

OLSR 路由协议中 MPR 节点安全性研究

张登银, 王振兴

(南京邮电大学 计算机学院, 江苏 南京 210003)

摘 要: OLSR(最优链路状态路由协议)是一种先应式路由协议,其MPR(多点中继)节点易受恶意攻击,严重时将导致路由协议崩溃。针对这一安全隐患,提出了一种MPR节点综合抗攻击方案:消息加密和消息频率检测技术。消息加密技术主要是对广播的HELLO消息进行加密,防止攻击节点冒充合法节点;频率检测是对HELLO消息发送频率进行检测,若频率过大则可以认为发送该HELLO消息的节点为恶意节点。仿真结果表明,该综合方案可以有效抵制对MPR节点的攻击,保证OLSR路由协议的安全。

关键词: 最优链路状态路由协议;多点中继;安全

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2011)12-0142-03

Security Study of MPR Nodes in OLSR Routing Protocol

ZHANG Deng-yin, WANG Zhen-xing

(College of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210003, China)

Abstract: OLSR (optimized link state routing protocol) is a first response routing protocol. The MPR (Multi-Point Relays) nodes are vulnerable to malicious attacks and the routing protocol will result in serious crash. In response to this security risk, present program of MPR nodes against attacks: technology of message encryption and message frequency detection. Technology of message encryption encrypts HELLO messages which are broadcasted to prevent the attack nodes; Technology of message frequency detection detects the frequency of HELLO messages, and if the frequency is too large, you can charge the HELLO message as a malicious node. Simulation results show that this scheme can effectively resist the attack of the MPR nodes to ensure the safety of OLSR routing protocol.

Key words: OLSR protocol; MPR; security

0 引言

移动自组网(Mobile Ad Hoc Network)^[1,2]是一种无基础设施的无线网络,最初是为军事应用,由于它具有开放的媒质、分布式的合作、动态的拓扑结构和受限的网络能力等特点,所以特别容易受到攻击,目前针对Ad Hoc网络的攻击^[3]有:虫洞攻击^[4,5]、协同欺骗攻击^[6]等,当然也有很多研究这些攻击的防御方案。OLSR协议^[7]是Ad Hoc网络中的路由协议,在优化网络负载的同时,使得网络的完整性和安全性在一定程度上比较容易受到恶意节点攻击,文中通过针对OLSR协议中MPR节点攻击的防御进行安全分析,这对于广泛应用于军事上的Ad Hoc网络安全问题有非常

重要的意义,目前该方面的研究国内还比较少。

1 OLSR 协议安全性分析

1.1 OLSR 协议机制

OLSR是由INRIA(法国国家信息与自动化研究所)提出,并被IETF MANET工作组确定为RFC标准的一种先应式无线移动Ad Hoc网络路由协议^[8],OLSR协议继承自LSR路由协议,采用MPR(多点中继)机制进行优化:

- (1)每个节点在自己的一跳邻居里寻找部分节点作为MPR节点,只有被选择为MPR的节点才作为消息中转站,减少了因发送消息过多而引起的洪泛效应;
- (2)OLSR中只有MPR才产生链路状态信息,即MPR节点只记录它与把它选为MPR节点间的链路。

OLSR是一种先应式的网络^[9],表现在节点定时广播HELLO和TC消息,HELLO消息主要用于实现链路侦测、邻居侦听的功能,以此建立节点的本地链路信息表,同时也用于向邻居节点通告本节点的MPR节点选择;TC消息用于执行MPR Selector链路状态声明,使得每个节点都能够感知全网拓扑图。OLSR协议的

收稿日期:2011-05-08;修回日期:2011-08-13

基金项目:国家自然科学基金(61071093);国家863计划(2009AA701202);Swedish Research Links Programme(348-2008-6212);留学回国人员项目(NJ209002)

作者简介:张登银(1964-),男,江苏靖江人,博士,研究员,博士生导师,CCF会员,研究方向为信息安全、信号与信息处理、IP网络技术;王振兴(1987-),男,江苏溧阳人,硕士研究生,研究方向为基于IP的下一代通信与系统安全。

主要工作过程为:首先,节点之间周期性地互相发送 HELLO 消息来完成邻居探测;其次,OLSR 协议中的 MPR 节点机制可以大幅度减少控制消息的洪泛规模,只有被选为 MPR 的节点才会把 TC 分组消息发送到全网;最后是构建路由表,每个节点周期性地通过它周围的 MPR 节点传播 TC 消息到网络中的所有节点,网络中的每个节点通过接收到的 TC 消息建立它的拓扑表,然后再利用最短路径算法来计算出它的路由表^[10,11]。

1.2 OLSR 协议的安全性

由于 OLSR 协议的开放性、分布式合作和动态的拓扑结构等特性导致其很容易受到攻击。目前针对 OLSR 协议的攻击有一种恶意攻击:针对 MPR 节点的攻击。

经过对 OLSR 协议的分析发现每个节点的 HELLO 消息中都带有一个 willingness 的字段,该字段表示发送消息的节点作为 MPR 节点的意愿程度,常用的有五种类型:WILL_NEVER 表示节点不能作为 MPR 节点;WILL_ALWAYS 表示节点必须被选择为 MPR;WILL_DEFAULT 表示节点可作为 MPR 但不是必须的,视具体的算法而定;WILL_LOW 表示节点作为 MPR 节点的优先级较低;WILL_HIGH 表示节点作为 MPR 节点的优先级较高。默认为 WILL_DEFAULT。

针对 MPR 节点的攻击,实质上就是针对其中的 willingness 字段。如图 1 所示,假设有 12 个正常节点 $X_i(i=0,1,\dots,11)$,2 个攻击节点 $G_j(j=1,2)$ 。 G_1 用于模拟被攻击节点 X_1 向周围一跳邻居节点发送 HELLO 消息,不过其中的 willingness 字段值为 WILL_NEVER,使得被攻击节点不能作为 MPR 节点,从而中断 X_0 节点与 X_3 节点的通讯,通过仿真发现通过修改攻击节点 G_1 发送 HELLO 消息的频率可以使得经过被攻击节点 X_1 的数据丢包率不断增加,当频率足够大时 X_0 节点与 X_3 节点之间的联系完全中断。实现了对已有链路的破坏后,另外攻击节点 G_2 开始工作,代替原 X_1 节点把

已经断开的连接重新连接,让数据消息通过攻击节点 G_2 ,从而达到攻击网络的目的,接下来就可以窃取或修改消息。在实际攻击中 G_1 节点攻击频率可以直接设置为能使得网络连接中断的值,而 G_2 节点同时开始工作,几乎使得网络无法感觉到被攻击。

2 MPR 节点抗攻击方案

针对以上分析,提出了在 MPR 节点上进行 HELLO 消息加密认证和频率监测两层抗攻击解决方案。

2.1 加密认证

通过分析 HELLO 消息的格式发现,其中有一个预留字段,基于这样一个字段可以在不增加 HELLO 消息长度的前提下给它加上验证来保证消息的安全。针对以上攻击采用以下的第一层过滤方案:修改 OLSR 协议,给发送的 HELLO 消息的预留字段加上一个加密的验证信息,但是必须保证大小不能超过 16 位表示范围的数或字符串,目前比较安全的加密方法是 MD5 加密法。每个 HELLO 消息都会在经由 MD5 加密的保护下发送,接收方在获取消息后首先进行消息安全验证,如果消息非法则选择丢弃。通过这一层的过滤,非法 HELLO 消息在加密的保护下能抵御大部分攻击,但是 MD5 并不是不可以破解,一旦这一层抗攻击被攻破还有以下频率检测的抗攻击方案来确保网络安全。

2.2 频率监测

提取 HELLO 消息中的 willingness 字段并判断其值是否为 WILL_NEVER,如果不是则说明没有受到攻击,正常处理 HELLO 消息;如果是则说明网络有可能受到攻击,通过在协议中添加了 HELLO 消息跟踪监控功能可以在这个时候监控发送该 HELLO 消息的一跳邻居节点发送消息的频率,如果在正常 HELLO 消息发送时间间隔过程中发现接收到 HELLO 消息频率大于原频率的 2^3 倍,可以认为网络受到攻击,此时选择丢弃该 HELLO 消息并且反馈网络节点受到攻击但被拦截的信息。

3 仿真和数据分析

3.1 参数配置

仿真平台是比较成熟的 NS2,网络模型是:600m * 600m 的区域内分布有 14 个节点,其中包含 2 个攻击节点,具体参数配置如表 1 所示。

3.2 仿真过程

仿真场景如图 1 所示,模拟 X_0 节点给 X_3 节点发送数据,首先让攻击节点 G_1 作用于网络,通过不断提高 G_1 节点 HELLO 消息的发送频率使得丢包率不断增加,当网络中添加文中提出的抗攻击方案后,丢包率稳定在 10% 左右,结果如图 2 所示,其中纵坐标表示丢

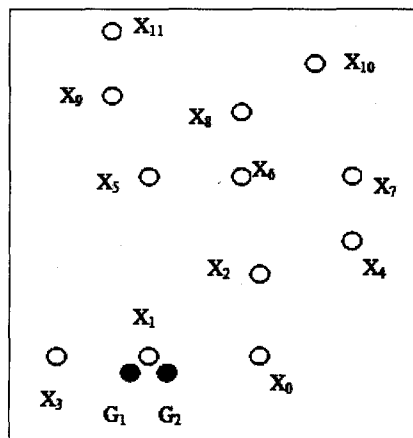


图 1 基于 MPR 攻击模拟

包率,横坐标表示 HELLO 消息发送频率提高到原来的 2^x 倍。

表 1 仿真参数

仿真时间	100s
通信方式	CBR(UDP)
发包速率	30Kb/s
带宽	11Mb

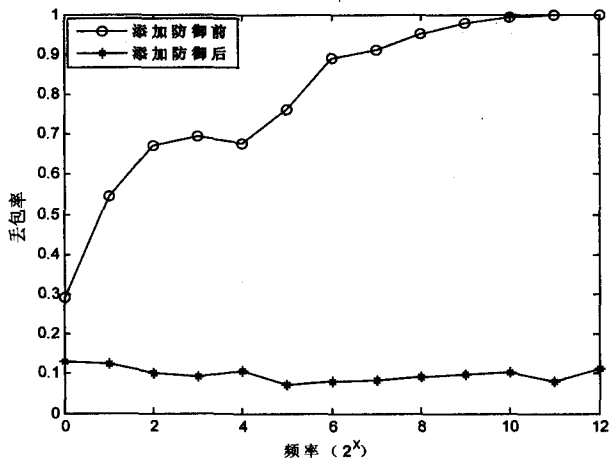


图 2 一个攻击节点攻击结果

先启动 G_1 节点,然后启动 G_2 节点,可以发现节点 X_0 到节点 X_3 之间的通路先被阻断后有恢复,针对以上攻击,网络中采用文中提出的防御方法,结果如图 3 所示,图中上面的线表示在没有防御情况下受到攻击的情况,随着攻击节点 G_1 的 HELLO 消息发送频率的增加网络丢包率不断增加直到完全中断, G_2 节点的启用使得网络恢复正常。下面那条线表示网络中添加了文中提到的防御功能后的情况,此时丢包率一直保持在一个正常的范围内。

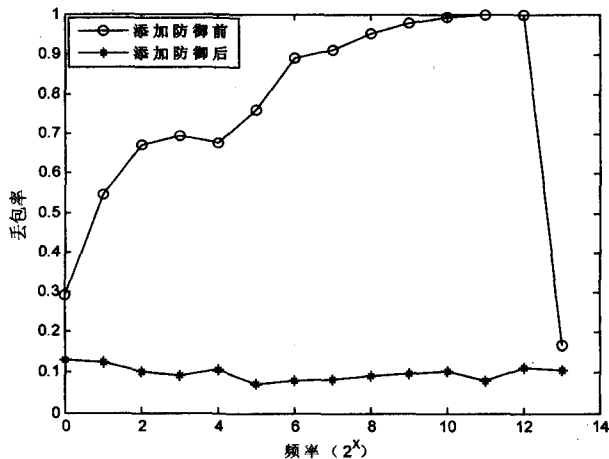


图 3 两个攻击节点攻击结果

3.3 数据分析

初始条件下恶意节点 G_1 发送 HELLO 消息的频率与正常节点一样,可以看出攻击效果不明显,但是使得 X_0 节点给 X_3 节点发送的小部分数据丢失,随着 G_1 节点发送 HELLO 消息频率的不断从图中可以看出

丢包率基本呈现出不断上升的趋势,当频率达到一定值后数据完全丢失,此时达到使网络瘫痪的目的。此时启动 G_2 节点,丢包率瞬间重新回到没有攻击时的正常水平。针对以上的攻击,若被攻击网络加上安全防御,如图 3 可以看出丢包率一直保持在正常状态,而且保证数据在此类攻击下不会被窃取或篡改,完全保证了网络在上述攻击下毫无影响。

4 结束语

文中针对 Ad Hoc 网络中 OLSR 协议的安全问题提出了一种针对 MPR 节点攻击的防御方案,通过仿真分析可以看出,在攻击情况下整个网络有瘫痪甚至有被攻击者窃取或篡改数据的危险,但是带有防御功能的网络能够完全避免受到此类攻击,这在军事上有非常重要的意义。

参考文献:

- [1] Murray D, Dixon M, Koziniec T. An experimental comparison of routing protocol in multi hops ad hoc networks[C]//Telecommunication Networks and Applications Conference. [s. l.]:IEEE,2010:1-8.
- [2] 刘宴涛,安建平,卢继华,等.无线自组网个体移动模型分析[J].通信学报,2010(2):36-43.
- [3] Alam M, Chan King-sun. Topological comparison based approach of detecting wormhole attacks in OLSR protocol[C]//Signal Processing and Communication System International Conference. [s. l.]:[s. n.],2010:1-5.
- [4] 付颖芳,张兴,张婷,等.无线 mesh 网络中的虫洞攻击检测研究[J].通信学报,2010(1):59-65.
- [5] 滕萍. Ad Hoc 无线网络虫洞攻击安全策略研究[J].网络安全技术与应用,2011(3):8-10.
- [6] 秦嵘,张尧弼.基于攻击树的协同入侵建模[J].计算机应用与软件,2005(4):116-118.
- [7] Javed S, Furqan-ul-Islam Pirzada A A. Performance analysis of OLSR protocol in a mobile Ad hoc wireless network[C]//International Conference on Computer, Control and Communication. [s. l.]:[s. n.],2009:1-5.
- [8] 张信明,曾依灵,干国政,等.用遗传算法寻找 OLSR 协议的最小 MPR 集[J].软件学报,2006(4):932-938.
- [9] Elshaikh M, Kamel N, Awang A. High throughput routing algorithm metric for OLSR routing protocol in wireless mesh networks[C]//Signal Processing & Its Applications International Conference. [s. l.]:[s. n.],2009:445-448.
- [10] de Rango F, Fotino M, Marano S. EE-OLSR: Energy efficient OLSR routing protocol for mobile ad-hoc networks[C]//Military Communications International Conference. [s. l.]:IEEE,2008:1-7.
- [11] 刘志远,杨植超. Ad hoc 网络及其安全性分析[J].计算机技术与发展,2006,16(1):231-232.