信,相当于从网络中撤销,显然这种仅依靠投诉数目撤销节点健壮性弱,易导致恶意节点的合谋攻击.文献[3]没有采用可信第三方,而是使用类似于文献[4]中的授权的票据.新加入节点的票据由其邻居节点颁发,恶意节点也是由邻居节点对其投诉,达到门限值时撤销其票据,没有票据的节点就没有权限与其它节点通信,意味着该节点从 Ad Hoc 网络中删除.虽然文献[4]对于错误投诉有很好的健壮性,但多个恶意节点合谋仍可发起对系统的攻击.文献[5]对于证书的撤销如同文献[2]一样依赖于对节点的投诉阈值,所有投诉信息迅速在全网广播,每条投诉都关联着一个取值范围在[0,1]之间的权值,但其在全网范围内根据投诉计算节点的信任度,显然通信量及计算量不可接受,而且很难做到同步.文献[6]提出基于簇的分布式投诉方案,系统中所有节点都可以参与投诉,且每条投诉对应于一个可变权值.权值的计算来源于节点历史行为的可靠性,可靠性越高,权值也就越高.当节点对其投诉而导致该节点的权值下降到门限值,其证书将被撤销.相比文献[5]极大提高了节点撤销的准确性,但由于簇内节点都参与计算,仍存在证书撤销延迟的问题.文献[7]提出一种激进的牺牲式分布撤销方案,投诉者广播签名的投诉消息,接收者收到消息后,会把投诉者及被投诉者的密钥都撤销.这虽然阻止了恶意节点伪造投诉消息,被投诉节点也可以很快被撤销,但是投诉者同时也被撤销,换言之,是牺牲一个节点来撤销潜在的攻击者.

2 Ad Hoc 网络节点状态

本文引入三重阈值控制节点状态.投诉阈值 δ_A决定是否将节点挂起,即投诉数目大于等于 δ_A,将节点状态挂起但不撤销;撤销阈值 δ_T决定是否将节点最终撤销,簇头节点根据收到的投诉计算节点信任度是否小于系统事先设定的 δ_T,如果小于立即广播对该节点的撤销;预警阈值 δ_W用于防止恶意节点的合谋攻击,如果一个节点短时间内连续因同一事由对某节点的投诉次数达到 δ_W时,则该投诉者状态置为预警状态.

Ad Hoc 网络初始化结束后节点分为以下两类:

①簇头节点(CH):簇头节点组成的 Ad Hoc 网络独立运行后在线可信第三方.簇头收集节点间相互投诉消息,根据投诉计算本簇内非簇头节点信任度,当某节点的信任度小于系统事先设定的 δ_T时,及时广播对该节点的撤销消息;非簇头节点也可以投诉簇头的非法行为.

②非簇头节点(Non-CH):非簇头节点收集到对某节点的投诉信息大于系统事先设定的投诉阈值 δ_A时,但还没有被簇头宣布撤销前,置该节点状态为挂起.即非簇头节点不计算信任度,但要统计投诉数目;当收到簇头的撤销消息,节点自适应的完成对其它节点的撤销.

根据以上描述,Ad Hoc 网络对节点管理模型如图 1 所示.

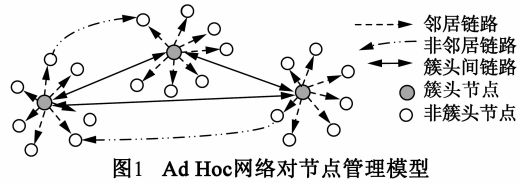


图1 Ad Hoc网络对节点管理模型

簇头及非簇头节点在初始化结束后都是可信的(假设可信第三方进行初始化时已对它们进行认证),运行一段时间后,可能分化出处于以下四种状态的节点:

①可信状态:这类节点的信任度大于等于 δ_T,位于节点可信列表(Node Trusted Lists,NTL).

②预警状态:这类节点由于在很短的时间内连续投诉一个节点,当投诉次数达到预警阈值 δ_W时,被列入节点预警列表(Node Warned Lists,NWL),防止混入 Ad Hoc 的恶意节点或被捕获节点发出虚假投诉,导致可信节点很快被挂起甚至被误撤销.进入 NWL 的节点仍可以投诉其它节点,其状态可能向挂起状态转化(被投诉数目$\geqslant\delta_A$),也可能转为可信状态(当被其连续投诉的节点撤销,证明其投诉是正确的),也可能被撤销(其信任度值$\leqslant\delta_T$).

③挂起状态:这类节点由于被其邻居节点投诉数目大于等于 δ_A,被列入节点挂起列表(Node Suspended Lists,NSL),暂时不能进行任何操作,直到簇头节点计算完其信任度,如果大于等于 δ_T,转为可信状态;小于 δ_T,则被撤销.

④撤销状态:这类节点由于信任度小于 δ_T,由簇头节点广播撤销报文,所有节点将其列入节点撤销列表(Node Revoked Lists,NRL),被隔离出 Ad Hoc 网络.

综上所述,节点状态转换过程如图 2 所示.

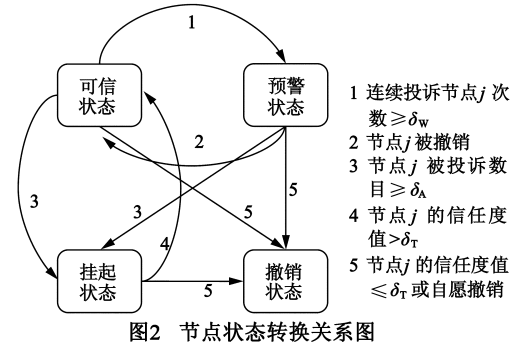


图2 节点状态转换关系图

3　Ad Hoc 网络节点撤销模型

3.1　系统假设

①每个节点都有唯一的 ID(Identity)号并且具有发现一跳邻居节点的机制.

②每个节点至少有 k 个一跳的邻居节点,不失一般性,节点 v_i的邻居节点集合表示为:$N_i=\{v_1,v_2,\cdots,v_k\}(k\leqslant n)$,$n$ 是整个 Ad Hoc 网络节点数.

③所有簇头节点组成集合 H,不失一般性,簇头集 $H_{\text{cluster}}=\{H_1,H_2,\cdots,H_m\}(m<n)$($n$ 是整个 Ad Hoc 网络节点数),同理,可信节点集合 $S_{\text{T}}=\{v_i\mid$当且仅当 v_i 在 NTL 中$\}(i\leqslant n)$,被预警节点集合 $S_{\text{W}}=\{v_j\mid$当且仅当 v_j 在 NWL 中$\}(j<n)$,被挂起节点集合 $S_{\text{S}}=\{v_k\mid$当且仅当 v_k 在 NSL 中$\}(k<n)$,被撤销节点集合 $S_{\text{R}}=\{v_l\mid$当且仅当 v_l 在 NRL 中$\}(l<n)$.

④每个节点都具有本地检测机制发现一跳邻居节点的不合法行为.

⑤(节点在初始化后拥有一对公/私钥,私钥由节点保存,公钥可公开,并持有本簇头节点公钥.

⑥本方案采用文献[8,9]轻量化机制,由簇头节点将簇内节点的公钥与其身份标识签名生成辅公钥,辅公钥是节点间进行相互认证的重要依据,即只要簇头是可信的,其签发的辅公钥也是可信的,因而本方案中无证书管理.

3.2　节点撤销算法

Ad Hoc 网络节点撤销系统是一个六元组 $\Pi=(W_i,A_i,T_i,C_{\text{CH}},R_i,\text{AC}_{\text{CHs}})$定义如下:

①监视算法 W_i:W_i 由节点 $v_i(i=1,2,\cdots,n)$执行,监视节点 v_i 一跳邻居节点行为.

②投诉算法 A_i:A_i 由节点 $v_i(i=1,2,\cdots,n)$执行,一旦邻居节点 $v_j(j\in N_i,j\neq i)$有不合法行为,则生成投诉报文以广播方式在邻居节点集合 $N_i=\{v_1,v_2,\cdots,v_k\}(k\leqslant n)$中广播,并以节点间逐跳转发方式向整个 Ad Hoc 网络扩散.

③节点状态转换算法 T_i:T_i 由 $v_i(i=1,2,\cdots,n)$节点执行,各节点根据收到的投诉报文,计算对节点的投诉数目,如果大于系统事先设定的投诉阈值 δ_{A},则将该节点置为挂起状态;如果统计某投诉者连续向一节点投诉数目大于预警阈值 δ_{W},则将该节点置为预警状态;如果时刻 T 收到由簇头节点发布的信任度报文,某被挂起或预警节点的信任度仍大于 δ_{T},则将其恢复至可信状态.

④信任度计算算法 C_{CH}:C_{CH}由簇头节点 $H_i(H_i\in H_{\text{cluster}})$执行,根据收到对节点的投诉报文,计算每个节点的信任度,更新节点信任度维护表,并定期广播节点信任度,如果某节点信任度小于系统事先设定的撤销阈值 δ_{T},立即以广播方式发出撤销报文.

⑤撤销算法 R_i:R_i 由节点 $v_i(i=1,2,\cdots,n)$执行,当收到撤销报文时,各节点立刻更新节点状态表,置撤销节点状态为不可信.

⑥激活算法 AC_{CH}:AC_{CH}由若干簇头执行,当某一簇的簇头节点被撤销时,选择该簇中节点信任度最高的节点进行激活,使其成为新的簇头,继续为簇内节点提供服务.

4　节点信任度评估

4.1　节点信任度定义

4.1.1　节点信任度定义

对节点信任度的评估就是对节点可信状态的评估,通过"信任度"概念来描述 Ad Hoc 网络节点由可信变为不可信这一过程,下面给出其定义.

定义 1　设 $0\leqslant\alpha_i(T)\leqslant1$,其中 T 为时间,称 $\alpha_i(T)$为"节点 v_i 在 T 时刻的信任度",它描述了节点 v_i 在时刻 T 的信任度值.

$\alpha_i(T)=1$ 信任度最高,节点 v_i 处于"完全可信"状态;$\alpha_i(T)=0$ 表示节点 v_i 处于"完全不可信"状态. $T=0$ 是 Ad Hoc 网络的初始时刻,根据上面的分析,有 $\alpha_i(0)=1$,表示这时候所有节点都是可信的,随着 Ad Hoc 网络的运行,节点信任度开始下降,所以 $\alpha_i(T')\leqslant\alpha_i(T)$,其中 $T'>T$.

根据定义 1,Ad Hoc 网络中一个节点在整个生存周期内的信任度可以用一个向量来表示:$\alpha(\text{ID}_i)=\{\alpha(T_{\text{start}}),\alpha(T),\alpha(T'),\cdots\cdots,\alpha(T_{\text{end}})\}$,$\alpha(T_{\text{start}})=1$,表示 Ad Hoc 网络初始时刻,$\alpha(T_{\text{end}})$表示 Ad Hoc 网络结束时刻,$T'>T$,$ID_i$是节点 v_i 的唯一标识.

4.1.2　节点信任状态定义

由节点信任度向量,可根据 Ad Hoc 网络执行任务的安全要求设定系统的撤销阈值 δ_{T}(δ_{T}是系统预先定义的撤销阈值),如果该节点某时刻的信任度小于 $\delta_{\text{T}}(0\leqslant\delta_{\text{T}}\leqslant1)$,则该节点不可信.由此给出"节点信任状态"定义.

定义 2　设 $\alpha_i(T)(0\leqslant\alpha_i(T)\leqslant1)$表示节点 v_i 在时刻 T 信任度值,当 $\alpha_i(T)=1$ 称节点 v_i 时刻 T 完全可信;$\alpha_i(T)=0$ 称节点 v_i 时刻 T 完全不可信;$\delta_{\text{T}}\leqslant\alpha_i(T)<1$,称节点 v_i 时刻 T 时可信;$0<\alpha_i(T)<\delta_{\text{T}}$ 称节点 v_i 时刻 T 时不可信.

4.1.3　投诉的定义

投诉事件权值即是不同的事件,对节点信任度计算的影响不同.将影响节点信任度的行为事件按照 Ad Hoc 网络安全需求及检测规则分为不同的等级,每个等

级对应一个权值 $\theta\in[0,1]$.对投诉给出如下定义:

定义 3 设 $S_{ij}(T)$代表节点 v_i 对节点 v_j 在 T 时刻的投诉评估函数:$S_{ij}(T)=\theta I$.式中:若本次投诉成功,则 $I=1$,反之则 $I=0$;参数 $\theta\in[0,1]$,代表节点 v_i 对节点 v_j 行为的不满意度.$\{v_i\rightarrow v_j, S_{\text{event}}, \theta, T\}$表示节点 v_i 对节点 v_j 的一次投诉,S_{event}表示投诉事件,θ 表示由投诉事件等级决定的节点 v_i 对节点 v_j 的不满意度,T 表示投诉时间.

4.2 节点信任度计算

根据以上分析,计算节点信任度的公式,如式(1)所示.

$$\begin{cases}\alpha_i(T)=1-\beta\left(\sum\limits_{j\in S_{\text{T}}}S_{ji}(T)\delta_{S_{\text{T}}}+\sum\limits_{j\in S_{\text{W}}}S_{ji}(T)\delta_{S_{\text{W}}}\right)\\ T=\text{首次计算节点信任度值时刻}\\ \alpha_i(T')=\alpha_i(T)-\beta\left(\sum\limits_{j\in S_{\text{T}}}S_{ji}(T')\delta_{S_{\text{T}}}+\sum\limits_{j\in S_{\text{W}}}S_{ji}(T')\delta_{S_{\text{W}}}\right)\\ T'>T\text{ 且 }\alpha_j(T)>\delta_{\text{T}}\end{cases}\tag{1}$$

$S_{ji}(T)$代表节点 v_j 对节点 v_i 在 T 时刻的投诉评估函数,详见定义 3.$\alpha_i(T')$是节点 v_i 在 T' 时刻的信任度,即 T' 是 T 的后一时刻,$\alpha_i(T)$反映节点 v_i 历史信任度,$\beta=1/n$代表 Ad Hoc 网络规模参数.S_{T}代表投诉节点来自可信节点集合,该集合平均信任度为 $\delta_{S_{\text{T}}}$,S_{W}代表投诉节点来自被预警节点集合,该集合平均信任度为 $\delta_{S_{\text{W}}}$,不失一般性 $\delta_{S_{\text{T}}}\geqslant\delta_{S_{\text{W}}}\geqslant\delta_{\text{T}}$.$\alpha_j(T)>\delta_{\text{T}}$ 是指投诉节点 v_j 在 T 时刻的信任度须大于系统预先设定的撤销阈值 δ_{T},其投诉才能成功.

投诉模型如图 3 所示,节点 3,4,5,7,9,均向节点 6 发出投诉,节点 6 同时也投诉了节点 3 和 9,意味着这时节点 6 的被投诉数目是 5,投诉数目是 2.

根据式(1),以图 3 为例,初始化结束后首次在 T 时刻计算各节点信任度,参数假设如表 1 所示,计算结果如表 2 所示.

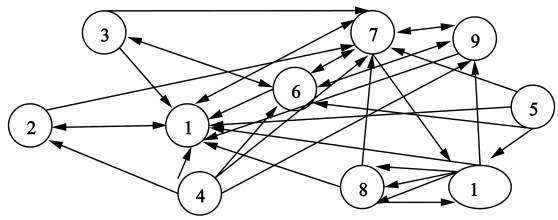


图3 节点间投诉模型

表 1 参数值设置

安全事件等级	θ 值	各门限参数	值
Ⅰ	0.01	$\delta_{S_{\text{T}}}$	1
Ⅷ	0.6	$\delta_{S_{\text{W}}}$	0.91
Ⅸ	0.7	δ_{W}	3
Ⅹ	0.8	δ_{A}	5
Ⅻ	0.99	δ_{T}	0.9

Ⅰ至Ⅻ为安全事件等级,等级越高意味着越不安全,对应的 θ 值越高(表中所列值只是举例说明,如Ⅻ代表泄露私钥极不安全行为,对应权值 θ 为 0.99,安全事件的分级不在本文研究范围).$\delta_{S_{\text{T}}}$是可信节点集合平均信任度值,初始化结束后所有节点都是可信的,因此平均值为 1.$\delta_{S_{\text{W}}}$是被预警节点集合平均信任度值,初始化时集合节点数为 0,进入到这个集合的节点很可能是潜在故意发送错误投诉的恶意节点或被捕获节点,因此 $\delta_{S_{\text{W}}}$可以设置为接近撤销阈值 δ_{T},目的是尽可能降低由于错误投诉导致合法节点被挂起或撤销.预警阈值 $\delta_{\text{W}}=3$,投诉阈值 $\delta_{\text{A}}=5$,撤销阈值 $\delta_{\text{T}}=0.9$.

由表 2 可见,由于各节点间的相互投诉,经过第一次信任度计算后,各节点的信任度值都发生了变化.$S_{\text{T}}=\{1,3,4,5,7,8\}$;$S_{\text{W}}=\{-\}$;$S_{\text{R}}=\{2,6,9,10\}$.节点 1 和节点 7 虽然被投诉的次数很多,迅速被挂起,但其信

表 2 节点信任度值

节点	投诉节点	S_{T} 个数	S_{W} 个数	投诉等级	θ 值	$\alpha_i(T)$	所属集合变迁
1	{2,3,4,5,6,7,8,9,10}	8	1	{8Ⅰ,Ⅻ}	{0.01,0.99}	0.9	$S_{\text{T}}\rightarrow S_{\text{S}}\rightarrow S_{\text{T}}$
2	{1,4}	2	0	{2Ⅸ}	0.7	0.87	$S_{\text{T}}\rightarrow S_{\text{R}}$
3	{6}	1	0	{Ⅰ}	0.01	0.99	$S_{\text{T}}\rightarrow S_{\text{T}}$
4	0	0	0	–	–	1	$S_{\text{T}}\rightarrow S_{\text{T}}$
5	0	0	0	–	–	1	$S_{\text{T}}\rightarrow S_{\text{T}}$
6	{3,4,5,7,9}	5	0	{3Ⅰ,2Ⅹ}	{0.01,0.8}	0.84	$S_{\text{T}}\rightarrow S_{\text{S}}\rightarrow S_{\text{R}}$
7	{1,2,3,4,5,6,8,9}	7	1	{7Ⅰ,Ⅹ}	{0.01,0.8}	0.92	$S_{\text{T}}\rightarrow S_{\text{S}}\rightarrow S_{\text{T}}$
8	{10}	0	1	{Ⅻ}	0.99	0.91	$S_{\text{T}}\rightarrow S_{\text{T}}$
9	{4,6,7,10}	3	1	{Ⅷ,Ⅸ,Ⅹ,Ⅻ}	{0.6,0.7,0.8,0.99}	0.71	$S_{\text{T}}\rightarrow S_{\text{R}}$
10	{5,7,8}	2	1	{3Ⅷ}	0.6	0.82	$S_{\text{T}}\rightarrow S_{\text{W}}\rightarrow S_{\text{R}}$

任度值经过计算大于 δ_T,重返 S_T 集合.节点 4,5 没有被投诉,信任度值不变.节点 3 只有一次安全级别很低的投诉($\theta=0.01$),经过计算信任度值还是很高.节点 8 被节点 10 连续投诉三次,只按一次计算(因为节点 10 已被预警),即使可能是错误投诉,$\theta=0.99$,也不能导致节点 8 被撤销.节点 2,9 虽然没有被挂起,但经过计算信任度值均小于 δ_T,被撤销.节点 6 先被挂起,后被撤销.节点 10 由于之前连续投诉节点 8,导致对一个节点的投诉次数等于 δ_W,被写入 S_W 集合,进而信任度迅速降为 0.91(等于 δ_{S_W}).同时节点 5,7,8 因同一事件(不妨假设事件为恶意投诉)投诉节点 10,导致节点 10 信任度值小于 δ_T,被撤销.节点 10 被证明是恶意节点后,之前凡是被 10 投诉过的节点在 T 时刻的信任度值将被重新计算,受节点 10 影响的节点 1,8,9 经重新计算,信任度值分别是:0.99,1,0.79,节点 9 仍然被撤销.至此,所有节点在 T 时刻的信任度值将被簇头节点广播.节点更新自己的节点状态列表,$S_T=\{\alpha_1(T)=0.99,\alpha_3(T)=0.99,\alpha_4(T)=1,\alpha_5(T)=0.99,\alpha_7(T)=0.92,\alpha_8(T)=1\}$;$S_W=\{-\}$;$S_R=\{2,6,9,10\}$.

在 $T'(T'>T)$时刻再次计算节点信任度,需重新调整 $\delta_A,\delta_W,\delta_{S_T},\delta_{S_W}$的值(因为节点数 n 发生变化),δ_T 可仍为 0.9,根据新的投诉关系,在 $S_T=\{\alpha_1(T)=0.99,\alpha_3(T)=0.99,\alpha_4(T)=1,\alpha_5(T)=0.99,\alpha_7(T)=0.92,\alpha_8(T)=1\}$基础上计算时刻 T' 各节点新的信任度值.

5　性能分析

5.1　节点撤销机制特点

本文所提 Ad Hoc 节点撤销机制具有下列特点:

(1)节点信任度的计算.本方案将节点的撤销精确量化,不单纯的依赖投诉数目,按照信任度值的大小决定节点是否被撤销,改变了前人方案仅依赖投诉次数撤销的武断性.

(2)四种节点状态的引入.本方案将节点分为四种不同状态,即挂起状态、预警状态、可信状态及撤销状态,使得对节点运动轨迹的刻画准确实时动态,而且状态的增多并没有影响撤销节点的速度.

(3)三阈值的运用.第一使得被多数节点投诉的节点立刻得以挂起,不至于在没有收到撤销命令前危害网络,保证了对潜在不可信节点控制的迅速性;其次通过计算节点信任度值而决定是否撤销,保证撤销的精确性,而预警阈值的存在很好的预防潜在恶意节点或被捕获节点发起的故意错误投诉,避免恶意节点合谋发起攻击;最后,系统安全性可根据 Ad Hoc 网络实际需求来调节投诉阈值 δ_A、预警阈值 δ_W 及撤销阈值 δ_T 的取值而满足不同的应用.

5.2　仿真实验

5.2.1　不同投诉阈值 δ_A 对节点被挂起速度的影响

考查投诉阈值的设定对节点被挂起速度的影响.仿真工具 OPNET[10],仿真场景详细配置见表 3.随机发送数据包,反复实验五次.攻击类型为选择性转发攻击(SFA,Selective Forwarding Attack)[11].设定投诉阈值 δ_A 分别取值为 3,7,13,观察随着节点规模的变化,不同投诉阈值对节点状态的影响.

表 3　仿真参数设置

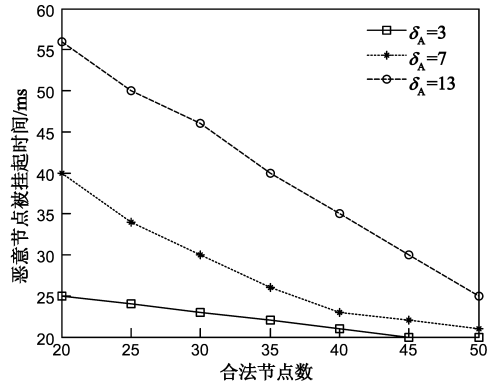
参数	参数值	参数	参数值
传输范围	250m	节点密度布置	$1km^2$
数据包大小	64bytes	仿真时间	600s
包交换时间间隔	30ms	合法节点规模	[10,50]
路由协议	AODV[12]	恶意节点规模	[1,25]

场景 1:恶意节点 10 个,合法节点规模逐渐从 20 增长至 50,考查随着 δ_A 的不同,10 个恶意节点被挂起速度的变化.结果如图 4(a)所示.

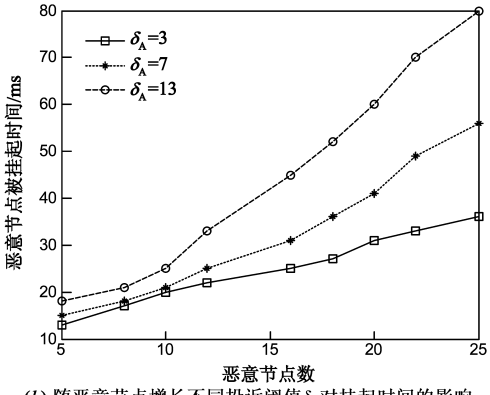
δ_A 越小,投诉达到门限值速度越快,使得拒绝转发的节点由于被其邻居节点投诉而很快达到投诉阈值,状态被挂起.随着节点规模的增大,$\delta_A=3,7,13$ 节点被挂起趋势接近,这是因为当一个节点被发现非法,周围有足够多的邻居节点发出投诉报文,导致很快达到投诉阈值 δ_A,且对 δ_A 的控制是全局分布,即当节点收到投诉报文自动更新 NSL(节点挂起列表),因此随着合法节点规模的增长,对恶意节点的投诉越多,恶意节点被挂起速度越快.

场景 2:合法节点规模为 50,恶意节点逐渐从 5 增加至 25,考查随着 δ_A 的不同挂起恶意节点的速度.结果如图 4(b)所示.

合法节点数量及 δ_A 一定,随恶意节点增多,需要将其挂起的时间随之增长;δ_A 越大,同样数量的恶意节点挂起时间也越长,因为需要等待更多合法节点对其投诉直到达到门限值 δ_A;恶意节点数量较小时,δ_A 取值的不同(此处指取值 3,7,13)对恶意节点被挂起影响不明显,因为这时候恶意节点与合法节点数量相比很少,使得投诉很容易达到门限值 δ_A.如恶意节点数为 5 时,$\delta_A=13$ 与 $\delta_A=3$,挂起所有恶意节点的时间比为 1.38,而这个比值在恶意节点数 2.5 时为 2.22,这是因为合法节点与恶意节点的比例大幅下降,没有足够的合法节点投诉恶意节点或者是需要更长的时间才能完成对大量恶意节点的投诉,导致这时候 δ_A 的取值对挂起速度有明显影响.



(*a*) 随合法节点增长不同投诉阈值δ_A对挂起时间的影响



(*b*) 随恶意节点增长不同投诉阈值δ_A对挂起时间的影响

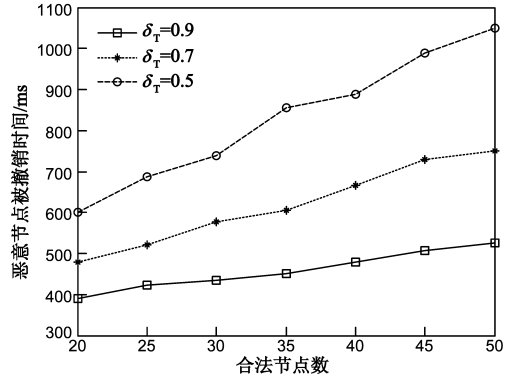
图4 不同投诉阈值对恶意节点被挂起时间的影响

5.2.2 不同撤销阈值 δ_T 对恶意节点被撤销速度的影响

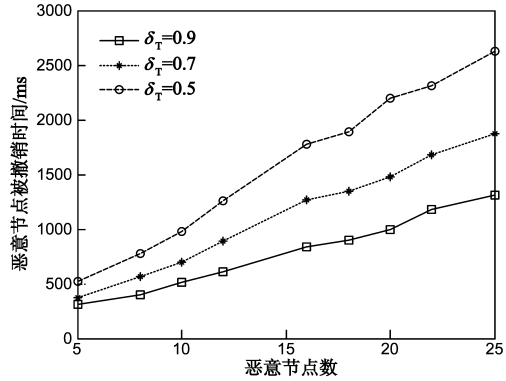
场景 1:恶意节点 10 个,合法节点规模逐渐从 20 增长至 50,考查随着 δ_T 的不同,10 个恶意节点被撤销速度的变化(仿真参数设置同表 3).

节点信任度的计算,并不是实时的,而是每隔一定时间由簇头节点计算并广播.对于实时变化的 Ad Hoc 网络,如果每个节点都运行信任度的计算,很难做到同步,导致不同节点计算的信任度可能不同,且增加非簇头节点的计算及通信代价.在仿真实验中设定每隔 300ms 由选定的簇头节点根据收到的投诉信息计算恶意节点的信任度(恶意节点不是随机的,选定 10 个节点拒绝转发数据包,开始默认其信任度为 1),设投诉事件安全权值 $\theta=0.5$(θ 值的选择有针对性,目的是在合法节点规模不大的情况下,能够使节点信任度值尽快达到门限值,但是对不同 δ_T 值,θ 不变,因此不影响仿真结果趋势走向).结果如图 5(a)所示.

合法节点数相同时,δ_T 越小,意味着需要投诉的节点越多,才可能导致一个恶意节点信任度值低于 δ_T 而被撤销.例如:节点规模为 20 时,$\delta_T=0.9$,只需有 4 个投诉即可导致恶意节点信任度值达到 δ_T;而 $\delta_T=0.5$,则需要至少 20 个投诉,才能使节点信任度值达到 δ_T.节点规模为 50 时,$\delta_T=0.9$ 与 $\delta_T=0.5$,所需投诉数分别为 10 与 50 才能撤销恶意节点.因此,δ_T 越大,所需投诉数越少,反之,则投诉数越多,相应的,时间代价也就越高.结合图 4(a),δ_A 使将恶意节点快速挂起,δ_T 则保证对恶意节点撤销的准确性.



(*a*) 随合法节点增长不同撤销阈值δ_T对撤销时间的影响



(*b*) 随恶意节点增长不同撤销阈值δ_T对撤销时间的影响

图5 不同撤销阈值对恶意节点被撤销时间的影响

场景 2:合法节点规模为 50,恶意节点逐渐从 5 增加至 25,考查随着 δ_T 的不同撤销恶意节点的速度.结果如图 5(b)所示.仿真细节描述同图 5(a),$\theta=0.5$.

分析同图 4(b),恶意节点数量较少时,δ_T(=0.9,0.7,05)对撤销时间影响不明显,随着恶意节点的增多,δ_T(=0.9,0.7,0.3)的不同对撤销时间的影响越明显.例:合法节点 50,恶意节点 25,$\delta_T=0.5$ 与 $\delta_T=0.9$ 撤销节点相差约 2.45 倍.

5.2.3 不同 δ_A 和 δ_T 取值对投诉报文数的影响

投诉报文总数直接影响撤销节点的通信代价,根据对图 4(a)至图 5(b)分析,不同 δ_A 和 δ_T 取值与投诉报文总量的关系如图 6 所示.

5.2.4 不同 θ 取值对节点信任度计算的影响

θ 代表投诉事先等级的权值,本例中令节点规模为 50,根据投诉数目及公式(1)计算节点信任度,以观察 θ 取值对信任度的影响.50 个节点初始化完成后,跟踪节点 v_i,分别在投诉数依次为[5,25]之间时刻计算节点 v_i 信任度,结果如图 7 所示.

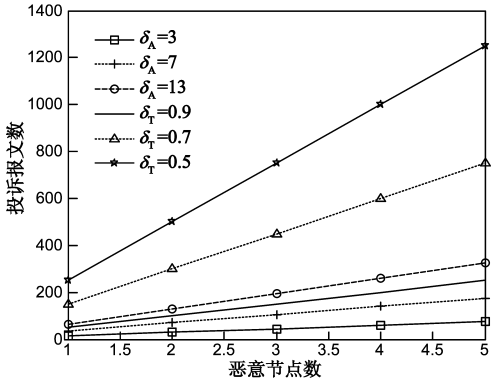


图6　δ_A和δ_T不同取值与投诉报文数关系

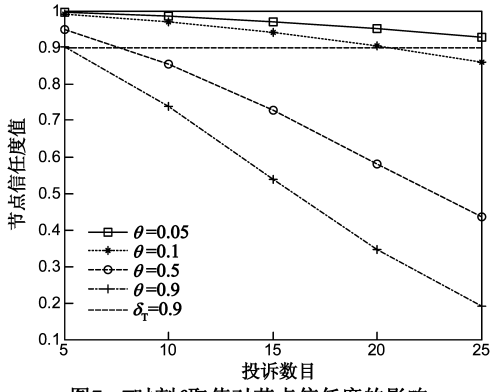


图7　T时刻θ取值对节点信任度的影响

θ 取值越大,在同等节点规模下,节点信任度值下降越快.这意味着对于极不安全事件(θ 很大),经式(1)计算,节点信任度会很快低于 δ_T 而被撤销,这时候投诉数目可能远未达到 δ_A,即节点并未被挂起.另一种情况是对于一些安全级别不是很高的行为(θ 较小),经式(1)计算,可能即使投诉数目很多,但节点信任度可能仍高于 δ_T,这种情况可以很好预防针对关键节点的诸如 DoS (Denial of Services)、泛洪、虫洞、黑洞等攻击[13].因此,δ_A 和 δ_T 的互补控制,精确设置,可极大程度保障对恶意节点的撤销既迅速又准确.

5.3　与其它撤销方案比较

与文献[2,5,6]就证书/节点撤销性能比较如表 4 所示.撤销方式上,本方案是分簇的分布式方案,有利于采用三阈值控制及信任度的计算.轻量化 CA 优于文献[2,5,6]的传统证书 CA,因此计算复杂性略优(仅从考虑证书管理的角度,三阈值意味着需额外统计两个阈值增量,但 δ_A 和 δ_W 只涉及简单加法,可忽略不计).文献[2,5]是全局策略,所有节点均参与投诉,通信量及存储量会大于采用分簇策略的文献[6]和本方案,本方案需额外统计两个阈值,通信量及存储量会比文献[6]略高.撤销的准确性而言,文献[2]仅凭投诉个数,不考虑投诉性质及投诉者是否可信,准确性及投诉可信性最差;文献[5,6]分别考虑投诉事由及投诉节点可信性,准确性及投诉可信性居中;而本方案全面考虑影响撤销节点的可能因素,准确性及投诉可信性最好,因此抗合谋攻击、DoS 攻击等健壮性亦最好.

表 4　各方案撤销性能比较

比较项	文献[2]	文献[5]	文献[6]	本方案
撤销方式	投诉数量阈值	投诉加权	分簇 + 投诉加权	分簇 + 三阈值控制 + 信任度计算
CA 构建方式	证书	证书	证书	轻量 CA
证书管理	相当	相当	相当	无证书管理
通信量	较高	较高	较低	居中
存储量	较高	较高	较低	居中
投诉可信性	最差	考虑投诉事由的权值	考虑投诉节点的可信性	既考虑投诉事由的权值,又评估投诉节点的可信性
准确性	最差	居中	居中	最好
快速性	撤销最快	撤销较慢	撤销居中	挂起最快,撤销居中
抗合谋攻击	最差	居中	居中	最好

5.4　安全性分析

5.4.1　对恶意节点的合谋攻击及各种不同类型 DoS 攻击的讨论

节点可能遭遇若干恶意节点的合谋攻击,比如故意投诉,使投诉阈值很快达到门限值 δ_A,导致其状态被挂起而失效.本文所提三阈值控制节点状态对恶意节点的合谋攻击很奏效,为说明这一点,设计如图 8 所示攻击模型.

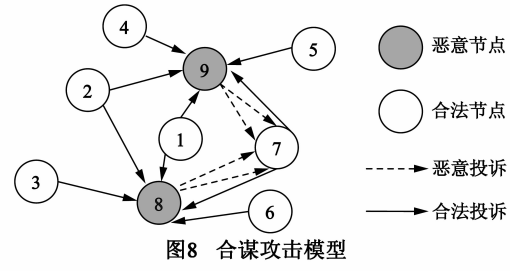


图8　合谋攻击模型

1~7 是合法节点,8,9 是恶意节点,保证每个恶意节点至少有 5 个合法节点为其直接邻居,2 个恶意节点对节点 7 发起恶意投诉攻击.不妨设定 $\delta_A = 5$, $\delta_T = 0.9$, $\delta_W = 3$, $\theta = 0.1/0.5$ 时,根据如图 8 所示投诉关系,计算节点 7,8,9 的信任度值,如表 5 所示.

恶意节点 8,9 分别对节点 7 最大投诉数为 3,受到 $\delta_W = 3$ 的限制,投诉者被列入预警列表,信任度快速下降接近 $\delta_T = 0.9$. $\theta = 0.5$(即取 θ 较大),按式(1)计算,节点 7 的信任度值为 $0.8 < \delta_T = 0.9$,暂时被撤销;节点

8,9 信任度值为 $0.75 < \delta_T = 0.9$,同时被撤销.观察节点 8,9 的投诉者是 5 个不同的节点,且投诉理由相同(如恶意投诉),判断节点 8,9 是恶意节点,之前对节点 7 的投诉全部来自这两个节点,所以将节点 7 从撤销列表中恢复到可信列表.$\theta = 0.1$(即取 θ 较小),节点 7 的信任度值为 $0.96 > \delta_T = 0.9$,节点 8,9 信任度值为 $0.95 > \delta_T = 0.9$,即节点 7,8,9 信任度值都没有达到 δ_T,但是节点 8,9 被投诉数为 5($\delta_A = 5$),被挂起.

表 5 攻击模型节点信任度值

节点 v_i	投诉节点	被投诉数	是否被挂起 ($\delta_A = 5$)	$a_i(T)$ ($\theta = 0.5$)	$a_i(T)$ ($\theta = 0.1$)
7	{8,9}	4	否	0.8	0.96
8	{1,2,3,6,7}	5	是	0.75	0.95
9	{1,2,4,5,7}	5	是	0.75	0.95

因此三阈值 δ_A、δ_T、δ_W 的联合控制,合理设置可高效的检测出恶意节点.δ_W 保证一个节点对另一个节点在短时间内的连续投诉不能很多,通常恶意节点有这样的行为,如针对某一关键节点发起连续攻击;δ_A 保证在 θ 取值较小,可疑节点信任度不能很快降低至 δ_T,根据投诉数量的设置迅速将可疑节点挂起,如泛洪攻击、频繁请求、黑洞攻击等各种不同类型的 DoS 攻击;δ_T 保证发生极不安全的恶意行为时,θ 取值相应较高,即使投诉数很少也能迅速将恶意节点撤销,如泄露私钥、公布系统安全参数等行为.

5.4.2 簇头节点的信任问题

簇头同时受非簇头节点及其它簇头节点的监视投诉,可能被挂起或撤销.簇头信任度的评估由其它簇头节点根据收到的投诉信息计算,如果信任度小于 δ_T,由距离最近的合法簇头节点广播撤销消息.这时由距离最近的合法簇头从被撤销簇头所在簇中选择信任度最高的节点,运行激活算法使其成为新的簇头继续提供服务.不可信簇头可能在撤销前已被挂起,或者直接从可信状态被撤销,如果是前者,那么挂起后将不能执行任何操作,如果是后者,意味着非法操作的安全级别很高,导致信任度迅速下降,无论是哪种情况,都意味着其非法行为可以很快被发现,并被隔离,因此造成的危害有限.

6 结论

本文研究 Ad Hoc 节点撤销机制,重新定义 Ad Hoc 节点状态,详细阐述影响节点信任度的因素,在此基础上计算节点信任度,提出一种三阈值控制的节点撤销机制.分析及仿真表明:三阈值控制的 Ad Hoc 节点撤销机制不仅迅速将可疑节点挂起,而且合理反映节点控诉力度,保障节点撤销的准确性;预警阈值 δ_W 有效防止非法节点的恶意投诉或合谋攻击,克服了以往方案中凭投诉数目武断撤销的不足,弥补了单纯计算节点信任度导致恶意节点撤销延迟的缺陷.

参考文献

[1] Deng H M, Mukherjee A, Agrawal D P. Threshold and identity-based key management and authentication for wireless Ad Hoc networks[A]. Proceedings of the International Conference on Information Technology: Coding Computing[C]. New York, USA: IEEE, 2004. 107 – 111.

[2] Liu W, Nishiyama H, Ansari N, et al. A study on certificate revocation in mobile Ad Hoc networks[A]. Proceedings of IEEE International Conference on Communications[C]. New York, USA: IEEE, 2011. 1 – 5.

[3] Luo H, Kong J, Zerfos P, et al. URSA: ubiquitous and robust access control for mobile Ad Hoc networks[J]. IEEE Transactions on Networking, 2004, 12(6): 1049 – 1063.

[4] 谭良,陈菊,周明天.可信终端动态运行环境的可信证据收集机制[J].电子学报,2013,41(1):77 – 86.
Tan L, Chen J, Zhou M T. Trustworthiness evidence collection mechanism of running dynamic environment of trusted terminal [J]. Acta Electronica Sinica, 2013, 41(1): 77 – 86. (in Chinese)

[5] Ganan C, Mata D J, Munoz J L. A modeling of certificate revocation and its application to synthesis of revocation traces[J]. IEEE Transactions on Information Forensics and Security, 2012, 7(6): 1673 – 1686.

[6] Wei L, Hiroki N, Ansari N, et al. Cluster-based certificate revocation with vindication capability for mobile Ad Hoc networks [J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(2): 239 – 249.

[7] Pushpalakshmi R, Kumar A V. A secure dominating set based routing and key management scheme in mobile Ad Hoc networks[J]. Wseas Transactions on Communications, 2011, 10 (10): 297 – 308.

[8] Dong X L, Wang L H, Cao Z F. New public key cryptosystems with lite certification authority[DB/OL]. http://ePrint.iacr.org/2006/154, 2013-03-16.

[9] 张学军,王玉,王锁萍,等.基于循环移位的轻量型相互认证协议研究[J].电子学报,2012,40(11):2270 – 2276.
Zhang X J, Wang Y, Wang S P, et al. Research on the cyclic shift lightweight mutual authentication protocol[J]. Acta Electronica Sinica, 2012, 40(11): 2270 – 2276. (in Chinese)

[10] 孙屹,孟晨. OPNET 通信仿真开发手册[M].北京:国防科技出版社,2005. 216 – 256.

[11] 潘勇,谢磊,徐勇军.一种传感器网络中选择性转发攻击的防御方法[P].中国专利:200810062842, 2008-12-16.

[12] RFC3651, Ad Hoc on-demand distance vector (AODV) rout-

ing[S].
[13] Martinovic I, Zdarsky F A, Wilhele M, et al. Wireless client puzzles in IEEE802.11 networks: security by wireless[A]. Proceedings of the 1st ACM Conference on Wireless Network Security[C]. Pittsburgh, USA: ACM, 2008.36 - 45.

作者简介

郭　萍　女,1973 年生,山东烟台人.分别于 1997 年、2005 年获兰州大学学士及硕士学位,2012 年获南京理工大学博士学位.现为南京信息工程大学计算机与软件学院讲师,研究方向为信息安全、无线网络认证及密钥管理、信任系统.
E-mail: guoping@nuist.edu.cn

周　未　男,1979 年生,江苏南京人.分别于 2002 年、2005 年获解放军理工大学学士及硕士学位.现为南京理工大学计算机科学与工程学院博士生,研究方向为信息安全、赛博空间安全.
E-mail: zhou_ziheng@126.com

成亚萍　女,1968 年生,山西太原人.于 1991 年获南京理工大学学士学位,2006 年南京信息工程大学硕士学位.现为南京信息工程大学计算机与软件学院副教授,研究方向为信息安全、信息隐藏及数据挖掘.