文章编号：2095-4980(2020)05-0924-05

WSNs 中基于密钥共享的安全路由

谷　波

(南阳医学高等专科学校第一附属医院 信息科，河南 南阳 473058)

摘　要：针对无线传感网络的安全路由，提出能效和安全多跳路由(ESMR)。ESMR 路由通过密钥共享策略，提高路由防御恶意节点的性能。ESMR 路由先依据节点的位置将网络划分不同区(Zone)，在每个 Zone 内，依据邻居节点位置划分多个簇；然后，每个 Zone 的簇头向基站传输数据，并依据密钥共享策略对数据进行加密。仿真结果表明，相比于同类路由，提出的 ESMR 在网络寿命、吞吐量、能耗以及端到端时延方面的性能得到有效提高。

关键词：无线传感网络；多跳路由；区；簇；密钥共享

中图分类号：TN915.05；TP393　　**文献标志码：**A　　**doi：**10.11805/TKYDA2019346

Secret key sharing-based security routing in Wireless Sensor Networks

GU Bo

(The First Affiliated Hospital of Nanyang Medical College，Information Center，Nanyang Henan 473058，China)

Abstract：For secure routing of Wireless Sensor Networks(WSNs), Energy-aware and Secure Multi-hop Routing(ESMR) is proposed. ESMR protocol increases the performance of energy efficiency with multi-hop data security against malicious actions. The network field is segmented into inner and outer zones based on the node location. Furthermore, in each zone, numerous clusters are generated on the basis of node neighborhood vicinity. Secondly, the data transmission from cluster heads in each zone towards the sink node is secured by using the proposed efficient secret key sharing scheme. The experimental results demonstrate the efficacy of proposed ESMR in terms of network lifetime, network throughput, energy consumption, average end–to–end delay in comparison with the existing work.

Keywords：Wireless Sensor Network；multi-hop routing；zone；cluster；secret key sharing

无线传感网络(WSNs)由大量微型的传感节点构成。这些传感节点先感测数据，再将数据传输到基站[1-2]，最后，由基站进行数据融合，再传输至控制中心。与传统的无线网络不同，WSNs 内的节点在处理能力、存储容量和能量方面存在限制，对 WSNs 内的数据收集提出了挑战。

多数传感节点需以多跳方式将数据传输至基站。因此，网络内的传感节点既要感测数据，又要转发数据，即扮演转发节点的角色[3]。若传感节点是诚实的，它能依据路由决策转发数据；反之，若传感节点是恶意的，它可能故意不转发，或篡改数据。这就涉及到路由安全问题。

此外，在多数 WSNs 应用中，传感节点自行操作(感测数据、转发数据)，容易受到安全攻击。文献[4–6]针对 WSNs 提出了不同的安全路由协议，但这些策略要求加密和认证操作，增加了传感节点的处理任务和路由成本[7-8]。文献[9]提出了环境信任传感路由(Ambient Trust Sensor Routing，ATSR)。ATSR 通过评估邻居节点的信任值，检测恶意节点。但 ATSR 是通过泛洪路由请求和路由响应包收集邻居节点信息，加大了能量消耗。类似地，文献[10]基于按需平均距离向量路由(Ad hoc On-Demand Distance Vector routing，AODV)，提出友善的 AODV 改进路由(Friendship based AODV，Fr-AODV)。Fr-AODV 通过估计节点声誉和节点身份，估计节点的信任值，但 Fr-AODV 采用了与 AODV 相类似的路由维护策略，也存在路由重发现和重传困境问题。文献[11]提出信任感知的安全路由框架(Trust-aware Secure Routing Framework，TSRF)。通过 TSRF 处理恶意节点的不正当行

收稿日期：2019-09-16；**修回日期：**2019-12-16
基金项目：国家自然科学基金资助项目(61172113)
作者简介：谷　波(1978–)，男，硕士，工程师，主要研究方向为网络信息安全。email:chen_leiei98@21cn.com

为。TSRF 估计了节点的直接和间接信任，并通过一致性检测避免恶意节点的攻击。但估计节点信任消耗节点较多能量，增加了节点负担。

为此，提出能效和安全多跳路由(ESMR)。ESMR 先依据传感节点离基站位置，将节点划分不同 Zone，再利用 k-最近邻居(k-Nearest Neighbor，k-NN)算法将 Zone 划分多个簇。然后，由簇头构成多跳路由。同时，通过密钥共享策略，簇头对数据进行加密，再将加密后的数据传输至基站。基站接收到加密数据后进行解密，进而获取数据。仿真结果表明，提出的 ESMR 有效提高了网络寿命，并降低了端到端传输时延。

1　系统模型

假定在传感区域 Ω 内随机部署 N 个传感节点，其中有 M 个恶意节点。每个传感节点具有相同的通信半径 R，相同的初始能量 E_{init}。

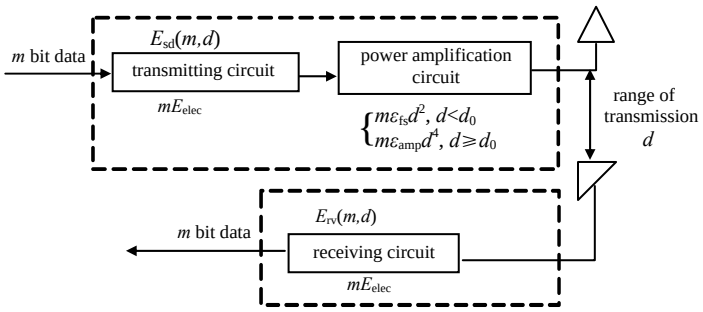

Fig.1 Model of energy consumption

图 1　能耗模型

考虑如图 1 所示的能耗模型[12]。传感节点每传输 d 米，传输 m 个比特数据，所消耗的能量为：

$$E_{\text{Tx}}(m,d)=\begin{cases} mE_{\text{elec}}+m\varepsilon_{\text{fs}}d^2, & \text{if } d\leqslant d_0 \\ mE_{\text{elec}}+m\varepsilon_{\text{amp}}d^4, & \text{if } d>d_0 \end{cases} \tag{1}$$

式中：E_{elec} 为发射电路每发射单比特数据所消耗的能量；$\varepsilon_{\text{fs}},\varepsilon_{\text{amp}}$ 分别为自由空间、双径衰落传输模型下的能量消耗因子；d_0 为判定自由空间和双径衰落的距离阈值，其定义如式(2)所示：

$$d_0=\sqrt{\frac{\varepsilon_{\text{fs}}}{\varepsilon_{\text{amp}}}} \tag{2}$$

若接收 m 比特数据，则消耗的能量 $E_{\text{Rx}}(m)$为：

$$E_{\text{Rx}}(m)=mE_{\text{elec}} \tag{3}$$

2　ESMR

2.1 区域构建

最初，基站向监测区域传输自己的身份和位置信息。一旦接收信息，传感节点就此信息存储于路由表中。然后，依据基站的距离定义每个区(Zone)的边界：

$$(\beta-1)\alpha<Z_\beta<\alpha\beta \tag{4}$$

式中：β 为 Zone 号，且 $\beta\in(1,2,\cdots,v)$，v 为总的 Zone 数；α 为预设的距离，如第 2 个 Zone(Z_2)，结合式(4)，可得 $\alpha<Z_2<2\alpha$。

令 Z_1 表示离基站最近的第 1 个 Zone。离基站越近的节点，向基站传输数据所消耗的能量越小；反之，需要消耗更多的能量。

划分 Zone 后，每个 Zone 进一步划分为簇。考虑节点能耗，引用轻量级的、简单的 k-NN 算法构建簇。每个 Zone 划分不同的簇，且给每个簇分配唯一的 ID 号。此外，为降低网络成本，将最靠近簇区中心位置的节点作为初始簇头。假定在特定簇 C_i 内有 n 个传感节点($s_1,s_2,s_3,\cdots,s_n$)，可依式(5)计算该簇 C_i 的中心位置：

$$C_i(\hat{x}_i,\hat{y}_i)=\frac{\sum_{i=1}^{n}x_i}{n}+\frac{\sum_{i=1}^{n}y_i}{n} \tag{5}$$

算法 1 为构建区和簇的过程。先计算离基站距离，然后依据式(4)构建 Zone。再将 Zone 划分不同簇，并计算簇头。

算法 1:

step 1: procedure zones_construction (Z)
step 2: compute neighbors distance and produce a routing table
step 3: compute dynamic distance: $(d)=(\beta-1)\alpha<Z_\beta<\alpha\beta$
step 4: for each node $i\in[1:d]$ do
step 5: decompose the nodes into particular zones Z_i
step 6: end for
step 7: if $Z_i[]!=\text{Null}$
step 8: partition the zone nodes into clusters C_i using k-NN
step 9: end if
step 10: for each node $i\in C_i$ do
step 11: compute centroid by equation(4)
step 12: node nearest to centroid is considered to be cluster header
step 13: end for
step 14: end procedure

2.2 基于 XOR 的加密

一旦划分了不同 Zones 后(Z_β)，离基站最近的区称为 Z_1，紧接着为 $Z_{\beta=2}$。首先，基站随机产生 v 个密钥 $(k_1,k_2,\cdots,k_v)$，每个密钥的尺寸为 b 比特；然后将密钥 k_v 传输至相应的 Z_v 内所有簇头[13]，簇头将数据 Data_v 与密钥 k_v 进行 XOR 操作，如式(6)所示：

$$E_v=Data_v\oplus k_v \tag{6}$$

E_v 为通过 XOR 加密后的数据。E_v 是处于区 Z_v 内的数据，Z_v 内的簇头就向区 Z_{v-1} 的簇头转发加密数据 E_v。一旦收到 E_v，区 Z_{v-1} 内簇头就利用本区的秘密 k_{v-1} 进行 XOR 操作加密。重复上述过程，直到数据传输至基站，如式(7)所示：

$$Data=k_1\oplus k_2\oplus k_3\oplus\cdots\oplus E_v \tag{7}$$

算法 2 为基于 XOR 的加密过程。基站接收到加密数据后进行解密，进而获取原始数据。

算法2：基于XOR的加密

step 1: Procedure secure multi-hop routing
step 2: BS generates random keys $(k_1,k_2,\cdots,k_v)$
step 3: k_i key is transmitted to cluster head Ch_i in Z_i
step 4: data packets D_v is encrypted with k_v
step 5: upper most zone Z_i encrypts data and forwards to BS
step 6: BS decrypts data using XOR and a set of secret keys
step 7: end procedure

3 性能仿真

3.1 仿真环境

利用 NS2++软件建立仿真平台。在 Ω=100 m×100 m 区域随机部署 N=100 个节点，恶意节点 M=1~5。具体仿真参数如表 1 所示。

为更好地体现 ESMR 性能，选择 Fr-AODV 和 TSRF 作为参照，并分析它们网络寿命、路由吞吐量、端到端时延的性能。

表 1 仿真参数

Table1 Parameters of simulation

parameter	value
range of simulation	Ω=100 m×100 m
number of nodes	100
number of malicious nodes	1–5
E_{elec}/(nJ/bit)	100
ε_{amp}/(nJ/bit/m^2)	100
ε_{fs}/(pJ/bit/m^4)	0.001 3
initial energy of node/J	2
range of nod's communication/m	25
simulation time/s	1 000

3.2 数据分析

3.2.1 网络寿命

网络寿命随恶意节点变化情况如图 2 所示。从图 2 可知，恶意节点数的增加，降低了网络寿命。这主要是恶意节点故意发布路由信息，转发路由数据包，加大了节点能耗，因此，缩短了网络寿命。

此外，相比于 Fr-AODV 和 TSRF 路由，ESMR 的网络寿命得到有效提升。相比 TSRF，ESMR 的网络寿命平均提高了 38%。原因在于 Fr-AODV 和 TSRF 在选择转发节点时，没有考虑网络拓扑信息，加大了节点能耗。

3.2.2 网络吞吐量

网络吞吐量随恶意节点数变化情况如图 3 所示。从图 3 可知，恶意节点数对网络吞吐量的影响并不大。恶意节点数在 1~5 变化期间，网络吞吐量变化较稳定。相比 Fr-AODV 和 TSRF，ESMR 的网络吞吐量得到有效提升，平均提高了近 34%。原因在于 ESMR 对数据进行了加密，避免了恶意节点丢失数据包。而 Fr-AODV 和 TSRF 并没有检测网络条件，转发数据包。

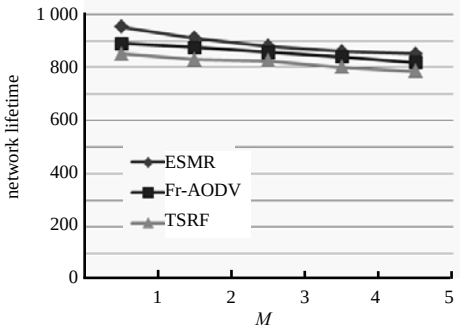

Fig.2 Network lifetime
图 2 网络寿命

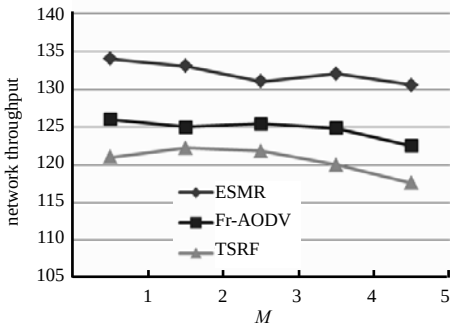

Fig.3 Network throughput
图 3 网络吞吐量

3.2.3 能量消耗

恶意节点对网络能耗的影响如图 4 所示。从图 4 可知，恶意节点数的增加，提升了网络能耗。相比于 Fr-AODV 和 TSRF，ESMR 的能耗得到有效控制。相比 TSRF，ESMR 的能耗降低了近 34%。Fr-AODV 和 TSRF 没有考虑网络条件，增加了路由断裂次数，传感节点需要重建路由，加大了能耗。

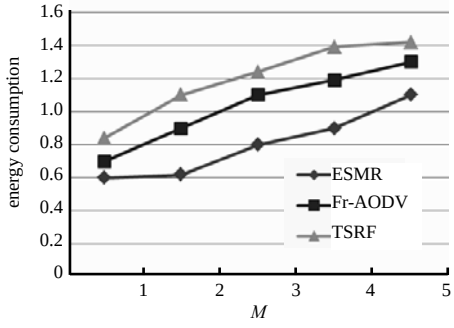

Fig.4 Energy consumption
图 4 能耗

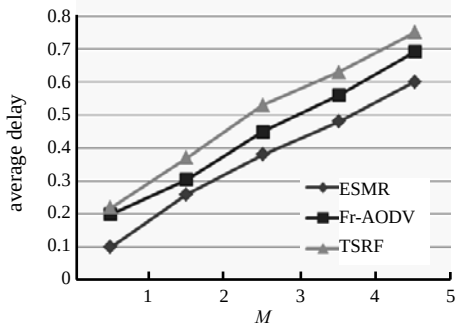

Fig.5 Average delay from node to node
图 5 平均端到端时延

3.2.4 平均端到端时延

路由协议的平均端到端时延随恶意节点的变化情况如图 5 所示。从图 5 可知，ESMR 的平均端到端时延得到有效控制，比 Fr-AODV 和 TSRF 平均降低了近 28%。原因在于 ESMR 依据最短路径原则选择最优转发节点，而 Fr-AODV 和 TSRF 选择的路径较长，消耗了更多转发节点的能量。路径越长，路由断裂的频率越高。

3.2.5 系统开销

ESMR,Fr-AODV 和 TSRF 的系统开销率随恶意节点数的变化情况如图 6 所示。系统开销率等于控制数据包数与基站接收的数据包数之比。从图 6 可知，ESMR 的系统开销高于 Fr-AODV，但低于 TSRF。说明 ESMR 在划分簇时，增加了一定的系统开销。在划分区时，节点需接收来自基站传输的身份和位置信息。

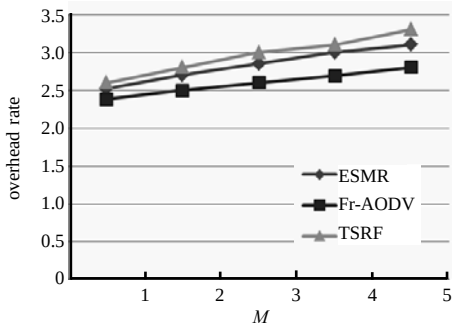

Fig.6 System overhead rate
图 6 系统开销率

4 结论

本文提出了 ESMR，旨在获取可靠、能效路由，防御恶意节点对数据包的恶意转发。ESMR 通过位置划分为 Zone，再将 Zone 划分不同的簇。同时，利用 XOR 操作加密。此外，ESMR 依据最短路径原则转发数据。仿真结果表明，ESMR 有效缩短了时延，并减少了能耗。

参考文献：

[1] NIAYESH G,BAKAR K A,HASHIM S M,et al. Collaborative mobile sink sojourn time optimization scheme for cluster-based Wireless Sensor Networks[J]. IEEE Sensors Journal, 2018,4(7):23-31.

[2] 江禹生,冯砚毫,管芳,等. 无线传感网非测距三维节点定位算法[J]. 西安电子科技大学学报(自然科学版), 2012, 39(5):140-147. (JIANG Yusheng,FENG Yanhao,GUAN Fang,et al. Range-free three-dimensional node location algorithm for the Wireless Sensor Network[J]. Journal of Xidian University(Natural Science), 2012,39(5):140-147.)

[3] KRISHNA M B,DOJA M N. Multi-objective meta-heuristic approach for energy-efficient secure data aggregation in Wireless Sensor Networks[J]. Wireless Person Communication:An International Journal, 2015,81(1):1-16.

[4] KUMAR K A,KRISHNA A V,CHATRAPATI K S. New secure routing protocol with elliptic curve cryptography for military heterogeneous wireless sensor networks[J]. Journal of Informational and Optimization Sciences, 2017,38(3):341-365.

[5] KRISHNAN A M,KUMAR P G. An effective clustering approach with data aggregation using multiple mobile sinks for heterogeneous WSN[J]. Wireless Personal Communication, 2016,90(2):423-434.

[6] ALAGIRISAMY M,CHOW C O. An energy based cluster head selection unequal clustering algorithm with dual sink(ECH-DUAL) for continuous monitoring applications in wireless sensor networks[J]. Cluster Computing, 2018,21(1):91-103.

[7] KUMARI S,KARUPPIAH M,DOS A K,et al. Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography[J]. Journal of Ambient Intelligence and Humanized Computing, 2018, 9(3):643-653.

[8] ADAMOVIC S,SARAC M,STAMENKOVIC D,et al. The importance of the using software tools for learning modern cryptography[J]. International Journal of Engineering Education, 2018,34(1):256-262.

[9] ZAHARIADIS T,TRAKADAS P,LELIGOU H C,et al. A novel trust-aware geographical routing scheme for wireless sensor networks[J]. Wireless Personal Communication, 2013,69(2):805-826.

[10] EISSA T,RAZAK S A,KHOKHAR R H,et al. Trust-based routing mechanism in MANET:design and implementation[J]. Mobile Networks and Application, 2016,18(5):666-677.

[11] DUAN J,YANG D,ZHU H,et al. TSRF:a trust-aware secure routing framework in wireless sensor networks[J]. International Journal of Distributional Sensor Network, 2014(3):1-14.

[12] 许力文,乔丽娟,陈杰. 基于 VANETs 修改的 K-means 分簇路由算法[J]. 计算机技术与发展, 2018,28(3):15-19. (XU Liwen,QIAO Lijuan,CHEN Jie. A K-means clustering routing algorithm based on modified VANETs[J]. Computer Technology and Development, 2018,28(3):15-19.)

[13] 曹斌,刘栓. IEEE 802.15.4 传感网络一种降低 RDC 路由协议[J]. 西南师范大学学报(自然科学版), 2016,41(11):170-176. (CAO Bin,LIU Shuan. On a routing protocol to reduce RDC in IEEE802.15.4 sensor networks[J]. Journal of Southwest China Normal University(Natural Science Edition), 2016,41(11):170-176.)