



基于序贯概率比检验的自私路径检测方法

王骐,王青萍,王怀兴,肖正安

(湖北第二师范学院,湖北 武汉 430205)

摘要:根据基于序贯概率比检验的无线传感器网络模型,对基于路由功能的自私路径的检测方法进行了研究。通过分析节点接收到的观测样本值,将计算得出的路径评判值与已知阈值进行比较,从而判定是否为自私路径。仿真结果表明,这种基于序贯概率比检验的序贯抽样方案所需观测值的数量大大减少,运行更快,且具有较高的检测精度。相比于其他固定抽样方案,这种方法无需事先确定检验统计假设所需的样本观测值数量,有利于对危害网络安全的行为做出快速响应,从而限制受损网络的范围。

关键词:无线传感器网络;序贯概率比检验;网络模型;自私行为检测;评判;NS-2 仿真

中图分类号: TN918.91

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016059

Detection method for selfish routes based on the sequential probability ratio test

WANG Qi, WANG Qingping, WANG Huaixing, XIAO Zheng'an

Hubei University of Education, Wuhan 430205, China

Abstract: According to a network model based on the sequential probability ratio test (SPRT), one detection method of selfish routes with respect to the routing functionality in wireless sensor network was developed. Through the analysis of the observed sample values of the nodes, the calculated routes evaluation values were compared with the known threshold values so as to determine whether it was selfish route. Simulation results show that the sequential sampling scheme based on the sequential probability ratio test had high detection accuracy, and the number of the required observation was greatly reduced, so it could operate faster. A merit of SPRT is that the number of observations required to test statistical hypotheses need not be determined in advance when compared to other methods based on a fixed number of observations. This allows for making prompt decision on the behavior of damage to the network, thus it can limit the scope of the damaged networks.

Key words: wireless sensor network, sequential probability ratio test, network model, misbehavior detection, evaluation, NS-2 simulation

1 引言

无线传感器网络是由无人值守的节点形成的一种动

态通信网络。在网络层的路由选择中,这种自组织网络需要节点间的相互协作,共同寻找到达目标节点的可行路径,共同参与数据分组的转发,否则将无法找到可行路径

收稿日期:2015-08-17;修回日期:2016-01-08

基金项目:湖北省高等学校优秀中青年科技创新团队基金资助项目(No.T201417)

Foundation Item: Hubei Provincial Department of Education Research Program (No.T201417)



完成端对端的数据分组传送。根据网络层的路由功能以及节点的行为,可将节点分为协作和自私两种类型。“自私”是一种故意的消极行为,为了节省资源,自私节点可能不参与数据分组的转发,丢弃部分或全部经由自身转发的数据分组^[1,2]。这些自私行为将会大大弱化网络性能,甚至会导致全网通信瘫痪。因此,从网络安全和性能的角度出发,需要找出网络中的自私节点。

如何检测出自私节点,一些国内外相关文献提出了一些解决办法。参考文献[3]介绍了一种将检测节点获得的单位时间特征量值与阈值进行对比来判断自私节点的方法;参考文献[4]采用基于序贯概率比检验(sequential probability ratio test, SPRT)的方法,对节点不与周围节点发生消息通信的时间进行阈值设定,从而检测发动态攻击的节点;参考文献[5]通过一种基于序贯概率比检验的检测算法,检测无线传感器网络中MAC层的非协作行为;参考文献[6]阐述了MAC层的自私行为问题,并将此问题转化为极小—极大顽健序列检测问题;参考文献[7]针对无线传感网络共享信道中自私节点(或恶意节点)对信道的不公平竞争行为,提出了一种基于网络性能特征序列的聚类检测方法。

以上这些检测方法检测的对象都是直接针对节点,观测值或取样样本的数量较大,不仅影响运行效率,对能耗要求也较高,不利于对危害网络安全的行为做出快速响应。与一般的检测方法不同的是,基于序贯概率比检验的自私路径检测方法采用序贯抽样方案,并不直接检测自私节点,而是首先检测自私路径,再从自私路径中检测自私节点。这样做的好处是缩小了检测范围,避免“大海捞针”,有利于降低能耗;另一方面,由于无需事先确定检验统计假设所需的样本观测值数量,因此所需观测值的数量大大减少,能有效提高运行效率和检测精度。

2 基于序贯概率比检验的网络模型

序贯概率比检验是数理统计学的一个分支,它研究的对象是“序贯抽样方案”及如何用这种抽样方案得到的样本进行统计推断。序贯抽样方案是指在抽样时不事先规定总的抽样个数(观测或实验次数),而是先抽少量样本,根据其结果再决定停止抽样或继续抽样、抽多少,直到决定停止抽样为止。反之,事先确定抽样个数的抽样方案,称为“固定抽样方案”。

考虑以下的无线传感器网络模型:该网络节点类型分

为自私型和协作型,节点集记作 $N=\{N_1, N_2, N_3, \dots, N_i\}$, 其中 $i=1, 2, 3, \dots, n$; 自私节点集为 $M=\{M_1, M_2, M_3, \dots, M_i\}$, 其中 $i=1, 2, 3, \dots, n$, 且 $M \subset N$ 。网络内的节点数量记作 $|N|$, 自私节点的数量记作 $|M|$, 所以协作节点的数量为 $|N|-|M|$ 。

一般来说导致分组丢失的因素主要包括以下几个方面。

- 自私节点。设任意自私节点 $i \in M$ 的分组丢失概率为 P_{selfish} 。
- 网络环境。比如网络层的拥塞、数据链路层的争用、信道衰落引起的通信受损等。为了简化起见,假定所有节点 $i \in N$ 因网络环境因素产生的分组丢失概率为 P_{drop} 。

下一步考虑不同节点具有不同分组丢失概率的情况。

定义 1 设网络内起始节点为 $s=h_0$, 目标节点为 d , 从起始节点 $s=h_0$ 到目标节点 d 之前的最后一个节点为 h_k , $R^{s \rightarrow d} = \{h_0, \dots, h_k\}$ 表示从起始节点 $s=h_0$ 到 h_k 之间路径上的有序节点集, 那么从起始节点到目标节点, 即 $h_0 \rightarrow h_k \rightarrow d$ 经历的跳数为 $k+1$ 。

定义 2 令 $R_i^{s \rightarrow d}$ 表示从中间节点 h_i 到 h_k , 即 $h_i \rightarrow h_k$ 上的有序节点集, $R_i^{s \rightarrow d} \subseteq R^{s \rightarrow d}$ 为节点集 $R^{s \rightarrow d}$ 的子集, 那么 $R_i^{s \rightarrow d} = \{h_i, \dots, h_k\}$, $0 \leq i \leq k$, 节点 h_i 到 h_k 即 $h_i \rightarrow h_k$ 的跳数为 $k-i+1$ 。

定义 3 $R^{s \rightarrow d}$ 上的有序关系为: $\forall x, y \in R^{s \rightarrow d}, x < y \Leftrightarrow \text{hop}(x, s \leftrightarrow d) < \text{hop}(y, s \leftrightarrow d)$, 其中, x, y 表示从起始节点 s 到目标节点 d 之间路径上的中间节点, 节点 $\text{hop}(x, s \leftrightarrow d), \text{hop}(y, s \leftrightarrow d)$ 分别表示从起始节点 s 到中间节点 x, y 之间所经历的跳数。

定义 4 如果 $\exists h_j \in R_i^{s \rightarrow d}$, 且 $h_j \in M, i < j \leq k$, 则路径 $R_i^{s \rightarrow d}$ 为自私路径, 即包含自私节点的路径; 否则为正常路径, 即不包含自私节点的路径。

3 自私路径的检测

3.1 序贯概率比检验概述

假定存在两种假设 H_1 和 H_0 , 在这两种假设中, 要么 H_1 正确, 要么 H_0 正确, 不可能同时正确。相应地, 两种假设下的条件概率分别为 $P[x|H_1]$ 和 $P[x|H_0]$ ^[3,4]。为了判断两种假设 H_1 和 H_0 哪个正确, 进行一系列的观测 $x_1, x_2, \dots$, 对于每个样本观测值 $x_n, n \geq 1$, 如果 $P[x|H_0] \neq 0$, 计算 $\frac{P[x_n|H_1]}{P[x_n|H_0]}$ 及 $T_n = T_{n-1} \times \frac{P[x_n|H_1]}{P[x_n|H_0]}$, 其中, $n \geq 1, T_0 = 1$ 。然后以 T_n 为依据, 根据以下准则进行判断。

判别式 1 ①如果 T_n 较大, 表明当前获得的样本观

测值 $x_1, \dots, x_n$ 更有可能是在假设 H_1 下获取的, 因此, H_1 正确; ②如果 T_n 较小, 则表明当前获得的样本观测值 $x_1, \dots, x_n$ 更有可能是假设 H_0 下获取的, 因此, H_0 正确; ③如果 T_n 值的大小不足以判别当前的样本观测值 $x_1, \dots, x_n$ 是在 H_1 还是在 H_0 下获取的, 那么就进行第 $n+1$ 次观测, 获取 x_{n+1} 的值, 计算 T_{n+1} 。如果根据 T_{n+1} 的值仍然无法确定 H_1 和 H_0 哪一个正确, 再进行第 $n+2$ 次观测, 获取 x_{n+2} 的值, 计算 T_{n+2} 。以此类推, 直到能根据①或②判别出 H_1 和 H_0 哪个正确为止。

在对 H_1 和 H_0 进行判别时, 也有可能做出错误的判断, 即理论上 H_1 是正确的, 但实际上正确的是 H_0 , 这种情况称为假肯定; 相反地, 如果理论上 H_0 是正确的, 但实际上正确的是 H_1 , 这种情况称为假否定。根据网络目标, 假设预期的假肯定率和假否定率的上限值分别为 α 和 β , 为了将二者限制在 α 和 β 内, 选取两个阈值 A 和 B , 且 $B < A$ 。阈值 A 和 B 分别有界, 且 $A \leq \frac{1-\beta}{\alpha}$, $B \geq \frac{\beta}{1-\alpha}$ 。如果以 $A = \frac{1-\beta}{\alpha}$ 和 $B = \frac{\beta}{1-\alpha}$ 作为阈值, 将会获得较高的检测精度^[9]。显然, α 和 β 的值越小, 那么当判断 H_1 和 H_0 哪个正确时, 系统所需要的样本观测值就越多。在获取一系列样本观测值 $x_1, \dots, x_n$ 之后, 由于选取了检验阈值 A 和 B , 那么判别式 1 可表述如下。

判别式 2 ①如果 $T_n \geq A$, 则 H_1 是正确的; ②如果 $T_n \leq B$, 那么 H_0 是正确的; ③如果 $B < T_n < A$, 那么就进行第 $n+1$ 次观测, 获取 x_{n+1} 的值, 计算 T_{n+1} 。如果根据 T_{n+1} 的值仍然无法确定 H_1 和 H_0 哪一个正确, 再进行第 $n+2$ 次观测, 获取 x_{n+2} 的值, 计算 T_{n+2} 。以此类推, 直到能根据①或②判别出 H_1 和 H_0 哪个正确为止。

3.2 基于序贯概率比检验的自私路径检测

根据第 3.1 节所述, 现假定存在两种假设 H_1 和 H_0 , 其中 H_1 表示自私路径, H_0 表示正常路径, 现在需要鉴别哪种假设成立。如果网络存在某种端对端数据分组传送的反馈机制, 且采用可靠的传输层协议 (比如 TCP), 那么传输层就会以 TCP 确认的方式来进行反馈。假定以“数据分组的确认 (acknowledgement, ACK)”作为数据分组发送成功的标志, 将观测值记为 ACK, 称作 ACK 事件; 以“数据分组的再发送 (retransmission, RET)”作为数据分组发送失败的标志, 将观测值记为 RET, 称作 RET 事件。因此, 当观测值为 ACK 时, 表明数据分组发送成功; 当观测值为 RET 时, 表明数据分组发送失败^[4,5]。假定节点 $h_i \in R^{s \leftrightarrow d}$, 路径 $R_i^{s \leftrightarrow d}$ 的评

判值表示为 $T(i, R_i^{s \leftrightarrow d})$ 。根据 $R_i^{s \leftrightarrow d}$ 上节点 h_i 的观测值 x_n 为 ACK 或 RET, 对路径 $R_i^{s \leftrightarrow d}$ 是否为自私路径进行评判, 则:

$$T(i, R_i^{s \leftrightarrow d})_n = \begin{cases} T(i, R_i^{s \leftrightarrow d})_{n-1} \frac{P[ACK | H_1]}{P[ACK | H_0]}, & x_n = ACK \\ T(i, R_i^{s \leftrightarrow d})_{n-1} \frac{P[RET | H_1]}{P[RET | H_0]}, & x_n = RET \end{cases} \quad (1)$$

其中, $n \geq 1$, $T(i, R_i^{s \leftrightarrow d})_0 = 1$ 。 $P[ACK]$ 和 $P[RET]$ 分别表示 $R_i^{s \leftrightarrow d}$ 上节点 h_i 的观测值为 ACK 或 RET 的概率。根据定义 4 以及判别式 1 和判别式 2, 路径 $R_i^{s \leftrightarrow d}$ 是否为自私路径的判别依据可进一步表述判别式 3。

判别式 3 ①如果 $T(i, R_i^{s \leftrightarrow d})_n \geq A$, 表明 H_1 正确, $R_i^{s \leftrightarrow d}$ 为自私路径; ②如果 $T(i, R_i^{s \leftrightarrow d})_n \leq B$, 表明 H_0 正确, $R_i^{s \leftrightarrow d}$ 为正常路径; ③如果 $B < T(i, R_i^{s \leftrightarrow d})_n < A$, 那么就进行第 $n+1$ 次观测, 获取 x_{n+1} 的值, 计算 $T(i, R_i^{s \leftrightarrow d})_{n+1}$ 。如果 $T(i, R_i^{s \leftrightarrow d})_{n+1}$ 仍然无法确定 H_1 和 H_0 哪一个正确, 再进行第 $n+2$ 次观测, 获取 x_{n+2} 的值, 计算 $T(i, R_i^{s \leftrightarrow d})_{n+2}$ 。以此类推, 直到能根据①或②判别出 H_1 和 H_0 哪个正确为止。

3.3 $T(i, R_i^{s \leftrightarrow d})$ 的计算

根据以上分析, 判断 $R_i^{s \leftrightarrow d}$ 是否为自私路径的问题, 就转化成了如何计算路径 $R_i^{s \leftrightarrow d}$ 的评判值 $T(i, R_i^{s \leftrightarrow d})$ 的问题。在起始节点 S 发送数据分组的事件中, 对于路径上的任意中间节点, 模型都有 $P[ACK] + P[RET] = 1$ 成立, 且 ACK 和 RET 为互斥事件。因此数据分组发送之后, 存在两种可能: 数据分组发送成功, 目标节点产生的观测值为 ACK; 数据分组丢失, 起始节点产生的观测值为 RET。对于任意节点 $h_i \in R^{s \leftrightarrow d}$, 获得的观测值要么是 ACK, 要么是 RET, 不会同时获得, 因此得到以下两个结论。

- 对于任意节点 $h_i \in R^{s \leftrightarrow d}$, 如果获得观测值 $x_n = ACK$, 由于网络运输层采用了可靠的 TCP, 因此所有其他节点 $h_j (k \geq j > i)$ 也将接收到相同的观测值 ACK。同理, 任意节点 $h_i \in R^{s \leftrightarrow d}$, 如果获得观测值 $x_n = RET$, 那么所有其他节点 $h_j (0 \leq j < i)$ 也将接收到相同的观测值 RET。
- 任意节点 $h_i \in R^{s \leftrightarrow d}$ 根据表达式 $T(i, R_i^{s \leftrightarrow d})$, 能评判的路径仅是 $R_i^{s \leftrightarrow d}$, 而不是完整路径 $R^{s \leftrightarrow d}$ 。因此, 如果节点 h_i 的实际观测值为 ACK, 却收到观测值为 RET 的数据分组, 则表明 ACK 在路径 $R_i^{s \leftrightarrow d}$ 上被丢弃, 这种情况下, 节点 h_i 将把数据分组 RET 看成新的数据分组。



根据以上分析,有:

$$P[ACK|H_1]+P[RET|H_1]=1 \quad (2)$$

$$P[ACK|H_0]+P[RET|H_0]=1 \quad (3)$$

考虑在 R_i^{s-v} 上发送数据分组, 节点 $h_i \in R_i^{s-v}$ 的观测值为 ACK 或 RET 的情况。令 $P[x_i]$ 表示数据分组被传送到目标节点的概率, 它表明数据分组没有因为网络环境因素或自私节点的自私行为, 而被路径 R_i^{s-v} 上的任意节点丢弃; 令 $P[x_2|x_1]$ 表示节点 h_i 获得观测值为 ACK (相当于一次成功发送数据分组) 的概率。因此, 有:

$$P[ACK]=P[x_i] \times P[x_2|x_1] \quad (4)$$

当节点 $h_i \in R_i^{s-v}$ 时, $P[x_i]$ 和 $P[x_2|x_1]$ 的大小受路径 R_i^{s-v} 上自私节点数量的影响。具体来说, 路径 R_i^{s-v} 上自私节点越多, $P[x_i]$ 和 $P[x_2|x_1]$ 的值就越小。

令 α 表示路径 R_i^{s-v} 上自私节点的实际数量, 那么 $\alpha = |R_i^{s-v} \cap M|$ 。如果路径为正常路径, 那么 $\alpha=0$; 否则, $1 \leq \alpha \leq \min(k-i, |M|)$, 其中, $k-i$ 为 $h_i \rightarrow h_k$ 路径上所经历的节点数量 (不包含起始节点 h_i)。假定路径 R_i^{s-v} 上自私节点的实际数量为 α , 分组丢失概率为 P_{selfish} , 那么路径 R_i^{s-v} 上至少有一个自私节点发生分组丢失的概率为:

$$P_{\Pi(\text{selfish})}=1-(1-P_{\text{selfish}})^\alpha \quad (5)$$

实际上 $P_{\Pi(\text{selfish})}$ 表示的是 α 个自私节点对自私路径 R_i^{s-v} 的总体影响, 因此有:

$$P[x_i]=(1-P_{\text{drop}})^{k-i} \times (1-P_{\Pi(\text{selfish})}) \quad (6)$$

$$P[x_2|x_1]=(1-P_{\text{drop}})^{k-i+1} \times (1-P_{\Pi(\text{selfish})}) \quad (7)$$

根据式(4)、式(6)、式(7), 有:

$$P[ACK]=P[x_i] \times P[x_2|x_1]=(1-P_{\text{drop}})^{2(k-i)+1} \times (1-P_{\Pi(\text{selfish})})^2 \quad (8)$$

因此, $P[ACK|H_0]$ 、 $P[ACK|H_1]$ 、 $P[RET|H_0]$ 和 $P[RET|H_1]$ 的值可以确定。

· 如果 R_i^{s-v} 为正常路径, 由式(5)有 $P_{\Pi(\text{selfish})}=0$, 根据式(8), 有:

$$P[ACK|H_0]=(1-P_{\text{drop}})^{2(k-i)+1} \quad (9)$$

$$P[RET|H_0]=1-(1-P_{\text{drop}})^{2(k-i)+1} \quad (10)$$

· 如果 R_i^{s-v} 为自私路径, 根据式(8), 有:

$$P[ACK|H_1]=(1-P_{\text{drop}})^{2(k-i)+1} \times (1-P_{\Pi(\text{selfish})})^2 \quad (11)$$

$$P[RET|H_1]=1-P[ACK|H_1]=1-[(1-P_{\text{drop}})^{2(k-i)+1} \times (1-P_{\Pi(\text{selfish})})^2] \quad (12)$$

综上所述, 根据 R_i^{s-v} 上节点 h_i 的观测值 x_m , 有如下结论。

· 如果 $x_i=ACK$, 根据式(1)、式(9)、式(11), 有:

$$T(i, R_i^{s-v})_n = T(i, R_i^{s-v})_{n-1} \times \frac{P[ACK|H_1]}{P[ACK|H_0]} = T(i, R_i^{s-v})_{n-1} \times (1-P_{\Pi(\text{selfish})})^2 \quad (13)$$

· 如果 $x_i=RET$, 根据式(1)、式(10)、式(12), 有:

$$\begin{aligned} T(i, R_i^{s-v})_n &= T(i, R_i^{s-v})_{n-1} \times \frac{P[RET|H_1]}{P[RET|H_0]} \\ &= T(i, R_i^{s-v})_{n-1} \times \frac{1-[(1-P_{\text{drop}})^{2(k-i)+1} \times (1-P_{\Pi(\text{selfish})})^2]}{1-(1-P_{\text{drop}})^{2(k-i)+1}} \end{aligned} \quad (14)$$

根据式(13)、式(14)及判别式3, 就可以判断路径 R_i^{s-v} 是否为自私路径。

4 模型的评估

运用 NS-2 工具对以上检测方法的精度进行评估。根据以上网络模型的定义, 模型中 P_{drop} 和 $P_{\Pi(\text{selfish})}$ 的具体值以及路径的具体跳数均不能具体指定, 但可给出它们的预估参数值。

4.1 模型的实现

模型的预估参数如下。

- P_{drop} : 根据节点周围网络分组丢失和数据分组转发的情况, 得出 P_{drop} 的预估值。
- $P_{\Pi(\text{selfish})}$: 根据式(5), 由于无法确定路径上自私节点的确切数量 (也就是模型中的 α 值), 所以 $P_{\Pi(\text{selfish})}$ 的值也无法确定。实际上, $P_{\Pi(\text{selfish})}$ 是根据网络目标而设定的网络参数, 是反映网络对自私行为容忍度的参数值, 表示为 $\tilde{P}_{\Pi(\text{selfish})}$, $P_{\Pi(\text{selfish})}$ 的实际值表示为 $\bar{P}_{\Pi(\text{selfish})}$ 。例如, 如果 $\tilde{P}_{\Pi(\text{selfish})}$ 的值被设定为 0.4, 那么网络的目标就是检测 $\bar{P}_{\Pi(\text{selfish})} \geq 0.4$ 的自私路径。这也表明, 网络能够容忍 $\bar{P}_{\Pi(\text{selfish})} \geq 0.4$ 的自私路径。
- 路径的跳数: 节点根据自身的路由表, 可以获取通往路径上某目标节点的跳数, 但是反过来, 从目标节点通往该节点的跳数无法确定。模型作了如下近似估计: 路径的总跳数 = 2 × 前向路径跳数。
- $T(i, R_i^{s-v})$ 的更新: 节点 $h_i \in R_i^{s-v}$ 保存每条活跃路径 R_i^{s-v} (即路由表项未过期的路径) 的评判记录值 $T(i, R_i^{s-v})$ 。每当 h_i 接收到 R_i^{s-v} 上的观测值 x_n 时, 都会对评判记录 $T(i, R_i^{s-v})$ 进行更新。在节点 h_i 的路由表中, 如果 R_i^{s-v} 被更新, 那么 $T(i, R_i^{s-v})$ 的值将会被重置为初始值。因此, 每条路径 $T(i, R_i^{s-v})$ 的评判是独立的。每个节点都保留模型的阈值 A 和 B , $T(i, R_i^{s-v})$ 记录的初始化和更新以及自私路径或正常路径的判别见第 2.2 节。

4.2 评估

本节对模型进行评估, 包括: 根据模型的参数预估值, 评估模型对自私路径和正常路径的检测能力; 对于给定的 $\tilde{P}_{\Pi(\text{selfish})}$, 当 $\bar{P}_{\Pi(\text{selfish})}$ 增大时, 它如何影响检测的精度。为此,

采用两种不同的设置,运用 NS-2 工具进行仿真。

- 第一种设置 $S_1: \tilde{P}_{\Pi(\text{selfish})}=0.4, \bar{P}_{\Pi(\text{selfish})}=0.75$ 。
- 第二种设置 $S_2: \tilde{P}_{\Pi(\text{selfish})}=0.4, \bar{P}_{\Pi(\text{selfish})}=1$ 。

网络由 100 个节点组成,分布在一个 10×10 的网格中,在可通信的范围内,每个节点有 4 个邻居节点(边缘节点和边角节点分别只有 3 个和 2 个邻居节点)。网络负载由恒定比特率的流量生成器产生,每次流量大约产生 200 个数据分组,随机选取数据分组的“源—目标对”。网络运输层采用可靠的 TCP,介质访问标准采用 IEEE 802.11,路由协议采用 AODV。以参考文献[8,9]中定义的真肯定和假否定作为基础,对模型进行评估。评估的依据是:①每个节点的判决结论(H_1 或 H_0);②根据所有节点的判决结论得出的假肯定率和假否定率。两种设置下的模型参数值为: $\alpha=5\%$, $\beta=10\%$ 。根据第 2.1 节所述,阈值 $A=\frac{1-\beta}{\alpha}$, $B=\frac{\beta}{1-\alpha}$, 因此 $A=18, B=10.53$ 。选取 5 种不同的 TCP 网络负载,各运行 30 次,实际得到的假肯定率和假否定率如图 1 所示。

- 假肯定率分析:图 1(a)表明,两种设置 S_1 和 S_2 下的假肯定率的收敛值大约为 3%,且几乎一致。假肯定的发生,是由于重新发送数据分组时,将正常路径错误地检测为自私路径。由于路径实际上是正常

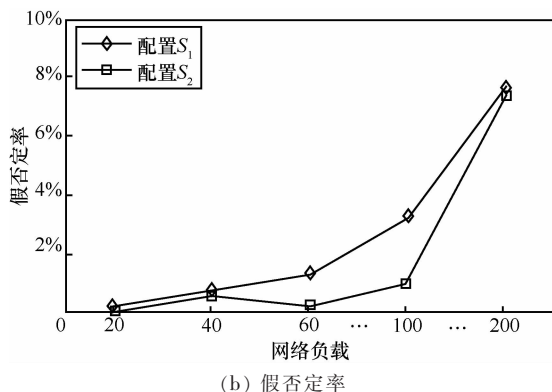
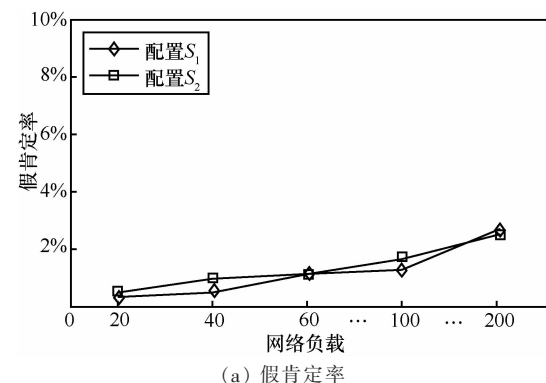


图 1 模型的检测精度

的,所以 $\bar{P}_{\Pi(\text{selfish})}$ 值的大小并不会影响数据分组的再发送。因此,对于给定的 $\tilde{P}_{\Pi(\text{selfish})}$,尽管 $\bar{P}_{\Pi(\text{selfish})}$ 的值不一样,但是假肯定率几乎是一致的。

- 假否定率分析:图 1(b)表明,两种设置 S_1 和 S_2 下的假否定率的收敛值大约为 8%,且随 $\bar{P}_{\Pi(\text{selfish})}$ 的增大而减小。假否定的发生是由于路径上发生 ACK 事件,将自私路径错误地检测为正常路径。随着 $\bar{P}_{\Pi(\text{selfish})}$ 的增大,在自私路径上发生 ACK 事件的概率会随之减小,因此,假否定率也会随之减小。
- 评估结论:仿真结果表明,即使模型参数的估计值存在误差,实际的假肯定率和假否定率仍然分别以 α 和 β 为界,说明这种基于序贯概率比检验的自私路径检测方法具有良好的检测能力;如果给定 $\tilde{P}_{\Pi(\text{selfish})}$,那么检测精度随着 $\bar{P}_{\Pi(\text{selfish})} - \tilde{P}_{\Pi(\text{selfish})}$ 差值的增大而增大。

5 结束语

本文介绍了一种基于序贯概率比检验的检测自私路径的方法,自私节点的检测成效应通过 3 个指标参数来评价:检测率(自私节点被检测出来的成功率)、假肯定率(协作节点被鉴别为自私节点的错误率)、假否定率(自私节点被鉴别为协作节点的错误率)。一种好的检测方式,应该具有较高的检测率以及较低的假肯定率和假否定率。相比于其他检测方法,SPRT 运行更快,且不需要预先确定样本观测值的数量。采用仿真工具 NS-2,验证了这种方法的检测精度。检测自私路径并不能完全消除自私行为带来的影响。如果自私节点(模型参数表示为 P_{selfish})对网络性能产生的不利影响远大于网络环境(模型参数表示为 P_{drop})所产生的不利影响,那么检测和隔离自私节点对网络的生存就显得至关重要,这方面的内容有待以后继续研究。

参考文献:

- [1] DJENOURI D, KHELLADI L, BADACHE N. A survey of security issues in mobile ad hoc and sensor networks [J]. IEEE Communications Surveys & Tutorials, 2005, 7(4): 2-28.
- [2] MICHIARDI P, MOLVA R. Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks[C]//The IFIP TC6/TC11 6th Joint Working Conference on Communications and Multimedia Security, September 26-27, 2002, Portoroz, Slovenia. New York: Springer US, 2002: 107-121.



- [3] 张帅, 张凤斌. 无线传感器网络中基于规范的入侵检测算法研究[J]. 计算机应用与研究, 2012, 29(9): 3464-3466.
ZHANG S, ZHANG F B. Research on intrusion detection algorithm based on specification for WSN [J]. Application Research of Computers, 2012, 29(9): 3464-3466.
- [4] HO J W, WRIGHT M, DAS S K. Distributed detection of mobile malicious node attacks in wireless sensor networks [J]. Ad Hoc Networks, 2011, 10(3): 512-523.
- [5] RONG Y, LEE S K, AND CHOI H A. Detecting stations cheating on backoff rules in 802.11 networks using sequential analysis [C]//IEEE INFOCOM '06, April 23-29, 2006, Barcelona, Catalunya, Spain. New Jersey: IEEE Press, 2006: 1-13.
- [6] RADOSAVAC S, BARAS J S, KOUTSOPOULOS I. A framework for MAC protocol misbehavior detection in wireless networks [C]//The 4th ACM Workshop on Wireless Security, September 2, 2005, Philadelphia, PA, USA. New York: ACM Press, 2005: 33-42.
- [7] 陈波, 毛剑琳, 郭宁, 等. 基于 K -means 算法的无线传感器网络节点自私行为检测方法 [J]. 系统仿真学报, 2014, (3): 580-585.
CHEN B, MAO J L, GUO N, et al. Detection method for selfish behavior of wireless sensor networks nodes based on K -means algorithm[J]. Journal of System Simulation, 2014(3): 580-585.
- [8] 王骐, 蔡子元, 范慧璞. 一种检测被捕获节点的基于异常的算法研究[J]. 压电与声光, 2014, 36(6): 1030-1034.
WANG Q, CAI Z Y, FAN H P. Research on an anomaly-based intrusion detection algorithm for compromised nodes in wireless sensor networks[J]. Piezoelectrics & Acoustooptics, 2014, 36(6): 1030-1034.
- [9] 王骐, 王殊, 孟中楼. 无线传感器网络中一种基于能效的入侵检测算法 -3N 算法研究[J]. 微电子学与计算机, 2010, 27(4):

153-157.

WANG Q, WANG S, MENG Z L. Research on energy-efficiency intrusion detection algorithm (3Nalgorithm) in wireless sensor networks[J]. Microelectronics & Computer, 2010, 27(4): 153-157.

[作者简介]



王骐(1970-),男,博士,湖北第二师范学院副教授,主要研究方向为无线传感器网络安全、嵌入式系统应用。



王青萍(1980-),女,博士,湖北第二师范学院副教授,主要研究方向为光电功能材料与器件。



王怀兴(1977-),男,博士,湖北第二师范学院讲师,主要研究方向为虚拟仪器技术。

肖正安(1974-),男,湖北第二师范学院讲师,主要研究方向为数字信号处理。