doi: 10.7690/bgzdh.2016.04.013

一种分簇无线传感器网络入侵检测算法

刘向阳
（蚌埠汽车士官学校司训勤务系，安徽 蚌埠 233011）

摘要：为检测出无线传感器网络（wireless sensor network，WSN）被非法入侵而遭到毒化的节点，借鉴分布式系统的思想，将 Lamport 算法引入 WSN 入侵检测领域，提出一种基于分簇的无线传感器网络入侵检测算法，并对算法的几种情况进行说明。分析结果表明：该算法能在一定程度上检测出毒化节点，降低 WSN 系统的风险，提高其安全性和容侵性。

关键词：无线传感器网络；入侵检测；网络安全
中图分类号：TP212 **文献标志码**：A

An Intrusion Detection Algorithm for Clustering Wireless Sensor Network

Liu Xiangyang
(*Department of Driver Training & Service*, *Bengbu Automobile Petty Officer School*, *Bengbu* 233011, *China*)

Abstract: In order to detect the illegal invasion nodes in wireless sensor network (WSN), borrowing ideas from distributed systems, Lamport algorithm is introduced into WSN intrusion detection field, and puts forward an intrusion detection algorithm for the clustering WSN, then the applications of the algorithm are described. The results show that the proposed algorithm can detect malicious nodes, reduce the risk of WSN system, and improve its security and intrusion tolerance.

Keywords: wireless sensor network; intrusion detection; network security

0 引言

近年来，随着无线通信、集成电路、嵌入式计算及微机电系统等技术的发展和日益成熟，具有感知、计算和通信能力的微型无线传感器被广泛应用于军事斗争、国家安全、环境监测、交通管理、医疗卫生、制造业和反恐抗灾等领域[1]。

无线传感器网络（wireless sensor network，WSN）通常由成百上千个传感器节点组成，使用自组织方式进行通信。WSN 通常被部署在一些重要区域，通过运行关键程序来收集重要数据信息，比如在战场上 WSN 被用来监测获取敌方情报信息等。由于 WSN 本身具有的开放无线链路、节点受体积限制等问题，加之网络往往被用于军事、国家安全等领域，使得 WSN 会成为敌人破坏的重要目标，导致敌人会采取各种不同方法对 WSN 进行干扰、破坏，网络中某些节点很容易被非法入侵而遭到毒化。如何检测出被毒化的节点，并采取行之有效的措施保证网络的安全，就显得十分重要。基于此，笔者提出了一种基于分簇的无线传感器网络入侵检测算法，在一定程度上能检测出毒化节点。

1 分簇无线传感器网络模型假设

为了方便研究，对分簇无线传感器网络模型作以下假设：

1) 节点被随机撒落在监测区域内，以自组织形式构成网络，整个网络由簇首节点、簇成员节点（普通节点）、网关节点和基站组成，分簇结构见图 1。

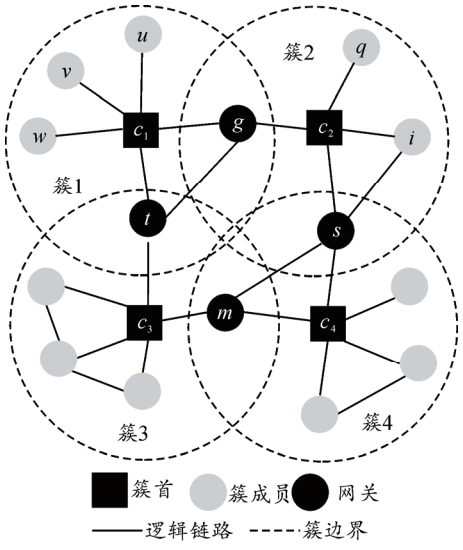

图 1 无线传感器网络分簇结构

收稿日期：2015-12-05；修回日期：2016-01-23
作者简介：刘向阳（1979—），男，陕西人，硕士，讲师，从事无线传感器网络、网络安全等研究。

2) 节点之间是对等的，并需要通过簇首节点与基站之间进行通信。

3) 网络的动态拓扑结构变化不大，节点配置好后位置相对固定。

4) WSN 采用基于簇的路由协议，比如 LEACH 协议等，使用随机公平的簇首选举算法，周期性地重新选举簇首节点[2]。

5) 网络初始化时，网络中的所有节点(包括簇首节点)在供电、计算、存储和通信等方面的能力都是相同的，并且是受限的。基站的能量不受限制，且具有较强的计算、存储能力。基站的信息是安全的[3]。

6) 入侵检测分为簇内检测和簇首间检测。簇内检测时，由簇首向每个节点发送一个不相同的随机数。各个节点之间相互转发这个随机数，并按照本文中提出的入侵检测算法修改各自的可信度列表，同时将检测向量发给簇首。簇首更新自己的可信度列表，对可疑毒化节点进行监控；簇首间检测时，由基站向相应的簇首发送一个不相同的随机数。各个簇首之间相互转发这个随机数，按照本算法修改各自簇首的可信度列表，同时将检测向量发给基站。基站更新自己的可信度列表，对可疑毒化簇首进行监控[4]。

7) 每个节点都有自己的可信度列表，用于记录自己和周围其他节点的可信度(可信度记作 C，$0 \leqslant C \leqslant 1$)。初始情况下，自己及其邻居节点的可信度为 1，每入侵检测一次，就更新一次可信度表，一旦某个节点或簇首的可信度低于可信度阈值α，该节点或簇首即被视为毒化节点，其他节点、基站立即切断与其通信，并对其进行相应的监控[5]。其中，α为可信度阈值，大小视实际应用中对网络的安全性要求的高低而定，安全级别要求越高，阈值就越大，但考虑到入侵检测的可用性，一般取 $0 < \alpha < 0.5$。

2 入侵检测算法描述

本入侵检测算法也称 Lamport 入侵检测算法，它最早由 Lamport 在 1982 年解决拜占庭将军问题时提出，主要用于分布式系统中，现被广泛应用于可信计算等领域[6]。本算法采用递归算法，可以很好地应用于入侵检测领域；因此，笔者将其应用在 WSN 网络安全领域。为了方便研究，笔者只考虑簇内毒化节点的检测、簇间检测和簇内检测。

笔者假设簇内有 4 个节点，其中 C 节点为毒化节点，另外 3 个节点为安全节点，现采用 Lamport 入侵检测迭代算法将该毒化节点从其他安全节点中检测出来。

第 1 步：由簇首向 4 个簇成员节点各发送一个不相同的随机数，为简单起见假设簇首 c_1 向节点 A 发送的随机数为 1，向节点 B 发送的随机数为 2，向节点 C 发送的随机数为 3，向节点 D 发送的随机数为 4，如图 2 所示。

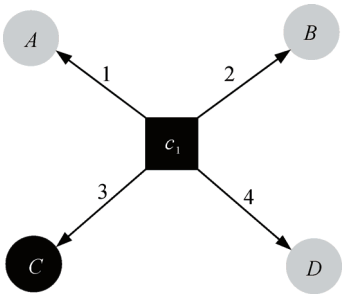

图 2 簇首向簇成员节点发送随机数

第 2 步：$ABCD$ 4 个簇成员节点之间相互发送各自收到的随机数，如图 3 所示。

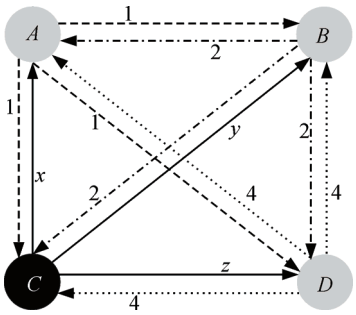

图 3 簇成员节点间相互发送随机数

ABD 3 个节点是安全节点，故向其他 3 个节点发送自己收到的真实随机数；C 为毒化节点，它向其他簇成员节点发送伪造的随机数 x、y、z。

每个簇成员节点都收到来自其他 3 个簇成员节点发送的随机数，加上自己发送的随机数，共 4 个随机数。将这 4 个随机数依次按节点的顺序排列成检测向量。其中节点 A 的检测向量为$(1, 2, x, 4)$，节点 B 的检测向量为$(1, 2, y, 4)$，节点 C 的检测向量为$(1, 2, 3, 4)$，节点 D 的检测向量为$(1, 2, z, 4)$。

第 3 步：每个簇成员节点将各自的检测向量再次分别发送给其他 3 个节点。ABD 3 个簇成员节点是安全节点，向其他节点发送自己真实的检测向量；C 为毒化节点，它向其他节点发送伪造的检测向量

(a, b, c, d)，(e, f, g, h)，(i, j, k, m)。

这样每个簇成员节点都收到其他 3 个节点发来的检测向量，加上自己的检测向量，依次按顺序排列成检测矩阵。

节点 A 的检测矩阵为

$$\begin{pmatrix} 1,2,x,4 \\ 1,2,y,4 \\ a,b,c,d \\ 1,2,z,4 \end{pmatrix}。$$

节点 B 的检测矩阵为

$$\begin{pmatrix} 1,2,x,4 \\ 1,2,y,4 \\ e,f,g,h \\ 1,2,z,4 \end{pmatrix}。$$

节点 C 的检测矩阵为

$$\begin{pmatrix} 1,2,x,4 \\ 1,2,y,4 \\ 1,2,3,4 \\ 1,2,z,4 \end{pmatrix}。$$

节点D的检测矩阵为

$$\begin{pmatrix} 1,2,x,4 \\ 1,2,y,4 \\ i,j,k,m \\ 1,2,z,4 \end{pmatrix}。$$

第 4 步：$ABCD$ 4 个节点通过检查自己所得到的检测矩阵中的第 i 个元素(即检查矩阵的每列)，如果哪个值为多数就把它放在结果向量里。如果不存在结果向量为多数的情况，那么结果向量中对应的元素被标记为 unknown。通过检查得知 4 个结果向量均为(1, 2, unknown, 4)，则可疑毒化节点 C 被检查出来。

第 5 步：每个安全节点将被检查出来的可疑毒化节点的可信度降低 r(其中 r 为信任度降低百分率，$0<r<1$)，并更新自己的可信任度表，对于小于可信度阈值α的邻居节点视为毒化节点，切断与其进行的通信活动。同时将结果向量发送给簇首，簇首修改自己的可信度列表，减少与可疑毒化节点的通信，同时监视可疑节点，适时切断与毒化节点的通信。

3　算法的几种情况说明

1) 该算法必须保证 2/3 以上的节点是安全节点，否则算法失效；

2) 使用该算法对 WSN 进行分簇时，必须保证簇内有 4 个以上节点，当簇内仅有 3 个以下(含 3 个)节点时，无法使用本算法[7]；

3) 簇首间入侵检测，其基本思想和簇内入侵检测算法基本思想完全相同，可依照簇内检测算法 5 个步骤依次进行。

4　结束语

无线传感器网络入侵检测研究是 WSN 中的一项重要内容。笔者提出了一种基于分簇的无线传感器网络的 Lamport 入侵检测算法，在一定程度上能检测出毒化节点，降低 WSN 系统的风险，提高 WSN 系统的安全性和容侵性。该算法可能带来额外的通信开销，特别是随着簇内节点个数的增加，通信开销也有所增加。如何降低通信开销，是下一步研究的一项重要内容。

参考文献：

[1] 孙利民. 无线传感器网络[M]. 北京: 北京清华大学出版社, 2005: 11.

[2] Heinzelman WR, Chandrakasan A, Balakrishnan H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks[C]. Havaii: In Proceedings of the Havaii International Conference on System Sciences, 2000: 4-5.

[3] 周贤伟. 无线传感器网络与安全[M]. 北京: 国防工业出版社, 2007: 130.

[4] 刘阳. 基于免疫原理的无线传感器网络入侵检测系统研究[D]. 北京: 中科院研究生院, 2008: 15-16.

[5] 蒋元曦, 赵保华. 无线传感器网络路由协议中的恶意节点发现和定位机制[J]. 合肥中国科技大学学报, 2008, 38 (3):235-240.

[6] Andrew S. Tanenbaum.分布式系统:原理与范例[M]. 北京:清华大学出版社, 2006: 373-375.

[7] 刘吕亮, 石照耀, 张敏, 等. 电感位移传感器结构特性研究[J]. 机电工程, 2014, 31(6): 684.