

基于信誉机制的多径源路由协议研究

梁克会¹ 许建真¹

摘要

为了提高无线 Mesh 网中多径源路由协议(MSR)的路由安全,在原协议基础上引入了信誉机制,在每个节点上维护 1 个信誉表.源节点在路由建立前对节点信誉度的进行验证,当节点的信誉度值低于限定值时,就孤立该转发节点.以此建立多个安全的路由路径,提高 WMN 中路由的安全.仿真结果表明:在包含恶意节点的 WMN 中,改进后的路由协议有较好分组投递率和较低的端到端时延.

关键词

无线 Mesh 网;多径源路由;路由安全;信誉机制

中图分类号 TP393

文献标志码 A

0 引言

Introduction

无线 Mesh 网^[1-2] (Wireless Mesh Network, WMN) 是 1 种高容量、高速率的分布式网络,它适合于区域环境覆盖和宽带高速无线接入场合.目前对 WMN 路由协议的研究主要关注的是其性能,很少关注路由协议的安全问题.在 WMN 中,网络内部节点可以通过攻击路由协议来误导路由,从而导致网络的崩溃.因此,随着 WMN 应用日益广泛,针对 WMN 路由协议的安全研究也显得越来越重要了.

在 WMN 中,根据 1 个路由请求所发现的路径的数量,路由协议可分为多路径路由^[3-5]和单路径路由,其中多路径又分为备份多路径路由和并行多路径路由.并行多路径路由使用 2 条及 2 条以上的路径同时传输数据,为 WMN 提供更高的带宽和可靠性,因此有着巨大的研究和实用价值.

WMN 中典型的多路径路由协议主要是在单路径路由协议 AODV^[6]和 DSR^[7-8]的基础上扩展而来的.其中 MSR^[9-10] (Multi-path Source Routing) 是基于 DSR 路由协议的 1 种并行多路径路由协议.在研究 MSR 的基础上,本文提出了 1 种基于信誉模型的多路径路由协议 MSRMM (Multi-path Source Routing Based on Reputation Mechanism),通过维护节点信誉度表,在源节点和目的节点间建立多条可信的路由路径,以此提高 WMN 的路由安全.

1 MSR 协议及分析

MSR protocol and analysis

MSR 是在 DSR 的基础上,利用 WMN 中源节点到目的节点可能存在多条路径的条件,以延迟作为路径规格的度量,通过主动探测 (Probing) 的方式感知路径状态,采用带权重的循环调度算法把数据流量分配到多条相对独立的路径上.

该协议是基于协作及依赖“相信邻居节点”的前提,这在实际应用中是不现实的.由于缺少信誉验证机制,路由建立过程中可能将恶意节点加入到路由中来,恶意节点会通过插入错误的路由更新、重放或修改路由信息、插入错误的路由宣传信息来破坏网络.如图 1 所示,

收稿日期 2009-07-05

作者简介

梁克会,男,硕士生,主要研究方向是计算机通信与网间互连技术. liangkh@njupt.edu.cn

节点 A 和 B 之间通过独立路径算法建立了 3 条路由路径,其中中间 1 条路由经过了恶意节点 C,节点 C 广播恶意路由将大量占用网络资源,从而导致数据传输失效.在 MSR 中,由于缺乏相应机制,导致无法孤立恶意节点,因此造成在 WMN 中路由不安全问题已经越来越突出.

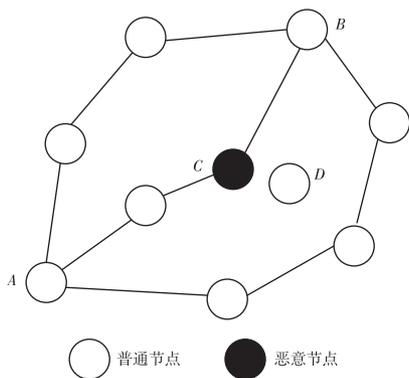


图 1 孤立恶意节点前

Fig. 1 Before isolating the hostile node

2 MSRRM 协议

MSRRM protocol

为了解决 WMN 中 MSR 路由协议不安全的问题,本文提出的 MSRRM 协议在 MSR 中引入了节点信誉机制,通过信誉机制孤立恶意节点,在源节点和目的节点间建立若干条安全的路由路径,以此提高路由的安全.如图 2 所示,在 MSRRM 协议中,通过信誉机制孤立信誉值低的节点 C,而选择了节点 D 作为路由中的转发节点,以此提高 WMN 的安全性和可靠性. MSRRM 协议主要包括 2 个部分:信誉管理部分以及路由发现和维护部分.

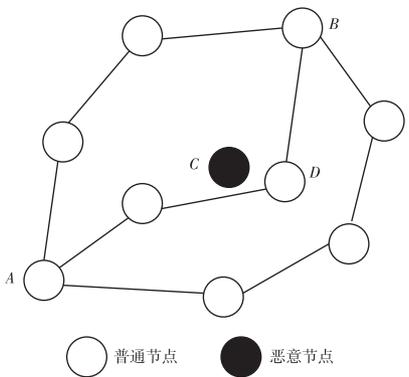


图 2 孤立恶意节点后

Fig. 2 After isolating the hostile node

2.1 信誉管理

信誉机制^[11-12]主要用以抵制系统内部节点的攻击.该机制分为 2 个模块:信息收集模块和信誉评价模块.信息收集模块负责收集其它节点在数据传输和检测过程中的一系列行为,然后由信誉评价模块进行量化分析,同时和其它节点的信誉系统进行交互,最后得到 1 个信誉表,在路由建立时用以指导节点的具体路由行为.周期性的信誉广播将节点的信誉报告附加在 HELLO 报文中,发送到邻节点.

在本机制中,1 个节点对其它节点的信誉值由 2 部分组成,即本节点通过对其它节点进行观察得到的主观信誉值和其它节点向本节点报告的间接信誉值.系统中确定了 5 个常量 T_{max} 、 T_{min} 、 T_{lim} 、 T_0 、 ΔT ,分别表示信誉等级最大值、最小值、最低门限值、初始值和变化门限值.当任 1 节点 i 对任 1 其它节点 j 的信誉值 $T_{i,j} \geq T_{lim}$ ($i \neq j$) 时,节点 i 认为节点 j 为可信节点;否则,认为节点 j 不可信.引入常量 T_{max} 是为了防止节点信誉值不断增大后进行恶意行为而不被孤立.引入常量 T_{min} 是为了防止将节点永久排除在路由之外.当 1 个节点的信誉值低于 T_{lim} 时,会被其它节点孤立,对于被孤立的节点,由于不再有数据交换过程,其它节点通过该节点的 HELLO 报文确认它的存在,每经过 1 个周期,将其信誉值加上 μ ,直至该值等于 T_{lim} 为止, μ 值的大小直接影响 1 个被孤立节点复活的时间间隔. T_0 为初始信誉值,一般大于或等于 T_{lim} . ΔT 是当 1 个节点对其它节点的信誉值的变化量超过该值时,产生 1 个触发,广播该事件,以使其它节点对该信誉值的变化作出及时反应.信誉的评价方法包括直接信誉值的计算和间接信誉报告的处理.每个节点都维护 1 个信誉值列表,反映本节点对其它节点的信誉度评价.信誉值列表中的记录由 1 个 4 元组 $\langle ID, T^d, T^c, T \rangle$ 确定. ID 为节点编号; T^d 为直接信誉值; T^c 为间接信誉值.记 $T_{i,j}$ 为节点 i 对节点 j 的信誉度评价,则

$$T_{i,j} = \delta T_{i,j}^d + (1 - \delta) T_{i,j}^c, \quad (1)$$

其中: $T_{i,j}^d$ 为节点 i 对节点 j 的直接信誉值; $T_{i,j}^c$ 为节点 i 对节点 j 的间接信誉值; $\delta \in [0, 1]$, 代表节点对直接信誉值和间接信誉值的采信程度.

当 1 个节点从另 1 节点接收到若干个数据报文后,对该节点的 T^d 值进行 1 次更新,叫做 1 个 T^d 更新周期.记第 m 个 T^d 更新周期有关某节点发生错误

次数为 f_m , 正确的次数为 s_m , 则在统计过程中, 该节点第 $m+1$ 个 T^d 更新周期的 s 和 f 的初值 s_{m+1}^0, f_{m+1}^0 按下式求得, 并从此初值开始计数.

$$s_{m+1}^0 = \left(\frac{\lambda_1 s_m + \lambda_2 s_{m-1} + \lambda_3 s_{m-2}}{3} \right) \left(\frac{s_m}{s_m + f_m} \right), \quad (2)$$

$$f_{m+1}^0 = \left(\frac{\lambda_1 f_m + \lambda_2 f_{m-1} + \lambda_3 f_{m-2}}{3} \right) \left(\frac{f_m}{s_m + f_m} \right). \quad (3)$$

其中 $\lambda_1, \lambda_2, \lambda_3$ 分别为前 3 个 T^d 更新周期的 s 和 f 值的权重, 反映了对历史统计数据的采信程度. 一般取 $\lambda_1 > \lambda_2 > \lambda_3$, 且 $\lambda_1 + \lambda_2 + \lambda_3 = 3$. 记第 m 个 T^d 更新周期所得到统计经验信誉值为 $T^{d,m}$, 则

$$T^{d,m} = \frac{s_{m+1}}{s_m + f_m + 2}, \quad (4)$$

依此计算第 m 个 T^d 更新周期的统计经验信誉值的增量 $\Delta T^d = T^{d,m} - T^{d,m-1}$, 然后通过 $T^d = T^d + \Delta T^d$ 对 T^d 进行更新.

当节点收到其它节点送达的信誉信息报文后, 查看本节点对该节点的信誉度, 若该节点为可信节点, 则根据该信誉报告更新 T^c , 否则不予处理. 设节点 i 收到节点 j 对节点 k 的信誉报告, 节点 i 对节点 j 的信誉等级大于可信门限值, 则更新节点 k 的 T^c 值, 计算方法为

$$T_{i,k}^c = T_{i,k}^c + (T_{j,k} - T_{i,k}^c) T_{i,j}. \quad (5)$$

2.2 路由发现和维护

MSRRM 协议的路由发现和维护过程与 MSR 类似, 下面将详细介绍这 2 个过程.

1) 路由发现. 当源节点要向目的节点发送信息时, 先检查自己的路由缓冲器, 如果有到达目的节点的路径, 就开始发送信息; 若无, 源节点首先查看本地信誉表, 然后向信誉值大于 T_{lim} 的节点发送 1 个路由请求分组 RREQ 发起路由发现过程. 接收到路由请求分组的中间节点, 检查它是否有到达目的节点的路径, 若有, 就沿反向路径发送路由回复分组 RREP; 若无, 就将该节点添加到路由信息表中, 查看本地信誉表后, 继续广播路由请求分组. 当 RREQ 分组到达目的节点, 目的节点返回路由回复分组 RREP. 源节点收到 RREP 后, 开始传送信息.

2) 路由维护过程. MSRRM 协议的路由维护通过路由错误分组 (RouteError, RERR) 和主动探测来实现. 具体的路由维护包含以下内容:

a 在通信时, 一旦中间节点发现需要使用的邻

接链路断开, 就会发送 RERR 分组给源节点. 源节点收到 RERR 分组后将失效路由从路由表中删除.

b 源节点通过主动探测检测路由状态, 如果在探测过程中发生链路中断, 源节点会收到来自中间节点的 RERR 分组, 并删除路由表中的失效路由.

c 当源节点的路由表中仅剩余 1 条路由时, 若主动探测获取的 RTT 值低于门限值, 表明路由状态良好, 源节点会继续使用该路由. 反之则表明这条路由可能将要断路, 于是重新启动路由发现过程, 以防止通信中断.

3 性能仿真与评估

Performance simulation and evaluation

衡量 WMN 路由协议性能的指标通常是分组平均投递率, 端到端平均时延和路由开销. 各参数简单介绍如下: 1) 分组平均投递率为所有接收端成功接收的分组总数与发送端发送的分组总数之比. 分组平均投递率越大, 网络性能越好. 2) 端到端平均时延包括路由查找时延、数据包在接口队列中的等待时延、传输时延及 MAC 层的重传时延. 3) 路由开销指仿真中传输的所有路由包的数目.

在 Ubuntu8.04 下搭建 1 个 NS2 (版本为 2.33) 仿真平台进行仿真, 仿真场景定义如下: 300 个节点; 随机分布在 $1\ 200\ \text{m} \times 1\ 200\ \text{m}$ 的区域内; 仿真中移动模型采用 PWP, 数据流为随机产生的 20 个 CBR 流; 流速率 $1\ \text{包} \cdot \text{s}^{-1}$; 每个分组长度 512 bits. 实验中本文采用 TwoRayGround 无线传播模型, 914 MHz 载频, $2\ \text{Mbit} \cdot \text{s}^{-1}$ 带宽, 节点通信半径 300 m. 节点的移动速度 $5\ \text{m} \cdot \text{s}^{-1}$, 节点到达指定位置后停留 5 s, 模拟时间 600 s. 在仿真过程中, 通过逐步增加恶意节点的数量来比较 MSR 和 MSRRM 协议的性能.

通过对分组平均投递率进行比较 (图 3) 发现, 当网络中恶意节点的个数为 0 时, MSR 和 MSRRM 均有较高的分组平均投递率, 约为 0.95; 当网络中恶意节点数目以公差为 10 的等差数列增加后, 使用 MSR 路由协议的网络的分组平均投递率急剧下降; 当网络中恶意节点数目为 100 时, 分组平均投递率约为 0.2, 这是由于 MSR 路由协议中缺乏相应的恶意节点孤立机制, 导致分组投递率下降. 而在使用 MSRRM 路由协议的网路中恶意节点为 100 个时候,

分组投递率仍然保持在 0.88 左右. 这说明使用信誉机制的 MSRRM 协议可以很好的孤立信誉度低的节点, 提高分组平均投递率.

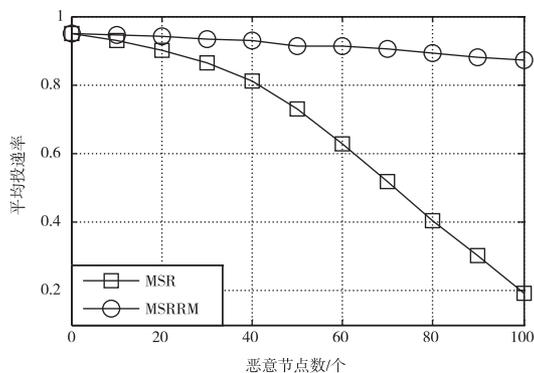


图3 在平均分组投递率上的比较

Fig. 3 The comparison of average packet delivery fractions

MSR 和 MSRRM 端到端时延与恶意节点数目关系如图 4 所示. 在恶意节点数目为 0 时, MSR 和 MSRRM 均有较低的时延. 随着节点数目的增加, MSR 端到端时延急剧增加. 当恶意节点数目为 100 时, MSR 端到端时延达到 60 ms, 而 MSRRM 协议端到端时延为 30 ms. 因此 MSRRM 协议在恶意节点数目较多的情况下要优于 MSR 协议.

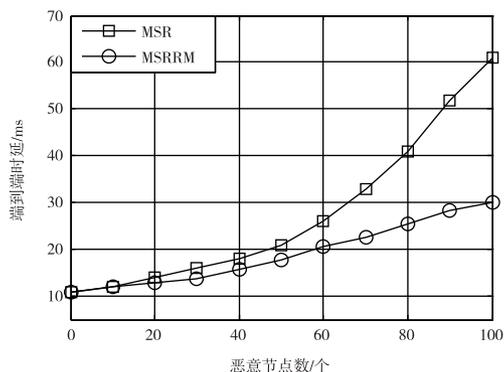


图4 端到端延迟上的比较

Fig. 4 The comparison of end to end delays

MSR 和 MSRRM 2 种路由协议的路由开销与恶意节点数目关系如图 5 所示. 由于 MSRRM 中增加了信誉机制, 信誉信息周期性和触发式的更新导致控制开销增大, 且随着网络中恶意节点增多, 控制开销增大速度比 MSR 协议要快.

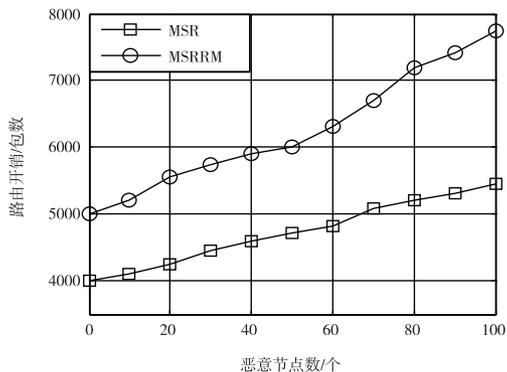


图5 在控制开销上的比较

Fig. 5 The comparison of overhead control

4 结论

Conclusion

为了增加无线 Mesh 网中多路源路由协议 (MSR) 的安全, 本文在 MSR 的基础上引入了信誉机制. 在改进后的路由协议 (MSRRM) 中, 源节点在发起路由建立过程前, 通过验证其它节点的信誉度值, 决定该节点是否可以加入到路由路径中来, 以此孤立恶意节点, 提高 WMN 中路由安全. 仿真结果表明, 在含有恶意节点的 WMN 中, MSRRM 比 MSR 有较好的平均分组投递率和端到端延迟, 当恶意节点个数增多时, MSRRM 仍能够保持较好的性能. 但是, 该方案要周期性的发送信誉信息, 因此增加了路由负载和控制开销. 在增加路由安全的情况下, 该协议在效率方面难免有所下降. 下一步研究重点可以通过限制 MSRRM 路由协议中路径的数量来降低路由负载和控制开销, 以达到在提高路由安全的目标下, 使路由仍然保持有较高的效率.

参考文献

References

- [1] Steve G, Marius P. Securing wireless mesh networks [J]. IEEE Wireless Communications, 2006, 13(2): 50-55
- [2] Bruno R, Conti M, Gregori E. Mesh networks: commodity multi-hop ad hoc networks [J]. IEEE Communications Magazine, 2005, 43(3): 123-131
- [3] Vaidya B, Pyun JaeYong, Park JongAn, et al. Secure multipath routing scheme for mobile ad hoc networks [C]. DASC, 2007: 87-99
- [4] Yang P, Huang B. Multi-path routing protocol for mobile ad hoc network [C]. CSSE, 2008: 1024-1027
- [5] Narula P, Dhurandher S K, Misra S, et al. Security in mobile ad-hoc networks using soft encryption and trust-based multi-path rou-

- ting[J]. Computer Communications, 2008, 31(4): 760-769
- [6] Lee SungJu, Belding R, Elizabeth M, et al. Scalability study of the ad hoc on-demand distance vector routing protocol [J]. International Journal of Network Management, 2003, 13(2): 97-114
- [7] 张勇, 郭达. 无线网状网原理与技术[M]. 北京: 电子工业出版社, 2007
ZHANG Yong, GUO Da. Principle and technology of wireless mesh network[M]. Beijing: Press of Electronics Industry, 2007
- [8] 张彦, 罗济军, 胡宏林. 无线网状网: 架构、协议与标准[M]. 北京: 电子工业出版社, 2008
ZHANG Yan, LUO Jijun, HU Honglin. Wireless mesh networking: architectures, protocols and standards[M]. Beijing: Press of Electronics Industry, 2008
- [9] WANG L, SHU Y, DONG M, et al. Adaptive multipath source routing in ad hoc networks [C]. International Conference on Communications ICC, 2001: 866-871
- [10] ZHANG Lifang, ZHAO Zenghua, SHU Yantai, et al. Load balancing of multipath source routing in ad hoc networks [C]. ICC, 2002: 3197-3201
- [11] Buttyan L, Hubaux J P. Stimulating cooperation in self-organizing mobile ad hoc networks [J]. Mobile Network and Applications, 2003, 8(5): 579-592
- [12] Cho Jinhyung, Kwon Kwiseok, Park Yongtae. Q-rater: A collaborative reputation system based on source credibility theory [J]. Expert Systems with Application, 2009, 36(2): 3751-3760

Study of multipath source routing protocol based on reputation mechanism

LIANG Kehui¹ XU Jianzhen¹

¹ College of Computer, Nanjing University of Posts & Telecommunications, Nanjing 210003

Abstract To enhance the routing security of MSR (Multipath Source Routing) in WMN, this paper introduces the reputation mechanism which maintains a reputation table at each node in MSR system. Before setting up the routing, the source node will verify the reputation degree of each node. If a node's reputation degree is lower than the limited value, it will be isolated. As a result, several safe routing paths are established between the source and destination nodes. Thus the routing security in WMN is improved. Simulation results show that the improved routing protocol has a better packet delivery fraction and lower end-to-end delay in WMN that contains hostile nodes.

Key words wireless mesh network; multipath source routing; routing security; reputation mechanism