THE ROLE OF PRECISE TIME IN IFF*

William M. Bridge

The MITRE Corporation
P.O. Box 208
Bedford, MA 01730

ABSTRACT

Precise knowledge of time of day can dramatically affect the design of military electronic systems. Small, inexpensive atomic clocks are becoming available that can provide free-running accuracies on the order of 10 to 100 microseconds for periods in excess of a month. Such clocks could revolutionize tactical communications, navigation, data links, IFF and ELINT systems.

This paper discusses the application of precise time to the IFF problem. The simple concept of knowing when to expect each signal is exploited in a variety of ways to achieve an IFF system which is hard to detect, minimally exploitable and difficult to jam. Precise clocks are the backbone of the concept and the various candidates for this role are discussed. The compact rubidium-controlled oscillator is the only practical candidate.

INTRODUCTION

Time has played a role in the battlefield identification of friend or foe (IFF) since the beginning of organized war. The challenge (question-and-answer) system for sentries has always involved the element of time. Eventually the challenge/password pair is compromised and must be changed. A returning soldier who missed the update is susceptible to fratricide. Present IFF techniques, although more sophisticated, bear some resemblance to this primitive system. Instead of a single challenge/password pair, there is a large library of coded challenge words which are paired with relatively few passwords for the duration of any given code-validity interval.

* This work was supported by the MITRE Independent Research and Development Program.

Security has always been a critical aspect of IFF systems. Any modern IFF system must have essentially perfect resistance to interrogation by the enemy or he (the enemy) will interrogate our forces and use our replies to determine whom and where to shoot. This situation is worse than no IFF at all and must be avoided at all costs.

The solution is a time-varying, cryptographic signalling scheme, and the security of such a system is improved by reducing the time interval for which the library of challenge/password pairs is valid (code-validity interval). However, as this interval is reduced, it becomes increasingly difficult to guarantee that all friendly forces receive a timely update of the challenge/password pairs. To be truly secure, the author believes that any new IFF system will have to be based on very accurate time synchronization.

SYSTEM CONSIDERATIONS

The current IFF system employs a signalling scheme where the library of challenge/password pairs remains valid for one day. Thus, if the enemy obtains even a single valid interrogation, he can interrogate and track our forces for the remainder of the day. The enemy can determine a valid interrogation by either listening to our IFF transmissions or by guessing interrogations until he receives a reply. The chances of guessing a valid interrogation are not all that bad and should yield results quickly. This condition seriously weakens the current system. One critical element of the answer is to drastically reduce the code-validity interval.

At this point we must distinguish between a code-validity interval and a cryptographic key-update interval. The key-update interval is related to the expected time that the enemy can be denied access to working IFF equipments. In peacetime the key-update interval can be fairly long provided there is a special, back-up key ready for immediate use when the war starts. Once the war starts, the length of the key-update interval becomes a complex question related to the progress of the war relative to the capture of our IFF equipment, the seriousness of IFF equipment compromise, and the difficulty of securely disseminating a new key under battle conditions. The latter two elements are the only ones that can be affected in the design of a new IFF system. Any new IFF system should certainly be designed so that the capture of working equipments, with or without the operators, is of minimal use to the enemy. The actual command and control information contained in an IFF transmission is of little use to the enemy and one might design the IFF system to take advantage of a public-key cryptographic system utilizing radio links rather than secure couriers for key distribution.

The code-validity interval can be much shorter than the cryptographic-key-update interval if each user has some form of synchronized clock. The actual encrypted IFF signal is then a function of time of day as well as the cryptographic key. As this code-validity interval shrinks, the system becomes increasingly difficult to exploit. Unfortunately, it also becomes increasingly difficult for our own forces to maintain time synchronization. If the code-validity interval can be made shorter than the time to guess a valid interrogation, this particular form of exploitation can be completely eliminated. However, the enemy still has the option of instantly repeating our valid interrogations omnidirectionally so that all friendly forces reply. The enemy can still track our forces but only when we choose to use the system. Unfortunately a minimum code-validity interval is set by the propagation time for the signal to reach the maximum range of the system. If this maximum range were 300 km, the minimum code-validity interval would be 1 ms. This minimum code validity interval still allows the enemy to instantly repeat interrogations from a short-range interrogator and elicit responses from all friendly forces out to the maximum range of the system. Thus, even with a minimum code-validity interval, the basic approach is vulnerable to repeat exploitation. However, a short code validity interval is certainly less vulnerable than a long one.

The reason that the minimum code-validity interval is set by the propagation time to maximum range is because IFF is thought of as a beacon-transponder system for the surveillance of friendly aircraft and not as an integral part of a fire-control system. The crucial difference is that a beacon-surveillance system demands replies from all friendly aircraft at all ranges and all azimuths, whereas a fire-control system needs an IFF reply only from aircraft that have been detected, tracked, and targeted by the weapon. The surveillance requirement proliferates the number of interrogations and replies, establishes a lower limit to the code-validity interval and results in a system that is inherently vulnerable to enemy exploitation.

TIME-SYNCHRONIZED APPROACH

If we give up the surveillance requirement and use IFF only as an adjunct to fire control, we can use accurate-time synchronization to achieve a system that is:

- hard to detect,
- virtually unexploitable, and
- difficult to jam.

Atomic clocks are available that can provide time with an accuracy on the order of one to ten microseconds for periods in excess of a day. Time synchronization with this accuracy allows spread spectrum signalling methods which include frequency hopping, time jitter, and a different intrapulse spreading code on each transmission. These essential characteristics of every transmission are known exactly to each friendly synchronized subscriber, but the enemy sees only an occasional, short-pulse, low-duty-factor signal which appears random in the dimensions of time, frequency, and intrapulse code.

Accurate-time synchronization can be employed in a variety of ways to achieve special ECCM features. The use of IFF as an adjunct to fire control requires selective interrogation of the tracked target in range and azimuth. Selective interrogation in range can be achieved by sending an interrogation pulse so that it will arrive at the target at a prescribed time of day known to both parties. The friendly responder simply opens a narrow gate at the prescribed time of day. The synchronized interrogator, knowing precisely the times that this receive gate is open, transmits his interrogation early by an amount equal to the propagation delay (measured a priori) to the tracked target. If the measured range is correct and the time synchronization is adequate the interrogation pulse should arrive at the desired target when the receive gate is open. This situation is depicted in figure 1. If the interrogation pulse subsequently arrives at a more distant friendly target within the antenna beamwidth (F_2 of figure 1), the additional propagation delay to the second target causes the pulse to arrive after the receive gate on the second aircraft has closed. Receipt of a pulse in the selective-interrogation gate tells the interrogatee that his range from the interrogator is approximately equal to the intended interrogation range. Of course, the specific times of day set aside for selective interrogation can be very frequent and ascribed in a pseudorandom fashion known only to friendly participants with accurately synchronized clocks.

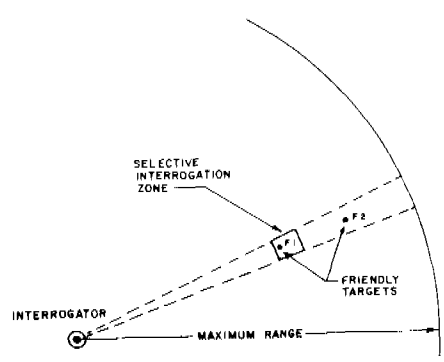

Figure 1. Selective Interrogation

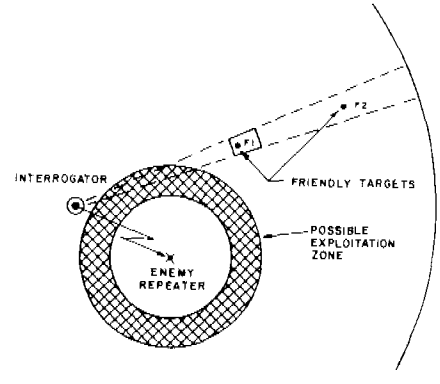

Figure 2. Repeater Exploitation

The width of this receive gate must be sufficient to accommodate the combined clock error at both terminals and any range-measurement error. If range-measurement error is negligible, as it should be in a fire-control system, and timing uncertainty at each terminal is within $\pm$ 10 μs, the receive gate could be as narrow as 40 μs. This means that only those targets within $\pm$ 6 km of the intended range receive a valid interrogation.

This approach to selective interrogation is operationally advantageous. It minimizes the number of inadvertent replies, markedly reducing the problem of reply interference or "fruit." It also greatly reduces the effectiveness of enemy repeat exploitation, as seen in figure 2. If the enemy repeater employs an omnidirectional antenna, the effective zone of exploitation becomes an annular ring centered at the location of the exploiter. The width of this exploitation ring is 12 km, for the above example, and its radius is determined by the intended range of the interrogation. If the intended range is less than the range to the exploiter, the effective zone of exploitation shrinks to zero. For intended interrogations at longer ranges, the radius for the annular zone of exploitation is equal to the intended-interrogation range minus the range delay to the exploiter minus the equivalent range delay through the repeater itself. The dependence on the range delay through the repeater forces the enemy to use a continuous-repeater amplifier such as a TWT. The enemy has no knowledge of the specific time or direction of a given interrogation and the duty factor of the interrogation signal can be extremely low. The output of the enemy TWT repeater in the absence of an interrogation is high-power noise. This makes the enemy exploiter very vulnerable to detection and attack by friendly forces. It must also be remembered that the effective zone of exploitation is not under the exploiter's control and only occasionally does it coincide with the location of friendly forces. Thus repeat exploitation is not a severe threat because the time-synchronized approach results in an effective code-validity interval limited by clock errors and not by the maximum range of the system.

If clocks are available with accuracies sufficient to support the concept of selective interrogation by range, then the concept of range measurement at the interrogatee can also be supported. This concept allows the interrogatee to measure the approximate range to each active interrogator. This if of little value to the interrogatee unless he receives additional information defining the weapon type at the interrogator. This weapon information, coupled with range measurement and selective interrogation, can form a sufficient basis for making an automated decision to reply or not.

If the measured range (to the interrogator) is well beyond the weapon range, the appropriate decision might be not to reply, particularly if the aircraft is over enemy territory where electromagnetic radiation of any sort can be hazardous.

Implementing a range-measurement scheme is not difficult. If the interrogation pulse for range measurement is sent at the prescribed time of day, it arrives at the interrogatee with a propagation delay commensurate with the range between the two parties. The interrogatee simply opens a receive gate at the prescribed time of day and measures the range delay to each interrogator. The width of this receive gate is set by the maximum range of the system (1 ms for 300 km). The uncertainty of the measurement is limited by the clock error at both terminals ($\pm$6 km for $\pm$10 μs error). This is not a very precise measurement of range, but it should be adequate for making the reply decision, and as improved clocks become available, the accuracy of this range measurement can be increased without involving a major redesign of the system.

The next question is how to send the few bits of information necessary to define the weapon at the interrogator. If this information is sent at a prescribed time of day exactly as the range-measurement pulse was sent, the interrogatee knows precisely when to expect the data pulse, independent of both range and clock error, provided his position has not changed appreciably between the previous range-measurement pulse and the current data pulse. This knowledge of the precise time of arrival of the data allows the interrogatee to set up an extremely narrow receive gate for the reception of this data. The width of this gate is related to the time resolution of the system, which might be on the order of 100 ns for an instantaneous bandwidth of 10 Mhz. Such an extremely narrow gate minimizes the risk of partial-time jamming.

Accurate-time synchronization can also be used advantageously in the reply signalling. The same spread spectrum techniques of frequency hopping, time jitter, and a different intrapulse spreading code on each transmission can be incorporated to achieve covertness and jam resistance on the reply. In order to take advantage of these techniques the exact characteristics (frequency hop, time hop, and PN code) must be known in advance to all friendly participants with synchronized clocks. This means that there need not be an exact one-to-one relationship between interrogations and replies. Multiple simultaneous, valid interrogations of an aircraft would result in a single reply at the prescribed, pseudorandom time, frequency, and PN code. This single reply would be available to all friendly interrogators whether they actually interrogate or just listen with their antenna aimed in the

direction of the replying aircraft. This is consistent with the concept of an automated decision process at the aircraft before a reply is made, and results in a number of interesting operational modes.

If the aircraft is subject to severe jamming it might, under pilot option, go into a mode of irregular, unsolicited replies. Each unsolicited reply would have the identical spread spectrum characteristics of a normal reply at that specific time and would be available to all friendly interrogators with synchronized clocks. The pilot might elect this option if he was severely jammed and over friendly territory where the risk of fratricide might be high. He might even be instructed to go into this mode over friendly territory so that all interrogators could remain silent without revealing their positions. The pilot might even elect a continuous-reply mode at every possible pseudorandom reply time. This could perform the function of an emergency beacon if the pilot has to ditch the aircraft. Even in this mode the signal would include pseudorandom time hopping, frequency hopping, and a different spread spectrum code on every transmission. Thus even the emergency-beacon mode would be difficult for the enemy to intercept and exploit.

Clock updating is a major concern in the design of any system requiring accurate-time synchronization. Eventually free-running clocks will drift outside the acceptable limits and require time updating. An aircraft mission time is fairly short and clock update information could be supplied just prior to or just after take off. The real problem for the aircraft is maintaining adequate time synchronization in the severe aircraft environment. Although not trivial, this problem can be addressed in the design and development of an airborne clock.

The ground-interrogation equipment associated with a Short-Range Air Defense (SHORAD) weapon system does not have the luxury of returning to a base for time calibration and update after each mission. Any viable IFF system must be designed to accommodate somewhat inferior clock synchronization for the SHORAD weapons systems, and clock update information should be automatically provided to these weapons systems as part of the normal reply signalling. This can be done based on the assumption that the clock in the aircraft is generally more precise than the one at the SHORAD interrogator. Thus the friendly aircraft can act as a portable secondary time standard for updating the SHORAD clocks.

The automatic-clock-update approach is based on a reply containing at least two pulses. If one pulse is sent at the prescribed pseudorandom reply time, it will arrive at the

interrogator after the appropriate range delay. The ground interrogation equipment knows the pseudorandom time that the pulse was sent and measures the apparent range delay relative to his clock. The term "apparent range delay" is used because it includes the relative clock error between the terminals as well as the true propagation delay. The second pulse of the aircraft reply is sent advanced or retarded from a prescribed pseudorandom reply time by an amount equal to the apparent range delay that the aircraft has measured for that interrogation. This offset reply pulse arrives at the interrogator after the same propagation delay as the previous pulse, provided the aircraft has not moved significantly since the previous pulse. The arrival time of this pulse, relative to the prescribed pseudorandom time at the interrogator, is exactly twice the propagation delay to the aircraft, independent of clock error at either terminal. Thus one reply pulse provides precise-range information while the other provides apparent-range information. This allows the SHORAD terminal to determine its clock error relative to the more accurate aircraft clock. This information can be collected, averaged, and eventually applied as an update to the SHORAD clock. It should be pointed out that an aircraft can provide clock update information for only one SHORAD at a time, and it is important that the SHORAD check for consistency in clock-update information before actually making a correction to the clock.

Precise timing allows the reply signalling to include additional information such as the specific tail number of the replying aircraft. This information would help the SHORAD equipment sort out enemy tag-along spoofers who simply repeat the reply signal from a friendly aircraft. The SHORAD equipment can easily recognize that the two replies give the same tail number, and the weapon operator can be alerted.

The basic IFF signalling scheme is shown in figure 3. All time is divided into interrogation periods followed by reply periods. Whenever an interrogation is initiated it will be accomplished in the next available interrogation period. The IFF responder listens at appropriate times during each interrogation period and collects the information to determine the validity and identity of the interrogation as well as its applicability to the specific responder. The responder evaluates this information and replies in the period immediately following the interrogation if a decision to reply is made. The interrogator then evaluates the reply information and either reinterrogates or makes a final determination of Friend, Spoofer or Enemy.

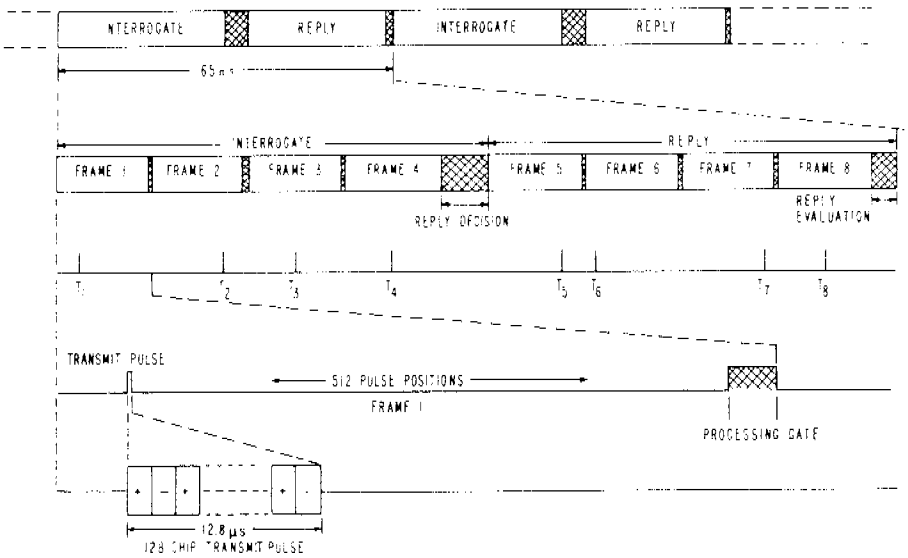

Figure 3. IFF Signalling Format

The interrogation and reply periods are each divided into four frames of about 8 ms each. The actual signalling consists of a short burst of RF energy 12.8 μs long in each frame. The specific transmission time within each frame is pseudorandomly determined from 512 possible time slots. The remaining time in each frame is used for signal processing in preparation for the next frame. The actual 12.8 μs transmission is phase modulated with 0.1 μs chips. Both the chipping code and the carrier frequency are pseudorandomly selected on each transmission. There are 64 carrier frequencies for a total frequency hop bandwidth of 640 MHz and there are 128 different chipping codes. The combination of time hopping, frequency hopping and spread spectrum coding results in a processing gain of 66 dB. This provides the basis for a system which is hard to detect, virtually unexploitable and difficult to jam.

The above discussion has highlighted certain aspects of a new IFF scheme based on accurate-time synchronization. The details of this approach are presented in a paper which was published in the September 1980 issue of the IEEE Transactions on Communications.[1]

TACTICAL CLOCKS

The entire concept of a time synchronized IFF system evolved out of the need to provide an "effective code-validity interval" (selective interrogation zone) which was much shorter than the maximum propagation delay of the system. If a minimum unambiguous range of 150 km is needed; the effective code validity interval should be much smaller than 500 μs. The range-measurement accuracy and the exploitability of the system both improve as this effective interval is reduced, but the clock accuracy required becomes increasingly stringent. Requiring a clock precision better than 1 μs is not realistic for tactical weapons, even with atomic clocks. A nominal system accuracy of $\pm$ 10 μs was selected as being the least stringent specification capable of providing substantial ECCM improvement. The concept developed in Reference 1 included a special mode which would allow SHORAD interrogators with degraded clocks to continue functioning and receive automatic clock updating until their synchronization degraded beyond $\pm$ 100 μs. A remaining question is the availability of practical, inexpensive clocks that provide the requisite performance in the tactical environment.

At this point we must distinguish between a precision oscillator and a precision clock. The precision oscillator is a device whose output frequency is extremely stable as a function of time and environment. The precision clock incorporates a precision oscillator and count-down circuits to provide an extremely accurate indication of time of day. Intermittent operation of a precision oscillator is acceptable provided the output settles down to the proper frequency within a reasonable time. Intermittent operation of a precision clock is totally unacceptable, even if the basic oscillator within the clock is extremely accurate and quickly settles down to the proper frequency, because its time indication is useless until its readout is synchronized with an adequate external standard.

The traditional appproach to precision clocks since 1760, when Harrison invented the first chronometer, has been to never shut the instrument off and never re-set the read out. Current readings are compared periodically with a time standard, and a running tabulation of the error is dutifully kept. A long history of performance is thus developed which not only builds confidence but provides useful interpolation prior to the next check with a time standard. The resynchronization approach is less reliable because the benefit of a long history is lost. Furthermore the setting of time rate or frequency is a difficult task, requiring a significant history of performance. Setting the hands of a pendulum clock is quick and easy, but setting the rate (pedulum length) requires days or even months, depending on the accuracy desired.

The only real candidates for the precision oscillator in a tactical clock are the cesium-controlled oscillator, the rubidium-controlled oscillator, and the quartz crystal oscillator. Both cesium and rubidium rely on the extreme stability of an atomic resonance phenomenon. Although the rubidium and cesium resonances were both demonstrated in the 1950's, the cesium device has dominated for absolute-frequency-standard applications. The cesium device is a primary standard whose output frequency can be accurately predicted from measurements of fundamental parameters such as pressure, temperature, and axial magnetic field. The rubidium device is a secondary standard because the accuracy of this predictive process is less precise than that of the cesium device. In practice, the frequency of a rubidium-controlled oscillator is trimmed, after manufacture, to the frequency of a primary standard. The quartz crystal oscillator relies on the mechanical resonance of an accurately machined quartz plate and its fundamental accuracy and long-term stability are inferior to that of the atomic oscillators. The quartz crystal oscillator has not been considered as a primary frequency standard for half a century, but the extensive history and success of this device as a very stable working oscillator still make it a candidate for an extremely stable, if not precision, clock.

The cesium-controlled oscillator is designed as a primary frequency standard and, as such, achieves the ultimate in performance. However it is extremely expensive ($26,000 to $30,000), it is heavy (70 pounds), and it is not designed to function in a tactical environment.

The rubidium-controlled oscillator is a much smaller device. One company (Efratom of California) is producing a unit for tactical military aircraft that is approximately 4" x 4" x 5" and costs about $6,000. This company is currently developing a smaller unit (2 1/4" x 3 1/2" x 4") for a tactical aircraft communications system[2]. This unit is expected to cost approximately $3,000 in large quantities. It is certainly a candidate for the oscillator in any tactical clock[3].

Some recent advances in quartz crystal oscillator technology make this device an interesting candidate. In particular, the new SC cut provides excellent spectral purity, low aging rate, and less sensitivity to vibration. These units are small (< 13 cubic inches), light (0.7 pounds), low-power (< 2W), and inexpensive ($750); but they do not have the fundamental accuracy or long-term stability of the atomic oscillators.

Frequency stability and long-term frequency drift are dominant factors in the choice of an oscillator for a accurate tactical clock. Frequency drift is a more or less random function and its

cause is not well understood. It can vary markedly from one time interval to the next and from unit to unit. If this were not so, then frequency drift could be modeled and its deterministic effects removed. In a sense the drift specification of an oscillator is simply an upper bound on long term, unexplained effects, and there is no guarantee that the drift function is either smooth or monotonic.

Figure 4 is a simplified extrapolation based on the frequency-drift specification of one of the best double-oven crystal oscillators on the market. The drift specification is less than 1×10^{-10} per day after a 30 day warmup. The unit sells for about $1800, consumes about 2.5 W of input power, and fits in a package 2 3/8" x 3 3/16" x 5". The dotted curve indicates that the nominal IFF system accuracy of $\pm$ 10 μs could be maintained for the first 1.5 days without clock update and the degraded limit of $\pm$ 100 μs could be maintained for about 5 days. The solid curves indicate the extrapolated performance with daily clock updates. After 5 days a clock update every day would be essential, and after 12 days the clock update interval would have to be less than 1 day even for the degraded mode of operation.

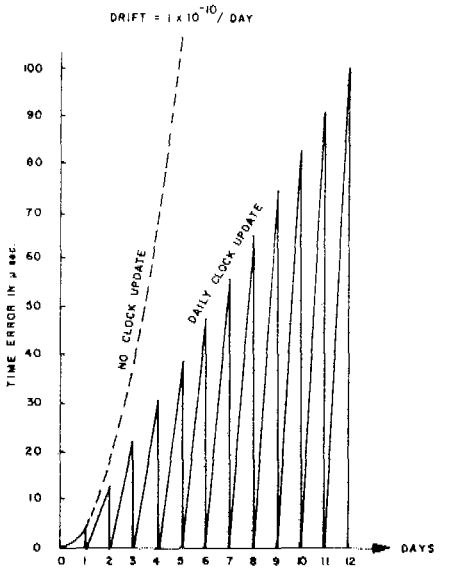

Figure 4. Crystal Oscillator Drift

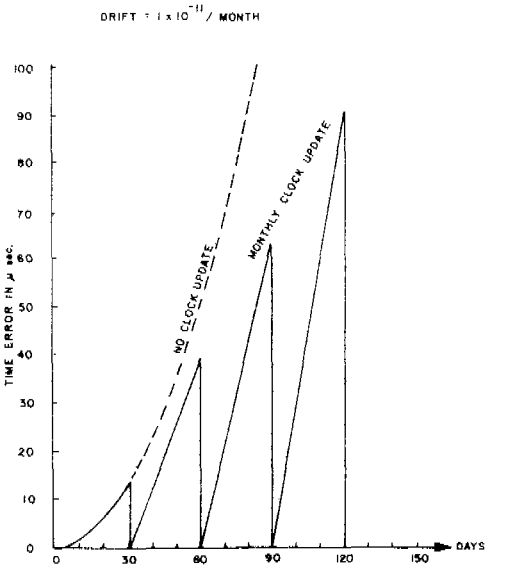

Figure 5. Rubidium Oscillator Drift

Figure 5 is a similar extrapolation for a small rubidium-controlled oscillator with a frequency drift specification of 1×10^{-11} per month. This unit sells for about $6000, consumes 13 W of power, and fits in a package approximately 4" x 4" x 5".

The dotted curve indicates that the nominal accuracy of $\pm$ 10 μs could be maintained for nearly 1 month without clock update and the degraded limit of $\pm$ 100 μs could be maintained for nearly 3 months. The solid curves indicate that operation within the degraded limit could be extended to better than 4 months if clock updates were obtained as infrequently as once per month. The performance of the crystal oscillator is marginal, at best, for the IFF application, and there is certainly no latitude for degraded performance in the tactical environment. On the other hand, the performance of the rubidium-controlled oscillator is clearly superior, and considerable latitude is available for degraded performance in the tactical environment.

Commercial cesium frequency standards have a long term frequency drift specification of 3×10^{-12}. This is better than the performance of the rubidium-controlled oscillator and should certainly be adequate for the IFF application, but its size, weight, and cost make it practical only as a primary standard at a major base.

Although stability and long-term drift are the dominant factors in the choice of an oscillator for a precision tactical clock, the final decision depends on a number of practical factors as well. The significant parameters of the three candidate oscillators are summarized in Table I.

It is clear from Table I that, unless one is willing to update the clocks very frequently, atomic oscillators will be required. Both the cesium and rubidium oscillators can provide more than adequate stability for the IFF application, but the rubidium oscillator is the only practical choice for a tactical system. The rubidium oscillator has a considerable margin of safety for degraded performance in the tactical environment and, as experience is gained with these units, the system synchronization requirements might be tightened to yield more accurate range measurement and improved ECCM performance.

CONCLUSION

Accurate time synchronization could form the essential basis of a new spread spectrum IFF system which offers substantial resistance to enemy jamming and makes spoofing and exploitation extremely difficult. The compact rubidium oscillator is the only viable candidate for a tactical clock with sufficient accuracy to support this IFF concept. The performance of these compact rubidium oscillators is extremely impressive for their current state of development, but additional production engineering is necessary to guarantee performance in the tactical environment. The application

Table I

Comparison of Oscillator Characteristics

	Cesium	Rubidium	SC Crystal
Aging Rate	3×10^{-12}/mo	1×10^{-11}/mo	1×10^{-10}/day
Aging Rate	4 μs/mo	13 μs/mo	4 μs/day
Warm up	30 min for 1×10^{-11}	4 min for 5×10^{-10}	24 hrs for 5×10^{-10}
		60 min for 1×10^{-11}	30 days for 1×10^{-10}
Retrace After 24 hr Shut Off	7×10^{-12}	1×10^{-11}	1×10^{-9} after 2 hr warmup
Temperature	-40° to 75°C	-55°C to 68°C	-55°C to 60°C
Vibration	MIL-167-1	Not Established Spec = 4×10^{-12}/G	Not specified
Size	9" x 17" x 16"	4" x 4" x 5" or 2 ¼" x 3 ½" x 4"	2.4" x 3.2" x 5"
Weight	70 lb.	4.5 or 2 lb.	2 lb.
Power	43 W	13 W	2.5 W
Cost	$26K	$6K - $3K	$1K - $2K

of accurate-time synchronization is not limited to IFF and its increasing use is expected to revolutionize the whole approach to secure, jam-resistant electronic systems for the military.

REFERENCES

1. W. M. Bridge, "IFF System Concept Based on Time Synchronization," IEEE Transactions Communication, pp. 1630-1637, September 1980.

2. H. Fruehauf, W. Weidemann, E. Jechart, "Development of a Sub-Miniature Rubidium Oscillator for Seek Talk Application," in Proc. 12th Annual Precise Time and Time Interval (PTTI) Applications and Planning Meeting, December 1980.

3. N. Houlding, "Clocks for Airborne Systems," Proc. 13th Annual PTTI Applications and Planning Meeting (this issue).

QUESTIONS AND ANSWERS

DR. STOVER, Defense Communications Agency

My question really doesn't have to do with the clocks themselves, but back to your figure that showed the four frames. Have you looked into the possibility that the enemy having captured one of these devices could gain considerable information even though he didn't know the code from the information in those four frames just as when the pulse was received and so forth?

Aren't you perhaps giving him information even though we can't get the code?

MR. BRIDGE:

I don't think so. I think what we've done is we've put all our eggs in the basket of the cryptographic key. As long as he has a valid key, he can use the system exactly as we would. If he captured one, he could certainly use it the way we would. And, now, the problem boils down to: Can he deduce the performance of the box externally without knowledge of that key. And I think that's a NSA problem, and they feel that he can't.

DR. STOVER:

Let me ask one more extrapolation. I interpreted that only a couple of those frames actually were coded. Are you saying all eight of them are coded?

MR. BRIDGE:

I failed to mention that. Let me explain a little bit more. The signal in each frame is hopped in time pseudo-randomly. It's hopped in frequency pseudo-randomly over 600 megahertz and it's hopped in spread-spectrum coding over 128 chips. Each pulse is different in all three parameters, and it really makes it looking for a needle in the haystack for the enemy to try to even find that signal, let alone exploit it.

Okay.

DR. STOVER:

That answers the question. Thank you.