

链路守卫节点合作监测检测恶意合谋攻击

谭运宝¹, 钟 诚¹, 玉 易^{1,2}, 刘 磊¹

(1 广西大学 计算机与电子信息学院, 广西 南宁 530004; 2 广西广播电影电视局信息中心, 广西 南宁 530022)

摘 要: 针对移动 Ad Hoc 网络环境中合谋节点的恶意丢包行为, 将源节点及其传输链路上各守卫节点所检测的结果结合起来, 设计一种通过守卫节点合作监测来检测发现恶意合谋攻击的方法. NS2 上仿真实验结果表明, 该方法能够有效应对合谋节点的恶意丢包行为, 降低恶意路由出现的概率, 提高网络的分组投递率.

关键词: 移动 Ad Hoc 网络; 合谋节点; 恶意丢包; 守卫节点

中图分类号: TP309; TP393

文献标识码: A

文章编号: 1000-7180(2011)09-0179-04

Detecting Malicious Colluding Attack Using Cooperation Monitoring of Guard Nodes

TAN Yun-bao¹, ZHONG Cheng¹, YU Yi^{1,2}, LIU Lei¹

(1 School of Computer and Electronics and Information, Guangxi University, Nanning 530004, China;

2 Information Center, Guangxi Radio and Films and Television Bureau, Nanning 530022, China)

Abstract: For the packet loss behavior of the malicious node collusion in the mobile Ad hoc network environment, this paper presents a detection method against colluding nodes. This detection method focuses on cooperation monitoring of guard nodes and computes the trust values of transmission link with the monitoring results between source node and related guard nodes, and then applies the link trust values to avoid colluding nodes. The NS2 based simulation results show that the proposed method can effectively reduce the probability of misbehaving routes caused by colluding nodes and improve the packet delivery rate.

Key words: mobile ad hoc network; colluding node; malicious packet dropping; guard node

1 引言

CONFIDANT 和 CORE 以及基于 Nuglet 计数器的节点合作机制的信任评估方法^[1-3]在一定程度上虽然可保证移动自组网中节点自己的数据包被其他节点转发, 提高了节点的合作性, 但是若出现恶意合谋丢包节点, 这些方法将失效.

在动态源路由协议 DSR 基础上, 文献[4]提出一种基于 ACK 的自私丢包检测方式 2ACK. 对于两个节点一起合谋发送错误 ACK 的情形, 2ACK 方法将不能起作用. 文献[5]提出一种恶意合谋节点检测机制, 但是该文的仿真实验只考虑了节点是静止

的情况. 文献[6]给出一种邻居合作监测信任模型 NCM, 它引入守卫节点来加强邻居节点间的合作监测, 将监听节点和无能为力. 其通信链路的守卫节点所监测的结果结合起来, 从而能快速准确地确定节点间的信任关系, 并以此作为路由选择的依据来促进节点间相互合作. 该信任模型以网络中自私节点只存在恶意丢包行为为前提, 对网络中恶意合谋丢包节点攻击的检测无能为力.

文中研究设计了基于守卫节点合作监测检测恶意合谋攻击的方法, 以缓解恶意合谋节点对移动 Ad hoc 网络性能造成的影响.

收稿日期: 2011-01-13; **修回日期:** 2011-01-27

基金项目: 广西自然科学基金项目(2011GXNSFA018152); 广西科学基金项目(桂科基 0575014); 广西大学拔尖创新团队建设计划(211-3-1-45)

2 守卫节点合作监测检测机制

网络节点通信场景如图1所示,其中节点 K 、 L 是通信链路 $M-m$ 的守卫节点,是节点 M 与节点 m 的邻居节点集的交集元素.节点 K 、 L 都能监听到节点 M 、 m 发送数据包的情况.若一个节点能直接监测到一条通信链路的发送节点与接收节点的通信活动,则这个节点称为该通信链路的守卫节点.

文中给出的合谋攻击节点检测机制在于链路守卫节点的合作监测,计算出通信链路的链路信任值,进而判断恶意合谋节点.其中每个节点依然采用NCM信任模型的处理方式得到对其他节点的节点信任值.

守卫节点合作监测检测恶意合谋攻击方法:

(1) 守卫节点计算间接监听转发率和链路信任值.设节点 Y 为链路 $M-m$ 的守卫节点,能监听到链路 $M-m$ 的通信情况.守卫节点 Y 设置计数器 $InSBF_Y(M,m)$ 和 $InABF_Y(M,m)$. $InSBF_Y(M,m)$ 表示在信任更新周期(τ)内,节点 Y 监听到节点 M 发送的数据包总数,这些数据包是节点 M 向节点 m 发送并要求节点 m 转发的. $InABF_Y(M,m)$ 表示在信任更新周期(τ)内,节点 Y 监听到节点 m 已转发的数据包总数,这些数据包来自节点 M .在每个信任更新周期结束后,节点 Y 通过公式(1)计算其所直接监测到的关于链路 $M-m$ 的间接监听转发率 $IDF_Y(M,m)$,并通过公式(2)计算对链路 $M-m$ 的链路信任值 $TL_Y(M,m)$.

$$IDF_Y(M,m) = \frac{InSBF_Y(M,m)}{InABF_Y(M,m)} \quad (1)$$

$$TL_Y(M,m) = \omega TL'_Y(M,m) + (1-\omega) IDF_Y(M,m) \quad (2)$$

其中, ω 为守卫节点对链路信任值的历史权重, $TL'_Y(M,m)$ 为上一周期守卫节点 Y 对链路 $M-m$ 的链路信任值.

(2) 守卫节点判断所监测链路的数据包转发是否异常.记 TH_{IDF} 为节点间接监听的阈值(即链路中两个节点正常转发率的临界值),若 $IDF_Y(M,m) \geq TH_{IDF}$,则守卫节点 Y 可以判定链路 $M-m$ 不存在恶意合谋节点,结束此周期的检测;否则转步骤(3).

(3) 守卫节点判断链路 $M-m$ 是否为合谋丢包链路.分两种情况处理:①当守卫节点 Y 收到由节点 M 发送过来的 REP_REQ 请求包时, Y 判定链路 $M-m$ 不存在恶意合谋节点,但可能存在自私节点,

并且协助节点 M 读取 REP_REQ 请求包,进而计算他们对节点 m 的节点信任值^[6],然后结束此周期的检测判断.②当守卫节点 Y 没有收到由节点 M 发送过来的 REP_REQ 请求包时,若 $TL_Y(M,m) > TH_{link_trust}$ (TH_{link_trust} 为链路是否恶意的链路信任临界值),则结束此周期的检测判断;否则 Y 怀疑链路 $M-m$ 为合谋丢包链路,向源节点汇报,转步骤(4).

(4) 守卫节点选择路由向源节点汇报监测情况.守卫节点 Y 直接查找自己的路由表,选择一条到源节点 S 且不包含 M 、 m 的路径,并向源节点 S 发送 $REP_Colluding$ 数据包($REP_Colluding$ 数据包包含 $TL_Y(M,m)$),报告链路 $M-m$ 为合谋丢包链路.如图1所示,节点 K 、 L 都是链路 $M-m$ 的守卫节点,分别通过路径 $\langle K-I-J-S \rangle$ 与 $\langle L-G-H-S \rangle$ 向源节点 S 发送 $REP_Colluding$ 数据包.如果守卫节点 Y 不能找到一条到源节点 S 的合适的路径,则暂时不发送,同时结束此周期的检测判断.

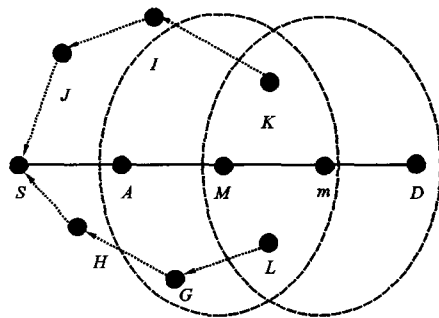


图1 节点通信场景

(5) 源节点汇总信息,判断链路 $M-m$ 的合法性.源节点 S 收到守卫节点 Y 发送的 $REP_Colluding$ 数据包,由于信任值大于等于 TH_{coop} 的节点视为合作节点,源节点 S 只对满足 $RF(S,Y) \geq TH_{coop}$ 的守卫节点 Y 发送过来的 $REP_Colluding$ 数据包进行处理,其余的丢弃.源节点 S 通过公式(3)计算得到对链路 $M-m$ 的链路信任值.

$$TLs(M,m) = \gamma \cdot TLs'(M,m) + (1-\gamma) \sum_{i=1}^n RF(S,N_i) TL_{N_i}(M,m) / \sum_{i=1}^n RF(S,N_i) \quad (3)$$

其中, γ 表示通信过程中源节点 S 对链路信任值的历史权重 TLs' ,表示上一周期源节点 S 对链路 $M-m$ 的信任值. n 表示源节点 S 收到的 $REP_Colluding$ 数据包的守卫节点数, $RF(S,N_i)$ 表示节点 S 对节点 N_i 的信任值. $RFR(M,m)$ 表示节点 M 对节点 m 的间接信任值, $RR(M,N_i)$ 表示节点 M 对节点 N_i 的推荐信任值, $i=1,2,\dots,n$.若 $TLs(M,m) \leq$

TH_{link_trust} , 则源节点可判定节点 M, m 为恶意合谋节点。

(6) 源节点反馈判断链路 $M-m$ 的结果。源节点 S 沿着之前的守卫节点 Y 发送 $REP_Colluding$ 数据包的反路径, 发送 $Confirm_Colluding$ 数据包, 所经过的节点 X (包括守卫节点 Y) 被告知节点 M, m 为恶意合谋节点, 节点 X 通过公式(4) 计算得到对链路 $M-m$ 的链路信任值。

$$TL_X(M, m) = \zeta \cdot TL_X'(M, m) + (1 - \zeta) \cdot TL_S(M, m) \quad (4)$$

其中, ζ 表示源节点 S 返回 $Confirm_Colluding$ 数据包的过程中, 所经过的节点 X 对链路信任值的历史权重, $TL_X'(M, m)$ 表示节点 X 对链路 $M-m$ 的历史信任值。

(7) 源节点选择一条信任值最高的路径进行传送数据包, 其中路径的信任值是指这条路径所经过的所有节点的综合信任值水平, 其值等于路径所有节点的信任值相乘。

合作检测机制中守卫节点能判断所监测链路的数据包转发是否异常, 进而判断所监测链路是否为恶意合谋链路。为减少单个守卫节点监测判断的失误率, 守卫节点合作检测机制将源节点及其传输链路的各守卫节点所监测的结果结合起来, 通过判断链路信任值的大小来判断链路是否为合谋链路, 此时合谋链路的链路信任值的降低必然会把恶意合谋节点排除在通信路由之外, 缓解了合谋节点对网络性能造成的影响。

3 仿真实验

3.1 网络环境及相关参数的设置

实验平台为 Pentium IV CPU 3.0GHz、512MB RAM 的 PC 机, 操作系统 Red Hat Linux 9.0, 网络仿真平台版本采用 NS-2.28。节点移动模型采用随机移动模型, 数据流类型采用 CBR, 分组长度为 512byte, 每秒产生 4 个分组, 节点发送范围为 250 米, 仿真时间默认为 800 秒。运行的过程其他参数设置为: $\tau = 5$ 秒, $\omega = 0.8$, $\gamma = 0.7$, $\zeta = 0.6$, $TH_{coop} = 0.4$, $TH_{IDF} = 0.7$, $TH_{link_trust} = 0.5$ 。

3.2 实验结果与分析

将守卫节点合作检测机制应用到 NCM 的信任模型称为扩展 NCM 信任模型, 记为 E_NCM 模型。在总节点数为 50, 恶意合谋丢包节点对数分别为 2、4、6、8、10 的情况下, 节点停留时间设置为 10 秒, 针对不同的恶意合谋节点对标准 DSR、NCM 和 E_NCM 进行仿真实验, 结果如图 2 所示。

NCM 进行仿真实验, 结果如图 2 所示。

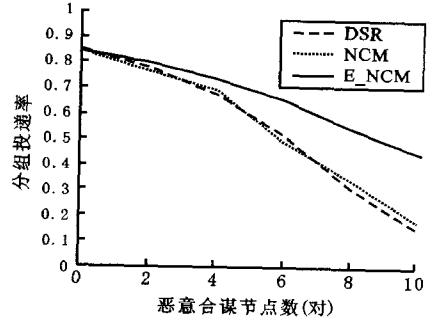


图2 分组投递率与恶意合谋节点数的关系

从图 2 可看出, 随着恶意合谋丢包节点对数目增多, 标准 DSR、NCM 和 E_NCM 的分组投递率都相应减小。在存在恶意合谋节点的环境下, E_NCM 比 DSR 和 NCM 具有更高的分组投递率, NCM 与 DSR 抵御恶意合谋节点的能力是一样的。

(2) 在总节点数为 50, 恶意合谋丢包节点对数为 8 的情况下, 节点停留时间设置为 10 秒, 采用不同的仿真时间分布对标准 DSR、NCM 和 E_NCM 进行实验, 结果如图 3 所示。

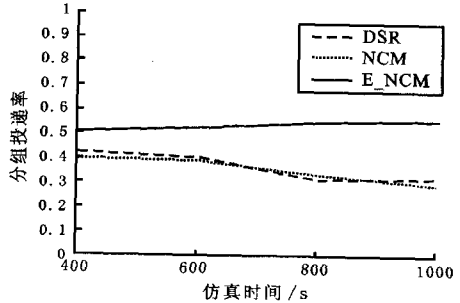


图3 分组投递率与仿真时间的关系

由于 DSR 与 NCM 都没有抵御恶意合谋节点攻击的能力, 而且作为恶意合谋节点的两个节点一直都相互处在可通信范围之内, 随着仿真时间的延长, 恶意合谋节点成为通信路由的中间节点的概率会相应增大。从图 3 可以看出, DSR 与 NCM 的分组投递率也随时间的延长略有下降趋势。而对于 E_NCM, 随着仿真时间的延长, 恶意合谋节点逐渐被排除到通信路由之外, 源节点与目的节点的通信路由趋于合作正常化, 这样对提高整个网络的分组投递率起到了一定的积极作用。

在总节点数为 50, 恶意合谋丢包节点对数目分别为 2、4、6、8、10 的情况下, 节点停留时间设置为 10 秒, 针对不同的恶意合谋节点对标准 DSR 和 E_NCM 进行仿真实验, 结果如图 4 所示。图 4 给出了路由开销与恶意合谋丢包节点对数目之间的关系, 其中“drop rrep”表示在当前环境下, 恶意合谋节点

只向另一个合谋节点转发来自于目的节点返回的 RREP 路由响应包,其余的 RREP 路由响应包均被丢弃。

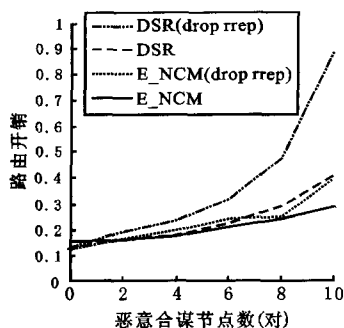


图4 路由开销与恶意合谋节点数的关系

图4的结果表明,随着恶意合谋节点对数目的增加,各种方法的路由开销都相应增大.这是由于随着恶意节点数目比例的增大,恶意路由出现概率必然增加,直接导致目的节点成功接收的数据分组的总和减少,从而致使网络的路由开销相应增大.由于DSR的控制分组类型数目小于E_NCM的控制分组类型数目,在不存在恶意合谋节点的情况下DSR的控制分组小于E_NCM的控制分组,此时E_NCM的路由开销大于DSR的路由开销.但随着恶意合谋节点的引入,目的节点成功接收的数据分组的总和相应减少,由于DSR没有抵御恶意合谋节点攻击的能力,其目的节点接收数据分组总和的减少程度要大于E_NCM相对应的减少程度,这种情况下DSR的路由开销大于E_NCM的路由开销。

4 结束语

通过引入链路信任值,将源节点及其传输链路的各守卫节点所监测的结果结合起来进行检测,能够有效应对合谋节点的恶意丢包行为,降低恶意路由出现的概率,提高网络的分组投递率.文中主要考虑的是数据传输阶段的自私节点丢包问题,如何解决自私节点在路由发现阶段的丢包问题,以及

如何应对多个守卫节点一起恶意合谋诬告其他节点,如何判断守卫节点的反馈信息是否值得依赖,将是下一步研究的问题。

参考文献:

- [1] Buchegger S, Boudec J Y L. Performance analysis of the CONFIDANT protocol[C]// Proceedings of ACM Mobile hoc, Lausanne, Switzerland: ACM, 2002: 226—236.
- [2] Michiardi P, Molva R. CORE: a collaborative reputation mechanism to enforce node cooperation in Mobile Ad hoc Networks[C]// Proceedings of the Sixth IFIP Conference OI3 Security Communications, and Multimedia. Portoroz, Slovenia: IEEE, 2002: 107—121.
- [3] Buttyan L, Hubaux J P. Stimulating cooperation in self-organizing Mobile Ad Hoc Networks[J]. Mobile Networks and Applications. 2003, 8(5): 579—592.
- [4] Liu K, Deng J, Varshney P K, et al. An acknowledgment-based approach for the detection of Routing Misbehavior in MANETs[J]. IEEE Transactions on Mobile Computing, 2007, 6(5): 488—501.
- [5] Graffi K, Mogre P S, Hollick M, et al. Detection of colluding misbehaving nodes in mobile ad hoc and wireless mesh networks[C]// Proceedings of 22007 Global Telecommunications Conference. Washington, DC: IEEE, 2007: 5097—5101.
- [6] 谭运宝, 钟诚, 张尊国. 一种基于邻居合作监测的移动ad hoc网络信任模型[J]. 微电子学与计算机, 2008, 25(10): 227—230.

作者简介:

谭运宝 男, (1983—), 硕士. 研究方向为网络信息安全.

钟诚 男, (1964—), 博士, 教授, 博士生导师. 研究方向为信息安全、并行分布计算.

玉易 女, (1985—), 硕士生, 助理工程师. 研究方向为网络与并行分布计算、信息安全.

刘磊 男, (1986—), 硕士生. 研究方向为网络信息安全.