Geoencryption with Loran

Di Qiu, Sherman Lo, Per Enge, *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.

Dr. Sherman Lo is currently a research associate at the Stanford University Global Positioning System (GPS) Laboratory. He is the Associate Investigator for the Stanford University efforts on the Department of Transportation's technical evaluation of Loran. He has received the International Loran Association (ILA) President's Award. He received his Ph.D. in Aeronautics and Astronautics from Stanford University.

Professor Per Enge is a Professor of Aeronautics and Astronautics at Stanford University, where he is the Kleiner-Perkins, Mayfield, Sequoia Capital Professor in the School of Engineering. He directs the Stanford GPS Research Laboratory. Enge has received the Kepler, Thurlow, and Burka Awards from the Institute of Navigation. He received his Ph.D. from the University of Illinois.

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, an attack model is developed and analyzed. In this attack model we discussed all the possible attacks that might weaken the protocol and means to defeat these attacks.

This paper describes the work on analyzing system performance using the designed attack model. In addition, this paper also provides preliminary results on the size of the geotag derived from Loran location-based parameters, which limits the security level of the system.

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 traditional cryptosystems, user encryption is based on possession of secret keys, which falls apart if the keys are not kept secret (i.e., shared with non-legitimate users). Furthermore, keys can be forgotten, lost, or stolen. Another type of cryptosystem is password based encryption. Most passwords are so simple that they can be easily guessed (especially based on social engineering methods) or broken by simple dictionary attacks. 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]. 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 an attack model to evaluate the vulnerabilities of the protocol and means to solve these vulnerabilities. As security of geoencryption depends on not only the design and implementation of the protocol but also characteristics of location-based parameters, several parameters are measured and analyzed. This paper then discusses some preliminary results on measuring location information 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 verification tag, 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].

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.

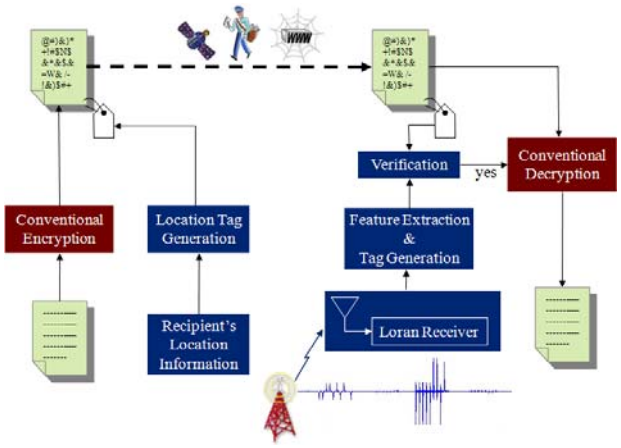

Figure 1: Geoencryption Overview

Loran as a Case Study

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.

Loran is transmitted from static transmitters and, as a result, there are many parameters that are location dependent. This is important as the security strength of the geolock is derived from the information content or randomness of the information used to generate it. In addition, Loran has good repeatable accuracy in position, which benefits the design of the geolock. Third, Loran is a high power low frequency signal. This means it is hard to spoof and hard to jam. Furthermore, the signal can reach some places such as urban canyons and indoor environment that may not be reachable by a line of sight system such as GPS. Finally, modernized Loran has a data channel that can carry authentication and time messages, which will be discussed in details in the later section.

SECURITY ANALYSIS

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 geoencryption protocol, we developed an attack model. An attack model should provide possible failure modes due to the availability of the system. Furthermore, an attack model defines all possible attacks that might threaten the system. Whether a given systems is secure or

not can depend dramatically on the attack model is considered.

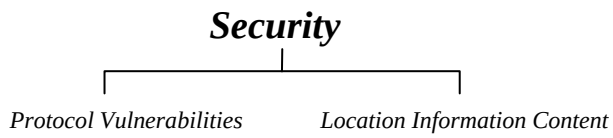

Figure 2: Security Analysis Outline

In cryptography, if there are no analytic attacks or 'structural weaknesses' in the algorithm or protocol used, the security of a system depends on spatial decorrelation and the key size or geotag size in geoencryption system. The amount of information in Loran location-based parameters determines the size of geotag. The rest of the paper follows this security analysis outline.

ATTACK MODEL

A cryptographic attack is a method for circumventing the security of a system by finding a weakness in cipher, cryptographic protocol or key management. In our attack model we focus on the weaknesses in the design and implementation of the protocol. It is necessary to define these analytic attacks and defeat them.

I. Signal Authentication on Loran

First weakness in the geoencryption algorithm is that the RF signals are not secure. An attacker or unauthorized user can simulate Loran signals to pretend they are at the location where they can achieve a correct geotag. 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 devices such as signal simulator to spoof the system into generating the correct geotag. Source authentication helps the receivers to verify the received data originating from the source and to monitor whether the data 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 Message Authentication Code (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]. MAC is a cryptographic function and is employed in several widely used security algorithms and protocols.

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.

Middletown Demonstration

The west coast chain of Loran, 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 MAC (h_i) and the delayed key (K_{i-d}) for a previous MAC. 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 3 where the key is delayed by two message/hash segments.

Figure 3: 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.

Authentication 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. 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.

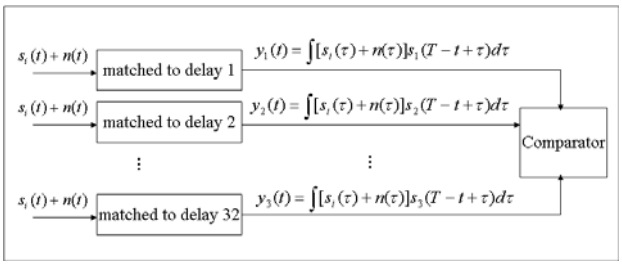

Figure 4: PPM Matched Filter

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),

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

Figure 5 on the left 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 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. 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. 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.

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 is modeled with an assumption of homogenous ground conditions. The model was developed by Dr. Ben Peterson and Dr. Sherman Lo. The signal strength of Middletown station is plotted in the middle of Figure 5. A constant noise level is assumed for GRI 9940 coverage area.

The contour plot of authentication probability of Middletown is shown in Figure 5 on the right. The axis limits indicate the availability coverage of GRI 9940. The white cross 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.

To test the authentication performance experimentally, a data collection trip was made. The data collection setup includes E-field Locus antenna, Locus LRS IIID receiver, Symmetricom Enhanced Loran Research Receiver (ELRR) and a laptop to log data. Five test locations appear as white dots in the authentication contour plot. The Loran messages were successfully demodulated and authenticated at all five locations.

II. Integrated Device

The security of a system depends on not only the design of the protocol but also the implementation. Improper Implementation may weaken the cryptographic protocol.

If the geoencryption protocol doesn't implement correctly, a couple of attacks can be performed to break the geoencryption protocol. First, attackers can bypass the authentication check by simulating Loran signals as well as TESLA messages. Furthermore, attackers use real authenticated Loran signals to bypass the signal source verification but modify the received location information and replay to spoof the decryption device. The second attack requires the attackers to stay in the coverage area of

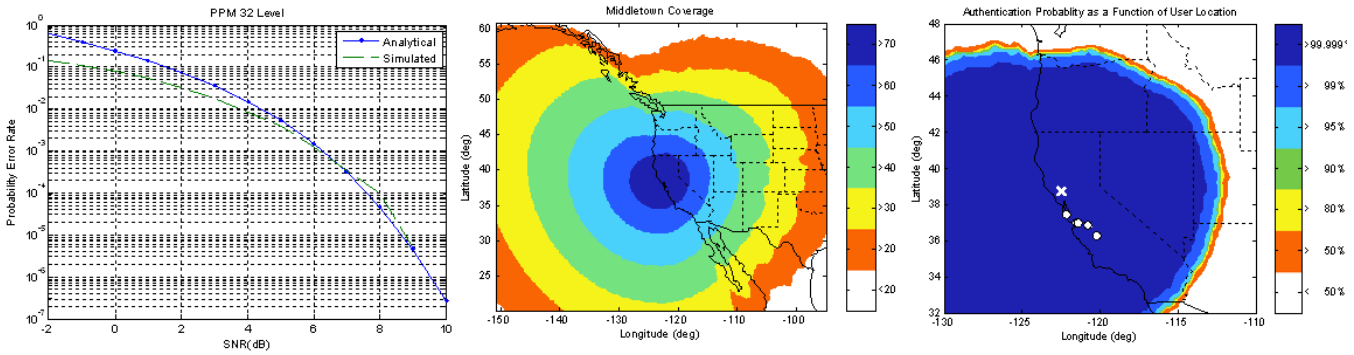

Figure 5: PPM 32 Error Probability (Left); Middletown Signal Strength (Middle); Authentication Probability (Right)

Loran stations.

To protect against these attacks, a certified Loran receiver can be used. The receiver integrates all the function in one device and it is tamper-resistant. The tamper-resistant device makes signal authentication more effective and defeats replay attack. In addition, 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 these attacks 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.

III. "Parking Lot" Attack

With the signal authentication and certified receiver, attackers are not able to spoof the receiver to bypass location verification and these protections force the attackers to perform the parking lot attack. Since there is no physical boundary to distinguish authorized user and attacker, an attacker can achieve a correct geotag by staying close to the user, for instance, in a parking lot. This approach replies on a probabilistic mapping from the user's location. Figure 6 illustrates this scenario. The variance of the feature depends on its accuracy, which is determined by noise, environment and devices, etc. The grid interval size is used to quantize the parameter and allow some degrees of variation.

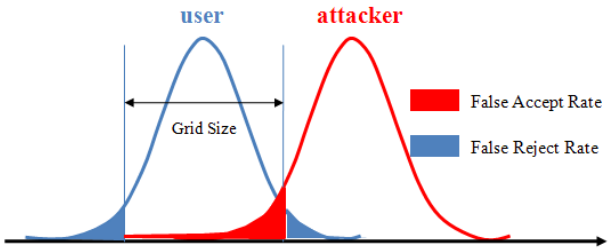

Figure 6: False Accept and False Reject

Geoencryption system makes two types of errors: 1) mistaking the measurements from two different locations to be from the same location, called false accept; and 2) 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 grid interval size chosen to quantize the continuous location features. These two types of errors can be traded off against each other by varying the grid interval size. Ideally, both low FAR and low FRR are desired. Practically, a more secure system aims for low FAR at the expense of high FRR, while a more convenient system aims for low FRR at the expense of high FAR. The desired interval size is highly dependent on the final application.

Figure 7: Test Locations

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 demonstrate this scenario; hence, the horizontal axis in Figure 6 can represent TDOA measurements. The TDOA measurements were collected in a parking structure at Stanford University, shown in Figure 7. 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. The data collection setup includes an E-field Locus antenna, Locus LRS IIID receiver and a laptop to log TDOA data from the receiver.

The relative TDOA measurements from station George, GRI 9940 are plotted on the left of Figure 8. Test location 1 was chosen to be an authorized user while test location 2 corresponds to a potential attacker's location. FAR and FRR values were estimated using these two data sets. With the assumption of white Gaussian noise in the presence of Loran signals, PDF of TDOA at two test locations can be estimated, illustrated in the middle of Figure 8. FAR is the red shaded area that incorrectly falls in the user's grid; on the other hand, FRR is shown in the blue tails. Performance capacity can be shown in the form of receiver operating characteristics (ROC) curve, shown on the right of Figure 8, in which the FAR is plotted versus the FRR with various interval sizes. ROC curve is used to distinguish an authorized user and an

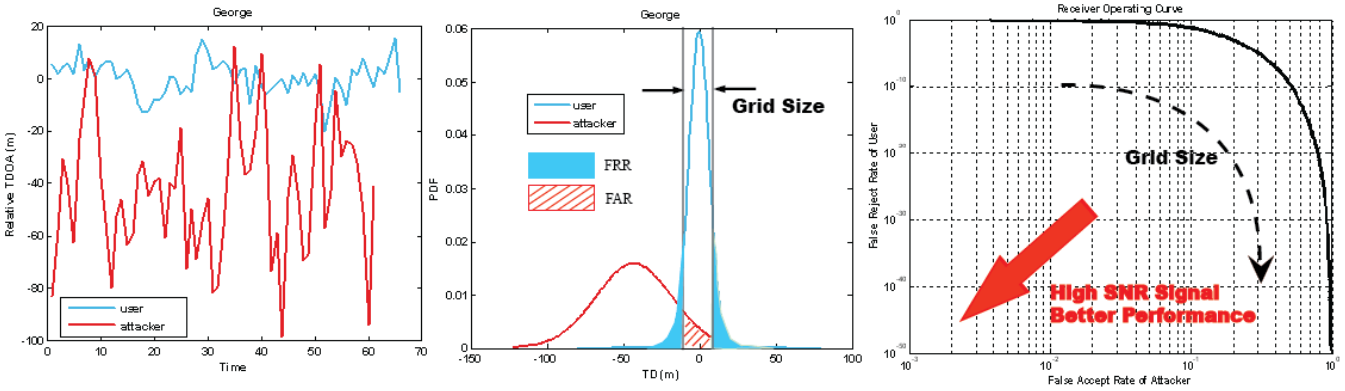

Figure 8: TDOA Measurements (left); PDF (Middle); Receiver Operating Curve (Right)

attacker statistically. Given the PDF, the two error rates can be estimated analytically using Q function. As a result, the FAR and FRR are a function of estimated variance of TDOA, grid interval size specified and the Euclidean distance of the location parameter between the user and attacker. As expected, increasing interval size improves user performance as well as the attacker's probability obtaining a correct geotag. The ROC curve shifts towards the origin as SNR increases. This indicates higher SNR results in better user performance and higher security level.

INFORMATION MEASURE

If a cryptographic protocol is well-designed and there is no analytic attack or 'structural weakness' in the protocol, the security level of the system depends on the key size, geotag size in geoencryption system. This leads to the question how much information there is in location-based parameters?

Information entropy [9], introduced by Shannon more than half a century ago, is used to measure information density within a set of values with known occurrence probabilities.

Spatial decorrelation is a measure of uniqueness for location-based features. It is the change or rate change of location parameters as a function of physical locations or distance. High spatial decorrelation indicates people can be distinguished from each other with a small separation. FAR is used to characterize and quantify spatial decorrelation. FAR is not the only evaluation function to characterize spatial decorrelation. Other possible evaluation functions include Euclidean distance, relative entropy, or correlation coefficient, which will be discussed in our next paper.

To examine the spatial decorrelation of location-based parameters, more data was collected in the same parking structure. Eleven test locations were chosen with a separation of 3 meters, shown in Figure 9 on the left. Test location 1 is considered as our master location. We analyze how the location parameters vary as the antenna is moved away from the master location. The data collection setup is the same as the one used in the parking lot attack experiment.

Applying the same FAR estimation algorithm in parking

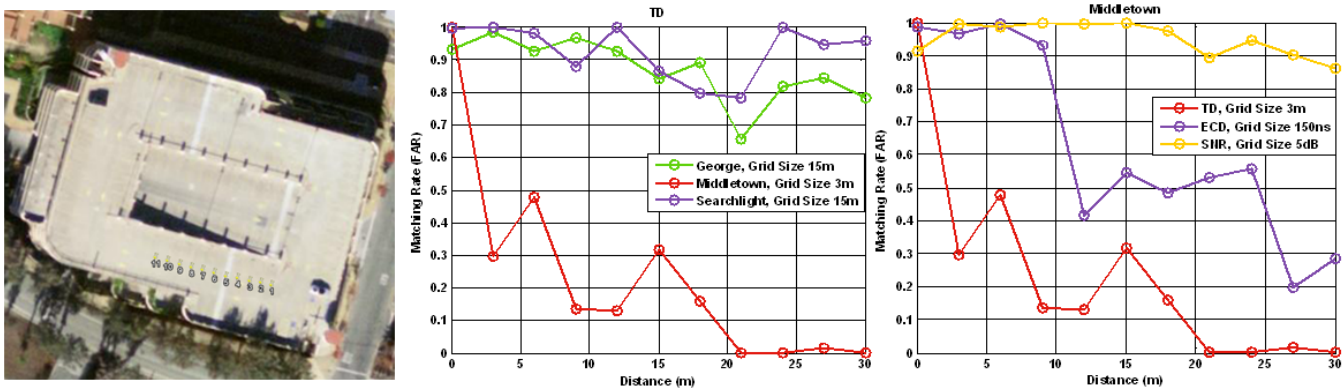

Figure 9: Test Locations (Left); Spatial Decorrelation of Different Stations (Middle); Spatial Decorrelation of Different Location Parameters (Right)

lot attack analysis, we first compare the spatial decorrelation of different stations in GRI 9940 for one particular location parameter, TDOA. The comparison result is illustrated in the middle of Figure 9. X-axis represents all test locations, while y-axis is the estimated FAR values. Middletown is the closest station to Stanford campus; hence, its SNR is the highest due to shorter propagation distance. The averaged SNRs for all stations in GRI 9940 are listed in Table 1. The grid interval sizes were chosen according to SNR of the different stations, 3 meters for Middletown and 15 meters for George and Searchlight. Middletown, shown in red curve, delays faster compared with George and Searchlight. Therefore, spatial decorrelation highly depends on SNR.

Table 1: GRI 9940 Station SNR

Station	SNR (dB)
Fallon	21
George	6
Middletown	32
Searchlight	8

To study the uniqueness or the strength of different location-based feature, we compare the spatial decorrelation of location parameters using the measurements from Middletown station. According to result shown in Figure 9 on the right, TDOA has the highest spatial decorrelation while the location parameter, SNR, has the least spatial variation. SNR is a parameter very sensitive to environment or local noise. The parameter doesn't change much in this experiment because test locations are in open-sky environment and closely separated; hence, this observation is expected.

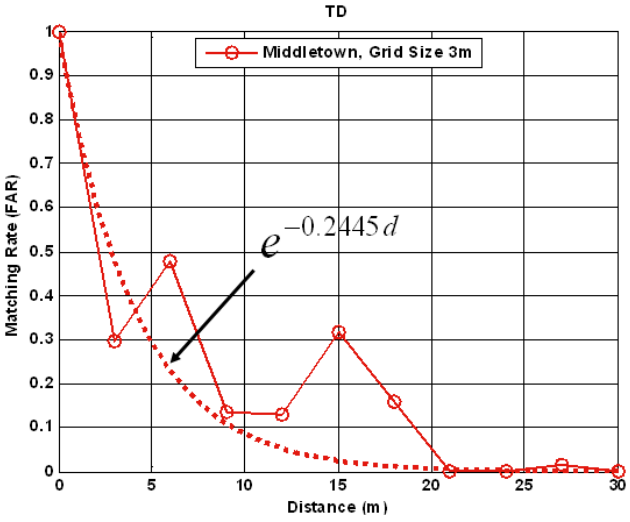

Figure 10: Decorrelation Distance

Decorrelation Distance

Decorrelation distance is defined as the minimum distance from the master location where the value of FAR is less than a reasonably small threshold. We chose the threshold to be 0.01 and estimated the decorrelation distance by curve fitting the estimated FAR values with an exponential function. A fitted curve is plotted in the dashed line in Figure 10. The decorrelation distance for this particular example is approximately 18 meters; hence, attackers who are 18 meters away from the master location have FAR less than 0.01. Decorrelation distance can be used as a guidance to choose a proper grid interval size to quantize the location-based parameters.

Geotag Length

The information content in location-based features plays an important role in the geotag size. The information in the Loran location-based parameters depends on the coverage of Loran stations, grid interval size, the spatial decorrelation and consistency of the parameter.

We calculated the information of parameters TDOA, ECD and SNR for Middletown station. The coverage of Middletown is limited to the areas where authentication probability is reasonably high. The Middletown coverage radius is approximately 800 km based on the signal authentication performance analysis. Spatial decorrelation determines the grid interval size to quantize location-based parameters. As a result, TDOA can contribute entropy of 15.5 bits while 6 bits can be generated from ECD and 4.5 bits from SNR. From this preliminary result, a geotag of 26 bits can be computed from Middletown.

CONCLUSION

In this paper, we analyzed the security performance of geoencryption in two aspects, structural weakness of the protocol and the location information content.

The signal authentication and integrated device are used to provide additional layers to enhance the security of protocol. To authenticate successfully, one should be inside the coverage area using signals with received SNR of 3dB or higher. The performance of the parking lot attack 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. A more secure system is in the favor of low FAR; on the other hand, a system that aims for better performance prefers low FRR.

The information content of location-based parameters determines the entropy or randomness to generate a geotag. A 26-bit geotag can be obtained from Middletown. This is a very short key in the modern

security world and a brute force attack can be used to break the system in a short period of time. However, with the protections of signal authentication and integrated device, attackers can't modify the geotag output; the brute force attack or trials of all the binary combinations of geotag can not be implemented. As a result, it requires attackers to try at least 2^{26} different locations to be able to obtain a correct geotag.

Each location-based parameter has its strength and weakness. A combination used of these parameters enhances the security level. More parameters will be studied and examined to increase geotag size as well as the cost of the attacks to achieve high security for the system. Furthermore, even though low SNR stations provide low spatial decorrelation and variant features compared with high SNR stations, algorithm can be developed to use the features from the low SNR stations and generate a stable and robust geotag.

ACKNOWLEDGMENTS

The author would like to thank Mitch Narins of the FAA, Loran Program Office for supporting this effort. I would like to thank Ben Peterson, Dan Boneh, and Logan Scott for their advice and suggestions. In addition, thanks go to US Coast Guard (USCG) Loran Support Unit (LSU) and Symmetricom for lending us their equipments for data collection. 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.
[9] T. Cover, Elements of Information Theory. John Wiley & Sons, Inc. 2001.