doi:10.3772/j.issn.1002-0470.2014.05.004

无线传感器网络的基于信任管理的分布式高可靠覆盖机制①

李小龙②*** 董书豪* 司丽娟③* 梁 海*

(*桂林电子科技大学计算机科学与工程学院 桂林 541004)

(**广西可信软件重点实验室 桂林 541004)

摘 要 为解决无线传感器网络中的安全覆盖问题,将覆盖算法整合到信任管理系统中,提出了一种基于信任管理的分布式高可靠覆盖机制(HRCMTM)。通过分析信任管理系统的潜在要求,从理论上推导和分析了网格尺寸选择。引入动态信任阈值新的概念,定量分析了覆盖节点集大小、联合信任度与动态信任阈值之间的关系。在此基础上,设计了确保可靠覆盖目标区域的节点调度覆盖算法。仿真结果验证了这一新的机制在覆盖率和联合信任度等方面的有效性。

关键词 无线传感器网络(WSN),信任管理,高可靠覆盖机制,动态信任阈值,网格,分布式

0 引 言

无线传感器网络(WSN)随着在战场监测、环境和交通监测等领域的广泛应用[1],迫切需要在受到资源约束和存在网络攻击的条件下提供可靠的服务。为了节约能量,现已开始在传统传感器网络中引入覆盖技术,以便使用尽量少的节点完成覆盖任务。为了避免网络攻击导致关键技术难以可靠运行,研究人员引入了信任管理的概念,以保证关键技术的安全性。目前,基于信任管理的安全路由技术[2]、安全簇头选举[3]、安全数据处理[4]和安全定位技术[5]研究已取得一些有价值的成果,但至今还没有行之有效的基于信任管理的安全覆盖机制。高可靠覆盖技术是实现高可信 WSN 的关键技术之一,WSN 通过节点间的相互协作执行监测区域、目标跟踪任务,但进行协作的前提和基础是参与节点是正常节点,而非恶意节点。为了提高网络覆盖质量的可靠性和屏蔽节点失效对覆盖质量造成的不利影响,研究人员提出了一些有效的解决方案。文献[6]通过在网络中额外添加一些监测节点,使其及时发现网络中的失效节点,并代替这些失效节点转发数据包,以支持传感数据安全、准确地到达汇聚节点。文献[7]提出了一种基于 2-Coverage 的可靠覆盖机制,通过增加冗余覆盖来屏蔽单个节点的失效,达到容错效果。文献[8]提出了一种基于虚拟势场的解决方案,其基本思想是把网络中每个传感器节点看作一个虚拟的电荷,各节点受到其它节点的虚拟力作用,向目标区域中节点密度较小的区域扩散,最终达到平衡状态。以上这些可靠覆盖机制主要用于解决减少节点失效对于覆盖质量的影响。然而在真实应用中,除了节点失效造成网络覆盖质量下降以外,网络攻击等都会对覆盖质量造成影响。例如,若监测节点或老化,或被敌方俘获成为恶意节点,发送的传感数据严重偏离于现实数据,这些虚假的数据将会引发错误警报,干扰用户决策。

信任管理是对传统安全机制的有效补充,已经应用于分布式网络的各个方面。当前,通用的信任管理模型有多种[9,10],其中 Ganeriwal 和 Srivastava 提出的基于声望的高完整性传感器网络框架(RFSN)[9]就是一种典型的基于声望的通用信任管理系统。为了减少因引入信任管理造成的较大的能量开销,Bao 等提出了一种基于不同能量的层次型的信任管理系统[10]。文献[11]虽然提出了一种基于信任管理的节点覆盖调度方案,但是该调度方案只是简单地把信任管理系统加入到节点中,具体调度时

① 国家自然科学基金(61063040, 61262074)资助项目。

② 男,1981 年生,博士,副教授,硕士生导师;研究方向:无线传感器网络,M2M 网络, Mesh 网络; E-mail: xlli@guet.edu.cn

③ 通讯作者,E-mail: sisihui88@126.com

(收稿日期:2013-09-30)

仅仅把信任管理系统给出的小于设定阈值的节点剔除，而没有把它整合到覆盖算法中。基于以上动机，本文提出了一种基于信任管理的分布式高可靠覆盖机制(Highly Reliable distributed Coverage Mechanism based on Trust Management，HRCMTM)。同时深入分析了信任管理系统有效运行时存在的潜在要求，在此基础上推导出剖分目标区域的合适网格尺寸。本文还提出了动态信任阈值的概念，定量分析了覆盖节点集大小、联合信任度与动态信任阈值之间的关系。结合之前的分析结果，提出了一种基于信任管理的覆盖算法，该算法能确保覆盖区域的高可靠覆盖，又能有效减少活跃节点的数量。论文将覆盖算法整合到信任管理系统中，为如何基于信任管理进行高可靠覆盖，提供了一种新的启示。

1 基于信任管理的模型

1.1 网络网格模型

为简化运算，本文将离散的点集代表连续的区域，将目标区域用网格进行剖分，目标区域用若干个网格点来表示。传感器网络对应的网络模型和采用的信任管理系统假定具有以下性质：(1) 目标区域为一个二维平面。传感器节点通过装置 GPS 设备或者利用某种定位算法可以获得节点的位置信息。(2) 传感器节点的通信模型和感知模型都是圆盘模型，节点的通信半径用 Rc 表示，传感半径用 Rs 表示。(3) 节点的信任度由信任管理系统给出，其值的大小反映感知数据的可信性。

1.2 网格尺寸的设置

任何节点行为由其它节点进行监督，是信任管理系统有效工作的前提和基础。节点行为根据功能可分为通信行为和感知行为。对于任意给定的网格点，为了使相邻网格内的节点能相互监督通信行为和感知行为，共同执行覆盖该网格点的监测任务，虚拟网格单元大小需满足于以下条件：(1) 网格内的任意传感器节点处于工作状态时，均能够有效地覆盖到整个网格区域，其中包含单元网格对应的 4 个网格点。在此条件下，容易推出网格点的相邻网格内的任意两个节点之间能够共同监测该网格点，其感知行为能够被彼此监督。(2) 网格点的相邻网格内的节点之间的通信行为，包括发送行为和接收行为，能够被同属该区域的任意工作节点监测到，以达到其间任意两个节点之间的通信行为能够被彼此监督的目的。基于条件(1)和条件(2)，网格尺寸 r 需分别满足不等式

$$R_s^2 \geqslant r^2 + r^2 \tag{1}$$

$$R_c^2 \geqslant (2r)^2 + (2r)^2 \tag{2}$$

因此，若该网格的尺寸设置为 $\min(\frac{\sqrt{2}}{4}Rc, \frac{\sqrt{2}}{2}Rs)$，可有效满足信任管理系统正常运行的要求。

为了便于算法描述，我们定义了下列符号：$N = \{n_1, n_2, \cdots, n_k\}$ 表示所有的传感器节点，$\{r_1, r_2, \cdots, r_k\}$ 是其对应的信任值，k 表示网络节点的个数；S_i 表示位于网格点 p_i 的相邻网格内并参与覆盖网格点 p_i 任务的节点集，k_0 表示覆盖节点集允许的最大节点个数 (k_0 为系统参数)，k 表示当前覆盖节点集的节点个数；$T_{\min}^k$ 为覆盖节点集个数为 k 时的节点信任阈值，并且 $T_{\min}^3 \geqslant T_{\min}^5 \cdots \geqslant T_{\min}^{k_0}$，信任度低于该阈值的节点被判定为恶意节点，$T_{\min}^{k_0}$ 缩写成 $T\min$；$T\max$ 代表网格点的联合信任阈值 ($T\max$ 为系统参数)；T_i 表示网格点 p_i 对应的覆盖节点集 S_i 获得的联合信任度，其中 $S_i \subseteq N$，$T_i(k)$ 表示网格点 p_i 对应的覆盖节点集个数为 k 时的联合信任度。

具体的选择节点、调度节点的过程和方法，将在本节之后进行详细阐述。本文首先给出一些定义。

定义 1 网格点 p_i 对应的覆盖节点集 S_i 中有一半以上的工作节点正常工作获得感知数据的概率称为该网格的联合信任度。

定义 2 若网格点 p_i 对应的覆盖节点集 S_i 获得的联合信任度 T_i 大于或等于 $T\max$ 的值，则称 p_i 被高可靠覆盖。

定义 3 若目标区域内每一个网格点都被高可靠覆盖，则称该区域被高可靠覆盖。

节点联合覆盖网格点的基本过程如图 1 所示。各个网格点在相邻网格内选择若干个工作节点作为

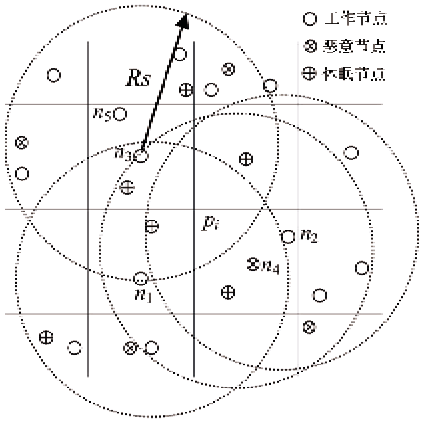

图 1 节点联合覆盖网格点的示意图

覆盖节点集,联合执行覆盖任务。如果当前覆盖网格点的大于信任阈值 $T_{\min}^{k}$ 的覆盖节点集得到的联合信任度高于预定值 $T\max$,说明该网格点已经达到了高可靠覆盖的要求。如果有网格点的联合信任度低于阈值 $T\max$,则需要重新进行调度。在图 1 中,对于网格点 p_i 来说,对应的覆盖节点集 $S_i = \{n_1, n_2, n_3\}$。

1.3 信任阈值的分析与讨论

为使目标区域监测能够具有更好的安全性和可靠性,要求覆盖节点集中有一半以上的工作节点正常工作获得感知数据的概率大于网格点信任度阈值 $T\max$,这样可保证经过数据融合(如数值融合)等相关处理后,融合数据为满足要求的高可靠数据。考虑到能量资源有限和经济成本等现实因素,在现实应用中,参与覆盖该网格点的工作节点个数,即覆盖节点集不宜过大,应限制在 k_0 个以内(k_0 为系统参数,值较小)。

(1)为避免工作节点个数过多,若 k_0 个超过或者等于信任阈值 $T\min$ 的节点组成覆盖节点集,对应的联合信任度达到联合信任阈值 $T\max$,就可将工作节点限制在 k_0 个以内。上述问题可归纳为求最小的 $T\min$:

$$\begin{cases} x^k + C_k^1 x^{k-1}(1-x)^1 + \cdots + C_k^{\frac{k-1}{2}} x^{k-\frac{k-1}{2}}(1-x)^{\frac{k-1}{2}} = T_{\max} \\ 0 < x < 1 \\ x \geqslant T_{\min} \end{cases} \tag{3}$$

其中 k 为奇数(原因将随后进行讨论)。当 $T\max = 0.95, k_0 = 5$ 时,得到的阈值 $T\min$ 不能小于 0.8。当 $T\max = 0.9, k_0 = 5$ 时,对应的 $T\min$ 等于 0.75。同理,当 $T\max = 0.95, k_0 = 7$ 时, $T\min = 0.77$;$T\max = 0.9, k_0 = 7$ 时,$T\min = 0.72$。

图 2 的 X 坐标为工作节点的个数 k,Y 坐标为选取的 $T\min$ 的值,Z 坐标为工作节点个数分别为 k 和 $k+1$ 时的联合信任度之差。通过图 2 我们发现,当 k 较小且为奇数时,再增加一个超过信任阈值 $T\min$ 的工作节点,不但没有使得联合信任度增加,反而使它大幅度的降低。此外,若处于 $T\min(0 < T\min < 0.8), k \leqslant 13$ 这个范围内,当所有工作节点的信任值均为 $T\min$,工作节点个数为 k 时,对应的联合信任度大于节点个数为 $k+1$ 时的值,令 $k_1 = \dfrac{k-1}{2}$,即有

$$x^k + C_k^1 x^{k-1}(1-x)^1 + \cdots + C_k^{\frac{k-1}{2}} x^{k-\frac{k-1}{2}}(1-x)^{\frac{k-1}{2}} > x^{k+1} + C_{k+1}^1 x^k (1-x)^1 + \cdots + C_{k+1}^{k_1} x^{k+1-k_1}(1-x)^{k_1} \tag{4}$$

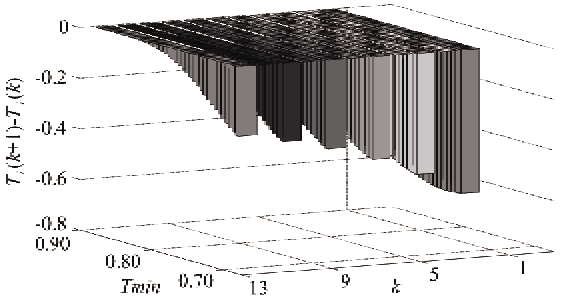

图 2 当 k 为奇数时,$T_i(k+1) - T_i(k)$ 与 k、$T\min$ 的关系图

通过以上分析,可以得出结论,在节点个数不超过 k_0 的情况下,参与任务的工作节点应为奇数个,若当前工作节点集得到的联合信任度小于 $T\max$,每次增加的节点个数应以 2 个递增。

(2)当 $k=1$ 时,若该网格点的邻居网格内有大于信任阈值 $T\max$ 的节点,则显然该节点单独工作,即可满足该网格点被高可靠覆盖。若不能,不妨假设最大值为 β,增加两个超过信任阈值 $T_{\min}$ 的节点能提升当前的联合信任度(反之,若不能提升联合信任度,则增加工作节点个数缺乏意义)。即 $k=3$ 时,得到的联合信任度值大于单个节点工作时的值 β。若令 $x = T_{\min}^3$,可推出如下公式:

$$\beta x^2 + 2\beta x(1-x) + x^2(1-\beta) > \beta \tag{5}$$

下面证明当 $k=5, 0.90 \leqslant T\max < 1$ 时,存在着以下定理。

定理 1 若 $0.90 \leqslant T\max < 1$,且

$$\begin{cases} \beta > x \geqslant x_1 \\ x_1^k + C_k^1 x_1^{k-1}(1-x_1)^1 + \cdots + C_k^{\frac{k-1}{2}} x_1^{k-k_1}(1-x_1)^{k_1} = T_{\max} \\ k_1 = \dfrac{k-1}{2} \\ 0 \leqslant x_1 = T_{\min} \leqslant 1 \\ k = 5 \end{cases}$$

对于 $\forall \beta \in (x, T_{\max}), \beta x^2 + 2\beta x(1-x) + x^2(1-\beta) > \beta$ 恒成立。

证明:采用求导的办法,容易证明当 $\beta \in [0.9, 1)$ 时,式(5)恒成立,故略。

通过该定理说明 $k_0 = 5$,只要 $0.90 \leqslant T\max < 1$ 时,增加两个信任值大于信任阈值 $T\min$ 网络节点,即能有效提升、增大联合信任值。联合(1)和(2)的分析结果,可以得到以下结论,当 $k_0 = 5$ 时,若 $T\max = 0.95$, $T_{\min}^3 = T\min = 0.8$;若 $T\max = 0.9$, $T_{\min}^3 =$

$T\min = 0.75$。对于 $k_0 = 7$ 时，若 $T\max = 0.95$，$T^3_{\min} = 0.80$，$T\min = 0.77$；若 $T\max = 0.9$，$k_0 = 7$，$T^3_{\min} = 0.72$，$T\min = 0.72$。

以上分析结果表明，若 $k_0 = 5$，$T\max = 0.95$，当网格点对应的覆盖节点集 $k = 3$ 时，信任阈值 $T^3_{\min}$ 为 0.8；当某个网格点对应的覆盖节点集 $k = 5$ 时，信任阈值 $T\min$ 保持不变。此时，覆盖节点集一定能高可靠覆盖该网格点。若 $k_0 = 7$，$T\max = 0.95$，当 $k = 3$ 时，此时覆盖节点集的节点的信任值必须大于或者等于信任阈值 $T\min$ 为 0.80；若 $k = 7$ 时，信任阈值下降到 0.77。在这里，信任阈值随着网格点的覆盖节点集个数增加，其值是动态发生变化的。对于其它的 k_0，$T\max$ 和 k 值，与信任阈值 $T^k_{\min}$ 之间的一一对应关系，均可以采用上述方法得到，在这里将不再赘述。

1.4 联合信任度的数学模型

假设网格点 p_i 的覆盖节点集 $S_i = \{n_1', n_2', \cdots, n_k'\} \subset N$，对应的信任值为 $\{r_1', r_2', \cdots, r_k'\}$，其中 $r_1' \geqslant r_2' \cdots \geqslant r_k'$。在这里，$k$ 表示覆盖节点集的大小，w_{ko} 表示这 k 个不同节点中恰好有 o 个节点感知数据错误的所有组合的集合，$w^j_{k,o}$ 表示第 j 个组合，其中 $1 \leqslant j \leqslant C^o_k$。例如，$w^1_{k,o} = \{n_1', n_2', \cdots, n_o'\}$ 代表感知数据错误的节点有 $n_1', n_2', \cdots, n_o'$。则网格点 p_i 的联合信任度可公式化成下式：

$$\begin{cases} T_i = \sum_{o=1}^{\frac{k-1}{2}} \{ \sum_{j=1}^{C^o_k} [\prod_{n_l' \in w^j_{k,o}} (1 - r_l') \prod_{n_l' \notin w^j_{k,o}} r_l'] \} + \prod_{l=1}^{k} r_l' \\ \forall r_l' \geqslant T^k_{\min} \end{cases} \tag{6}$$

2 基于信任管理的覆盖算法

本节给出了算法设计的设定目标，并详细描述该算法实施节点调度的具体实现过程。

2.1 算法设定的目标

（1）尽可能选取最少的工作节点来保证网络的高可靠覆盖，延长整个网络的寿命。

（2）算法应该是分布式算法，即基于邻居节点的信息进行决策。

（3）选取工作节点的过程应考虑到节点的信任值，尽量调度信任值高的节点，有利于提高目标区域在覆盖性能上的高可靠性。

（4）选取的工作节点在覆盖区域内应较为均匀地分布。

2.2 算法描述

基于信任管理的覆盖算法要求网格中存在着若干个活动节点监控着目标区域，而让其余节点进入休眠状态，达到既保持覆盖质量又能延长网络生存时间的效果。本文将运行时间以时间片进行划分，每一个时间片又分为节点调度阶段和工作阶段，在调度阶段内节点通过下面的方法进行调度，判断是否参与覆盖任务。若参与，则在工作阶段一直保持在活动状态，否则进入到休眠状态直到下一个时间片来临。在给出具体算法之前，为了便于描述，首先给出相关节点集的定义。

定义 4 以网格点 p_i 为中心，处于相邻网格内或者边框上的传感器节点称为 p_i 的相关节点，p_i 的相关节点集我们用 Ω_i（$\Omega_i = \{n_1, n_2, \cdots, n_8\}$）来表示。根据设置的虚拟网格尺寸，$p_i$ 的相关节点均能覆盖到 p_i。很显然，p_i 的覆盖节点集 $S_i \subseteq \Omega_i$。

为了之后表述方便，把节点分为 4 类。第 1 类是属于且仅属于 S_i 中的节点集，用 $\widehat{S}_i$ 表示；第 2 类是属于但不仅属于 S_i 中的节点集，用 $\hat{S}_i$ 表示；第 3 类是不属于 S_i 但属于 $S_j (j \in \{N - \{i\}\})$ 的节点集，用 $\tilde{S}_i$ 表示；第 4 类是不属于 S_i 但也不属于任何 S_j 的节点集，用 $\bar{S}_i$ 表示。令 $\hat{\Omega}_i = \hat{S}_i \cup \tilde{S}_i = \{\hat{n}_1, \hat{n}_2, \cdots, \hat{n}_l\}$，它们对应的信任值为 $\{\hat{r}_1, \hat{r}_2, \cdots, \hat{r}_l\}$，并且 $\hat{r}_1 \geqslant \hat{r}_2 \geqslant \cdots \geqslant \hat{r}_l$。令 $\bar{S}_i = \Omega_i - \hat{\Omega}_i = \{\bar{n}_1, \bar{n}_2, \cdots, \bar{n}_f\}$，其中它们对应的信任值为 $\{\bar{r}_1, \bar{r}_2, \cdots, \bar{r}_f\}$，并且 $\bar{r}_1 \geqslant \bar{r}_2 \geqslant \cdots \geqslant \bar{r}_f$。令 $\Omega_i = \{n_1', n_2', \cdots, n_{l+f}'\}$，对应的信任值为 $\{r_1', r_2', \cdots, r_{l+f}'\}$，其中 $r_1' \geqslant r_2' \cdots \geqslant r_{l+f}'$。显然，若某一个节点 n_j 参与覆盖的网格点集 $W_{nj} = \{p_i\}$，则表示 $n_j \in \widehat{S}_i$；若 $W_{nj} = \{p_i, *\}$，$*$ 号表示数量大于 1 的网格点集，则表示 $n_j \in \hat{S}_i$；若 $W_{nj} = \varnothing$，则表示在工作阶段节点 n_j 不参与任何覆盖网格点的任务，它将调整到休眠状态。

p_i 获取对应的覆盖节点集 S_i 的算法基本原则如下：节点集的数量越小越优先，其次是在数量相同的情况下，优先选择 $\hat{\Omega}_i$ 中的节点。就是说，尽可能选择小的覆盖节点集，以减少对于单个网格来说处于工作状态的节点的数量；优先选择 $\hat{\Omega}_i$ 中的节点，是尽可能地在总量上减少节点处于工作状态的数量。基于该基本原则，算法的实现步骤如下：

初始化： 在节点调度阶段，根据系统参数 k_0、$T_{\max}$，计算出 $T^3_{\min}, T^5_{\min}, \cdots, T^{k_0}_{\min}$ 的值。将 Ω_i、$\bar{S}_i$ 和 $\hat{\Omega}_i$

中的节点按照信任值的大小从大到小的顺序依次排列。

步骤 1:令 $k=1$,若 Ω_i 中,$r_1' < T_{max}$,则执行步骤 2。否则,判断是否 $\hat{r}_1 \geqslant T_{max}$,若成立则让 $\hat{n}_1$ 单独执行覆盖 p_i 的任务,即 $S_i = \{\hat{n}_1\}$,$\hat{\Omega}_i$ 中的其它节点以及 $\bar{S}_i$ 中的节点都不再参与覆盖网格点 p_i 的任务。若不成立,则令 $S_i = \{\bar{n}_1\}$,$\hat{\Omega}_i$ 中的节点以及 $\bar{S}_i$ 中的节点都不再参与覆盖网格点 p_i 的任务。

步骤 2:令 $k=3$,将 Ω_i、$\bar{S}_i$ 和 $\hat{\Omega}_i$ 中信任值小于 T^3_{min} 的节点暂时剔除。判断 Ω_i 中是否存在 k 或者 k 个以上的节点,若没有,则执行步骤 3。若有,则判断节点集 $\{n_1', n_2', n_3'\}$ 得到的联合信任值是否大于等于 T_{max},若不成立,则执行步骤 3。若成立,判断 $\{n_1', n_2', n_3'\}$ 中哪些节点属于 $\hat{\Omega}_i$,然后首先尝试 k 节点集 $\{\hat{n}_1, \hat{n}_2, \hat{n}_3\}$,判断得到的联合信任值是否大于等于 T_{max},若成立,则 $S_i = \{\hat{n}_1, \hat{n}_2, \hat{n}_3\}$,若不成立,则将依次尝试将当前 k 节点集中属于 $\hat{\Omega}_i$ 的信任值最小的节点,与不属于 k 节点集、$\bar{S}_i$ 中的信任值最大的节点替换,直到满足得到的联合信任值大于等于 T_{max} 为止,若当前 k 节点集已等于 $\{n_1', n_2', n_3'\}$,则结束。例如,若 $n_1' = \hat{n}_1, n_3' = \hat{n}_2$,则依次尝试 $\{\hat{n}_1, \hat{n}_2, \hat{n}_3\}$、$\{\hat{n}_1, \hat{n}_2, \bar{n}_1\} = \{n_1', n_3', n_2'\}$;若仅 $n_1' = \hat{n}_1$,则依次尝试 $\{\hat{n}_1, \hat{n}_2, \hat{n}_3\}$、$\{\hat{n}_1, \hat{n}_2, \bar{n}_1\}$、$\{\hat{n}_1, \bar{n}_2, \bar{n}_1\} = \{n_1', n_3', n_2'\}$。

步骤 3:令 $k = 5 < k_0$,按照步骤 2 的方式进行。

…

步骤 $\frac{k_0+1}{2}$:当 $k = k_0$,将 Ω_i、$\bar{S}_i$ 和 $\hat{\Omega}_i$ 中信任值小于 T_{min} 的节点在本步骤中暂时剔除。判断 Ω_i 中是否存在 k_0 个或者 k_0 个以上的节点,若没有,则表明 p_i 不能实现高可靠覆盖。若有,由对信任模型的定义可知,节点集 $\{n_1', n_2', \cdots, n_{k0}'\}$ 得到的联合信任值一定大于等于 T_{max}。接着判断该节点集中哪些节点属于 $\hat{\Omega}_i$,然后首先尝试 $\hat{\Omega}_i$ 中所有的节点与 $\bar{S}_i$ 的信任值最大的那些节点共同组成 k_0 节点集,判断得到的联合信任值是否大于等于 T_{max}。若成立,则得到 S_i,若不成立,则将依次尝试将当前 k_0 节点集中属于 $\hat{\Omega}_i$ 的信任值最小的节点,与不属于 k_0 节点集、$\bar{S}_i$ 中的信任值最大的节点替换,直到满足得到的联合信任值大于等于 T_{max} 为止。若当前 k_0 节点集已等于 $\{n_1', n_2', \cdots, n_{k0}'\}$,则结束。

步骤 $\frac{k_0+1}{2}+1$:重新调整 Ω_i 中每一个节点参与覆盖的网格点集,根据各个节点的网格点集,重新生成 $\bar{S}_i$、$\hat{S}_i$、$\tilde{S}_i$ 和 $\setminus S_i$。

假设网格点 p_i 的相关节点集 $\Omega_i = \{n_1, n_2, \cdots, n_8\}$,如图 3 所示,在第 1 个时间片至第 4 个时间片各个节点信任值的变化情况如图(a)-(d)所示,假设在第 1 个时间片中 n_2 参与了除网格点 p_i 的其它覆盖任务。在第 2、3 个时间片中 n_1、n_2、n_3 参与了除网格点 p_i 的其它覆盖任务。在第 4 个时间片中 n_2、n_3 参与了除网格点 p_i 的其它覆盖任务。根据我们提出的算法,网格点 p_i 在各个时间片中对应的覆盖节点集如图 3 所示。通过该例子表明,本文算法既能完成高可靠覆盖网格点的任务,也能有效减少参与覆盖任务处于工作状态的节点的个数。

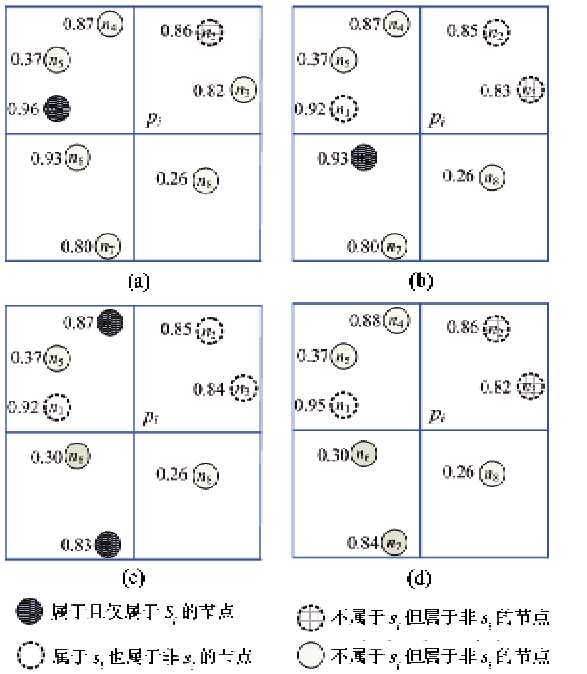

图 3　关于节点调度过程的演示

3　仿真实验

在仿真实验中,目标区域为 100m × 100m 的区域,节点个数为 30 ~ 400,节点的感知半径为 10m,通信半径为 30m,能量消耗模型与文献[12]相同,信任管理系统采用文献[9]中的 RFSN 系统。基于解释的目的,假设网络中有 $\alpha = 15\%$ 的恶意节点,剩余节点中 50% 的普通节点有 $\beta = 30\%$ 的概率发生非恶意的恶意行为,其他节点没有恶意行为。对于

其它的 α、β 值，可获得类似的观察结果。

为了比较算法的性能，基于 MATLAB 仿真平台，本文实现了文献[11]中的基于信任选择模型的节点调度覆盖算法(coverage-preserving node scheduling scheme based on trust selection model, CNSSTS)以及文献[12]中的节点覆盖调度(node self-scheduling, NSS)算法。前者属于一种仅仅根据节点阈值选择候选节点的节点调度覆盖算法，后者为一种没有整合信任管理的、经典的节点调度覆盖方法。本文将这两种算法与我们提出的基于信任管理的分布式高可靠覆盖算法(HRCMTM)在覆盖率和联合信任度等方面进行性能比较，以评价我们提出的这种将信任管理机制和覆盖算法整合成一体的高可靠覆盖机制的有效性和优劣性。

图 4 反映了在部署节点数量足够满足高可靠覆盖的情况下(设定为部署 400 个)，三种不同算法随网络运行时间的进行，各自覆盖率的变化。随着时间的增加，HRCMTM 算法获得的覆盖率变化幅度不大，达到第 280 轮时，覆盖率依然能维持在 80% 以上，而另外两个算法都远远低于了 80%。

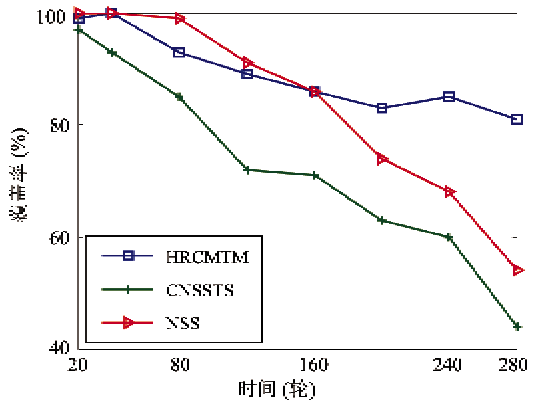

图 4 网络覆盖率随运行时间的变化

图 5 给出了部署节点数目与覆盖率的关系。从图中可以看到，虽然在节点较少的情况下，NSS 算法的覆盖率高于本文算法，但是随着部署节点数的增加，二者几乎可以同时达到完全覆盖。而 CNSSTS 算法，由于没有合理的调度，需要更多的节点才能达到要求。

图 6 反映的是三种不同算法随着整个网络运行时间的增加，目标区域平均的联合信任度的变化。从图中可以看到，随着时间的增加，HRCMTM 获得的联合信任度要大于 CNSSTS 算法，并且远大于 NSS 算法。

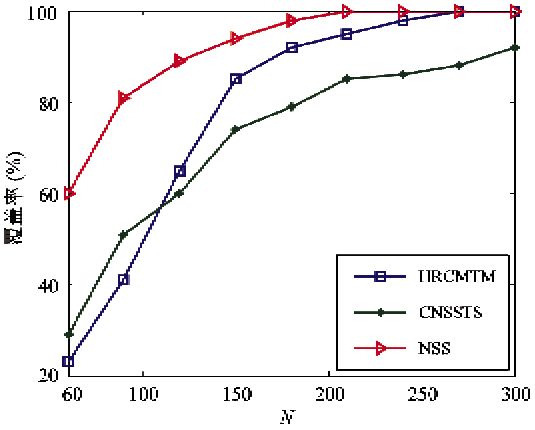

图 5 覆盖率随节点个数的变化

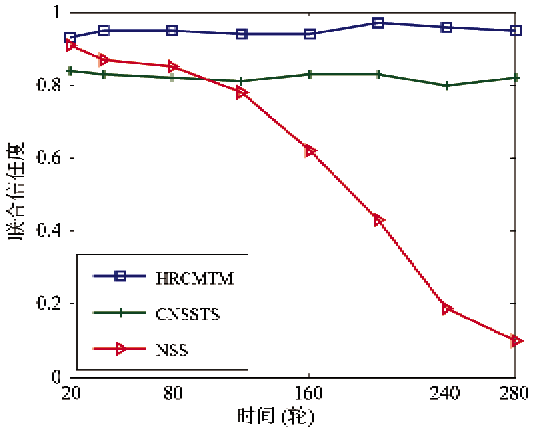

图 6 平均的联合信任度随运行时间的变化

4 结 论

本文提出了一种基于信任管理的分布式高可靠覆盖机制，解决了传感器网络中的安全覆盖问题。通过深入分析信任管理系统的潜在需求，推导出网格边长的上界应为 $\min(\frac{\sqrt{2}}{4Rc}, \frac{\sqrt{2}}{2Rs})$。在覆盖节点集个数限制在较小的 k_0 之内的约束下，分析推导出节点覆盖集包含的节点个数应为奇数在给定节点覆盖集大小的条件下，给出了动态信任阈值的求解方法。仿真实验表明，与以往的工作相比，本文提出的基于信任管理的高可靠覆盖算法，能有效地提高覆盖区域的联合信任度，增大目标区域的覆盖率。

针对任意部署的传感器节点，建立非网格式的传感器网络覆盖算法，将是我们下一步的工作任务。此外，如何进一步降低恶意节点对覆盖质量的影响，也是我们重点考虑的研究方向。

参考文献

[1] 唐秋玲,杨柳青,覃团发等. 无线传感器网络中 PPM 节能调制方案. 中国科学(E 辑:信息科学), 2007,37(12):1583-1596

[2] Liu Z Y, Lu S J, Yan J. Analytical models for trust based routing protocols in wireless ad hoc networks. *SIGSOFT Software Engineering Notes*, 2012, 37(4)

[3] Huang Y, Huang C. Cluster Algorithm for Electing Cluster Heads Based on Threshold Energy[C]. International Conference on Electrical and Control Engineering 2010, 2692-2695

[4] Feng H, Li G, Lu W, et al. Trust based secure in-network data processing schema in wireless sensor networks. *Journal of networks*, 2011, 6(2): 295-302

[5] Leligou H C, Trakadas P, Maniatis S, et al. Combining trust with location information for routing in wireless sensor networks. *Wireless Communications and Mobile Computing*, 2012, 12(12):1091-1103

[6] Zabihi S, Hadidi S, Khani M. A New Energy-Efficient Reliable Data Transfer Protocol for Data Transfer in WSN. *Journal of Basic and Applied Scientific Research*, 2012, 2(2):1972-1980

[7] 徐强,汪芸. 容错节能无线 WSN 中可靠覆盖问题的解决方案. 软件学报, 2006, 17(zk): 184-191

[8] Ma H D, Zhang X, Ming A. A Coverage-Enhancing Method for 3D Directional Sensor Networks. In: Proceedings of INFOCOM, Riode Janeiro, Brazil, 2009. 2791-2795

[9] Ganeriwal S, Srivastava M. Reputation-based framework for high integrity sensor networks. In: Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Network(SASN 2004), New York, USA, 2004. 66-77

[10] Bao F, Chen I R, MoonJeong Chang, et al. Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routin and Intrusion Detection. *IEEE Transactions on network and service management*,2012,9(2):169-183

[11] Yin Z, Zhao H, Lin K, et al. A coverage-preserving node scheduling scheme based on trust selection model in wireless sensor networks. In: Proceedings of ISPCA, Shenyang, China, 2006. 696-698

[12] Tian D, Georganas ND. A node scheduling scheme for energy conservation in large wireless sensor networks. *Wireless Communications and Mobile Computing*, 2003, 3(2):271-290

Highly reliable distributed coverage mechanism based on trust management for wireless sensor networks

Li Xiaolong*,**, Dong Shuhao*, Si Lijuan*, Liang Hai*

(*School of Computer Science and Engineering, Guilin University of Electronic Technology, Guilin 541004)

(**Guangxi Key Laboratory of Trusted Software, Guilin 541004)

Abstract

To realize the secure coverage in wireless sensor networks, a Highly Reliable distributed Coverage Mechanism based on Trust Management (HRCMTM) was proposed by integrating a coverage algorithm into a trust management system. Through the analysis of the underlying requirements of trust management systems, the proper grid size was derived theoretically. The new concept of dynamic trust threshold was introduced to quantitatively analyze the relationship between the size of coverage node set, the joint trust level and the dynamic trust threshold. Futher more, a node scheduling coverage algorithm was designed to guarantee that the target area is covered reliably. The experimental results demonstrated the effectiveness of this mechanism in terms of coverage ratio and joint trust level.

Key words: wireless sensor networks (WSN), trust management, highly reliable coverage mechanism, dynamic trust threshold, grid, distributed