A division of AMIRIX

Tel: (902) 450-1700
Fax: (902) 450-1704 www.vemco.com

Application Note

False Detections: What They Are and How to Remove Them from Detection Data

Document #: DOC-004691 Version 03
April 17, 2012

Author: Douglas G. Pincock, PhD

Table of Contents

List of Tables

List of Figures

1. Overview

This note shows how false detections (i.e. a detection of a transmitter code that isn't actually present) can occur in the field and how you can identify them. While such occurrences can be disconcerting, you should be aware that:

1. Any digital communication system (particularly one using acoustics underwater) will generate false detections.

2. The rate at which they occur with VEMCO coded tags is very low – and can be managed by ensuring that one doesn't set *tag delay* too low for anticipated greatest tag residency (i.e. number of tags simultaneously present) at a receiver.

3. They can be identified and removed by the methods discussed here.

2. Introductory Comments on Digital Communication

2.1 Transmission Errors Exist in All Systems

The combination of tags transmitting ID and Sensor information to a receiver constitutes a digital communication system and, like all such systems, there will be transmission errors (i.e. a deviation between what the receiver detects and what was actually sent).

So the real question is what the system designer does about transmission errors. In some cases, it is perfectly acceptable to do nothing. Consider, for example, the transmission of a digital television signal. If a pixel is received in error (i.e. the receiver assigns the wrong value to it), it will not be visible to the viewer unless there are many such occurrences in each frame. On the other hand, a system communicating messages over the internet to initiate an electronics funds transfer must have mechanisms in place to ensure that any transmission errors are rejected by the receiving entity.

The transmission of ID codes from a tagged fish are more like the latter example – we want to make sure that a transmission error doesn't cause us to assume a fish was present that was not. This creates a significant challenge due to the nature of the medium for underwater acoustics which means that transmission errors will be common regardless of the communication method used.

2.2 Detection of Transmission Errors

In any communication system requiring the rejection of erroneous transmissions, the approach is to transmit extra bits in the form of an Error Detection Code (EDC) which is calculated according to some formula from the data bits and added to the transmission. At the receiver, the EDC is recalculated from the data bits and compared to the received EDC. Transmissions in which the calculated and received EDCs differ are rejected as this could only occur as a result of a transmission error.

2.3 False Detections

Will error detection techniques detect all possible transmission errors? The answer is no; again, regardless of the scheme used, there will always be a non-zero probability that a transmission error will slip through the test creating a False Detection (i.e. a tag that appears to be present but isn't). The best one can do is increase the "robustness" of the EDC to the point that the probability of such False Detections becomes insignificant. Of course, you never get something for nothing and the cost of more robust error detection is that a higher portion of the bits transmitted are for error detection rather than the actual data.

3. Transmission Errors and Error Detection with VEMCO Coded Tags

3.1 Communication Philosophy

VEMCO coded telemetry uses a single transmission frequency to achieve robust, scalable technology forming the foundation for a world wide network of compatible transmitters and receivers. This is a very conservative approach; more aggressive approaches are possible[1] but at the price of an increase in complexity and Transmission Error rate[2].

3.2 Error Detection

A consequence of the conservative approach we use is that the rate at which bits can be transmitted is low; so we do not want to consume more of this small bandwidth than necessary for error detection purposes.

3.2.1 Receiver Operation – Valid Sequence Detection

The detection of transmitted codes is based on the measurement of time intervals between transmitted pulses. Therefore, a transmission error results whenever timing of pulses seen at the receiver differs[3] from what was transmitted. While in theory a number of factors can cause this to happen, the predominant cause is pulses arriving from some other source (another transmitter, noise, etc.). Figure 3-1 presents an example. Assuming the interfering pulses shown in red are detected by the receiver, it will have no way of distinguishing these from the pulses from the transmitter and it will attempt to decode the lower sequence shown in the figure.

The receiving algorithm is looking for the correct number of intervals for a particular coding scheme and that they all fall with the certain valid range of lengths which is pre-programmed into the receiver via the receiver code map. If this occurs, it identifies the sequence as valid. Clearly, for the example shown in Figure 3-1, the interfering pulses cause some of the intervals to be too short and the test fails. The receiver then abandons the attempt to decode the sequence until it sees another SYNC interval.

[1] And will increasingly be used by VEMCO for enhancements to meet some specific requirements.
[2] Too aggressive an approach can actually cause error rate to become so high that less data gets through than would be the case with a more conservative approach.
[3] Obviously within some tolerance.

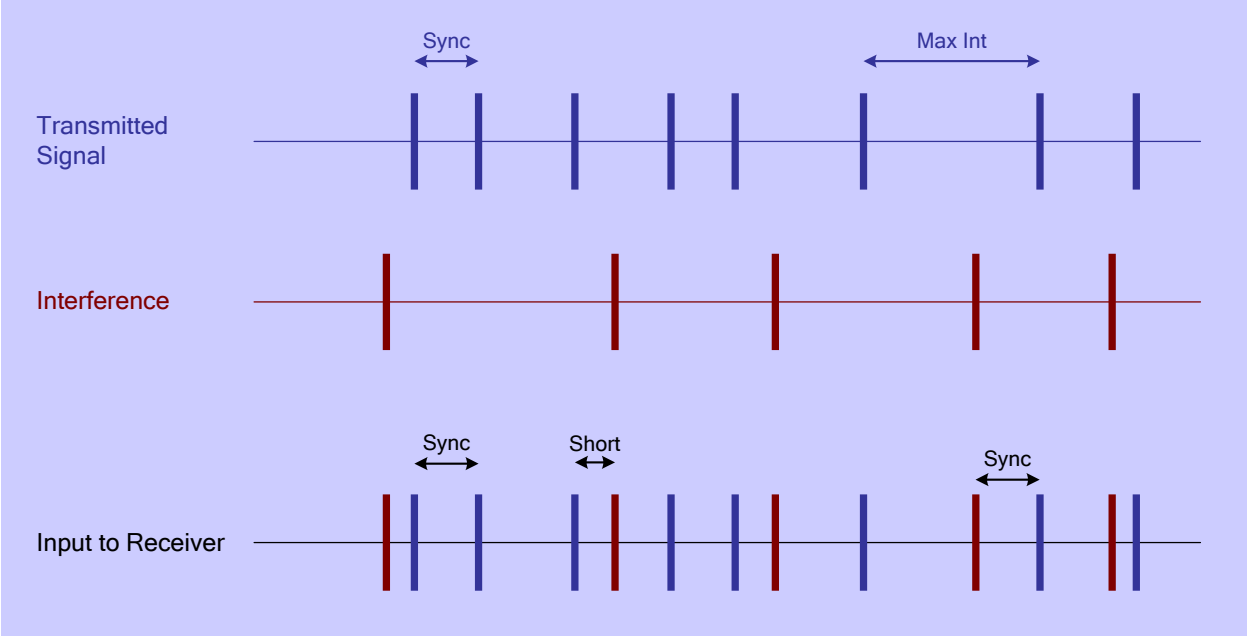

Figure 3-1: Interference Producing an Invalid Sequence at the Receiver

3.2.2 Transmission Errors Due to Collisions

The remainder of this note will concentrate on transmission errors resulting from collisions (i.e. two or more transmissions arriving together at a receiver) and the possibility of a false detection arising from such collisions. It is worth noting that, while false detections could theoretically be caused by other factors, one can show that:

1. The probability of such occurrences is much less than is the case for those caused by collisions.

2. Even should such a false detection occur, it would be rejected by the methods discussed here for dealing with false detections due to collisions.

Figure 3-2 shows a typical situation in which the interfering source is another transmitter. In this case, the receiver rejects the sequence because one of the intervals is either too long or too short.

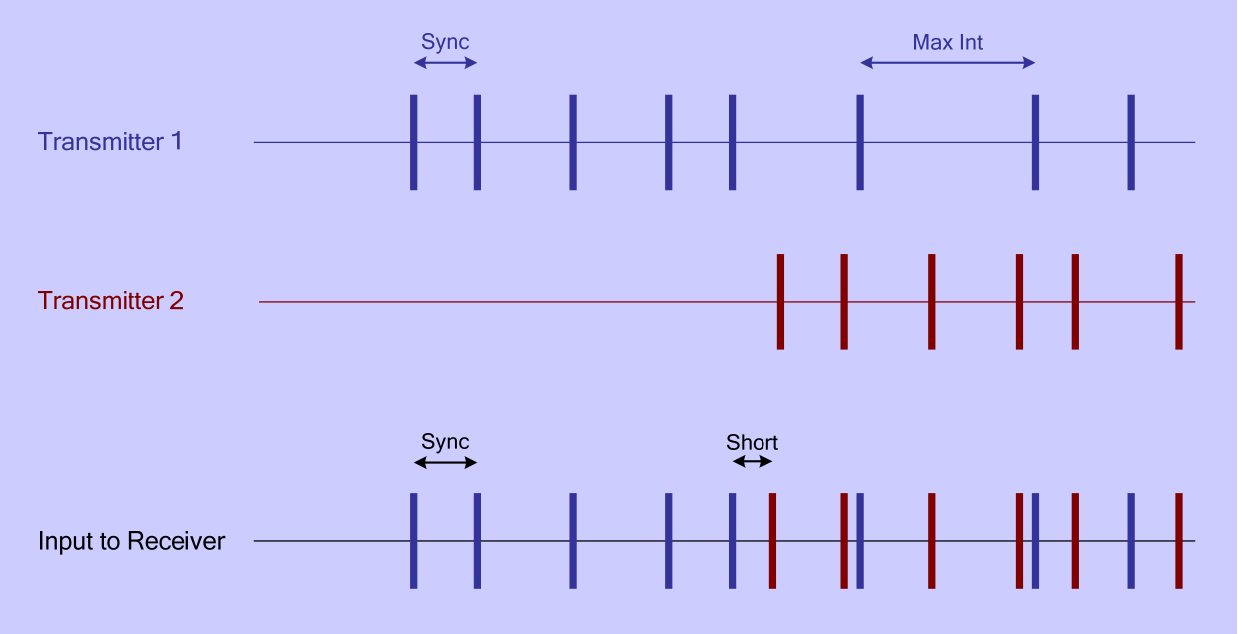

Figure 3-2: Invalid Sequence Produced by Collision with another Transmission

3.2.3 Receiver Operation – Valid Sequences and Error Detection

Occasionally, the timing between two transmitters will be such that the resulting train of pulses seen by the receiver is valid – i.e. the correct number of intervals that fall within the expected ranges (see Figure 3-3 as an example). However, since the intervals making up the valid sequence actually come from more than one transmitter, the error detection test should reject the sequence.

We have previously mentioned that no error detection method can reject all false positives and, with a finite and limited number of error bits in the transmitting algorithm, there are some number of valid sequences that should be rejected that are not.

Putting all of the above together, we see that the following conditions are necessary for a false positive detection to occur:

1. A collision of two or more tag transmissions (or interference of some sort).
2. The sequence resulting from the collision is a Valid Sequence, i.e. the pulse intervals are valid lengths.
3. The error detection algorithm fails to identify the transmission error.

Knowledge of the probability of such occurrences is a key component of ensuring that no false positive detections are interpreted as actual detections. This is discussed in the following section.

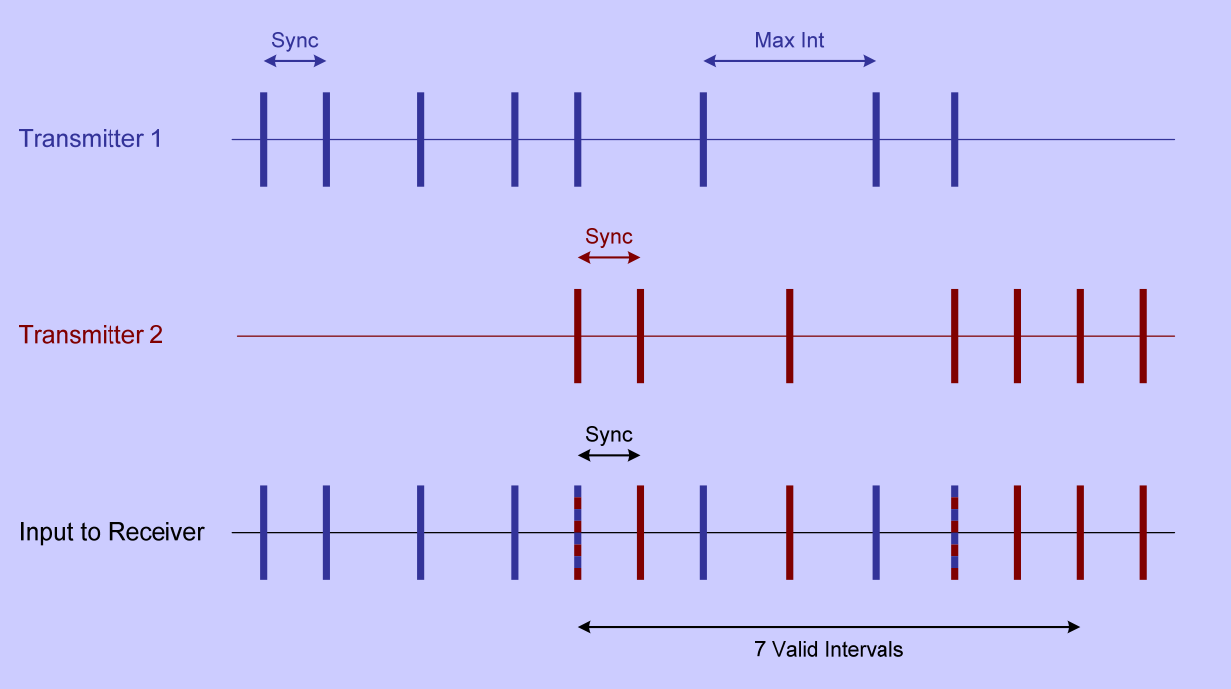

Figure 3-3: Valid Sequence Produced by Collision with Another Transmission

4. False Detection Statistics

The statistics of this situation are not simple and certain aspects can only be determined by simulation. This section outlines current results from our research into this.

Before digging into any details, it is perhaps useful to present an example showing the variability of results. The following summarizes results from a simulation involving 5 resident transmitters (Average Delay = 60 seconds):

- Total Simulation Length 2000 hours
- Average Time between False Detections 29 hours
- Total Number of False Detections 67
- Unique IDs in False Detections 6

Note from the last piece of data presented above that the IDs created are certainly not different every time; clearly IDs will often repeat themselves. This contradicts the often used assumption that the false codes which arise are random. This shouldn't be surprising considering that most sequences resulting from collisions will be rejected and only a small subset will get by the error checking. Over time, this small subset will get repeated given that the same set of tags and environmental conditions are present.

The other important information coming from this simulation is wide variability of the timing between successive false positives. This is demonstrated in Figure 4-1.

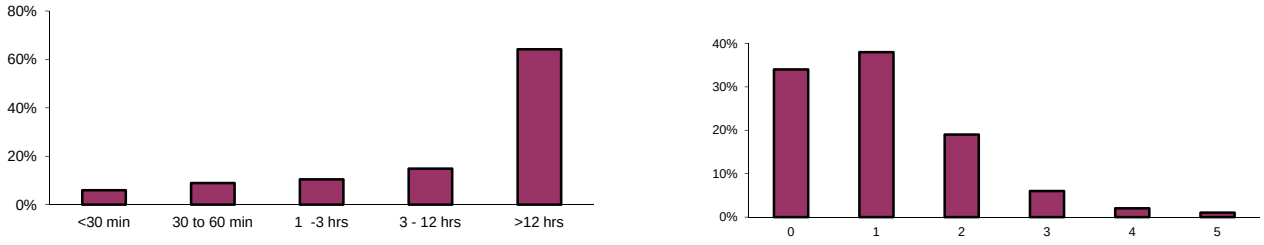

Figure 4-1: Timing between False Detections with a Set of Five Resident Transmitters having Average Delay = 60. Left hand plot shows distribution of times between successive False Detections. Right hand plot shows distribution of number of False Detections occurring in a 20 hour period.

Combining the information presented in Figure 4-1 with the fact that only a small number of False IDs are generated, we see that in the conditions simulated here, there is a distinct possibility that we could see the occurrence of the same False ID twice within 30 minutes or less.

Continuing with the same set of transmitters, Table 4-1 summarizes the occurrence of false detections of some typical situations for 5, 10 and 15 resident tags and average delays of 60 and 120 seconds.

Number of Tags	Delay	Average Time between False Detections
5	60sec	29 hours
10	60 sec	7 hours
15	60 sec	5 hours
5	120sec	88 hours
10	120 sec	21 hours
15	120 sec	12 hours

Table 4-1: False Detection Rates for a Set of IDs

Different sets of valid IDs may provide different results but the important point is that for continuously resident tags, there will be far more long intervals than short (see Figure 4-1) between successive detections of the same false ID[4] and this forms the basis of acceptance tests described in the next section.

Two final observations are worth noting:

1. In terms of the number of false detections, there appears to be no particular advantage to using random codes over contiguous ones.

2. Results for A69-1303 and A69-1206 codes spaces are very similar. Newer code spaces have improved error detection, and will result in fewer repeated IDs.

[4] Recall as well that successive detections of False IDs will not usually be the same ID; however, it is prudent to assume they will be.

5. Acceptance Criteria

5.1 Overview

The criteria presented in the next section are intended to err on the side of conservatism – i.e. sufficiently strict that no false detections are erroneously accepted. We will refer to this as first scan acceptance.

We suggest that users first apply such first scan criteria to any detection data that might contain false detections – i.e. virtually any situation where there are multiple tags present at a receiver. Depending on the number of detections rejected by the first scan – usually very small – there may or may not be a need for a second scan.

5.2 First Scan Acceptance Criteria

The information presented in Table 4-1 (or an extrapolation of it if Tag Delays other than 60 or 120 seconds are used) provides the kind of information one needs to qualify detections.

Acceptance of a Tag ID has traditionally been based on the fact that it is seen at least twice at a receiver within some time interval. However, if we combine the results shown in Figure 4-1 and Table 4-1 with the fact that successive false detections could well have the same ID, we see that such criteria need to be applied with care. This will be illustrated by an example simulation:

- Average Tag Delay = 60 seconds.
- Up to 10 Tags simultaneously present at a receiver.

On average, this showed a false positive rate of one every 7 hours with a very occasional pair less than 30 minutes apart (average once every 30 days); so, if the test ran long enough, even a requirement that there be successive detections less than 30 minutes apart introduces a higher risk of accepting a false detection than one might like to accept.

Based on the above, we recommend the following criteria for accepting a detection as valid.

1. At least one short interval
2. More short intervals than long

The second condition recognizes the fact that while a short interval is quite possible, the probability of more short than long intervals (e.g. more intervals shorter than 30 minutes than there are longer than 12 hours in the above example) is virtually zero.

The actual criteria for what represents short and long intervals depends on the programmed delay of tags used and anticipated maximum residency. We suggest that the short interval time be set at 30 times average delay and long interval time at 720 times average delay. We may refine this advice as our research advances.

Two final observations are related to the fact that False IDs can very possibly be similar or identical to those IDs of the actual tags present:

1. The above assumes that the probability of successive false positives having the same ID is 1. Clearly, this isn't the case but it's the only safe thing to do.

2. In a situation where one is trying to determine site fidelity, it is probability best to assume the fish has left each time there is a long interval and doesn't return until another short interval seen.

5.3 Second Scan Acceptance Criteria

The fact that a detection is isolated and fails the first scan test does not guarantee that it is a false detection but rather it indicates that there is a high probability that it is false. Therefore, users often wish to do deeper analysis to see if more of their detections can be accepted. In doing so, one needs to keep in mind that acceptance of a single detection or a set of widely spaced detections is risky if there are collisions at the time of detection even if the ID is one that you suspect might be in the area. The reason for this is that False IDs can be similar to the IDs of the actual colliding tags.

As a consequence, an isolated detection should be considered for acceptance under a second scan ONLY if there is concrete evidence that:

1. There is no collision activity.
2. The receiver is not installed in a location where severe noise causes spurious pulse detections by the receiver.

We cannot emphasize enough that it is very risky to accept any detections that fail the first scan if either of the above conditions is not satisfied. This is true for all VEMCO code spaces.

Reviewing the receiver data log and receiver statistics can be helpful in determining whether collisions, echoes or other noise sources are possible during the time in question.

By examining the data log from the receiver within VUE, you can manually inspect to see if there were many other transmitters being detected in and around the time of the detection in question.

In addition, you can review the receiver statistics to get an indication of the receiving conditions. To better understand this, we need to first go over the receiver statistics definitions:

- Each VEMCO transmitter emits a number of pings. The first two pulses form a Sync interval. VEMCO receivers record the number of pings and the number of Sync intervals detected.

- Each VEMCO receiver also records the number of detections that were rejected because of an invalid Error Detection Code.

- VR2W receivers log receiver statistics every day allowing the user to review receiving conditions on a daily basis. VR2 receivers only log a single set of statistics for the entire deployment.

5.4 Evaluating Receiving Conditions

In a good receiving environment, with no collisions and no echo problems, one should expect to see roughly 8 times as many Pings as Syncs and no Rejects for A69-1303 (R64k) tags. If the number of Pings is excessively high or low relative to the Syncs, it may suggest a large number of collisions, echoes and/or a noise source all of which can contribute to causing false detections. In this case it would be very risky to accept a detection that has failed the first scan.

A further note on echoes and other noise sources; these types of conditions can sometimes be identified prior to your study. During range testing in your environment, using a single tag, you would expect to see no rejects and close to perfect SYNC to Ping ratios. If you do not see this, one should be led to conclude that the position of the receiver may not be appropriate due to echoes or possibly some other form of interference and an alternate location should be chosen.

5.5 Acceptance Criteria Are a Trade off

It is not realistic to draw a line with all detections on one side valid and all on the other false. Assuming acceptance of a False detection is the greater sin, the philosophy employed throughout this discussion, and in any further analysis, is to try to draw the line so that no False detections are accepted and as few valid detections as possible rejected.

As well, detections on another receiver – particularly if they occur some time after, at a logical time and place, can help reinforce that a single detection is valid – again assuming that the 2nd scan acceptance criteria are met.

