Fault-Tolerant Wireless Multihop Transmissions with Byzantine Failure Detection

Norihiro Sota and Hiroaki Higaki
1 Tokyo Denki University, Japan

Abstract—Wireless multihop networks consist of numbers of wireless nodes. Hence, introduction of failure detection and recovery is mandatory. Until now, various failure detection and recovery methods such as route switch and multiple routes detection have been proposed based on an assumption with stop failure model. However, the assumption that failed wireless nodes never transmit any messages is too restrictive the area where the proposed methods can be applied. In order to solve this problem, we propose a novel failure detection and notification method that supports not only stop failure but also Byzantine failure. That is, it is possible for failed wireless nodes to transmit malicious messages not according to the data message transmission and the failure detection and notification protocols unconsciously due to failure or even intentionally. Here, the design of failure detection and notification protocols is critical. In this paper, Byzantine failures in an intermediate node are detected by its multiple neighbor wireless nodes cooperatively since the neighbor wireless nodes are also vulnerable and might transmit erroneous failure notifications. From the performance viewpoint, no additional control messages are required to be transmitted while no failure wireless node is detected, i.e., in usual data message transmissions.


1. Introduction

In mobile wireless ad-hoc networks (MANETs) and wireless sensor networks, data messages are transmitted according to wireless multihop transmissions where each intermediate wireless node along the wireless multihop transmission route forwards them from the source wireless node to the destination one. Usually, the wireless transmission range of each wireless node is limited and the wireless nodes are assumed to be distributed densely enough for all the wireless nodes to be possible to communicate with some neighbor wireless nodes directly and to communicate with almost all the other wireless nodes by the wireless multihop communication. This is because, all the observation area is required to be covered by at least one sensor node and the sensor data messages are required to be transmitted to one of the sink nodes in sensor networks and enough high connectivity by wireless multihop transmissions is required in usual mobile wireless ad-hoc networks.

Such wireless multihop networks consist of numbers of wireless nodes. Hence, it is impossible to operate such wireless multihop networks continuously without failure detection, notification and recovery mechanisms. That is, higher resilient wireless multihop networks are required. Until now, various techniques for fault-tolerant distributed systems such as distributed failure detection, notification and recovery algorithms and systems have been proposed [3], [10]. For wireless multihop networks, only a naive watchdog method and its slight extensions have been proposed. Here, almost only the stop failure model in which failed wireless nodes become silent and never transmit any data and control messages is supported. Even though some methods support the Byzantine failure model, desirable behavior such as only erroneous data messages are transmitted is assumed. As discussed in this paper, erroneous and/or malicious data message transmissions deviated from the application protocols and erroneous and/or malicious failure detection and notification transmissions are required to be supported. This paper proposes a novel cooperative watchdog method and designs a data message transmission protocol with an extension of the Byzantine failure detection and notification and a routing protocol for detection of watchdoggable wireless multihop transmission routes based on flooding based ad-hoc routing protocols such as AODV [7].

2. Related Works

Suppose a wireless multihop transmission route \( R := \langle ||N_0(=N^*) \ldots N_n(=N^d)\rangle \rangle \) from a source wireless node \( N^* \) to a destination one \( N^d \) in a wireless multihop network such as a mobile wireless ad-hoc network and a wireless sensor network. If one of the intermediate wireless nodes \( N_f \) \((0 < f < n)\) is detected to be failed by one of its neighbor wireless nodes, a failure notification message is transmitted to the source node \( N^* \) and another wireless transmission route \( R' \) without \( N_f \) is searched and detected. Then, data messages are transmitted through not \( R \) but \( R' \). Until now, some failure detection, notification and recovery by re-routing have been proposed [4], [9]. In addition, for avoidance of high communication and time overhead for search of a detour wireless multihop transmission route, various multiple route detection protocol have also been proposed where multiple wireless multihop transmission routes are detected in a routing protocol and the routes are switched each time a failed intermediate wireless node is detected along an available wireless multihop transmission
route [1], [5], [8]. These papers only discuss the methods to switch wireless multihop transmission routes after detection of failure of one of the intermediate wireless nodes. The discussion of failure detection and notification is almost out of range.

There are some various failure model for wireless nodes [10]. Almost all of them assume that wireless nodes fail according to the following stop failure model where the failed wireless nodes become silent and the stop failure is detected by at least one of the other wireless nodes by using periodically transmitted “Hello” or “I’m alive” messages.

[Stop Failure Model]
A failed wireless node stops. It becomes silent, i.e., it never transmits and receives any data and control messages.

A stop failure usually detected by using a timer [2]. A neighbor wireless node $Q$ of another wireless node $P$ sets its timer. If $Q$ does not receive a message from $P$ before the expiration of the timer, $Q$ detects failure of $P$. In wireless multihop data message transmissions along $R$, in cases that there are no failed wireless nodes in $R$, within a certain interval after the time when an intermediate wireless node $N_{i-1}$ forwards a data message $m$ to its next-hop wireless node $N_i$, $N_i$ forwards $m$ to its next-hop wireless node $N_{i+1}$. As shown in Figure 1, under an assumption of the disk model wireless signal transmissions, $N_{i-1}$ is surely within the wireless transmission range of $N_i$ and $m$ transmitted from $N_i$ to $N_{i+1}$ is surely overheard by $N_{i-1}$. Hence, if $N_{i-1}$ does not overhears $m$ forwarded by $N_i$ to $N_{i+1}$ during a certain interval after $N_{i-1}$ forwards $m$ to $N_i$, $N_{i-1}$ detects that $N_i$ is failed.

3. Proposal

3.1 Problems
As discussed in the previous section, the stop failure model is supported in various fault-tolerant methods for wireless multihop networks. The Byzantine failure model is more general than the stop failure model and it is much difficult to support [10].

[Byzantine Failure Model]
Failed wireless nodes do not always become silent. They might transmit and receive data and control messages. In addition, the transmission of the messages are not always according to application protocols. The failed wireless nodes might transmit erroneous and/or malicious data and control messages.

Different from the stop failed wireless nodes, the Byzantine failed intermediate wireless nodes in a wireless multihop transmission route might transmits different data messages from those they have received to their next-hop wireless nodes and might transmits data messages to their next-hop wireless nodes even though they have not yet receive any messages from their previous-hop wireless nodes. For such problems, some watchdog methods by the previous-hop nodes have been proposed [6]. If the wireless transmissions are based on the disk model, the transmitted data message from an intermediate node $N_i$ to its next-hop wireless node $N_{i+1}$ is overheard by its previous-hop node $N_{i-1}$. As shown in Figure 2, if $N_i$ transmits a different data message $m'$ to $N_{i+1}$ from $m$ that $N_i$ has received from $N_{i-1}$, $N_{i-1}$ detects the failure of $N_i$ by receipt of $m'$ different from $m$. That is, the Byzantine failure in $N_i$ is detected by $N_{i-1}$ by the comparison of data messages received and transmitted by $N_i$.

Fig. 1: Stop Failure Detection in Wireless Multihop Networks.

![Fig. 1: Stop Failure Detection in Wireless Multihop Networks.](image)

Fig. 2: Byzantine Failure Detection in Wireless Multihop Networks.

![Fig. 2: Byzantine Failure Detection in Wireless Multihop Networks.](image)
failed wireless nodes is initiated. Generally, $n$-simultaneous failure is defined as follows [3]:

[$n$-Simultaneous Failure]

The number of failed wireless nodes are at most $n$ at any instance. Failed wireless nodes are never recovered by themselves and removed from the wireless network system by a certain maintenance procedure.

Fig. 3: Simultaneous Byzantine Failures in Wireless Multi-hop Networks.

On detect the failure of an intermediate wireless node $N_i$, a wireless multihop transmission of a failure notification message $F_{not}$ to the source node $N_s$ is initiated by $N_{i-1}$. On receipt of the $F_{not}$, $N_s$ searches a wireless multihop transmission route $R'$ to the destination wireless node $N_d$ without the failed intermediate wireless node $N_i$. Until now, the failure detection is assumed to be correctly done in any intermediate wireless node. However, the failed intermediate wireless node $N_{i-1}$ might erroneously detect a failure of its neighbor wireless node especially its next-hop intermediate wireless node $N_i$ and initiate the transmission of the failure notification control message by transmission of a failure notification message $F_{not}$ of $N_{i+1}$ to its previous-hop wireless node $N_{i-2}$ even though $N_i$ does not fail as shown in Figure 4. Since it is impossible for $N_{i-2}$ to find the $F_{not}$ is transmitted by $N_{i-1}$ erroneously, $N_{i-2}$ and the other intermediate wireless nodes forwards the message to their previous-hop wireless nodes along $R$. Here, the source node is notified for requirement of re-routing due to failure not in $N_{i-1}$ but in $N_i$. Hence, newly detected wireless multihop transmission route surely excludes not $N_{i-1}$ but $N_i$, which is a serious problem to be solved.

The failure notification control message $F_{not}$ of $N_i$, transmitted by $N_{i-1}$ is also received by $N_i$. Hence, it can detect the erroneous or malicious transmission of $F_{not}$. In order to notify the failure of $N_{i-1}$ to $N_s$, an additional wireless transmission route from $N_i$ to $N_s$ without $N_{i-1}$ is required. In addition, since $N_s$ receives two different failure notification messages from $N_i$ and $N_{i-1}$, $N_s$ is required to select one of them for recovery.

Fig. 4: Erroneous Failure Detection of Byzantine Failure.

3.2 Neighbor Watchdog Wireless Nodes

In order to solve the problem discussed in the previous subsection, that is, under the 1-simultaneous Byzantine failure assumption, one of the intermediate wireless nodes along a wireless multihop transmission route might erroneously or maliciously transmit a failure notification control message, this paper proposes a cooperative watchdog method with the help of a neighbor wireless node $O_i$ of $N_{i-1}$ and $N_i$ as shown in Figure 5. Here, a neighbor watchdog wireless node $O_i$ is within the wireless transmission ranges of both $N_{i-1}$ and $N_i$. Hence, $O_i$ overhears the data messages transmitted both from $N_{i-1}$ to $N_i$ and from $N_i$ to $N_{i+1}$. Hence, same as $N_{i-1}$, $O_i$ also detects the failure of $N_i$ by comparison of data messages transmitted from $N_{i-1}$ to $N_i$ and from $N_i$ to $N_{i+1}$. Therefore, even if $N_{i-1}$ erroneously or maliciously transmits a failure notification message $F_{not}$ of $N_i$, to $N_{i-2}$, $O_i$ detects that the $F_{not}$ message while $N_i$ correctly works.

Fig. 5: Cooperative Watchdog Neighbor Wireless Nodes.

In cases that $O_i$ detects the erroneous transmission of the $F_{not}$ message, $O_i$ should prevent the wireless multihop transmission of $F_{not}$ of $N_i$ to $N_s$ and initiate the wireless multihop transmission of $F_{not}$ of $N_{i-1}$ since $O_i$ has de-
ected the failure of $N_{i-1}$. Hence, a control message $Fnot$ for notification of failure of $N_{i-1}$ is transmitted from $O_i$ to $N_{i-1}$. However, $N_{i-2}$ is not always a neighbor wireless node of $O_i$ and the $Fnot$ message is required to be transmitted not through the failed intermediate wireless node $N_{i-1}$. In order to realize the later discussed lower overhead route detection based only on the neighbor node information in each wireless node, $O_i$ and $N_{i-2}$ are required to be 1-hop neighbor or 2-hop neighbor through an intermediate wireless node $I_i$ as shown in Figure 6. The role of $I_i$ is only forwarding the $Fnot$ message from $O_i$ to $N_{i-2}$.

![Fig. 6: Intermediator Wireless Nodes for Notification.](image)

Now, we discuss the procedure in wireless nodes $N_{i-1}$, $N_i$, $O_i$, and $I_i$ for detection and notification of the 1-simultaneous Byzantine failure of one of these nodes to $N_{i-2}$. In the following discussion, the $Fnot$ message from $O_i$ is transmitted to $N_{i-2}$ through $I_i$; however, almost the same procedure is possible to be applied without the intermediate node $I_i$.

First, in the cases free from the Byzantine failures of all the intermediate, the neighbor watchdog and the intermediary wireless nodes, a data message $m$ is transmitted through the wireless transmission route $R$ according to the forward of $m$ by the intermediate wireless nodes $N_i$ as shown in Figure 7. There are no additional control message is required to be transmitted.

In cases that the intermediate wireless node $N_i$ fails according to the Byzantine failure model, the data message $m$ forwarded from $N_{i-1}$ to $N_i$ is not transmitted from $N_i$ to $N_{i+1}$, a different data message $m'$ from $m$ is transmitted from $N_i$ to $N_{i+1}$ even though no data message is transmitted from $N_{i-1}$ to $N_i$. Anyway, as shown in Figure 8, both $N_{i-1}$ and the neighbor watchdog wireless node $O_i$ detect the difference of data messages transmitted through the wireless links from $N_{i-1}$ to $N_i$ and from $N_i$ to $N_{i+1}$. At this time, the same failure notification control messages $Fnot$ for the failure of $N_i$ are transmitted from $N_{i-1}$ to $N_{i-2}$ and from $O_i$ to $N_{i-2}$ through $I_i$. Thus, $N_{i-2}$ receives these two $Fnot$ messages.

![Fig. 7: Data Message Transmissions with No Node Failure.](image)

![Fig. 8: Detection of Failure in $N_i$.](image)

In cases that $N_{i-1}$ transmits a failure notification message $Fnot$ for $N_i$ to $N_{i-2}$ though $N_i$ works correctly, $N_{i-1}$ fails according to the Byzantine failure model as shown in Figure 9. Due to the 1-simultaneous Byzantine failure assumption, $N_i$ does not fail. $O_i$ detects that $N_{i-1}$ transmits the $Fnot$ message for $N_i$ to $N_{i-2}$ though $N_i$ does not fail by overhearing the transmitted data and control messages. Thus, $O_i$ transmits a failure notification message $Fnot$ for $N_{i-1}$ to $N_{i-2}$ through $I_i$.

Same as the previous cases, even though $N_i$ does not fail and works correctly, $O_i$ erroneously detects the failure of $N_i$ and notifies it to $N_{i-2}$ through $I_i$ as shown in Figure 10. Due to the 1-simultaneous Byzantine failure assumption, $N_{i-1}$ does not fail. $N_{i-1}$ detects that $O_i$ transmits a failure notification control message $Fnot$ for $N_i$ though $N_i$ does not fail by overhearing the transmitted data and control messages. Then, $N_{i-1}$ transmits a failure notification message $Fnot$ for $O_i$ to $N_{i-2}$. Thus, $N_{i-2}$ receives two different failure notification messages $Fnot$ for $N_i$ from $O_i$ and from $O_i$ from $N_{i-1}$.

Finally, in cases that $N_i$ does not fail and one of $O_i$ and $N_{i-1}$ fails according to the Byzantine failure model and
transmits a failure notification control message \( F_{\text{not}} \) for the other to \( N_{i-2} \) as shown in Figure 11. Here, the correct wireless node detects the erroneous or malicious transmission of the failure notification control message \( F_{\text{not}} \) from the failed one. Thus, it transmits another failure notification control message \( F_{\text{not}} \) to \( N_{i-2} \). Hence, \( N_{i-2} \) receives two different \( F_{\text{not}} \) messages for \( N_{i-1} \) and \( O_i \).

The following Table 1 summarizes the above discussion. If one of the wireless nodes \( N_{i-1}, N_i \) and \( O_i \) fails, two failure notification control message \( F_{\text{not}} \) from \( O_i \) and \( N_{i-1} \) are transmitted to \( N_{i-2} \). Thus, when \( N_{i-2} \) receives one \( F_{\text{not}} \) message for one of the wireless nodes \( N_{i-1}, N_i \) and \( O_i \) from \( I_i \) or \( N_{i-1} \), it waits for receiving another \( F_{\text{not}} \) message. Then, \( N_{i-2} \) determines the really failed wireless node in accordance with Table 1 and transmits a composite failure notification control message to \( N_{i-3} \), which is transmitted to \( N^p \) along \( R \) for re-routing for the removal of the failed wireless node.

Usually, a failure of an intermediate wireless node \( N_j \) is detected by its neighbor watchdog wireless node \( O_j \) and/or its previous-hop wireless node \( N_{j-1} \) and a transmission of a failure notification control message \( F_{\text{not}} \) is initiated. Based on the 1-simultaneous Byzantine failure assumption, all the intermediate wireless node between \( N_{j-2} \) and \( N^p \) are surely correct. So that, these intermediate wireless nodes safely forward the failure notification control message to their previous-hop nodes. However, since the Byzantine failure model is assumed, a transmission of a failure notification message for an intermediate node \( N_j \) might be initiated by another intermediate wireless node \( N_i \) for re-routing for the removal of the failed wireless node. The unique chance to detect the erroneous or malicious failure notification control message is when the message is initiated. If the \( F_{\text{not}} \) message for \( N_j \) is initiated by \( N_j, N_i \) transmits a \( F_{\text{not}} \) message for \( N_j \) though it has not received the message from \( N_{i+1} \), all of which is observed by the neighbor watchdog wireless node \( O_{i+1} \). Hence, it is possible for \( O_{i+1} \) to transmit the \( F_{\text{not}} \) message for \( N_j \) to \( N_{i+1} \) and to induce the confirmation procedure in \( N_{i+1} \). However, if this confirmation procedure is introduced in each intermediate wireless node for transmission of \( F_{\text{not}} \) message hop-by-hop, longer transmission delay is required for \( F_{\text{not}} \) transmission since transmitted \( F_{\text{not}} \) message and the additional \( F_{\text{not}} \) message from \( O_{i+1} \) are required to be synchronized at \( N_{i-1} \) for confirmation. The transmission delay overhead for the failure notification control message is too high for realization of fault-tolerant wireless multihop networks. Thus, in our protocol, for confirmation of the failure notification message,
digital signature of the initial wireless node of the failure notification control message is attached to the \( F_{not} \) control message.

For determination whether a wireless communication link \( |N_i N_{i+1}| \) is a watchdoggable one or not, the neighbor relation with \( N_{i-1} \) is required. Hence, in order to determine the possible next-hop wireless nodes satisfying the watchdoggable wireless communication links, each node requires the neighbor relation of two hop neighbor wireless nodes. Thus, each wireless node achieves its location information by using GPS and advertise the location information to its 2-hop neighbor nodes.

The detailed proposed protocol would be discussed in our future research papers.

4. Evaluation

By using the data message transmission protocol with the Byzantine failure detection and notification, fault-tolerant wireless multihop transmissions of data messages are provided. In order to apply the proposed failure detection and notification, the wireless multihop transmission route is required to consist of only watchdoggable wireless communication links. Such a route is able to be detected by a flooding-based routing protocol such as AODV. Here, the protocol has two phases; a flooding phase for a route request control message \( R_{req} \) transmissions and a unicast phase for a route reply control message \( R_{rep} \) along a detected wireless multihop transmission route \( R \). There are no additional control message transmissions and no additional synchronization overhead for data message transmissions without failure of intermediate wireless nodes.

However, in order to detect the watchdoggable wireless multihop transmission route based on the flooding of an \( R_{req} \) control message as discussed in the previous section, each candidate of an intermediate node is required to keep the two-hop neighbor relation as discussed in subsection 3.3. That is, each wireless node broadcasts its location information to all its 2-hop neighbor nodes by using TTL centric broadcasts independently of the transmission requests. For data message transmissions, no additional data and control messages are required to be transmitted. Additional control message transmissions are only required to detect and notify the failure of \( N_{i-1} \), \( N_i \) and \( O_i \) to \( N^* \). These \( F_{not} \) control messages are transmitted to \( N_{i-2} \) and synchronized there which requires communication and synchronization overhead.

In the proposed method, a wireless multihop transmission route is required to consist of only watchdoggable wireless communication links. Hence, a part of wireless communication links are not included in the wireless multihop transmission routes and the available wireless communication links ratio is expected to depend on the density of wireless nodes. Thus, we evaluate the effect on the route detection ratio by the restriction on the wireless communication links in the proposed method in simulation experiments. Figure 14 shows the simulation settings. \( N^d \) is a destination wireless node and \( N^s \)'s are a source wireless node or intermediate ones. Additionally, 1,000–20,000 wireless nodes are randomly distributed in the 600m x 600m simulation area whose
wireless transmission ranges are 10m.

Fig. 14: Simulation Setting.

Figure 15 shows the simulation results. The x-axis represents the numbers of wireless nodes, y-axis represents the distance from the source wireless node to the destination one, and z-axis represents the successful route detection ratio. For comparison, the route detection ratio in AODV is also evaluated. In both method, the route detection ratio monotonically increases according to the number of wireless nodes and is almost independent of the distance from the source wireless node to the destination one. In highly dense and sparse distribution of wireless nodes environment, the route detection ratio is almost constant. In the middle range, the route detection ratio steeply changed. In AODV, the threshold of high route detection ratio is 8,000 and the threshold of low route detection ratio is 6,000. On the other hand, in the proposed method, the threshold of high route detection ratio is 11,000 and the threshold of low route detection ratio is 6,000. Thus, in the range 8,000-11,000, the proposed method reduces the route detection ratio, which is almost only the disadvantage of the proposed method. The detection, notification and recovery of the Byzantine failed wireless nodes are critical technique for achieving the fault-tolerant wireless multihop networks and the merits of the proposed method surpass the disadvantage for reliable wireless multihop transmission requirements.

5. Concluding Remarks

This paper has proposed a novel communication protocols, i.e., for wireless transmission route detection and for data message transmissions in wireless multihop networks with failure detection, notification and recovery. Though almost all the conventional methods only support the stop failure, the proposed method supports the Byzantine failure where failed wireless nodes does not become silent and continues to communicate with the others out of their application protocols, i.e., erroneous and malicious data messages are also transmitted. This makes difficult to realize the failure detection and notification. The proposed method introduces the cooperative watchdog method where two successive intermediate wireless nodes and an additional neighbor watchdog wireless node cooperate. In the proposed protocol, no additional control message transmissions are needed and the failed wireless node is correctly removed. In addition, the simulation experiments show that the proposed method has a little disadvantage on the successful route detection ratio. However, in the usual density of wireless node to assure the wireless multihop connectivity, almost no reduction in route detection ratio is expected.

References