

基于感应数据值的无线传感器网络分簇算法

张 兴^{1,2}, 韦 潜¹

(1 北京工业大学 计算机学院, 北京 100124; 2 辽宁工业大学 电子与信息工程学院, 辽宁 锦州 121001)

摘 要: 提出了一种无线传感器网络的分簇算法, 用于协助基于簇的入侵检测方案检测网络中的各种恶意攻击行为. 它将整个网络划分成若干个簇, 使得簇内各传感器节点物理位置临近, 并且采集的数据值接近. 这一特性使得识别异常节点非常容易, 并且保证入侵检测方案具有较高的检测精度和较低的误报率. 该算法也使得网内数据处理变得异常简单, 从而能够有效节省传感器节点的能量, 延长网络的寿命.

关键词: 无线传感器网络; 安全; 入侵检测; 分簇算法

中图分类号: TP212.9

文献标识码: A

文章编号: 1000-7180(2010)06-0064-03

Readings-Based Clustering Algorithm for Wireless Sensor Networks

ZHANG Xing^{1,2}, WEI Qian¹

(1 College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China;

2 School of Electronion and Information Engineering, Liaoning University of Technology, Jinzhou 121001, China)

Abstract: This paper proposes a clustering algorithm for wireless sensor networks with the goal of helping the cluster-based intrusion detection schemes to detect malicious attackers. It partitions the whole network into a set of clusters with each cluster sensing a similar phenomenon. The sensors within the same cluster are physically close to each other. This feature insures that the intrusion detection schemes can identify anomaly nodes more easily and can achieve a lower false alarm rate and a higher detection accuracy rate than the existing detection schemes. At the same time, it can also make innetwork processing simpler, so it can reduce the node's power consumption and prolong the network lifetime.

Key words: wireless sensor networks; security; intrusion detection; clustering algorithm

1 引言

由于大规模无线传感器网络的覆盖范围广阔和节点数量众多, 需要采用层次结构进行管理, 而对无线传感器网络进行分簇就能够适应这种需求^[1-2]. 在当前的无线传感器网络分簇算法研究中, 主要存在利用基站的集中化方法^[3]、基于生成森林的方法^[4]和层次化的分布式方法^[5]等. 文中在原始分簇算法的基础上进行改进, 取得了满意的结果.

2 原始的分簇算法

While ($T_{\text{random}}(i)$ is not up) & ($\text{clustered} = \text{False}$)

If ($\text{receive} < \text{"Clustering"}, r_j, f_{ri} >$) & ($d(f_i, f_{ri})$

$\leq \delta/2$) & ($\text{hops}(i, r_j) \leq h/2$)

$r_i := r_j;$

$\text{clustered} := \text{True};$

$p_i := j;$

$f_{ri} := f_{rj};$

$\text{broadcast} < \text{"Clustering"}, r_i, f_{ri} >;$

If ($\text{clustered} = \text{False}$)

$r_i := i;$

$\text{clustered} := \text{True};$

$p_i := i;$

$f_{ri} := f_i;$

$\text{broadcast} < \text{"Clustering"}, r_i, f_{ri} >;$

其中, clustered 是初始值为假的布尔变量, 表示

收稿日期: 2009-05-14; 修回日期: 2009-07-14

基金项目: 北京市自然科学基金暨北京市教育委员会科技发展计划重点项目(KZ200610005003)

传感器节点是否已加入簇; r_i 和 p_i 分别为节点 i 所在簇的根节点和其父节点; f_i 和 f_{ri} 分别为节点 i 和根节点 r_i 采集到的数据值; $d(f_i, f_{ri})$ 为 f_i 和 f_{ri} 之间的欧几里德距离; $\text{hops}(i, r_j)$ 为节点 i 和根节点 r_j 之间的跳数; h 为簇内预设的最大跳数值. 传感器节点被部署后, 要等待一个随机时间 $T_{\text{random}}(i)$ 以避免节点间的瞬时大面积冲突. 如果它在这段时间内从邻居节点接收到一个簇请求消息并且尚未加入任何簇, 则计算它所采集的数据值 f_i 与接收到的簇请求消息中簇头节点 r_j 所采集的数据值 f_{rj} 之间的欧几里德距离, 以及这两个节点之间的跳数, 如果 $d(f_i, f_{ri}) \leq \delta/2$ 并且 $\text{hops}(i, r_j) \leq h/2$, 则加入该簇. 因为根据三角不等式可知组内任意两节点间采集数据的差距不超过 δ , 并且它们之间的距离不超过 h . 所以, 同一簇内的传感器节点物理空间上位置临近, 并且具有相近的观测数据值. 如果此传感器在 $T_{\text{random}}(i)$ 时间后仍未加入任何簇, 它便构造一个新簇并将自己作为簇头节点, 同时向邻居节点广播簇请求消息.

3 改进的分簇算法

原始的分簇算法随机地确定簇头节点, 致使被选定的簇头节点有可能是整个网络中采集到极值数据的传感器节点. 而且, 根据原始的分簇算法, 被选中加入此簇的传感器节点数量将会很少, 并且这些节点不能再次加入到其他更适合的簇中, 这将导致整个传感器网络被划分成许多小规模簇. 这种分簇方式并不适合运行基于分簇的入侵检测算法, 并且会消耗更多的能量. 因此本文提出了改进的基于感应数据值的分簇算法, 其中额外使用到的符号 f_{rj_max} 、 f_{rj_min} 和 f_{rj_avg} 分别为簇内当前采集数据的最大、最小和平均值, f_{rj_count} 为簇内当前传感器节点的数量.

```

While ( $T_{\text{random}}(i)$  is not up) & (clustered = False)
  If (receive < "Clustering",  $r_j$ ,  $f_{rj\_max}$ ,  $f_{rj\_min}$ ,  $f_{rj\_avg}$ ,  $f_{rj\_count}$  >)
     $f_{rj\_avg} = (f_{rj\_avg} * f_{rj\_count} + f_i) / (f_{rj\_count} + 1)$ ;
     $f_{rj\_max} = \max(f_{rj\_max}, f_i)$ ;
     $f_{rj\_min} = \min(f_i, f_{rj\_min})$ ;
    If ( $d(f_{rj\_max}, f_{rj\_avg}) \leq \delta/2$  & ( $d(f_{rj\_min}, f_{rj\_avg}) \leq \delta/2$ ) & ( $\text{hops}(i, r_j) \leq h/2$ )
       $r_i = r_j$ ;
      clustered = True;
       $p_i = j$ ;

```

```

broadcast < "Clustering",  $r_j$ ,  $f_{rj\_max}$ ,  $f_{rj\_min}$ ,  $f_{rj\_avg}$ ,  $f_{rj\_count} + 1$ ;
If (clustered = False)
   $r_i = i$ ;
  clustered = True;
   $p_i = i$ ;
   $f_{rj\_max} = f_{rj\_min} = f_{rj\_avg} = f_i$ ;
  broadcast < "Clustering",  $r_i$ ,  $f_{rj\_max}$ ,  $f_{rj\_min}$ ,  $f_{rj\_avg}$ , 1 >;

```

下面证明改进的基于感应数据值的分簇算法满足簇内任意两个传感器节点之间采集数据的差距不超过阈值 δ , 并且它们之间的距离不超过 h 的要求. 当传感器节点构造新簇并将自己作为簇头节点时, 簇内只有一个节点, 显然满足以上的要求. 当执行改进的分簇算法的新节点加入簇时, 满足 $d(f_{rj_max}, f_{rj_avg}) \leq \delta/2$ 和 $d(f_{rj_min}, f_{rj_avg}) \leq \delta/2$, 因此任意两节点 i 和 j 之间的度量值 $d(f_i, f_j) = |f_i - f_j| \leq |f_i - f_{rj_avg}| + |f_{rj_avg} - f_j| \leq 2 * \max(d(f_{rj_max}, f_{rj_avg}), d(f_{rj_min}, f_{rj_avg})) \leq \delta$, 并且 $\text{hops}(i, j) \leq \text{hops}(i, r) + \text{hops}(j, r) \leq h/2 + h/2 = h$. 因此, 簇内任意两个传感器节点之间所采集数据值的差距不超过 δ , 并且它们之间的距离不超过 h .

在上述两种分簇算法中, 选择竞争时间 $T_{\text{random}}(i)$ 时应确保传感器节点在构造新簇前等待足够长的时间. $T_{\text{random}}(i)$ 可以利用随机数生成函数乘以传感器节点间平均消息传递时间 t 计算得到, 在最多经过 $\max(T_{\text{random}}(i)) + ht/2$ 时间后, 网络中的传感器节点都将执行完分簇算法.

4 性能分析

我们将 150 个 Crossbow 的 IRIS 和 MICAz 传感器节点部署在八层的办公楼内, 用于采集各个房间内的温度、湿度、光照数据. 分别根据这三种数据, 利用上述两种分簇算法将整个无线传感器网络进行分簇.

图 1 显示了原始分簇算法和改进分簇算法在不同的温度、湿度和光照度量条件下的平均簇大小. 显然, 改进分簇算法能够划分出比原始分簇算法更大规模的簇.

在网络实例中各个簇的大小所占的比例在两种分簇算法中有所不同, 原始分簇算法中小规模簇所占的比例要远大于其在改进分簇算法中所占的比例. 这种小规模簇并不适合于运行基于簇的入侵检

测算法,应尽量减少它们的数量.改进的分簇算法通过调整加入簇的判定条件,获得了较优的分簇效果.

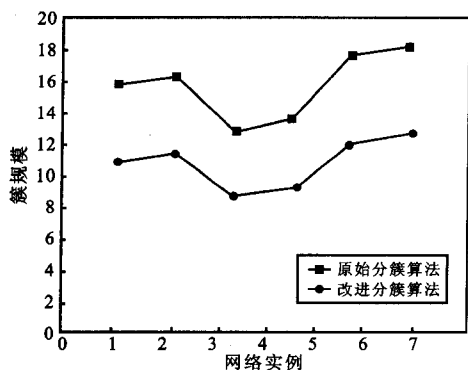


图1 两种分簇算法得到的平均簇规模

误报率是正常传感器节点被误判为异常传感器节点的比率,检测精度是异常传感器节点被成功识别出的比率.它们是评测入侵检测方案性能的两个关键性指标.图2显示了基于上述两种分簇算法的内部攻击者检测方案^[6]中误报率和检测精度性能的比较.从图中可以看出,基于改进分簇算法的入侵

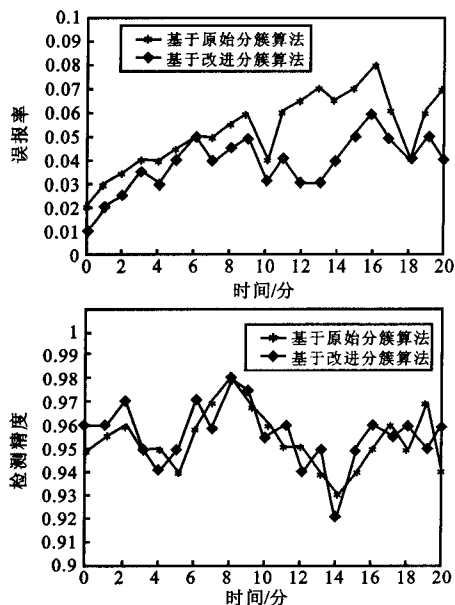


图2 内部攻击者检测方案在基于两种不同分簇算法时的误报率和检测精度比较

检测方案具有较低的误报率,但它们的检测精度比较接近.

5 结束语

文中提出了适用于无线传感器网络的基于感应数据值的网络分簇算法,用于协助基于簇的入侵检测方案检测网络中的各种恶意攻击行为.实验结果表明,该算法能够获得非常好的分簇效果,平均簇规模较大,小规模簇的比例很小,并且使采用此分簇算法的入侵检测方案具有较低的误报率和较高的检测精度.

参考文献:

- [1] 龚本灿, 李腊元, 蒋廷耀, 等. 基于生成树的无线传感器网络分布式路由协议[J]. 微电子学与计算机, 2008, 25(11): 77-80.
- [2] 郭新华, 蒋艳, 曹建霞. WSN中动态自适应蚁群路由算法[J]. 微电子学与计算机, 2008, 25(12): 157-160.
- [3] Ng A Y, Jordan M, Weiss Y. On spectral clustering: Analysis and an algorithm[J]. NIPS, 2002(14): 849-856.
- [4] Meka A, Singh A. Distributed spatial clustering in sensor networks[C]// The 10th International Conference on Extending Database Technology. Munich, Germany, Berlin, Springer-Verlag, 2006: 980-1000.
- [5] Ng R T, Han J. Efficient clustering methods for spatial data mining[J]. VLDB, 1997(25): 186-195.
- [6] Liu F, Cheng X, Chen D. Insider attacker detection in wireless sensor networks[C]// Proceedings of the 26th IEEE International Conference on Computer Communications. Canada: Quebec, 2007: 1937-1945.

作者简介:

张兴男, (1975-), 博士研究生, 讲师. 研究方向为无线传感网络安全.

韦潜男, (1970-), 博士研究生, 讲师. 研究方向为移动Ad Hoc与无线Mesh网络安全.