基于 AODV 协议的自组网络安全机制的研究

李 喆,刘 军
(东北大学信息科学与工程学院,辽宁沈阳 110004)

摘 要: 路由协议的安全性是移动自组网络安全中最重要的一环,AODV 路由协议因简单和控制开销小而广泛用于自组网络,但其没有任何安全机制保障,为此,本文探讨了 AODV 路由协议存在的主要安全隐患,对协议进行必要的改进,增加攻击检测功能,并为网络中节点建立信誉机制,二者相互作用共同完成协议安全性保障. 利用 NS 进行仿真,结果表明改进后的算法能够检测到网络中节点的恶意行为并迅速做出反应,实现对网络内部及外部攻击的防范.

关键词: 移动自组网络; 路由安全性; 攻击检测; 信誉度; AODV
中图分类号: TP393 **文献标识码**: A **文章编号**: 0372-2112 (2006) 02-0272-05

The Research on Security Mechanism Based on AODV Routing Protocol in Mobile Ad Hoc Network

LI Zhe, LIU Jun
(School of Information Science & Technology, Northeastern University, Shenyang, Liaoning 110004, China)

Abstract: Security of routing protocols is the most important secure factor in the mobile Ad Hoc networks. AODV protocol is used widely in the Ad Hoc networks for its simplicity and small control overhead, but it does not have any security mechanism. With some potential insecure factors in AODV protocol analyzed, some necessary improvements are made to AODV protocol, including adding attack detection and building up credence mechanism, which would collaboratively guarantee the network security. Simulation results indicate that it can react quickly when some malicious behaviors in the network are detected and effectively protect the network from kinds of attacks.

Key words: mobile Ad Hoc network; routing security; attack detection; credence; Ad Hoc on demand distance vector (AODV)

1 引言

Ad Hoc网络[1]是由多个移动节点通过无线链路相连接、具有时变拓扑结构的多跳、临时性自治系统,广泛应用于军事战场信息系统建设、民用紧急救助和执法等场合,并逐渐运用于商业和民用环境,其安全问题受到广泛的关注. 其动态拓扑、资源受限、无线通信等特点使得路由协议的安全比传统有线网络要复杂得多[2]. 本文将主要针对 Ad Hoc网络中 AODV (Ad Hoc On Demand Distance Vector)路由协议[3]所面临的安全问题进行研究,提出了一种基于 AODV 路由协议的自组网络安全机制.

2 AODV 路由协议的基本思想

AODV 路由协议是一种重要的 Ad Hoc网络按需路由协议,主要是通过路由建立和路由维护两个方面来完成路由功能.

路由建立:当源节点需要和新的目的节点通信时,发起路由发现过程,通过广播路由请求报文 RREQ 来查找相应路由. 当 RREQ 到达目的节点或一个拥有足够新的到目的节点路由的中间节点时,目的节点或中间节点通过原路向源节点返回一个路由应答 RREP来确定路由.

路由维持:节点监视一个活动路由中下一跳节点的状况,当发现链路断开时,就发出路由错误 RERR 消息通知其他节点.

3 AODV路由协议的安全问题

3.1 针对 AODV协议的攻击

从上面 AODV 路由协议的工作过程中可以看到,它不需存储和维护包含全网所有节点信息的路由表,并没有安全机制,目前针对 AODV 协议的攻击主要有:

收稿日期: 2005-03-31;修回日期: 2005-09-12
基金项目:国家高技术发展计划项目 (No. 2002AA784030)

路由干扰攻击:

(1)攻击者可以插入路由包,产生路由环,引起无效路由,从而消耗能量和带宽.

(2)伪造路由信息把所有的分组都传向攻击节点,攻击者把分组全部或有选择地抛弃,形成黑洞或灰洞攻击.

(3)攻击节点不按路由规则转发数据及控制分组,引起网络分割.

能量消耗攻击:攻击节点插入大量冗余数据或控制分组,严重时造成节点能量不足,引起网络的瘫痪.

3.2 相关研究工作

针对 AODV 路由协议存在的主要安全威胁,协议的安全机制就成为一个研究的热点问题,现阶段该领域的研究主要分为 4个方面:

(1)加密和认证[4,5],主要是通过将路由请求、路由应答等报文内容加密、认证来进行安全防范.但 Ad Hoc网络中拓扑频繁变化,报文的加密解密过程实现复杂,且网络节点可能被截获而泄露密码,导致攻击从内部产生.

(2)增强合作,鼓励节点参与网络转发,主要采用:基于惩罚的方法[6],利用邻居监视,不参与网络交换将被排除出网络;引入虚拟流通的概念[7,8],给节点提供激励,使节点能够遵守协议规则,自觉完成流通前向传输分组的转发操作; CORE[9]机制通过协同监测技术和声誉机制创建安全性列表以显示节点的合作性.

(3)入侵检测,主要有静态的基于统计的异常检测方法[10]以及基于代理的入侵检测方案[11]等.

(4)改进策略,例如对于黑洞攻击问题,辛辛那提大学的 Hongmei Deng等人提出了一种解决方案[12].即当中间节点应答 (设为节点 B)时,必须把它的下一跳节点 (设为节点 C)的信息附加在 RREP中发给源节点.源节点根据该信息从其它路由给节点 C发验证包以查询 C是否真有到目的节点和到该应答节点的可用路由.

针对 AODV 协议安全性问题,本文提出一种安全机制.一方面为 AODV 协议增加攻击检测功能;另一方面,借鉴有线网中对实体信用判断的信誉评价机制 Reputation Systems[13],为网络中节点建立信誉机制.该安全机制在网络规模较小且拓扑较稳定时 (节点相对运动速度小于每秒 20米)能够较好地保障网络安全,今后将进一步对此模型进行深入研究,使其具有更大的应用范围.

4 基于 AODV 协议的安全机制

4.1 攻击检测功能

本文对 AODV 协议进行改进,使其具有攻击检测功能,主要体现在以下几个方面:

(1)对黑洞攻击的检测

攻击节点利用网络中节点对于全网拓扑的不了解,向网络广播一些欺骗性的消息,更改路由,吸引网络数据,形成“黑洞 ”.主要手段包括伪造距离向量和伪造序列号.

令网络节点工作在混杂模式,要求回送 RREP消息的中间节点必须同时回送下一跳信息.这样每个节点都能监听其邻居发送的路由条目,通过这种方式,保存其邻居的部分路由表.

下面通过一个例子来说明该检测方法的原理:

如图 1所示,节点 S和节点 D 进行通信.假设节点 X为恶意节点,在其发送的 RREP中标明下一跳为 Y.

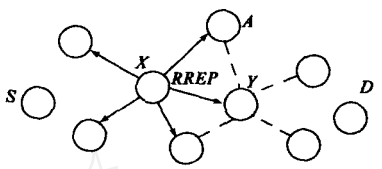

图 1　黑洞攻击的检测方法

(a) Y不是 X的邻居节点. X的邻居节点收到 X回复的 RREP报文中下一跳是 Y,不在 X的邻居表中,立即判断 X为恶意节点.

(b) Y是 X的邻居节点. Y也收到了该 RREP报文. Y查找自己的路由表,若没有到 D的路由,则立即判断 X为恶意节点.否则核对 RREP中的跳数是否等于 Y到 D的跳数加 1,若不满足则也判断 X为恶意节点.

(c)其他某些节点,如上图中的 A节点,它们是 X和 Y共同的邻居,在收到 X的 RREP报文后,根据本地掌握的信息对 X的行为进行判断.

(2)对路由表溢出攻击 (DDOS攻击)的检测

路由表溢出是指恶意节点不停的发送 RREQ,要求与不存在的节点建立路由,大量消耗网络资源.

通过检测网络中是否存在某节点大量发送 RREQ 就能发现是否存在攻击.

(3)对伪造 RERR报文攻击的检测

恶意节点向网络中发送其伪造的 RERR 报文,破坏路由,造成网络分割.收到 RERR 报文的节点发送一个测试分组,探测路由错误 (RERR)报文中的节点是否真的不可达.

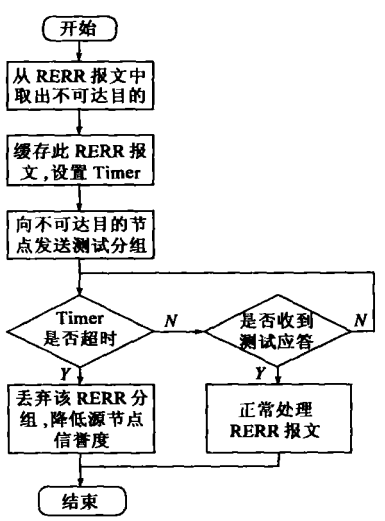

图 2　伪造 BERR报文攻击的检测流程图

如果收到了对应测试分组的应答,则说明发送此 RERR的节点可疑,检测流程见图 2.

(4)对中断路由攻击 (自私节点)的检测

自私节点接收到路由包后不按路由机制进行转发,而是将路由包丢弃,从而造成网络的分割.我们将信誉机制应用其中,实现对这种自私行为的检测.

以上方法得到的检测结果均作用于建立在 AODV 协议之上的信誉机制,共同构成路由协议的安全防御体系.

4.2 信誉机制

定义:对这个实体不会做出恶意行为的信任和对这个系统将会抵御恶意操纵的信任,称为信誉. 信誉度就是衡量网络实体信誉的一个量度.

信誉机制的主要目标是防止网络中不良行为节点的安全威胁,特别是对抗自私节点发出的攻击,主要包括:

(1)提供用以判定节点是否可信的可靠信息;

(2)鼓励节点的合作行为;

(3)排斥不良节点获取机制所保护的合作服务.

4.2.1 信誉机制的建立

信誉是对一个网络实体不会做出恶意行为的信任,是对一个网络实体已有行为的评价. 所以信誉的建立与对网络实体行为的监测密不可分,为了更准确地评估节点的信誉,根据网络的层次划分,将节点的信誉按其行为分类如下:

(1)路由信息信誉子类:评价节点对路由报文的处理行为;

(2)数据转发信誉子类:评价节点对数据报文的转发行为;

(3)恶意行为信誉子类:评价针对 AODV 协议的攻击行为,如黑洞攻击,路由表溢出攻击,网络分割攻击等.

这种分类机制对节点的行为有更准确的评价,从而更充分地利用网络资源,更有效地发现恶意节点.

4.2.2 信誉度的计算

4.2.2.1 路由信誉子类及转发信誉子类的信誉度计算

定义 R_r 为路由信誉子类的信誉度,影响该值的参数有:成功转发路由报文的次数 R_{rs}和不成功转发路由报文的次数 R_{rf}.

成功转发路由报文时提高信誉度,表示该节点可信,令 R_r 在 $[0, +1)$间变化,且随着 R_{rs}的增加 R_r 无限趋近于 1,对于新加入网络的节点在其成功转发路由报文时应迅速提高信誉度,因此理想的以 R_{rs}为自变量的 R_r 函数可以表示为:

$$R_r = \begin{cases} 1 - \dfrac{2}{R_{rs} + R_{rf}}, & \text{当 } R_{rs} + R_{rf} \neq 0 \\ 0, & \text{其他} \end{cases} \tag{1}$$

当不成功转发路由报文时,降低信誉度,表示该节点不可信,R_r 在 $[-1, 0)$间变化,且随着 R_{rf}的增加 R_r 无限趋近于 -1,对于新加入网络的节点,在其不转发路由报文时应迅速降低其信誉度,将其隔离出网络. 因此理想的以 R_{rs} 为自变量的 R_r 函数可以表示为

$$R_r = \begin{cases} \dfrac{2}{R_{rs} + R_{rf}} - 1, & \text{当 } R_{rs} + R_{rf} \neq 0 \\ 0, & \text{其他} \end{cases} \tag{2}$$

总结公式(1)、(2),得出路由信誉子类的信誉度为:

$$R_r = \begin{cases} \dfrac{R_{rs} - R_{rf}}{R_{rs} + R_{rf}}, & \text{当 } R_{rs} + R_{rf} \neq 0 \\ 0, & \text{其他} \end{cases} \tag{3}$$

同理得出转发信誉子类信誉度与报文转发数据成功的次数的关系如下:

$$R_f = \begin{cases} \dfrac{R_{fs} - R_{ff}}{R_{fs} + R_{ff}}, & \text{当 } R_{fs} + R_{ff} \neq 0 \\ 0, & \text{其他} \end{cases} \tag{4}$$

这里 R_f 表示转发信誉子类的信誉度,R_{fs}表示成功转发数据报文的次数,R_{ff}表示不成功转发数据报文的次数.

4.2.2.2 攻击行为信誉子类的信誉度计算

R_m 表示恶意行为信誉子类的信誉度,其中 m 表示节点产生行为的次数. 攻击行为信誉子类的信誉度计算考虑到以下两个方面:

(1)网络节点的正常行为增加其信誉度.

(2)当实体(即网络节点)行为不正常时,进行以下考虑:

考虑此类信誉评价实体是否有攻击行为,一旦出现攻击行为则大幅降低该实体的信誉度. 当该实体以前工作正常时($R_m > 0$),将其信誉度减半,同时为了防止其信誉度接近 0时减半操作不会给信誉度带来大的影响,再减少一个 ΔR;当该实体以前出现过不正常的情况($R_m < 0$),采用线性递减策略,但减幅较大,同样迅速降低其信誉度. 因此,可以得到 R_{m+1}与 R_m 的关系如下:

$$R_{m+1} = \begin{cases} R_m + \Delta R, & \text{当实体行为正常时} \\ \left.\begin{array}{ll} R_m/2 - \Delta R, & R_m > 0 \\ R_m - 2 * \Delta R, & R_m < 0 \end{array}\right\} & \text{当实体行为不正常时} \end{cases} \tag{5}$$

当实体(即网络节点)的行为正常时,ΔR 表示每做一次正常行为信誉度的增量. 由 $R_{m+1} = R_m + \Delta R$ 可得:$R_m = m * \Delta R + R_0$(R_0 为初始信誉度),这是一个关于 m 的一次函数,随着 m 的增加 R_m 线性增长;变量 ΔR 的大小影响着信誉度变化的激缓.

例如:

当 $R_m > 0$时,由 $R_{m+1} = R_m/2 - \Delta R$ 可得:

$$R_m = 2^{-m} R_0 - 2\Delta R(1 - 2^{-m}) \tag{6}$$

令 $R_m = 0$,可得:

$$m = \log_2\left(\frac{R_0}{2\Delta R} + 1\right) \tag{7}$$

当 R_0 取 1(表示实体已被完全信任),ΔR 取 0.167(1/6,表示经过 6次合法行为该实体就会被完全信任)时,m = 2. 这个结果说明,当一个实体经过一系列合法的操作已经得到完全信任的情况下,突然发起攻击时,经过连续的两次恶意行为后其信誉度就会变为 0,所以能够迅速发现恶意节点.

当 $R_m < 0$时,R_m 线性减小,提高了降低的速率,使其快速的到达报警阈值.

4.2.2.3 总体信誉度的计算

根据不同情况下网络实体

对其他实体所提供不同服务的期望不同 (例如,A 可能希望 B 转发数据而不在乎它提供的路由是否可靠. 这样,A 仅对 B 的数据信誉子类要求较高),总体信誉度应为各信誉子类信誉度的加权和. 即

$$R = W_f \times R_f + W_r \times R_r + W_m \times R_m \quad (8)$$

其中,R 为某网络实体的总体信誉度,R_f 为转发子类信誉度,R_r 为路由子类信誉度,R_m 为恶意行为的信誉度;W_f 为转发信誉子类的权重,W_r 为路由信誉子类的权重,W_m 为恶意行为信誉子类的权重 (权重值可以根据具体情况决定).

4.2.3 信誉的撤销

当节点做出恶意行为后,其信誉度随之降低. 当降低到一定程度时,检测其行为的节点将发出报警信息,在确定该实体是一个恶意实体后,网络中的其他实体将其放入黑名单中,不再与其通信,也不再维护其信誉,有关此实体的信誉将被删除,至此完成对其信誉的撤销.

5 仿真结果及性能分析

本文使用公开源代码的网络仿真软件 NS2. 26搭建网络仿真平台进行仿真. 该模型由 30个移动节点构成,并在 1000m ×1000m 的范围内以最大速度 20m /s做随机运动,节点采用单一增益的全向天线,无线发射范围 250m,仿真时间 1000s.

5.1 对网络性能的影响

攻击者进行攻击的目的有两个:一个是窃取网络中对之有用的数据;另一个是影响网络的正常通信. 对于第一个目的,只能通过对数据加密的手段来解决,在本文中不做讨论. 而对于第二个目的,分组投递率 (信宿收到的分组数量与信源发送的分组数量的比值)是评价网络性能的一个重要指标.

以伪造距离向量攻击和伪造路由错误报文攻击为例,在网络不同负载情况下对标准 AODV 协议和具有安全机制的 AODV 协议受到攻击时的分组投递率进行仿真分析. 仿真过程中上层流量为以节点 29为目的节点的 CBR (恒定比特率)数据流,数据包尺寸为 512byte,每个数据流发送分组速率为 2个 /s.

图 3(a)是受到伪造距离向量攻击时的投递率曲线,从中可以看到,在伪造距离向量攻击之下的 AODV 协议的分组投递率虽然明显低于正常情况,但是却随着连接数的增加有微弱的提高,这是因为,随着连接数的增加,攻击节点无法及时提供最新序列号的路由信息,所以网络中错误的路由会被目的节点提供的新的路由信息所替代,这样就造成图中的现象,图中第二条曲线是具有安全机制 AODV 协议的分组投递率曲线,明显高于在伪造距离向量攻击之下的标准 AODV 协议,说明具有安全机制的 AODV 协议具备良好的抗攻击性能.

图 3(b)是受到伪造错误报文攻击时的投递率曲线.

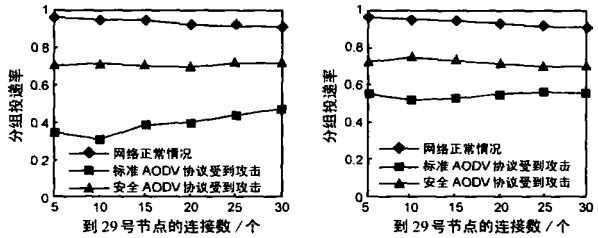

图 3　分组投递率比较. (a)伪造距离向量攻击; (b)伪造错误报文攻击

从中可以看出,伪造路由错误 (RERR)报文会造成网络分割,标准的 AODV 协议分组投递率非常低. 当 CBR 连接数增大时,网络的分组投递率有一定的升高,这是因为 CBR 连接数的增加使得在分割后所形成的子网内部的通信增加,从而提高了全网分组投递率. 而采用具有安全机制的 AODV 协议后,网络性能有明显地提高,在本仿真场景下大约维持在 70%左右.

表 1　攻击检测方法性能表

检测方法 \ 指标	正确率	误判率	反应时间 (s)
序列号攻击	90.2%	9.8%	9.7
伪造距离向量攻击	85.6%	12.6%	8.5
路由表溢出攻击	83.8%	13.2%	8.2
伪造距离向量攻击	86.5%	11.6%	10.3
中断路由攻击	82.5%	13.8%	12.3

5.2 检测安全机制的准确性

本文使用两个指标来衡量检测效果,一个是攻击检测的正确率 ——发现的恶意节点数占恶意节点总数的比率;另一个是攻击检测的误判率 ——将非恶意节点判定为恶意节点的数目占非恶意节点的总数.

按以下仿真参数下进行仿真 (信誉度报警阈值为 -0.1,信誉度变化幅度 $\Delta R = 0.1667$),得出各种攻击检测的性能指标如表 1所示,表中可以看出,在十几秒以内的反应时间里,使用攻击检测方法时达到了较高的正确率.

6 总结

本文对 Ad Hoc网络的路由安全问题进行研究,分析了 AODV 路由协议的安全隐患,为协议增加了具有攻击检测、基于信誉度的安全机制,使之能够检测到网络节点的恶意行为并迅速做出反应,实现对网络内部及外部攻击的防范. 仿真分析表明,所提出的基于 AODV 协议的自组网络安全机制,将有效地保障路由安全,提高网络的可用性.

参考文献:

[1] C-K Toh. Ad Hoc Mobile Wireless Networks: Protocols and Systems[M]. Indiana: Prentice Hall PTR, 2002. 55-77.

[2] Yang H. Security in mobile Ad Hoc networks: Challen-

ges and solutions[J]. IEEE Wireless Communications, 2004, 11(1): 38 - 47.

[3] Charles E Perkins, Elizabeth M Belding Royer, Samir R Das. Ad hoc on-demand distance vector(AODV) routing[EB/OL]. http://www.ietf.org/rfc/rfc3561.txt, 2003 - 07.

[4] Ingo Riedel. Security in Ad Hoc networks: Protocols and ECC on Embedded System[D]. Bochum: Ruhr University, 2003.

[5] 谢冬莉,周晓峰. 对AODV路由协议的三种攻击方法及相应的解决方案[J]. 计算机与现代化, 2004, (10): 101 - 104.
Xie Dong-li, Zhou Xiao-feng. Three attack methods to AODV and corresponding solutions[J]. Jisuanji yu Xiandaihua, 2004, (10): 101 - 104. (in Chinese)

[6] Sonja Buchegger, Jean-Yves Le Boudec. Performance analysis of the confidant protocol: Cooperation of nodes-Fairness in distributed ad-hoc networks[A]. IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing(MobiHOC2002)[C]. Lausanne, 2002. 226 - 236.

[7] Sheng Zhong, Jiang Chen, Yang Richard Yang. Sprite: A simple, cheat proof, credit-based system for mobile ad-hoc networks[A]. The 22nd Annual Joint Conf IEEE Computer and Communications Societies (INFOCOM 2003)[C]. San Francisco: CA, 2003. 1987 - 1997.

[8] Butty'an L, Phuhaux J, Nuglets. A virtual currency to simulate cooperation in self-organized Ad Hoc network[R]. Swiss: Swiss Federa Institute of Technology-Lausanne, 2001.

[9] Pietro michiardi, Refik molva. CORE: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks[A]. Sixth IFIP conference on security communications, and multimedia(CMS 2002)[C]. Slovenia: Portoroz, 2002. 107 - 121.

[10] Yongguang Zhang, Wenke Lee. Intrusion detection techniques for mobile wireless networks[J]. Wireless Networks, 2003, 9(5): 545 - 556.

[11] 李玲娟,王汝传. 一种基于移动代理的MANET IDS模型[J]. 计算机工程与应用, 2005, (20): 139 - 141.
Li Ling-juan, Wang Ru-chuan. A mobile Agent based IDS model for MANET[J]. Computer Engineering and Applications, 2005, (20): 139 - 141. (in Chinese)

[12] Hongmei Deng, Wei Li. Routing security in wireless Ad Hoc networks[J]. IEEE Communication Magazine, 2002, 40(10): 70 - 75.

[13] Resnick, Paul, Zeckhauser, et al. Reputation systems[J]. Communications of the ACM, 2000, 43(12): 45 - 48.

作者简介:

李 喆 女, 1967年生于辽宁沈阳,东北大学教授,博士生导师,主要从事新一代网络及无线通信系统方面的研究.
E-mail: lizhe@mail.neu.edu.cn.

刘 军 男, 1969年生于辽宁沈阳,博士研究生,主要从事无线通信及卫星通信方面的研究.