Security Analysis of Geoencryption: A Case Study Using Loran

Di Qiu, *Stanford University*

BIOGRAPHY

Di Qiu is a Ph.D. candidate in Aeronautics and Astronautics working in the Global Positioning System (GPS) Laboratory, Stanford University. Her Research interests are geoencryption and signal authentication. She received a B.S. in Aerospace Engineering from UCLA and a M.S. in Aeronautics and Astronautics from Stanford University.

ABSTRACT

The term "geoencryption" or "location-based encryption" refer to a security algorithm that limits the access or decryption of information content to specified locations and/or times. The algorithm does not replace any of the conventional cryptographic algorithms, but instead adds an additional layer of security. Loran is chosen as a case study to implement geoencryption due to its many properties that are beneficial to this protocol. Loran's stationary transmitters result in many location dependent parameters. Low frequency and high power signal can reach places like urban canyons and indoor environments. Enhanced Loran can provide a data channel useful for geoencryption.

In order to evaluate the effectiveness of Loran for geoencryption we need to perform two tasks: 1) build a testbed to implement geoencryption protocol, and 2) examine the performance and security of the system.

The prototype of geoencryption demonstration was built and further refinements are needed. To accomplish the second task, a threat model is developed and analyzed using the testbed built in the first task. In this threat model we discussed false positives and false negatives of the system. The signal to noise ratio (SNR) provides as an important metric to judge the performance analysis.

This paper describes the work on analyzing system performance using the designed threat model. In addition, some data collections were done using the geoencryption testbed. This paper also provides a comparison on the experimental results and analytical results.

Keywords: geoencryption, Loran, authentication, security

INTRODUCTION

Traditional encryption is used to provide assurance that only authorized users can use the secure content. However, there are circumstances where the security provided by traditional encryption is not adequate. In many instances, it would still be useful to have an additional layer of security that provides assurance that the secure content can only be used at authorized location and/or time [1]. The concept of location based encryption or geoencryption is being developed for such a purpose. The capability has tremendous potential benefits to applications such as managing classified/secure data and digital movie distribution where controlling access is the predominate concern.

To implement geoencryption, in principle, a device performing the decryption integrates a location sensor and cryptographic algorithms. Different radio frequency (RF) signals were studied and compared. Loran was chosen as a case study due to its potentials to geoencryption. A practical concern for implementing this device is whether it can be made resistant to unauthorized use and "tampering". By tampering, we mean both physical attacks on the hardware and attacks on the implementation such as spoofing. If the device is vulnerable to tampering, it may be possible to for an adversary to modify it and bypass the location check [2]. To protect against spoofing, a signal authentication protocol, Timed Efficient Stream Loss-tolerant Authentication (TESLA) is proposed. We proposed a mean on implementing TESLA on Loran for authentication. Some preliminary results of authentication performance were discussed in our previous paper [3].

This paper further investigates the performance and security of geoencryption protocol. The structure of the paper is as follows. It first gives a brief review on geoencryption and how the protocol builds on conventional cryptographic algorithms and provides an additional layer of security. The paper then describes how we develop a threat model to evaluate the security

performance of the protocol. Some theoretical analysis of threat model performance will be discussed. A data collection was made in a parking structure at Stanford University. The security analysis is evaluated experimentally using the collected data. This paper then provides a comparison between the theoretical analysis and experimental results and concludes with future directions of the research.

BACKGROUND

Geoencryption and Its Application

Geoencryption is the use of position navigation and time (PNT) information as means to enhance the security of a traditional cryptographic system. The information is used to generate an additional security key, a "geotag", that is necessary to access the encrypted data or application.

Possible applications of geoencryption are digital film distribution and data security. In this paper, we will use digital film distribution as an example to explain the concept of geoencryption. The idea of geoencryption and its use in digital film distribution was proposed and developed by Logan Scott, Dr. Dorothy Denning, and their colleagues at Geocodex [1]. The overview of the modified system is shown in Figure 1. This modified system uses geotag as a location verification. Traditional encryption is an integral part of the system. Geotag is derived from specific user location (and time) dependent parameters by quantizing these parameters into grid spaces. The detailed description of geoencryption is discussed previously in [3].

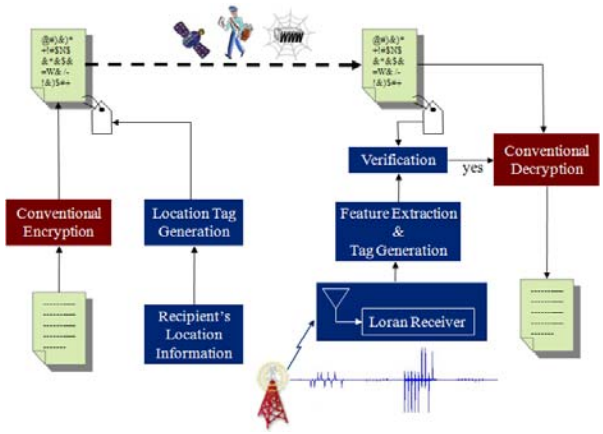

Figure 1: Geoencryption Overview

Under this system a content provider ("sender") distributes the encrypted film (ciphertext) 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. The goal is to provide encrypted films a location tag that is decryptable only at a specified location (theaters) and times. The goal is for the decryption process to fail and not reveal information about the plaintext should there be an attempt to decrypt the data at another location, this should be true whether it is by an authorized or unauthorized user. Therefore, the geoencryption algorithm can be used to ensure that film cannot be retrieved except at the theater by authorized personnel who are located at the specified location.

Signal Authentication on Loran

Loran has many characteristics that can be used to generate a robust geotag. Additionally, it is being modernized to a next generation system known as enhanced Loran (eLoran), which will have a data channel that can benefit its use for geoencryption [4]. The modernization will also reduce the amount of variation in some of the location-based parameters.

The purpose of geoencryption is to provide security to the transmission of information. As such, it is important that every linkage of the geoencryption chain is secure. This includes not only the protocol itself but also the broadcast of RF signal. The security of the RF navigation signal is provided by message authentication. Authentication is about the verifying the source of the data/messages. One goal is to prevent the user from being fooled into believing that a message comes 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 [5].

Adding security in a broadcast communication system is complicated by untrusted or uncertified users and unreliable communication environments. The concern is that untrusted users may employ items such as signal simulator to spoof the system into generating the correct geotag. Source authentication helps the receivers to verify the received data originates from the source and has been modified in transit.

TESLA is implemented to provide the source authentication of the RF navigation signal. TESLA uses symmetric authentication mechanism by appending MAC at the end of each message, which is transmitted from a sender to a receiver, and time (delayed key disclosure) to achieve asymmetry property required for a secure broadcast authentication [5].

Enhanced Loran will transmit data via a data channel, which can be used to carry authentication messages **Error! Reference source not found.**. The current proposal is ninth-pulse modulation. The modulation is chosen to minimize the impacts on the current operational Loran signal. An additional pulse is inserted after the eighth pulse of pulse group of secondary stations [6]. Third-two state Pulse Position Modulation (PPM 32) resulting in 5

bits/pulse is used to change the time delay of the ninth pulse from 1000 microseconds after the eighth navigation pulse.

Under the current proposed ninth pulse communications, each Loran message has 120 raw data bits and consists of a 4-bit header, a 41-bit payload, and 75-bit parity component. This results in a data bandwidth of 37.5%. The Reed-Solomon (RS) codes are used for parity check. This forward error correction (FEC) coding method provides error correction capacity and integrity [7]. It provides to ability to align the message and to verify that the message has been validly decoded with high probability.

Geoencryption Demonstration

The west coast chain of Loran, group repetition interval (GRI) 9940 is used to perform the authentication demonstration. The stations of this chain are Fallon, NV, George, WA, Middletown, CA and Searchlight, NV. Middletown, the closest secondary station to Stanford University, is chosen to implement this authentication scheme to ensure the performance of decoding.

Middletown broadcasts both time and authentication messages. The time message is generated by United States Coast Guard (USCG) to test the performance of 9^{th} pulse modulation. Stanford University generates the authentication messages to verify authentication performance and demonstrate geoencryption protocol. The time and authentication messages are broadcasted alternatively. 50% bandwidth is obtained for authentication messages. Since Middletown transmits on only one rate every 0.0994 seconds, a raw data rate of roughly 50 bits/sec is achieved. This results in one message every roughly 2.4 seconds.

Under TESLA, each segment of the chain consists of a message (m_i), a Message Authentication Code (h_i) and the delayed key (K_{i-d}) for a previous MAC. MAC, message authentication code, is a cryptographic function and is employed in several widely used security algorithms and protocols. The amount of delay, d, is a design parameter. In our proof of concept demonstration, a three segment sequence is used. A broadcast illustration is shown in Figure 2 where the key is delayed by two message/hash segments.

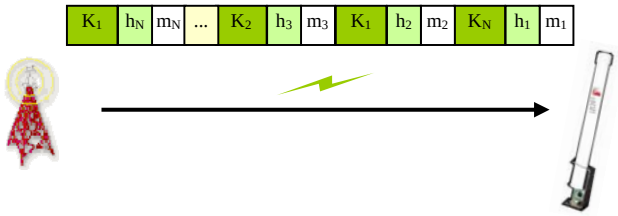

Figure 2: Circular TESLA Chain

The details of the geoencryption and MAC verification are discussed previously in [3]. The software implementation of all cryptographic functions is done in MATLAB.

THREAT MODELS

In the decryption phase, the performance of the Loran receiver plays an important role. The receiver's performance directly affects the performance of geoencryption protocol and its security. The certified Loran receiver integrates the cryptographic functions to perform authentication and conventional Loran receiver to extract location-based parameters. A flowchart is shown in Figure 3 to illustrate how certified Loran receiver works. The integrated device consists of three modules, navigational receiver, authentication module and cryptographic module. The navigational receiver performs functions of signal conditioning, demodulation, and decoding. The authentication module verifies source of the incoming signals. The cryptographic module extracts location-based parameters and maps them into binary bits. Without successfully authenticating the MACs, the user can not move on the next step to extract location-dependent parameters and compute a geotag. We assume the Loran certified receiver is tamper resistant. Someone should not be able to extract any information from the device.

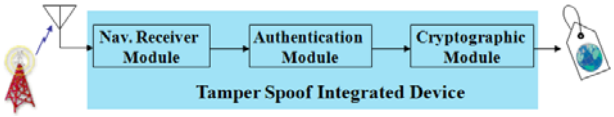

Figure 3: Loran Certified Receiver

The security analysis of a protocol is complicated as there are no standard metrics to precisely quantify the subject of security. To judge the performance and security of the Loran certified receiver, we developed threat models for both authentication stage and geotag generation stage. A threat model should provide possible failure modes due to the availability of the system. Furthermore, a threat model defines all possible attacks that might threaten the system. Whether a given systems is secure or not can depend dramatically on threat model is considered. For the threat model at each stage, we discuss false negatives and false positives.

At authentication stage, a false negative is the case that a user fails to authenticate even though he is inside the authentication coverage area. This depends on the receiver performance and system availability. A false positive is the case that an attacker forges authentication messages and successfully authenticates even though he is outside the authentication coverage area.

At geotag generation stage, false estimate of location-based parameters resulting from errors and biases is used to judge the system performance. A false negative is the case that when the estimated parameter of the user is outside the security range, or the correct grid space, although the real position of the user is inside. A false positive is the case when the estimated parameter of the attacker achieves a correct geotag although the user is actually outside the security range.

AUTHENTICATION THREAT MODEL

Authentication plays an important role in enhancing the system's security. Aforementioned, it allows the user to verify whether RF signal is from a real Loran transmitter and protect against spoofing from attackers. In this threat model, we'll study the factors that have impact on the authentication performance and what these impacts are.

Demodulation Performance

The authentication module in a Loran receiver takes the output or the decoded messages from the demodulation module and performs TESLA verification using the cryptographic functions, as shown in Figure 3. Hence, the probability of authentication solely depends on the demodulation results. There are two important factors that need to be considered when evaluating demodulation [8]: 1) signal to noise ratio (SNR) required for data reception and 2) sky wave and cross rate rejections in a receiver.

Even though sky wave and cross rate interference represent the primary source of interference to Loran, we only consider noise in this paper for simplification. Therefore, SNR is the primary metric we used to judge the signal authentication implementation.

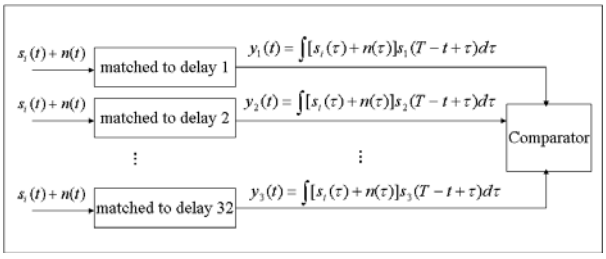

Figure 4: PPM Matched Filter

The performance of demodulation technique in the presence of noise determines the required SNR and signal power necessary to receive data. One demodulation technique to demodulate 9th pulse data is matched filter. A matched filter performs convolutions of a time-reversed version of a reference signal with the input signal. By multiplying the input signal with a time shifted version of the reference signal and integrating the product, the maximum of the integrals is the demodulated symbol [8], shown in Figure 4.

We assume the noise is additive white Gaussian noise (AWGN), and examine the effects of Loran signal in the presence of noise as it passes through the filters. Another assumption is that the filters contribute negligible noise to the signals so the outputs from each of the filters are correlated and the noise variance and covariances can be determined. A 30 kHz noise equivalent bandwidth (NEBW) is used in this matched filter model. We can develop an upper bound on the probability that a sent symbol is not correctly demodulated by a receiver for a given signal to noise ratio [8]. The bound is the sum of the error probability of each incorrectly demodulated symbol, given in equation (1).

Given the following definitions,

$P(y_i > y_j \mid j)$ = probability that the maximum output from matched filter i is greater than that from match filter j given that signal j was sent

F_{norm} = cumulative density function for the standard normal variable

d_{ij} = Euclidean distance between s_i and s_j

h(t) = 30kHz bandpass filter

Therefore, for PPM 32 (M = 32),

$$P_e \le \sum_{j=1,\, j\neq i}^{M} P(y_j > y_i \mid i) = \frac{1}{M}\sum_{i=1}^{M}\sum_{\substack{j=1 \\ i\neq i}}^{M} F_{norm}\left(\frac{\int [s_j(t)-s_i(t)]s_i(t)dt}{\sqrt{\frac{N_0}{2} d_{ij}^{\,2} \int_{-\infty}^{\infty} |h(t)|^2 \, dt}}\right) \quad (1)$$

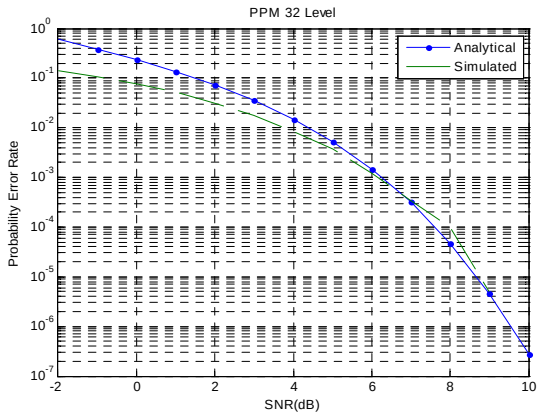

Figure 5: 32-State PPM Probability of Error

Figure 5 shows the error bound for a 32-state PPM as function of SNR along with simulation results. The discrepancy of the analytic and simulated results likely comes from the use of an ideal bandpass filter for the

analytic model and a second order Butterworth filter for the simulation [8].

A packet consists of five raw data bits that a modulated pulse can carry in ninth pulse communications (NPC). The packet loss rate can be determined using the overbound for the probability of bit error. With 45 bit payload and 75 bits parity check for each Loran message, the percentage of message loss can be calculated using Reed-Solomon (RS) coding with an assumption that the packet loss is approximately Gaussian. RS coding is a well-known forward error correction method [7] and used for channels with burst losses. The performance using RS coding can achieved as the following.

$$P(error/decorder\_failure) = \sum_{j=t+1}^{n} \binom{n}{j} p^j (1-p)^{n-j} \qquad (2)$$

The analytic message loss and packet loss rate are plotted in Figure 6. In this plot, message loss is the probability of decoder failure and the different packet loss rate comes from different SNR. We assume independent packet losses.

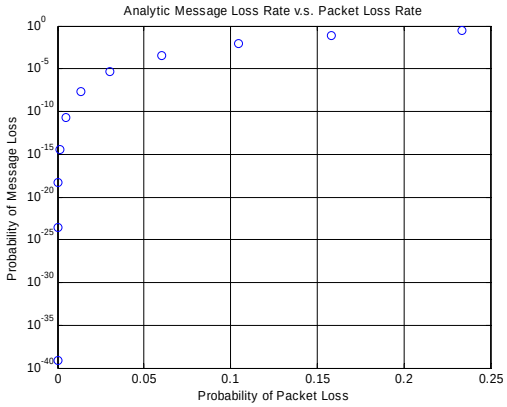

Figure 6: Message Loss vs. Packet Loss Rate

False Negative

False negative measures the probability that a user fails to authenticate even though he is inside the Loran GRI coverage area. The authentication performance primarily depends on the demodulation results. Understanding Loran receiver demodulation scheme and its capacity, the probability of authentication can be analyzed using SNR as a metric. The authentication message consisting of key and MAC is 320-bit long. MAC is generated for data between previous authentication message and the current. With a payload of 41 bits for each Loran message, 9 messages are required to carry one authentication message. Another factor that affects authentication results is the bandwidth allocated to authentication (authentication bandwidth), or authentication data rate. This is an implementation issue. With an assumption that the decode failure of each Loran message is independent from each other, the probability of authentication can be estimated as,

$$N = ceil(9/BW)$$
$$P\{authentication\} = (1-p)^N \qquad (3)$$

In equation (3), N is the sum of number of Loran data message to be authenticated and number of Loran messages to carry one authentication message, and p is message loss rate. BW is the authentication bandwidth which is the percentage of messages that whose sole purpose is for authentication. The number of Loran messages to carry one authentication message is fixed. Hence, as BW decreases, number of data messages to be authenticated increases, resulting in an increase of N. For instance, GRI 9940 has a raw data rate of 50 bits/sec. A 50% bandwidth results in an authentication raw data rate of 25 bits/sec. Figure 7 illustrates the probability of authentication as a function of SNR.

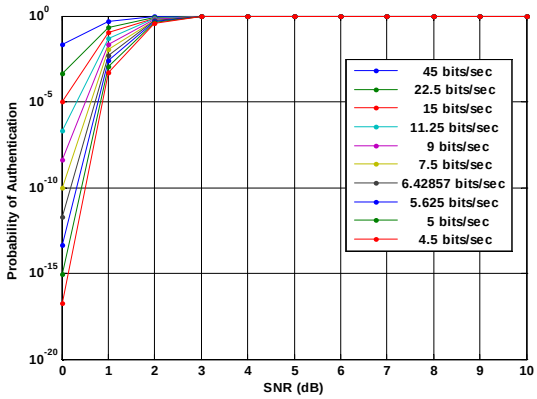

Figure 7: Authentication Performance

As SNR increases, the probability of error and message loss rate decreases and this results in an increase of probability of authentication. Furthermore, higher authentication bandwidth results in fewer number of Loran messages. This also results in an increase of the probability of authentication.

A contour plot is developed to analyze the authentication probability geographically. The received SNR depends on the range from transmitter to receiver, the transmitter radiated power and local noise level. The field strength of Loran ground, modeled with an assumption of homogenous ground conditions, is provided as follows.

$$a = 17.52; b = 1.1036$$
$$E_{sig}{}^2 = \left(\frac{9.48}{1000r}\right)^2 * P * 10^{-0.1a(r/1000)^b} \qquad (4)$$

where r is the range from transmitter to receiver in km and P is the transmitter radiated power in watts [8].

A constant noise level is assumed for GRI 9940 coverage area. The contour plot of authentication probability of Middletown is shown in Figure 8.

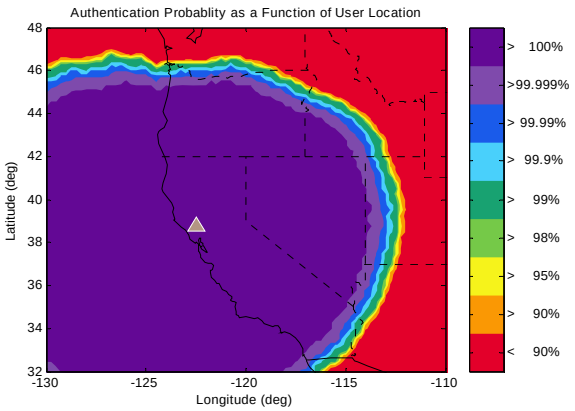

Figure 8: Contour Plot of Authentication Probability

The axis limits indicate the availability coverage of GRI 9940. The triangle shown in this figure represents the Middletown station. As the received signal power is inversely proportional to distance from the transmitter, probability decreases as a user moves away from the transmitter. An authentication bandwidth of 50% is applied in this analysis.

False Positive

Attackers who want to forge a correct geotag will have to bypass the authentication check first. These attackers are not necessarily located at the user location. What they can do is to simulate the Loran signal to pretend they are at the location where they can achieve a correct geotag. In the case of digital film distribution, the user location is known to the public. They also need to simulate their own TESLA messages for MAC verification in a certified Loran receiver.

To protect against this attacker, we propose the idea that embedding the last key of the TESLA one way key chain inside Loran certified receivers. In this way, receiver has to verify the received key with this embedded key before performing the MAC verification. If there is a chance that the embedded key is recovered by the attackers, they still should not be able to derive the rest of TESLA keys from the embedded key because of one-way-ness property of hash functions.

The cost of this attack is potentially expensive. At a minimum, the attacker requires a RF simulator and certified Loran receiver to receive simulated signal. A signal simulator is used to generate Loran signals. TESLA messages can be computed and the modulation of authentication messages on simulated signal can be done in MATLAB or other software.

GEOTAG THREAT MODEL

Once the source of the navigation signal is verified, geotag generation is the next key procedure to enhance the security of the conventional cryptographic protocol. Geotag threat model defines the threat space as all the false estimates of location-base parameters and it is used to analyze the performance of geotag generation. A false estimate occurs when the actual parameter of the user/attacker is different from the measured parameter.

We apply estimation theory to model the false measurements of location-based parameters. Figure 9 can help demonstrate the problem. False negative represents false reject rate, the percentage of authorized persons who are incorrectly denied acceptance. False positive indicates false accept rate, the percentage of unauthorized persons accepted in error. The probability distribution function (pdf) illustrates location-based parameter estimation in the presence of arbitrary Gaussian noise. The shape of the curve depends on the variance of the noise. As variance goes down, the curve becomes narrower. The grid space is equivalent to quantization level of location-based parameters and determines the probability of correct geotag.

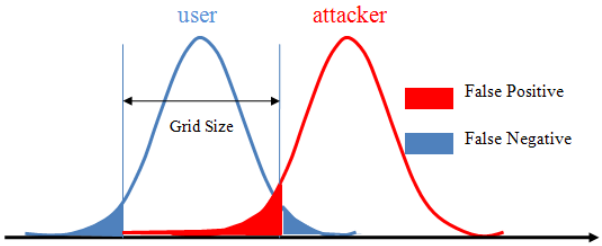

Figure 9: False Negative and False Positive

Figure 9 represents only one location-based parameter, hence the pdfs are shown in one-dimension. For strong geotag computation, more than one location-based parameter should be used to achieve high entropy and strong geotag. For simplicity, we used the location-based parameter, time difference of arrival (TDOA), as an example to explain the concept of false negative and false positive in details.

False Negative

The correctness of geotag depends on both the receiver accuracy and the grid space size a user specifies. In this analysis, we also assume AWGN presented in the Loran signal. The presence of noise results in errors in the measured TDOA, thus an error in location-based parameter estimation.

The range and TDOA error variances can be modeled as follows.

$$\sigma_{M/S}^{\ 2} = 36 + \frac{3000^2}{(2\pi)^2 * 2 * N * SNR} \tag{5}$$

$$SNR \propto \frac{P}{r^3}$$

$$Q = \begin{bmatrix} \sigma_M^{\ 2} & 0 & 0 & 0 \\ 0 & \sigma_W^{\ 2} & 0 & 0 \\ 0 & 0 & \sigma_X^{\ 2} & 0 \\ 0 & 0 & 0 & \sigma_Y^{\ 2} \end{bmatrix}$$

$$D = \begin{bmatrix} -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}$$

$$\overline{Q} = DQD^T$$

$$= \begin{bmatrix} \sigma_M^{\ 2} + \sigma_W^{\ 2} & \sigma_M^{\ 2} & \sigma_M^{\ 2} \\ \sigma_M^{\ 2} & \sigma_M^{\ 2} + \sigma_X^{\ 2} & \sigma_M^{\ 2} \\ \sigma_M^{\ 2} & \sigma_M^{\ 2} & \sigma_M^{\ 2} + \sigma_Y^{\ 2} \end{bmatrix} \tag{6}$$

Equation (5) is range error variance derived by Dr. Ben Peterson for all stations, where N is the number of pulses for averaging, and the component, 36, comes from an estimation of maximum transmitter jitter error. Equation (6) is the derived covariance matrix for TDOA error.

SNR is an important metric in this analysis. We study the performance of geotag for different grid space sizes and averaging time. As SNR and grid space size increase, the false negative or user reject probability decreases and this results in an improvement on the user's performance.

The probability can also be improved as averaging time goes up. Longer averaging time reduces the noise level since the Gaussian noises are not correlated with each other.

False Positive: "Park Lot" Attack

False positive is the case that attacker achieve a correct geotag even though he is not at the correct location. The presence of noise creates this significant security issue for users. This leaves the system open to what is known as "parking lot" attack. An antenna and a certified Loran receiver are required for the attacker. The attacker can stay at a location close to the user, for instance, a parking lot. Since he is receiving the actual Loran broadcast, signal authentication from TESLA passes.

The level of security can be judged using false positive, shown in Figure 9. False positive is the probability of an attacker getting the correct geotag, given he is outside the security perimeter. Security level is affected by the noise level, receiver performance, grid space specified, and the distance between the user and the attacker.

In the previous section, we mentioned increasing the grid space size can improve user performance; on the other hand, it also provides the attacker a greater probability to achieve a correct geotag. This increases in the likelihood of having a false positive. Therefore, grid space size should be chosen to achieve a reasonably good user performance but it should not be too large due to the tradeoff between geotag performance and security.

The dilemma we face here is the choice between false negative of users and false positive of attackers. The solution to this problem is to improve the receiver accuracy so a smaller grid space size can be used for geotag generation for a desired security level.

DATA COLLECTION

To examine the security analysis of geoencryption experimentally, Loran data was collected in a parking structure at Stanford University. Two test locations were chosen to evaluate both false positive and false negative performance. The Loran chain tracked is GRI 9940. Data sets were taken on multiple days.

Experimental Setup

The data collection setup consists of an E-field Locus antenna, Loran LRS IIID receiver and a laptop, shown on the top in Figure 10. The receiver first conditions the noisy signals and extracts navigation data from the raw RF signals. The receiver averages the raw RF for one minute to lower the noise floor. A PC laptop is used to log the navigation output.

Figure 10: Data Collection Setup

The layout of the parking lot is shown on the bottom of figure 10. The separation of two test locations is approximate 70 meters. Both locations have open sky views while the second location has a slightly higher noise floor due to its environment.

Results

Test location 1 was chosen to represent an authorized user while test location 2 corresponds to a potential attacker's location. For simplicity, only TDOA is used for this analysis and the relative TDOA measurements are plotted in figure 11. Averaged SNRs are illustrated in the following table. Middletown has higher SNR than George due to its relative closeness to the test locations.

Station	Test Location 1	Test Location 2
George	-5.8 dB	-12 dB
Middletown	23.4 dB	15.6 dB

False negative and false positive values were examined using these data sets. Performance capacity can be shown in the form of receiver operating characteristics (ROC) curves, in which the false positive is plotted versus the false negative with various interval sizes. ROC curve is used to distinguish an authorized user and an attacker statistically. The ROC curves are plotted on the right of Figure 11. The solid curves are estimated using Eqn. (6) derived from Dr. Peterson's TOA error variance model, while the dots indicate the experimental results of the false positive and false negative values. The analytic model overestimates the variances of the collected data and provides an upper bound on the false positives and false negatives. As expected, increasing grid interval size improves user performance as well as the attacker's probability obtaining a correct geotag. Ideally, we need both false negative and false positive 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.

CONCLUSION

In this paper, we analyzed the performance of geoencryption in two stages, authentication stage and geotag generation stage. To authenticate successfully, one should be inside the coverage area using signals with received SNR of 3dB or higher. The performance of the geotag depends on not only the signal-to-noise ratio, but also the grid space a user specifies and the distance between a user and an attacker. From the above experiments, the optimal grid size for Middletown is five meters to achieve low false positive and false negative values, while 37 meters for George due to its lower SNRs.

To solve the dilemma of choice of false negative of users and false positive of attackers, we need to improve receiver accuracy and apply more location-dependent parameters to provide more randomness to compute a geotag Loran time difference of arrival (TDOA) alone does not achieve both availability and security for the system. Some future work includes developing a more sophisticated error model and collecting more Loran data to study signal characteristics to design a more robust geotag.

ACKNOWLEDGMENTS

The author would like to thank Mitch Narins of the FAA, Loran Program Office for supporting this effort. I would

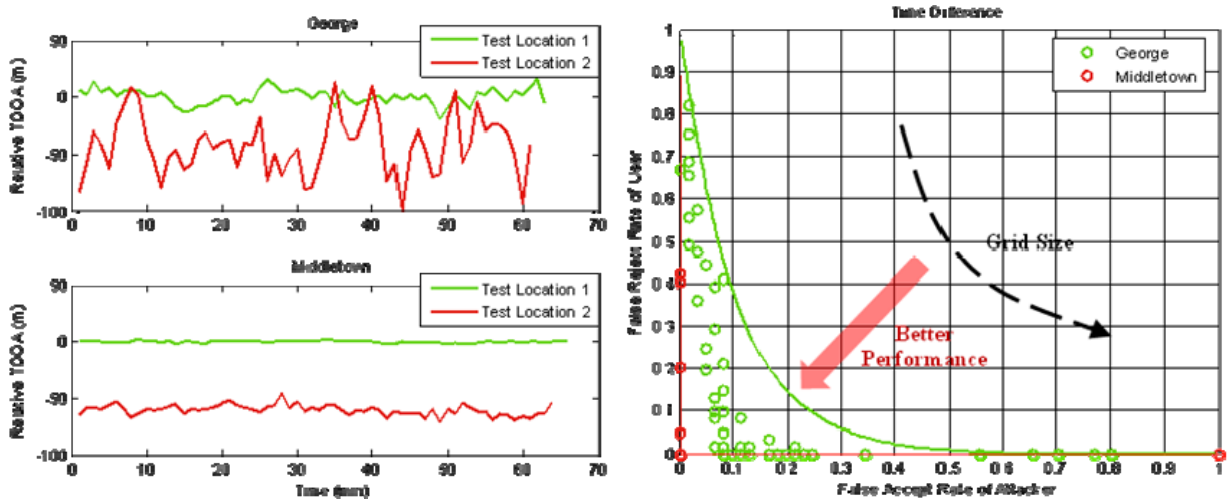

Figure 11: TDOA Measurements and Receiver Operating Curves

like to thank Sherman Lo, Per Enge, Dan Boneh, and Logan Scott for their advice and suggestions. In addition, thanks go to US Coast Guard (USCG) Loran Support Unit (LSU) for lending us the use of their E-field antenna and LRS IIID receiver to collect data. Finally, I also would like to thank Lt. Kirk Montgomery and USCG for their support of the Middletown tests.

REFERENCE

[1] L. Scott, D. Denning, "Location Based Encryption & Its Role In Digital Cinema Distribution", *Proceedings of IONGPS/GNSS 2003*, pp288-297.
[2] L. Scott, D. Denning, "A Location Based Encryption Technique and Some of Its Applications", *Proceedings of ION NTM 2003*.
[3] D. Qiu, "Geoencryption Using Loran", *Proceeding of ION NTM 2007*.
[4] International Loran Association (ILA), "Enhanced Loran (eLoran) Definitions Document", January 2007. Available at the ILA website (http://www.loran.org/)
[5] A. Perrig, R. Canetti, J.D. Tygar, D. Song, "The TESLA Broadcast Authentication Protocol", CryptoBytes, 5:2, Summer/Fall 2002, pp. 2-13.
[6] B. Peterson, A. Hawes, K. Shmihluk, "Loran Data Channel Communications using 9th Pulse Modulation".
[7] K M. Carroll, A, Hawes, B. Peterson, K. Dykstra, P. Swaszek, S. Lo, "Differential Loran-C". Proceedings of European Navigation Conference GNSS 2004.
[8] S. Lo, "Broadcasting GPS Integrity Information Using Loran-C". Ph.D. Thesis.