Ad Hoc网络中基于信任机制的安全ZRP协议分析

姚放吾[1,2],任娟娟[1]
(1.南京邮电大学 计算机学院,江苏 南京 210003;
2.南京邮电大学 计算机技术研究所,江苏 南京 210003)

摘 要:移动Ad Hoc网络是一种无中心、自组织的多跳网络。由于其移动性、不可靠的传递介质、缺少基础设施以及生存环境的恶劣,使得安全性问题成为Ad Hoc网络展开应用的巨大障碍。文中基于ZRP协议提出一种使用信任机制的安全路由协议。该协议在每个节点上加入信任模块,以供选择信任度高的安全路由。通过NS仿真软件对该安全路由协议进行分析,给出了仿真结果。

关键词:移动Ad Hoc网络;信任值;安全路由;邻居检测
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)06-0160-03

Analysis of Secure ZRP Protocol Based on Trust Integrated Architecture in Ad Hoc Network

YAO Fang-wu[1,2], REN Juan-juan[1]
(1. College of Computer, Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. Institute of Computer Technology, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Mobile Ad Hoc networks are multi-hop networks which are acentric and self-organized. Their mobility, the unreliable wireless media, lacking of basic equipments, and the odious living environment make Ad Hoc networks difficult to be applied. Based on the basic Ad Hoc network protocol ZRP, proposed a secure Ad Hoc network protocol using the trust integrated cooperation architecture. In this protocol, reliable modules are added to all the nodes for selecting high reliable routes. Simulation results are given after by evaluating the secure protocol with NS.

Key words: mobile Ad Hoc network; trust value; secure route; neighbor monitoring

0 引 言

移动Ad Hoc网络是一种无中心、自组织的多跳网络,没有基础设施,能够适合于战场、医疗、自然灾害等比较恶劣的环境中。但是由于其自身的特点,安全问题成为阻止其广泛应用的障碍。路由安全是其中最主要的部分[1]。目前,移动Ad Hoc网络路由协议主要有表驱动和按需驱动路由协议两种。表驱动路由协议每个节点都维护一张到网络中其他节点的路由表,消耗有限的网络资源;按需驱动路由协议能够有效使用网络带宽,但是会增加延时。ZRP协议是一种具有表驱动和按需驱动两种路由协议优点的分级式路由协议,所以,文中以它为基本协议进行研究[2]。

收稿日期:2008-09-10;**修回日期**:2008-12-29
基金项目:国家高技术研究发展计划(863计划)(2006AA01Z208)
作者简介:姚放吾(1953-),男,教授,研究方向为计算机在通信中的应用、并行计算及其体系结构和嵌入式技术。

1 ZRP协议

1.1 ZRP协议区域划分

ZRP协议中将整个网络划分成以各个节点为中心,以一定跳数为半径的区域。各个区域之间重复度很高[3]。图1为以A为中心,跳数为2的路由区域;节点M和K在区域外,其余节点在区域内。

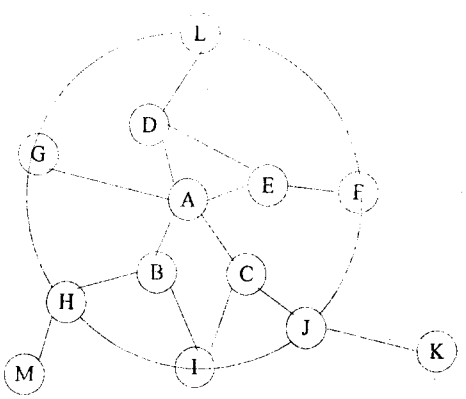


图1 ZRP协议中节点分类情况

1.2 ZRP 协议结构

ZRP 由三个部分组成：IARP，IERP 和 BRP。ZRP 区域内部执行主动路由选择部分称为域内路由协议(IARP)；区域外部执行按需路由协议称为域间路由协议(IERP)。IERP 和 IARP 并没有指定具体的路由协议。ZRP 协议的体系结构如图 2 所示[3]。

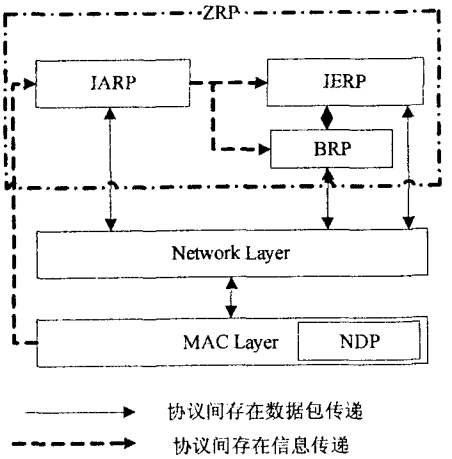


图 2　ZRP 协议体系结构

2　基于节点信任值 ZRP 策略

其路由策略是：在执行主动路由协议的范围内，每个节点都监测邻居节点的行为，同时计算该邻居节点的信任值，以备在路由选择时使用，在路由建立过程中考虑信任值、跳数、带宽等情况下选择路由。每个节点上运行的监测机制具有类似于 IDS 的功能，能够检测出异常和常见的攻击，并对这些攻击做出反应：把异常节点的信任值降低或者把攻击节点加入黑名单；把异常节点的情况发送给与异常节点相关的各节点或者和它们一起做联合检测，把异常节点驱逐出网络[4]。

2.1 信任值管理模块和邻居检测模块

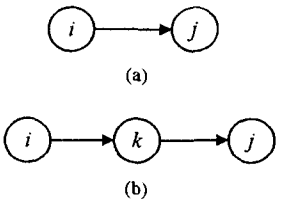
在 IARP 使用的具体路由协议中增加一个邻居信任值评估模块，该模块根据与其交互的邻居的具体情况，计算出邻居节点的信任值，为 IARP 和 IERP 做路由选择时提供所需要的参考信息。邻居监测模块用来监视邻居节点的行为和自身运行的状态。信任值管理模块和邻居监测模块互相提供支持。

2.2 信任值的计算和维护

信任节点之间的信任关系如图 3 所示，分为直接信任关系和推荐信任关系。对应地，节点信任值也分为直接信任值和推荐信任值。

2.2.1 直接信任值的计算

当邻居发现协议(NDP)发现新的节点加入时，可以通过参照与该新加入节点存在直接信任关系的节点对该节点的信任值，为新加入节点赋予一个初始的信任值，以后通过该新加入节点的行为更新对其的直接信任值。



(a)　直接信任　(b) 推荐信任

图 3　节点信任关系示意图

直接信任值的计算公式：

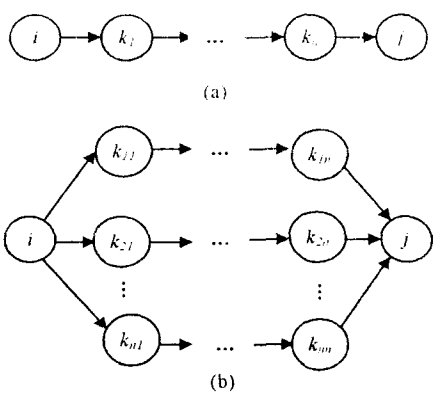
$$\begin{cases} DT_{i-j}(t_{a+1}) = \min\{1, [DT_{i-j}(t_a) + \mathrm{eval(action)}]\} \\ \quad \text{action 为良性行为} \\ DT_{i-j}(t_{a+1}) = \max\{-1, [DT_{i-j}(t_a) + \mathrm{eval(action)}]\} \\ \quad \text{action 为异常行为} \end{cases}$$

上面公式中，$DT_{i-j}(t_a)$ 来表示在时间 t_a 节点 i 对节点 j 的直接信任值，eval(action) 来表示对一个行为通过评估以后得出的值，如果一个行为是良性的则评估值为介于[0，+1] 之间的小数，如果该行为为恶性的则评估值介于[−1,0]之间。文中信任值取值范围为[−1，+1] 之间的任意值，取值越大，表示信任度越高[5]。

2.2.2 推荐信任值的计算

推荐信任值是评估主体根据推荐者的可信程度对推荐者所提供的客体信任值进行处理，最终给出对客体的信任评估。

如图 4，节点间的推荐路径分为单一推荐路径和并行推荐路径两种。文中用 $RT_{i-j}(t_a)$ 来表示在 t_a 时刻节点 i 对节点 j 的推荐信任值，其中 i 为评估主体，j 为评估客体。



(a) 单一推荐路径　(b) 并行推荐路径

图 4　节点间的推荐路径

对于单一推荐路径，如图 4(a) 所示，在 t_a 时刻节点 i 对节点 j 的推荐信任值为 $RT_{i\sim k1k2\cdots kn-j}(t_a)$。其计算公式如式(1) 所示。

$$RT_{i-j}(t_a) = DT_{i-k_1}(t_a) \times DT_{k_1-k_2}(t_a) \times \cdots \times DT_{k_n-j}(t_a) \quad (1)$$

对于 n 条并行推荐路径，如图 4(b) 所示，在 t_a 时刻节点 i 对节点 j 的推荐信任值计算公式如式(2) 所示。

$$RT_{i-j}(t_a) = \frac{1}{n}\sum_{k=1}^{n} RT^k(t_a) \quad (2)$$

2.2.3 信任值的初始化与维护

为了方便初始化节点信任值以及如何确定是否发起推荐信任值获取过程，引入两个参数：ET 和 CRIT_VAL。ET 是一个介于[-1,1]之间的实数，表示节点对周围环境的信任值。CRIT_VAL 表示需要发起推荐信任值获取过程的临界值。

Ad Hoc 网络在初始化时，网络遭受攻击的可能性最低，把每一个节点对邻居节点的信任值都设为最大值 1。这时，ET 值为 1，代表本节点对所有邻居节点都信任。随着网络运行，本节点对邻居节点的直接信任值会发生变化，把本节点对所有邻居的信任值的平均值赋给 ET。

区域内路由协议 IARP 保存有以本节点为中心到区域内其它节点的路由信息和本区域内的链路状态信息，根据这些资源可以得到本节点可以利用哪些节点来获取新邻居 X 节点的推荐信任值。如果没有节点可以利用，则把 ET 的值作为对该新节点 X 的信任值，也就是把本节点对周围环境的总体认识，默认为对该新节点的信任值。

为了记录邻居节点的信任值，每个节点维护一张 Neighbor List 表，记录邻居节点的 ID 和对该邻居节点的信任值，该节点是否可信，即其信任值是否能作为路由的下一跳节点。

2.3 邻居检测模块

邻居检测模块与信任管理模块相互支持。邻居检测模块主要功能为检测常见异常，评估节点行为，为信任管理模块服务；并利用节点信任值进行联合检测，避免节点协作中的相互诽谤。

3 仿真实验及结果分析

实际情况下，改进后的 ZRP 协议(为了方便描述，将其称为 TZRP)和原有的 ZRP 协议的性能和安全性需要通过仿真来比较。选择 NS2 对以上协议进行仿真，使用 Linux 操作系统。仿真面积为 800m×800m，节点数为 100，初始位置随机，最大移动速度 0.1m/s。

实验验证以下两方面特性：

(1)包传输率：成功接收到的数据包总数与发送端产生的数据包总数的比率。包传输率越高，网络安全性越高。

(2)平均端到端时延：源节点发送路由申请到目的节点回答路由响应这个过程的平均时间。

从仿真结果图 5 看出，当恶意节点增加时，TZRP 协议的包传输率明显高于 ZRP 协议的包传输率，因此在相同情况下 TZRP 协议的丢包数更少，可靠性更高。但是 TZRP 协议将节点信任值、跳数以及带宽等因素综合考虑得出一条相对安全的路由进行数据传输，因此不能保证所选路由是最短的，正如图 6 所示，TZRP 协议端到端时延会比原 ZRP 协议端到端时延略微增加。而这种微小牺牲在需要高安全性的实际应用中是值得的。

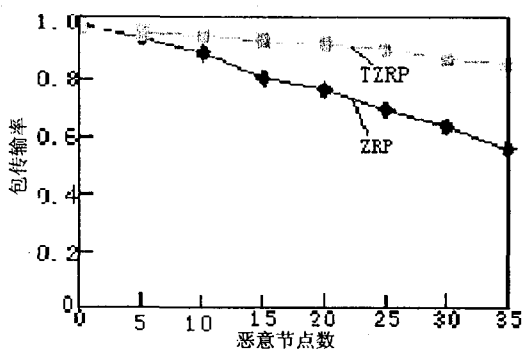


图 5 包传输率比较

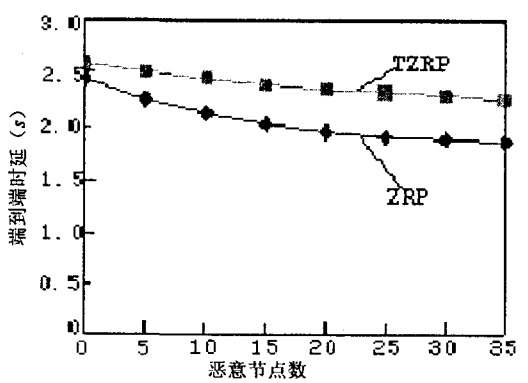


图 6 平均端到端时延比较

4 结束语

文中将节点信任机制应用于 ZRP 协议，并进行了仿真分析。通过分析和比较，可知这种新协议在满足安全性要求上更有优势，能够抵御大多数攻击，具有可行性。由于协议中采用了一些安全措施，导致新协议在时间效率上略低，因此适用于对时间性能要求不高，更加注重高安全性的实际应用中[6]。

文中介绍的新协议能够有效对抗网络中的主动攻击，但是窃听等被动攻击并没有被考虑在攻击范围之内，这也是以后研究的主要方向。

(下转第 167 页)

[12] Abu - Ghazaleh N, Lewis M J. Differential deserialization for optimized SOAP performance[C]//proceedings of the ACM/IEEE conference on Supercomputing. Seattle WA: [s. n.], 2005:21 - 31.

[13] Suzumura T, Takase T, Tatsubori M. Optimizing Web services performance by differential deserialization[C]//proceedings of the IEEE/ACM International Conference on Web Services. Orlando, USA:[s. n.],2005:185 - 192.

[14] Abu - Ghazaleh N, Lewis M J, Govindaraju M. Performance of dynamically resizing message fields for differential serialization of SOAP messages[C]//proceedings of International Symposium on Web Services and Applications. [s. l.]:[s. n.],2004:783 - 789.

[15] Wei Jun, Hua Lei, Niu Chunlei, et al. High performance SOAP processing driven by data mapping template[C]//proceedings of the DAIS 2006. [s. l.]:[s. n.],2006:152 - 168.

[16] 花　磊,魏　峻,牛春雷,等.动态模板驱动的高性能 SOAP 处理[J].计算机学报,2006,29(7) :1145 - 1156.

[17] Ying Ying, Huang Yan, David W. A performance evaluation of using SOAP with attachments for e - Science[EB/OL]. [2008 - 06 - 01]. http://www. allhands. org. uk/2005/proceedings/papers/422. pdf.

[18] 戴国安,张立臣.压缩 SOAP 改善 XML Web Service 性能的研究[J].福建电脑,2006(9):126 - 127.

[19] Ericsson M. The Effects of XML Compression on SOAP Performance[J]. World Wide Web,2007,10(3):279 - 307.

[20] Alex N, Paul G, Chen Shiping. A study of the impact of compression and binary encoding on SOAP performance[EB/OL]. [2008 - 06 - 20]. http://mercury. it. swin. edu. au/ctg/AWSA05/Papers/ng. pdf.

[21] 吕海华,杨大全,杨希来,等.利用高速缓存技术提高 SOAP 性能[J].微处理机,2004(3):43 - 45.

[22] Kiran D, Daniel A. SOAP optimization via client - side caching [EB/OL]. [2008 - 06 - 20]. http://www. cis. ksu. edu/dan/despot/icws03. pdf.

[23] Kiran D, Daniel A. SOAP optimization via parameterized client - side caching[EB/OL]. [2008 - 06 - 20]. http://www. cis. ksu. edu/dan/despot/392 - 227. pdf.

[24] 陈庆奎,那丽春.采用动态缓冲池的 SOAP 并行通信模型[J].北京邮电大学学报,2008,31(1):40 - 44.

[25] 刘　钊,卢正鼎.大数据量传输下 SOAP 的性能研究[J].华中科技大学学报:自然科学版,2004,32(3):65 - 67.

[26] 刘志都,贾松浩,詹仕华.SOAP 协议安全性的研究与应用[J].计算机工程,2008,34(5):142 - 144.

[27] 陈天煌,李　帆.利用 SOAP 扩展实现 Web 服务中 SOAP 消息的安全[J].武汉理工大学学报:交通科学与工程版,2007,31(3):518 - 520.

[28] 李慧盈,张长海,李德昌.基于 SOAP 协议的 Web Services 安全性扩展实现[J].计算机应用研究,2006(1):106 - 107.

[29] 许晓宁.Web Services 中 SOAP 消息传递的安全性研究[J].微计算机信息,2006,22(11 - 3):115 - 117.

[30] 孟　军,盛　雨,刘洪波.基于.NET 的 SOAP 加密方法研究与实现[J].计算机科学,2005,32(8):52 - 54.

[31] Scott S. Understanding WS - Security[EB/OL]. [2008 - 06 - 20]. http://msdn. microsoft. com/en - us/library/ms977327. aspx.

[32] 石伟鹏,杨小虎.基于 SOAP 协议的 Web Service 安全基础规范(WS - Security)[J].计算机应用研究,2003(2):100 - 102.

[33] 田　捷,熊前兴.基于 SOAP 的消息传递安全性技术研究[J].计算机应用,2003,23(S1):284 - 286.

[34] 王　杨,王朝斌,林　涛,等.SOAP 消息传递机制在计算网格中的安全性[J].计算机工程,2007,33(4):154 - 156.

[35] 王　凡,李　勇,朗宝平,等.基于 WS - Security 构筑安全的 SOAP 消息调用[J].计算机应用,2004,24(4):121 - 123,126.

[36] 汤卫东,周永权.Web 服务消息级安全模型的设计及评价[J].计算机工程与设计,2006,27(10):1873 - 1875.

[37] 赵　军,朱清新.基于 XML 的 SOAP 消息安全引擎模型的研究[J].科技信息:学术版,2007(5):246 - 247.

[38] 刘振鹏,周冬冬,薛林雁.一个基于 SOAP 消息的 Web 服务综合安全模型[J].武汉大学学报:理学版,2006,52(5):570 - 573.

[39] 崔晓玲,李　磊,魏　峻.一种新型 SOAP 消息附件安全保障模型[J].计算机科学,2007,34(4):243 - 249.

[40] 张功萱,宋　斌,王平立.基于 SOAP 的网络消息安全策略[J].南京理工大学学报:自然科学版,2007,31(1):66 - 70.

(上接第 162 页)

参考文献:

[1] 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 - 235.

[2] 朱道飞,汪东艳,刘欣然,等.移动 Ad hoc 网络安全路由协议综述[J].计算机工程与应用,2005,41:116 - 133.

[3] Haas Z J, Pearlman M R, Samar P. The Zone Routing Protocol (ZRP) for Ad Hoc Networks[CP/DK]. 2002. draft - ietf - manet - zone - zrp - 04. txt.

[4] Blaze M, Feigenbaum J, Ioannidis J, et al. The role of trust management in distributed systems security[C]//Secure Internet Programming: Issues for Mobile and Distributed Objects. Berlin: Springer - Verlag, 1999:167 - 173.

[5] Balakrishnan, Venkat, Varadharajan, et al. Trust Integrated Cooperation Architecture for Mobile Ad - hoc Networks[C]//Wireless Communication Systems, 2007. ISWCS 2007. 4th International Symposium. [s. l.]:[s. n.],2007:592 - 596.

[6] 何昆鹏,李腊元.Ad Hoc 网络中按需路由协议的仿真与性能分析[J].计算机技术与发展,2008,18(3):81 - 84.