Research Article

A Novel Markov Model-Based Low-Power and Secure Multihop Routing Mechanism

Songxiang Yang ¹, Lin Ma ¹, Shuang Jia ¹ and Danyang Qin ²

¹School of Electronics and Information Engineering, Harbin Institute of Technology, Harbin 150080, China

²Department of Communication Engineering, Heilongjiang University, Harbin 150080, China

Correspondence should be addressed to Lin Ma; malin@hit.edu.cn

Received 28 February 2019; Revised 31 July 2019; Accepted 9 September 2019; Published 7 October 2019

Academic Editor: Ghufraan Ahmed

Copyright © 2019 Songxiang Yang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

For the severe impact of limited energy and network attacks caused by open transmission channels on data transmission, this paper presents a low-power and secure multihop routing mechanism based on the Markov state transition theory. The random selection of transmission paths enables the network to resist typical attacks such as interference and interception, thus ensuring the security of data transmission. Meanwhile, the proposed algorithm can reduce the overall energy consumption of the network and balance the load according to the residual energy of each path. Simulation results prove that the routing mechanism proposed in this paper can improve the energy efficiency and the security of the wireless ad hoc network.

1. Introduction

A wireless ad hoc network is a kind of noncentral network which is established by a large number of sensor nodes through self-organization. A wireless ad hoc network with self-organized, distributed, and dynamic characteristics can often be deployed in a harsh environment without relying on fixed facilities [1–3]. Compared with the traditional centralized network, the distributed wireless multihop network has the advantage of lower cost, better universality, and wider application field [4–7]. However, nodes in the wireless ad hoc network are powered by energy-limited batteries. The system cannot perform normal sensing and data transmission when the node's battery is exhausted. Therefore, how to improve the energy efficiency of nodes is a problem that the wireless ad hoc network must solve in practical applications. Security is also crucial for a wireless ad hoc network due to the openness of transmission channels. A routing mechanism should resist some common attacks taking into account energy efficiency, so a routing mechanism with high security and energy efficiency is the key to improving the performance of a wireless ad hoc network [8–14]. However, it is difficult to take both energy efficiency and security into account for existing computationally intensive routing algorithms. These

practical requirements pose new challenges to the security and efficiency of wireless ad hoc network routing algorithms.

To improve the security of routing in wireless ad hoc networks, researchers have proposed many relevant algorithms, such as the data encryption algorithm [15, 16], the trust-based security routing algorithm [17–20], and the game theory-based security transmission algorithm [21–23]. The large amount of computation makes it challenging to apply the traditional encryption algorithm directly to the energy-constrained wireless ad hoc networks. Specifically, the trust-based security algorithm is poor in universality, and all nodes in the system need to be trusted so that this kind of security algorithm cannot meet the actual demand of a wireless ad hoc network. The performance of the game theory-based security algorithm is significantly affected by the network environment. Reference [24] proposes a low-complexity sybil attack detection mechanism which can be implemented in both hierarchical and centralized wireless sensor networks. Extensive simulations prove that the proposed scheme is able to detect sybil attacks with higher probability and lesser computational cost and power consumption as compared to existing schemes. Reference [25] is based on the ant colony optimization algorithm to select the shortest path and balance the traffic load from the source node to the destination

FIGURE 1: Research framework.

node, so as to prolong the network lifetime. The security of information transmission is guaranteed by anonymous services, symmetric functions, and hash functions. However, the energy consumption of data forwarding is not specifically optimized. Reference [26] proposes an energy-aware routing protocol in WSNs, which makes efficient use of energy and increases reliability in data delivery. An adaptive power-control-based energy-efficient routing is proposed in [27], which increases the network lifetime and reduces communication interference and collision.

A number of researches show that reasonably selecting routing can not only improve the security of data transmission but also optimize the energy efficiency of a network. This kind of method is also known as the random routing algorithm. The random routing algorithm can search multiple neighbor nodes and select the next hop node of the transmission link according to specific probability distribution in order to guarantee the randomness and security of the routing selection. In this paper, the residual energy of nodes on the transmission link is introduced in the probability density distribution to balance the network load, which can improve the overall energy efficiency of wireless ad hoc networks. The information transmission path cannot be obtained by the intruder in the absence of the node residual energy and the state transition probability model, which can guarantee the security of the data transmission. A reasonable improvement of the energy efficiency can extend the network lifetime, thereby improving the overall performance of the network. Reference [28] adopts secret sharing and multipath routing to achieve secure information transmission. Firstly, all shared paths are determined. The traditional node-disjoint multipath constraint is relaxed to allow multiple paths within a particular elliptical region to have common nodes, thereby improving transmission security and energy efficiency. However, these methods only optimize performance for static WSN networks and do not adjust for the networks with mobile nodes. For the resource-limited multihop network, the energy efficiency needs to be taken into account while ensuring security. Therefore, the reasonable selection of a data transmission path is crucial to optimize network energy consumption, data transmission security, and network load.

The main contributions of this paper can be summarized as follows: this paper establishes a data-oriented Markov state transition model and designs a low-power and secure multihop routing mechanism. The protocol randomly selects a transmission path such that the network has the ability to resist typical attacks, so as to ensure the security of data transmission. Meanwhile, the protocol can reduce the overall energy consumption of the network and balance the load

according to the remaining energy of each path. We implemented the proposed LSRM in our lab and evaluated its performance. The experiment results show that LSRM can succeed to resist typical attacks and improve data transmission. Meanwhile, LSRM can distribute the network load to each path evenly and reduce the overall energy consumption. The overall research idea of this paper is shown in Figure 1.

2. Model Introduction

2.1. System Model. Considering the practical application of a wireless ad hoc network, the nodes in the network are limited in energy and communicate with other nodes through the wireless connection. This is because the energy consumption of a wireless transceiver is far higher than that of information collection and computing, and the energy consumption of relay nodes on transmission links is generally large due to their frequent relay forwarding. In contrast, the energy consumption of both source nodes and destination nodes is relatively small. To ensure the security of data, all nodes in the network have trust modules which are used to check the threshold of the routing measure and to adjust the threshold periodically or as required. The source node adopts the reactive routing protocol to establish multiple paths. The time lag between two successive routing discovery processes is known as a routing phase. The communication process is divided into several routing phases, and each routing phase is also divided into a few states, known as the t_i period. The routing mechanism updates the relevant data during t_i . The routing protocol selects one of the multiple paths created in each interval to send the packet based on this value function. Figure 2 shows a communication process.

For a random multipath routing scenario, the sequence diagram in Figure 2 shows the path selection of three consecutive routing phases and each state transition cycle, as well as the path switching between different time slots.

Assuming that there are N paths in a routing phase, the transmission energy consumption of the j th node on the i path during the period t_i is $e_{i,j}$. In different routing phases, the values of N and $e_{i,j}$ will change with time. The probability mass function of N is represented by $e^{\sim}(N)$, and the corresponding cumulative mass function is $E^{\sim}(N)$. The energy consumption vector of path l is represented by $e_k = \{e_{l,1}, e_{l,2}, \dots, e_{l,k}\}$. Therefore, the total transmission energy consumption on the path l is $E_l = \sum_{j=1}^l e_{l,j}$. The probability density function of E_l is $\hat{e}_l$, and the cumulative distribution function is $\hat{E}_l$.

FIGURE 2: The sequence diagrams of the routing protocol.

FIGURE 3: Attack model.

2.2. Attack Model. In wireless ad hoc networks, mobile nodes transmit data in wireless channels through multihop, which provides an opportunity for attackers to jam and intercept data. The attacker can intercept the data from any intermediate node easily. An attacker with a high-power transmitter can generate a strong signal to suppress the destination node and to disrupt the data transmission. An attacker can also block a data channel, thus causing data loss or damage. The routing protocol of a wireless ad hoc network faces a variety of attacks, including internal attacks and external attacks. Internal attacks are mainly launched by the damaged nodes to publish false information to the network. Such attacks are difficult to identify accurately due to the frequent changes of network topology. External attacks often interfere with relay nodes and intercept and steal data transmission to affect the normal operation of a network, as shown in Figure 3. In Figure 3, A~F denote the nodes in the network. Two external attacks, sniffing and tampering, are considered during the simulation in this paper.

The traditional routing protocol has no special security protection, so this kind of attack is prevalent. The introduction of an encryption algorithm can improve the difficulty of decoding data packets, thus playing a defensive role. However, the complex operation of such algorithms will lead to much energy consumption, so it is not effective in practical applications. The risk of these attacks can be reduced by obfuscating the data transmission path.

2.3. Establishment of Data Transmission Link. In wireless ad hoc networks, the routing mechanism establishes numerous paths to transmit the packets. Meanwhile, all potential paths are discovered in the routing discovery phase. All the paths between the source node and the destination node are constructed by using the on-demand routing protocol in the

FIGURE 4: The model of the data transmission link.

routing discovery phase due to the large amount of system overhead generated by the active routing protocol. These paths are selected for data transmission between nodes randomly.

Each packet contains a minimum energy measure ($\min_em$) during communication. The $\min_em$ of a path is the $\min_em$ of all nodes on a path. The source node transmits a routing request message whose $\min_em$ is 0 to establish the transmission path between nodes. An intermediate node will compare its $\min_em$ to the energy measure threshold of a routing request message when the routing request message is received. And the node will compare its $\min_em$ with that of the routing request message if the $\min_em$ is no less than the threshold. Otherwise, the routing request message will be terminated. If the $\min_em$ of the node is smaller than that of the message, the latter one will be replaced by the former, and the total hops will plus 1. The routing request message is transmitted and the intermediate node will forward it directly if the $\min_em$ node is larger than that of the routing request message. Eventually, the paths with different hops will be discovered, as shown in Figure 4.

The different transmission paths will be established between S and D when D receives multiple routing request packets. The destination node can select the path by setting the threshold of hops in the actual operation of a network. Then, the $\min_em$ of the routing request packet selected by the destination node is attached to the routing response packet and passed back to the source node via the original path. Subsequently, the source node selects the routing with the highest initial probability distribution to transmit the packets.

2.4. Markov State Transfer Model

2.4.1. Background. The Markov state transfer model can be used as a mathematical model for transitions between series states, and it is a common random method to predict system performance. The Markov state transfer model is based on a

FIGURE 5: Markov state transition model.

probability distribution, which can predict the transitions between various states. Since the number of states is limited and the transitions between different states are based on a certain probability distribution, it can adapt to the time variability of node communication. Besides, the transition probability between different states is independent of the previous phase. The set of all states in the Markov state transfer model is called the state space, i.e., $L = \{L_1, L_2, \dots, L_l\}$. O represents the mapping between different states. The routing protocol can execute any O allowed in the state to switch the path from L_i to L_j , and the transition probability of this process is p_{ij} . The system will send response $r(L_i, L_j, O)$ after the state transition is completed. The transition probability is p_{jj} if the two states are consistent.

2.4.2. Probability Analysis. L_i represents the transmission path. $\mathbf{P}$ is the transition probability matrix. $p_{ij} \in \mathbf{P}$ is the transition probability from L_i to L_j , as shown in Figure 5.

A_i is the initial probability distribution. The transfer probability matrix $\mathbf{P}$ of the Markov state transition model can be constructed by setting p_{ij} . As defined above, the energy measure of path L_i is represented by $\min_em$. A path with a maximum $\min_em$ is selected as the initial path, so the initial probability distribution A_i of path L_i can be determined:

$$A_i = \frac{\min_em_i}{\sum_{k=1}^l \min_em_k}. \quad (1)$$

The energy of nodes on the path will be consumed, and the energy measure of the path will decrease gradually during the process of data transmission. em is adopted to represent all vectors of a path energy measure:

$$em = [\min_em_1, \min_em_2, \dots, \min_em_l]. \quad (2)$$

The calculation of p_{ij} under different conditions is shown in (3), where $\sum_l p_{ij} = 1$. And $\alpha (\alpha \geq 2)$ is the performance parameter and mainly used to reduce the path

transfer probability. The main reason for setting this parameter is that the probability of moving from a path with a higher energy measure to one with a lower energy measure is relatively low.

$$p_{ij} = \begin{cases} \frac{|\min_em_i - \min_em_j|}{\sum_l |\min_em_i - \min_em_l|^\alpha}, & L_i \neq L_j, \min_em_i > \min_em_j, \\ \frac{|\min_em_i - \min_em_j|}{\sum_l |\min_em_i - \min_em_l|^\alpha}, & L_i \neq L_j, \min_em_i < \min_em_j, \\ 1 - \sum_{k \in l} p_{ik}, & L_i = L_j, L_i \neq L_k. \end{cases} \quad (3)$$

Since A_i can guarantee energy efficiency, the system can ensure the security and efficiency of a transmission at the same time when switching path randomly according to A_i . The transmission path of the next phase can be determined by A'_i when the first state transition is completed, where $A'_i = A_i \times p_{ij}$.

3. Markov Model-Based Low-Power and Secure Multihop Routing Mechanism

The secure multihop routing under an energy constraint is very important for ensuring the security of a data transmission. Considering that each routing phase in the ad hoc network contains a large number of potential transmission paths, it is difficult to guarantee the convergence of the routing discovery model with a large amount of computation. To solve this problem, an online numerical iterative method is proposed to calculate the value function, and a convergence environment is established to reduce the computational complexity and obtain the optimal solution.

3.1. Markov-Based Routing Model. The characteristics of the Markov state transition model are determined by four objects, namely the state set, behavior set, transition probability, and the feedback function of each phase. The state set is $\{L_1, L_2, \dots, L_l\} \in L$, where L_i denotes the selected transmission path in each routing phase. O represents the behavior set of the Markov model. $\{O(L_1), O(L_2), \dots, O(L_l)\} \in O$, and $O(L_i)$ is defined in Definition 1. $P[L_j | L_i, O(L_i)]$ denotes the transition probability matrix of the Markov model, and its definition is shown in (3). $E(L_i, O(L_i)) = \sum_{k=1}^i e(k, O(k))$ represents feedback function, and $e(k, O(k))$ denotes the feedback information of node k under $O(k)$, which is determined by the energy model.

Definition 1. O is the mapping of packets switching from one path to another. Selecting the appropriate O can minimize $E(L_i, O(L_i))$, which means the energy consumption of a packet transmission can be reduced to the minimum.

$E(L_i(t), O(L_i(t)))$ is the total transmission energy consumption in time slot t :

$$\begin{aligned} C_{t_r} &= \sum_{t=1}^T E(L_i(t), O(L_i(t))), \\ C_t &= \sum_{r=1}^{t_r} C_{t_r}, \end{aligned} \quad (4)$$

where C_{t_r} denotes the system overhead in routing phase t_r , and C_t represents the total system overhead of the entire communication process. Under $O(L_i(t))$, the theoretical minimum system overhead of $L_i(t)$ is

$$C_{\min} = \min C \left\{ \lim_{T \rightarrow \infty} \sum_{t=1}^T \beta^t E(L_i(t), O(L_i(t))) \right\}, \quad (5)$$

where $\beta \in [0, 1)$ denotes a calculation factor, and the specific value is determined by the random state transfer process. The value of β can balance the result quality and the convergence speed. The smaller the value of β is, the faster the converge speed, and the worse the result quality is. Non-negative terminal energy consumption $F(L_i)$ is generated during network operation. L_i is defined as the initial state, and the minimum system overhead that can be achieved under $O(L_i)$ is $v^t(L_i)$. $v^t(L_i)$ can be calculated by using the initial state, namely, $v^0(L_i) = F(L_i)$. The random routing process $\{L_i(t)\}$ can be treated as a finite state Markov process because the transmission paths of packets change dynamically. State selection depends only on the initial probability distribution if $t = 1$. Equation (3) shows the transition process of different states under the given initial probability distribution when $t > 1$. The system cost function $v(L_i)$ is shown as follows:

$$v(L_i) = \min_{O(L_i)} \left\{ E(L_i(t), O(L_i(t))) + \beta \sum_{L_j} P[L_j | L_i, O(L_i)] v(L_j) \right\}, \quad (6)$$

where $v^*(L_i)$ represents the minimum system overhead, and $O^*(L_i)$ denotes the optimal strategy. In addition, the result of (6) is unique since the Markov model is not repeatable under all stable strategies. The amount of calculation is enormous because there are many available paths in each routing phase. To solve this problem, an iterative algorithm is adopted to reduce the computation complexity.

3.2. An Iterative Algorithm Based on Stochastic Dynamic Approximation. The functions are iterated by the Bellman optimization principle in this paper, and the optimal solution is obtained. Let R represent the set of all v . The vector graph

$V: R^{L_i} \rightarrow R^{L_j}$ is defined to calculate any v .

$$V_{L_i}(v) = \min_{O(L_i)} \left\{ E(L_i(t), O(L_i(t))) + \beta \sum_{L_j} P[L_j | L_i, O(L_i)] v(L_j) \right\}. \quad (7)$$

For any v and v' , $\|V(v) - V(v')\|_{\infty} \leq \beta \|v - v'\|_{\infty}$ is always workable. This paper defines an iteration cycle as the minimum time interval for all paths to be accessed at least once. A routing phase is divided into several iterative cycles for operation. $\ell(i)$ represents the time for path L_i to be accessed, and v_{ℓ} represents the system overhead in ℓ iteration cycle. The iterative algorithm starts from v_0 , and the two adjacent iterative cycles satisfy

$$v_{\ell+1} = V(v_{\ell}). \quad (8)$$

The iterative process will eventually converge to v^* , and v^* is the optimal solution at this time. At the end of cycle ℓ , the function of cycle $\ell + 1$ will be updated as follows:

$$\begin{aligned} v_{\ell+1}(L_i) &= v_{\ell}(L_i) + \lambda_{\ell} \min_{O(L_i)} \{E_{\ell+1}(L_i(t), O(L_i(t)))\} \\ &\quad + \lambda_{\ell} \min_{O(L_i)} \left\{ \beta \sum_{L_j} P[L_j | L_i, O(L_i)] v_{\ell}(L_j) - v_{\ell}(L_i) \right\}, \end{aligned} \quad (9)$$

where $\lambda_{\ell} \in [0, 1)$ denotes the calculation metric in cycle ℓ . Subsequently, O is updated as shown in

$$O_{\ell+1} = \arg \min V(v_{\ell+1}). \quad (10)$$

The iterative process can be summarized as Algorithm 1.

3.3. Algorithm Convergence Analysis. β_{ℓ} represents the calculated factor sequence, which meets the following conditions:

$$\begin{aligned} \sum_{\ell} \beta_{\ell} &= \infty, \quad \beta_{\ell} \geq 0, \\ \sum_{\ell} \beta_{\ell}^2 &< \infty, \end{aligned} \quad (11)$$

where C_{ℓ} represents the mathematical expectation of the system overhead, and P_{ℓ} represents the conditional probability.

$$\begin{aligned} Y_{\ell}(O(L_i)) &= E_{\ell}(L_i(t), O(L_i(t))) \\ &\quad + \beta \sum_{L_j} P[L_j | L_i, O(L_i)] v_{\ell}(L_j) - v_{\ell}(L_i), \\ \rho M_{\ell}(O(L_i)) &\triangleq Y_{\ell}(O(L_i)) - C_{\ell}[Y_{\ell}(u(L_i))], \\ A_{\ell-1} &\triangleq P_{O_{\ell}} \lambda_{\ell-1} + (1 - \lambda_{\ell-1}) \mathbf{I}, \\ B_{\ell-1} &\triangleq P_{O_{\ell-1}} \lambda_{\ell-1} + (1 - \lambda_{\ell-1}) \mathbf{I}, \end{aligned} \quad (12)$$

where $P_{O_{\ell}}$ and $\mathbf{I}$ denote the $\mathbf{I} \times \mathbf{I}$ transmission probability matrix under O_{ℓ} . $\rho M_{\ell}(O(L_i))$ represents the boundary of


```

(1) Begin
(2) Initialization
(3)  $t = 0, \ell = 0$ 
(4)  $v_0 \leftarrow EC_{terminal}, O_0 \leftarrow V(v_0)$ 
/*  $EC_{terminal}$  is the terminal energy consumption */
(5) Begin  $L_0$ 
(6) activate algorithm
(7) for  $i := 1$ 
(8)    $v_{\ell+1}(L_i) = v_\ell(L_i) + \lambda_\ell \min_{O(L_i)} \{E_{\ell+1}(L_i(t), O(L_i(t)))\} + \lambda_\ell \min_{O(L_i)} \{\beta \sum_{L_j} P[L_j | L_i, O(L_i)] v_\ell(L_j) - v_\ell(L_i)\}$ 
(9)    $\arg \min V(v_{\ell+1}) = O_{\ell+1}$ 
(10)   if  $\|v_{\ell+1} - v_\ell\| < \delta_v$  then
(11)     stop
(12)   else
(13)     back to (8)
(14)   end if
(15) End

```

ALGORITHM 1: Iteration algorithm.

any ℓ and the calculation factor sequence that satisfies (11). For any set $O_0, O_1, \dots, O_m$, $\rho_m = \beta(\lambda_m) > 0$ is always workable. There is a positive integer m which makes

$$\begin{aligned} [A_m, A_{m-1}, \dots, A_1]_{L,I} &\geq \rho_m, \\ [B_m, B_{m-1}, \dots, B_1]_{L,I} &\geq \rho_m, \end{aligned} \quad (13)$$

where $1 \leq L_i \leq L$, and $[\cdot]_{L,I}$ represents the $(L_i I)$ element in the matrix. $e = [1, 1, \dots]^T$ is a I -dimensional vector and $\lim_{\ell} v_\ell = v_\infty$ is always workable. Steady-state value satisfies

$$(T_I(v_\infty) - v_\infty(u^I(L_i)))e + v_\infty = T(v_\infty). \quad (14)$$

The optimal result is $v^*(L_i) = T_I(v_\infty) - v_\infty(u^I(L_i))$, and the optimal strategy is $O^* = \arg \min T(v_\infty)$. It can be concluded from (13) that state $u(L_i)$ can be obtained from any $u(L_i)$ state through some transition steps, and the transformation results are feasible in most certain cases.

4. Simulation Results and Performance Evaluation

This section analyzes the performance of the proposed low-power secure routing mechanism in terms of security and energy efficiency.

4.1. Simulation Environment. NS-2 is adopted to verify the performance of the proposed low-power secure routing mechanism. The nodes in the network will be randomly deployed in a square area of $1000 \times 1000 \text{ m}^2$ according to the principle of two-dimensional uniform distribution. The MAC layer protocol is IEEE 802.11b, and the transfer agent is UDP. In the simulation process, the source node transmits data at a fixed bit rate, and the packet size is 512 bytes. Compared with AODV, AOMDV, and PAAODV, the performance of the proposed routing protocol (Low-power and Secure Routing Mechanism (LSRM)) is evaluated in terms

TABLE 1: Parameters and their values.

Parameter	Value
α	2
Packet number	300
Node number	100
Energy threshold	400 J
Routing phase number	20
State transition period	20 ms
Node communication distance	300 m

of security and energy efficiency. The remaining simulation parameters are shown in Table 1.

4.2. Security Simulation. The average packet delivery rate of four routing protocols under a sniffing and tampering attack is shown in Figures 6 and 7.

It can be seen that the average packet delivery rate of LSRM under two attack conditions is higher than that of other algorithms in Figures 6 and 7. The main reason is that LSRM can randomly switch between multiple paths according to the energy measure, which ensures the security of data transmission. The node energy on each link will be consumed continuously with the network operation, and the paths for data transmission will be reduced. Therefore, the packet delivery rate shows a downward trend, which also conforms to the fundamental rules of actual network operations.

4.3. Transmission Stability Simulation. The packet error rate comparison of four routing protocols under different data packet transmission rates is shown in Figure 8.

The packet error rate of LSRM increases gradually, while the other three routing algorithms increase sharply with the increase of the packet transmission rate. LSRM can switch the path over time to reduce the probability of the data packet being attacked, which can guarantee the security of data transmission.

FIGURE 6: The average packet delivery rate under a sniffing attack.

FIGURE 7: The average packet delivery rate under a tampering attack.

FIGURE 8: Packet error rate with different packet sending rates.

FIGURE 9: Data throughput with different node moving speeds.

FIGURE 10: Average network delay with different node moving speeds.

The information throughput rate of different node moving speeds is compared as shown in Figure 9 when the node density is 20. LSRM performs better than the other three routing algorithms in terms of information throughput rate. The main reason is that LSRM can transmit numerous packets through different paths. On the contrary, the source node may only send a few packets in the other three routing algorithms due to the insufficient stability of transmission links. The information throughput rate of four routing protocols will decrease as the nodes move continuously, which is in line with the fundamental rules of actual network operations.

Figure 10 shows the average network delay of four routing protocols at different moving speeds. The average delay of LSRM is significantly lower than that of the other three routing protocols. LSRM establishes a more stable transmission path to reduce the number of routing phases, which can optimize the average network delay. The number of routing phases is enhanced with the augmentation of node moving speed, which leads to the increase of network delay.

4.4. Energy Efficiency Simulation. The system energy consumption in different routing phases is shown in Figure 11. LSRM has a slightly higher system energy consumption in the first six routing phases compared with the other three routing algorithms. The main reason is that LSRM sends a large number of packets during the initial routing phases. However, the total system energy consumption is still lower than the other three routing protocols.

Figure 12 shows the load comparison of four routing protocols in different dynamic network environments. LSRM has a slightly higher routing overhead than the other three routing protocols. LSRM selects the path for data transmission randomly. Therefore, LSRM has more transmission control packages, thus resulting in higher routing overhead.

Figure 13 shows the relationship between the average energy consumption of each packet and the total number of packet transmissions. The average forwarding energy consumption of each packet increases as the amount of packet transmission increases. This is because the buffer time and channel bandwidth required for the packets will also increase

FIGURE 11: System energy consumption of each routing phase.

FIGURE 12: The routing overhead with different node moving speeds.

FIGURE 13: The energy consumption of per packet.

FIGURE 14: Number of alive nodes versus time.

when the packets transmitted per second increase. In addition, the average energy consumption is proportional to the node density. The average energy consumption of a single packet in LSRM is lower than that of the other three routing protocols since the transmission path can be selected according to the energy measure randomly.

Figure 14 shows the number of alive nodes versus simulation time with 100 nodes. Compared with AODV and PAAODV, LSRM takes into account the residual energy of each node in the network, rather than just look for the shortest path for information transmission. Therefore, the performance of the proposed algorithm in this paper is better in terms of network load balancing. Moreover, the average energy consumption of a single packet in LSRM is lower than that of the other three routing protocols, so the network lifetime is longer.

5. Conclusion

The wireless ad hoc network is an important component of modern mobile communication systems. However, network performance is affected seriously due to the breakage of the data link and frequent changes of the network topology. Therefore, a low-power and secure multihop routing mechanism is proposed in this paper. The energy measure of the data transmission link is taken as an important parameter for the mathematical model. The mathematical model is constructed, and the optimal solution is obtained by using the iterative algorithm. The simulation results show that the routing protocol proposed in this paper can distribute the network load to each path evenly and improve the data transmission. In addition, the routing protocol can effectively resist packet interception, routing hijacking, and interference attacks. Future research will propose a novel solution to resist the attack from internal malicious nodes, which can guarantee the security and effectiveness of data transmission in the network. Meanwhile, the iterative algorithm will be optimized to reduce the computational overhead in the network.

Data Availability

The data results used to support the findings of this study are presented in this paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (61971162, 61771186, 4181101180, and 61571162) and the University Nursing Program for Young Scholars with Creative Talents in Heilongjiang Province (UNPYSCT-2017125).

References

- [1] C. Lal, V. Laxmi, M. S. Gaur, and S. B. Ko, "Bandwidth-aware routing and admission control for efficient video streaming over MANETs," *Wireless Networks*, vol. 21, no. 1, pp. 95–114, 2015.
- [2] K. Abrougui, A. Boukerche, R. W. Pazzi, and M. Almulla, "A scalable bandwidth-efficient hybrid adaptive service discovery protocol for vehicular networks with infrastructure support," *IEEE Transactions on Mobile Computing*, vol. 13, no. 7, pp. 1424–1442, 2014.
- [3] W. Li and H. Song, "ART: an attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2016.
- [4] J. Yao, S. Feng, X. Zhou, and Y. Liu, "Secure routing in multi-hop wireless ad-hoc networks with decode-and-forward relaying," *IEEE Transactions on Communications*, vol. 64, no. 2, pp. 753–764, 2016.
- [5] A. M. Moucha, V. Cerny, J. Kubr, and J. Janecek, "Distributed phase-shift beamforming power balancing in ad-hoc and sensor networks," *Telecommunication Systems*, vol. 57, no. 4, pp. 367–377, 2014.

- [6] M. Rajesh and J. M. Gnanasekar, "Path observation based physical routing protocol for wireless ad hoc networks," *Wireless Personal Communications*, vol. 97, no. 1, pp. 1267–1289, 2017.
- [7] Q. Wu, X. Zhou, and F. Ge, "A cross-layer protocol for exploiting cooperative diversity in multi-hop wireless ad hoc networks," *Wireless Networks*, vol. 23, no. 5, pp. 1591–1610, 2017.
- [8] F. Sattar, F. Karray, M. Kamel, L. Nassar, and K. Golestan, "Recent advances on context-awareness and data/information fusion in ITS," *International Journal of Intelligent Transportation Systems Research*, vol. 14, no. 1, pp. 1–19, 2016.
- [9] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "On the evaluation of reputation and trust-based schemes in mobile ad hoc networks," *Security and Communication Networks*, vol. 8, no. 18, 4052 pages, 2015.
- [10] S. Fouchal, D. Mansouri, L. Mokdad, and M. Iouallalen, "Recursive-clustering-based approach for denial of service (DoS) attacks in wireless sensors networks," *International Journal of Communication Systems*, vol. 28, no. 2, pp. 309–324, 2015.
- [11] K. P. R. Prabha and N. Jeyanthi, "A trust and fuzzy cluster based dynamic secure routing algorithm for mobile ad hoc networks," *Wireless Personal Communications*, vol. 98, no. 3, pp. 2959–2974, 2018.
- [12] A. Joshi, P. Srivastava, and P. Singh, "Security threats in mobile ad hoc network," *International Journal of Research in Science and Technology*, vol. 3, no. 4, pp. 53–64, 2013.
- [13] N. Hassan, N. M. Khan, G. Ahmed, and R. Ramer, "Real-time gradient cost establishment (RT-GRACE) for an energy-aware routing in wireless sensor networks," in *2013 IEEE Eighth International Conference on Intelligent Sensors, Sensor Networks and Information Processing*, pp. 1–7, Melbourne, VIC, Australia, 2013.
- [14] W. Zhang, G. Han, Y. Feng, J. Lloret, and L. Shu, "A survivability clustering algorithm for ad hoc network based on a small-world model," *Wireless Personal Communications*, vol. 84, no. 3, pp. 1835–1854, 2015.
- [15] A. Mathur, "A research paper: an ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms," *International Journal on Computer Science and Engineering*, vol. 4, no. 9, pp. 1650–1657, 2012.
- [16] H. C. Liao and Y. H. Chao, "A new data encryption algorithm based on the location of mobile users," *Information Technology Journal*, vol. 7, no. 1, pp. 63–69, 2008.
- [17] P. Kautoo, P. K. Shukla, and S. Silakari, "Trust formulization in dynamic source routing protocol using SVM," *International Journal of Information Technology and Computer Science*, vol. 6, no. 8, pp. 43–50, 2014.
- [18] S. A. Thorat and P. J. Kulkarni, "Opportunistic routing in presence of selfish nodes for MANET," *Wireless Personal Communications*, vol. 82, no. 2, pp. 689–708, 2015.
- [19] R. Feng, S. Che, X. Wang, and N. Yu, "A credible routing based on a novel trust mechanism in ad hoc networks," *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, Article ID 652051, 2013.
- [20] W. Bo, H. Chuanhe, L. Layuan, and Y. Wenzhong, "Trust-based minimum cost opportunistic routing for ad hoc networks," *Journal of Systems and Software*, vol. 84, no. 12, pp. 2107–2122, 2011.
- [21] Y. Liu, H. H. Chen, and L. Wang, "Physical layer security for next generation wireless networks: theories, technologies, and challenges," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 347–376, 2017.
- [22] X. Fang, N. Zhang, S. Zhang, D. Chen, X. Sha, and X. Shen, "On physical layer security: weighted fractional Fourier transform based user cooperation," *IEEE Transactions on Wireless Communications*, vol. 16, no. 8, pp. 5498–5510, 2017.
- [23] M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J. P. Hubaux, "Game theory meets network security and privacy," *ACM Computing Surveys*, vol. 45, no. 3, pp. 1–39, 2013.
- [24] M. Saud Khan and N. M. Khan, "Low complexity signed response based sybil attack detection mechanism in wireless sensor networks," *Journal of Sensors*, vol. 2016, Article ID 9783072, 9 pages, 2016.
- [25] I. Jean de Dieu, N. Assouma, M. Muhamad, W. Jin, and S. Lee, "Energy-efficient secure path algorithm for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 8, no. 4, Article ID 751784, 2012.
- [26] N. M. Khan, Z. Khalid, and G. Ahmed, "GRADient Cost Establishment (GRACE) for an energy-aware routing in wireless sensor networks," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, Article ID 275694, 2009.
- [27] G. Ahmed and N. M. Khan, "Adaptive power-control based energy-efficient routing in wireless sensor networks," *Wireless Personal Communications*, vol. 94, no. 3, pp. 1297–1329, 2017.
- [28] S. Su and H. Yu, "Secure and efficient data collection in wireless image sensor network based on ellipse batch dispersive routing," *Security and Communication Networks*, vol. 8, no. 14, 2430 pages, 2015.