A Detection Scheme of Clone Attack Based on Clustering in Wireless Sensor Networks*

LUO Yongjian, *CHEN Tao*, *XIAO Fugang*, *SHI Deyang*
(*Xi'an Communications Institute*, *Xi'an* 710106, *China*)

Abstract: Since wireless sensor networks facing with node clone attacks, a detection scheme based on clustering is proposed. All the messages are marked on the source node's ID in the scheme, the cluster-heads judge whether there is cloned node in each cluster according to nodes' ID and RSSI in clustering phase, and then all nodes' ID are delivered to the Sink node. The Sink node detects whether there are abnormalities, namely the same ID belongs to multiple clusters by the fact that each cluster is a disjoint subset in clustering algorithm. Simulation results show that the proposed scheme not only has higher detection rate, but also reduces the storage and communication costs of network.

Key words: wireless sensor networks; node clone attack; clustering algorithm; attack detection
EEACC: 7230; 6150P **doi**: 10.3969/j.issn.1004-1699.2014.02.015

基于分簇的无线传感器网络克隆攻击检测方案*

罗永健*, 陈 涛, 肖福刚, 史德阳
(西安通信学院, 西安 710106)

摘 要: 针对无线传感器网络面临的节点克隆攻击, 提出了一种基于分簇的检测方案。该方案给网络中的消息都标记上其源节点的 ID, 在成簇阶段依据节点 ID 和 RSSI 值由簇头判断各个簇内是否存在克隆节点, 待全部节点的 ID 汇聚至基站后, 利用分簇算法中各个簇是不相交的子集这一特点, 在基站处检测是否存在同一个 ID 属于多个簇的异常情况。仿真实验表明, 该方案不但有较高的检测率, 还能降低网络的存储和通信开销。

关键词: 无线传感器网络; 分簇算法; 节点克隆攻击; 攻击检测
中图分类号: TP393 **文献标识码**: A **文章编号**: 1004-1699(2014)02-0220-05

无线传感器网络具有廉价、自组织的性质, 在战场环境监视、故障诊断、生物医学、家庭安全及智能空间等领域有着广泛的应用前景[1], 但无线传感器网络的无人照管操作使得传感器节点易于被敌方物理性地控制[2], 面临着较为严重的安全威胁。而无线传感器网络面临的各种攻击中, 以节点克隆攻击的危害尤为巨大。在节点克隆攻击中, 攻击者通过俘获网络中一个或多个节点, 提取出节点中的私密信息, 如节点身份标识(ID)、用于与其他节点建立安全信道的密钥等, 利用这些信息复制出无限数量的具有相同 ID 和私密信息的节点, 并将这些克隆节点投放到网络中[3]。因为克隆节点拥有合法的身份信息, 它可以作为正常节点参与网络操作, 肆意地发起对整个网络的攻击[4], 例如往网络中注入错误数据、利用克隆节点分隔网络以及破坏网络中其他协议等等。因此, 对节点克隆攻击检测的研究具有重要意义。

节点克隆攻击检测方案主要分为两类: 集中式的检测方案和分布式的检测方案[5]。集中式的检测方案利用基站资源丰富的特点, 把普通节点收集到的相关信息都传递到基站处, 由基站运行检测算法对收到的信息进行处理, 判断有无克隆攻击。例如, 文献[6]提出的检测方案中, 每个节点把自己的邻居列表以及位置信息发送给基站, 由基站来检测有无克隆节点; 文献[7]中每个节点依据自身的邻居信息按照一定规则产生一个指纹信息, 并传递此

项目来源: 国家自然科学基金项目(61179002, 61102106); 陕西省自然科学基础研究计划项目(2011JM8030)
收稿日期: 2013-11-20 **修改日期**: 2014-01-13

指纹信息到基站,由基站通过节点指纹信息和 ID 号检测异常;文献[8]中每个节点记录自己密钥的使用次数并告知基站,如果节点密钥使用次数大于设定的阈值,则判定该节点为克隆节点。集中式的检测方案能够实现较高检测率,但节点直接向基站发送消息导致距离基站近的节点能耗较小,而距离基站远的节点能耗较大,网络中节点能耗不均衡,且网络分布区域较大时,受无线传感器节点通信距离的限制,距离基站较远的节点的难以直接同基站通信。

分布式的检测方案又分为随机性和确定性检测方案。随机性检测方案是指节点在每轮检测过程中的验证节点不是固定的[9],文献[6]中提出的随机多播和 LSM(Line-Selected Multicast)属于随机性分布式检测方案。在随机多播算法中,每个节点的位置信息被发送到网络中随机选取的多个验证节点,如果网络中存在克隆节点,根据生日悖论,至少有一个验证节点收到两个冲突的位置信息是一个高概率事件。LSM 算法对随机多播算法进行了改进,每个节点减少了随机选取的验证节点的数目,但在位置信息转发路径上的节点记录下位置信息,成为验证节点,该方案与随机多播相比降低了通信复杂度。徐军在文献[3]中提出的两种基于随机种子的检测方案 RS-Ⅰ(Random Seed-Ⅰ)和 RS-Ⅱ中,节点通过 ID 和随机种子计算出验证节点,每轮的验证节点不发生变化,属于确定性分布式检测方案。如果网络中存在克隆节点,将在验证节点处检测到冲突信息。分布式的检测方案容易组织实施,但网络中每个节点都要参与检测,检测信息被收发多次,通信开销和存储开销都很大。

本文提出的基于分簇的检测方案是一种特殊的集中式检测方案,能够克服一般的集中式检测方案的不足。该方案首先在局部检测克隆攻击,即由每个簇头检测它的簇内是否有克隆节点,待全网节点的 ID 汇聚至基站后,由基站检测是否存在单个 ID 出现在两个或多个簇里的情况。该方案具有集中式检测方案检测率高的优点,同时利用了分簇算法的数据传输机制,能够降低通信开销和存储开销。

1　网络模型

考虑有 N 个无线传感器节点随机分布在一个面积为 $L\times L$ 的正方形区域 A 内。模型假设如下:

(1)所有节点的功能相同,具备数据融合的功能,每个节点都有唯一的 ID。

(2)网络中只有一个基站,且是永久可信的,无线传感器节点和基站在部署后不再发生移动。

(3)对于不同距离的接收者,节点可以自由调整其发射功率以减小能量消耗。

(4)链路是对称的,若已知对方发射功率,节点可以根据接收信号的强度 RSSI(Received Signal Strength Indicator)[10]计算出发送者到自己的近似距离。

(5)无线通信是加密的。通过加密认证机制,接收方能够确认数据是否来自发送方,传输过程中是否受到篡改。

文中采用与文献[12]相同的传输能量消耗模型。数据发送能量消耗由发射电路损耗和功率放大损耗两个部分组成,即

$$E_{TX}(l,d)=\begin{cases} lE_{elec}+l\varepsilon_{fs}d^2 & d<d_0 \\ lE_{elec}+l\varepsilon_{mp}d^4 & d\geqslant d_0 \end{cases}$$

其中,l 表示发送的比特数,d 表示发送距离,ε_{fs} 和 ε_{mp} 表示自由空间模型和多路径衰减模型下功率放大所需的能量,d_0 为判断采用自由空间模型或多路径衰减模型的临界点。数据接收消耗的能量为 $E_{RX}(l)=lE_{elec}$。

无线传感器网络运行分簇算法,被分成多个簇。无线传感器网络中的分簇算法是为了均衡节点能耗,延长网络寿命而设计。它把整个网络中的节点分入不同的簇,每个簇通常选举一个称为簇头的管理节点,对簇内节点进行管理维护,并周期性进行簇头轮换和簇重组,能有效延长无线传感器网络寿命[11]。LEACH(Low-Energy Adaptive Clustering Hierarchy)算法[12]是最早被提出的分簇算法,它是由 W. R. Heinzelman 在 2000 年的一次会议上提出,图 1 为 LEACH 分簇算法拓扑结构示意图。目前,已有大量的分簇算法被提出,其在无线传感器网络中的应用也越来越广。

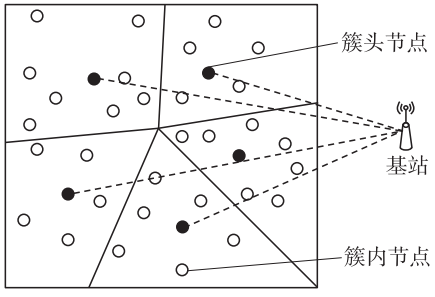

图 1　LEACH 分簇算法拓扑结构图

2　方案设计

分簇算法中一个节点只能属于一个簇,该特点有利于判断网络中是否有 ID 重复的节点。本文的克隆攻击检测方案正是基于分簇算法的这种特点,

对网络中产生的消息都标记上其源节点 ID,然后依次在分簇算法成簇阶段和基站处检测是否存在克隆节点。

簇内节点向簇头传输数据时采用时分复用策略,簇头会给每个簇内的节点分配时隙,所以一个节点只能属于一个簇,各个簇的交集为空。假设 S 为网络中节点的集合,C_1、C_2、$\cdots C_{n-1}$、C_n 表示各个簇中节点的集合(包括簇头和簇内节点),n 表示簇的数目,则有式(1)、式(2)成立。

$$S=C_1\cup C_2\cdots C_{n-1}\cup C_n \tag{1}$$

$$C_1\cap C_2\cdots C_{n-1}\cap C_n=0 \tag{2}$$

若网络中存在克隆节点,当它们不在同一簇内时,则会出现式(3)情况。

$$C_1\cap C_2\cdots C_{n-1}\cap C_n\neq 0 \tag{3}$$

本文的检测方案基于分簇的机制,但不限定具体的分簇算法,因为在实际应用中,可以根据网络的规模选取合适的分簇算法。

文中方案的具体步骤如下:

(1)对网络中生成的所有消息都标记上其源节点的 ID。

(2)在分簇算法成簇阶段,通过判断 RSSI 和 ID 是否一致来检测克隆节点。在分簇算法中,成为簇头的节点广播其当选簇头的通告消息,非簇头节点至少会收到一个簇头的通告信息。选择相应的簇头组簇时,非簇头节点会向该簇头发送通告消息,簇头就可以通过其簇内节点发来的消息来检测簇内是否存在一个 ID 号有多个 RSSI 值的情况。倘若在此阶段不做检测,会使检测方案存在漏洞,因为当节点与其克隆节点在一个簇内时,簇头会把二者当作同一个节点,从而给二者只分配一个时隙,而利用该时隙的很可能是克隆节点。成簇阶段的检测是局部区域小范围的检测,节点与其克隆节点距离较近时才能够检测出来。

(3)簇头对其 ID 和簇内节点 ID 以图 2 形式进行整理后,同数据一起被传送至基站。基站从全局角度对网络中的 ID 进行检测,由于每个节点只能属于一个簇,如果网络不存在克隆攻击,就不会出现一个 ID 号出现在两个或多个簇内的情况,各个簇中节点的集合满足式(2)。

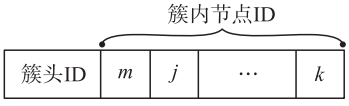

图 2 节点 ID 信息的组织形式

该方案在分簇算法的基础上展开,具体流程如图 3 所示。

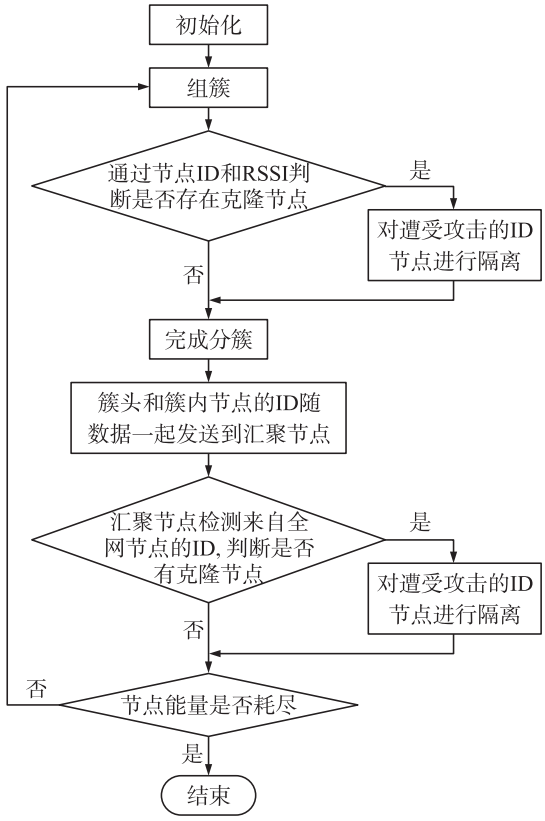

图 3 本文检测方案的流程图

3 新方案性能分析

通过与 LSM 算法及 RS-Ⅱ算法相比较,本节从理论分析和仿真实验两个方面来分析文中方案的性能。其中,N 表示无线传感器网络中的节点数目,g 表示节点的邻居节点数目。

3.1 理论分析

新方案的通信和存储开销与 LSM 算法以及 RS-Ⅱ算法的比较如表 1 所示,其中通信和存储开销均表示单个节点的开销。由于无线传感器节点的大部分能量用于节点间通信,文中检测方案的通信开销又小于另外两种算法,所以本文方案在能量受限的无线传感器网络中适用性更强。文中检测方案的存储开销因分簇算法的不同会略有差别,一般簇头的存储开销会略大,如果网络中簇头数目为 c,则每个簇头的平均存储开销为 N/c,多数分簇算法里 c 也是 N 的函数,所以存储开销量级仍为 $O(1)$。视簇头产生方法的不同,非簇头节点的存储开销也不同,若簇头是随机产生(如 LEACH 算法),则非簇头节点的存储开销为 $O(1)$;若簇头是通过各节点信息交互后选举产生(如 HEED 算法),则非簇头节点的存储开销为 $O(g)$。

表 1　本文方案与 LSM 算法、RS-Ⅱ算法开销的理论界限比较

协议	通信开销	存储开销
LSM 算法	$O(\sqrt{N})$	$O(\sqrt{N})$
RS-Ⅱ算法	$O(\sqrt{N})$	$O(g)$
本文方案	$O(1)$	$O(g)$或 $O(1)$

3.2　仿真实验

仿真使用 MATLAB 软件,参数设置为 $L=200$ m,节点初始能量 $E=0.5$ J,$\varepsilon_{fs}=10$ pJ/bit/m^2,$\varepsilon_{mp}=0.001\ 3$ pJ/bit/m^4,d_0 为 88 m,E_{elec}值为 50 nJ/bit。

本文方案基于 LEACH 分簇算法运行,LEACH 分簇算法簇头生成的概率 p 等于 5%。

LSM 算法和 RS-Ⅱ算法中每个地理位置消息大小为 46 byte,其中数字签名为 40 byte,ID 需要 2 byte,地理位置信息占用 4 byte,本文方案不需要节点的地理位置信息,检测消息大小为 42 byte。LSM 算法和 RS-Ⅱ算法的参数分别与文献[3,6]中相同,节点的平均邻居节点个数都为 40 个,检测消息的 TTL(Time to Live)同为$\sqrt{N}$,邻居节点转发检测消息的概率分别为 $6/g$ 和 $3/g$。

(1)存储开销比较

本文方案中簇内节点只需存储其所在簇簇头的信息,存储开销很小,而簇头节点需要存储全部簇内节点的 ID 和 RSSI 值(RSSI 值占用 2 byte),簇头节点被占用的存储空间在 4 byte·$(1/p)$左右。文中以节点可能的存储开销的较大值—簇头节点的存储开销来衡量本文方案的性能。图 4 反映了各方法中相应节点存储的字节数目,本文方案中簇头的平均存储开销较小。因为 LSM 算法中,每个转发节点都要存储验证消息的 ID 和地理位置信息,且随着网络中节点数目的增多,存储的检测消息的数目也逐渐增大。而 RS-Ⅱ算法中每个节点平均有 $g+1$ 个验证节点,g 的平均大小为 40,所以,平均每个节点存储的检测消息在 240 byte 左右。

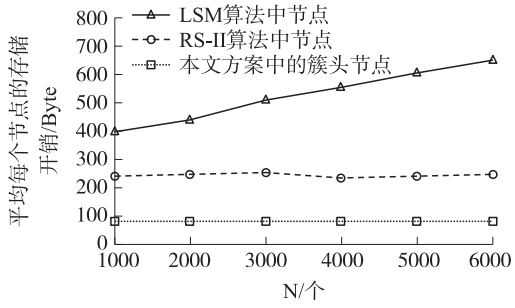

图 4　3 种方法中相应节点的存储开销比较

(2)通信开销比较

由于无线通信消耗掉传感器节点的绝大多数能量,本文通过比较各方法的检测次数与存活节点数目的关系,来间接反映各方法每次检测的通信开销大小。在 $N=1\ 000$ 的情况下,假设网络中不进行数据的收集,只发送和接收攻击检测消息,图 5 为各方法运行次数与存活节点个数的关系。

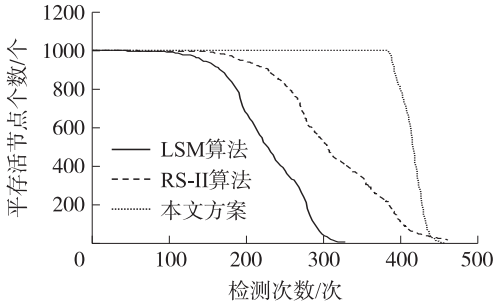

图 5　3 种方法检测次数与存活节点数目的关系

从图中可以看出基于 LEACH 分簇算法的检测方案(即本文方案)能够降低能耗,减小通信开销。

(3)检测率对比

若节点间的无线通信满足不发生丢包且都能够成功收发的理想情况,本文方案的检测率能够达到 100%。图 6 为在理想情况下,令网络中只有一个克隆节点,N 取不同值时各方案的检测率对比。

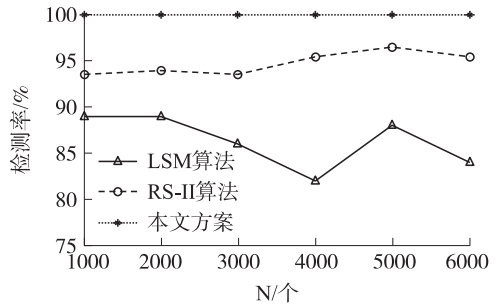

图 6　理想情况下 3 种方法的检测率比较

当然,实际情况中无线通信具有一定的失败概率,会对跳数较多的检测方案产生一定影响。因为检测信息被传递次数的增多,将增大检测信息传递不成功的概率。

4　结论

本文提出的基于分簇的检测方案是一种优化的集中式检测方案,该方案通过簇头和基站分别从局部和整体对网络进行克隆攻击检测,提高了检测率。同时,充分利用了分簇算法的数据传输机制,降低了通信和存储开销,对资源受限的无线传感器网络具有较强的适用性。

参考文献:

[1] 孙勇,景博,张宗麟. 基于不均匀环带模型能量有效的无线传感器网络节点放置方法[J]. 传感技术学报,2006,19(4):1287-1289.

[2] 曾梅梅,蒋华,王鑫. 一种新的无线传感器网络恶意节点追踪方法[J]. 传感技术学报,2013,26(1):122-127.

[3] 徐军. 无线传感器网络恶意节点攻击若干问题研究[D]. 合肥:中国科技大学,2012.

[4] 李端端,曾子维,潘晓红,等. 无线传感器网络克隆攻击检测协议[J]. 计算机工程,2009,35(16):161-163.

[5] 刘丽珍. 无线传感器网络中克隆节点攻击检测协议研究[D]. 长沙:中南大学,2012.

[6] Parno B, Perrig A, Gligor V. Distributed Detection of Node Replication Attacks in Sensor Networks[C]//Proc IEEE Symp Security and Privacy(S&P'05),2005. 49-63.

[7] Xing K, Liu F, Cheng X, et al. Realtime Detection of Clone Attacks in Wireless Sensor Networks[C]//Proc 28th Int Conf Distributed Computing Systems(ICDCS'08), June 2008. 3-10.

[8] Zhu B, Addada V, Setia S, et al. Efficient Distributed Detection of Node Replication Attacks in Sensor Networks[C]//Proc 23rd Ann Computer Security Applications Conference (ACSAC'07), Dec 2007. 257-267.

[9] Sheela D, Priyadarshini, Mahadevan Dr G. Efficient Approach to Detect Clone Attacks in Wireless Sensor Networks[C]//2011 3rd International Conference on Electronics Computer Technology (ICECT 2011), April 2011. 194-198.

[10] 陈姗姗,杨庚,陈生寿. 基于 LEACH 协议的 Sybil 攻击入侵检测机制[J]. 通信学报,2011,32(8):143-149.

[11] 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.

[12] Heinzelman W, Chandrakasan A, Balakrishnan H. Energy-Efficient Communication Protocol for Wireless Microsensor Networks[C]// Proceedings of the 33rd Hawaii International Conference on System Sciences. Maui, Hawaii, USA: IEEE Computer Society, 2000.

[13] 李成法,陈贵海,叶懋,等. 一种基于非均匀分簇的无线传感器网络路由协议[J]. 计算机学报,2007,30(1):27-36.

罗永健(1971-),男,湖北人,西安通信学院教授,博士,主要从事阵列信号处理、雷达目标识别及多用户通信等工作;

陈 涛(1988-),男,河南人,在读硕士研究生,研究方向为无线传感器网络,953284937@qq.com。