Sensors and Materials, Vol. 36, No. 12 (2024) 5215–5232
MYU Tokyo

S & M 3863

Performance of Media Access Control Protocol in Multi-hop Wireless Sensor Networks for Bridge Detection Systems

Zhengsong Ni,[1] Shuri Cai,[2*] and Cairong Ni[2]

[1]College of Big Data and Artificial Intelligence, Fujian Polytechnic Normal University,
No. 1 Campus New Village, Longjiang Street, Fuqing, Fuzhou, Fujian 350300, China
[2]Institute of Highway Science, Ministry of Transport, Beijing University of Posts and Telecommunications,
8 Xitucheng Road, Haidian District, Beijing 100086, China

(Received April 30, 2024; accepted October 29, 2024)

Keywords: multi-hop wireless sensor network, media access control protocol, bridge detection, hidden terminal, exposed terminal

The multi-hop wireless sensor network is a type of data acquisition and transmission technology, which has wide application prospects in bridge detection systems. To achieve efficient and reliable data transmission, the media access control (MAC) protocol is essential. The purpose of this study is to evaluate the performance of different MAC protocols in bridge detection systems on multi-hop wireless sensor networks. By comparing several commonly used MAC protocols, we analyzed their differences in data transmission delay, energy efficiency, and network capacity. First, we simulated the multi-hop wireless sensor network in a bridge detection system by establishing a network model. Then, we selected several common MAC protocols as evaluation objects, including CSMA/CA, TDMA, and ALOHA. We simulated different practical application scenarios by setting different parameters and scenarios in the network model. Through the analysis of the experimental results, we found that there are some differences in the performance of different MAC protocols. The CSMA/CA protocol performs well in terms of data transfer latency, but poorly in terms of network capacity and energy efficiency. The time division multiple access (TDMA) protocol performs well in terms of network capacity and energy efficiency, but is sensitive to data transmission delays. The ALOHA protocol performs poorly in terms of network capacity, but can provide a lower data transfer latency. On the basis of the evaluation of the performance of these protocols, the following conclusions are drawn. For multi-hop wireless sensor networks in bridge detection systems, it is very important to choose a suitable MAC protocol. The CSMA/CA protocol is a good choice in application scenarios that require real-time responses, whereas the TDMA protocol can provide higher network capacity and energy efficiency when no data transmission latency is required. In addition, note that the performance of the MAC protocol may vary under different network loads and topologies. Therefore, in practical applications, it is crucial to choose the right MAC protocol according to the specific situation. In summary, in this study, we provide reference and guidance for selecting a suitable MAC protocol by studying the performance of multi-hop wireless sensor networks in

[*] Corresponding author: e-mail: caishuri@126.com

https://doi.org/10.18494/SAM5119

ISSN 0914-4935 © MYU K.K.
https://myukk.org/

bridge detection systems. Our research results are of great significance for improving the data transmission efficiency and reliability of bridge detection systems.

1. Introduction

Wireless sensor networks (WSNs) have become an important part of many real-time monitoring and control systems. In the field of bridge structural health monitoring, the application of WSNs first involves the deployment of wireless sensor nodes and network coverage to collect and transmit bridge structural information in real time. However, the challenges of bridge detection systems include limited node energy, an uneven distribution density of sensor nodes, and limited signal propagation. In addition, data conflict between nodes and a multipath propagation effect will also lead to the degradation of network transmission performance.(1)

To solve these problems, researchers have proposed a number of media access control (MAC) protocols based on multi-hop communication, which are designed to improve the performance and extend the lifetime of the network.(2) These protocols utilize multi-hop communication to maximize the coverage of the network and are optimized in terms of energy consumption and transmission latency. However, most existing MAC protocols are not designed with the special needs of bridge detection systems in mind.

Therefore, in this work, we aim to study the performance of the MAC protocol in multi-hop WSNs in bridge detection systems.(3) Specifically, we will focus on the following areas.

First, the applicability and limitations of the existing MAC protocols in bridge detection systems are discussed. By analyzing the existing protocols, we can understand their advantages and disadvantages in meeting the needs of bridge monitoring.(4)

Second, we will propose an improved MAC protocol design for bridge detection systems. The new protocol will fully consider the characteristics of the bridge structure, including node energy limitation, data collision, and multipath propagation, and optimize the network performance.(5)

Then, the performance of the proposed improved protocol in bridge detection systems is evaluated on the basis of simulation experiments. By comparing with existing MAC protocols, we can evaluate the feasibility and effectiveness of the improved protocols.(6)

Finally, we will summarize the research results and put forward the prospect of future work. We will discuss the advantages and limitations of the improved protocol and how to further improve and extend this research.(7)

Through the development of this research, we hope to provide an effective MAC protocol for WSNs in bridge detection systems, so as to improve the performance and reliability of the network. This will provide more accurate and real-time data for bridge structural health monitoring and strong support for bridge maintenance and management decisions.(8)

2. Research Status at Home and Abroad

The application of WSNs in bridge detection systems has attracted extensive research interest. In this field, the research of MAC protocols in multi-hop WSNs is very important. The following will introduce the research status of this topic at home and abroad.

Foreign research status:

(1) S-MAC: S-MAC is a classic multi-hop MAC protocol designed to extend network life and reduce energy consumption. It saves energy by periodically going into the sleep mode and uses slot synchronization to reduce data conflicts. However, S-MAC does not take into account the special needs of bridge detection systems.(9)

(2) T-MAC: T-MAC is another MAC protocol based on slot synchronization. It introduces a clustering mechanism to reduce energy consumption and data conflicts. However, T-MAC also does not take into account the special needs of bridge monitoring systems.(10)

(3) B-MAC: B-MAC is a MAC protocol for low-power sensor networks. It uses low-power slot synchronization and conflict avoidance mechanisms to minimize energy consumption. However, B-MAC does not take into account the problems of data collision and multipath propagation in bridge detection systems.(11)

Domestic research status:

(1) MAC protocol based on TDMA: Some domestic research teams have proposed the MAC protocol based on TDMA to solve the problem of data conflict and energy consumption. By allocating time slots to each node, they avoid data conflicts and improve the throughput of the network. However, this protocol still has some limitations in terms of node failure and network dynamics.(12)

(2) Routing-based MAC protocol: Some domestic researchers have proposed the routing-based MAC protocol to improve network performance by optimizing data transmission paths and dynamically adjusting routes. This protocol can adapt to the environment of uneven node density and multi-path propagation, but its effectiveness in practical applications needs to be further verified.(13)

(3) Other improved protocols: Some researchers have proposed protocols based on channel selection and power control to improve network performance and energy utilization efficiency. These improved protocols take into account the special needs of bridge detection systems and are optimized in terms of energy consumption and data transmission.(14)

Considering the research status at home and abroad, the application of MAC protocols in multi-hop WSNs in bridge detection systems is still facing challenges. The existing protocols do not fully consider the characteristics of bridge monitoring systems, such as node energy limitation, data conflict, and multipath propagation. Therefore, it is necessary to further study and improve the MAC protocol to improve the network performance and reliability of bridge detection systems.

For wireless data communication, the average large-scale path loss of the wireless signal from the sender to the receiver can be expressed as(1)

$$\overline{PL}(d) \propto \left(\frac{d}{d_0}\right)^n . \tag{1}$$

Here, n is the path loss index, the value of which depends on the propagation environment. n is 2 when the signal propagation is approximated to the free space model and 4 when the signal propagation is approximated to the two-path model, and d_0 is the reference distance of the antenna far field. As can be seen from Eq. (1), the power of the radio wave signal decreases exponentially with the increase in distance between the two communication parties. Therefore, when long-distance communication is carried out, in order to ensure reliable wireless data transmission, a large transmission power must be used to obtain a sufficient signal-to-noise ratio level at the receiving antenna. In contrast, if the distance between wireless nodes is very small, then under the same bit error rate conditions, a small antenna transmission power can be used compared with long-distance communication, thus achieving energy savings of the nodes. On the basis of the above considerations, a short-range wireless communication unit with micro-power consumption is selected. A micro-power, short-distance wireless communication unit can save node energy but also make the wireless network topology more complex, because to achieve long-distance wireless data transmission, it must pass through a number of node relays, that is, wireless nodes organized into a multi-hop network.

In the bridge wireless detection system, a large number of wireless sensor nodes must share a limited wireless channel under the management of the MAC protocol, which directly affects the performance indicators of the network such as throughput, delay, and energy consumption, especially in the multi-hop network topology. Overcoming the impact of hidden and exposed terminals is a key issue to be addressed first.

3. Hiding and Exposing Terminal Problems

Hidden and exposed terminals are typical problems of multi-hop wireless networks. Figure 1 shows the concept of a hidden terminal. A hidden terminal is a node C that is outside the radio wave coverage of the sending node A but within the radio wave coverage of the receiving node B. The hidden terminal C cannot receive the data sent by the sending node A to the receiving node B. During the communication between the nodes A and B, if the node C sends data to the node D, transmission conflicts will occur at the node B, resulting in the node B being unable to interpret any information, thus reducing channel utilization and increasing system power consumption. Similarly, when the node C sends information to the node B, the node A is also a hidden terminal for the node C. Hidden terminal conflicts cause the communication node to retransmit the sent information. If hidden terminal conflicts continue after retransmission, the network communication will fall into a vicious circle.(15)

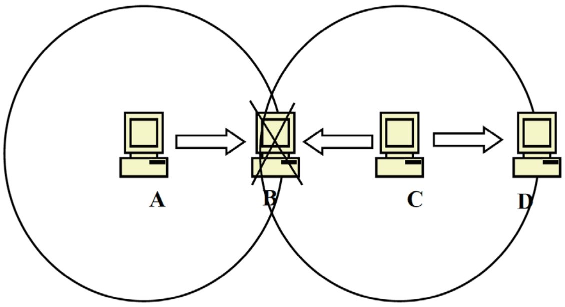

Fig. 1. (Color online) Hidden terminal.

Figure 2 shows the concept of an exposed terminal. An exposed terminal is a node C that is outside the radio wave coverage of the receiving node A, but within the radio wave coverage of the transmitting node B. Although the transmission of the node C will not interfere with the reception of the node A, after detecting the data sent by the node B, the node C cannot determine whether its data transmission will affect the data transmission of the node B, so it delays the transmission of its data to the node D. Exposed terminal problems will considerably reduce wireless link utilization.(16)

For hidden and exposed terminals, the common solution is to use control packets to shake hands with each other before sending data. For example, in Fig. 1, when the node A wants to send data to the node B, the node A first sends an request to send (RTS) packet to the node B. After receiving the RTS packet, the node B sends a clear to send (CTS) packet to the node A if it agrees to receive the data. After receiving the CTS packet, the node A can send data to the node B. If the node A does not receive the CTS packet within a specified period, the node A considers that a conflict occurs and resends the RTS packet. Under this mechanism, the hidden terminal C receives the CTS packet sent by the node B and knows that the node C wants to receive data from the node A, so as to delay its own transmission. This reduces the problem of hidden terminals. Similarly, according to Fig. 2, the exposed terminal listens to the RTS packet sent by the sending node B, but not to the CTS packet returned by the receiving node. Knowing that the node B has data to send, it normally sends its own services. A simple handshake mechanism can only reduce the conflict of data groups, but cannot fundamentally eliminate the problem of hidden and exposed terminals.

4. Performance Analysis of IEEE 802.11MAC in Multi-hop Networks

IEEE 802.11 is a communication protocol widely used in wireless LAN. Its MAC layer protocol defines two types of MAC mechanism, point coordination function (PCF) and distributed coordination function (DCF). PCF is suitable for polling access control with access control points (aps), and the network topology is a single-hop network, whereas DCF can provide distributed access control, which is suitable for a single-hop or multi-hop network.

IEEE802.11DCF is a MAC protocol based on CSMA/CA, which is mainly used to solve the competition problem when multiple wireless nodes use a shared wireless channel. To overcome the problem of hidden nodes in wireless networks, IEEE 802.11DCF completes the access

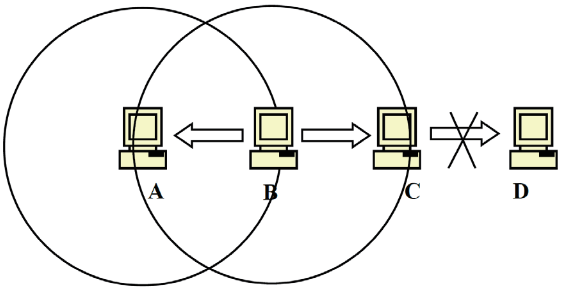

Fig. 2. (Color online) Exposed terminal problem.

process of distributed DATA services through the four-handshake mechanism of RTS-TS-DATA-ACK. Each node that needs to send data determines whether the channel is idle before sending data. If the channel is detected to be idle for a continuous distributed inter-frame space (DIFS) interval, the source and destination nodes first exchange RTS and CTS control frames. The source node sends a DATA frame and the destination node sends an ACK frame to the source node after correctly receiving the DATA frame. After receiving the ACK frame, the source node can confirm that the destination node has correctly received the data, thus completing a transmission, as shown in Fig. 3(a). If the source node detects that the channel is busy, it delays transmission until the channel is idle again. Then, the source node randomly selects a backoff counter within the contention window (CW) range [0, $CW - 1$] with equal probability. When the channel is idle, the regression counter decays one by one after each time slot interval, but stops decaying when the channel is busy. Only when the value of the regression counter decays to zero can the node send, as shown in Fig. 3(b). Because the counter value is randomly selected, the probability of different nodes selecting the same counter value is small, which can reduce the conflicts caused by sending between nodes in the same time slot, but cannot completely avoid the occurrence of conflicts. If the node conflicts with other nodes or fails to send, the node will start the binary backoff algorithm. The initial value of CW is the minimum competition window value CW_{min}. Every time there is a conflict, the value of the competition window will be doubled until the competition window reaches the maximum CW_{max}, and then the maximum competition window value will be maintained until the successful transmission. After each successful send, the competition window is reduced to a minimum.

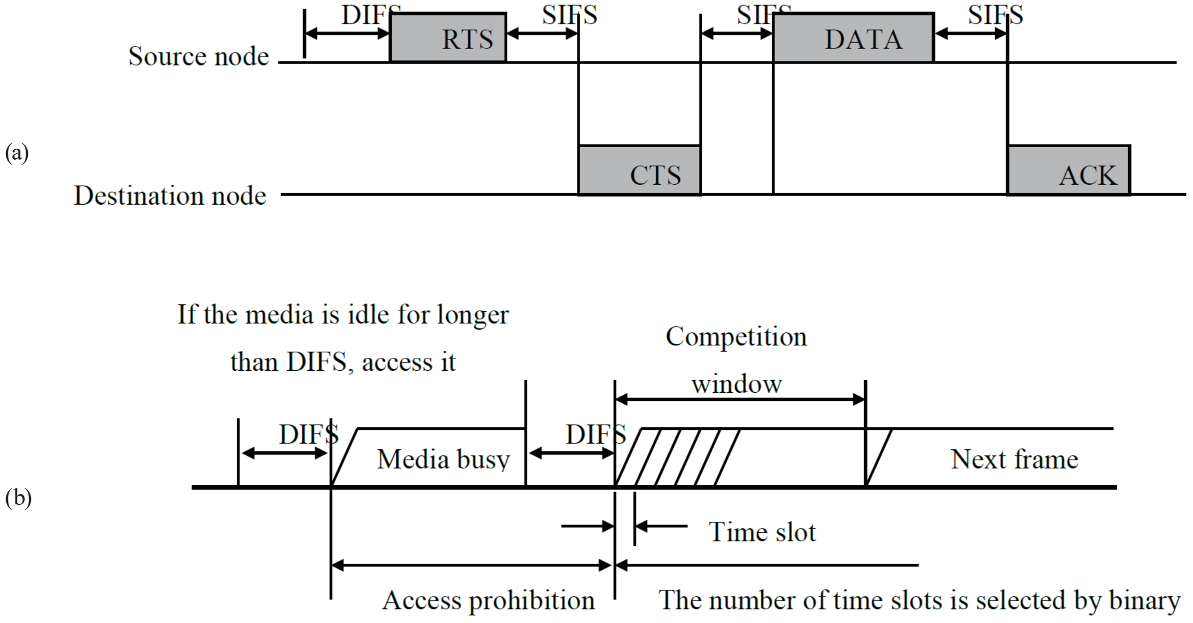

Fig. 3. Working procedure of IEEE 802.11DCF.

4.1 System analysis model

Assuming that the wireless nodes are randomly distributed in the *A* plane region and the positions of the nodes follow the two-dimensional Poisson point distribution with density of λ, the probability of *i* nodes in the region with area *A* can be expressed as

$$p(i,A)=\frac{(\lambda A)^i}{i!}e^{-\lambda A}. \tag{2}$$

All nodes do not carry out transmission power control, and the transmitting and receiving distance is *R*. If the distance between two nodes is less than or equal to *R*, they are neighboring nodes. The average number of neighboring nodes of a node is denoted. Note that the length of a $N = \lambda\pi R^2$ slot is σ. We ignore the data transmission errors attributable to error codes caused by channel noise and interference, and consider that the cause of packet transmission errors is the conflict caused by multiple nodes transmitting data at the same time. We assume that all nodes always have data to send and the network is saturated.

4.2 Sending probability of the node

Let $b(t)$ represent the value of the retreat counter of a node in the *t* time slot and $s(t)$ represent the retreat stage of the node in the *t* time slot. In this way, the working process of each node can be represented by a 2D Markov chain with state space $\{s(t), b(t)\}$, as shown in Fig. 4.[3] In the figure, *m* is determined by $CW_{max} = 2mCW_{min}$. When a node sends a packet and the number of collisions exceeds *m*, the competition window will remain at CW_{max} and will not increase. W_i represents the probability that a node conflicts when sending packets. W_i indicates the size of the competition window in the *i* retreat phase ($W_i = 2iCW_{min}$).

$b_{i,k} = \lim_{t\to\infty} P\{s(t)=i, b(t)=k\}$, $i \in (0,m)$, $k \in (0,W_i-1)$ is defined as the steady-state distribution probability of this Markov chain model, and the following relationship exists:[4]

$$b_{i,0} = p_c^i \cdot b_{0,0},\ 0<i<m, \tag{3}$$

$$b_{m,0} = \frac{p_c^m}{1-p_c}b_{0,0}. \tag{4}$$

According to the regularity of this Markov model, for $k \in [0, W_i - 1]$, each has

$$b_{i,k} = \frac{W_i-k}{W_i}\cdot\begin{cases}(1-p_c)\sum_{j=0}^{m-1}b_{j,0}, & i=0\\ p_c \cdot b_{i-1,0}, & 0<i<m\\ p_c\cdot\left(b_{m-1,0}+b_{m,0}\right). & i=m\end{cases} \tag{5}$$

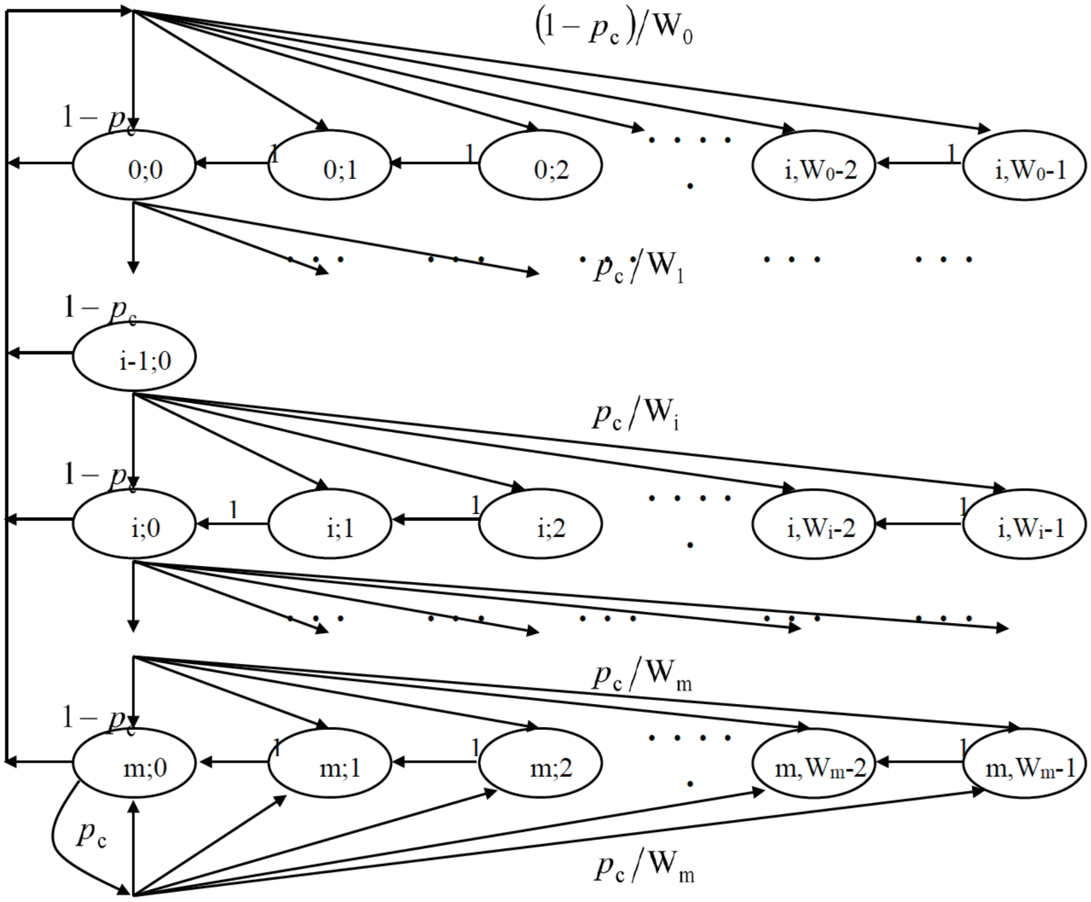

Fig. 4. Markov chain model of wireless node retreat process in IEEE.

With Eq. (4), Eq. (5) can be simplified to

$$b_{i,k} = \frac{W_i - k}{W_i} \cdot b_{i,0},\ 0 \le i \le m,\ 0 \le k \le W_i - 1. \tag{6}$$

Applying the normalization condition to the probability $b_{i,k}$ of a node in a certain state, we can obtain

$$1 = \sum_{i=0}^{m} \sum_{k=0}^{W_i - 1} b_{i,k} = \sum_{i=0}^{m} b_{i,0} \sum_{k=0}^{W_i - 1} \frac{W_i - 1}{W_i} = \sum_{i=0}^{m} b_{i,0} \frac{W_i - 1}{2}. \tag{7}$$

This leads to

$$b_{0,0} = \frac{2(1-2p_c)(1-p_c)}{(1-2p_c)(W_0+1) + p_c W_0 \left(1-(2p_c)^m\right)}. \tag{8}$$

According to IEEE 802.11DCF, when a node enters state $b_{i,0}$, $0 \le i \le m$ will send packets, so the probability of a node sending packets in any time slot is

$$\tau = \sum_{b=0}^{m} b_{i,0} = \frac{b_{0,0}}{1-p_c} = \frac{2(1-2p_c)}{(1-2p_c)(W_0+1)+p_c W_0\left(1-(2p_c)^m\right)}. \tag{9}$$

In Eq. (9), the sending probability of nodes is expressed as a function of the probability p_c that conflicts occur when nodes send packets.

4.3 Calculation of average time slot length and saturation throughput

In the above IEEE 802.11DCF wireless node Markov model, it is assumed that under all circumstances, the retreat counter of the wireless node will decrease by one in each time slot. This means that at the start of a time slot, regardless of whether the channel is busy or idle, the wireless node's retreat counter will be in a retreating state. This statement is inconsistent with the IEEE 802.11 protocol. In accordance with the protocol, the backoff counter should halt its counting when the channel is busy. It remains in this state until the channel reverts to the idle state. At that point, the backoff counter resumes decreasing once again. To take this characteristic into account in the network throughput analysis model, the mean time slot is used instead of the physical time slot. The average slot time $\varDelta$ is defined as

$$\varDelta = \pi_i \delta + \pi_s T_s + \pi_c T_c. \tag{10}$$

Here, π_i, π_s, and π_c are the steady-state probabilities of channels in idle, successful transmission, and conflict states, respectively; δ is the physical slot length; T_s is the duration of successful transmission; T_c is the duration of a conflict. For convenience, the various amounts of time involved are normalized to δ and are equal to 1. For IEEE 802.11DCF, the time T_s when the channel is in the successful transmission state and the time T_c when the channel is in the conflict state are as follows:

$$T_s = RTS + SIFS + \sigma + CTS + SIFS + \sigma + Header + DATA + SIFS + \sigma + ACK + DIFS + \sigma, \tag{11}$$

$$T_c = RTS + DIFS + \sigma\cdot \tag{12}$$

Here, σ is the propagation delay.

To determine the steady-state probabilities π_i, π_s, and π_c of channels in idle, successful transmission, and conflict states, respectively, the method in Ref. 5 is adopted. Consider defining the channel as a circular area with the radius R', in which some wireless nodes are distributed. Nodes in these areas can communicate with each other and have a weak connection with nodes outside the area. A weak connection means that the process of nodes in the area deciding to perform transmission and retreat is almost unaffected by nodes outside the area. Therefore, the state of the channel is determined only by the successful or failed transmission in the area. We set the transmission radius of the wireless node as R. When the area radius R' is $R/2$, the nodes within this area can form a single-hop network. When $R' = 2R$, all the direct neighbors and hidden nodes of the intermediate node will be included.

Now, consider an arbitrarily selected node x in the network; the channel it uses can be described by a three-state Markov chain model. As shown in Fig. 5, the three states are idle, successful transmission, and conflict. It is very difficult to accurately calculate the transition probability of this Markov model, so an approximate method is adopted in the analysis process. The transfer probability of the channel from the idle state to the idle state (P_{II}) is equal to the probability that no node will transmit in the area with a radius of $2R$ centered on the node x in the next physical time slot, and its value is given by

$$P_{II} = \sum_{i=0}^{\infty} (1-\tau)^i \frac{\left(4\lambda\pi R^2\right)^i}{i!} e^{-\left(4\lambda\pi R^2\right)} = e^{-\tau\left(4\lambda\pi R^2\right)}. \tag{13}$$

The transfer probability of the channel from the idle state to the successful transmission state (P_{IS}) is defined as the probability that only one node successfully completes the four-step handshake communication in the area with a radius of $2R$ centered on the node x, while other nodes do not transmit. Its value is given by

$$P_{IS} = \sum_{i=1}^{\infty} i p_s (1-\tau)^{i-1} \frac{\left(4\lambda\pi R^2\right)^i}{i!} e^{-\left(4\lambda\pi R^2\right)} = 4\lambda\pi R^2 p_s e^{-\tau\left(4\lambda\pi R^2\right)}. \tag{14}$$

Here, p_s is the probability of a node achieving a successful four-step handshake communication, which is currently unknown. The channel Markov model shown in Fig. 5 is

$$\begin{aligned} \pi_i &= \pi_i P_{II} + \pi_\mathrm{s} + \pi_\mathrm{c} \\ &= \pi_i P_{II} + 1 - \pi_i. \end{aligned} \tag{15}$$

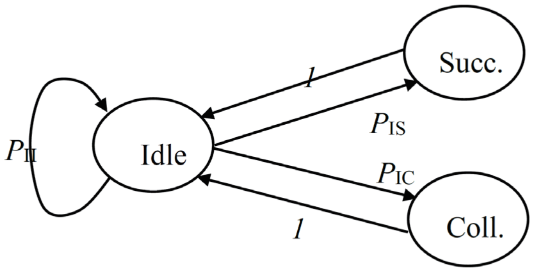

Fig. 5. Markov chain model of wireless channel.

Thus, there is

$$\pi_i = \frac{1}{2 - e^{-\tau\left(4\lambda\pi R^2\right)}}. \tag{16}$$

In addition,

$$\pi_s = \pi_i P_{IS} = 4\pi_i \lambda\pi R^2 p_s e^{-\tau\left(4\lambda\pi R^2\right)}, \tag{17}$$

$$\pi_c = 1 - \pi_i - \pi_s. \tag{18}$$

Thus, the average timeslot *Δ* defined by Eq. (10) can be calculated from Eqs. (11), (12), (16), (17), and (18). However, the equation also contains an unknown quantity, p_s, which is the probability that a node can successfully complete a four-step handshake communication. The calculation formula of p_s is determined according to the state evolution process of the node *x*.

In the case of saturation (there is always data to be sent), the wireless node *x* can only be in one of the three states of retreat, successful transmission, or conflict in any given time slot, so its working process can also be described by a three-state Markov chain model. As shown in Fig. 6, the three states are retreat state B, successful transmission state S, and conflict state C. The steady-state probabilities of the node *x* in the three states are Π_B, Π_S, and Π_C, respectively. Assuming that the node is in the retreat state at the initial moment, after the arrival of the next time slot, the working state of the node has three possible transfer modes: (1) The transfer probability P_{bb} continues to remain in the retreat state and the residence time is the average time slot length *Δ*. (2) P_{bs} enters the successful transmission state with the transfer probability and returns to the retreat state with a probability of 1 after T_s time, preparing for the next transmission. (3) The transition probability P_{bc} leads to entering the conflict state. Once in this state, it remains for T_c time. After that, it returns to the retreat state with a probability of 1, being ready to send data the next time.

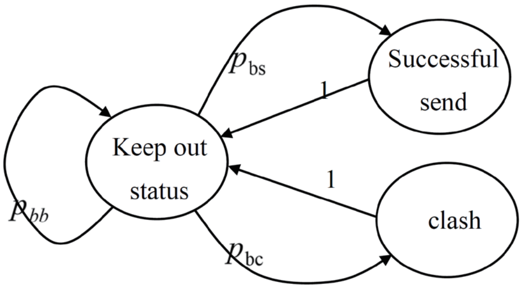

Fig. 6. Markov model of wireless node.

The transition probability P_{bb} of the node x remaining in the retreat state in the next time slot is the probability that the node x does not send, and the surrounding nodes do not send, which can be expressed as

$$P_{bb} = \left(1-\tau\right)e^{-\tau N}. \tag{19}$$

Obtained by the Markov chain model,

$$\Pi_B = \Pi_B \cdot P_{BB} + \Pi_S + \Pi_C. \tag{20}$$

Thus, we have

$$\Pi_B = \frac{1}{2-\left(1-\tau\right)e^{-\tau N}}. \tag{21}$$

Below, we determine the steady-state probability Π_S of the node x in the successful sending state. In a multi-hop wireless network, the successful transmission of the node x depends not only on the state of its neighbors, but also on the neighbors of the target node. As shown in Fig. 7, the source node x sends data to the target node y, and the distance between the two is r. $N(x)$ and $N(y)$ are used to represent the communication areas of the nodes x and y, respectively, which are circles of radius R. Region $B(r) = N(x) \cap N(y)$ and region $C(r) = N(x) - N(y)$. The node in zone C is the hidden node of the node x, and the communication between x and y is affected by all the nodes in zone $N(x) \cup N(y)$.

Whether the packet sent by the wireless node x to the node y will encounter a conflict is not solely determined by whether the neighboring node of the node x transmits packets. It is also related to the status of the receiving node y and its neighboring nodes in region C. On the basis of these factors, when the node x sends packets to the node y at the distance r, the transition probability from the retreat state to the successful sending state can be expressed as[6]

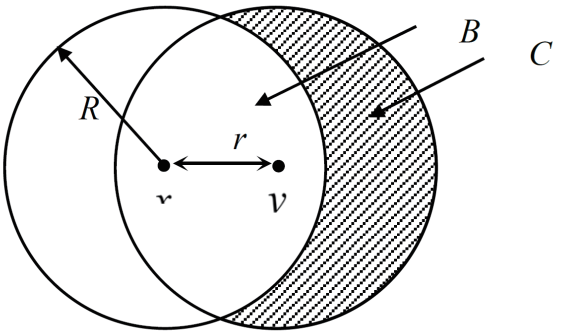

Fig. 7. Communication diagram in multi-hop network of wireless node.

$$\begin{aligned} p_{bs}(r) = {} & \text{Prob}\{\text{Node } x \text{ sends in one time slot}\} \cdot \text{Prob}\{\text{Node } y \text{ does not send data in the same time slot}\} \cdot \\ & \text{Prob}\{\text{Nodes in area } B \text{ do not send data in the same time slot} \mid r\} \cdot \\ & \text{Prob}\{\text{Nodes in the } C \text{ zone do not transmit within } 2RTS{+}1 \text{ time slot interval} \mid r\}. \end{aligned} \tag{22}$$

The reason for the last item in Eq. (22) is that the vulnerable period for the node *y* to correctly receive RTS signals is twice as long as $2RTS + 1$. Further conflicts that may occur after the node *y* correctly receives RTS signals are ignored in the calculation process. Therefore, the nodes in zone *C* cannot transmit within the $2RTS + 1$ slots. Clearly, the first and second items are τ and $1 - \tau$, respectively. The probability that none of the nodes in zone *C* sends in a time slot is given by

$$\text{Prob}\{\text{Nodes in area } B \text{ do not send data in the same time slot} \mid r\} = \sum_{i=0}^{\infty}(1-\tau)^i \cdot \frac{(\lambda B(r))^i}{i!} e^{-\lambda B(r)} = e^{-\tau N}. \tag{23}$$

Therefore, the fourth item in Eq. (22) is

$$\text{Prob}\{\text{Nodes in area } C \text{ do not send packets within } 2RST{+}1 \text{ time slot interval}\} = e^{-\tau\lambda C(r)(2RTS+1)}. \tag{24}$$

$C(r)$ in Eq. (25) represents the area of zone *C*, which can be obtained from Ref. 7 as

$$C(r) = \pi R^2 - 2R^2 q\left(\frac{r}{2R}\right). \tag{25}$$

One of these is

$$q(t) = \arccos(t) - t\sqrt{1-t^2} \cdot \tag{26}$$

Assuming that the source node selects a node among its neighbors as the destination node in an equal probability manner, the probability density function of the distance *r* between the source node and the destination node is set as $R = 1$, and *R* is normalized as[8]

$$f(r) = 2r, 0 < r < 1. \tag{27}$$

Now, p_{bs} can be expressed as

$$p_{bs} = \int_0^1 2r \cdot p_{bs}(r)\mathrm{d}r = 2\tau(1-\tau)e^{-\tau N}\int_0^1 r \cdot e^{-\tau N(1-2q(r/2)/\pi)(2RTS+1)}\mathrm{d}r. \tag{28}$$

The conflict transition probability obtained from Eqs. (19) and (28) is

$$p_{bc} = 1 - p_{bb} - p_{bs}. \tag{29}$$

Therefore, the steady-state probability of the node *x* in the successful transmission state (Π_S) is

$$\Pi_S = \Pi_B \cdot P_{bs} = \frac{P_{bs}}{2-(1-\tau)e^{-\tau N}} = p_s. \tag{30}$$

Equation (30) is the unknown p_s in Eq. 14, so if the transmission probability is further determined, the average time slot length Δ can be calculated from Eqs. (10), (16), (17), and (18).

The steady-state probability of the node *x* in conflict state Π_S (which is also the node conflict probability p_c) can be expressed as

$$p_c = \Pi_C = 1 - \Pi_B - \Pi_S. \tag{31}$$

By combining Eqs. (9) and (31), a nonlinear system of equations about the sum can be obtained, and a unique solution can be deduced by numerical calculation.

The saturation throughput of a single node in a multi-hop network can then be calculated. The saturation throughput of a node is defined as the percentage of time in which valid data is successfully sent within a unit time. As shown in Fig. 6, the formula for calculating the saturation throughput of a node is

$$TH = \frac{\Pi_S \cdot DATA}{\Pi_B \cdot \Delta + \Pi_S \cdot T_s + \Pi_C \cdot T_c}. \tag{32}$$

5. Numerical Simulation Result

The simulation parameters of the IEEE802.11DCF protocol are shown in Table 1, and the saturation throughput of nodes in the multi-hop network topology can be calculated using Eq. (32).

Table 1
Simulation parameters of IEEE802.11DCF protocol.

MAC header	272 bits
PHY header	128 bits
RTS	160 bits + PHY header
CTS	112 bits + PHY header
ACK	112 bits + PHY header
Channel bit rate	2 Mbps
Slot time	20 μs
SIFS	10 μs
DIFS	50 μs
m	5

Figure 8 shows the curve of node saturation throughput with packet length when the initial competition window of nodes is 32 and the numbers of neighboring nodes (*N*) are 3, 5, 8, and 12. Overall, the throughput of nodes is low and increases with the packet length. When the number of neighboring nodes increases, the throughput decreases significantly, because when the number of neighboring nodes increases, there will be more nodes to compete for the channel, so the nodes will spend more time to retreat.

Figure 9 shows the curve of node saturation throughput in relation to packet length when the initial node competition window is set to 128 and the numbers of neighboring nodes *N* are 3, 5,

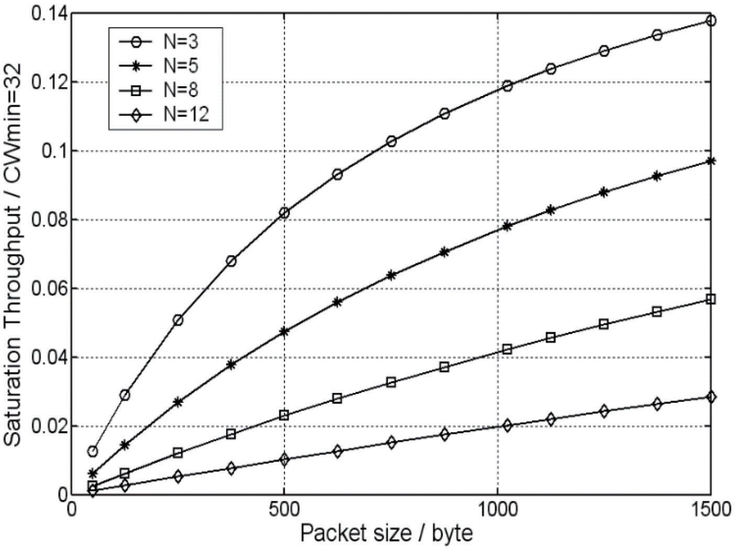

Fig. 8. Node saturation throughput in multi-hop topology.

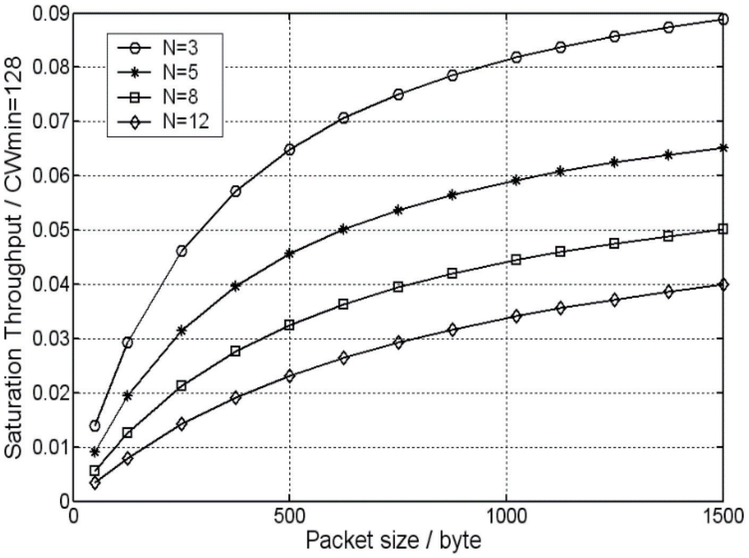

Fig. 9. Node saturation throughput in multi-hop topology.

8, and 12. A comparison of Figs. 9 and 8 reveals that when the number of neighboring nodes is small and a large initial competition window is employed, the saturated throughput diminishes. Conversely, when the number of neighboring nodes is large, the saturated throughput shows a slight increase. When the initial competition window value is large, the node's backoff time will increase correspondingly. This implies that the sending probability of the node will decrease. When the number of neighboring nodes is large, the probability of conflict decreases, thereby increasing the node throughput. However, when the number of neighboring nodes is small, as the sending probability decreases, the channel capacity will be wasted.

6. Conclusions

In this study, we analyzed the performance of IEEE802.11DCF on the basis of the asynchronous competition mechanism in multi-hop wireless networks. It can be seen that in the multi-hop configuration, the probability of node sending conflict is high, resulting in a low network throughput. In addition, the IEEE 802.11 protocol does not provide a network clock synchronization mechanism, because under this protocol, wireless nodes obtain the right to use the channel through competition. Inequality in channel use among nodes is inevitable. As a result, some nodes occupy the channel for an extended period. In contrast, for other nodes, it is difficult to gain control of the channel. This makes the clock synchronization of wireless nodes in the network very difficult. More importantly, IEEE 802.11DCF does not consider the energy-saving problem of nodes, and all wireless nodes must always monitor the channel, resulting in unnecessary energy waste. Corresponding to the MAC protocol based on the competition mechanism, there are also a class of noncompetitive MAC protocols such as TDMA, FDMA, and CDMA. In the TDMA mode, the right to use the channel is divided into a series of time slots; each node has one or several time slots and begins to use the channel to send data after the arrival of its time slot, and in the time slots belonging to other nodes, one can close one's own RF unit to achieve energy saving. The FDMA system divides the wireless channel into several subchannels, and the wireless nodes communicate in the allocated subchannels, while the CDMA system assigns a unique random spread spectrum code to each node, and the receiving node receives the signal according to the spread spectrum code of the sending node, and extracts useful information from the received signal that is interfered by noise and other nodes. For the above noncompetitive MAC protocol, the system assigns the channel usage mode to the wireless node in advance, so that the node can easily handle its own data communication behavior and realize the purpose of energy saving. Because the communication technology based on CDMA is relatively complex, it is not suitable for cheap wireless sensor nodes, so the noncompeting MAC protocols that can be used in actual wireless sensor networks are mainly TDMA and FDMA. FDMA requires receivers to use the same subchannel; otherwise, the normal communication cannot be carried out, which makes the design of the multi-hop network protocol based on FDMA very difficult. The TDMA mode is relatively flexible. In multi-hop networks, it can also effectively coordinate nodes to achieve the utilization of channels. However, the prerequisite for this is that the network must achieve global synchronization. To reduce the impact of synchronization errors, we generally set a protection interval between time slots.

On the basis of the above factors, a MAC protocol based on TDMA and FDMA is designed for bridge wireless detection systems, which can make the whole network run in a synchronous state and can not only meet the requirements of signal synchronous sampling for structural state detection, but also realize the energy-saving operation of wireless sensors. Under the control of the top-level protocol, the bridge load test data can be transmitted reliably, and the data collected by some key sensor nodes can be transmitted in quasi-real time.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 61473329), the Fujian Provincial Natural Science Foundation of China (No. 2021J011235), and the phased research result of the provincial major research project on the education and teaching reform of undergraduate colleges and universities in Fujian Province [project name: Research on Three Innovation Education Projects of Internet of Things Engineering (project no.: fbjg202101018)].

References

1 A. Mohammed, M. Moamin, and R. Ramona: Electronics **11** (2022) 2837. https://doi.org/10.3390/ELECTRONICS11182837
2 W. Ye, J. Heidemann, and D. Estrin: IEEE/ACM Trans. Networking (TON) **12** (2004) 493. https://doi.org/10.1109/TNET.2004.828953
3 Z. Li, T. Pei, and S. Yang: Advanced Materials Research **1227** (2011) 768. https://doi.org/10.4028/www.scientific.net/AMR.216.768
4 W. Elijah, B. Marlan, and M. Fernando: Struct. Control Health Monit. **29** (2022) 10. https://doi.org/10.1002/STC.3013
5 I. Arshad and L. T. Jin: IEEE Internet of Things J. **8** (2021) 14822. https://doi.org/10.1109/JIOT.2021.3072038
6 J. Wu, and X. Qu: J. Intell. Connected Veh. **5** (2022) 260. https://doi.org/10.1108/JICV-06-2022-0023
7 A. Felix, T. Thomas, E. Dario, M. J. Mauricio, and P. Martin: Phys. Rev. Lett. **129** (2022) 120501. https://doi.org/10.1103/PHYSREVLETT.129.120501
8 I. Arshad and L. T. Jin: IEEE Internet of Things J. **8** (2021) 14822. https://doi.org/10.1109/JIOT.2021.3072038
9 X. Liu, J. Yu, Zhang W. Zhang, and Tian Hui: Comput. Electr. Eng. **91** (2021). https://doi.org/10.1016/J.COMPELECENG.2021.107093
10 W. Chen, Q. Guan, H. Yu, F. Ji, and F. Chen: IEEE Internet of Things J. **15** (2021) 12398. https://doi.org/10.1109/JIOT.2021.3063462
11 M. Zareei, A. K. M. Islam, N. Mansoor,S. Baharun, E. M. Mohamed, and S. Sampei: EURASIP J. Wireless Comm. and Networking **1** (2016) 1. https://doi.org/10.1186/s13638-016-0652-y
12 L. Han and L. Hao: IEEE Internet of Things J. **8** (2021) 11249. https://doi.org/10.1109/JIOT.2021.3053290
13 M. Buddhikot, A. Hari, K. Singh, and S. Miller: Mobile Netw. Appl. **10** (2005) 289. https://doi.org/10.1007/s11036-005-6423-3
14 I. Ullah and H. Y. Youn: J. Supercomput. **76** (2020) 1. https://doi.org/10.1007/s11227-020-03236-8
15 O. Takyu and A. Kamio: IEICE Commun. Express **11** (2022) 302. https://doi.org/10.1587/COMEX.2022XBL0008
16 B. Han, M. Dong, R. Zhang, L. Ling, M. Fan, P. Liu, and B. Wang: Mol. Catal. **515** (2021) 111926. https://doi.org/10.1016/J.MCAT.2021.111926

About the Authors

Zhengsong Ni received his bachelor's degree from Fuzhou University in 1995, his master's degree from Beijing Information Science and Technology University in 2007, and his doctorate degree from Beijing University of Posts and Telecommunications in 2010. From 2010 to 2012, he was a lecturer at Tianjin Polytechnic University, from 2012 to 2014, he was an assistant professor at Tsinghua University, and since 2014, he has been an associate professor at Fujian Normal University of Technology. His research interests include MEMS, big data, and sensors. (460532802@qq.com)

Shuri Cai received his bachelor's degree from Fujian Normal University in 1997 and his master's and doctoral degrees from Beijing University of Posts and Telecommunications in China in 2004 and 2008, respectively. Since 2007, he has worked as an associate researcher at the Institute of Highway Science under the Ministry of Transport. His research interests include MEMS, big data, and sensors. (710207335@qq.com)

Cairong Ni received her bachelor's degree from Sunshine College in 2022. She has been working as a teaching assistant at Fujian Normal University of Technology since 2022. Her research interests include MEMS, big data, and sensors. (3247146792@qq.com)