文章编号:1671-4598(2018)08-0243-04 DOI:10.16526/j.cnki.11—4762/tp.2018.08.054 中图分类号:TP393 文献标识码:A

基于信誉系统对 GRID 网格 Leader 选择协议的安全性研究

韩 帅,矫文成
(陆军工程大学石家庄校区 电子与光学工程系,石家庄 050003)

摘要:针对 GRID 路由协议中的网格 Leader 选择协议,首先运用基于有限状态机的形式化分析方法对它的安全性进行了分析,之后基于现有信誉系统,提出一种基于信誉度的信誉模型;模型包括信誉度计算、信誉管理和信誉决策,依据节点信誉度的变化以及设置的信誉度阈值识别并处理内部恶意节点,保证网络通信的安全可靠;仿真实验表明,该模型能够有效识别出恶意节点,显著提高网络分组投递率,但节点间传输平均时延有所延长,需进一步优化。

关键词:GRID;Leader 选择协议;形式化分析;信誉系统;信誉度

Security Research of GRID Leader Selection Protocol Based on Reputation System

Han Shuai, Jiao Wencheng
(Army Engineering University, Shijiazhuang 050003, China)

Abstract: In view of the Grid Leader Selection Protocol in GRID routing protocol, first analyzes its security by using the formal analysis method based on finite state machine. Then combined with the existing reputation system, this paper proposes a reputation model based on creditworthiness. The model includes reputation calculation, reputation management and reputation decision. According to the change of the credibility of the nodes and set the credibility threshold to identify and deal with internal malicious nodes, ensure the safe and reliable communication network. Simulation results show that this model can effectively identify malicious nodes and significantly improve the delivery rate of network packets, but the average transmission delay between nodes is prolonged, which needs to be optimized.

Keywords: GRID; leader selection protocol; formal analysis; reputation system; creditworthiness

0 引言

移动 Ad Hoc 网络(mobile ad hoc networks, MANET)[1]是由若干个带有无线通信设备的移动节点组成的。MANET 面临的安全威胁日益严峻,无线链路本身易受到外部节点攻击,而网络路由的不断变化也会导致节点间的信任关系产生动态变化,容易遭受内部节点背叛攻击[2]。因此 MANET 的安全性已经成为一大研究热点。

随着定位技术的不断发展,定位精度越来越高,因此基于位置的路由协议也引起了人们的重视[3]。GRID 路由协议是 WEN—HWA LIAO[4]等人提出的完全基于位置的路由协议,它利用位置信息完全解决了路由中的查找路由、数据转发、维护路由 3 个关键问题。该协议将网络所覆盖的范围划分为网格状的区域,每个网格内通过子协议网格 Leader 选择协议(Grid Leader Selection Protocol)选取一个带有定位装置的节点,作为该网格的 Leader,负责该网格的数据转发[5]。本文将对该子协议的安全性进行研究。

本文将利用形式化分析的方法,先对网格 Leader 选择协议的安全性进行分析[6],更形象地分析它可能存在的安全漏洞,之后利用信誉系统[7]对其进行改进,更好的解决其安全漏洞,以满足 MANET 通信的安全目标。

1 形式化安全分析

形式化分析方法是用数学方法描述和推理,对协议及安全属性进行形式化建模,将对协议的安全性分析转化为对应形式化模型的分析[8],运用这种方法可以避免协议安全性分析的局限性,有可能发现安全协议的一些未知攻击。

本文利用有限状态机(Finite-state machine, FSM)对网格 Leader 选择协议进行形式化建模。有限状态机,又称有限状态自动机,是表示有限个状态以及在这些状态之间的转移和动作等行为的数学模型[9]。FSM 是一种算法思想,由一组状态、一个初始状态、输入和根据输入及现有状态转换为下一个状态的转换函数组成。通常使用状态图来对 FSM 进行精确地描述。有限状态机是一个五元组 $M=(Q, \Sigma, \delta, q_0, F)$,其中:

收稿日期:2018-01-11; **修回日期**:2018-01-26。

作者简介:韩 帅(1994-),男,山西介休人,硕士研究生,主要从事网络信息安全方向的研究。
矫文成(1970-),男,副教授,硕士研究生导师,主要从事软件保障、信息安全与对抗方向的研究。

$Q=\{q_0, q_1, \ldots, q_n\}$ 是有限状态集合，$\Sigma=\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ 是有限输入字符集合，$\delta: Q\times\Sigma\rightarrow Q$ 是状态转移函数，$q_0\in Q$ 是初始状态，$F\subseteq Q$ 是最终状态集合[10]。

GRID 路由协议中，每个网格中的节点运行网格 Leader 选择协议来维护本网格的 Leader，保证该网格的数据转发。网格 Leader 选择协议规定距离网格中心最近的节点将被选为网格 Leader，只要某节点被选为 Leader，直到它移出网格才重新选取新 Leader。定义 $S=\{S_0, S_1, S_2\}$，表示原网格 Leader 选择协议的状态集，S_0 表示初始状态，$F=\{S_0\}$ 表示终结状态。其 FSM 模型如图 1 所示。

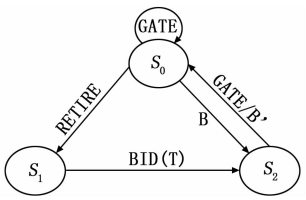

图 1 FSM 模型

网格 Leader 周期性发送 $GATE(g, loc)$ 分组，其中 g 是该网格坐标，loc 是当前位置。当它离开该网格时，广播 $RETIRE(g, T)$ 分组，g 是原网格坐标，T 是它保存的路由表。保存 T，并由状态 S_0 转移到 S_1。若在一个周期内网格内节点没有接收到 $GATE$ 分组，则节点 A 广播 $BID(g, loc)$ 分组，g 是网格坐标，loc 是 A 的当前位置，转入状态 S_2。若 Leader 仍在该网格中，则向 A 回复 $GATE$ 分组；非 Leader 节点 X 收到 BID 分组时，若它离网格中心比分组中的 loc 近，就向 A 回复 $BID(g, loc')$ 分组，loc' 为 X 当前位置，并广播 BID 分组；若没有收到新的 $GATE$ 或 $BID(g, loc')$ 分组，将自己认定为新的网格 Leader，返回状态 S_0。由于新 Leader 是节点自己认定的，因此同一网格中可能存在多个 Leader。当一个自认为是网格 Leader 的节点收到其他离网格中心更近的节点发送的 $GATE$ 分组时，就认为自己不是 Leader，不再发送任何 $GATE$ 分组[11]。

由图 1 及其分析可知，网格 Leader 选择协议在面临选择新节点时的优先级只考虑到离网格中心的位置，容易引起内部恶意节点的攻击。若网格内存在恶意节点，当 Leader 离开时会广播 RETIRE 报文，包含网格坐标，若恶意节点通过篡改将自己的位置坐标改为前网格 Leader 坐标，则它将被选为新的网格 Leader，控制该网格的数据传输，在路由过程中窃取有用数据，破坏路由协议的工作过程。因此需要对网格 Leader 选择协议进行改进增加它的安全性，本文结合现有的信誉系统，提出基于信誉度的信誉系统对 Leader 进行改进，增加选择新网格 Leader 的依据，抑制内部背叛节点攻击。

2 网格 Leader 选择协议改进

2.1 SGRP 的安全方案

陈晶[12]等人在 GRID 协议的基础上提出了安全的网格路由协议 SGRP（Security Grid Routing Protocol），它利用单向散列函数为基础而改进的 TESLA 认证方案[13]，对新加入网络的节点进行认证，并提出了一种基于 CONFIDENT[14]的信誉系统来抑制内部恶意节点的破坏行为。仿真表明 SGRP 可以检测出报文转发时的恶意中断攻击者，同时有一定概率可以发现内部背叛节点。但 SGRP 没有针对子协议网格 Leader 选择协议进行安全性分析，也没有对防止内部节点破坏进行设计。本文在 SGRP 协议的基础上对网格 Leader 选择协议进行改进，增加它对内部恶意节点的处理决策。

2.2 网格 Leader 选择协议的改进

针对网格 Leader 选择协议中面临的内部攻击问题，结合 SGRP 中的信誉机制对它进行了安全性改进。信誉模型以信誉度为依据，由信誉度计算、信誉管理及信誉决策三层组成，以信誉度计算为基础，将第一手信誉度、信誉报告综合成信誉等级，根据信誉度门限值进行信誉决策，高效判别出恶意节点，合理进行 Leader 选择，提高网络通信的安全可靠。

本文提出的信誉模型由信誉度计算、信誉管理和信誉决策组成。信誉度计算是模型的基础，信誉管理是核心，信誉决策是目的。结构如图 2 所示。

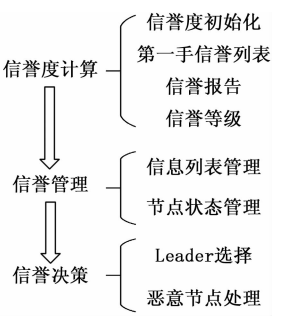

图 2 信誉模型结构图

信誉度计算主要完成信誉度初始化，第一手信誉信息计算、信誉报告及信誉等级的具体计算过程。信誉管理主要负责网格内节点信誉度及保存路由表的更新，实现节点信息的动态管理。信任决策以信誉度为重要标准选择网格 Leader，通过节点信誉度识别恶意节点，并对识别到的恶意节点进行处理，从而提高网络的安全性。

2.2.1 信誉度计算

2.2.1.1 初始化

模型主要维护节点保存的信息列表，详细记录节点间交互信息及信誉度列表，每个周期对节点的信誉度进行更新。信息列表如表 1 所示。

表 1 信息列表

节点 ID	交互 ID	交互成败	历史信誉度
ID_i	ID_j	Success	0.6
ID_j	ID_i	Failure	Default
…	…	…	…

其中，ID_i、ID_j 是节点 i，j 的身份标识；历史信誉度表示在网络运行期间节点通信过程中的信誉等级，范围为[0，1]，0 表示节点完全不可信，节点须立即移出网络，1 表示节点完全可信，如果没有计算结果则显示为 default，若为新节点，则设置为信誉度默认值，取值为 0.6。

需要强调的是，节点自身不能保存自己的状态列表，无法查看自己在其他邻节点列表中的信誉度大小，以防恶意节点通过查询自己的信誉度而发动掩饰攻击将自身的信誉度提高。

2.2.1.2　计算

网络内每个节点通过自身检验得到第一手信誉信息，然后按照周期越近信誉权重越高的原则计算最近 3 个周期的信誉信息，计算得到的信誉值再传递给其他节点，节点就可以根据自身的信誉值及其他节点的信誉值综合得到信誉等级，来判断节点的可信程度。

假设节点 i 与节点 j 相互观察，第一手信誉信息可以用 F_{ij} 表示，信誉报告值用 FR_{ij} 表示，信誉等级用 R 表示。在一个周期内若观察到节点正常，信誉值加 α，若观察到节点异常，则减 β，若一个周期内没有观察到节点行为，则减 δ，要求 $\alpha<\delta<\beta$，这样可以更快地剔除恶意节点。在 3 个周期末，按公式（1）计算 FR_{ij}：

$$FR_{ij} = 0.5F_{ij}^{1} + 0.3F_{ij}^{2} + 0.2F_{ij}^{3} \tag{1}$$

这里系数可以根据实际环境中的硬件条件或其他条件进行调整，应保持最近周期内的信誉度权重更高，确保信誉值得新鲜性。

为避免因为节点故障而产生误判，计算信誉等级还需考虑周围节点的信誉报告。假设节点 i 收到节点 j 的信誉报告 FR_{kj}，节点 i 依据公式（2）更新信誉等级 R_{ij}：

$$R_{ij} = w \cdot FR_{ij} + (1-w) \cdot FR_{kj} \tag{2}$$

其中：w 可设定参数。节点 i 接收到所有关于 j 的信誉报告都应执行该过程。在初始化时，设定初始值 r_0、最大值 $r_{\max}$ 和门限值 r_{thresh}，当 $R_{ij} > r_{thresh}$ 时，节点 i 与 j 互相信任，否则认为 j 是恶意节点。

当节点间开始交互报文时，首先计算第一手信誉信息。在一个周期内若节点 i 与 j 正常交互，则 $F_{ij}+\alpha$，若失败则 $F_{ij}-\beta$，若没有交互则 $F_{ij}-\delta$，其中($\alpha<\delta<\beta$)。

每过 3 个周期，节点 i 按照公式（1）计算信誉报告。同时考虑周围节点的信誉报告，按照公式（2）计算节点 i 的信誉等级，并作为最终信誉度写入信息列表中。

信誉系统有一定的局限性，很难判定恶意节点和故障节点，设定 $\Delta = r_{\max} - r_{thresh}$，随着 Δ 的增大，误判率会降低，但系统灵敏度会随之下降，因此只能在误判度和灵敏度之间寻求一个平衡。

2.2.1.3　更新

网络正常运行阶段，随着网络的动态变化以及恶意节点的攻击，节点信誉度会发生变化，因此必须更新信誉度。计算得出新的信誉等级后要对节点本地列表中的历史信誉度进行更新，从而保持节点对邻节点信誉信息的动态掌握。更新历史信誉度采取加权求和的方式，若历史信誉度为默认值，则用新信誉度进行替换，否则按公式（3）进行更新。

$$R_{ij} = \lambda R_{ij}^{old} + (1-\lambda) R_{ij}^{new} \tag{3}$$

其中：λ 为历史信誉度权重，可根据不同网络环境进行设置。

2.2.2　信誉管理

信誉管理是该模型的核心，负责网络中信誉信息的存储、提取、更新、删除等任务，确保节点信誉度的新鲜、高效和安全。

网络建立初期，节点的信息列表为空，节点间相互发送如下报文交换信息并保存在自己的信息列表中。当网络运行到一定周期后，就会伴随有节点信息列表的更新和删除。

表 2　报文格式

ID	位置	速度	Leader 标识	TESLA 单向密钥链	第一手信誉信息	信誉报告	信誉等级

节点信息列表管理流程为：当网络开始运行，节点 A 与 B 开始交互，查看交互报文中节点 B 的信誉信息，并与信誉阈值进行比较，若小于阈值，则将节点 B 标记为非正常节点，不建立信息列表；若大于阈值，则计算节点 A 与 B 的信誉度，并保存到节点 A 的信息列表中。随着网络的运行，每过 3 个周期节点 A 更新关于 B 的历史信誉度，保证列表的新鲜性。

2.2.3　信誉决策

信誉决策主要是利用信誉度进行网格 Leader 选择，识别出恶意节点，并选择信誉度高且距离网格中心近的节点作为网格 Leader，负责网格数据转发，保证网络的安全运行。因此本部分主要包括两方面：恶意节点识别和网格 Leader 选择。

2.2.3.1　恶意节点识别

恶意节点的识别是提高网络安全的重要环节，能够准确识别并处理恶意节点是衡量信任模型性能的关键[15]。本文定义了两个阈值分别是处理阈值 θ 和预警阈值 φ，以及定义了节点的 3 种状态分别是争创状态、怀疑状态、驱除状态。

正常状态表示节点的信誉等级在允许的范围内，可以将此节点选为可靠的 Leader 进行数据转发。怀疑状态表示节点新的信誉信息与历史信誉信息变化较大，超过了预警阈值 φ，故将此类节点定义为怀疑状态，继续观察一个周期，若再次发生异常，则将该节点采取处理措施。驱除状态表示节点信誉度低于处理阈值 θ，直接移出网络。

2.2.3.2　网格 Leader 选择

根据节点计算得信誉等级进行网格 Leader 的选择，是信誉决策的目的。本文充分考虑节点信誉等级和距离网格中心距离，利用信誉度进行网格 Leader 选择的流程如图 4 所示。

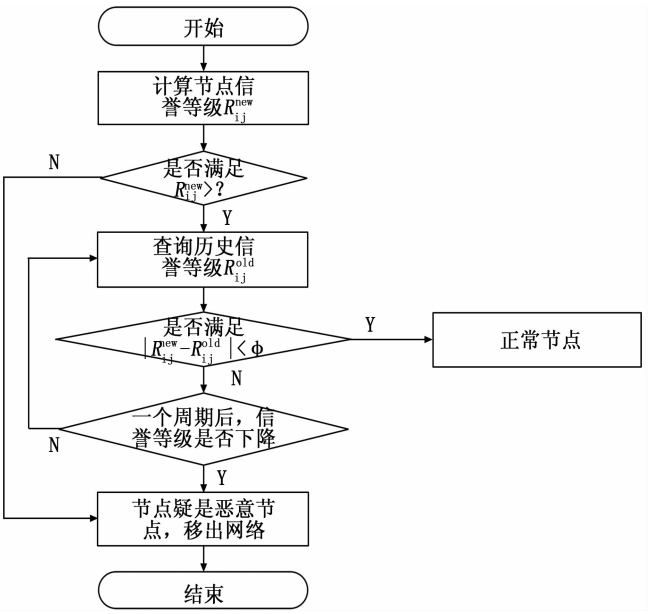

图 3 恶意节点识别流程图

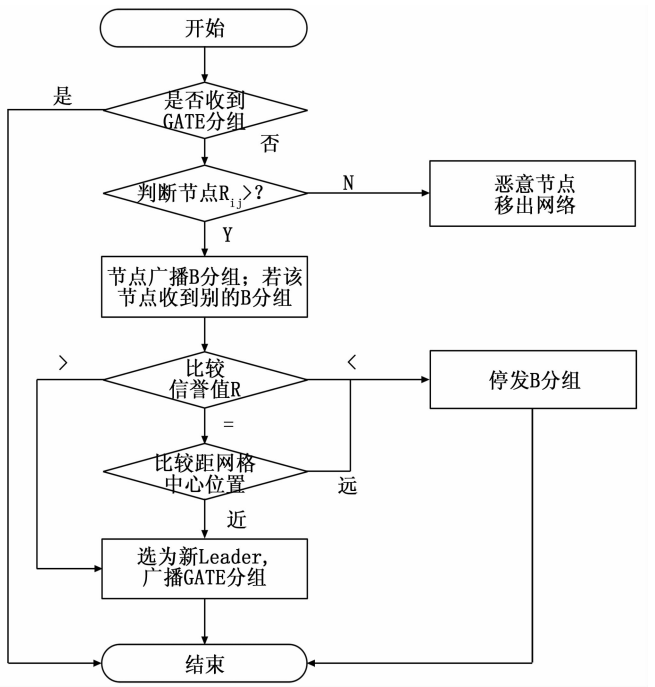

图 4 网格 Leader 选择流程图

3 仿真性能分析

利用 NS2 仿真实验工具[16]来验证信誉模型的安全性及测试网络性能。在仿真中，节点总数设置为 100 个，节点运动区域为 500 m×500 m，网格大小为 100 m×100 m，节点传输半径为 80 m，在区域内以 0－10 m/s 的随机速度随机运动，到达目标点后短暂停留，继续向新目标点随机运动，直到仿真结束。其中设置部分恶意节点，在网络中发动多种攻击，包括数据报丢弃攻击，篡改攻击，诽谤攻击以及掩饰攻击等。节点以固定比特率发送数据包，大小为 128 bit，每秒发送 4 个报文，仿真时间为 300 s。具体的仿真参数如表 3 所示。

表 3 实验仿真参数

α	β	δ	r_0	r_{max}
0.2	0.5	0.3	0.6	1
r_{thresh}	φ	θ	ω	λ
0.3	0.45	0.3	0.4	0.3

3.1 节点信誉度变化

随着网络的运行，节点之间有了信息交互，节点信誉度发生变化。如图 5 所示，节点的初始信誉值为 0.6，随着网络运行时间的增长，正常节点的信誉等级呈现平滑缓慢上升趋势，而由于恶意节点对邻节点的恶意影响，恶意节点的间接信誉度对信誉等级产生较大影响，因此恶意节点的信誉等级出现快速下滑趋势，当信誉等级达到预警阈值 0.45 以下时，先观察一个周期，发现其信誉等级仍存在下降趋势，将其剔除出网络。

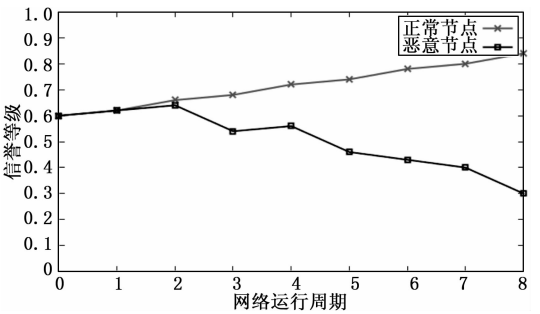

图 5 节点信誉等级变化趋势图

3.2 性能分析

图 6 表示在恶意节点数不同时的分组投递率变化。可以看出随着网格内恶意节点数的增加，两个协议的分组投递率都在减小，但改进的网格 Leader 选择协议的分组投递率高于原网格 Leader 选择协议的分组投递率，这是因为网格内恶意节点数增多，恶意节点的各种攻击行为中断了正常节点的报文传送，而信誉系统及时检测处理恶意节点，因此随着恶意节点数的增加，改进后的网格 Leader 选择协议比原网格 Leader 选择协议的分组投递率影响更小。

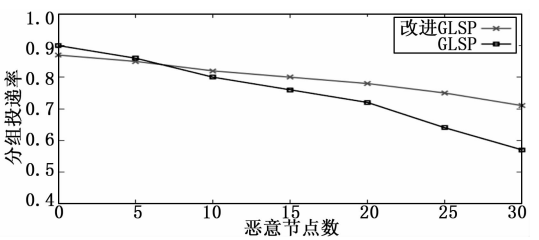

图 6 不同恶意节点数下的分组投递率

图 7 表示在恶意节点数固定为 20，节点在不同周期时的点到点平均时延。可以看出基于信誉系统的网格 Leader

（下转第 251 页）