Distributed Fuzzy Control of Communications

Aivars Celmiņš

U.S. Army Research Laboratory
celms@arl.mil

Abstract

This paper deals with the control of battlefield radio communications. The particular properties of battlefield communications in modern warfare make a distributed access control highly desirable. Inputs for such a control are approximate descriptions of the status of the network. The control rules are heuristic because the controlled process does not have a set point. On the other hand, the network nodes have ample computing power that can be used to analyze the input and exercise access control algorithms. These circumstances suggest the use of fuzzy-logic control procedures. The author has developed such control procedures and tested their behavior on a computer model of battlefield communications.

1. Introduction

A typical communications network in a battlefield consists of a moderate number of nodes that are broadcasting on a single low-bandwidth radio channel. Problems arise when more than one node tries to access the channel at the same time. The ensuing message collisions can cause a breakdown of communications just at those times when information exchange is important.

To ensure smooth communication and to enhance the information throughput rate, a control of network access is mandatory. However, a hierarchical control is not practical in a battlefield environment for two reasons. First, the status of the network changes dynamically. Therefore, a regulating node must be constantly supplied with information about the present status. Such information gathering would use up broadcasting time, and the received information might be outdated on arrival. Second, the concentration of control in a single node makes the communications network more vulnerable.

These difficulties can be avoided by using a distributed control where each node listens to the network traffic and makes independent decisions for accessing the network. This is possible because in a modern battlefield communication system the nodes are computers, and the communication is in digital form among these computers. That is, each node has ample computing power to analyze the network traffic and make decisions.

The inputs for the control procedures are obtained by passive listening that provides only approximate, albeit up-to-date, information about the network status. Therefore, the control rules must be of such type that allows approximate input. Also, the goal of the control is defined only approximately as "enhance the information throughput". The system has no set point and control rules that are based on error terms are not applicable. This suggests the use of fuzzy-logic control rules. This paper describes such control procedures that have been developed at the U.S. Army Research Laboratory.

2. Network access algorithm

We are seeking access control procedures with the following properties:
1) All nodes have equal chances for access.
2) Information throughput is enhanced.
3) Priority messages have higher access chances.

An algorithm that achieves these goals can be constructed around the following broadcast procedure. A monitor at each node constantly listens to the radio channel and informs the access manager program when the channel is free. At that time \( t \), the manager determines which message from its message queue should be broadcast, chooses a random time interval \( A \) from a prescribed access delay interval range \((0, D)\), and sets a tentative broadcast time \( t + A \) for the message. If the channel is still free at the set time, then the message is broadcast. Otherwise, the manager aborts the procedure and waits for the next free time signal.

Obviously, the procedure satisfies the first property if all nodes use the same access delay interval \( D \). The procedure would also prevent...
The procedure would also prevent message collisions, if the response time of the nodes would be zero and the propagation speed of radio signals infinite. In practice, however, the response times are finite, and it is estimated that messages from different nodes will be broadcast simultaneously and collide if their set times differ by less than 0.5 s. (A typical message length is of the order of one to ten seconds.) Collisions reduce the information throughput rate because collided messages must be repeated. The probability of collisions is reduced by increasing the size of the access delay interval $D$. On the other hand, a large $D$ means long idle times for the network and the idle time is reduced by reducing $D$. Hence, there exists an optimal $D$ that corresponds to a maximum throughput rate and somehow depends on the size and state of the network. The goal of the control procedure is to find an optimal $D$ from information that can be obtained by monitoring the network traffic.

The third property is taken care of by reducing the global $D$ for high-priority messages and increasing it for low-priority messages. The priorities are assigned automatically by the message-generating programs. (The messages are composed, encoded, and broadcast automatically from data such as unit strength, unit location, action orders, enemy activities, and atmospheric conditions that are entered into the node's computer.)

### 3. Input information

The state of a battlefield communications network is completely described by the number and state of the nodes, the message queue at each node, and the characteristics of external noise. However, the current values of these state parameters are not available to the access managers at the nodes. Instead, the network conditions must be inferred from approximate information that is obtained by listening to the network traffic. We have chosen three groups of network parameters that can be obtained by listening. These parameters represent time averages of observations during a listening time interval $L$ prior to the reference time $t$. One group consists of the relative usage time of the radio channel during the time interval $(t - L, t)$ in three usage categories. A second group consists of the relative number of network accesses during the same time interval in the three categories. A third group consists of average message lengths in the three categories. The categories of network usage time are:

1. Idle time
2. Successful transmissions.
3. Collided transmissions.

For effective control, one needs also predictions about the expected status of the network. Such predictions can be obtained from the trends of the observed parameters that usually are obtained by numerical differentiation. However, in the present problem, simple numerical differentiation cannot be used because of the oscillatory character of the data. Therefore, trend indicators were obtained by subtracting from the simple averages of the parameters corresponding weighted averages over the same averaging interval $L$ with linearly decreasing weights.

The length $L$ of the listening interval cannot be chosen arbitrarily. A too short length provides only useless data about the instant channel status, while an averaging over a too large $L$ is not sufficiently responsive to changing trends of the averaged parameters. Therefore, the access controller also controls the listening and averaging interval $L$ by adjusting it as necessary if network conditions change.

### 4. Control rules

#### 4.1. Control of monitoring

The proper size of the monitoring and averaging interval $L$ was found by experiments to be about 40 to 50 times the average length of transmitted messages. (These and other experiments were done with a computer model of battlefield networks [1].) To accommodate changing network conditions, $L$ was controlled dynamically, that is, $L$ was increased or decreased from its current value if it deviated significantly from the set value of 50 times the current message length. The deviation was expressed in terms of the dimensionless quotient

$$Q = \frac{L}{(50 \cdot a) - 1}$$

where $a$ is the average message length. The correction of $L_{\text{old}}$ was expressed by a factor $\lambda$ as follows:

$$L_{\text{new}} = L_{\text{old}} \cdot (1 + \lambda)$$

The control rule that was used can be expressed in terms of a fuzzy-rule table as follows:

<table>
<thead>
<tr>
<th>$Q$</th>
<th>NL</th>
<th>N</th>
<th>Z</th>
<th>P</th>
<th>PL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda$</td>
<td>PL</td>
<td>P</td>
<td>Z</td>
<td>N</td>
<td>NL</td>
</tr>
</tbody>
</table>

where NL, N, Z, P, PL denote fuzzy sets that define...
the categories "negative large", "negative", "zero", "positive", and "positive large", respectively.

4.2. Control of access

The access to the radio channel is regulated by the size of the access delay interval $D$. In principle, the size of $D$ can be efficiently controlled by the simple algorithm

$$D_{\text{new}} = D_{\text{old}} \cdot (1 + \delta),$$

where $\delta$ is an output of the control rules. In practice, this simple procedure must be modified to ensure that after an initialization time all independent controllers indeed produce the same value of $D$, even when starting from different initial conditions. For clarity, we shall first describe the control rules in the context of Eq. (3) and discuss the modifications of the algorithm later.

Let $c - i$ be the difference between the relative uses of channel time for colliding messages and for idling, respectively, during the listening interval $L$. An obvious control rule is "increase $D$ if $c - i > 0$ and decrease $D$ if $c - i < 0". In terms of a rule table,

<table>
<thead>
<tr>
<th>$c - i$</th>
<th>NL</th>
<th>N</th>
<th>Z</th>
<th>P</th>
<th>PL</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\delta$</td>
<td>NL</td>
<td>N</td>
<td>Z</td>
<td>P</td>
<td>PL</td>
</tr>
</tbody>
</table>

This set of rules turns out to be very effective but it does not account for the possibly different message lengths. Thus, a single collision involving a very long message can increase the average collision time $c$ as much as many collisions involving short messages, but in each of these cases, the proper control strategy is different. Therefore, as a second input, the trend of the number of colliding accesses was used. Let $\tau_c$ be the observed trend. Then the rule table is

| $\tau_c$ | NL | N | Z | P | PL |
| $\delta$ | NL | N | Z | P | PL |

To make the control more responsive to extreme conditions, two more inputs were considered: "idle time over a threshold" and "collision time over a threshold". The rule table for the former was

| $i - t_f$ | NL | N | Z | P | PL |
| $\delta$ | O | O | O | NL | NL |

Experiments show, however, that the last two sets of rules have only a minor effect on the performance of the control if used in addition to the first two sets of rules. If used without the first two sets of rules, then the performance of the control was not as good as with the first two sets alone.

The outputs from the rules were combined using the compositional rule of inference ([2] - [5]), and the fuzzy result was defuzzified using the center of gravity method [4]. A combination of rules in the form of two-dimensional rule tables was also tried and found to perform equally well.

The described control works efficiently if all nodes start with the same initial value of $D$ and have the same observational input. In practice, one can only assume that the monitored inputs are approximately equal for all nodes, but the initial conditions can be quite different because different nodes might join the network at different times. Therefore, the updating formula (3) for $D$ must be modified such that after an operation over a reasonable time (several minutes) differences among the nodes become negligible. One method to achieve this is to replace Eq. (3) by an absolute output instead of the corrective one. However, experiments indicate that such a control is not efficient because absolute outputs cannot be easily adapted to changing network conditions. We now describe a replacement of Eq. (3) that was found satisfactory.

First, we separate in Eq. (3) the dimensional factor $D$ from the nondimensional corrector $F = 1 + \delta$, and devise for $F$ an updating procedure such that the factor drifts with time to a fixed value that is independent of its initial value. Let $\Delta t$ [s] be the difference between the current and previous times of network parameter readings. (Network parameters are updated at discrete times after the end of each activity, that is, at the end of each transmitted message, because only at those instants the average usage times and access numbers can be computed.) Let $f$ be a fixed value of $F$ to which the correction factor should drift with increasing time. Let $\epsilon = \exp(-\Delta t/60)$. Then the factor is updated as follows

$$F_{\text{new}} = (f \cdot (1 - \epsilon) + F_{\text{old}} \cdot \epsilon) \cdot (1 + \delta).$$

One can show that the exponential factor in the
formula has the effect that the starting value of \( F \) becomes insignificant after a few minutes. Hence, if all nodes would use the same \( f \), then equalization among the nodes would result. Experiments show, however, that an \textit{a priori} assignment of a unique value of \( f \) for all conditions is not desirable. Rather, to have efficient access control, its value should be allowed to vary typically between 0.001 and about 80. We achieve equalization of \( f \) by assigning to it only a limited number of discrete values within this range. In particular, the access controllers assign to \( f \) values in steps of four according to the following algorithm:

- If \( \delta_{\text{old}} > 0 \) and \( \delta_{\text{new}} > 0 \) then increase \( f \).
- If \( \delta_{\text{old}} < 0 \) and \( \delta_{\text{new}} < 0 \) then decrease \( f \).

Equalization of the factor \( f \) among the nodes occurs in short time, because the control output \( \delta \) typically continuously increases or decreases over more than twenty readings.

A reasonable value for the dimensional factor \( D_{\text{old}} \) is, for instance, the average idle time. However, that average increases when \( D \) is increased and vice versa, thereby accelerating any corrections by the control. In extreme conditions this results in a drift of \( D \) to zero or infinity. We avoid such excursions by using the logarithm of the average idle time instead of the average itself. The average idle time is also subject to smaller oscillations between readings that are not conductive to access control. These oscillations were reduced by using a weighted average of the current and previous reading of the average idle time. The weighting was again done with an exponential factor that reduces the influence of old readings. Let

\[
\nu = \exp(-\Delta t/300)\.
\]

Then the effective value of the average idle time is computed by

\[
i_{\text{eff}} = (i_{\text{old}} \cdot \nu + i_{\text{new}}) / (\nu + 1) .
\]  

The final formula for the access delay time that replaces Eq. (3) is with these modifications

\[
D_{\text{new}} = (0.01 + \log(1 + i_{\text{eff}}/A)) \cdot F_{\text{new}} .
\]

4.3. Granulation

In all sets of rules five categories of input and output were found to be sufficient. The membership functions that define the categories were restricted to symmetric trapezoids. The utility programs that were developed and used for rule combinations and defuzzifications accept arbitrary forms of membership functions but it was found that more general functions are not needed to achieve optimal control. Numerous experiments were carried out to determine optimal definitions of input/output categories under different conditions. Results of these experiments indicate that the best membership functions are robust in the sense that similar functions perform well for a wide variety of networks, and that the corresponding minima are flat. If the control should be implemented in field equipment then special fuzzy-logic chips would be used for the fuzzy-logic operations. The results of the numerical experiments will provide guidance for the design of such chips.

5. Examples

Let the network consist of \( n \) nodes and let us assume that the message generation rate is sufficiently high so that all nodes accumulate queues of messages for broadcasting. Let further the message generation stop at a preset time. Then a good measure for the performance of access control is the time that is needed to empty all queues. Using different control strategies with the same set of message queues, one can compare the control performance by comparing the corresponding completion times. We present an example of a network with four nodes. The information content, measured by the total length of all messages in a queue was approximately equal for all nodes but the average lengths of messages were different for different nodes. In Figure 1, the results of an experiment with fixed access delay time are compared with the results with controlled delay time. The left-hand graph shows curves of network usage times for a fixed access delay time \( D \) of 13 seconds. All queues are emptied in about 34 minutes. The graph shows that during that time the channel has been used for message transmissions about 17 minutes (dashed curve), for idling about 11 minutes (solid curve), and for colliding messages about 6 minutes (dotted curve). It is obvious that during the first 20 minutes the access delay time interval \( D \) was too short, causing many message collisions. On the other hand, during the last 10 minutes of the experiment, there were no new collisions (the dotted curve is flat), and a smaller \( D \) could be used to reduce the idle time. The right-hand graph shows the same network with a controlled delay time interval \( D \). We observe that the dynamically adjusted \( D \) equalizes the collision and idle times and achieves a shorter completion time. In this experiment, the dynamically adjusted access delay time \( D \) was varied between less than one and about 65 seconds.
6. Conclusion

The distributed control of battlefield communications has been found effective and the optimal parameters of the investigated control algorithm were found to vary little under very different conditions. This result makes the design of an efficient general fuzzy-logic control of battlefield communications possible.

7. References


Figure 1. Network usage with fixed and controlled access