基于激励机制的贝叶斯博弈防御模型*

王 静,袁凌云,夏幼明,杨荣芳,陈 彬
(云南师范大学 信息学院,云南 昆明 650092)

摘 要:基于贝叶斯博弈理论并结合自私节点激励机制构建了一个入侵检测模型,并运用这一理论制定了一种改进的安全路由协议,证明了该模型中存在贝叶斯纳什均衡。仿真实验表明,该模型能够有效地抑制节点的自私行为并提高网络的服务质量。

关键词:贝叶斯博弈;激励机制;无线传感器网络;入侵检测
中图分类号:TP393 **文献标识码**:A **文章编号**:1674-7720(2011)10-0066-03

A Bayesian game approach with incentive mechanism for IDS

Wang Jing,Yuan Lingyun,Xia Youming,Yang Rongfang,Chen Bin
(Department of Information,Yunnan Normal University,Kunming 650092,China)

Abstract: In this paper, we model the interaction of nodes in WSN and intrusion detection system (IDS) as a Bayesian game formulation and use this idea to make a secure routing protocol. As this game approaches to Nash equilibrium, it leads to a defense strategy for the network. Simulation results show that the model can availably repress the selfish behavior of nodes and raise the service quality of the network.

Key words: Bayesian game;incentive mechanism;WSN;intrusion detection

一个WSN网络包含成百上千个低能量低消耗节点,这些节点通过无线的方式进行通信[1]。在很多情况下,安全问题对于WSN来说是极其重要的。有许多适用于Ad Hoc网络的IDS的系统模型[2-3],但是都不适用于WSN,因为这些节点在内存、处理器和电池电量方面有着更加严格的限制。同样的原因,加密机制也不适合在WSN中使用,因为计算消耗大,这些节点时间和能量都不够充足。另外,要保障无线通信信道安全也很困难。

本文提出了一个基于贝叶斯博弈的安全策略,在监视设备和传感器节点之间实施协作,可以防御主动DOS攻击[4],恶意节点一经发现,就会从网络中隔离,并且入侵检测系统会对博弈过程的每个阶段实施监控,根据路由节点的信誉值提供安全路由。

入侵检测系统负责监视节点。IDS是一个软件或硬件系统,对网络中的事件进行自动检测,分析其安全特征[5]。简单的安全算法(例如加密)不能满足必要的安全需求。加密算法只能防御来自外部节点的攻击,但是不能防御内部的恶意节点。

1 改进的LEACH协议

LEACH协议是WSN中极其重要的基于簇的路由协议,通过在不同的时间段让每个节点都有机会成为簇头节点来最小化能量的消耗。簇头节点(CHs)需要对数据进行数据融合,并负责把数据传递给基站(BS)。LEACH协议在能量消耗方面比其他路由协议都要好,能够将系统寿命提高一个数量级[6]。

本文提出一种基于贝叶斯博弈理论的安全路由协议,结合自私节点激励机制[7],使入侵检测系统取得更好的检测效果,这种协议称之为"S-LEACH",在基站上的入侵检测系统称为"全局IDS",其他的入侵检测系统在簇头节点上,称为"本地IDS"。整个过程分为设置和持续两个阶段。在设置阶段,选出簇头节点(CHs)。某一节点以一定的规则被选为簇头节点,对其他的节点广播这个消息。这个过程中,簇头节点使用CSMA MAC协议,用相同的广播能量发送这个消息。其他节点就可以根据接收到的广播信号的强度确定它们属于哪一个簇,然后再发送一个消息给首选的簇头节点。第二个阶段,

*基金项目:云南省应用基础研究计划(2008CD113);云南省教育厅基金项目(08Y0136)

簇头节点安排时间段给簇中的节点，就可以在不同时间段发送数据给这些节点（基于 TDMA 的方法）。节点只能在分派的传送时间段内发送数据。如果一个节点被认为是自私节点，本地 IDS 就不会分派任何时间给自私节点。这个阶段与 LEACH 协议相同。

假设节点总是有数据要传送，本地 IDS 就会寻找在数据包传送过程中的不合作的节点（自私节点），并记录这个节点的 ID。在每一个阶段结束时，节点的信誉值都会被传送到全局 IDS。全局 IDS 负责核查所有节点的信誉值，并将那些信誉值低于阈值的节点的 ID 广播到整个网络。而本地 IDS 不会分派任何时间段给自私节点，从而减少系统资源的浪费。

如果节点是静止不动的，就没有必要用到全局 IDS，本地 IDS 可以监视节点并计算隶属于它们簇中每个节点的信誉值，以表格的形式存储。

2 IDS 与 WSN 之间的贝叶斯博弈

在这里提出一个贝叶斯博弈模型，有 2 个参与者，一个是位于簇头节点中的 IDS（本地 IDS），用 j 表示；另一个是簇中的某一个节点，用 i 表示。参与者 i 有两种类型：正常节点 $\theta_i=0$；自私节点 $\theta_i=1$。节点类型是私有信息，参与者 j 不知道参与者 i 是自私节点还是正常节点。节点有两种纯策略：合作与不合作。合作意味着要优先转发数据包。参与者 j 只有一种类型，正常的 IDS 的 $\theta_j=0$。它也有两种纯策略：报警和不报警。报警是指发现一个节点是自私的，并相应降低该节点的信誉值；不报警就是认为该节点是正常节点。

为了加强节点间的协作，本文提出信誉值(reputation)的概念，用 R 来表示。IDS 也有信任度，当它发现恶意节点时，$R+1$；当节点优先转发数据包时，节点的信誉值 $R+1$，否则 $R-1$。

IDS 捕获一个节点的成本等于它在此过程中消耗的能量，用 C_c 来表示。自私节点不会有任何的成本，因为不转发数据包也不会消耗任何额外的能量。当自私节点没有传递数据而且也没有被 IDS 捕捉时，自私节点就会有收益，用 G 来表示。

表 1、表 2 是博弈收益表。α 表示 IDS 正确检测出自私节点的概率，β 表示 IDS 发出错误警报概率，$\alpha,\beta\in[0,1]$。

在表 1 中，组合策略（不合作，报警），节点的信誉值会降低，减少的值就是被发现是自私节点的次数，而 IDS 的信誉值会增加，增加的值是它正确检测的次数；组合策略（不合作，不报警），参与者 i 获得了收益，同时也增加了信誉值，增加的值是未被 IDS 检测出的次数，与此同时，参与者 j 会因为错误的检测而减少信誉值。另外两种组合策略，当参与者 i 合作时，它的收益就等于信誉值，也就是它表现正常的次数。如果参与者 j 什么都不做，就不会有能量消耗，也不会得到信誉值的增加，否则就会既损失成本又得到了错误的检测结果。收益矩阵对正常节点也是一样的道理。

表 1 自私节点博弈收益矩阵

	报警	不报警
不合作	$-\alpha R,\alpha(R-C_c)$	$G(1-\alpha),R(\alpha-1)$
合作	$\beta R,-\beta(R+C_c)$	$R(1-\beta),R(1-\beta)$

表 2 正常节点博弈收益矩阵

	报警	不报警
合作	$\beta R,-\beta(R+C_c)$	$R(1-\beta),R(1-\beta)$

3 贝叶斯纳什均衡[8]

首先假设节点有一个先验概率，参与者 i 是自私节点的概率为 p。在博弈理论[9-10]中通常都会假设参与者是理性的，并且都想最大化它们的收益。所以参与者 i 始终不想合作，不想因为转发数据而有能量的消耗，同时也不想被 IDS 捕获。另一个方面，IDS 想发现自私节点，不想因为错误的检测而浪费能量。

如果参与者 i 是自私节点就选择不合作，是正常节点就选择合作。IDS 报警策略的收益期望是：$E_{\mu_j}(\text{catch})=p\alpha(R-C_c)-(1-p)(\beta R+\beta C_c)$；IDS 不报警策略的收益期望为：$E_{\mu_j}(\text{miss})=pR(\alpha-1)+(1-p)(R-R\beta)$。

如果 $E_{\mu_j}(\text{catch})>E_{\mu_j}(\text{miss})$，也就是 $p>\dfrac{\beta C_c+R}{2R+C_c(\beta-\alpha)}$，IDS 将会执行报警策略。当 IDS 报警时，自私节点选取的最优策略就是合作，所以（（自私节点 不合作，正常节点 合作），报警，p）显然不是纯策略的纳什均衡。

当 $p<\dfrac{\beta C_c+R}{2R+C_c(\beta-\alpha)}$ 时，IDS 的最优策略就是不报警。这时，（（自私节点 不合作，正常节点 合作），报警，p）就是一个贝叶斯纳什均衡。为了证明在这个博弈模型中不存在其他的纯策略的纳什均衡，假设参与者 i 都是合作的（不管是正常节点还是自私节点），这种情况下，IDS 的最优策略就是不报警，这时，参与者 i 就会在下一个阶段改变策略。所以，（（自私节点 合作，正常节点 合作），不报警）不是一个贝叶斯纳什均衡。

但是，当 $p>\dfrac{\beta C_c+R}{2R+C_c(\beta-\alpha)}$ 时，存在一个混合策略的贝叶斯纳什均衡。假设 p' 是参与者 i 不合作的概率，q' 是参与者 j 报警的概率，那么，IDS 报警的收益期望为：

$$E_{\mu_j}(\text{catch})=pp'\alpha(R-C_c)-p(1-p')(\beta R+\beta C_c)-(1-p)(\beta R+\beta C_c)$$

IDS 不报警的收益期望为：

$$E_{\mu_j}(\text{miss})=pp'R(\alpha-1)+p(1-p')(R-R\beta)+(1-p)(R-R\beta)$$

令 $E_{\mu_j}(\text{catch})=E_{\mu_j}(\text{miss})$，得到 $p'^{*}=\dfrac{\beta C_c+R}{pC_c(\beta-\alpha)+2pR}$，这时，对于参与者 i 来说选择合作或不合作是没有区别的。同理，参与者 i 不合作与合作的收益期望分别为：

$$E_{\mu_i}(\text{Do not cooperate})=-q'R\alpha+(1-q')(G-G\alpha);$$

$E_{\mu_i}(\text{Cooperate})=2q'R\beta+2(1-q')(R-R\beta)$。

令 $E_{\mu_i}(\text{Do not cooperate})=E_{\mu_i}(\text{Cooperate})$，得到 $q'^{*}=\frac{G(\alpha-1)+2R(1-\beta)}{G(\alpha-1)+R(2-4\beta-\alpha)}$，这时，对于参与者 j 来说，选择报警或不报警也是没有区别的。所以组合策略((自私节点 p'^{*}，正常节点 合作)，q'^{*}，p)是一个混合策略的贝叶斯纳什均衡。

4 仿真实验及结果

这里用网络模拟软件 NS2 来对算法进行仿真。节点分布在 1 000 m×1 000 m 的区域范围内，仿真时间为 1 200 s，假设在实验一开始所有节点都有相同的能量。

图 1 显示的是未转发的数据包的数量与自私节点占总节点数的百分比之间的关系。在无防御的网络中，数据包丢失的数量比有博弈理论的防御系统多很多。在该系统中，节点通过信誉值的激励作用来选择合作策略；如果不合作，节点就会被检测系统从网络中隔离。

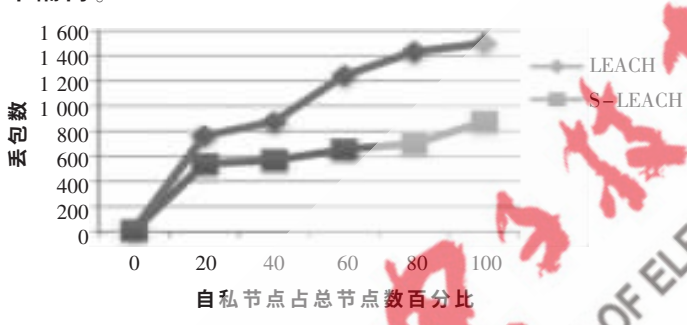

图 1 丢包数与自私节点所占百分比关系图

图 2 显示的是当自私节点占总节点的 40%时，网络的吞吐量与时间的关系。在前 400 s，IDS 发现了一些自私节点，但是因为恶意行为的次数还没有超过预先设定的阈值，所以 IDS 没有采取任何行动，使得 LEACH 与 S-LEACH 的表现大致相同，但是随着时间的推移，自私节点被隔离，这时整个网络的吞吐量就不断增大。

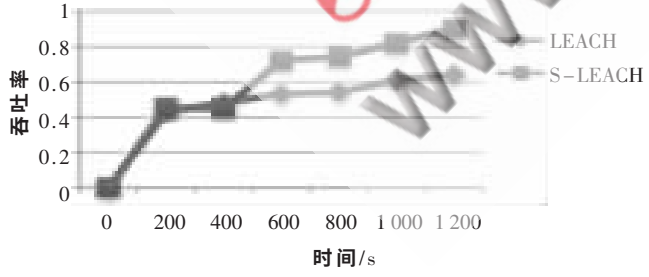

图 2 网络吞吐量与时间关系图

图 3 显示的是自私节点所占比例与时间的关系。在实验一开始，自私节点占总节点的 60%，正常节点占 40%，随着时间的变化，自私节点的比例越来越小，因为 IDS 会不断地捕获自私节点，并将它们从网络中隔离。

图 4 显示了丢包率与节点数目之间的关系。在所有

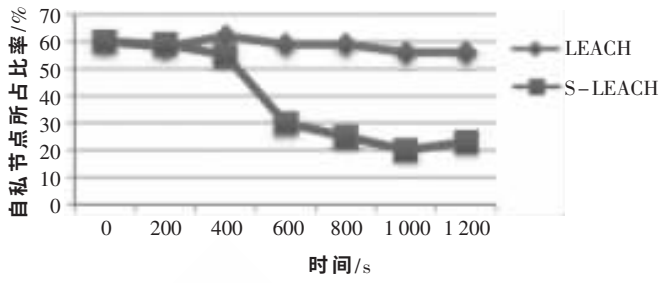

图 3 自私节点所占比例与时间关系图

图 4 丢包率与节点数目关系图

节点中，始终保持有 50%的自私节点。当节点数不是很多时，在 LEACH 实验中丢弃的数据包要比 S-LEACH 实验中的多很多，这是因为簇头节点能够在分配给各个成员节点的时间段中，检测出节点的类型。

本文提出了一个入侵检测系统与传感器节点之间的贝叶斯博弈防御模型，并证明了在该模型中存在两个贝叶斯纳什均衡。下一步的研究工作，要将该模型改为动态的贝叶斯博弈模型，IDS 不是根据节点的类型来修改先验概率，而是可以动态更新先验概率。

参考文献

[1] 陈林星.无线传感器网络技术与应用[M].北京：电子工业出版社，2009.

[2] DONADIO P, CIMMINO A, VENTRE G. Enhanced intrusion detection systems in Ad Hoc Networks using a grid based agnostic middleware[C].In proceedings of the ACM, 2008.

[3] KACHIRSKI O, GUHA R. Intrusion detection using mobile agents in wirelless Ad Hoc networks[C]. In Proc. of the IEEE Workshop on Knowledge on Media Networking,2006.

[4] STRIKOS A A. A full approach for intrusion detection in wireless sensor networks[J]. Computer Networks,2007.

[5] 陈海光.无线传感器网络中若干安全问题研究[D].上海：复旦大学，2008.

[6] HEINZELMAN W R,CHANDRAKASAN A,BALAKRISHNAN H. Energy-efficient communication protocol for wireless sensor networks[C]. In the Proc.of the Hawaii Int'l. Conf. on System Sciences, Hawaii, Jan. 2000.

[7] HABIB A,CHUANG J.Service different-iated peer selection: an incentive mechanism for Peer-to-Peer media streaming [C]. In Proc.of the IEEE Transactions on Multimedia,2004.

[8] 姚国庆.博弈论[M].北京:高等教育出版社,2007.
[9] 曹晖,王青青,马义忠,等.基于静态贝叶斯博弈的攻击预测模型[J].计算机应用研究,2007,24(10):122-124.
[10] 张辉,许峰.WSN 中基于权值的 Leach 协议的研究与改进[J].微计算机信息,2010(22):199-201.

(收稿日期:2010-11-27)

作者简介:

王静,女,1985年生,硕士研究生,主要研究方向:无线传感器网络。