# 一种有效的无线传感器网络安全路由方案

姚宣霞 郑雪峰 周 芳
(北京科技大学信息工程学院 北京 100083)

**摘 要** 为了在无线传感器网络中实现安全、有效的路由,根据节点的分组转发率、距离目标节点的距离和节点的剩余能量建立了一个本地信任模型。并利用所建立的信任模型和多目标决策技术,以节点的剩余能量、信任值、方向因子和到目标节点的距离为依据选择路由的下一跳节点,同时,在相邻节点之间使用基于对称密码体制的加密和认证机制,确保分组的安全转发。所提出的路由方案不但可阻止大多数路由攻击、实现安全路由,而且能够在网络寿命和有效性之间进行很好的平衡,实现有效的路由。

**关键词** 无线传感器网络,剩余能量,信任值,下一跳,多目标决策
**中图法分类号** TP393 **文献标识码** A

## Efficient Secure Routing Scheme for Wireless Sensor Networks

YAO Xuan-xia ZHENG Xue-feng ZHOU Fang
(School of Information Engineering, University of Science & Technology Beijing, Beijing 100083, China)

**Abstract** In order to realize secure and efficient routing in wireless sensor networks, a local trust model was built. In this local trust model, the trust value of a node was determined by the ratio of the packets delivery, the distance to the target sink node and the residual energy. And using this local trust model and the multiple criteria decision making technology, the next hop was chosen on the basis of the residual energies, the trust values, the direction factors and the distances to the target sink node of its neighbors. At the same time, the encryption and authentication mechanism based on the symmetric cryptography were used between neighboring nodes so as to ensure the secure packets forwarding. The proposed routing scheme can not only prevent most routing attacks and realize secure routing, but also can balance the life of the network and the efficiency of routing well to achieve efficient routing.

**Keywords** Wireless sensor networks, Residual energy, Trust value, Next hop, Multiple criteria decision making

在无线传感器网络(WSN, Wireless Sensor Networks)中,节点具有双重身份,既要完成感应和处理任务,又要完成路由功能。路由技术是无线传感器网络的关键技术,多跳路由是无线传感器网络的基本路由机制,路由协议往往与特定的应用相结合。常见的有基于查询的路由[1,3]、基于簇的路由[4]和基于位置的路由[5,6],它们一般假定网络中的节点都是正常节点,会相互合作完成数据转发,在设计时并没有考虑安全因素。事实上这种假设是不可靠的,多跳路由不仅有许多易于遭受攻击的特点,而且路由过程要受多种因素的影响。同时,无线传感器网络作为一种以数据为中心的网络,常用于军事和民用的各个领域进行监测和跟踪,一般部署在无人照看的环境中,并可能涉及到敏感的数据,安全问题非常严峻。因此,对无线传感器网络来说,安全、有效的路由至关重要,是完成其基本任务的关键。

## 1 相关工作

### 1.1 无线传感器网络的安全路由技术

在无线传感器网络中实现安全路由非常困难,最主要的问题是如何解决节点资源的局限性和安全性要求之间的矛盾,为此,必须使用尽可能轻量级的安全机制。基于对称密码体制的加密和认证是轻量级的安全措施,已被用于许多路由协议[11-13],它们可以抵御外部攻击,但不能抵御内部恶意的或被俘节点发起的路由攻击,如选择转发、女巫攻击等。信任技术可用于评估节点的行为,有助于抵御选择转发和女巫等路由攻击[7,8],不过目前还没有完善的无线传感器网络信任模型。例如,基于信任的路由框架[7]虽然有助于检测失败节点的无效性和被俘节点的选择转发攻击,但只根据分组的重传率和分组转发的协同性估计节点的行为过于简单,且不能及时反映节点的真实状态。文中,尝试根据节点的分组转发率、剩余能量和距离目标节点的距离,建立一个新的本地信任模型,以对其邻居节点的信任度作出正确评估。

### 1.2 无线传感器网络路由决策的依据

根据无线传感器网络的特点,能量是其进行各项操作首先要考虑的问题,也是路由决策的基本依据[4,10]。不过只简单地将能量作为路由决策依据不能实现高效率的路由。目前,虽然已有一些路由协议[9]将距离或跳数与能量开销同时

到稿日期:2008-08-29 返修日期:2009-02-05
姚宣霞(1971-),女,博士,讲师,CCF会员,主要研究方向为网络与信息安全和无线传感器网络,E-mail:yaoxuanxia@163.com;郑雪峰(1951-),男,教授,博士生导师,主要研究方向为网络与信息安全;周 芳(1972-),女,博士研究生,讲师,主要研究方向为网络安全。

作为路由选择的依据以提高路由的效率，但仍然不能在路由效率和网络寿命之间进行很好的平衡。本文所提出的安全路由方案采用能量均衡策略来延长网络的寿命，将节点的剩余能量、信任值、节点到目标汇聚节点的距离以及方向因子同时作为路由选择的依据，并从简单的角度出发，使用多目标决策技术中的平方和加权法进行路由选择，可在实现安全路由的同时，缩短延迟、延长网络寿命。

## 2 模型描述

为了便于描述，需要对本方案运行的网络、所使用的能量模型、节点之间距离的测算方法以及信任模型分别进行说明。

### 2.1 网络模型

在本方案中，我们对网络作了如下假设。

1)所运行的网络是一个大型静态网络，网络中的所有节点均匀分布在目标区域中，对大多数节点来说，它们到汇聚节点需要多跳，而且，网络的密度足够大，使得每个节点有多个邻居节点。链路是双向的，邻居关系是相互的。

2)所有传感器节点的初始能量、通信半径(范围)、计算能力、存储空间和在网络中的地位都相同。节点的能量很有限，每个节点只与其邻居节点通信，且每次通信的距离都等于其通信半径。每个节点都具有 RSSI 测距功能(根据到达信号的强度进行测距的功能)，距离的单位为 0.1 倍的 $dr$，其中 $dr$ 是节点的通信半径。

3)网络中可以有多个汇聚节点，所有汇聚节点都是可信的、且有足够的资源。每个汇聚节点与各传感器节点共享一个唯一的密钥。每个汇聚节点可以直接向网络中的所有传感器节点广播信息。

4)每对相邻传感器节点之间都有一个共享密钥，以保证通信的安全性。

### 2.2 能量模型

在无线传感器网络中，能量主要消耗在分组的收发过程中。本文使用 W. R. Heinzelman 等人提出的能量模型[10]计算节点的剩余能量。在该模型中，如果节点 $i$ 向节点 $j$ 发送 $k$ 位数据，那么节点 $i$ 消耗的能量为：

$$E_i = E_{elec} \cdot k + \varepsilon_{amp} \cdot k \cdot d^2 \tag{1}$$

其中，$E_{elec}=50nj/\text{bit}$，$\varepsilon_{amp}=100pJ/\text{bit}/\text{m}^2$，$d$ 是节点 $i$ 到节点 $j$ 的距离。在本方案中，由于每个节点只与其邻居节点通信，并且总是以与节点的通信范围对应的能量级别发送数据，因此，$d$ 等于节点的通信范围 $dr$。

节点 $j$ 消耗的能量为：

$$E_j(k) = E_{elec} \cdot k \tag{2}$$

这样，每个接收并转发数据的中间节点 $i$ 消耗的能量为：

$$E_i = 2 \cdot E_{elec} \cdot k + \varepsilon_{amp} \cdot k \cdot d^2 \tag{3}$$

从而，节点 $i$ 的剩余能量 $ER_i$ 可定义为：

$$ER_i = ER_i - E_i \tag{4}$$

显然，节点的剩余能量在 0 和 $E_{max}$ 之间，$E_{max}$ 是节点的初始能量。在网络部署之初，所有节点的剩余能量相同，均为 $E_{max}$。需要说明的是，不同的应用对节点的最小剩余能量有不同的要求，不一定总是 0，为了方便描述，用 $E_{min}$ 表示节点剩余能量的下限。如果一个节点的剩余能量小于应用所要求的 $E_{min}$，该节点就成为不可用节点。在无线传感器网络正常工作期间，每个可用节点应根据其自身的行为，及时更新其剩余能量，并向其邻居节点作周期性的报告。如果一个节点在两个连续的周期内都没有收到其某个邻居节点的报告，就认为该邻居不可用，并将其从邻居节点列表中删除。

### 2.3 节点之间距离的测量

根据 2.1 节中的网络模型，节点之间距离的测量采用 RSSI 测距技术，在初始化阶段完成。节点 $i$ 和节点 $j$ 之间的距离用 $D_{i,j}$ 表示，$i$ 和 $j$ 既可以是一般的传感器节点也可以是汇聚节点。具体测距时，可以分为两种情况：一是相邻节点之间距离的测量，根据收到的邻居发现消息的信号强度，估算与该邻居节点之间的距离。二是各传感器节点与各汇聚节点之间距离的测量，具体做法见 3.1 节。

### 2.4 信任模型

在本方案中，为了对节点的信任值进行客观、正确的评价，引入了 3 个信任评估因子，即基于分组转发的信任评估因子、基于剩余能量的信任评估因子和基于距离的信任评估因子。

#### 2.4.1 基于分组转发的信任评估因子

分组转发率是评估节点可信度的一个重要因素，节点 $i$ 到其邻居 $j$ 的动态分组转发率可定义为：在一个给定的时间窗口内，从节点 $j$ 收到应答的分组个数与从节点 $i$ 向节点 $j$ 转发的所有分组数之比[7]。根据节点的分组转发率，可将基于分组转发的信任评估因子 $TF_{i,j}$ 定义为：

$$TF_{i,j} = \begin{cases} \dfrac{reply_{i,j}}{n_{i,j}}, & n_{i,j} > 0 \\ T_{i,j} \cdot \dfrac{Treply_{i,j}}{Tn_{i,j}}, & n_{i,j} = 0 \end{cases} \tag{5}$$

其中，$n_{i,j}$ 和 $reply_{i,j}$ 分别是在当前时间窗口内从节点 $i$ 向节点 $j$ 转发的分组数和节点 $i$ 从节点 $j$ 收到应答的分组数。$Tn_{i,j}$ 和 $Treply_{i,j}$ 分别是从开始到现在从节点 $i$ 向节点 $j$ 转发的所有分组数和节点 $i$ 从节点 $j$ 收到应答的分组个数。$T_{i,j}$ 是在前一个时间窗内计算的节点 $i$ 对节点 $j$ 的信任值。

#### 2.4.2 基于剩余能量的信任评估因子

相邻节点之间关于剩余能量的周期性通告对节点行为具有一定的暗示作用，因此，可将邻居节点在周期性通告消息中声称的剩余能量作为计算信任值的一个参数。该参数能够尽可能早地检测到恶意节点。

按照 2.2 节中所描述的能量模型，每个节点可根据它要求其邻居节点转发分组的情况估算其邻居节点的剩余能量。通过对估算值和节点实际报告的剩余能量值的对比，可以及时发现恶意节点。假定节点 $i$ 对节点 $j$ 估算的剩余能量用 $EE_{i,j}$ 表示，节点 $j$ 向节点 $i$ 报告的剩余能量为 $ER_j$，那么节点 $i$ 对节点 $j$ 基于剩余能量的信任评估因子可以定义为：

$$TE_{i,j} = \begin{cases} 0, & EE_{i,j} \geqslant ER_j \geqslant E_{min} \\ -0.5, & \text{其他情况} \end{cases} \tag{6}$$

#### 2.4.3 基于距离的信任评估因子

根据 2.1 节中的网络模型，邻居节点到目标汇聚节点的距离和节点自己到目标汇聚节点的距离之间存在着一定的关系。即：如果节点 $i$ 到目标汇聚节点 $x$ 的距离为 $D_{i,x}$，那么从节点 $i$ 的邻居节点 $j$ 到 $x$ 的距离 $D_{j,x}$ 的最小值和最大值应分别为 $(D_{i,x}-10)$ 和 $(D_{i,x}+10)$。根据该关系，能够在一定程度上推断某个邻居节点是否为恶意节点。这样，节点 $i$ 对其邻居节点 $j$ 基于距离的信任评估因子可定义为：

$$TD_{i,j}=\begin{cases}0,(D_{i,x}-10)\leqslant D_{j,x}\leqslant(D_{i,x}+10)\\-0.5,D_{j,x}<(D_{i,x}-10)\text{或}\ D_{j,x}>(D_{i,x}+10)\end{cases}\tag{7}$$

2.4.4 信任值的计算

根据上述的3个信任评估因子，将节点 $i$ 对其邻居节点 $j$ 的信任值 $T_{i,j}$ 定义为：

$$T_{i,j}=TF_{i,j}\cdot(1+TE_{i,j}+TD_{i,j})\tag{8}$$

在初始状态，所有节点的信任值都被置为1，显然，$T_{i,j}$ 应为0和1之间的一个值。由于每个应用对节点信任值的要求不同，为了便于描述，将节点信任值的阈值用 $\theta$ 表示。

在无线传感器网络的正常生命期内，每个节点应按照该信任模型周期性地维护其所有邻居节点的信任值以保持其新鲜性。

## 3 算法描述

本路由方案包括3个阶段，即初始化阶段、路由发现或分组转发阶段及确认阶段。

### 3.1 初始化阶段

初始化阶段可以被进一步划分为离线初始化和在线初始化两个阶段。在离线初始化阶段，部署服务器将用于为相邻节点建立共享密钥的安全资料和一些参数的初始值分配给每个节点，例如将节点的初始信任值置为1。在线初始化阶段的任务主要包括5个方面。

1)计算节点到各汇聚节点的距离。为了简单起见，先考虑网络中只有一个汇聚节点的情况。汇聚节点以能够覆盖整个网络的能量向网络广播 hello 消息。每个节点根据收到的 hello 消息的信号强度计算它到汇聚节点的距离。如果网络中有多个汇聚节点，让各汇聚节点依次向整个网络广播 hello 消息，每个节点可以同样的方式计算它到各汇聚节点的距离。

2)每个节点通过广播邻居发现消息进行邻居发现，并根据收到的邻居发现消息的强度计算它到各邻居节点的距离，为每个节点构造邻居节点列表。

3)按照选定的密钥管理方案，例如，分组密钥预分配方案[14,15]为相邻节点建立共享密钥。

4)为每个节点 $i$，构造它到每个汇聚节点 $x$ 的下一跳候选节点集合 $LN_{i,x}$。集合 $LN_{i,x}$ 中节点与节点 $i$ 相邻，且到汇聚节点 $x$ 的距离不大于节点 $i$ 到 $x$ 的距离。如果集合 $LN_{i,x}$ 为空，汇聚节点 $x$ 将被节点 $i$ 标记为不可用。

5)为每个节点建立黑名单。显然，在刚开始时，黑名单为空。

### 3.2 路由发现阶段

在本方案中，路由发现过程即分组转发过程。路由发现阶段的主要任务是选择下一跳邻居节点并将分组转发给它。

为了在实现安全路由的同时延长网络的寿命，路由决策过程被分成两个子过程，在第一个子过程中，根据候选节点集合，建立信任值和剩余能量都满足应用要求的待选节点集合。在第二个子过程中，根据剩余能量、方向因子和到目标汇聚节点的距离，从第一个子过程所建立的待选节点集合中选出下一跳节点。同时，为了满足路由决策的简单性要求，在第二个子过程中，采用平方和加权法进行路由决策。在三个路由决策依据中，方向因子和到目标汇聚节点的距离反映了节点经候选节点到目标节点的物理距离，具有同等重要性。而从网络的寿命考虑，节点的剩余能量要比方向因子和到目标汇聚节点的距离更加重要，因此，将节点的剩余能量、到目标汇聚节点的距离和方向因子的权重因子分别设置为0.4，0.3和0.3。

具体地，对于节点 $i$，本路由方案按如下步骤工作。

第一步　如果节点 $i$ 为源节点，应在所有可用汇聚节点中找出一个与之距离最小的汇聚节点 $x$ 作为目标汇聚节点。否则，直接进入第二步。

第二步　节点 $i$ 查看集合 $LN_{i,x}$ 中是否有目标汇聚节点 $x$，若有，直接将 $x$ 作为下一跳节点，转到第八步。

第三步　如果节点 $i$ 中已有集合 $STE_{i,x}$，将其清空，否则为节点 $i$ 产生一个空集合 $STE_{i,x}$。

第四步　对于集合 $LN_{i,x}$ 中的每个节点 $j$，计算 $i$ 对它的信任值 $T_{i,j}$，如果 $T_{i,j}$ 不小于信任值的阈值 $\theta$，并且节点 $j$ 的剩余能量 $ER_j$ 能满足应用的需要，将 $j$ 放入 $STE_{i,x}$ 中。否则，节点 $i$ 将从集合 $LN_{i,x}$ 中删除节点 $j$。如果 $T_{i,j}$ 小于信任的阈值 $\theta$，将 $j$ 放入节点 $i$ 的黑名单中。

第五步　如果集合 $STE_{i,x}$ 为空，并且 $i$ 为源节点，将汇聚节点 $x$ 标记为不可用，返回第一步。

第六步　如果集合 $STE_{i,x}$ 为空，且 $i$ 不是源节点，节点 $i$ 向前趋节点 $p$ 报告它没有满足安全性和能量要求的邻居节点。节点 $p$ 收到该报告后，将节点 $i$ 从集合 $STE_{p,x}$ 中删除。如果不幸 $STE_{p,x}$ 也变为空，从第五步开始执行。

第七步　对于集合 $STE_{i,x}$ 中的每个节点 $m$，分别计算 $A_m$ 和 $ERDA_{m,x}$。其中，$A_m$ 是节点 $i$ 与汇聚节点 $x$ 和节点 $m$ 的夹角 $\angle ixm$ 的余弦值，$ERDA_{m,x}$ 是按照平方和加权法计算的决策值。

$$A_m=(D_{m,x}{}^2+D_{i,x}{}^2-D_{i,m}{}^2)\div(2\cdot D_{m,x}\cdot D_{i,x})\tag{9}$$

$$ERDA_{m,x}=0.3(DM-D_{m,x})^2+0.4(ERM-ER_m)^2+0.3(AM-A_m)^2\tag{10}$$

其中，$DM$ 是集合 $STE_{i,x}$ 中的节点到目标汇聚节点 $x$ 的距离中的最小值，$ERM$ 是集合 $STE_{i,x}$ 中节点的剩余能量的最大值，$AM$ 是 $A_m$ 的最大值。

具有最小 $ERDA_{m,x}$ 的节点是下一跳的最佳选择节点。如果不止一个节点具有最小的 $ERDA_{m,x}$ 值，可从中随机选择一个作为下一跳节点，或选择 $A_m$ 的值最大者作为下一跳节点。假定节点 $t$ 是所选择的下一跳节点。

第八步　节点 $i$ 构造分组，并用 $i$ 和下一跳节点 $t$ 的共享密钥对分组中的数据加密，然后转发给节点 $t$。同时，节点 $i$ 更新自己的剩余能量，估算节点 $t$ 的剩余能量，并将 $n_{i,t}$ 和 $Tn_{i,t}$ 分别加1。

第九步　节点 $t$ 收到节点 $i$ 转发给它的分组后，如果 $t$ 为目标汇聚节点，进入确认阶段，否则，$t$ 成为一个新的中继节点，转到第二步重复该过程。

### 3.3 确认阶段

在本方案中，一条路由需持续到超时或收到相应的确认分组。当分组被成功地转发到目标汇聚节点 $x$ 后，汇聚节点 $x$ 会沿着路由的反方向为源节点发送确认消息。如果某个节点 $u$ 不是源节点，并且在超时之前从其邻居 $v$ 收到了由目标汇聚节点 $x$ 发给源节点的确认分组，它会将此确认分组转发给它在该路由中的前趋节点 $p$，并删除该路由。同时分别对 $reply_{u,v}$ 和 $Treply_{u,v}$ 加1，更新剩余能量的相关信息。节点 $p$

收到确认任分组后，重复节点 $u$ 的工作，该过程继续直到确认分组到达源节点。源节点收到确认分组后只需删除路由，并进行相关的更新操作即可。

## 4 性能分析

首先，本文提出的安全路由方案具有较好的安全性。主要体现在4个方面。第一，由于每次通信都需要建立路由，因此，针对路由信息的欺骗、篡改等攻击就没有了生存的机会。第二，由于相邻节点之间共享一个唯一的密钥，分组和确认信息都可以被加密和认证，因此能够实现通信的机密性和完整性。第三，通过使用信任值、剩余能量、方向因子以及到目标节点的距离来选择下一跳节点，可以避免选择转发攻击、污水井攻击、蛀洞攻击和女巫攻击。第四，所建立的本地信任模型可以帮助节点根据它和邻居节点之间的消息或行为，及时调整它对邻居节点的信任值，使得信任值能够真实地反映节点的当前状态。

其次，本方案比较简单，所有操作都是一些简单的数学运算、集合运算和加解密运算，能够满足无线传感器路由的简单性要求。

另外，本方案具有低开销、低延迟等特点，能够适应节点的动态变化等。

最后，本方案也存在一些缺陷，例如，没有考虑数据的汇聚，相邻节点之间的周期性通告消息会造成资源的浪费，没有对权重因子进行优化，所建立的信任模型也还有待于在更多的应用中进行验证等。

**结束语** 安全路由是无线传感器网络正常工作的关键。一条路由对应一次通信的策略能够适应节点的动态变化，避免了针对路由信息的各种攻击。在相邻节点之间的通信采用加密和认证机制，可以保证通信的机密性和完整性，抵御各类外部攻击。利用信任技术可以避免选择转发、女巫等内部攻击。综合考虑影响路由的众多因素可以在路由的有效性和网络的寿命之间进行较好的平衡。本文所提出的综合安全路由方案正是在这些策略的基础上形成的，并采用目标节点确认机制以进一步验证路由和信任值的正确性，能够在实现安全路由的同时缩短延迟、延长网络寿命。

## 参 考 文 献


[1] Intanagonwiwat C, Govindan R, Estrin D, et al. Directed diffusion for wireless sensor networking[J]. IEEE/ACM Trans. on Networking, 2002, 11(1): 2-16

[2] Braginsky D, Estrin D. Rumor Routing Algorthim for Sensor Networks[C] // Proceedings of the 1st ACM International Workshop on Wireless Sensor Networks and Applications. Atlanta, Georgia, USA. ACM Press, 2002: 22-31

[3] Chu M, Haussecker H, Zhao F. Scalable information-driven sensor querying and routing for ad hoc heterogeneous sensor networks[J]. The Int'l Journal of High Performance Computing Applications, 2002, 16(3): 293-313

[4] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy-efficient communication protocol for wireless sensor networks [C]// IEEE Proceedings of the Hawaii International Conference on System Sciences. Washington: IEEE Communications Society, 2000: 175-187

[5] Karp B, Kung H T. GPSR: Greedy perimeter stateless routing for wireless networks[C]// Proc. of the 6th Annual Int'l Conf. on Mobile Computing and Networking. Boston, MA, ACM Press, 2000: 243-254

[6] Yu Y, Estrin D, Govindan R. Geographical and Energy Aware Routing: a recursive data dissemination protocol for wireless sensor networks[OL]. http: // www2. parc. com/spl/members/zhao/stanford-cs428/readings/ Networking/Estrin_geo-routing01. pdf. 2001

[7] Cheng Weifang, Liao Xiangke, Shen Changxiang, et al. A Trust-Based Routing Framework in Energy-Constrained Wireless Sensor Networks[C]// WASA 2006. LNCS 4138, 2006: 478-489

[8] Ganeriwal S, Srivastava M. Reputation - based framework for high integrity sensor networks[C]// Proceedings of 2nd ACM workshop on security of ad hoc networks. 2004: 66-77

[9] Zeng Kai, Ren Kui, Lou Wenjing, et al. Energy - Aware Geographic Routing in Lossy Wireless Sensor Networks with Environmental Energy Supply[C]// QShine'06, The International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks. Waterloo, ON Canada, August 2006

[10] Heinzelman W R, Chandrakasan A, Balakrishnan H. Energy efficient communication protocol for wireless micro-sensor networks[C]// Proceedings of the IEEE Hawaii International Conference on System Science. January 2000

[11] Perrig A, Szewczyk R, Wen V, et al. SPINS: security protocols for sensor networks[C]// Seventh Annual ACM International Conference on Mobile Computing and Networks (Mobicom 2001). Rme, Italy, July 2001: 189-199

[12] Karlof C, Sastry N, Wagner D. TinySec: A Link Layer Security Architecture for Wireless Sensor Networks[C]// Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems(SenSys 2004). November 2004: 162-175

[13] Capkun S, Buttyan L, Hubaux J - P. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks[C]// ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN). Washington, USA, October 2003

[14] Li Guorui, He Jingsha, Fu Yingfang. Key Pre - distribution in Sensor Networks[C]// UIC 2006, LNCS 4159. 2006: 845-853

[15] Liu Donggang, Ning Peng, Du Wenlisng. Group-Based Key Pre-Distribution in Wireless Sensor Networks[C]// Proceedings of the 4th ACM workshop on wireless security. Cologne Germany: ACM Press, 2005: 11-20