文章编号:1673-0062(2009)01-0072-04

基于J-Sim的无线传感器网络拥塞攻击应对方法研究

邹 旸,陈志刚

(中南大学 信息科学与工程学院,湖南 长沙 410008)

摘 要:阐述了无线传感器网络可能遭受到的攻击及J-Sim仿真平台,针对无线传感器网络物理层的拥塞攻击,提出了一种拥塞攻击行为判断算法和跳频实施策略.仿真结果表明,该方法可以有效应对拥塞攻击.

关键词:无线传感器网络;J-Sim;安全性;拥塞攻击;仿真

中图分类号:TP393.08 **文献标识码**:A

Research on Methods Dealing with Congestion Attack of WSN Based on J-Sim Platform

ZOU Yang, CHEN Zhi-gang

(School of Information Science and Engineering, Central South University, Changsha, Hunan 410008, China)

Abstract: This paper introduces the possible attack of WSN(Wireless Sensor Networks) and the J-Sim platform. Then, a congestion attack judgment algorithm and changing-frequency policy is proposed. The simulation results show that our method can effectively deal with the congestion attack.

Key words: WSN; J-Sim; security; congestion attack; simulation

无线传感器网络一般部署在广阔的区域内,存在收到无关人员或者敌方人员破坏的可能性;无线电通信信号在物理空间上是暴露的,任何设备,只要调制方式、频率、振幅、相位都和发送信号匹配,就可以获得完整的通信信号.无线传感器网络开放性及广播特性使传感器网络节点的部署变得容易和高效,但同时也带来了安全隐患,如信息泄露、空间攻击等[1].

事实上,无线传感器节点协议栈的每一层都可能遭受到攻击[2].物理层会受到拥塞攻击和物理破坏,攻击节点通过发送无用信号或修改物理节点去干扰或破坏无线通信网络的正常通信.数据链路层容易受到碰撞攻击[3]、耗尽攻击和非公平竞争攻击等,恶意节点通过不停的发送碰撞包、与受攻击节点持续通信、不断发送高优先级的数据包占据信道等方式,使网络其它节点失效或在

收稿日期:2009-02-17

作者简介:邹 旸(1984-)男,江西安福人,中南大学信息科学与工程学院硕士研究生.主要研究方向:无线传感器网络.

通信中处于劣势. 网络层的攻击有丢弃和贪婪破坏攻击、方向误导攻击、汇聚节点攻击和黑洞攻击等. 当恶意节点加入到网络中后,它会故意丢弃一些数据包,或将自己的数据包设为很高的优先级发送,从而破坏网络通信秩序;或者在收到一个数据包后,选择一条错误的路径发送出去,从而破坏网路的路由;或者攻击在网络中具有非常重要的作用的汇聚节点,给网络造成比较大的威胁;恶意节点也可通过发送 0 距离公告,误导其周围的节点把所有的数据包都发送给恶意节点,从而在网络中形成一个路由黑洞.

1　J - Sim 仿真平台

J - Sim 是一个开放源码,基于组件合成的仿真平台,它使用 Tcl/Java 结合的双重语言环境. J - Sim 定义了抽象的网络模型,其中包括基本的系统结构和网络协议的组件,新的协议和算法则可以通过扩展基本类库来实现. 在不同的网络场景之下采用"即插即用"的组件叠加方式就可以构建出所需要的仿真环境和网络协议栈,如无线传感器网络[1]. J - Sim 以自治组件架构(ACA)为基础,为无线传感器网络仿真提供了广泛的、基本的组件(类/子类库),使用 TCL 脚本语言就可以将组件组合在一起来构建我们需要的仿真场景.

J - Sim 仿真是通过执行线程表来实现. 仿真运行开始,先构建各节点,随后目标节点开始生成监测数据,目标节点将监测数据选择发送给最佳的传感器节点,传感器节点获得数据后在汇聚节点分配的时隙内将数据上传. 仿真流程如图 1 所示.

2　拥塞攻击应对方法

随着无线传感器网络规模日渐扩大,层次化结构逐渐在传感器网络结构中占主导地位. 层次化网络结构采用层次化路由协议[4-5],即将所有节点分为若干簇,每个簇选举一个节点做为簇头,簇头收集簇内其它节点的数据,转发给汇聚节点. 在分簇的网络中,MAC 层一般采用 CSMA 机制和 TDMA[6] 机制相结合的 CSMA/TDMA MAC 协议,即簇内节点通信采用 TDMA 机制,簇头之间通信采用 CSMA/CA 机制.

2.1　攻击行为判断

对于任何一种网络干扰,首先要判断其是否是恶意的攻击. 本文监测网络攻击的算法只针对拥塞攻击,通过定期监测网络的状态,确定网络是否受到攻击.

首先,在簇头中定义变量 Delay_time、Total_Node_Number、New_Node_Number、Rate. Delay_time 控制簇头监测网络的状态;Total_Node_Number 和 New_Node_Number 分别记录了簇头在连续两次监测网络状态的前次和后次的簇内节点总数. Rate 代表一个阈值,即当(New_Node_Number/Total_Node_Number) < Rate,认为网络正在受到攻击.

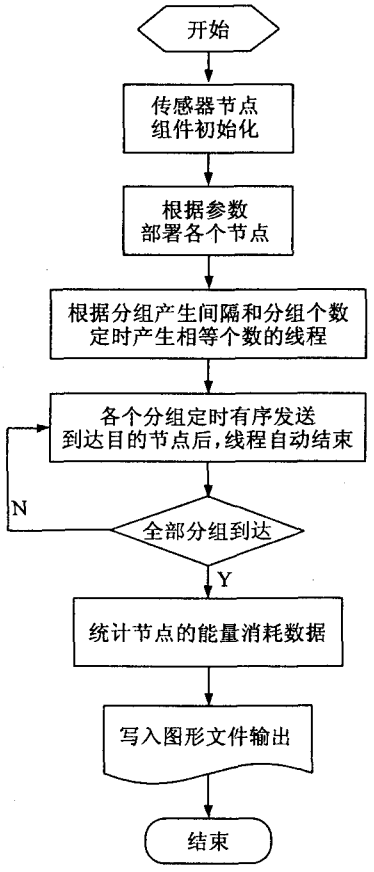

图 1　仿真流程

Fig. 1　Simulation flow

如果在 time 时间内,簇头无法联系到的节点超过一定比率 rate 时,则认为该簇遭受到拥塞攻. 判断攻击行为的算法如下:

1)簇头发送 ACK 广播包获取当前节点总数 Total_Node_Number;

2)延迟 Delay_time 秒;

3)重新发送 ACK 广播获得当前节点数 New_Node_Number;

4)判断是否受到攻击. 如果 (New_Node_

Number/Total_Node_Number) < Rate,则认为当前网络受到攻击,执行第 5 步;否则,Total_Node_Number = New_Node_Number,回到第 2 步.

判断流程如图 2 所示.

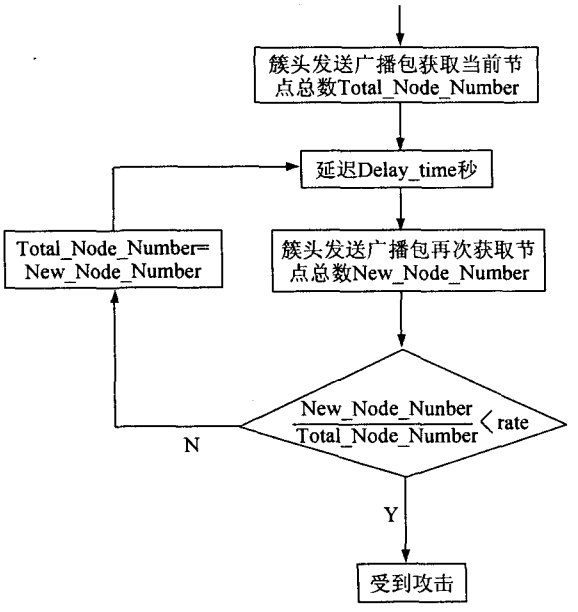

图 2 拥塞攻击判断

Fig. 2 Congestion attack judge

2.2 跳频实施

跳频实施就是当簇头判断网络遭受攻击时,发出控制包改变簇内节点的通信频率,使簇内节点跳到一个没有受到干扰的信道继续通信,这样,网络将不再遭受恶意节点攻击,攻击节点会随着其能量的耗尽而失效.

每个无线传感器网络节点都有多个备用的信道,当判断到节点所在的簇遭受到拥塞攻击时,簇头和簇内节点全部跳频,跳到预先定好的下一信道进行通信. 对于簇内单个节点,如果在一定时间内一直没有与簇头通信,则自动启动跳频机制,跳到一个新的频率与簇头通信.

簇头向簇内所有节点广播跳频控制帧,通知簇内所有节点跳到下一频率进行通信. 簇内节点收到跳频控制帧后,只要重写无线收发芯片的信道控制寄存器即可改变通信频率. 对于正在遭受到攻击的节点,无法收到簇头的跳频通知时,它会在有限的时间内自动跳到下一频率与簇头通信,如果在该频率仍无法找到簇头,将再次跳率,直到找到簇头为止.

3 仿真结果与分析

3.1 仿真场景设定

由 J-Sim 仿真平台生成 40 个传感器节点和 2 个目标节点,通过网络初始化,最终形成 38 个传感器节点,1 个汇聚节点、2 个目标节点以及 1 个攻击节点,分布在一个 550 m × 550 m 的区域内,其网络拓扑结构如图 3 所示. 每个节点的通信半径是100 m,确保了传感器节点与汇聚节点之间可以通信. 此外,在仿真过程中,假定全部节点都是静止的.

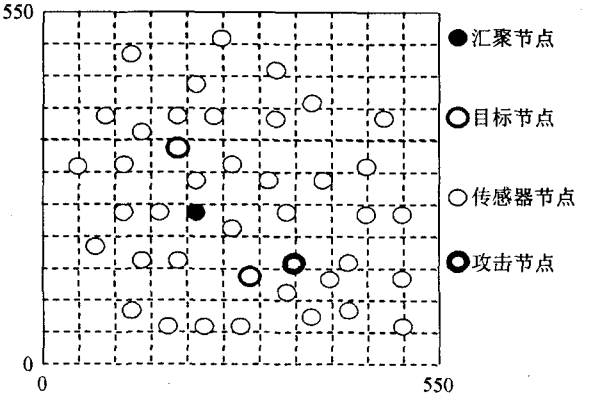

图 3 仿真场景

Fig. 3 Simulation scenarios

3.2 仿真结果与分析

在仿真实验中,将 delay_time 定义为 5 分钟,Rate 定位 10%. 备用频道为 3 个,且 3 个频道拉开一定频距[7]. 增加了一个攻击节点,攻击节点持续向无线信道发送垃圾信息,进行拥塞攻击,随着攻击节点自身能量的消耗殆尽,攻击行为结束.

从图 4 可以看出,在受到攻击时,汇聚节点和目标节点之间的信噪比突然下降到很低,表明受到攻击时,汇聚点收到的有效信息非常少,随着簇头和簇内各传感器节点陆续转换频率后,网络通讯也逐步恢复正常.

在遭受攻击期间,从图 5 可以清晰地看到三类节点的能量消耗情况:缓慢消耗的簇内节点(节点 1,蓝色线条;节点 3,青绿色线条)、下降消耗的簇头节点(节点 2,黄色线条)以及急剧消耗的攻击节点(节点 4,墨绿色线条). 簇头节点在遭受攻击时,能量消耗比平时下降得快一些,这是由于簇头节点一直处于活动状态,大量接收到垃圾信息而导致,但很快簇头节点判定攻击行为发生,转换频率,恢复正常.

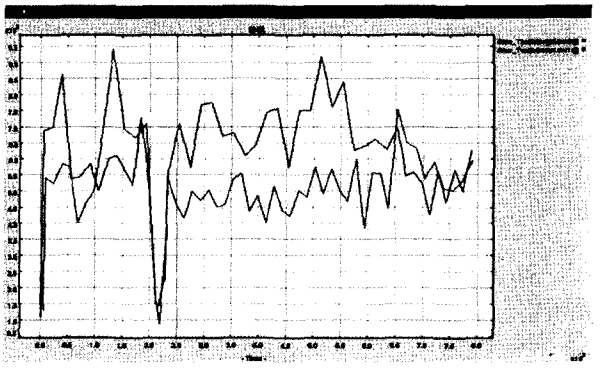

图 4　汇聚节点和目标节点之间的信噪比

Fig. 4　The signal - noise ratio between cluster node and the target node

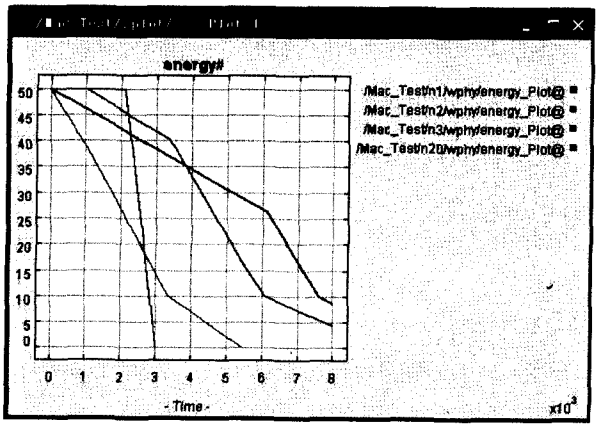

图 5　部分节点能耗输出图

Fig. 5　Energy exhaustion output diagram of part of nodes

4　总结

随着微电子技术的不断发展,无线传感器网络应用将越来越广泛.与此同时,无线传感器网络的底层安全问题也将引起更多的关注.跳频是防范拥塞攻击非常有效的手段,本文给出的拥塞攻击行为判断算法和跳频实施策略可以更准确、更高效、更及时和更容易地应对和处理拥塞攻击行为,保障无线传感器网络的底层安全.

参考文献:

[1] 孙利民,李建中,陈　渝,等.无线传感器网络[M].北京:清华大学出版社,2005.

[2] Wood A D, Stankovic J A. Denial of Service in Sensor Networks[J]. IEEE Computer, 2002, 35(10): 54 - 62.

[3] 陈　洋,龚建荣.无线传感器网络安全研究[J].中国新通信(技术版),2008(7):38 - 42.

[4] Heinzelman W, Chandrakasnan A, Balakrishnan H. Energy - eficient communication protocol for wireless microsensor networks[C]//Maui, Hawaii: Proc ofthe Hawaii International Confe. rence on System Sciences, 2000:3005 - 3014.

[5] Younis O, Fahmy S. HEED: A hybrid, energy - eficient, distributed clustering approach for Ad Hoc sensor networks[J]. IEEE Tran - sactions on Mobile Computing, 2004, 3(4):366 - 379.

[6] Arisha K A, Youssef M A, Younis M F. Energy - Aware TDMA - based MAC for sensor networks[C]//Proc. of the IEEE Workshop on Integrated Management of Power Aware Communications. New York: Computing and NeTworking, 2002:69 - 74.

[7] 高章飞,蒋正义,朱善安.基于多信道跳频的 Ad Hoc 网络 MAC 层协议研究[J].自动化仪表,2005,26(12):5 - 8.