

Security for Insecure Times

Geoencryption with Loran

Nov 1, 2007

By: [Di Qiu](#), [Sherman Lo](#), [Per Enge](#)

GPS World

Location-based encryption can prevent stolen data from being decrypted outside a particular facility. Modernized Loran, hard to spoof and hard to jam, with good repeatable position accuracy and signal availability, shows strong potential for securing sensitive data.



The emergence of the Internet and personal computers has produced unprecedented information content and access and placed volumes of data at practically anyone's fingertips. While the spread of such technology has increased efficiency and knowledge, it has also made information theft easier and more damaging.

One common form of information theft is the unauthorized copying and distribution of copyrighted material. Today, one can obtain pirated versions of the latest movies, often before release, by making a quick visit to a file-sharing network or a less-than-reputable shop. Surprisingly, the pirated material often comes from Hollywood insiders, such as the employees of the post-production shop, or individuals who receive pre-release screener DVDs.

Theft of equipment containing sensitive or valuable information has also become widespread. Laptops containing personal information such as social security numbers, personal financial information, credit-card numbers, and so on make attractive targets. These thefts can happen in the most surprising places. Qualcomm CEO Irwin Jacobs left his laptop unattended for a few minutes to field questions from a business audience after a speech — and it disappeared.

These emerging problems have stimulated interest and significant growth in the field of information security. Geoencryption or location-based encryption furnishes a means to enhance security, and is suitable to these two scenarios, digital film distribution and laptop security.

The terms geoencryption and location-based encryption refer to a security algorithm that limits the access (decryption) of information content to specified locations and/or times. More generically, the restriction can be based on any set of navigation parameters. The algorithm does not replace any of the conventional cryptographic algorithms, but instead adds an additional layer of security.

In its basic form, location-based encryption can ensure that data cannot be decrypted outside a particular facility. Any attempts to access the secure information at an unauthorized location will result in a failure of the decryption process. For example, a digital movie file can only be decrypted inside the theater to which it is sent. In the scenario of laptop security, the valuable information on the laptop or hard drive can be encrypted so that it can be accessed only at the laptop owner's home or office. The theft of such data has the potential of jeopardizing personal and national security.

Geocryption increases security by augmenting current cryptosystems, such as passwords. Even today, many people do not employ very strong passwords. Eight-character passwords of mixed numbers and letters can be recovered within 60.5 hours on supercomputers that have a speed of 1 billion passwords per second. Even with very strong passwords, geocryption provides extra security because it prevents authorized users from accessing sensitive data at unsecured locations.

Digital Film Distribution

Logan Scott, Dorothy Denning, and colleagues at Geocodex proposed and developed the idea of geocryption for digital film distribution. **FIGURE 1** shows a modified version of the system. A content provider (sender) distributes the encrypted film (cipher text) to an authorized user (recipient). This is done via many methods such as satellite data links and, as such, may be readily available to unauthorized users.

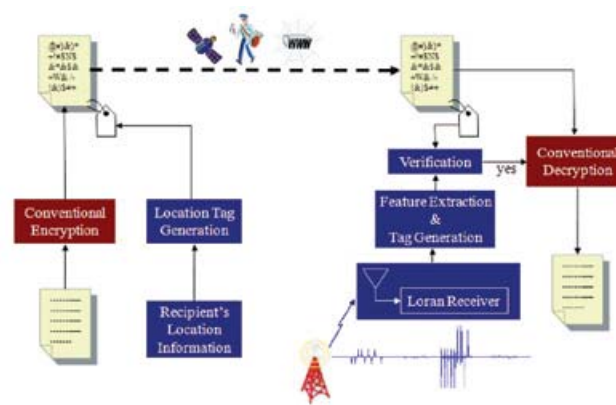


Figure 1 Geocryption overview

Films encrypted using the geocryption protocol can be decrypted only at a specified location (theaters). That means that the decryption process should fail and not reveal information about the plaintext if there is an attempt to decrypt the data at another location. This should be true whether it is by an authorized or unauthorized user. Therefore, the geocryption algorithm can be used to ensure that film cannot be retrieved, except at the theater by authorized personnel.

Traditional encryption is an integral part of the system. The sender encrypts the data file or plaintext using a conventional cipher with a random key. A location tag (geotag) is derived from specific user location- (and time-) dependent parameters and generated by mapping the recipient's location information into binary bits.

The recipient should have three channels to receive information: a data receiver to capture a digital-encrypted data file; a navigation receiver to receive radio frequency (RF) signals, whose location-dependent parameters are needed to generate the geotag; and a third channel for secure key exchange. Once the geotag is computed from received navigation signals, it is compared with the received location tag. Identical geotags indicate correct location. If the location verification is bypassed, the decryption process is performed using the right random key and received encrypted data file.

Loran Case Study

The most important required feature of a navigation signal is its ability to generate a strong geotag. The strength of the geotag is determined by the quantity and quality of location-dependent signal parameters. By quantity, we mean the number of different location-dependent parameters that can be generated. By quality, we mean that amount of unique location-dependent information provided by each parameter. The information content is

related to the spatial variation of the parameter. Greater spatial variation results in more unique information. By having many parameters each providing its unique information content, we can generate a strong geotag.

At the same time, the parameters should be relatively insensitive to temporal changes that weaken the uniqueness of the information. Temporal variations essentially reduce the uniqueness of the location-dependent information. As a result, repeatability and repeatable accuracy are desirable qualities. It allows a recipient to provide his location-dependent parameters, or the derived geotag, to the sender at one time — and still have those parameters valid at a later time. In other words, the signal characteristics should be consistent enough so that when the recipient is ready to decrypt, measurements at the same location will yield the same previously generated geotag.

Several other features are highly desirable. First and foremost, the signal should have anti-spoofing capabilities. If the signal is vulnerable to spoofing, it may be possible for an adversary to bypass the location check and decrypt correctly. Furthermore, it is desirable that the signal be available indoors, where many of the anticipated applications of geoencryption will likely occur. This includes applications such as the management and distribution of secure digital data. Often, it is good if this data is only accessible inside certain building(s).

Loran Potential. Loran is a terrestrial, low frequency, pulsed navigation system that operates in much of the northern hemisphere. It has many properties useful to geoencryption, and it is being modernized to a next-generation system known as enhanced Loran (eLoran) which will have additional capabilities that can facilitate geoencryption.

Loran uses static transmitters and, as a result, there are many parameters that are location-dependent. Each parameter offers different amounts of information or potential information density. Parameters with higher density result in higher security levels. This is important, as the security strength of the geotag is derived from the information used to generate it. A combination of various parameters, as well as increased accuracy of these parameters, increases the security strength. Signals from static transmitters may have many location-dependent characteristics or parameters. The possible useable Loran parameters are time of arrival or time difference of arrival (TOA/TDOA), envelope to cycle difference (ECD), absolute or relative signal-to-noise ratio (SNR/SNR), signal strength measured at the third zero crossing, and shape of the envelope.

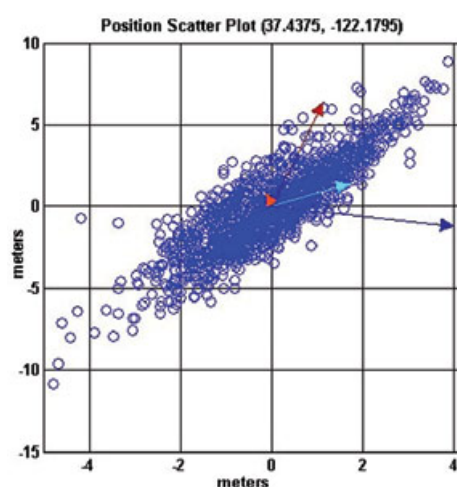


Figure 2 Loran position scatter plot

Loran has good repeatable position accuracy, which benefits the design of the geotag. The repeatable accuracy specified by United States Coast Guard (USCG) is 60–300 feet (18–94 meters). A set of data collected for several hours at Stanford University on January 8, 2006, illustrates the repeatable accuracy (**FIGURE 2**). The position error in the east-west direction is less than 10 meters, and the error in the north-south direction is less than 25 meters.

A high-power, low-frequency signal, Loran is hard to spoof and hard to jam. Furthermore, the signal can reach places such as urban canyons and indoor environments, where reception of a line-of-sight signal such as GPS is difficult.

Finally, enhanced Loran has a data channel that can carry authentication and time messages. Both features are important to the authentication scheme proposed for Loran. An authentication message provides verification of the source of the Loran signals, and a time message helps synchronizing the user and the Loran transmitters.

Information Measure

Once the location-based parameters are chosen for geoencryption, it is important to examine properties of these parameters. Location-based parameters can be extracted from the conditioned and digitized signals and computed to a geotag using a particular key-generation algorithm. The feature extraction and key-generation algorithms are integrated with location devices. When implemented, the integrated device should be tamper-resistant; one should not be able to extract information from the device.

A basic requirement of a geoencryption system is the need to distinguish users at different locations. Not only must we have the ability to distinguish, we also must have significant differences in the location-based information from different locations. This is so that the geotag from one location cannot be easily guessed, even with information from a nearby location. There are two basic criteria for parameters of interest:

- **Uniqueness.** Can a user be distinguished based on this parameter? The feature must vary to a reasonable extent to achieve a strong geotag.
- **Stability.** How permanent is the parameter? The feature must vary as little as possible to achieve a stable geotag.

The information content of location-based parameters should be measured and examined based on these two requirements. Information entropy is a measure of information density within a set of values with known occurrence probabilities. Spatial entropy is an indicator for quantitative information capacity of each location feature. High spatial entropy indicates a large potential value space and provides a large size of geotag. Technically speaking, spatial entropy can be estimated only based on the potential information capacity of location features. However, practically, if an attacker knows an authorized user's location, an active attack can be performed, and the effective spatial information capacity will be reduced.

Uniqueness of a feature for geoencryption is quantified using spatial decorrelation. Spatial decorrelation is a measure of variations of features over different locations. For features with low spatial decorrelation, it can be expected that users in different locations will result in similar or identical values. Higher decorrelation value helps provide more uniqueness to the geotag for users at different locations. Therefore, larger spatial decorrelation results in stronger geotag and a higher security level of the system.

Temporal entropy is used as a metric to measure the time stability of location-based parameters. Feature variation reflects instability or degree of scatter within a particular parameter at a given location. For geoencryption, feature stability or low temporal entropy is a fundamental requirement. If a feature has large temporal variation, there is a probability that the geotag generated for decryption is not the same as the one for encryption for an authorized user. Many factors can result in temporal entropy. Some are related to the receiver or algorithms employed. Proper design can eliminate these variations. Others are related to propagation and changes in the environment.

Spatial entropy, spatial decorrelation, and temporal entropy are somewhat correlated. High temporal entropy will result in a reduction in spatial entropy and decorrelation. Therefore, the effective geotag length depends on all these metrics. Ideally, high spatial entropy and low temporal entropy are desired.

System Attributes

Performance and robustness to circumvention are two important attributes to consider for the geoencryption system. Performance, the ability of the system to function as designed, means providing access when authorized and denying access when unauthorized. In geoencryption, circumvention is associated with the ability of foolproof location-based parameters. This capability makes it difficult for attackers to circumvent or break the geoencryption process.

Performance Analysis. Geoencryption systems make two types of errors: mistaking the measurements from two different locations to be from the same location, called false accept; and mistaking the measurements from the same location to be from two different locations, called false reject. Both false accept rate (FAR) and false reject rate (FRR) depend on the accuracy of the receiver and the interval size chosen to quantize the continuous location

features. These two types of errors can be traded off against each other by varying the interval size. A more secure system aims for low FARs at the expense of high FRRs, while a more convenient system aims for low FRRs at the expense of high FARs. The desired interval size is highly dependent on the final application.

The parking-lot attack (FIGURE 3) represents one scenario. Since there is no physical boundary to distinguish authorized user and attacker, an attacker can achieve a right geotag by staying close to the user, for instance, in a parking lot. This approach relies on a probabilistic mapping from the user's location. The variance of the feature depends on its accuracy, which is determined by noise, environment, and devices. The interval size is chosen to quantize the parameter and allow some degrees of variation.

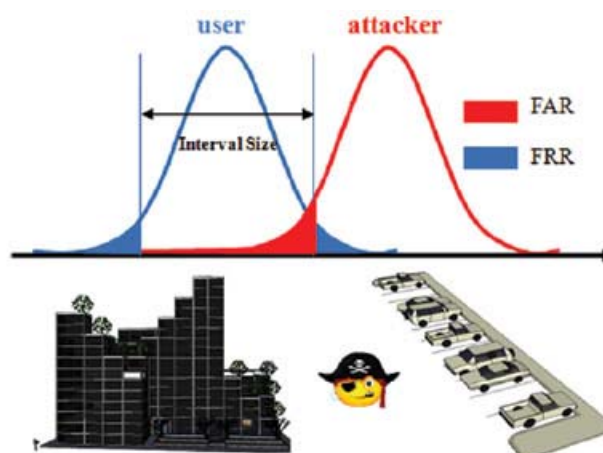


Figure 3 Parking-lot attack

We examine the system performance based on the parking-lot attack and assume the noise is Gaussian distribution. The location feature, TDOA, is used as an example to illustrate this scenario; hence, the horizontal axis in Figure 3 can represent TDOA measurements. The TDOA measurements were collected in a parking structure at Stanford University. Two test locations were chosen and the separation between these locations is approximately 70 meters. The measurements were collected for one hour at each test location.

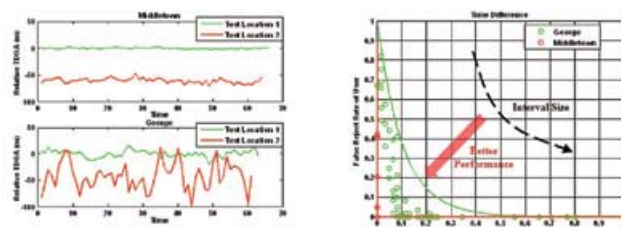


Figure 4 TDOA measurements and receiver operating characteristics

Performance capacity can be shown in the form of the receiver operating characteristics (ROC) curve, shown on the right of Figure 4, in which the FAR is plotted versus the FRR with various interval sizes. The ROC curve is used to distinguish an authorized user and an attacker statistically. The solid curves are analytical values that provide an upper bound, while the dots indicate the experimental results of the FAR and FRR values. As expected, increasing interval size improves user performance as well as the attacker's probability of obtaining a correct geotag. Ideally, we need both FAR and FRR as low as possible. The ROC curve shifts towards the origin as SNR increases. This indicates higher SNR results in better user performance and higher security level.

Practically speaking, there is no perfect protection. However, the system is designed to make the FAR as low as possible, and forgery attempts as costly as possible.

Signal Authentication

The main concern of geocryption is that location features can be forged. An attacker or imposter can simulate RF signals to spoof a receiver and pretend he is an authorized user. To protect against forgery of RF signals, signal authentication is applied on Loran.

The purpose of geoencryption is to provide security to the transmission of information. As such, it is important that every link in the geoencryption chain is secure. This includes not only the protocol itself, but also the broadcast of an RF signal. The security of the RF navigation signal is provided by message authentication to verify the source of the data and messages. One goal is to prevent the user from being fooled into believing that a signal and its message come from a particular source when this is not the case. Another goal is to allow the receivers to verify whether the messages have been modified during transmission.

We are studying the use of TESLA authentication on Loran to provide authenticity and improve system integrity. TESLA uses a symmetric authentication mechanism by appending MAC (see sidebar) at the end of each message, which is transmitted from a sender to a receiver, and time (delayed key disclosure) to achieve the asymmetry property required for a secure broadcast authentication. It requires buffering for both sender and receiver sides, but the receiver can authenticate the message as soon as enough messages, keys, and MACs are buffered.

We have designed and tested a preliminary implementation of TESLA on Loran. The message design conforms to the ninth pulse modulation format being proposed for eLoran. The proof of concept design has been tested using the Loran station at Middletown, California. We are currently working on trying to make sure that the bandwidth usage on ninth pulse is such that it can support TESLA along with all the other required messages.

Middletown broadcasts both time and authentication messages. The time message is generated by the United States Coast Guard (USCG) to test the performance of ninth pulse modulation. Stanford University generates the authentication messages to verify authentication performance and demonstrate geoencryption protocol. The time and authentication messages are broadcast alternatively; 50 percent bandwidth is obtained for authentication messages. With only one secondary station carrying data message, a data rate of 50 bits/second is achieved.

The authentication message consists of the key and the MAC, and results in a total length 320 bits. With a 41-bit payload in Loran messages, at least eight messages are needed to carry a complete authentication message. Subtypes are used to help the receivers distinguish the MACs and keys in authentication messages. The data type for an authentication message is 0011. Subtypes 1 to 4 are for identification of MACs and subtypes 6 to 10 are for keys. Subtype 5 consists of a 12-bit MAC, a 13-bit padding, and a 12-bit key. A total of 10 messages are needed to carry one TESLA packet, and it takes 23.856 seconds to transmit these messages via GRI 9940. For testing purpose, only three key and MAC pairs were generated and broadcast periodically.

Basic Cryptographic Concepts

The basic goal of encryption algorithms is to transmit some data, termed the *plaintext*, in such a way that it cannot be recovered by unauthorized agents. This is done by using a cryptographic key and algorithm to convert the plaintext into encrypted data or ciphertext. Only authorized agents should be able to convert the ciphertext back to the plaintext. There are two general types of key-based algorithms: symmetric and asymmetric (or public-key). In most symmetric algorithms, the encryption key and the decryption key are the same. These keys are often called session keys.

Authentication is another important concept in cryptography. It allows the receiver of information (such as data or decryption key) to ascertain its origin. While authentication is not necessarily used in encryption or decryption protocols, it is often necessary for ensuring that the information is being received from the proper parties. In regards to geoencryption, verification of the signal origin and hence the source of the navigation information is vital to prevent spoofing. Hence, we will discuss providing signal authentication later in this article.

A message authentication code (MAC), also known as data authentication code (DAC), is a one-way function with the addition of a key. One-way functions are relatively easy to compute, but significantly harder to reverse. The MAC output is a function of both the input and the key. Unlike encryption, authentication does not hide the plaintext, but tags the MAC at the end of the plaintext for the recipient to verify whether the plaintext has been modified during distribution.

Basic Cryptographic Concepts

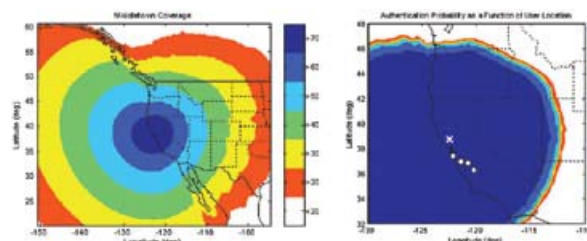


Figure 5 Middletown authentication performance

collected at different locations to test the Middletown authentication performance. The five test locations appear as white dots in **FIGURE 5**. The contour plot on the left indicates the

TESLA performance depends on the SNR of the performance of modulation technique and authentication bandwidth. A matched filter model in the presence of noise for the receiver processing of the signal is used to analyze the performance. Data was

signal strength of Middletown while the plot on the right represents the probability of authentication as a function of user location estimated analytically based on the signal strength. Loran data was successfully authenticated in all five locations.

Conclusion

Geoencryption allows data to be decrypted at a specific location. The protocol provides protection against location bypass. With proper implementation of signal authentication, the protocol provides strong protection against location spoofing.

While location-based encryption appears to be well suited for applications such as digital film distribution or laptop security, the important technical and system challenges must be further investigated. A poorly implemented geoencryption system can give users a false sense of security, leading to complacency. On the other hand, a well-implemented system can provide the necessary security safeguards for protecting valuable information from would-be attackers.

Acknowledgments

The authors would like to thank Mitch Narins, FAA Loran Program Office, for supporting this effort; Logan Scott and Daniel Boneh for advice and suggestions; Symmetricom and Greg Johnson at Alion Science and Technology for data-collection equipment and data; and Lt. Kirk Montgomery and the USCG for supporting the Middletown tests.

Manufacturers

The data-collection setup includes an **Locus** *E-field* antenna, a **LRS IIID** Loran receiver, a **Symmetricom** *Enhanced Loran Research Receiver (ELRR)*, and a laptop to log TDOA data from the receiver.

DI QIU is a Ph.D. candidate in aeronautics and astronautics in the GPS Research Laboratory, Stanford University. Her research interests are geoencryption and signal authentication.

SHERMAN LO is a research associate at the Stanford GPS Research Laboratory, and associate investigator for the Stanford University efforts on the Department of Transportation's technical evaluation of Loran. He received his Ph.D. in aeronautics and astronautics from Stanford.

PER ENGE is a professor of aeronautics and astronautics at Stanford, where he is the Kleiner-Perkins, Mayfield, Sequoia Capital Professor in the School of Engineering. He directs the Stanford GPS Research Laboratory. He received the Kepler, Thurlow, and Burka Awards from the Institute of Navigation, and his Ph.D. from the University of Illinois.