RESEARCH   Open Access

Hidden node aware routing method using high-sensitive sensing device for multi-hop wireless mesh network

Shamsad Parvin[*] and Takeo Fujii

Abstract

Throughput maximization is one of the main challenges in multi-hop wireless mesh network (WMN). Throughput of the multi-hop WMN network seriously degrades due to the presence of the hidden node. In order to avoid this problem, we use a combination of the high-sensitive sensing function and beacon signalling at the routing. The purpose of this sensing function is used to avoid the hidden node during route formation in the self flow. This function is considered to construct a route from the source node to the destination node without any hidden node. In the proposed method, high-sensitive sensing device is utilized in both route selection and in the media access. The accuracy of our proposed method is verified by numerical analysis and by computer simulations. Simulation results show that our proposed method improves the network performance compared with the conventional systems which do not take account of the hidden node.

1 Introduction

Wireless Mesh Networks (WMN) are emerging as a new attractive communication paradigm owing to their low cost, easy maintenance and rapid deployment. The application scenarios for WMN include wireless broadband internet access, intelligent transportation systems, transient networks in convention centers, and disaster recovery. In WMNs, nodes are comprised mesh routers and mesh clients [1]. Wireless mesh routers are interconnected as a multi-hop backbone to provide mesh clients, network access. As shown in Figure 1, among all mesh routers, some have client connectivity (mesh access points), and some have internet gateway capability. The mesh backbone then supports multi-hop communication among mesh routers. WMNs are dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves and compatible with conventional WLAN. Many research challenges still remain open in the design of the WMNs [1,2]. Routing in multi-hop WMNs has been a hot research area in recent years, with the objectives to

achieve as high throughput as possible over the network [3,4]. Typically, the source and the destination nodes for a particular data packet are not within direct communication range. This leads to a multi-hop scenario where the packet must be routed and forwarded through other nodes in the network on the way to the destination nodes. Many routing protocols have been studied for sending data from the source node to the destination node [5,6]. These protocols ignore the Effect of the hidden node problem. The hidden node is related to the Transmission range, Carrier sense range and Interference range of a station [7,8]. The hidden nodes refer to the nodes within the interference range of the intended destination and out of the carrier sense range of the source node [8]. Then packet collision occurs at the intended destination node due to the hidden node. Moreover, compared with the infrastructure Basic Service Set (BSS) WLAN networks, the wider coverage area in WLAN mesh networks causes more frequent packet collision thus limits the network capacity. IEEE 802.11 standard adopts a CSMA/CA protocol as the main body of Distributed Coordination Function (DCF) in the MAC layer [9]. However, the performance of CSMA/CA networks is severely affected by hidden node problem. Although the IEEE 802.11 standards employ the Request to Send/Clear to Send (RTS/CTS) mechanism to solve

* Correspondence: sumi@awcc.uec.ac.jp
Advanced Wireless Communication Research Center (AWCC), The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan
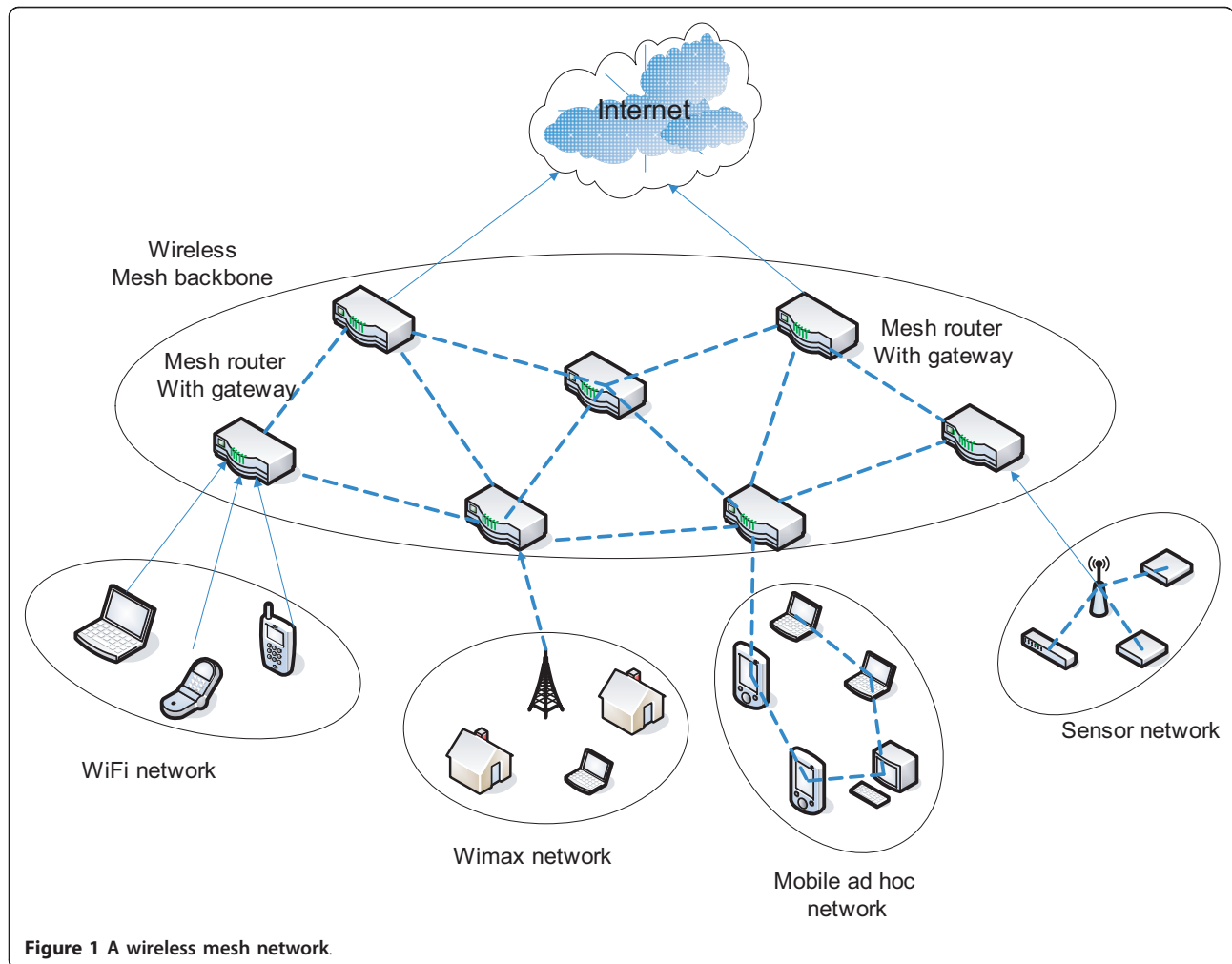
Figure 1 A wireless mesh network.

the hidden node problem, it increases overhead for communication and is not used for short-sized packet [10].

A fundamental problem of the multi-hop WMN is the degradation of performance with the increasing the number of hops [11]. The limitation is mainly because of the self flow and multi-flow interference caused by the hidden node in the multi-hop network. In this paper we classify the interference due to the hidden node into two types: self flow interference and multi-flow interference. Self flow interference is caused by the hidden nodes in the same flow. On the other hand, multi-flow interference is caused by the other flow of the neighbor node. In these interference, self flow interference is a serious problem because their own transmitted packets are collide each other in the flow. The self flow interference and multi-flow interference caused by the hidden node are shown in the Figure 2. Some works have been done to improve the network throughput and to decrease the number of packet collision by optimizing

the carrier sense range [12-19]. Vaidya [15] shows that the MAC overhead, bandwidth dependent and bandwidth independent have a significant effect on the choice of carrier sensing range. Zhai [16] identify the optimum carrier sensing range for different data rates. However, they did not consider the next hop selection of the routing protocol.

Therefore, in this paper we focus on the hidden node avoidance technique for the self flow interference. The aim of this paper is to select a route between the source node and the destination node that is protected from the hidden node of the self flow. This is accomplished using a high-sensitive sensing function in the route construction. In the proposed routing method, it is considered that every node utilizes high-sensitive sensing devices like the secondary terminal in the cognitive radio [20-22]. Every node senses the medium for selecting the route as well as for the medium access control. In the proposed routing method, we uses beacon signal to select the next hop node. The beacon signal is used
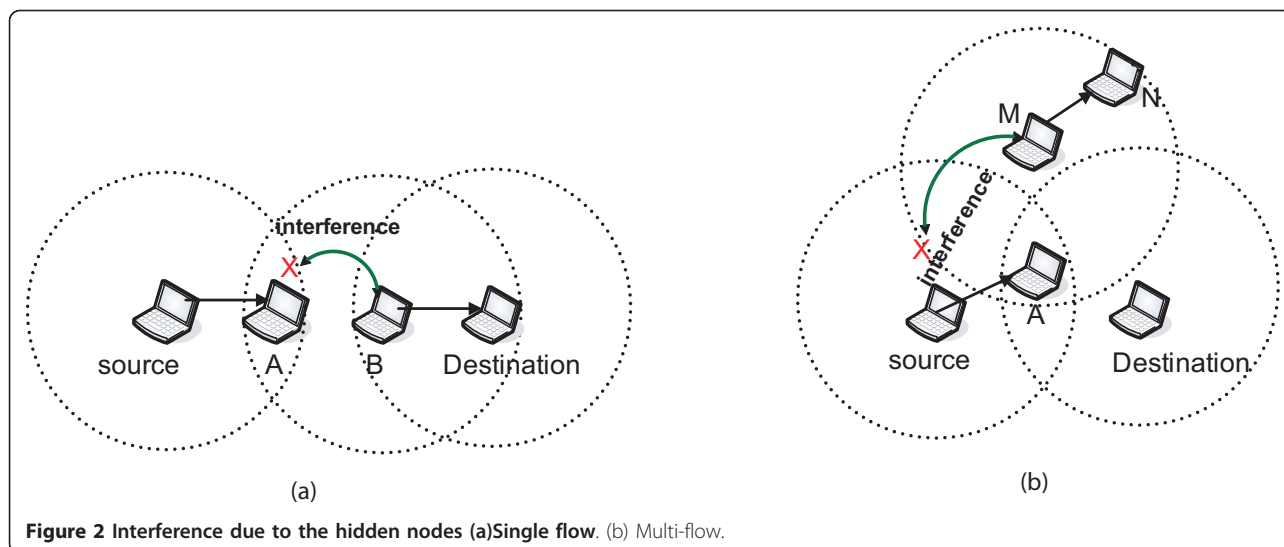
Figure 2 Interference due to the hidden nodes (a)Single flow. (b) Multi-flow.

for selecting the next hop node. First a node broadcast a Route Request (RREQ) packet. In the next frame, the same node transmits the beacon signal to inform all neighbor nodes about its presence. All the nodes that receive the beacon signal from that node relay the RREQ packets. The node will be selected as the next node of the route. Such operation is repeated from the source node until the RREQ packet arrives at the destination node. The destination node then sends the Route Reply (RREP) packet toward the source node. Since all nodes in the route can detect the beacon signal of its previous hop node, the route can be selected as to remove the self flow interference due to the hidden nodes.

Different types of routing metrics are proposed in the multi-hop WMN to find the best possible paths between the source and the destination node [6,23-25]. In [23], the Expected Transmission Count (ETX) was proposed to minimize the expected total number of transmissions required to successfully deliver a packet over a wireless link. The Expected transmission time (ETT) [24] metric is an extension of ETX which considers Different link routes or capacities. ETT is the expected time to successfully transmit a packet at the MAC layer. The Airtime routing metrics specified in IEEE 802.11s [25] is based on the ETT with additional consideration given to channel access and the protocol overhead to reflect the amount of channel resources consumed by transmitting the data packets over a wireless link. Hop count is the traditional routing metric used in most of the common routing protocols like DSR [5] and AODV [6] designed for multi-hop wireless networks. It finds paths with the shortest number of hops. These metrics unfortunately fail to address directly the impact of the hidden node problem in WMN. This means the path selected by

these metrics unable to remove the self flow interference in a flow due to the hidden node problem and causes frequent data collisions. Therefore, in this paper, we propose a routing method that selects a path without any hidden node. For this purpose we chose a node as a next node of the route that is not a hidden node using beacon signaling. The aim of the proposed routing method is to construct a route without any hidden node. The proposed routing method can mitigate the hidden node, no matter which routing metrics is used for the route selection. As the conventional routing protocol, AODV uses hop count metric to choose the shortest hop length path we also use hop count metric for path selection. However, the proposed routing scheme also works well if it use other routing metrics such as ETX and ETT for path selection. This is because most of the routing metrics does not concern about the hidden node collisions due to the self flow interference.

In the proposed routing method, spectrum sensing is considered to detect the beacon signal of the previous hop node. Several spectrum sensing methods have been studied [26,27]. Energy detection is one of the very popular methods because of its simplicity and adequate performance [26]. The sensing function of our proposed method is based on this energy detection method. This method detects unknown signals embedded in the noise by comparing the observed received signal power level with a threshold. After constructing the route, data transmission will be performed using the IEEE 802.11 DCF as the MAC protocol. The only change of the IEEE 802.11 DCF on the data transmitting period is just to change the carrier sensing level to the appropriate lower sensing level. With low sensing level, a node can detect the existence of a hidden node. On the other hand, with

high sensing level, the node often miss the detection of the hidden node. Since the conventional wireless LAN uses CSMA/CA MAC protocol with high sensing level, the hidden node problem cannot be removed. The proposed method combines the beacon signal and the high-sensitive sensing function at routing to remove the self flow hidden node problem. During the route construction, beacon signaling is used to inform the nodes (that are not hidden node) the presence of previous hop node. In this way, our proposed route avoids the self flow hidden node collision in the multi-hop WMN. Hidden node collision between the multi flows is also minimized with appropriate low sensing level. Therefore, the hidden node problem is removed because all the nodes utilize a cognitive radio sensing technique for detecting the beacon signal of the hidden node. In the proposed routing method, a hidden node does not start its transmission as it senses the medium as busy. Thus the hidden node problem is removed during the routing method. So that it can avoid redundant packet collision or redundant transmission termination among self flow nodes.

The rest of the paper is organized as follows. In Section 2 we present a brief overview of the background. The proposed method is described in Section 3 and the network model and the analysis of the proposed method is explained in Section 4. The performance evaluation through simulation is present in the Section 5. Finally, we conclude the paper in Section 6.

2 Background

In cognitive radio, a spectrum sensing system is considered for detecting the signal of the primary system at the secondary system to improve the spectrum sharing efficiency [22]. The sensing function for cognitive radio can be defined as a technique where the secondary transmitter senses the surrounding wireless channel and checks the other active primary transmitter around it before transmission. If the signal of the primary transmitter is detected, the secondary transmitter prevents the transmission. The proposed routing method is based on such kind of sensing function. In general, the sensing device of the primary system is a conventional carrier sensing device used in the wireless LAN. The sensitivity of the sensing used in such legacy wireless LAN is low and the sensing level is relatively high compared with that considered in the secondary system of the cognitive radio. In the proposed routing method, we assume that all the relay node is equipped with a high-sensitive sensing device alike the secondary terminal. The sensing range is an area in which a node can detect the signal of the other node. A high-sensitive sensing device with low sensing level detects the farthest hidden node as compared with the low sensitive sensing device. This is

because the carrier sensing area of the high-sensitive device with low sensing level is larger than the low sensitive sensing device. In this paper, such kind of high-sensitive sensing device with low sensing level for route construction as well as for the medium access is used. Figure 3a shows the carrier sensing area of high-sensitive sensing device and low sensitive sensing device.

2.1 Hidden node problem

Multi-hop networks are naturally vulnerable by the hidden node. This problem was first mentioned by Tobagi and Kleinrock in [28]. Any node within the communication range of the intended destination but outside the carrier sense range of the transmitter is potentially a hidden node [28]. The hidden node region to the source node, denoted by A_{h} shown in Figure 3b can be easily calculated using geometry as:

$$A_{\mathrm{h}} = \begin{cases} 0 & (d_{cs} \geq d_{tx} + d) \\ \beta d_{tx}^2 + dd_{cs}|sin\alpha| - \alpha d_{cs}^2 & (d_{tx} - d \leq d_{cs} \leq d_{tx} + d) \\ \pi(d_{tx}^2 - d_{cx}^2) & (d_{cs} \leq d_{tx} - d), \end{cases} \quad (1)$$

where, $\alpha = \cos^{-1}\left(\frac{d_{cs}^2 + d^2 - d_{tx}^2}{2dd_{cs}}\right)$, $\beta = \pi - \cos^{-1}\left(\frac{d^2 + d_{tx}^2 - d_{cs}^2}{2dd_{tx}}\right)$

3 Proposed method

In this section we explain the proposed method using a simple graph model. The detail explanation of our proposed method also explained in this section with example.

3.1 Graph model

In this paper, we consider a multi-hop WMN. All nodes communicate using identical, half duplex high-sensitive sensing device based on IEEE 802.11 DCF mode. Our objective is to construct a route with high throughput capacity for a given source and destination pair. We can model the network with two undirected graph G and G^*. $G(V, E)$, represents the set of all nodes V in the network and the set of edges E. An edge e_{ij} exists between transmitter nodes n_i and the receiver nodes n_j ($e_{ij} \varepsilon E$) if the two nodes are within the transmission rang of each other. In $G^*(V^*, E^*)$, V^* is the number of nodes within the carrier sensing area and E^* is the edge between the nodes within the carrier sensing area. To illustrate our proposed routing method consider the network topology in Figure 4. The solid circle represents the transmission range of the node which is located in the centre of the circle. The dotted circle in Figure 4a represents the carrier sense area of the conventional method. In Figure 4b, the dotted circle is the carrier sensing area of the proposed method. A route between the node S and the node D is required to establish. For explaining the proposed routing method some notation are defined as follows:

Figure 3 Illustration of area (a)carrier sensing (b)hidden node.
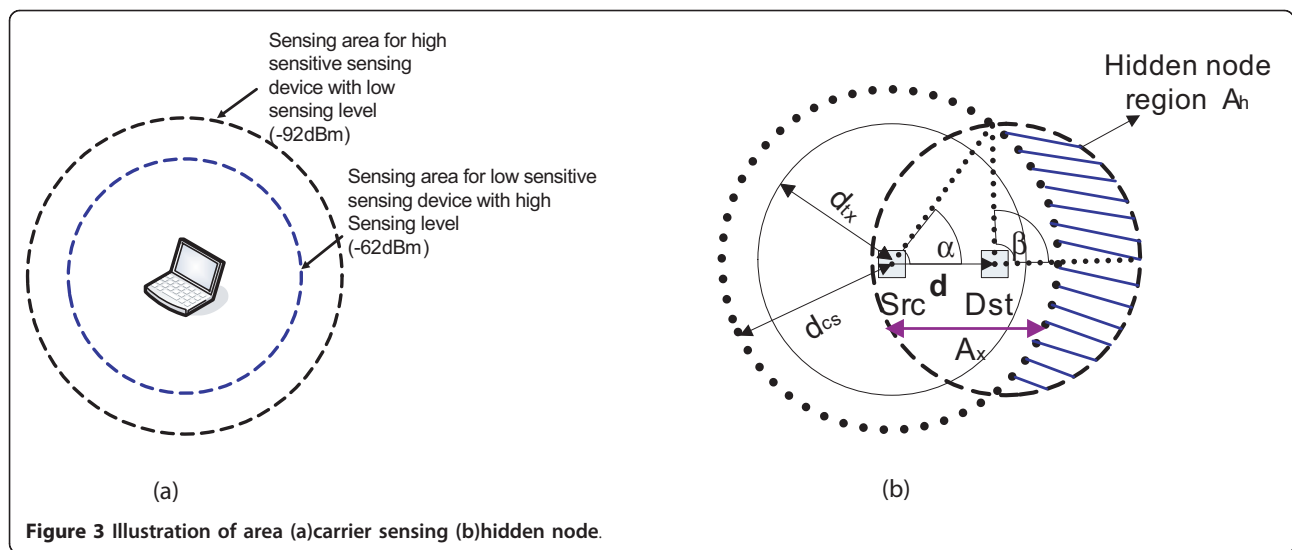
$v(i)$: Set of neighbors of the node

$v^*(i)$: Set of nodes within the sensing range of the node

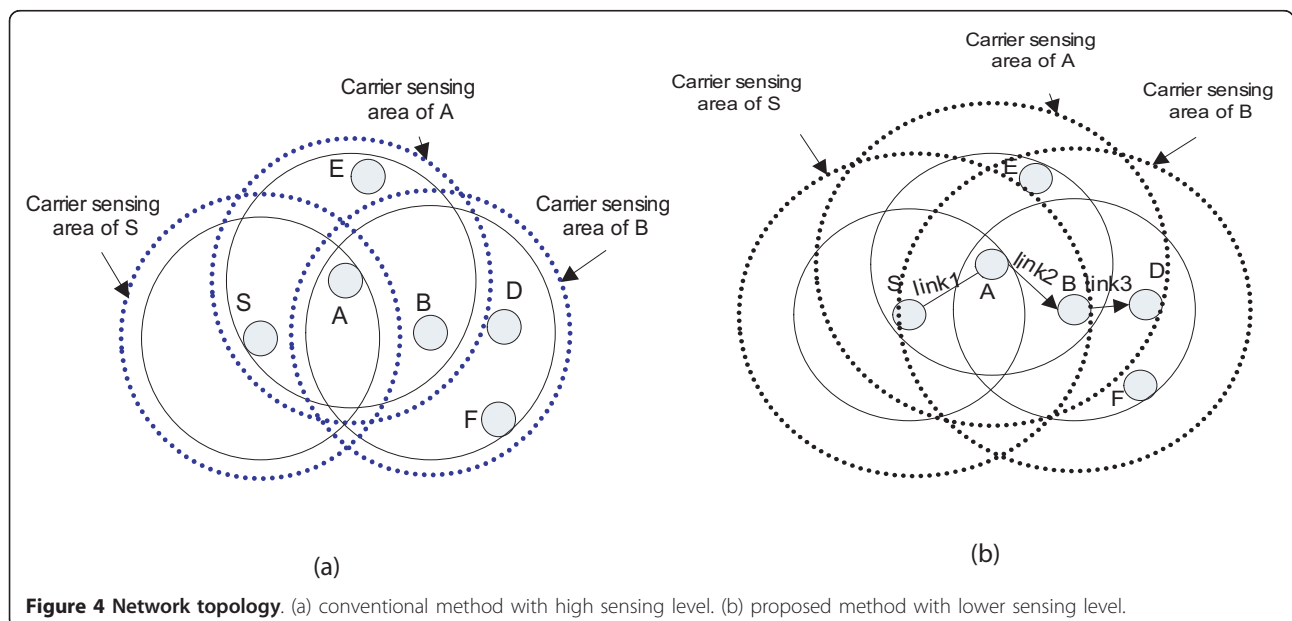$h(i)$: Set of hidden nodes of the node

The undirected graph $G(V, E)$ for the network topology of Figure 4 is shown in Figure 5a. By considering the graph, $G(V, E)$; $v(S)$ is referred to the node A; $h(S)$ is referred to the nodes B and E. $v(A)$ is referred to nodes B, E and S. The network using the proposed sensing area of Figure 4b is represented by the graph $G^*(V^*, E^*)$ shown in Figure 5b. According to this graph, $v^*(S)$ is referred to the nodes A and B, $v^*(A)$ is the nodes S, B, D and E. In the proposed routing method, B node can sense the previous hop node S. The node B i.e., ($v^*(S) \cap$
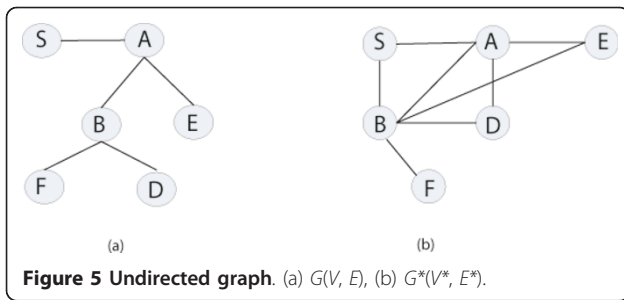
$v(A)$) is selected as the next hop node of the route. However, node E can not sense the previous hop node S. Next, node D can sense the previous hop node A, node D i.e., ($v^*(A) \cap v(B)$) is the next node of the path. A route [S, A, B, D] is established between the source and destination pair (S, D) without any hidden node. The proposed route is constructed using the following formula as:

$$N_i = v^*(i - 2) \cap v(i - 1). \tag{2}$$

Here, i is the hop number and N_i is the ith hop candidates node of the route.

In order to realize the route with avoiding the hidden node, the proposed routing method uses beacon signal

Figure 4 Network topology. (a) conventional method with high sensing level. (b) proposed method with lower sensing level.

**Figure 5 Undirected graph**. (a) *G(V, E)*, (b) *G*(V*, E*)*.

during the route construction. If each node after the transmission of the RREQ packet receives the same RREQ packets in the next time frame, the node transmits a beacon signal to the surrounding nodes. The beacon signaling is used for the detection of a node that is not hidden node. The beacon transmission timing is shown in Figure 6. Here the node *S* transmits the RREQ packet. If the node *S* receives the same RREQ packet in the next time frame (from first hop node *A*), it transmits a beacon signal to all of its surrounding nodes. This beacon signal transmitted from the node *S*, used to inform the existence of nodes without hidden node situation. All the nodes that can receive the beacon of the node *S* are selected for the candidate of the next hop node for the route.

When a source node has a data packet to transmit to a destination, it checks the routing table for the destination entry. If the route is unknown it generates a RREQ packet and broadcasts to its neighbor nodes. Each RREQ packet contains an ID, source and destination IP addresses, sequence number, hop count, and time out field. The ID field uniquely identifies each RREQ packet and the sequence number indicates the freshness of the packets. The hop count represents the path length between the source and the destination. The time out field indicates the time duration, during which each intermediate node waits for sensing the beacon of the previous hop node. When an intermediate node receives RREQ packet, it checks the source IP and ID pair. If any intermediate node receives two RREQ packets with the same source and ID pair then it will drop the duplicate RREQ packet. If the node receives multiple RREQ from different nodes, it forwards the first received RREQ and drops the others RREQs. After receiving the RREQ packet, the intermediate node senses the spectrum to detect the beacon of the previous hop node. If it cannot detect the beacon signal within the time out field duration it drops the RREQ. The RREQ packet is rebroadcast by the intermediate node if the node can detect the beacon signal and increment the hop count. The intermediate nodes also create and preserve a reverse route to the source node for a certain interval of time. There may be several RREQ packets finally arriving at the destination node along different paths. The route selection is made at the destination node. The destination node can use a routing metric to select the best route between the source and the destination node. Many routing metrics are proposed for this purpose. The proposed routing method will avoid the hidden node, no matter which routing metrics it uses for the route selection. In this paper, we use hop count routing metric to select a route. However, the proposed routing method can also perform well with other routing metrics such

Figure 6 Transmission timing of the beacon signal.
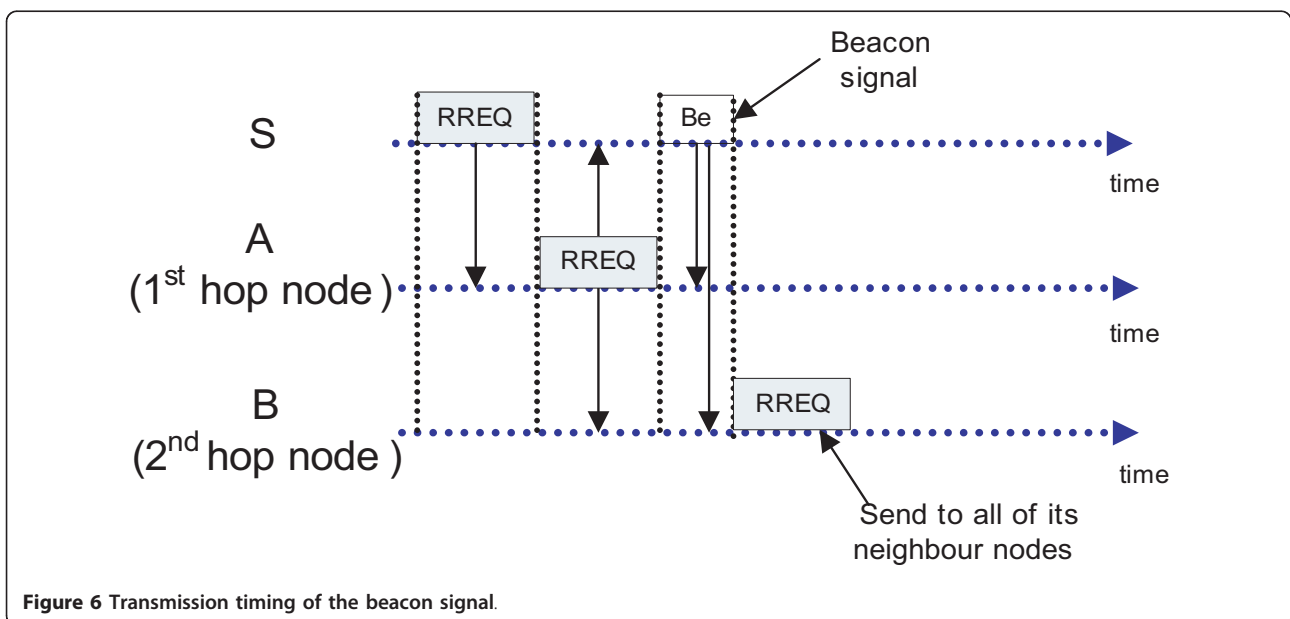
as ETX and ETT. In order to evaluate the numerical analysis, we use the hop count metric for the path selection. It simply chooses the route with minimum hop count. The destination node then generates a RREP packet, which contains the route record in RREQ and sends back to the source node via the reverse path.

3.2 Route construction example

The proposed route establishment procedure is explained below in details with an example. The image of the selected route is shown in Figures 7 and 8. The source node transmits the RREQ packet toward the surrounding nodes. Here, in Figure 7 the node A receives the RREQ from the source node and relay the RREQ to its entire surrounding nodes B, E and the source node S. When the source node S receives the RREQ packet from the node A, the source node sends the beacon signal. This beacon signal is used to inform the nodes that are not hidden nodes of the node S to be selected as the candidate node for the route. All the nodes surrounding the node A sense the beacon signal of the source node. If any node can sense the beacon signal of the source node, that node forward the RREQ to its surrounding nodes. In Figure 8, the node B can sense the beacon of the source node S and forward the RREQ packets to its surrounding nodes. However, node E cannot receive the beacon of the source node and it drops the RREQ packets. This is because, the node E is located outside of the carrier sensing area of the source node S. In the similar way, when the node A receives the RREQ from the node B, it broadcasts a beacon signal. All the surrounding nodes of the node B sense the beacon of the previous hop node A. This process will repeat until the destination node receives the RREQ. When the destination node receives the RREQ, it transmits the RREP to the source node by tracing the reverse path of the RREQ. Therefore, [S, A, B, D] route is constructed using the proposed method. When the node S is transmitting data to the node A, the second hop node B does not

start its transmission because the node B can sense the signal from the node S. In the conventional system, AODV routing protocol does not use any beacon transmission and sensing criteria during the route construction. Therefore, the relay node E may be in the route from the source to the destination. In this case, since the node S and the node E are the hidden node, the flow throughput degrades. The proposed routing method can avoid above self flow hidden node problem.

4 Network model and analysis

In this section first the successful transmission probability is derived. The next hop selection of the proposed routing method and the convention routing method (AODV) is calculated. Finally, we calculate the throughput performance of the proposed routing method and the conventional method.

4.1 Propagation model

In this paper, the propagation model we use only considers the distance attenuation due to path loss. For simplicity in analysis and in simulation we neglect the multi-path fading, or fading due to obstacles. Let P_t denote the transmit power, d is the distance between the transmitter and the receiver, λ is the wavelength of the signal, d_o is the reference distance and γ is the path loss exponent. The received power P_r can be written as:

$$P_r = P_t + 20 \ \log_{10} \left(\frac{\lambda}{4\pi d_o} \right) + 10\gamma \ \log_{10} \left(\frac{d_o}{d} \right). \quad (3)$$

Let, CS_{th} denote the carrier sensing threshold. We can drive the carrier sensing range d_{cs} of each station based on the propagation model as:

$$CS_{th} = P_t + 20 \ \log_{10} \left(\frac{\lambda}{4\pi d_o} \right) + 10\gamma \ \log_{10} \left(\frac{d_o}{d_{cs}} \right). \quad (4)$$
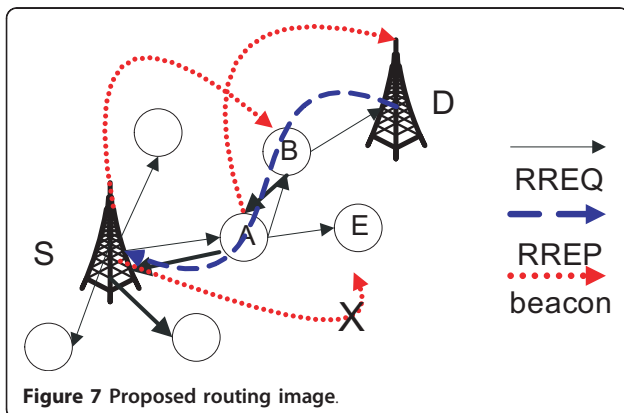
4.2 Network model

In this paper, we make some assumptions:

- Nodes are randomly distributed on a 2-D plane according to the Poisson distribution with density μ. In an area A, the probability of there being N, stations is:

$$P_n = \frac{(\mu A)^N}{N!} e^{-\mu A}. \quad (5)$$

- We assume all the stations in the network use fixed transmit power. We also assume the

Figure 7 Proposed routing image.

Figure 8 Operation of the proposed routing method.

transmission range d_{tx} and the interference range d_i are equal for all nodes.

• Packet generation follows the Poisson distribution with density λ^p/s.

• The receiver can decode the packet correctly if the Signal to interference and noise ratio (SINR) at the Receiver exceeds the minimum required SINR:

$$\text{SINR} = \frac{P_r}{P_i + \text{noise}} \geq \phi(dB), \qquad (6)$$

where P_i is the interference power and noise is the background noise.

4.3 Successful transmission probability

For an active node let P_a is the transmission probability and P_c is the collision probability. The packet transmission probability at a randomly chosen time slot can be given by [29,30]

$$P_a = \frac{2}{1 + \text{CW} + P_c \text{CW} \frac{(2P_c^m - 1)}{2P_c - 1}}, \qquad (7)$$

where CW is the minimum back off window size and m is the retry limit. A transmission attempt probability may collide by one or more nodes within region A_x as shown in Figure 2b when their back off counter reaches 0 at the same time. One or more node in the region A_h

also caused collision. Let P_x and P_h be the probability of this two collision events, respectively. Therefore, the probability of collision P_c is given by

$$P_c = P_x + P_h - P_x P_h. \qquad (8)$$

In our analysis, we assume for simplicity that the contention window size is held constant and P_x is fixed for simplicity. From [29], this is given by

$$P_x = \frac{2}{\text{CW} + 1}. \qquad (9)$$

Probability of hidden node collision can be expressed as

$$P_h = 1 - (1 - P_a)\mu A_h e^{-\mu A_h}. \qquad (10)$$

By plugging Eqs. (8), (9) and (10) into Eq. (7) we can calculate the value of P_a and P_c. Therefore, the probability of successful transmission can be obtained as

$$P_{\text{suc}} = P_a(1 - P_c). \qquad (11)$$

Let the probability that a time slot is a successful transmission slot, an idle slot and a collision slot as P_{suc}, P_{idle}, and P_c, respectively, and the corresponding duration as T_{suc}, T_{idle} and T_c, respectively. The mean duration required to transmit a packet successfully, T can be expressed as

$$T = P_{suc}T_{suc} + P_{idle}T_{idle} + P_cT_c. \tag{12}$$

The probability that a node is idle in a time slot is,

$$P_{idle} = 1 - P_{suc} - P_c. \tag{13}$$

The time duration can be expressed as

$$\begin{aligned} T_{suc} &= H + P + DIFS + ACK + SIFS \\ T_c &= H + P + DIFS + SIFS \\ T_{idle} &= \theta, \end{aligned} \tag{14}$$

where H and P are the time for the packet header (PHY and MAC headers) and the payload, respectively, and θ is the physical slot time.
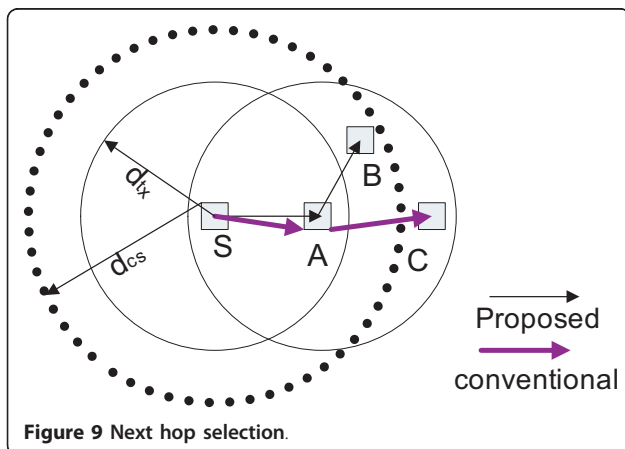
4.4 Next hop selection
4.4.1 Proposed routing
If a node can sense the beacon signal of its previous nodes it can be a candidate for the next hop node of the route. Let P_{cand} denote the probability of the candidate node that can be select as the next hop of the route. In our proposed method every node sense its previous hop node's beacon signal. The probability of the number of node that can sense the beacon of the node S as in Figure 9 is given by,

$$P_{be} = Pr\left[S^{be}|P_S\left(\frac{d_o}{d}\right)^\gamma \geq CS_{th} \right], \tag{15}$$

where, S^{be} is the number of the nodes that can sense the beacon of the node S, d is the distance between the node S and the nodes S^{be} and P_S is the transmit power of the node S (all nodes have same the transmit power, P_t). CS_{th} is the carrier sensing threshold. Probability of the number of candidate node for the next hop node can be expressed as

$$P_{cand} = P_{beacon} \cap P_A, \tag{16}$$

where, $P_A = \mu d_{tx}e^{-\mu d_{tx}}$ is the probability of the number of node exist within the node A's communication region. Let P_{sel} denote the probability that a node is selected as the next hop node of the route, it is given by:

$$P_{sel} = P_{suc}P_{cand}. \tag{17}$$

4.4.2 Conventional routing
We use AODV routing protocol as a conventional routing method to select the route between the source and destination pair. In the AODV routing protocol, the further stations have higher priority for the selection of the next hop node without considering hidden node. The probability of the candidate node for the next node in AODV is given by

$$P_{cand} = P_A. \tag{18}$$

$$P_{sel} = P_{cand}P_{suc}. \tag{19}$$

4.4.3 Throughput
Finally, we can use the value of P_a, P_c, T, and P_{sel} to calculate the throughput of the proposed and the conventional routing method as,

$$TH = P_{sel}P_a(1 - P_c)\text{Payload}\frac{\text{rate}}{T}. \tag{20}$$

where Payload is the packet payload size and rate is the data rate of the network.

5 Performance evaluation
In this section, we evaluate the performance of the proposed routing method using analysis and computer simulation. Furthermore, we compare it with the conventional AODV routing method.

5.1 Simulation set up
The simulation is carried out using MATLAB simulator. In our simulation, we adopt free space model as the propagation model. AODV routing protocol is chosen as the conventional routing protocol. The simulation parameters for MAC are identical to IEEE 802.11a standard listed in Table 1. The relay stations N are randomly distributed in $1,000 \times 1,000$ simulation area follow the Poisson distribution. Packet generation also follows the Poisson distribution. Each packet size is fixed to 1,500 bytes. The beacon packet size is 106 bytes. The source node and the destination node pairs are separated by R meter distance as shown in Figure 10. The carrier sensing threshold CS_{th} for the conventional system is set as -62 dBm. The proposed method uses appropriate lower sensing level which can be changed as a parameter. We measure the network throughput, collision probability and the network delay as the main evaluation metrics. Their definition as follows

Figure 9 Next hop selection.

Table 1 Simulation parameters.

Frequency	5 GHz
Transmitter power	10 dBm
Required SINR (data packet)	10 dB
Routing SINR	20 dB
Noise level	-95 dBm
Path loss exponent	2
Reference distance	1
Data rate	11 Mbps
Packet size	1,500 bytes
Que size	10
Slot time	9 us
DIFS	34 us
SIFS	16 us
ACK	5 us
CW_{min}-CW_{max}	15-1,023
Retry limit	3
Simulation time	800 ms

Network throughput It is defined as the amount of packets received successfully by the destination per unit time (in Mb/s).

Collision probability The ratio of the total number transmission failures over the total number of transmission attempts.

Network delay It is defined as the total time taken by the destination node to receive the packet successfully sent from the source node. It consists of two parts: route establishment delay and data transmission delay. Route establishment delay means the time required to transmit the RREQ from the source node to the destination node. Data transmission delay is the time that the packet spends in the wireless medium.

5.2 Appropriate sensing level

In order to find out the appropriate sensing level for the proposed method, the network throughput is derived by varying the sensing level. In this case, both the Proposed and conventional method uses hop count metric for route selection. We set $N = 200$ and $R = 400$ m. Figure 11a shows the throughput of the network using the proposed and conventional method by varying the sensing level from -110 to -60 dBm. We give both analysis and simulation results. It is seen from Figure 10a, in the proposed method the throughput is slightly decreasing as the sensing level is increasing from -91 to -60 dBm. This is because, the sensing range becomes smaller with the higher sensing level. In our proposed routing method, since the number of hop will increase with small sensing range, throughput becomes small. On the other hand, the throughput is also slightly decreasing with decreasing the value of the sensing level from -94 to -110 dBm. With this low sensing level the throughput is reduced because of lower frequency reuse in the flow. It is concluded that the proposed method achieves

Figure 10 Simulation model.
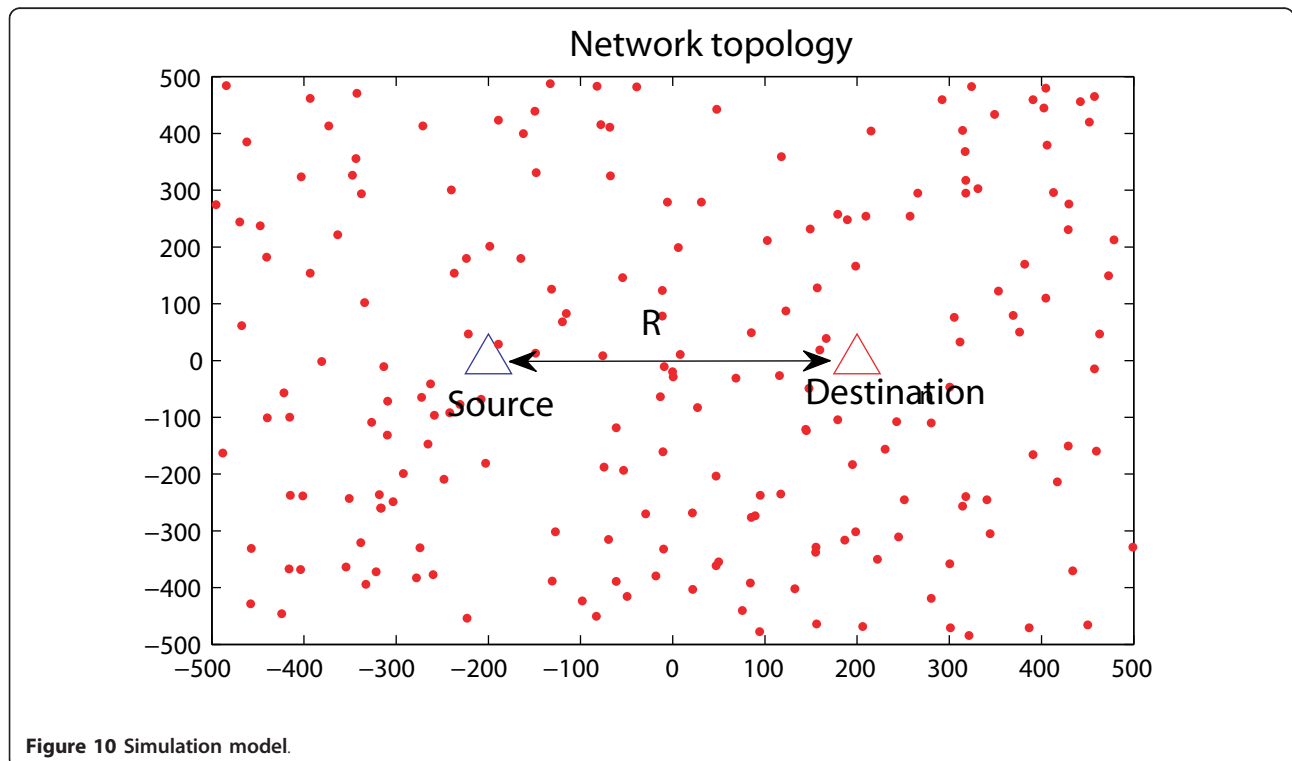
highest throughput when the sensing level is between -96 and -90 dBm. Therefore, in this paper we select -92 dBm as the appropriate sensing threshold, CS_{th} for the proposed method. With lower sensing level, the proposed and the conventional method performs the same. The reason is that the distance between each hop node in the route is fixed (SNR for routing is fixed to 20 dB) and the conventional method can avoid hidden node collision with lower sensing level. However, the throughput of the conventional method is rapidly decreasing compared with the proposed method with higher sensing level. This is because the conventional routing protocol AODV does not consider the existence of the hidden node during the route construction. In the media access CSMA/CA with higher sensing level cannot remove the hidden node. Therefore, the conventional method has lower throughput performance with higher sensing level. From Figure 11a, we can confirm that the proposed method has robustness against difference of sensing level. This is because the proposed method can avoid the hidden node even if the sensing level is higher. In general, the sensing level is decided as the receiver detection device ability. The robustness to the sensing level is very important for the realization of the wireless mesh network without effect of hidden node problem.

5.3 Results and discussions
5.3.1 Impact on network throughput
We first study the impact of single flow on throughput. Figure 11b depicts the impact on the network throughput for a single flow. In this case, R is varied from 100 to 1,000 m between the source and the destination pair.

The number of data packet is fixed to 200. The proposed method uses the appropriate sensing level -92 dBm and the conventional sensing level -62 dBm. According to Figure 11b, we can see that with small distance like 100-200 m, the throughput is almost the same for both the proposed system and the conventional system. The reason behind this is, direct communication can be established from the source to the destination with small distance and both systems do not have any hidden node i.e., the performance of both the proposed method and the conventional method is the same with the small distance between the source and the destination. However, the proposed method performs better than the conventional method with increasing distance due to the presence of hidden node. The proposed method also performs better even if it uses the conventional higher sensing level, -62 dBm. In the conventional system AODV does not consider the existence of the hidden node during the routing process and the media access CSMA/CA MAC protocol uses high sensing level of, -62 dBm so that it can not avoid hidden node problem.

Next we examine the throughput performance for high density networks, by changing the number of flow. Since the network area is fixed the more flow makes the network denser. The number of relay nodes is set to 200. The source and destination pairs are randomly selected. The distance between each source and destination is fixed as 400 m. The traffic load is fixed to 200 packets/s for each flow. The impact of the network density on the throughput is shown in Figure 12a. As the number of flow increases our proposed method performs better than the conventional method. The reason
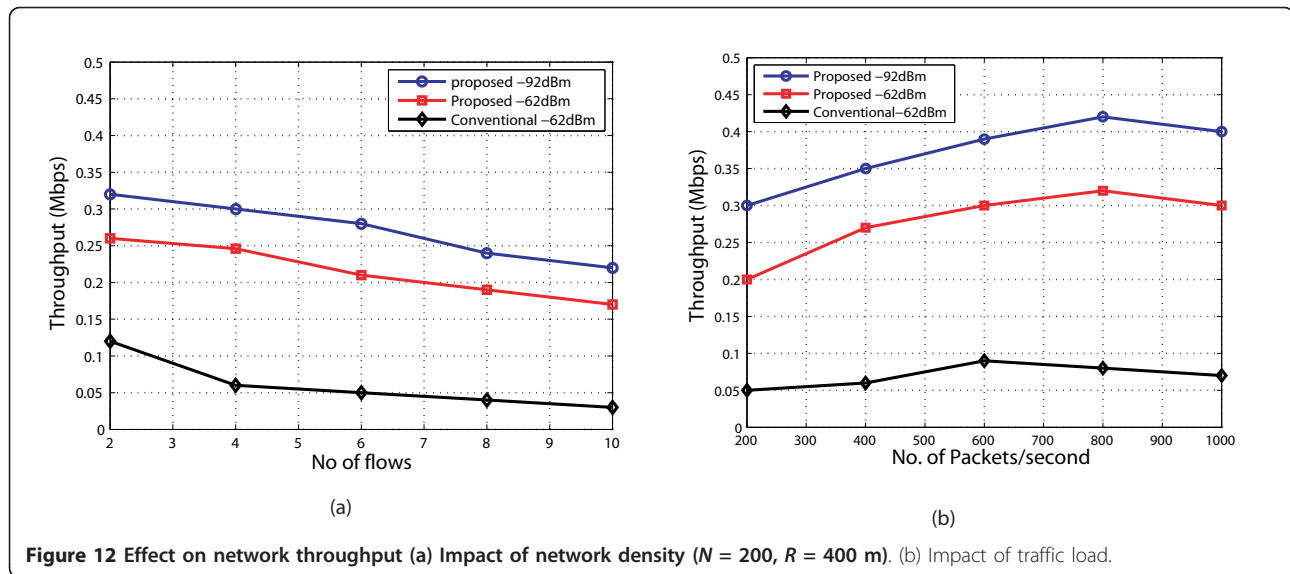

Figure 11 Effect on throughput for single flow. (a) simulation versus analysis with N = 200, R = 400 m, (b) varying distance between the source and the destination with N = 200.
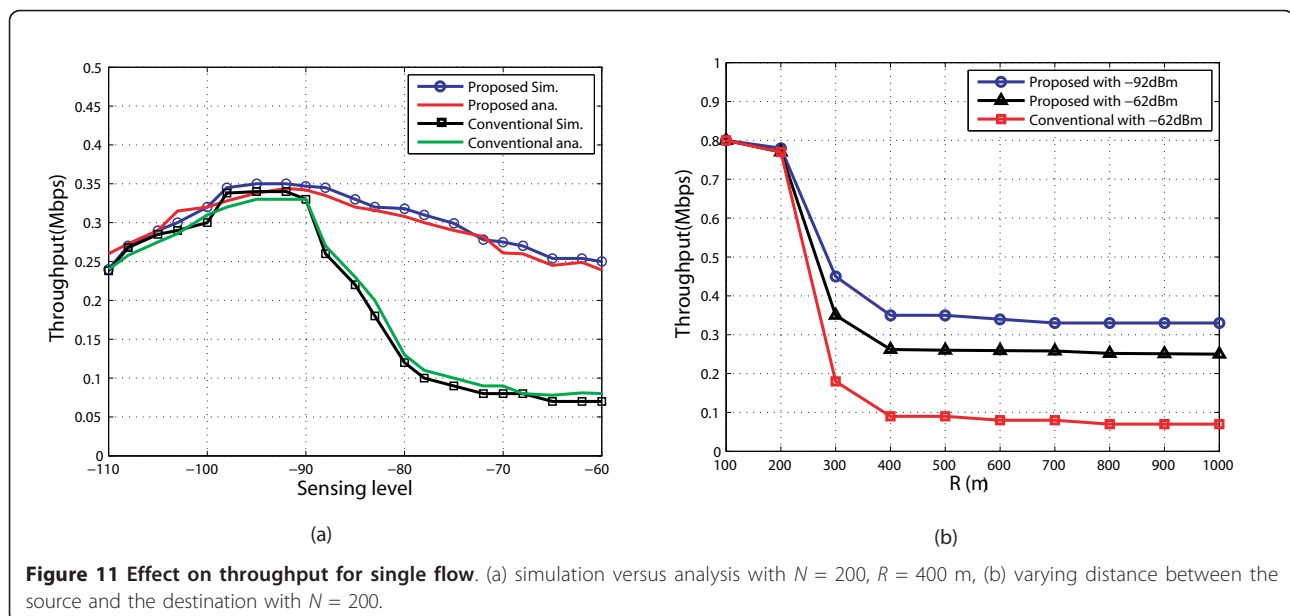
Figure 12 Effect on network throughput (a) Impact of network density ($N = 200$, $R = 400$ m). (b) Impact of traffic load.

is that with appropriate sensing level of the proposed method can remove the self flow interference as well as the multi-flow interference due to the hidden node. With high sensing level, -62 dBm, the proposed routing method also performs well. This is because of the hidden node collision absence in the self flow. However, as the number of flow continues to increase, the conventional method suffers a throughput drop due to more collision resulting from the hidden node.

In order to examine the impact of traffic load on the throughput we change the packet generation rate from 200 to 1,000 packets/s. The traffic flow is set to 4. The throughput under different traffic load is shown in the Figure 12b. The throughput of the proposed method with appropriate sensing level -92 dBm and conventional sensing level -62 dBm keeps increasing with traffic loads. This is because with high traffic load our proposed method does not have collisions due to hidden node. However, the throughput of the conventional method decreases as the traffic load increases. The reason for this is the collisions due to the high traffic load can not overcome.

Moreover, we can see the performance of the proposed method by changing the routing metrics for the route selection. In this case, we use other two routing metrics ETX and ETT. The throughput performance of the proposed method and the conventional method by changing the routing metrics is shown in Figure 13. In this case, both the proposed and the conventional methods use the conventional sensing level -62 dBm. When we used the routing metrics ETX and ETT, the proposed method performs better than the conventional routing method that also uses ETX and ETT. The reason is that, these routing metrics do not affect the

influence of the hidden node. However, the proposed routing method avoids the hidden node during the route formation. It can achieve a significant throughput improvement, no matter which routing metrics is used for the route selection.

5.3.2 Impact on collision probability

We first compare the probability of collision between the proposed method and the conventional method for single flow shown in Figure 14a. In this case, the proposed method uses the appropriate sensing level -92 dBm and the conventional sensing level -62 dBm. The probability of collision due to the hidden node in our proposed method is zero. This is because our proposed method chooses a route without hidden node. The self flow inference due to the hidden node can be avoided in the proposed method. However, in the conventional method with increasing the number of hop in the route, the probability of collision due to the hidden node also increases.

The proposed method achieves a significant throughput improvement compared with the conventional method because it efficiently eliminates the collision from hidden node. This can be observed in Figure 14b, which shows the collision probability under different network density. In this case we fix the traffic load to 200 packets/s for each flow. As shown in the figure, the proposed method has the lowest collision probability compared with the conventional method. We can also observe from this figure that the collision probability of the conventional method increases sharply when the network becomes denser (e.g., more than four flows). This is because when the network becomes busy, self flow and multi-flow collisions occur due to the presence of the hidden node. The proposed method with -62
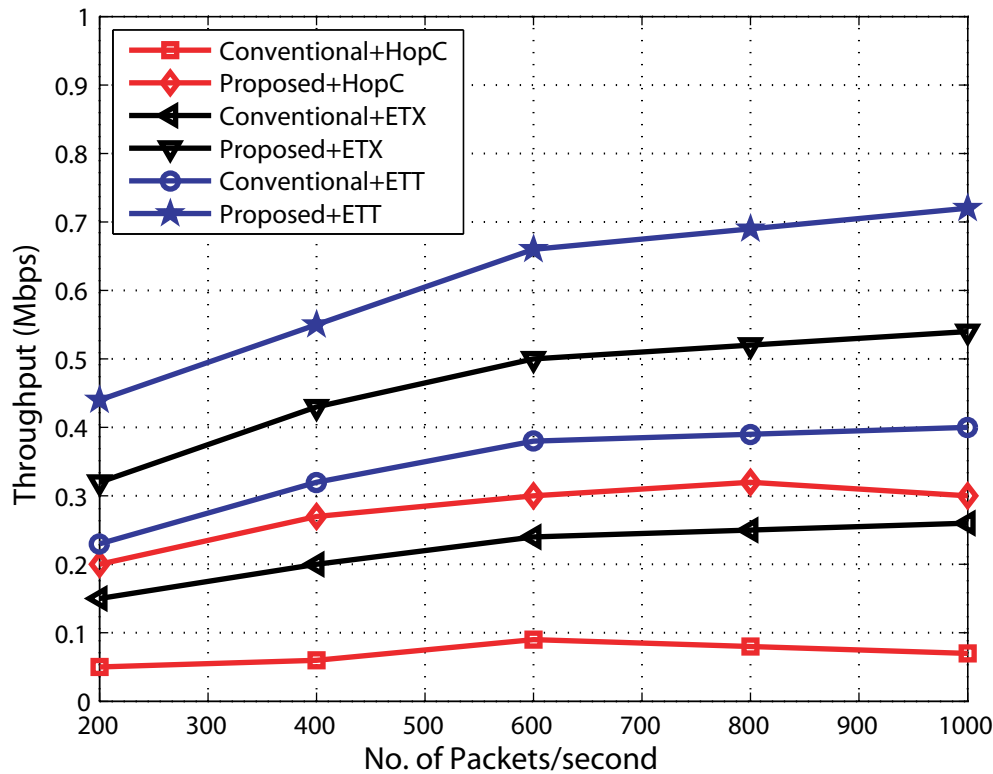
Figure 13 Impact on Throughput by changing Hopcount, ETX and ETT routing metrics (*N* = 200)**.

dBm sensing level provides better performance because it removes the self flow interference. However, with appropriate sensing level -92 dBm the proposed method can minimize the multi-flow interference due to the avoidance of hidden node. Therefore, the proposed methods possess a leading performance in both aggregate throughput and collision probability even in dense networks. Compared with Figure 12b, we can find that the impact of traffic loads on collision probability is similar to that of network densities. More specifically, the collision probability increases with the traffic loads, and the proposed method also has the lowest collision probability under all the different traffic loads which is shown in Figure 15a.

Beacon signal is used in our proposed method during the route construction. Every node transmits beacon signal after the transmission of the RREQ packet. For high density network there is some probability of beacon collision. In order to investigate the effect of the network density on the beacon signal, the probability of the beacon collision is calculated by varying the number of the multi-hop flow is shown in Figure 15b. In this case, the traffic generation rate is fixed to 200 packets/s for each flow. The number of relay node is 200. The source node

and the destination node are randomly generated within the simulation area. We assume all pairs start routing phase simultaneously and we check the collision of beacon signal. It is observed from Figure 15b, the probability of beacon collision is very low. Because the duration of the beacon packet is very small and the beacon packet takes priority over the data packet transmission. Thus the beacons are rarely collide.

In addition, to observe the impact on the probability of collision we change the routing metrics from hop count to the ETX and ETT. In this case we change routing metrics for both the proposed and the conventional method. From Figure 16, we can see that the proposed method yields the lowest collision probability compared with the conventional method, with all routing metrics. This is due to the absence of the hidden node in the proposed routing method.

5.3.3 Impact on network delay

Figure 17a shows the route establishment delay of the proposed routing method against the conventional routing method. Compared with the conventional routing, the proposed routing yields larger delay. This is because, the proposed routing uses the sensing function to sense the beacon signal of the previous hop node. It took
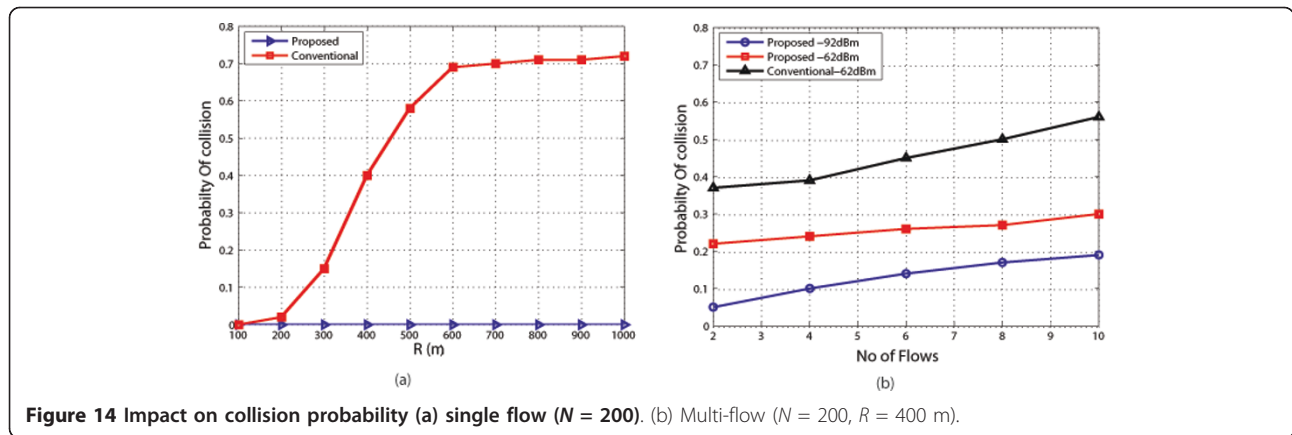
Figure 14 Impact on collision probability (a) single flow (*N* = 200). (b) Multi-flow (*N* = 200, *R* = 400 m).
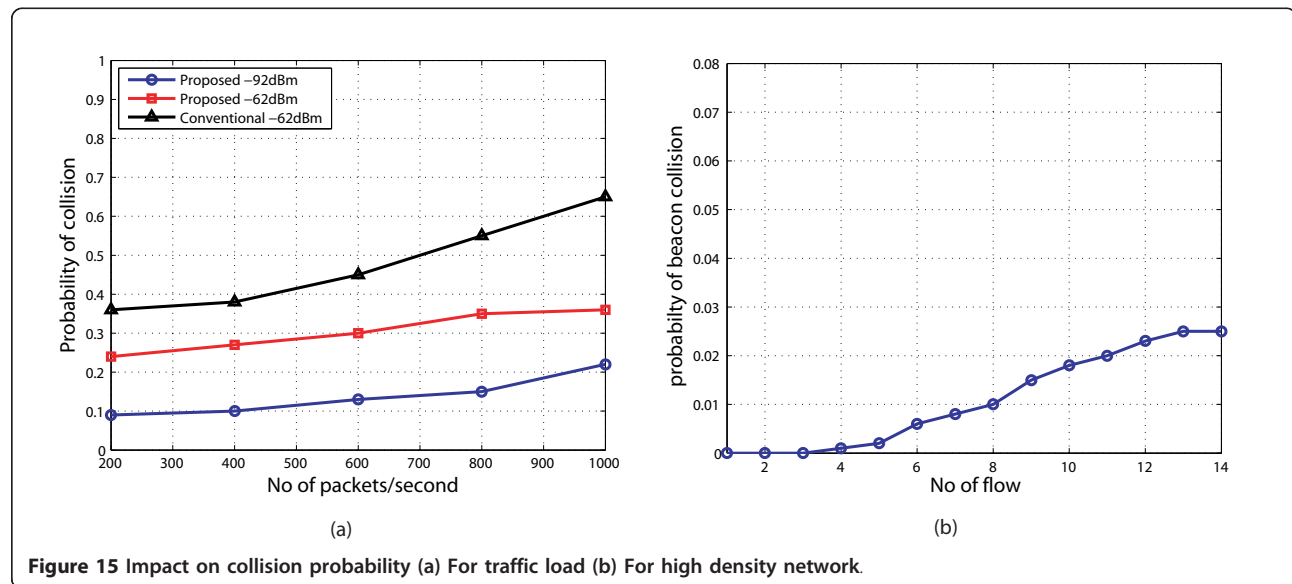

Figure 15 Impact on collision probability (a) For traffic load (b) For high density network.

some extra time for constructing the route compared with the conventional routing method. However, Figure 17b illustrates that the proposed method performs much better than the conventional method in terms of the data transmission delay. This is caused by the hidden node problem avoidance. During the data transmission, the packet collision occurs in the conventional method due to the presence of the hidden node. However, in the proposed method, there is no data collision due to the hidden node. That is why, our proposed method has lower data transmission delay. Figure 18 shows the overall network delay comparison. From this simulation result, we can conclude that the proposed method has lower network delay than that with the conventional method.

6 Conclusions

In this paper, we present a novel routing method using a high-sensitive sensing function for a multi-hop

wireless mesh network. Using the sensing function, all nodes sense the medium of the interfered nodes before constructing the route. Beacon signal is used to avoid the existence of a self flow hidden node. During the route construction, all nodes sense the beacon of its previous hop nodes. The next node of the route is selected depending on this beacon signal sensing result. In this way, the proposed method choose a node as the next hop node for the route which is not a hidden node. Thus the constructed route in this way is a hidden node free route. Due to this sensing technique, the hidden node does not start its transmission if its previous hop node is busy. Using appropriate lower sensing level high end-to-end network throughput is achieved. We use the hop count routing metric for numerical analysis. However, the proposed method also performs well with other routing metrics such as ETX and ETT checking with computer simulation. From the computer simulation, it is confirmed that the proposed routing method
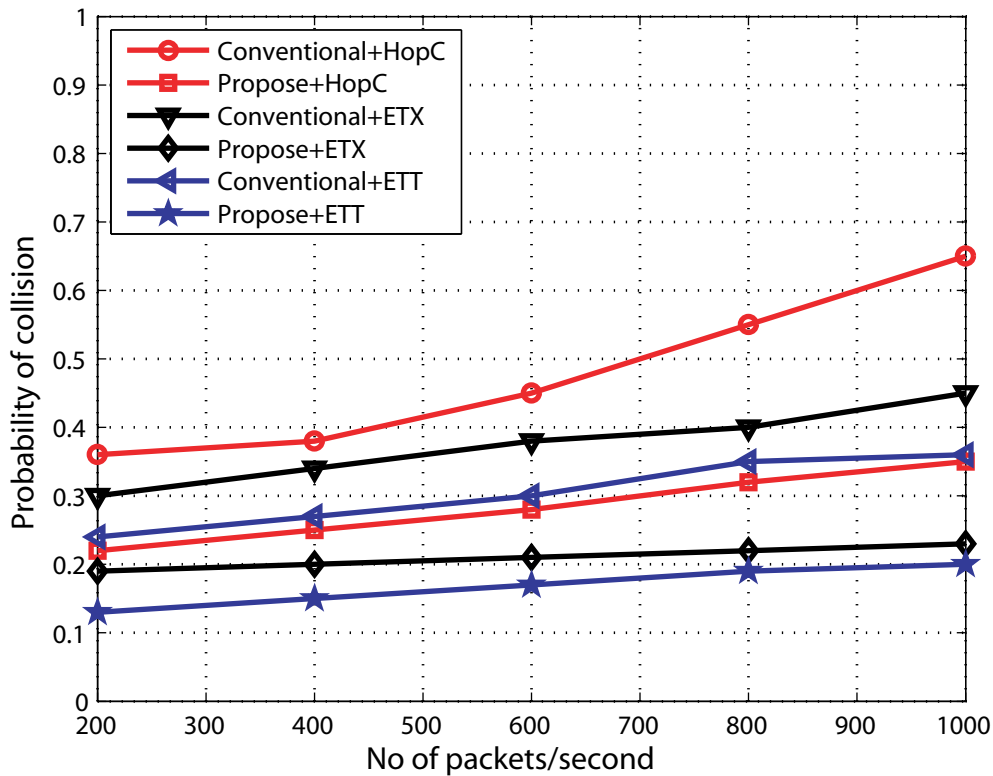
Figure 16 Impact on Probability of collision with Hopcount, ETX and ETT routing metrics (*N* = 200).

improves the network throughput as well as reduce the probability of collision with ETX and ETT routing metrics. Our numerical and simulation results agree quite well. It is concluded that the network throughput

has been significantly improved due to the absence of the hidden node. This is because, the proposed method can avoid the hidden node problem by combining the sensing criteria and beacon signal during the route
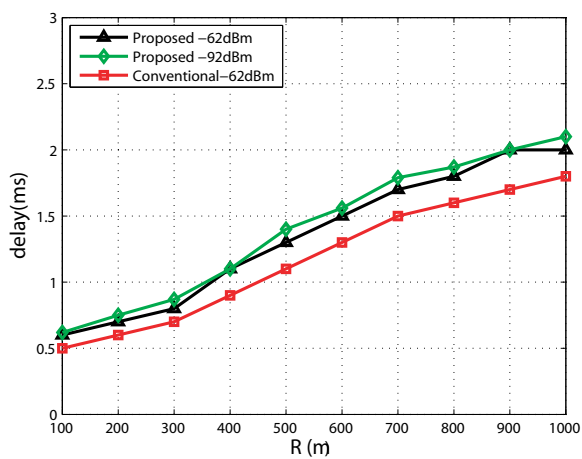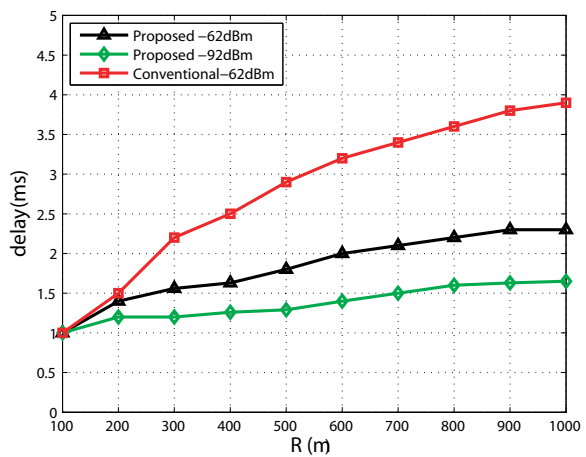
Figure 17 Effect on delay. (a) Route establishment delay, (b) data transmission delay.
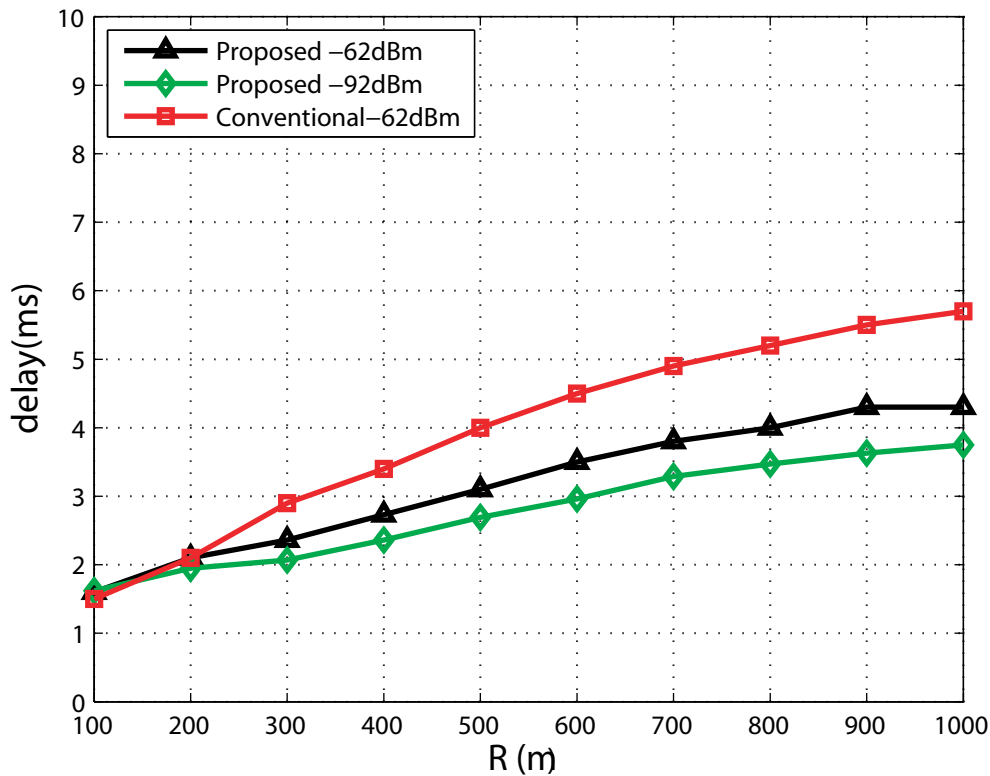
Figure 18 Network delay (route establishment delay + data delay).

construction. It can be confirmed that the proposed routing method achieves better performance compared with the conventional method, because the proposed system can avoid the hidden node problem. The numerical analysis of the proposed routing method with routing metrics ETX and ETT is our future works. Moreover, we will evaluate the performance of the proposed routing method with other routing metric like Airtime in the future.

Competing interests
The authors declare that they have no competing interests.

References
1. IF Akyildiz, X Wang, W Wang, Wireless mesh networks: a surveys. IEEE Comput Netw. **47**(4), 445–487 (2005)
2. R Bruno, M Conti, E Gregori, Mesh networks: commodity multihop ad hoc networks. IEEE Commun Mag. **43**(3), 123–131 (2005)
3. Y Zhang, L Jijun, H Honglin, *Wireless Mesh Networking*, (Auerbach publication, Boca Raton, 2007)
4. MS Gast, *802.11 Wireless Networks: The definitive Guide*, (O'Reilly & Associate, USA, 2002)
5. DB Johnson, DA Maltz, *Dynamic Source Routing in Ad Hoc Wireless Networks*, ed. by Imielinski T, Korth H, Proceedings of Mobile Computing,chapt. 5 (Kluwer Academic Publishers, Dordrecht, 1996), pp. 153–181
6. C Perkins, EM Royer, SR Das, *Ad Hoc On-Demand Distance Vector (AODV) routing*, in *IETF RFC 3561* (Jul 2003)
7. S Khurana, A Kahol, AP Jayasumana, Effect of Hidden Terminal On The Performance of IEEE 802.11 MAC Protocol, in *Proceedings of IEEE LCN'98*, 12–22 (Oct 1998)
8. Z Hadzi-Velkov, L Gavrilovska, Performance of the IEEE 802.11 Wireless LANs Under Influence Of Hidden Node, in *Proceedings of IEEE PWCS*, 221–225 (Feb 1999)
9. ANSI/IEEE Std 802.11, Part II: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. (1999)
10. K Xu, M Gerla, S Bae, Effectiveness of RTS/CTS handshake in IEEE 802.11 based adhoc networks. Ad Hoc Netw J. **1**, 107–123 (2003)
11. P Gupta, PR Kumar, The capacity of wireless networks. IEEE Trans Inform Theory. **46**(2), 388–404 (2000)
12. J Deng, B Liang, PK Varshney, Tuning the Carrier Sensing Range of IEEE 802.11 MAC, in *Proceedings of IEEE Globecom'04*. **5**, 2987–2991 (Dec 2004)
13. R Hekmat, PV Mieghem, Interference in Wireless Multi-hop Adhoc Networks and its Effect on Network Capacity, in *Proceedings of Med-hoc-Net* (Sept 2002)
14. J Zhu, X Guo, LL Yang, WS Conner, Leveraging Spatial Reuse in 802.11 Mesh Networks with Enhanced Physical Carrier Sensing, in *Proceedings of IEEE ICC* (June 2004)
15. X Yang, NH Vaidya, On the Physical Carrier Sense in Wireless Ad Hoc Networks, in *Proceedings of IEEE Infocom* (Mar 2005)

16. H Zhai, Y Fang, Physical Carrier Sensing and Spatial Reuse in Multirate and Multihop Wireless Ad Hoc Networks, in *Proceedings of IEEE Infocom* (Apr 2006)

17. TS Kim, H Lim, JC Hou, Improving Spatial Reuse Through Tuning Transmit Power, Carrier Sense Threshold, and Data Rate in Multihop Wireless Networks, in *Proceedings of ACM MobiCom* (Sept 2006)

18. Z Zeng, Y Yang, JC Hou, How Physical Carrier Sense Affects System Throughput in IEEE 802.11 Wireless Networks, in *Proceedings of IEEE Infocom* (Apr 2008)

19. J Fuemmeler, N Vaidya, VV Veeravalli, Selecting the Transmit Powers and the Carrier Sensing Thresholds for CSMA Protocols, in *Proceedings of Wicon*, 1321–1329 (Aug 2006)

20. E Hossain, VK Bhargava, *Cognitive Wireless Communication Networks*, (Springer, Berlin, 2007)

21. D Cabric, SM Mishra, RW Brodersen, Implementaion issues in spectrum sensing for cognitive radios. Proc Signals Syst Comput. **2**, 772–776 (2004)

22. J Mitra, GQ Maguire Jr, Cognitive radio: making software radios more personal. Proc IEEE Pers Commun. **6**(4), 13–18 (1999)

23. D De Couto, D Aguayo, J Bicket, R Morris, A High-Throughput Path Metric for Multi-Hop Wireless Routing, in *Proceedings of ACM MobiCom* (Sept 2003)

24. J Padhye, R Drave, B Zill, Comparison of routing metrics for static multi hop wireless networks. in *Proc ACM SIGCOM* (Sept 2004)

25. Wireless Medium Access Control (MAC) and physical layer (PHY) specifications: Amendment: ESS Mesh networking. IEEE P802.11s/D1.00 (Nov. 2006)

26. H Uchiyama, K Umebayashi, Y Kamiya, Y Suzuki, T Fujii, F Ono, K Sakaguchi, Study on Cooperative Sensing in Cognitive Radio Based Ad-Hoc Network, in *Proceedings of IEEE Pimrc* (Sept 2007)

27. H Urkowitz, Energy Detection of unknown deterministic signals. Proc IEEE. **55**(4), 523–531 (1967)

28. F Tobagi, L Kleinroack, Packet Switching in radio channels: Part II—The Hidden Terminal Problem in carrier Sense Multiple-Access and the Busy-Tone Solution. IEEE Trans Commun. **23**, 1417–1433 (1975)

29. G Bianchi, Performance analysis of the IEEE 802.11 distributed coordination function. IEEE J Sel Area Commun. **18**(3), 535–547 (2000)

30. F Cali, M Conti, E Gregori, Dynamic tuning of the IEEE 802.11 Protocol to Achieve a Theoretical Throughput Limit. IEEE/ACM Trans Netw. **8**(6), 785–799 (2000)