文章编号:1001 - 9081(2007)05 - 1062 - 02

Ad Hoc 网络中 OLSR 路由协议的蠕虫防御

冯庆煜
(西华师范大学 计算中心,四川 南充 637100)
(fqy_work@163.com)

摘 要: 针对目前网络蠕虫防御系统的不足,传统路由协议又不能从根本上保证 Ad Hoc 网络的安全。通过剖析优化的链路状态路由协议(OLSR)中存在的蠕虫路径问题,在现有解决方案的基础上,提出一种有效的路径选择方案,保障了数据端到端传输的可靠性,从而增强了路由协议的安全性。

关键词:Ad Hoc 网络;路由安全;优化的链路状态路由协议;蠕虫防御
中图分类号: TP391 **文献标识码**:A

Worm recovery of OLSR protocol in Ad Hoc

FENG Qing-yu
(*Center of Computing, China West Normal University, Nanchong Sichuan* 637002, *China*)

Abstract: The current worm recovery system has limitation, and traditional security routing protocol cannot adapt to mobile Ad Hoc networks. This paper analyzed the wormhole problem in Optimized Link State Routing protocol (OLSR) in detail, and proposed a valid strategy to solve it on the basis of the current one. It ensures the reliability of data transfer from end to end, thus increases the security of routing protocol.

Key words: Ad Hoc network; routing security; Optimized Link State Routing protocol(OLSR); worm recovery

0 引言

优化的链路状态路由协议(OLSR)是 Ad Hoc 网络中的一种表驱动式的链路状态路由协议。Ad Hoc 网络系统是一种具有高度变化的拓扑结构、不依赖于固定主干网、无基站支持的多跳、能快速部署到位、完整、强大、高抗毁的、能提供有效的数据和多媒体通信服务的独立的网络通信系统。由于 Ad Hoc 网中节点需要同时扮演主机和路由器双重角色,Ad Hoc 网具有无基础设施需求、节点间链接脆弱、拓扑结构动态变化、身份认证缺乏以及无线信道的开放性等特征,因此其 OLSR 路由协议比传统网络面临更多的安全问题。

1 OLSR 路由协议的工作方式

OLSR 主要采用 HELLO 和 TC(Topology Control) 两种控制分组。其中 HELLO 用于建立一个节点的邻居表,包括邻居节点的地址以及本节点到邻居节点的延迟或开销;OLSR 采用周期性地广播 HELLO 分组来侦听邻居节点的状态,节点之间无线链路的状态包括:非对称链路,对称链路,连接多点中继站 MPR(Multipoint Relay)的链路。同时 HELLO 分组用于计算该节点的 MPR,HELLO 分组只在一跳的范围内广播,不能被转发;与之相反,TC 分组必须被广播到全网,在 TC 分组中包含了将发送 TC 分组的节点选为 MPR 的邻居节点的信息,节点根据收到的 TC 分组来计算出网络的拓扑图。

每个节点都要周期性地转发 TC 分组,在 TC 分组中就包含了将该节点选为 MPR 的邻居节点地址(称为 MPR selector),当节点收到 TC 分组时,首先判断自己是不是属于源节点的 MPR,如果发现自己属于源节点的 MPR,再根据 TC 分组中的序列号来判断该 TC 分组是否是最新的,如果是,则转发该 TC 分组,否则丢弃该分组。通过 MPR 机制来控制 TC 分组在网络中广播的规模,减少控制分组给网络带来的负荷。这些信息足以让网络中的各个节点形成网络拓扑图,进而独立地根据最短路径优先的原则来计算路由表。

2 OLSR 路由协议的蠕虫攻击

蠕虫攻击,是一种针对 Ad Hoc 路由协议,特别是带有防御性的路由协议的严重攻击,它是在两个串谋恶意节点间建立一条私有通道,攻击者在网络中的一个位置上记录数据包或位信息,通过此私有通道将窃取的信息传递到网络的另外一个位置。在数据包的传递过程中,蠕虫攻击者可以故意传递部分数据包,或篡改数据包的内容,将造成数据包的丢失或破坏。同时因为蠕虫能够造成比实际路径短的虚假路径,它会扰乱节点间的路径选择,从而导致路由发现过程的失败。

OLSR 路由协议通过周期性地发送 HELLO 分组来检测邻居节点,如果攻击者通过私有通道将由节点 A 发出的 HELLO 分组传送给节点 B 附近的串谋攻击者,同样攻击者通过私有通道将节点 B 发出的 HELLO 分组传递给先前的攻击者,那么 A 和 B 将相信它们互为邻居节点,这将导致如果它们实际不是邻居节点时,路由协议将不能找到正确的路径。在如图 1 所示,A 和 B 为正常节点,但是它们彼此检测不到,M 为恶意节点,它可以检测到 A 和 B。

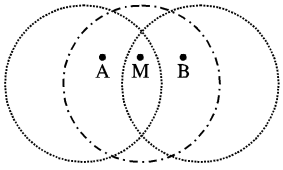

图 1 虫洞问题

M 节点攻击如下:

1) $A \rightarrow *$:*HELLO_MESSAGE*, A, *neighbor*(A);
neighbor(A) 表示节点 A 的邻节点

2) $M \rightarrow *$:*HELLO_MESSAGE*, A, *neighbor*(A);

收稿日期:2006 - 12 - 01;**修订日期**:2007 - 02 - 11
作者简介:冯庆煜(1950 -),男,四川中江人,副教授,主要研究方向:计算机网络信息系统、网络安全、程序设计.

3）节点 B 检测到 A 发出的 *HELLO_MESSAGE*,它就认为节点 A 是其邻节点。

4）$B \rightarrow *$:*HELLO_MESSAGE*, B, *neighbor*(B);

5）$M \rightarrow *$:*HELLO_MESSAGE*, B, *neighbor*(B);

6）节点 A 检测到 B 发出的 *HELLO_MESSAGE*,它就认为节点 B 是其邻节点。

于是 M 使得节点 A 和 B 相信它们互为邻节点。

3　OLSR 路由协议的蠕虫防御

蠕虫非常难于检测,因为它用于传递信息的路径通常不是实际网络的一部分;同时它还特别危险,因为它们能够在不知道使用的协议或网络提供的服务的情况下进行破坏。目前,已经有一些研究人员提出不同蠕虫问题的解决方法。其中有一部分解决方案是基于加密算法的安全策略,比如:Papadimitratos 提出的路由协议安全扩展[4]、Hu 等提出的 SEAD[5]、Yi 提出的 SAR[6]。这些安全路由协议可以提供较完善的路由安全保障,主要使用加密方法改变无线传输中的位信息,但一旦节点妥协,这种方法就可能失败。

卡内基大学的 Hu 等人提出了一种称为“数据包限制”(packet leashes)的机制[5],采用一种有效的认证协议 TIK 来检测并防御蠕虫攻击,即匹配每个数据包的时间戳和位置戳以检测系统中是否有蠕虫入侵。每个数据包被发送节点打上了非常精确的时间信息或几何位置信息的标签,目标节点将数据包到达的时间和位置信息与标签相比较,如果数据在不切实际的时间长度内传送了不切实际的距离,那么就认为网络中有蠕虫。

结合前面的研究,现提出一种新的蠕虫防御方案,旨在加强邻节点关系的建立。在无线传输范围之内,只有通过了身份认证的节点才能成为邻节点,相邻节点关系确立后,达到防御蠕虫攻击的目的。

(1) 初始阶段安全假设

我们假设网络是双向链接的,即若从节点 A 能传送数据包到节点 B,那么从节点 B 也能传送到节点 A。

设想每个合法节点均拥有一对密钥,对相应节点 A 为 $(K_A, K^{-1}{}_{CA})$,K_A 是公钥,$K^{-1}{}_{CA}$ 为私钥。节点身份的可信度由第三方信任实体 CA 颁发的证书保证,节点 A 的身份证书基本格式为:

$$Cert_A = \{ID_A, K_A, VTime_A\}_{K^{-1}{}_{CA}}$$

为简化设计,假设 Ad Hoc 网络合法节点已通过安全方法获得本节点的身份证书及其他合法节点的公钥、证书版本号等相关资料。

(2) 邻居节点位置的确定

我们对邻居作如下定义:只有距节点一跳距离范围并通过了身份认证的节点才能成为邻居节点。

因为蠕虫的距离长于一跳间的距离,那么在其间数据包的传输时间肯定大于一跳间的传输时间。如果我们知道数据包准确的传输时间 t,就可以得到数据实际的传送距离 $L = t \times c$,其中 c 是无线信号的传播速度。同时,节点的无线网卡的传输范围 R 是已知的,如果 $L > R$,那么网络中可能存在蠕虫,反之则无。假设节点 B 收到了陌生节点 A 发出的 *HELLO* 分组,它将执行以下步骤:

· 节点 B 向节点 A 发送一个检测包,同时启动一个计时器;

· 节点 A 收到检测包后,立即发送一个应答包,同时也启动一个计时器;

· 一旦节点 B 收到节点 A 发出的应答包,立即停止计时,并也向节点 A 发送一个应答包。节点 B 获取了时间间隔 Δt_b,那么节点 A 和 B 之间的距离 S 就可以得到为 $(\Delta t_b/2) \times c$,如果 $S > R$,节点 B 不会加 A 为邻节点,否则将对节点 A 作身份认证;

· 节点 A 收到了从节点 B 发出的应答包后,马上停止计时,记录下数据包传输的时间间隔 Δt_a,计算出节点间的距离 $S = (\Delta t_a/2) \times c$,如果 $S > R$,节点 A 不会加 B 为邻节点,否则将对节点 B 作身份认证。

(3) 节点的身份认证

在通过了邻居位置的确认后,下一步就是进行节点的身份认证。

· 节点 A 生成一个数据包,包括一个随机数 R_a,身份证书和包的哈希值,将其发送到节点 B;

$A \rightarrow B$:$A, B, Cert_A, R_A, sign(H(A, B, Cert_A, R_A))$;

其中,$H()$ 是一个哈希函数,$sign()$ 表示数字签名操作。

· 节点 B 收到从 A 发出的数据包后,它将首先校验 A 的身份证书,以获取 A 的公钥来检验数据包的数字签名。所有这些完成后,节点 B 同样发送一个包含随机数 R_b,节点的身份证书和哈希值的数据包到节点 A。

$B \rightarrow A$:$B, A, Cert_B, R_B, sign(H(B, A, Cert_B, R_A, R_B))$

· 节点 A 收到从节点 B 发出的数据包,在校验了节点 B 的身份证书和数据包的数字签名之后,A 向 B 发出一个应答包,并相信节点 B 为其邻节点,将其加入节点 A 的邻居表中。

$A \rightarrow B$:$A, B, sign(H(A, B, R_A, R_B))$

· 节点 B 在收到节点 A 的应答包后,也相信节点 A 为其邻节点,并将其加入节点 B 的邻居表中。

在经过了邻居位置的确认和节点的身份验证后,节点 A 和 B 就能够建立起信任的邻居关系。

4　仿真检测与性能分析

4.1　网络仿真

1）采用 NS-2 仿真器,对 50 个节点进行仿真,节点随机分布在 1 000m × 1 000m 的矩形区域内,不同的移动场景文件使用不同的暂停时间。开始仿真后,节点在暂停时间内保持静止,然后随机选择一个目的地,以 0 或最大速度之间的某个速度向目的地移动,达到目的地后再在暂停时间内暂停,再随机选定另一个目的地,重复前面的过程。在整个仿真过程中,节点会一直重复上述的过程,整个仿真时间为 1 000s。定义移动最大速度为 20m/s。和 7 个不同暂停时间的移动模式。暂停时间 t 分别为 0s,200s,400s,600s,800s,1 000s。

2）通信流量仿真,采用 CBR 流量源,以每秒 4 个的速率发送包,每个包的大小均为 64B,网络中含有 20 或 30 个 CBR 源。

4.2　性能评估参数

1）分组投递率:目的节点接收到的数据包与 CBR 源节点发出数据包的比率;

2）平均端到端时延:从开始建立路由,到回传信息,一直到数据传送完毕所需的时间。

4.3　结果与分析

第一组实验数据,如图 2,是 OLSR 和 WOLSR 下不同的分组投递率。图 2 反映出 WOLSR 下的分组投递率有所提高,表明协议安全性有所增强。

此外,在增加 CBR 源的情况下,WOLSR 可以减少大量路由开销,分组投递率降低得很少,且在源数目较多的时候,时延有所减少。这是由于 WOLSR 减少了网络中的拥塞,降低了平均端到端时延。

(下转第 1079 页)

而图 3(b)显示的是选择最近邻居的择优策略和随机选取邻居的随机策略之间的比较,可以看出随机策略在仿真时间内很好的保证了全网连通,这是因为随机策略不受网络的局域特征的影响。

仿真结果显示,增大 k 值和使用随机策略有助于保持连通性。但是随机策略没有择优能力,实际意义不大,而 k 值也必须限制在一定范围内。k 值大小一方面受节点存储容量限制,更重要的是 Gossip 协议是一种类洪泛的传输机制,太大的 k 值会造成转发的数据包以几何级数增加,导致网络拥塞。

3.2　进一步的分析

综合以上理论分析和仿真结果,在采用随机自组织策略的情况下,使用类 Gossip 机制的自组织行为能以很大的概率保持演化中网络的连通性,而考虑了实际网络的局域特征和节点选择时的非随机行为后,网络的分区几乎无法避免。虽然很多复杂的自组织协议并不仅仅以最短的连接作为选择邻居的唯一标准[3],并且同时引入了确定性选择和随机性选择。但是由于网络的局域特征,同一区域的网络节点在很多性质上都存在一定的共性,而自组织逻辑网络的演化本身又以优化逻辑网络连接为目的,这种择优策略的存在,并不能在自组织模式下完全保证网络的连通性。

产生分区的主要原因,就是网络中区域间的某些关键性的长连接被短连接替换掉了。但是由于自组织网络没有中心控制节点,不能全局掌控整个网络中的所有信息,而那种关键连接只有作为整个网络考虑时,才能够体现出它的重要性。因此无法确定地衡量连接在整个网络中的重要性,导致了可能出现的分区行为。使用类 Gossip 机制进行拓扑维护和信息传递的 Gnutella[4] 对等网络系统的早期版本中,存在较严重的断链和分区现象,除其控制协议的不足外,类 Gossip 机制的自组织演化行为本身对网络的连通性也会产生一定的破坏。

4　结语

本文分析认为由于真实网络的局域特征和网络节点邻居的优化选择,使得自组织逻辑网络的演化过程中对于网络连通性的保障极大的下降了。而且网络的自组织是一个周期性、长期性的行为,出现网络分区的概率在反复的操作下会被放大。一旦网络中出现了逻辑分区,网络中信息的传递只能限于局部进行,在没有外在因素介入的前提下,网络连通性无法恢复,只能维持被割裂的状况。因此这种分区行为的危害很大。对于这种无中心的自组织逻辑网络,有必要以一定的手段保证演化过程中网络的连通性。

致谢　在此,我们向为本文给予无私帮助的老师和同事表示感谢。

参考文献:

[1] EUGSTER P, GUERRAOUI R, KERMARREC AM, *et al*. Epidemic information dissemination in distributed systems[J]. IEEE Computer, 2004,24:60 - 67.

[2] CHEN G, FAN ZP, LI X. Modelling the complex Internet topology [M]. Complex Dynamics in Communication Network, Springer Verlag, 2005, 213 - 235.

[3] JELASITY M, BABAOGLU O. T-Man: Gossip-based overlay topology management[A]. Proceedings of Engineering Self-Organising Applications (ESOA'05)[C]. 2005.

[4] LUA EK, CROWCROFT J, PIAS M, *et al*. A Survey and Comparison of Peer-to-Peer Overlay Network Schemes[M]. In IEEE Communications Survey and Tutorial, 2004.

(上接第 1063 页)

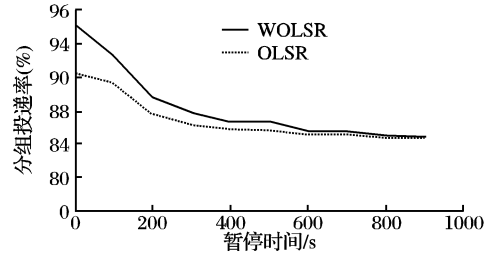

图 2　OLSR 和 WOLSR 下不同的分组投递率

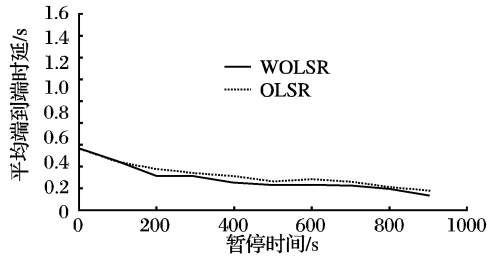

图 3　OLSR 和 WOLSR 下不同的路由延时

5　结语

随着移动 Ad Hoc 网络研究的深入,路由安全越来越受到重视。针对移动 Ad Hoc 网络 OLSR 路由协议中的蠕虫路径,提出确立相邻节点关系,通过节点身份的有效验证,保障了邻居节点发现过程的安全性,使用蠕虫检测方法防御蠕虫攻击,实现路由协议中的蠕虫防御,保证了网络中节点间的可靠通信。

网络蠕虫防御的研究是目前网络安全的热点,只有在足够短的时间内检测到蠕虫,才可能有效地防御蠕虫的攻击和蔓延。

威胁路由安全的漏洞有多种,虫洞只是其中之一,如何有效地防御蠕虫攻击和来自其他方面的安全威胁,还有许多工作要做,努力找到更好的办法,更有效地遏制网络蠕虫的传播。

参考文献:

[1] CLAUSEN T, JACQUET P. Optimized Link State Routing Protocol (OLSR). IETF Internet Draft. RFC 3626[S]. 2003.

[2] 郭 晔,朱淼良. 面向 Agent 的网络蠕虫防御系统研究[J]. 计算机应用,2006,26(12):2931 - 2934.

[3] 王华,柴乔林,杜胜永. 无线传感器网络中数据可靠传输的节能路由算法[J]. 计算机应用,2006,23(1):25 - 27.

[4] PAPADIMITRATOS P, HAAS ZJ. Secure Routing for Mobile Ad Hoc Networks[A]. Proceeding SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)[C]. 2002.

[5] HU YC, PERRIG A, JOHNSON DB. A SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks[A]. WMCSA[C]. 2002. 3 - 13.

[6] YI S, NALDURG P, KRAVETS R. A Security Aware Routing Protocol for Wireless Ad Hoc Networks[A]. The 6th World Multi-conference on Systemics, Cybernetics and Informatics (SCI 2002)[C]. 2002.