基于可信分簇的传感器网络密钥管理策略①

Trust Clustering—Based Key Management Strategy in Wireless Sensor Network

沈金波　许　力　（福建师范大学 网络安全与密码技术重点实验室 福建 福州 350007）
曾　毅　（福建省建欧市立医院网络中心 福建 建欧 353000）

摘　要： 密钥管理是实现无线传感器网络安全的重要环节。在基于可信度的分簇算法基础上，结合门限秘密共享的思想，得出了一种基于可信分簇的密钥管理策略。通过仿真，把该策略与基于最小 ID 分簇和无分簇情况下进行比较，得出结果表明了其性能良好。

关键词： 无线传感器网络 安全 可信度 分簇 密钥管理

1　引言

无线传感器网络（Wireless Sensor Network，WSN）[1]是由众多具有通信和计算能力的传感器节点用无线通信的方式连接而成，每个传感器节点具有低成本、低功耗、协同合作等功能，可以从环境中实时地监测、感知和收集信息，并向远端的数据收集点发送。无线传感器网络有易于部署、网络规模可变、容错能力强等优点。由于传感器网络一般配置在环境恶劣、无人管理的区域或者是敌方阵地，因而传感器网络的安全显得尤为重要，它直接影响到相关应用的结果。为了避免无线传感器网络在运行过程中被监听通信、冒充节点或提供虚假信息，必须对通信的内容进行加密和认证，因此邻居节点之间必须建立对密钥，而密钥的分配和管理就成为了一个关键的问题。

近年来不少学者在无线传感器网络的密钥管理方面做了大量工作。Eschenauer L. 等人提出随机密钥预分配方案[2]，在此基础上有不少学者提出了许多方案和协议，如 q－Composite 随机密钥预分配方案[3]和对称多项式随机密钥预分配方案[4]等等。针对分簇式网络，有学者提出了低能耗密钥管理[5]和轻量级密钥管理[6]等方案。我们也在组合设计基础上提出了基于 Cover－Free 结构的密钥预分配方案并应用于组密钥的分发和更新[7]。在基于可信度的分簇算法基础上，结合门限秘密共享的思想，得出了一种基于可信分簇的密钥管理策略，并通过仿真实验来分析密钥管理策略的性能。

2　基于可信分簇的密钥管理

2.1 可信度值的判断

基于网络邻居节点的监控以及节点信息的交互，我们可以得知节点的可信度[8]。节点对其它节点的可信度评价

$$TE = (f_1 V_{sr} + f_2 V_{ir} + f_3 V_{of}) \times V_{ibl} \quad (1)$$

其中 TE：可信度评价；V_{sr}：主动观测值；V_{ir}：间接观测值，从其他节点处获得的经验值，是通过信息的交换获得的；V_{of}：其它一些因素的影响，如能量剩余等；V_{ibl}：由入侵检测系统列出的恶意节点表，1 为好节点，0 为恶意节点；f_i（i＝1，2，3）是权值，不同情况下可设不同的值，假设 $f_1 + f_2 + f_3 = 1$，并进行归一化，使得 $TE \in [0,1]$，且 $f_1 > f_2$，为防止敌人的恶意诋毁。

2.2 可信分簇策略

在传感器网络中存在各种攻击方式，无论是发送错误的路由包还是不转发数据包等攻击行为，它们都会造成网络的不可用。通过网络邻居节点的监控以及节点信息的交互方式而得知节点的可信度，以此作为选举簇头的标准，使可信度高的节点成为簇头。首先将全网划分成若干簇，每个簇的簇头 CH（cluster head）一起构成一个逻辑网络。网络中各节点之间通过互相检测和指控来识别恶意节点，若某节点 A 有恶意行为，同簇的其它节点就会向

① 基金项目：国家自然科学基金（60502047）；福建省教育厅重点项目（JA07030）

簇头指控该节点,当簇头收到指控信息时,将把 A 的可信度减去一个给定的值 α,当 A 的可信度值降到某个给定的阈值以下时,簇头把该节点确定为恶意节点,撤消其合法身份,并将其加入黑名单。

2.3 节点的加入

依据文献[3],我们称一个节点加入网络时的过程为登陆,登陆过程如下:

第一步,加入节点广播加入请求,任何节点都可以通过可信度认证该节点并颁发许可,获得足够许可后,便可计算出一个合法的身份证书,成员只有凭此证书才能与其它节点进行通信。

第二步,节点选择可信度高的簇头节点作为簇头,发送加入信息。该加入过程可能有两种情况:一种为节点首次加入网络,另外一种为节点从一簇移动到另一簇。在基于簇结构的传感器网络中,节点可能从一个簇漫游到另一个簇,某些恶意节点可能实施簇间漫游攻击:当在一个簇中实施了大量破坏导致可信度降到某一水平时,漫游到另一个簇,重新加入网络,从而刷新自己的可信值,然后对新簇实施破坏。为了对抗恶意节点的这类攻击本文采用以下机制,即当一个节点 N 申请加入某个簇 A,首先需要提交自己的证书,簇 A 的 CH 从证书中取出序列号 NS,将 NS 加密后组播给其它 CH,每个 CH 得到 NS 后在自己的信息表中查找该序列号,对于任意一个其他簇 K 的 CH 来说,若找到 NS 则说明节点是从本簇漫游到 A 中的,簇 K 的 CH 就将 N 的记录信息发给 A,若无则发送一条简单的回复信息,然后簇 A 的 CH 根据其它 CH 发回的信息判断节点 N 是漫游节点还是新节点,以及是否被其它簇撤消过,由此来决定是否允许 N 加入本簇。若该节点被允许加入簇,它将得到簇密钥。

2.4 节点的退出

设节点的离开并不会使网络间断,若离开节点为成员节点,它的离开就只会在其所在的簇内产生影响,则只需在簇内采用 PKI,更新此簇密钥,不会影响到其它簇。若离开节点为 CH,则采用分布式密钥管理,密钥更新将需在网络的主干网中进行。

3 性能分析

3.1 性能指标

为衡量可信分簇下的密钥管理性能优势,引用节点成功登陆比率与成功登陆时间作为指标。其中节点成功登陆比率 = 成功登陆的节点数/申请加入的节点总数,时间用节点总跳数定义,如节点经过 10 跳收到门限个证书,则登陆时间为 10 单位时间。成功登陆定义为节点请求加入到成为正式成员,在这段时间里,节点需要获得门限个认证,并合成有效身份证书,利用此证书寻找到簇头 CH。根据传感器网络通信可靠性,我们设只有可信度大于某阈值的节点方可百分百发送认证,而低于阈值的节点只按一定概率转发,分以下三种情况比较讨论:

(1)基于可信度的分簇结构,节点可向 CH 请求认证,此情况 CH 可信度值均大于阈值。

(2)基于最小 ID 的分簇结构,节点可向 CH 请求认证,此情况 CH 可信度值不一定大于阈值。

(3)无分簇结构,节点向所有节点发送请求,此时用 DSR 路由协议,此情况会遇到大量的恶意节点不转发请求。

3.2 模拟环境

当前适合传感器网络的模拟软件有 NS(Network Simulator)和 GloMoSin 等,但是这两种模拟软件目前没有集成分簇算法,本文利用 VC + +6.0 进行模拟仿真研究。

在此模拟环境中,暂时不考虑背景噪声,分组的传输差错和分组的冲突对分簇算法性能的影响。因为模拟环境对各算法而言是平等的,简化实现并不会影响算法比较结果的准确性。由于考虑的是同质传感器网络,各节点的传输功率(范围)相同。

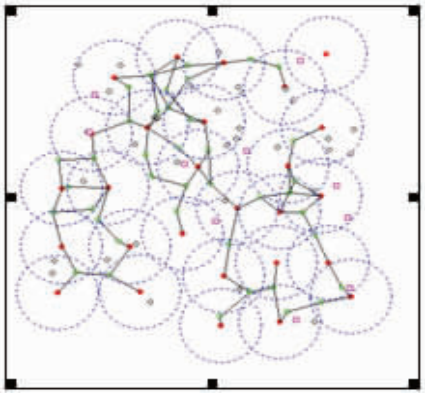
我们在一个 X * Y 单位距离的区域内随机放置 N 个节点,节点的移动方向在[0,360°]内随机分布,节点的移动速度可以在[0,maxV]之间随机选择。节点到达区域边界时,它将向区域内反射。在模拟中,系统区域节点数,节点的传输范围(以单位距离数表示),节点移动速度,申请加入节点数,成功登陆所需的证书门限数,可以根据要求进行动态调整。在此我们在 300 * 300 单位距离的区域内随机生成 100 个节点,节点最大速度 maxV = 30,申请加入节点数为 10,各个节点随机分布在系统区域内。

下面分析节点在传输范围 r = 40,50 时。节点登陆比率与节点登陆时间随所需证书门限数从 5 ~ 50 变化曲线。数据结果是经过 10 组 20 次独立重复模拟仿真取平均值得到的。

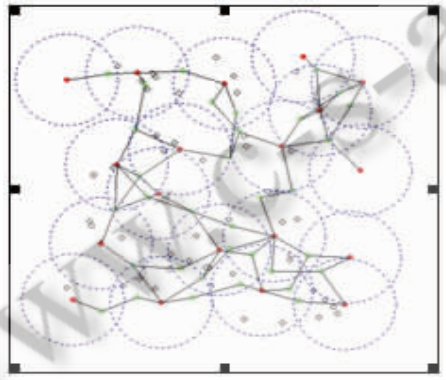
3.3 结果分析

(1)传输半径不同,网络分簇情况有所不同,图 1

为半径分别为 40、50 时，基于可信分簇的实例。



A r = 40



B r = 50

图 1　可信分簇算法(实心为簇头，空心为簇成员)

(2)设传输半径 r = 40，成功登陆所需要证书数分别取 5、10、15、...、50 共 10 组，图 2 中采用可信分簇，最小 ID 分簇和不分簇三种情况下，成功登陆比率随所需证书数变化的曲线。从图 2 中可以看出在证书数越大时，可信分簇成功登陆比率明显大于另外两种情况。图 3 为传输半径 r = 50 时的情况，同样可见可信分簇的明显优势。

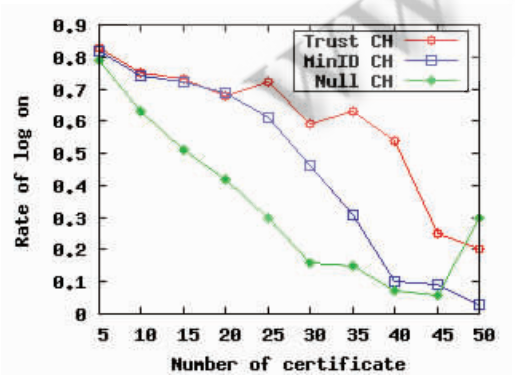


图 2　r = 40 成功登陆比率随所需证书数变化的曲线

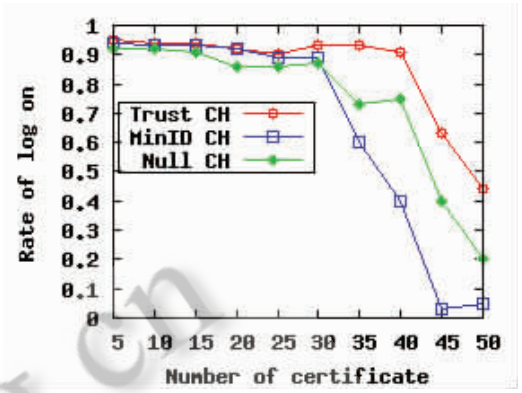


图 3　r = 50 成功登陆比率随所需证书数变化的曲线

(3)设传输半径 r = 40，成功登陆所需要证书数分别取 5、10、15、...、50 共 10 组，图 4 中采用可信分簇，最小 ID 分簇和不分簇三种情况下，成功登陆节点中平均每个节点成功登陆所花的时间变化曲线。从图 4 中可以看出，随着所需证书数的增加，登陆时间也将变长，但是在可信分簇下增长速度明显比另外两种情况小。图 5 为传输半径 r = 50 时的情况，同样可见可信分簇的明显优势。

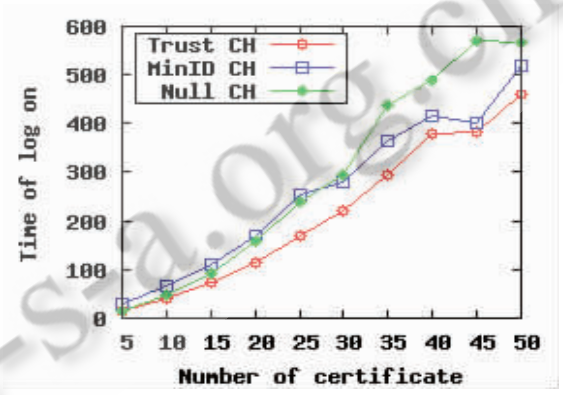


图 4　r = 40 成功登陆所花的时间变化曲线

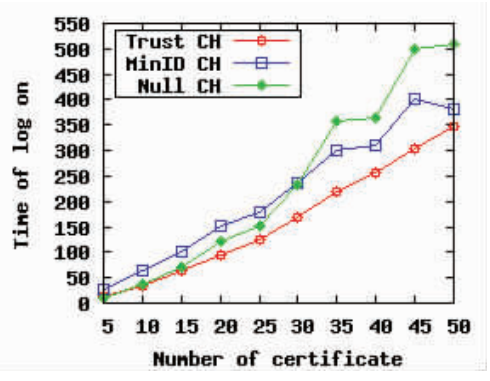


图 5　r = 50 成功登陆所花的时间变化曲线

(4)在所需要证书数相同的条件下,传输半径对网络分簇结构有影响。图 6 为半径分别取 30、40、50 时,证书数取 30 时,采用可信分簇,最小 ID 分簇和不分簇三种情况下,成功登陆比率比较,可看出可信分簇下,成功登陆比率都是最高的。图 7 为同样情况下,成功登陆节点中平均每个节点成功登陆所花时间比较,可看出,可信分簇下所花时间总是最小的。

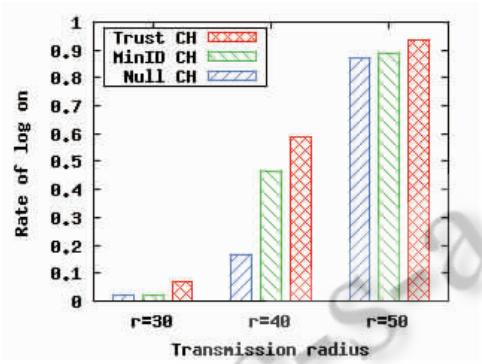


图 6　证书数为 30 时不同半径的成功登录比率

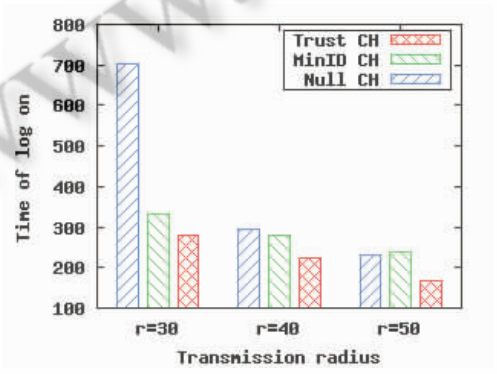


图 7　证书数为 30 时不同半径的成功登录时间

4　结论

本文通过对传感器网络中基于可信分簇的密钥管理系统进行仿真研究,分析节点传输范围和所需证书数对节点成功登录比率和成功登录时间的影响,并与基于最小 ID 分簇和无分簇情况进行比较,得到的结论是:随着所需证书数的增加,该方案中节点成功登录比率将减小,成功登录时间也将变长;所需证书数相同,节点传输范围变大,成功登录比率也将增大;基于可信分簇的密钥管理系统性能优于基于最小 ID 分簇和无分簇的。

参考文献

1 Akyildiz F, Su W, Sankarasubramaniam Y, et al. A survey on sensor networks . IEEE Communications Magazine, 2002, 40 (8): 102 – 114.

2 Eschenauer L, Gligor V. A Key Management Scheme For Distributed Sensor Networks. In: Proceedings of 9th ACM Conference on Computer and Communication Security, Washington: ACM Press, 2002: 41 – 47.

3 Chan H, Perrig A, Song D. Random Key Pre – Distribution Schemes For Sensor Networks. In: IEEE Symposium on Research in Security and Privacy. Berkeley, California: IEEE Computer Society, 2003: 197 – 213.

4 Liu D, Ning P. Establishing pairwise keys in distributed sensor networks. In: Proceeding of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press, 2003, 52 – 61.

5 G Jolly, KuscuM C, Kokate P, et al. A Low2Energy KeyManagementProtocol forWireless Sensor Networks . In: Proceedings of the 8 th IEEE Symposium on Computer and Communications (ISCC), 2003, 335 – 340.

6 M Eltoweissy, M Younis, K Ghumman. Lightweight Key Management for Wireless Sensor Networks. In: IEEE International Conference on Performance Computing and Communications, 2004. 813 – 818.

7 CHEN JIANGWEI, LI XU, YI MU. A New Group Rekeying Scheme Based On T – Packing Designs For Ad HOC Networks [M/CD]. The Proceeding of IF0SCALE2007, ACM Press, 2007.

8 章静,许力,黄榕宁. 自组网中可信的分簇策略,武汉大学学报(理学版), 2006,52(SL):1 – 5.

9 M. Bechler, H – J. Hof, D. Kraft, et al. A cluster – Based security Architecture for Ad Hoc Networks. Proc. IEEE INFOCOM, 2004, 4: 2393 – 2403.