Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Performance Analysis of Multi-hop Token Relay Strategy in HF Networks

Mohammad Hossein Madani (madani@mut.ac.ir)
Malek-Ashtar University of Technology https://orcid.org/0000-0002-6737-2066
Pooriya Gholipoor
Malek-Ashtar University of Technology
Sajad Poursajadi
Malek-Ashtar University of Technology

Research Article

Keywords: Media Access Control, High Frequency, Token ring protocol, Multi-hop relay, NS3

Posted Date: March 10th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1244046/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Version of Record: A version of this preprint was published at Telecommunication Systems on June 12th, 2023. See the published version at https://doi.org/10.1007/s11235-023-01019-z.

Abstract

High Frequency (HF) tactical link is one of the most widely used types of long-range telecommunication. Media Access Control (MAC) protocols play a pivotal role in HF network management by affecting data transmission. STANAG 5066 in its 3rd edition recommends HF Wireless Token Ring Protocol (HFWTRP) as a MAC protocol with some features dedicated to HF networks. To deal with temporary link interruption as a natural specification in the HF channel, Relay strategy in HFWTRP is proposed to provide better throughput under this situation. Even though one-hop relay is considered in STANAG, multi-hop relay can retain throughput in more link outages when there are mobile nodes or variable environment like weather changes. Based on the algorithm of the relay in STANAG, a loop in multi-hop relay should be found which can be a detrimental effect on the network and can be solved by adding some bits as relay controller in management frame of HFWTRP. This paper presents a proper evaluation on effect of one-hope relay in the Quality of Service (QoS) of HF networks. Additionally, two-hope relay as a multi-hop relay in the HFWTRP based on the proposed solution for loop creation are simulated and analysed too. The results obtained by NS3 simulator show that two-hop relay in long duration of link outages like 90% probability of disconnection gives 700 bps more throughput with acceptable mean delay vs one-hop relay.

1 Introduction

For sharing a common channel between multiple nodes, a MAC protocol is needed to manage access of the nodes to the channel [1]-[4]. There are two approaches to design a MAC protocol: contention-base and contention-free [2]. In the contention-free, in contrast to the contention-base, the nodes do not compete to access the channel, and nodes based on an algorithm for a limited period can reach it freely. In Token Ring protocol that is a contention-free MAC protocol, there is a management frame called Token, which rotates between the nodes. There are some types of token frames which one of them is Right to Transmit (RTT) [5]. Each node that takes RTT Token from its predecessor node in the channel can send data instantly and other nodes must be quiet. If a node lacks any data to send, it generates an update token and sends it to its successor via the channel immediately. Based on this algorithm, Wireless Token Ring Protocol (WTRP) is used in broadband ad-hoc wireless networks. HF radio communications in 3-30 MHZ band is being used by the help of ionospheric bending of the waves [6], [7]. In HF ad-hoc networks, because of its special characteristics like a narrow band, suffering from severe fading and loss, temporary link outage and so on, the MAC protocol must be taken into account seriously [2],[8]. The STANAG 5066 in its 3rd edition recommends a modified version of WTRP as HFWTRP with some unique features for HF networks. Relay Token is a kind of HFWTRP management frame. If a node cannot reach its successor to deliver RTT Token directly, it sends a relay token to another node that has access to unreachable node, via which RTT can be delivered to unreachable nodes [9],[10]. In this situation with a limitation on hop count like two-hop, if the unreachable node was still irresponsible, it could be assumed to be out of network. Thus, relay token can deal with these temporary link outages. Nonetheless, a loop can be established between candidate nodes to accomplish the relay strategy for more than one-hop. This event has not been seen in STANAG and it can have a detrimental effect on the operation of the network in real-world and tactical situations that must be taken into account. Many studies have been carried out on WTRP and HFWTRP, some of which describe algorithm of WTRP. Mustafa Ergen et al. [5] review the structure of the WTRP. A comparison between the token ring algorithm and Distributed Coordination Function (DCF) based on IEEE 802.11 was proposed [5], in which the token ring is simulated with Request to Send/Clear to Send (RTS/CTS) overloads. A comprehensive comparison between wireless MAC protocols based on HF turnaround time is performed by Eric E. Johnson et al. [11],[12]. They confirm that the token ring protocol has a good and reliable response in heavy and light traffic. There is some other research on the token relay and HFWTRP fundamentals. Token relay for military HF radio networks was found in [13] too. The authors also discussed the token relay on HFWTRP to optimize the joining of a node to a ring [14]. An Improved WTRP (IWTRP) for Wireless Metropolitan Area Networks (WMAN) is proposed in [15]. IWTRP is based on the concept of spatial reuse to enhance the throughput of a WMAN which can use multiple tokens in a multi-hop network. The results showed that IWTRP outperforms WTRP in terms of throughput in dense networks and saturation areas [15]. A multi-channel token ring MAC protocol for inter-vehicle communication is proposed in [16]. Based on organizing vehicles into multiple rings on different service channels, with token-based access, the network throughput is improved for non-safety multimedia applications like their safety [16]. The results illustrated that this usage of token passing through multiple channels can guarantee QoS requirements in vehicular networks. In [17], it is explained that HFWTRP does not consider the air node. High-Frequency Token Protocol with Reserve (HFTP-R) is described for the MAC layer of the HF Ground-to-Air IP network. It lets air nodes like Airborne Warning and Control Systems (AWACS) join in the network during the initialization period and can send data to reserve channel and receive tokens. According to the results, the HFTP-R is faster during the initialization period and is better than TDMA when traffic is small while being more robust [17]. Token-based Adaptive MAC (TA-MAC) scheme is proposed for two-hop Internet of Things (IoT) in Mobile ad-hoc Networks (MANET) [18]. In this scheme, nodes are partitioned into different one-hop groups and a Time Division Multiple Access (TDMA) super frame is proposed to allocate time slots to different nodes to overcome hidden terminal problems. By adapting the MAC parameters to varying network conditions, it can achieve minimal average delay for end-to-end transmissions and high aggregate throughput [18]. An improved TA-MAC is proposed in [19]. The scheme divides the super frame into four sub-frames and there are five tokens circulated between the nodes. When a node holds a token, it is assigned a slot for transmitting a packet at first and then the token to another node. The results showed that this scheme can maintain higher throughput and lower end-to-end delay. However, it can be suitable for two-hop and can be affected by the hidden terminal for more hops [19].

In this paper, we will focus on relay token performance after ring creation when a node cannot reach its successor directly. Therefore, the relay token can deliver the RTT token to the unreachable node. Especially, a two-hop relay, which is not mentioned in STANAG 5066, is proposed in this paper as an additional ability to preserve throughput as much as possible. We generally pay attention to the third edition of STANAG 5066 for model description and simulations and analyzing one- and two-hop relay on NS3 simulator. The remainder of the paper is organized as follows. A review of HFWTRP is described in Section 2. In Section 3, the relay strategy is discussed based on STANAG 5066 and the model for one and two-hop relay operation is presented. The suggested method for preventing loop creation is proposed as well. The performed analysis on simulation results in NS-3 simulator and conclusions are presented in Sections 4 and 5, respectively.

2 Token Passing Structure For Hf Networks

This section reviews the WTRP and HFWTRP fundamentals.

2.1 WTRP

As mentioned earlier, WTRP has some types of MAC frames to control channel access. Fig. 1 shows the general frame of WTRP as discussed in [5].

In Fig. 1, Frame Control (FC) determines the token type. One of the MAC token types is RTT, possessing which means that a node has permission to send data. Ring Address (RA) contains the ring owner node which creates the ring at first. DA and SA define the destination and the source address, respectively. The number of nodes (NoN) denotes the total Number of Nodes in the ring. Generation Sequence Number (GSN) and Sequence Number (SN) are sequential numbers that are increased by the ring owner and each node in token passing, respectively [5]. ACK token is another useful MAC frame in the token ring algorithm. ACK is a positive response sent from a node that takes RTT to the predecessor node to show that RTT is received correctly. Consider Fig. 2, which contains four nodes in a network.

Node D receives a packet from an upper layer and generates a data frame. In Fig. 2 (a), node D is not allowed to send its data frame because it does not have RTT. Consequently, it reserves its frame and waits until taking RTT. In Fig. 2 (b), it holds RTT and sends its data frame to the destination via the channel immediately. After that, it must deliver the RTT to its successor. The network can be configured in any voluntary topology and the nodes are not required to form as a ring structure and being in common radio coverage suffices. WTRP does not try to keep the nodes in network if they do not be active for a while. For example, if node D in Fig. 3 (a) misses its link for a short time based on mobility or channel destruction and cannot be responsible to its predecessor with ACK token, node C as in Fig. 3 (b) discards node D from the ring after a while.

In this situation, node C sends RTT to node A. Fig. 4 shows this concept.

The temporary link outage which is a natural specification in HF channel can reduce QoS (especially throughput) of the network. In Fig. 4, if node D contains data to send and it is not allowed, it must take a considerable delay to return to the ring. Therefore, a data frame that contains a packet can be out of date and it may drop the packet. Hence, SATANG 5066 proposes HFWTRP as a modified version of WTRP in the HF channel.

2.2 HFWTRP

As the Token Ring algorithm was discussed in the previous subsection, the general fundamentals of the HFWTRP are the same as WTRP. Fig. 5 (a) demonstrates the MAC header of a general frame of the HFWTRP [8]. Fig. 5 (b) shows the MAC payload of a general frame of the HFWTRP [9].

As mentioned, we have a header and a payload in HFWTRP [9]. In Fig. 5 (a), the Next Successor (NS) section is added to help relay operation and it defines the address of an unreachable node. Transmit Order List (TOL) and Distance Matrix (DM) are two informative data sets that can help the management of the ring. TOL is a vector in which each node with RTT places its address orderly. Therefore, this vector can help determine the length of the ring and the order of the nodes. As shown in Fig. 6 (a), TOL is presented by $\{S_A > S_B > S_C > S_D\}$, where S_A stands for Station (node) A. Based on Fig. 6 (a) node C sends RTT to node D and it is not responsible for an ACK. Therefore, node C decides to request another node to deliver RTT to the unreachable node, as demonstrated in Fig. 6 (b). In this case, there are three operational nodes:

- Relay Requester, shown by node C.
- Target or unreachable node, shown by node D
- Relayer node, which needs to be defined.

DM is useful in relay strategy in an HF network. This matrix shows the distance between each pair of nodes in hop count. The Relay Requester node computes this matrix and selects a node based on it with one-hop distance to the target node. As a result, a token called REL (Relay) token is sent to the Relayer node.

In Fig. 7 (a), node C chooses node A as the Relayer and sends the REL token to its it. In Fig. 7 (b), node A receives REL token, generates an RTT token and replaces the DA part of new RTT with the NS field on REL token. Therefore, node A sends RTT to node D. The following section focuses on the relay strategy and explains its structure. For more than one-hop, a loop in relay operation may be established based on the algorithm of the relay in STANAG 5066, which must be taken into account in real and tactical scenarios for HF tactical networks.

The next section describes the proposed scheme to deal with this problem. Additionally, a two-hop relay will be investigated based on the proposed method in an HF network.

3 Relay Strategy

As reviewed in Section 2, a relay as a kind of HFWTRP tokens is required to address temporary link outages. DM is an important factor in relay strategy. Behind DM, an Adjacency Matrix (AM) needs to be formed at first [9]. AM is an N × N matrix for N nodes in network. Each element of AM defines the connectivity between pair of nodes in the algorithm:

AM= [$a_{i,j}$=1 if a link exists between node i and node j, $a_{i,j}$= 0 otherwise]

Moreover, DM elements are:

DM= [$dist_{i,j}$= the minimum distance in hops from node i to node j]

An AM should be established and updated based on the received frames. STANAG emphasizes that node j may put $a_{i,j}$ and $a_{j,i}$=1 if an ACK Data link Protocol Data Unit (DPDU) is received from node i. This proves that an ACK connotes that the link is bidirectional. Moreover, node j should be set $a_{i,j}$=1 whenever a DPDU is received from node i. As a result each node can set each element on its row whenever it hears ACK after sending a DPDU to them and can set the related elements in other rows when it hears a DPDU from them. For other elements, we need to sniff the receiving frames on the modem to detect link availability between other nodes. Based on the topology of Fig. 7, the AM can be formed as (1):

$$AM = \begin{bmatrix} a_{AA} & a_{AB} & a_{AC} & a_{AD} \\ a_{BA} & a_{BB} & a_{BC} & a_{BD} \\ a_{CA} & a_{CB} & a_{CC} & a_{CD} \\ a_{DA} & a_{DB} & a_{DC} & a_{DD} \end{bmatrix} \quad (1)$$

The main diagonal is set to 1 because each node is connected to itself. Assume that we want to create AM for node A. In this case,$\mathrm{a_{AA}}$,$\mathrm{a_{BB}}$,$\mathrm{a_{CC}}$, and $\mathrm{a_{DD}}$will be 1. If node A sends a DPDU to node B and it responds to node A with an ACK frame, then $a_{AB}$and $a_{BA}$are set to 1. This concept is identical for a_{AC} anda_{AD}. If node A hears a DPDU from node B, then a_{BA} is set to 1. This concept is the same for a_{CA} anda_{DA}. We can sniff our channel to find any DPDUs from other nodes to set other elements asa_{BC}, a_{CB}, a_{BD},a_{DB} ,a_{CD} anda_{DC}. Since there might be no data frame for a while elements of AM will not be updated completely. Thus, both data and MAC token frames are used to update AM elements. This point is so important in updating the AM whenever a node is not responsible for the RTT frame and its connectivity must set to 0. As a result, some time is required to sniff and configure AM in each node. Based on Fig. 6 with a complete link between the nodes A, B, and C and link outage between the nodes C and D, we have AM as (2):

$$AM_C = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \quad (2)$$

If node B can hear from node D but node D cannot send anything to it, the AM in node C can be as (3).

$$AM_C = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \quad (3)$$

STANAG does not recommend an algorithm to compute DM from AM. However, there are some algorithms including DIJKSTRA, Bellman ford, A search, Floyd-Warshall. This paper incorporates DIJKSTRA as an algorithm to find the shortest path between the nodes in a graph as a ring. DIJKSTRA is dedicated to positive costs on each connection between the nodes and we replace them by 1 or 0 based on their connectivity, respectively. Therefore, a function is established based on (4) to compute that its input argument is AM and selected node to compute shortest path to others and its output is DM related row.

$dist[N] = DIJKSTRA(\text{int } AM[N \times N])$ (4)

Algorithm 1 demonstrates the DIJKSTRA function. The AM and a number related to each node are first applied and by setting all connections infinity, the shortest path is calculated as the desired output based on graph theory. Each node takes its DM and puts its row in DM payload as Fig. 5 (b). We use one-hop relay as Fig. 7to cope with link outage. Node C chooses node A as the Relayer as shown in Fig. 8 (a).

Algorithm 1: DIJKSTRA algorithm to find the shortest path.
Input: Adjacency Matrix (int AM[N][N]), Source node (int s) Output: Related Row of Distance Matrix (int DM[N])
1. For each vertex V in Adjacency Matrix:
2. dist[V]:=infinity
3. previous[V]:=undefined
4. dist[S]:=0
5. While Q is not empty:
6. u:=node in Q with smallest path[]
7. remove u from Q
8. For each neighbor V as u:
9. alt:=dist[u] + dist_between(u,V)
10. if alt<dist[V]
11. dist[v]:=alt
12. previous[V]:=u
13. Return previous[]

Based on Algorithm 1, the DM payload based on Fig. 7 can be as (5)

$$DM_C = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 0 & 2 \\ 1 & 1 & 2 & 0 \end{bmatrix} \quad (5)$$

Because each node has “0” step distance to itself, so the main diagonal of DM is set to "0" [9]. Based on this algorithm node C must choose a node which has minimum distance to node D from the last column of matrix (4) [9]. So node A is selected to be Relayer. The one-hop relay flowchart as used in this paper is shown in Fig. 8 (b). Node A employs this algorithm to send RTT to node D that is temporarily unreachable. Now consider this situation, where the link between the Relayer and the target node is corrupted as well. In this situation, we must drop out that target from the ring. However, besides the one-hop relay, the effect of two-hop relay on QoS of the network is also evaluated in this paper. In the two-hop relay, the Relayer node has an action as given in Fig. 8 (c) and computes another Relayer that has one-hop distance from that target node.
In Fig. 9 (a) node A sends RTT token to node B and as can be seen in Fig. 9 (b), node B is not responsible. Therefore, node A in Fig.10 (a) selects node D as the Relayer. Node D sends RTT token to node B but it is not responsible yet. Fig. 10 (a)-(c) show these concepts, respectively.

In this situation, based on Fig. 10 (c), node D decides to try another hop to reach node B. Therefore, it selects node C as the secondary Relayer and sends RTT token to node B. Fig. 11 (a) and (b) show these two operations, respectively. This action can increase the delay in the network, but the data frame can be delivered to an unreachable node as much as possible. Hence, throughput can be preserved in HF unreliable channel. This is evaluated by simulations in this study.

3.1 Prevention of Loop Creation

STANAG 5066 in its 3rd edition proposed one-hop relay to assist a node to reach its unreachable node. Accordingly, that unreachable node should be deleted from the ring after the operation of the one-hop relay [9]. This algorithm can be employed for more than one-hop [9]. However, it is assumed that, based on long-range transmission, the nodes in an HF network can reach to each other in one-hop. Nonetheless, channel interruptions must be considered in the HF link which can be a temporary event for some time. Consequently, to preserve the throughput and reach an unreachable node, two-hop or multi-hop relay should be used with a bound as a limitation to control relay operation in an attempt to avoid selecting the Relayer as much as possible. Hence, we should see a loop to select a Relayer one after another when an unreachable node is irresponsible. This event can be a challenge for delay in network and also is a pretext for bringing out the nodes from ring. Especially, this point is a challenge for a real-time message transmission request. When a real-time message is not delivered in its suitable time, it will be worthless. This problem is an operational challenge experienced in STANAG. This critical point was observed in our primary simulations and this problem must be solved in the real-world implementation of HF networks. In general header of DPDU of HFWTRP, three unused bits can be found based on the 3rd edition of STANAG 5066 (Annex L) [9]. To control relay performance and avoid creation of a loop in the network for selecting

Relayer node after second hop which is our selection and it can be investigated to more hops too, these unused bits are adopted in this study as an algorithm like Time to Live (TTL) in IP header structure. As a result, at first, we set two first bits in terms of maximum hops like$b_1b_0 = 10$ in binary representation (2 in decimal). Based on the proposed method, the relay requester decreases one bit from this field before sending REL token to the first Relayer. When the first Relayer takes the REL token and finds $b_1b_0 = 01$ in its header, it knows that it can use the second hop in relay strategy if it is required. Therefore, it must try to deliver RTT to unreachable node firstly. If it is unsuccessful, it can try another hop after setting$b_1b_0 = 00$. So, the second Relayer knows that its action is the last hop and if the unreachable node is irresponsible, it drops it from TOL and continues normal operation of the ring. This scheme can control the multi-hop relay strategy and avoid loop creation in Relayer selection by the nodes. By default, the limitation on maximum hops can be 3 in decimal based on two bits of b_1b_0 or 7 in decimal based on $b_2b_1b_0$. However, more hops are supported by more number of nodes and this selection in an HF network is not suitable. Because by increasing the number of nodes in a network, performance will be decreased [9]. Hence two-hop is a reasonable choice in a tactical and real implementation of an HF network.

4 Simulation Results

In this section we have a comparison between the algorithms of WTRP and HFWTRP to show the difference in QoS when there is relay or not. We use NS-3, which is a Linux based open-source discrete event simulator [20]. A low rate CSMA/CA module has been overwritten completely and replaced by a token ring algorithm as a MAC protocol. A low rate physical layer with 20 kbps and LOG distance normal is used as propagation loss model and the range is scalable. Before defining the scenarios and analyzing the simulation results, it is better to introduce evaluation criteria based on NS-3 recommendations as follows [20]:

$Throughput = \frac{8 \times Total\ \ Packets \times Packet\ \ Size}{Simulation\ \ Time}$ (6)

$Mean\ \ Delay = \frac{Sum\ \ of\ \ Delays}{Number\ \ of\ \ Flows}$ (7)

$PLR = q = \frac{LostPackets}{RxPackets + LostPackets}$ (8)

$PDR = 1 - PLR \triangleq 1 - q$ (9)

There is a common channel for all nodes in simulation scenarios. Therefore, moving away for the nodes is considered as link breaking with a uniform probability function in simulation time, which is Probability of Disconnection (P.O.D). The queue in the data link layer in NS-3 is not limited and is assumed as good hardware with small packet sizes. Accordingly, the damaging effects of the channel and physical error corrections such as minimum SNR can drop or hurt the data packets if the token ring algorithm is executed correctly. However, for harder situations, we assume congestion in data transmission and also a deliberate drop is used after eight efforts by a Logical Link Control (LLC) layer to check whether there is RTT or not. If this condition holds, that queued packet can be dropped. Hence, this point of view is helpful in the simulations as it is more similar to real-world implementations. We used Random Tree Walk mobility model in our simulation which is one of the random mobility models in NS-3.

4.1 One-Hop vs No Relay Evaluation

At first, the relay existence is investigated. Assume the HF network as shown in Fig. 7 (a) and (b) with the following scenario:

- Number of nodes: 4
- Structure of packets: 10 packets with size of 250 bytes
- Transmission strategy: each 1^{sec} all nodes want to send data and we have congestion
- Number of iterations: 5

Figure 12 (a) depicts the mean delay vs POD of the network between HFWTRP without using relay like the algorithm of WTRP and HFWTRP with one-hop relay based STANAG 5066. As can be seen, HFWTRP based on its relay helps node D (Fig. 7) to send its packets, and the delay on the queue is not so incredible. However, in HFWTRP without Relay, when deliberately drop is not used, all packets are preserved on the queue and when node D returns to a stable link and rejoins the network it takes the channel and sends all its queued packets. Therefore, the mean delay is very high. If deliberately drop is used as what we have done in this paper, the packets are dropped even more when POD is increased. Because NS-3 does not trace dropped packets, the mean delay must be smaller than the previous situation. However, the throughput for HFWTRP in this situation is not desirable. Figure 12 (b) shows this concept. HFWTRP with deliberate drop and no Relay failed to preserve the packets and dropped them. Therefore, based on (6), the throughput must be decreased, unfortunately. As one can observe, HFWTRP with Relay can deliver RTT to an unreachable node and the throughput can be preserved as much as possible. When a node is 100% disconnected, we have three nodes practically. Therefore, Figure 12 (a) and (b) show a normal behavior at the lower side of the graphs for 100% POD for HFWTRP with no Relay parts. With increased POD and link outage, if HFWTRP without relay is being used, we should expect to see more packets which have been dropped. Fortunately, in HFWTRP, the relay can be helpful to save packets. Figure 12 (c) and (d) show Packet Loss and Delivery ratios, respectively.

4.2 Performance of a Two-Hop Relay

As mentioned in Section 3, two-hop relay as an additional feature in limited token passing time in the ring can help preserve the throughput in network as much as possible. The algorithm based on in Fig. 8 (c) and a network topology as given Fig. 11 is used in the following network structure:

- Number of nodes: 5 (as Fig. 11)
- Structure of packets: 50 packets with size of 100 bytes
- Transmission strategy: each 1^{sec} all nodes want to send data and we have congestion
- Number of iterations: 5

The simulation time is divided into two types. At first, until 50% of POD between node B and D, which are target and Relayer respectively, there is not link outage and relay with one-hop can be done. However, respect to mobility of the nodes, after 50% POD, the link between nodes D and B is broken and RTT needs to be delivered to node B by another hop with node C.

Whenever the POD of node B is increasing, a reliable relay strategy is more needed. Fig. 13 (a) provides a mean delay in this scenario, which a deliberate drop is used and some cases face the problem that ACK token cannot be delivered correctly. Thus, a challengeable scenario is defined to create a hard practical situation in HF networks.

As can be seen in Fig. 13 (a), by increasing link outages in the network, a higher delay is observed for the two-hop relay because of additional process and sending relay token in contrast to the case with a one-hop relay. However, the throughput can be preserved as much as possible even better than the case with a one-hop relay. Fig. 13 (b) shows this concept. After 50% POD, better performance is observed with the second hop relay. This concept tells us that RTT token delivery with a two-hop relay can guarantee the throughput as much as possible.

For example with 90% of POD and acceptable delay, two-hop relay gives us about 700 bps more throughput than one-hop. The other pivotal point is the decrease in rejoin process of the unreachable node. This action is common in very low rate operation in HF networks like those with 75 bps data rate. Packet Loss and delivery ratios are shown in Fig. 13 (c) and (d), respectively. As was expected with a two-hop relay, more packets can be delivered and lower loss ratio can be reached.

5 Conclusion

Wide use of HF channel for long-range communication in some applications like military usages or critical times as communication backbone, leads us to take consideration of HF networking. After 50% POD, many packets queued in the target node are lost. However, with a two-hop relay strategy, RTT can be delivered to an unreachable node and the queued packets can be transmitted. Even though mean delay in two-hop is more than one-hop relay, but throughput preserving is much better than one-hop with increasing POD. In this paper after a review of the algorithm of WTRP and HFWTRP, we discussed their reaction to link outages in HF wireless radio networks. As seen, this event can decline the QoS of the network based on WTRP which does not use relay operation. Relay strategy in HF radio networks proposed by HFWTRP in 3rd edition of STANAG 5066 and can deal with temporary link outages. A two-hop relay as a multi-hop relay feature can assist to have a helpful scenario when a one-hop link is not sufficient and a two-hop relay can preserve the throughput as much as possible even with a higher acceptable mean delay in the network. A method for preventing of loop creation was also discussed in this paper and a two-bits hop controller was introduced to limit the Relayer selection The simulation results demonstrated that in more probable link outages, two-hop relay with acceptable delay based on its more operational steps, can deliver more packets to destination and preserve throughput vs one-hop relay. For example with 90% of POD and acceptable delay, two-hop relay gives us about 700 bps more than one-hop in terms of throughput. However, a sufficient number of hops can be adopted for delivering RTT to unreachable nodes; it is better to have a trade-off between our number of hops in relay strategy and acceptable delay which depends on traffic generation like time sensitive messages in the voluntary network and its conditions.

References

1. Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). PRENTICE HALL
2. Johnson, E. E., Koski, E., Furman, W. N., Jorgenson, M., & Nieto, J. (2012). *Third-generation And Wideband HF Radio Communications*. Artech House
3. Kumar, S., Raghavan, V. S., & Deng, J. (2006). Medium Access Control protocols for ad hoc wireless networks: A survey. *Ad hoc networks*, 4(3), 326–358
4. Jurdak, R., Lopes, C. V., & Baldi, P. (2004). A survey, classification and comparative analysis of medium access control protocols for ad hoc networks. *IEEE Communications Surveys & Tutorials*, 6(1), 2–16
5. Ergen, M., Lee, D., Sangupta, R., & Varaiya, P. (2004). WTRP-WirelessToken Ring Protocol. *IEEE Transactions on Vehicular Technology*, 53(6), 1863–1881
6. Umaisaroh, U., Hendrantoro, G., et al. (2019). Capacity of 2 × 2 MIMO HF NVIS Channels With Linearly Polarized Horizontal Antennas. *IEEE Wireless Communications Letters*, 8(4), 1120–1123
7. Witvliet, B. A., & Alsina-Pagès, R. M. (2017). Radio communication via Near Vertical Incidence Skywave propagation: an overview. *Telecommun Syst*. https://doi.org/10.1007/s11235-017-0287-2
8. NSA/1283 (2008). C3/5066. (2088). STANAG 5066 Ed. 2 Profile For Hf Radio Data Communications
9. NS0/0414 (2015). C3B/5066. (2015) STANAG 5066 C3B (EDITION 3)- PROFILE FOR HF RADIO DATA COMMUNICATIONS
10. Kurtulus, T. (2010). Improvement and Development of High-Frequency Wireless Token-Ring Protocol. Master of Science thesis, Middle East Technical University
11. Johnson, E. E., et al. (2003).Impact of Turnaround Time on Wireless MAC Protocols https://doi.org/10.1109/MILCOM.2003.1290132
12. Johnson, E. E., et al. (2004). Performance of the HF token protocol. IEEE Military Communications Conference. https://doi.org/10.1109/MILCOM.2004.1494985
13. Johnson, E. E., et al. (2003). Robust token management for unreliable networks. IEEE Military Communications Conference.https://doi.org/10.1109/MILCOM.2003.1290136
14. Johnson, E. E., et al. (2005). Token relay with optimistic joining. IEEE Military Communications Conference. https://doi.org/10.1109/MILCOM.2005.1605998
15. Cheng, R. G., & Chang, R. T. (2007). Improved wireless token ring protocol (IWTRP) for wireless metropolitan area networks. IEEE Vehicular Technology Conference. https://doi.org/10.1109/VETECS.2007.19

16. Bi, Y., et al. (2009). A Multi-Channel Token Ring Protocol for QoS Provisioning in Inter-Vehicle Communications. *IEEE Transactions on Wireless Communications*. https://doi.org/10.1109/TWC.2009.081651.
17. Xiao, H., Yunjiang, L., et al. (2014). Token-based multiple access technique in High Frequency ground-to-air IP network. 10th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2014). https://doi.org/10.1049/ic.2014.0140
18. Ye, Q., & Zhuang, W. (2017). Token-Based Adaptive MAC for a Two-Hop Internet-of-Things Enabled MANET. *IEEE Internet of Things Journal*, 4(5), 1739–1753
19. Shu, R., & Shen, C. (2020). Improved Token-Ring-Based MAC Scheme for Two-Hop Ad Hoc Network. 12th International Conference on Communication Software and Networks (ICCSN) https://doi.org/10.1109/ICCSN49894.2020.9139079
20. NS-3 documentation. Accessed: November 2020 [Online]. Available: https://www.nsnam.org/documentation/

Figures

FC	RA	DA	SA	NON	GSN	SN
1	6	6	6	2	4	4

Figure 1

The general frame of WTRP [5]

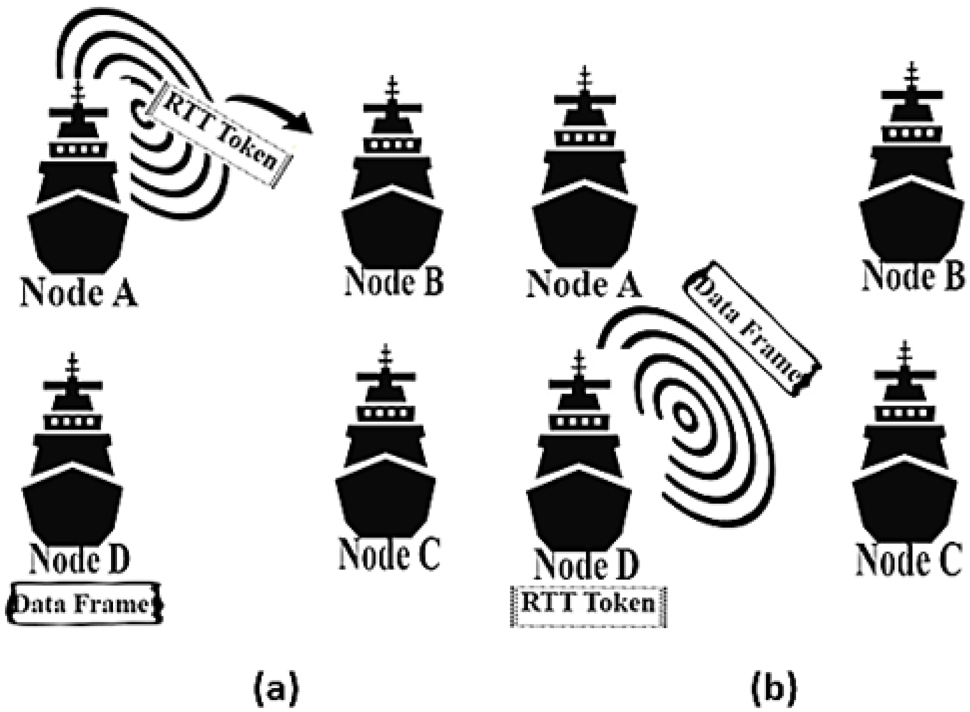

Figure 2

(a) node D is not allowed to send data, (b) node D holds RTT and sends data

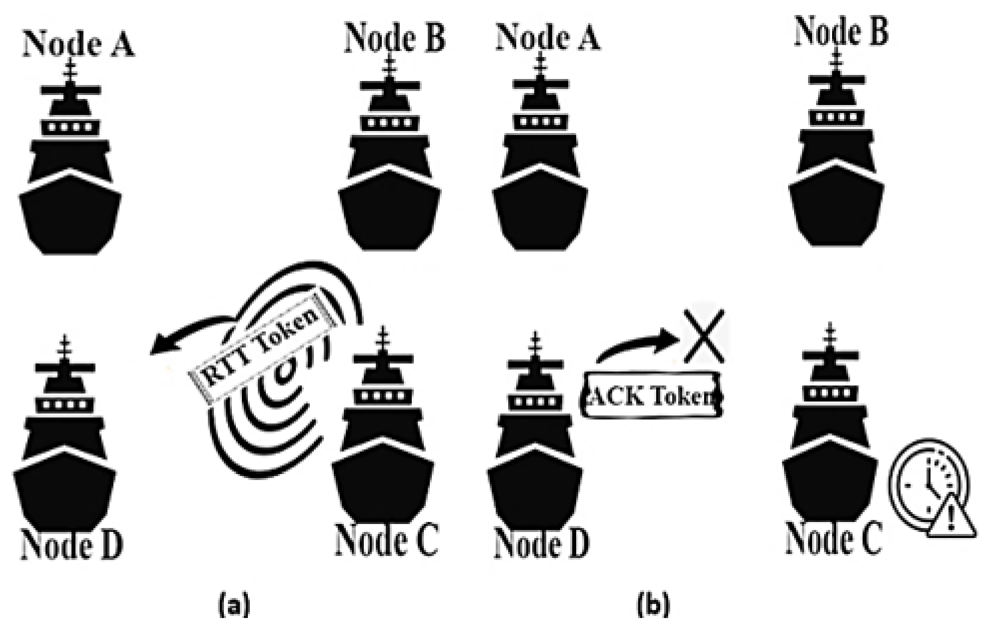

Figure 3

(a) Sending RTT from node C to node D, (b) node D did not send an ACK frame

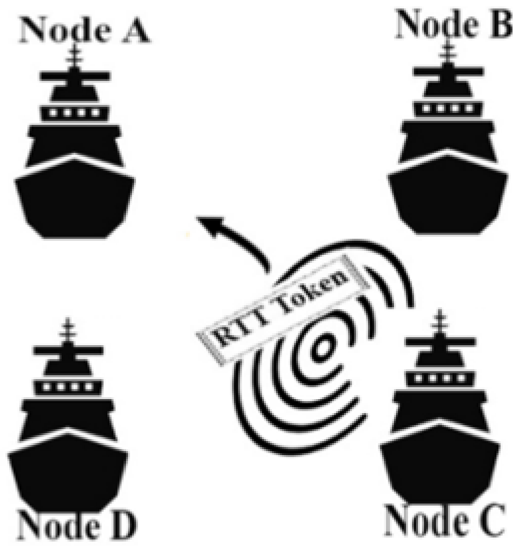

Figure 4

Sending RTT from node C to node A

FC	RO	DA	SA	SN	GSN	NS	NON
1	3.5	3.5	3.5	2	2	3.5	2

(a)

TOL	DM

(b)

Figure 5

(a) General header of HFWTRP, (b) Payload of HFWTRP [9]

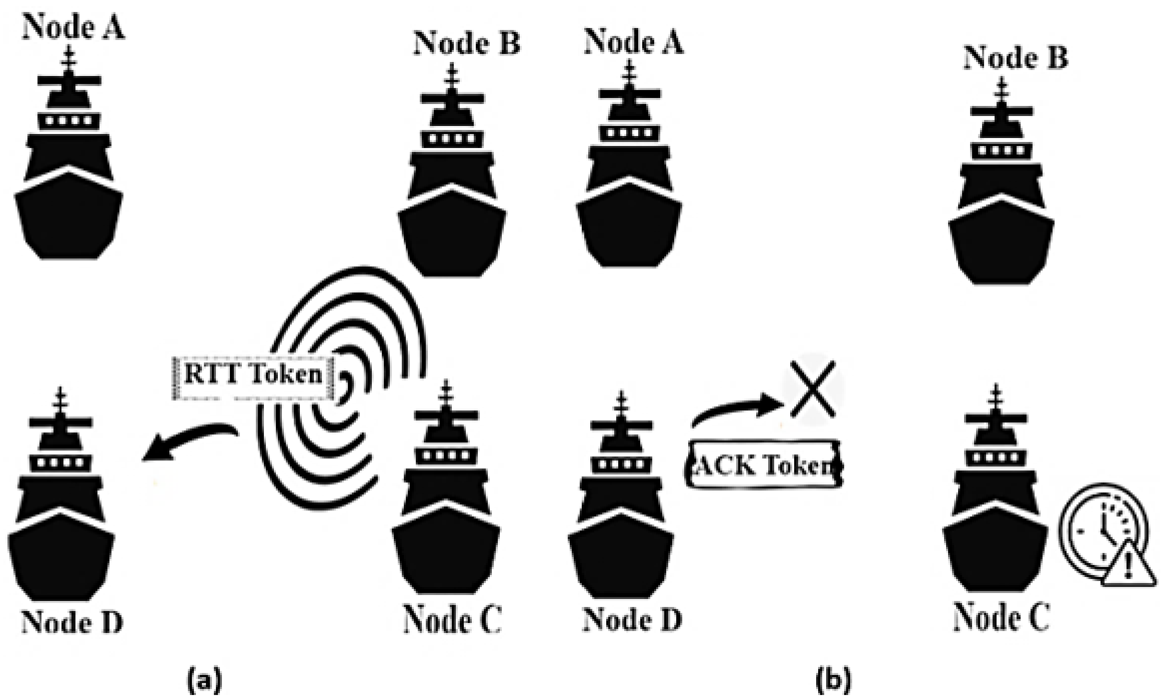

Figure 6

(a) Sending RTT token to node D, (b) node D is not responsible

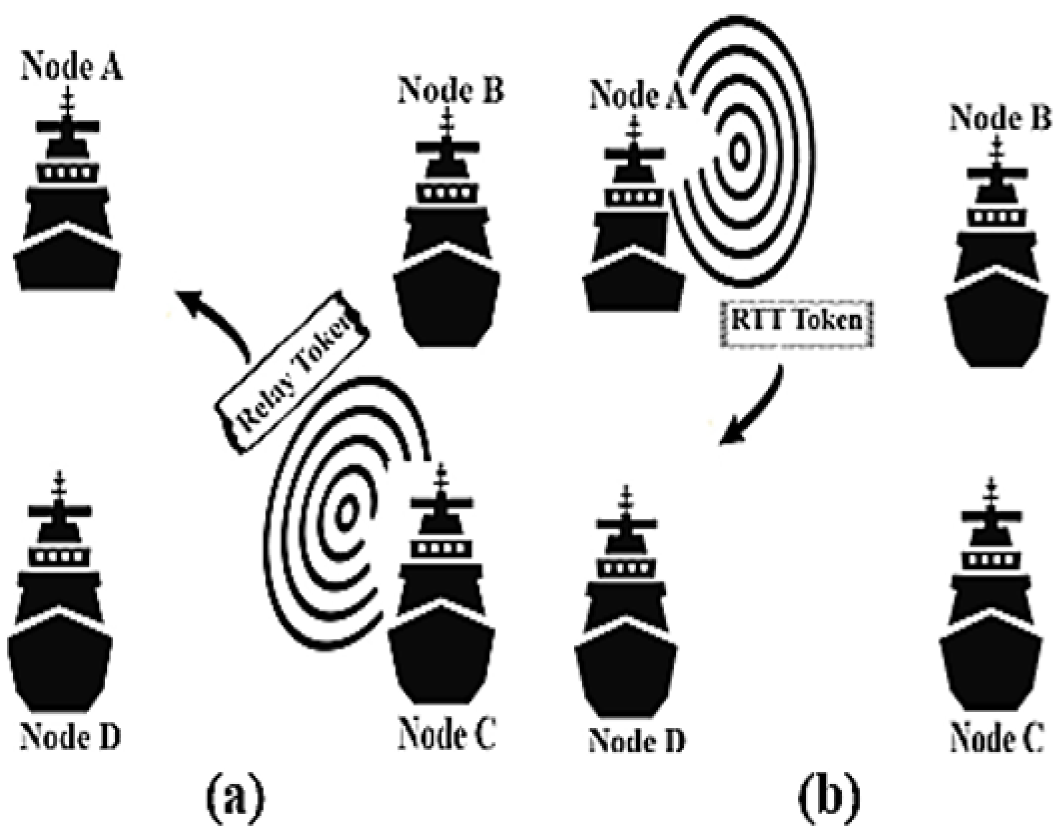

Figure 7

(a) node C sends Relay token to node A, (b) node A sends RTT token to node D

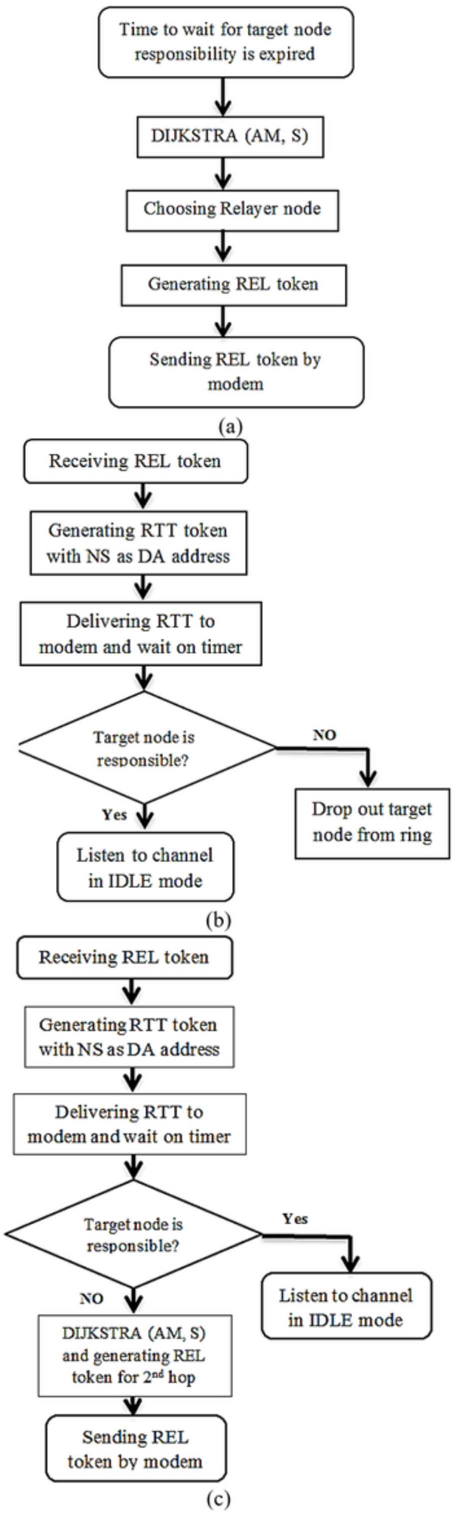

Figure 8

(a) Choosing the Relayer node in the requester node, (b) Flowchart of the one-hop relay in the Relayer node, (c) Flowchart of the tow-hop relay in the Relayer node

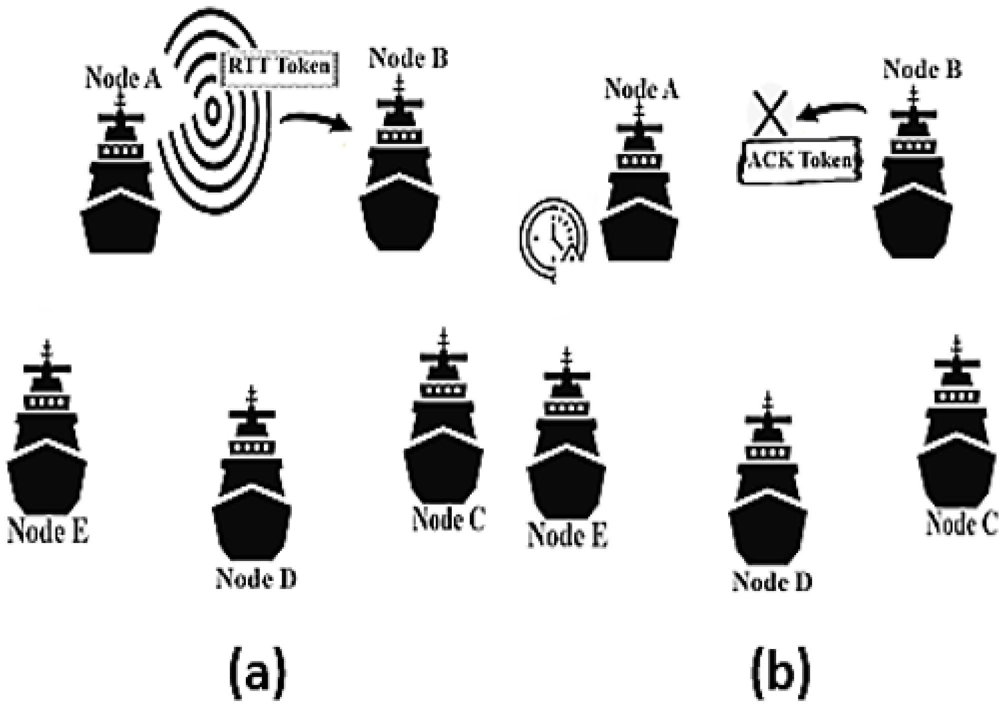

Figure 9

(a) Node A sends RTT token to node B, (b) Node B is not responsible

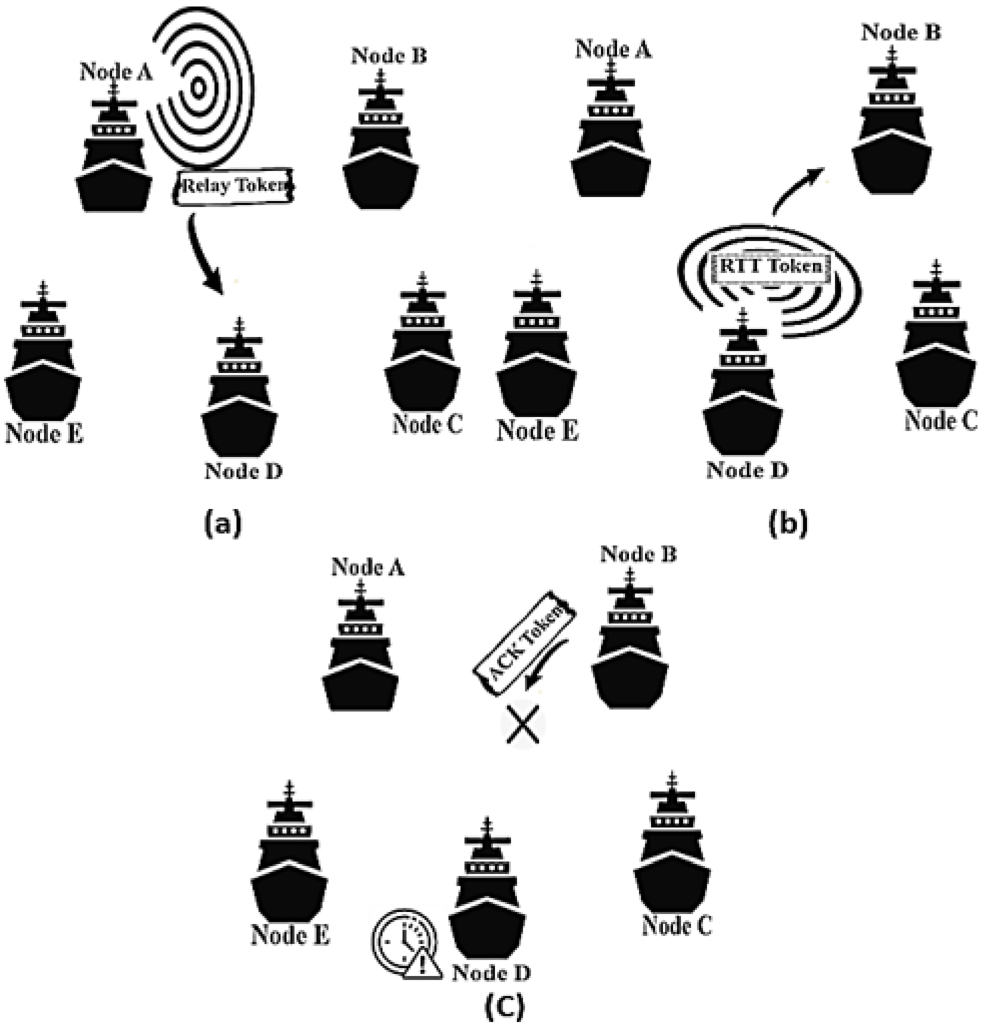

Figure 10

(a) Node A sends relay token to node D, (b) Node D sends RTT token to node B, (c) Node B is not responsible

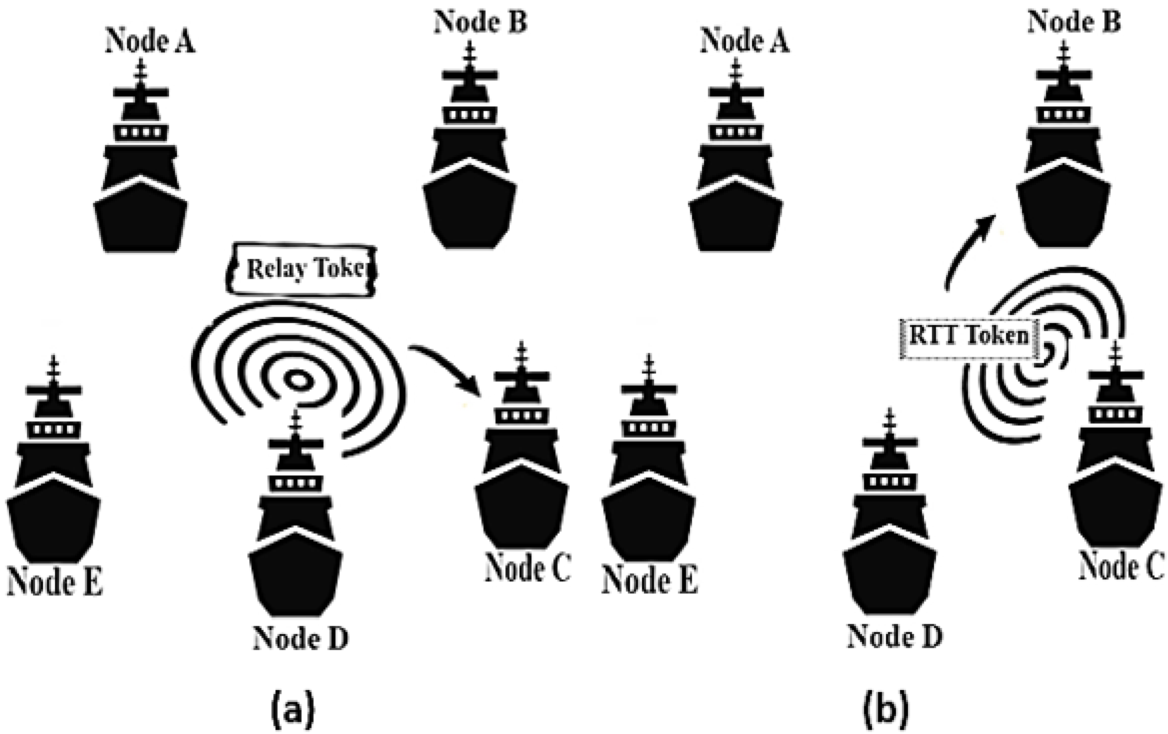

Figure 11

(a) Node D sends relay token to node C, (b) Node C sends RTT token to node B

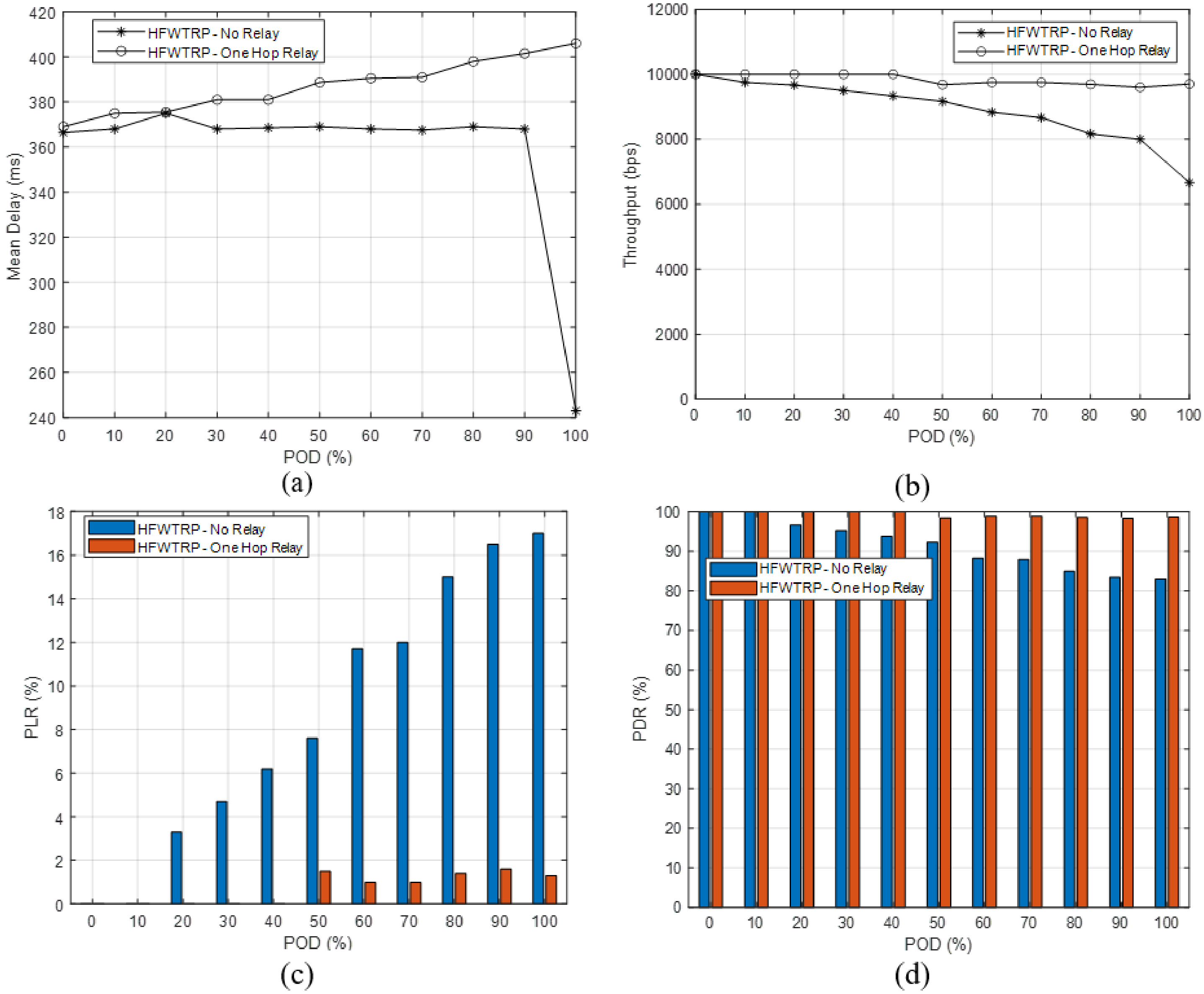

Figure 12

(a) Mean delay, (b) Throughput, (c) Packet Loss Ratio, (d) Packet Delivery Ratio VS POD for HFWTRP (no relay vs one-hop relay)

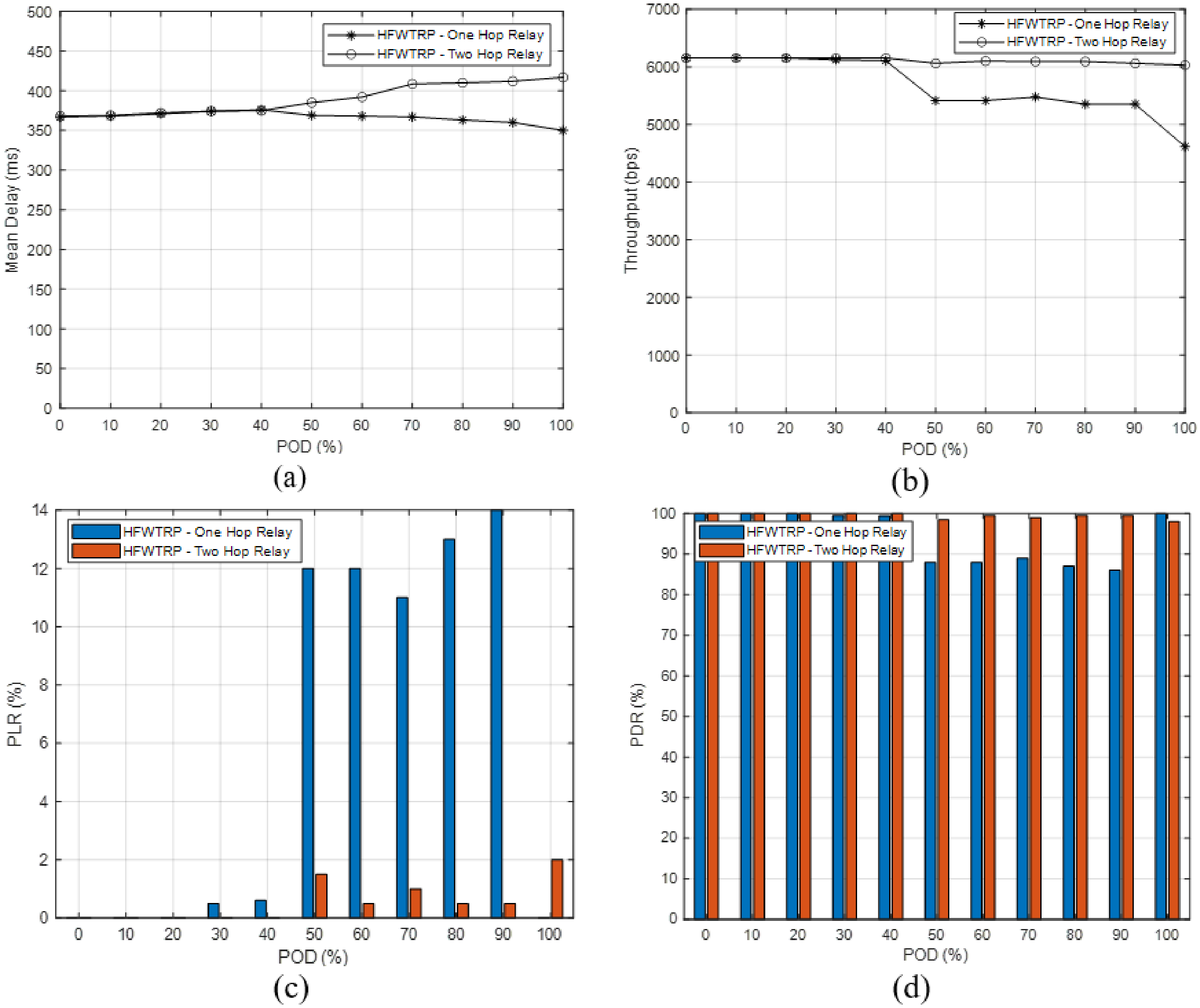

Figure 13

(a) Mean delay, (b) Throughput, (c) Packet Loss Ratio, (d) Packet Delivery Ratio VS POD for one- and two-hop relay