A Measure of Loran Location-based Information

Di Qiu, Sherman Lo, Per Enge
Department of Aeronautics and Astronautics
Stanford University, Stanford, CA 94035
Email: {qiudi, daedalus, penge}@stanford.edu

Abstract – **In cryptography, a verification tag is a piece of information used to authenticate a message. In geoencryption, location-based information is defined as the amount of information that can be used to construct a verification tag or "geotag" to identify one's location. The term "geoencryption" or "location-based encryption" refers to a security algorithm that limits the access or decryption of information content to specified locations and/or times. Loran is chosen as a case study to implement geoencryption due to its many properties that are beneficial to this protocol. The security of a geoencryption system resides in the geotag. In order to evaluate the security level of geoencryption system, we develop a mathematical framework to measure the information content of Loran location-based parameters.**

I. 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.

Geoencryption is the use of position navigation and time (PNT) as means to enhance the security of a traditional cryptographic system. The location-based parameters are used to generate an additional verification tag, a "geotag", that is a piece of information that allows authentic users to validate their physical locations and proceed to the decryption process. Geotag is derived from specific user location (and time) information by quantizing these parameters into grid spaces. 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 [2]. Traditional encryption is an integral part of the system and geoencryption provides an additional layer of security but doesn't replace any conventional cryptographic algorithm. The detailed description of geoencryption is discussed previously in [3].

The security of a cryptographic system depends on not only the protocol design but also the implementation. In principle, to implement geoencryption a device performing the decryption integrates a location sensor and cryptographic algorithms. 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 location information 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 of implementing TESLA on Loran for authentication. The analysis and experimental results of authentication performance were discussed in our previous paper [4].

Additionally, the geoencryption system security resides in the amount of information in Location features. This paper further investigates the security of geoencryption protocol by developing an approach to measure the information content of Loran location-based parameters. We consider the measures of location feature strength from an information theoretic point of view.

The structure of the paper is organized as follows. Section II defines a geoencryption system security model. Section III first gives a short tutorial or review on information theory and then elaborates an approach to quantify security based on the concepts in information theory. We evaluate this information theoretic approach using two data sets in section IV. One set of data is from Stanford Seasonal Monitor station; the other set of data uses portable data collection. This paper then provides a quantitative result of the information measures and concludes with future directions of the research.

II. System Security

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 first investigate a threat model that provides the possible attacks that might threaten or weaken the system. 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 previous study, we focus on the weaknesses in the design and implementation of the protocol: 1) authenticating Loran signals to protect against spoofing; 2) tamper resistant device that doesn't allow attackers to modify location information. Signal authentication allows users to verify the source of the incoming signals. The authenticated message, carried in the

Loran data channel (LDC), includes data message, verification message of the data and a key to generate the verification message. Attackers cannot simulate Loran signals or use any mean to spoof the certified Loran receiver because they don't have the key used to generate authenticated messages. The tamper resistant device integrates the Loran receiver and cryptographic algorithms. Both authentic user and attacker only have the access of the output and neither can spoof the device by modifying Loran location information. If there is an unauthorized tamper access, for instance, one of the screws on the cover is partially removed, the system assumes a tampering is being attempted and the circuit is designed to destroy all the sensitive information contained in this device. With signal authentication and tamper resistant device, one has to use this device and collect real Loran signals to bypass location validation, then proceeds to the decryption process. The detailed analysis of the attacks is discussed previously in [4]. If the cryptographic protocol has been proved secure, the security metric is the geotag length. In the paper we assume there is no structural weakness and focus on the location dependent information measure and estimate an upper bound on the geotag length.

A. System Model

A simple mathematical model is developed to explain geotag generation process, shown in Fig. 1. The true location-based parameter is represented as X while the received one is Y, which is contaminated by noise and bias. To allow certain degree of variation of the received parameter Y, we first quantize or cluster Y using a grid of a particular size. The grid size is chosen based on the variation of Y, and the detailed calculation of the grid size will be discussed in the later section. The possible outputs of clustering are Y_1, Y_2 … Y_N. We model the channels, $P(Y_i|i)$, as the probability to map X into Y_i, where i = 1, 2… N. Then a hash function or mapping function is applied to the quantized parameter Y_i to computer K_i, which is the derived binary geotag. A hash function is a cryptographic function that has the properties of one-way-ness and collision resistance. It is easy to compute a hash function but relatively hard to invert the hash output or digest. One cannot recover the input of hash function from its output.

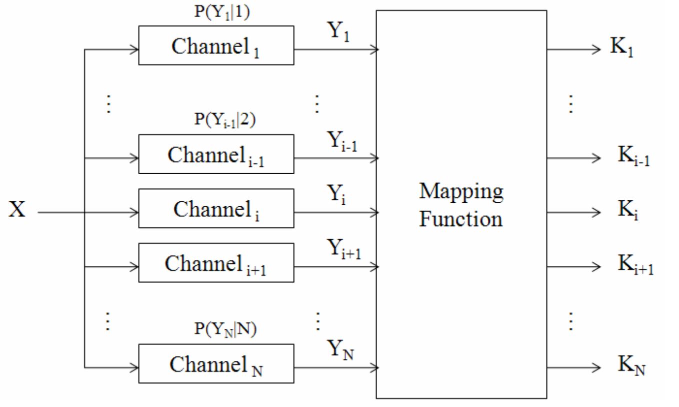

Fig. 1. Geotag Generation Model

B. Performance Metrics

The problem of deciding whether the received parameter is authentic or not, can be seen as a hypothesis testing problem. The task is to decide which of the two hypotheses H_0 (accepting as an authorized user) or H_1 (rejecting as an attacker) is true for an observed location measurement. Geoencryption system makes two types of errors: 1) mistaking the measurements from the same location to be from two different locations and accepting hypothesis H_1 when H_0 is true, called false reject; and 2) mistaking the measurements from two different locations to be from the same location and accepting H_0 when H_1 is true, called false accept. Both false reject rate (FRR) and false accept rate (FAR) depend on the accuracy of the Loran receiver and the grid size chosen to quantize the continuous location features. These two types of errors can be traded off against each other by varying the grid size. If Y_i is the recipient's desired quantized location dependent parameter, FRR is $1\text{-}P(Y_i|Y_i)$ and FAR is the $P(Y_i|Y_j)$, where $j \neq i$. 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.

C. Location-based Parameter Requirement

The most important required feature of a navigation signal is its ability to generate a strong geotag. If there are no analytic attacks or 'structural weaknesses' in the algorithm or protocol designed, the security of the geoencryption system depends on navigation signal properties and amount of information contained in them.

The strength of the geotag is determined by the quantity and quality of location dependent features. By quantity, we mean the number of different location dependent parameters that can be generated. Equivalently, the more numbers of X in Fig. 1, the longer the geotag we can derive. The quantity of the features is also determined by the number of available Loran stations.

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. The larger the spatial variation, the lower $P(Y_i|Y_j)$, the probability of false accept rate or attacker successful rate, can be. By having many parameters each providing its unique information content, we can generate a strong geotag.

At the same time, it is desirable to have the parameters be relatively insensitivity to temporal changes which weakens the uniqueness of the information. Temporal variations essentially reduce the uniqueness of the location dependent information. Small temporal variation implies $P(Y_i|Y_i)$ is high with an adequate grid size chosen. As a result, repeatability and repeatable accuracy are desirable qualities. It allows a recipient/user to receive his location-dependent parameters 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.

Additionally, there are several characteristics that 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 is available indoors. This is because many of the anticipated applications of geoencryption will likely occur indoors. This includes applications such as the management and distribution of secure digital data.

Loran has many characteristics that can be used to generate a robust geotag. First, it is being modernized to a next generation system known as enhanced Loran (eLoran), which will have a data channel that can carry authentication message and benefit its use for geoencryption [5]. The modernization will also reduce the amount of variation in some of the location-based parameters. Loran uses static transmitters and, as a result, there are many parameters that are location-dependent. Each parameter offers different certain amount of information or potential information density. Parameters with higher density result in higher security levels. The possible useable Loran parameters are *time of arrival* or *time difference* (TOA/TD), *envelope to cycle difference* (ECD), *absolute or relative signal to noise ratio* (SNR/ΔSNR), *signal strength*, and shape of the envelope. In addition, Loran is a high power, low frequency signal. This means that it is hard to spoof or jam. The signal can reach places such as urban canyons and indoor environments.

III. Information Measure

In this paper we develop an approach to measure consistency and uniqueness of location-based information based on information theory. We define "location-based information" as the amount of information can be used to generate a geotag to identify one's location due to a set of measurements.

A. Information Theory Review

This section presents some fundamental concepts of information theory. Information entropy, introduced by Claude Shannon more than half a century ago [6], is a measure of information density within a set of values with known occurrence probabilities. The information entropy of a discrete random variable X is defined by

$$H(X) = -\sum_{x \in X} p(x) \log p(x) \tag{1}$$

The entropy of a finite measurement depends on the probability distribution of the random variable. The units for entropy are "nats" when natural logarithm is used and "bits" for base-2 logarithm [6]. We use base-2 logarithm instead of natural logarithm in this paper since base-2 logarithm provides more intuitive descriptions. If the probability distribution is uniform, the entropy can be represented as

$$H(X) = \log N \tag{2}$$

The uniform distribution provides the maximum information entropy for discrete random variables. The total number of occurrences is N while the probability of each occurrence is 1/N. It is worth to mention that the normal distribution gives the maximum entropy for continuous random variables.

Another important definition in information theory is relative entropy or Kullback-Leibler divergence. Relative entropy $D(P_X||P_Y)$ measures the difference between two probability distributions P_X and P_Y.

$$D(P_X \parallel P_Y) = \sum_{x \in X} P_X(x) \log \frac{P_X(x)}{P_Y(x)} \tag{3}$$

Relative entropy is also a measure of inefficiency of assuming that the distribution is P_Y when the true distribution is P_X. Since it is not symmetric, it is more a divergence measure than a distance measure, even though it has often been used as a distance metric [7].

The numerical estimation of entropy for a finite data is fully discussed in [8]. Finite size data introduces systematic errors that should be considered. What we observe is that entropy not only fluctuates around its true value, but gets underestimated. The followings are the corrected estimation

$$H \approx H^{observed} + \frac{M-1}{2N} \tag{4}$$

Here $H^{observed}$ denotes the observed entropy using a finite number of N data samples to estimate the probability of M discrete states.

B. Location-based Information Measure

Information measure plays important roles in connection with secure cryptographic systems. Entropy-based arguments can provide a way to quantify consistency and uniqueness as well as upper bound on the geotag length in the geoencryption system.

i. Temporal Entropy

One important fundamental requirement of location-based information is consistency. We define temporal entropy 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. For a given grid size, the larger temporal variation, the higher the likelihood that an authorized user will not generate the correct geotag. Many factors can result in high 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.

The temporal entropy, H_T, can be computed using Eqn. (4) for given probability distribution of any quantized received location-based parameter, Y_i. The temporal entropy is inversely proportional to the parameter grid size. To ensure the user is able to generate a correct geotag and decrypt successfully, a reasonable grid size should be chosen in order to overbound the variation of the parameters. However, the grid size cannot be too excessively large as it will increase an attacker's false accept rate and reduce the total information entropy. We assume Gaussian noise in the presence of received location-based parameters and develop a model to estimate a proper grid size for each parameter. The tails of a Gaussian distribution with a known standard deviation can be computed using Q function, thus the grid size can be determined by inversing of the Q function. For instance, with a user successful decryption rate 99.9% or FRR of 0.001, grid size is approximately equal to 6.58σ. The standard deviation σ can be estimated from the measurements or calculated from the parameter variance model. If users' measurements are not long enough to estimate true σ, a σ model that gives an upper bound can be applied. Loran TOA and ECD models, developed by Dr. Ben Peterson, are shown as follows

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

$$\sigma_{ECD}{}^2 = \frac{29^2}{N * SNR} \tag{6}$$

These models are intuitively understandable. The variance of location-based parameters is inversely proportional to the SNR of the received Loran signal as well as the number of pulses to average, N. The SNR depends on the transmitter radiating power, the distance between the transmitter and receiver, and the local noise floor. The σ_{TOA} has a unit of meter while σ_{ECD} is in μsec.

ii. Spatial Entropy

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

As mentioned earlier, we model the problem as a hypothesis testing. Let the two hypotheses, H_0 and H_1, have the probability distributions P_{Q0} and P_{Q1}. The two possible errors that can be made in a decision are α = FRR for accepting hypothesis H_1 when H_0 is true and β = FAR for accepting H_0 when H_1 is true. The relative entropy $D(P_{Q0}||P_{Q1})$ is used to estimate spatial entropy that is the information to distinguish the two probability distributions by hypothesis testing. Let d(α, β) be

$$d(\alpha,\beta) = \alpha \log\frac{\alpha}{1-\beta} + (1-\alpha)\log\frac{1-\alpha}{\beta} \tag{7}$$

$$d(\alpha,\beta) \le D(P_{Q_0} \,||\, P_{Q_1}) \tag{8}$$

If a proper grid size is chosen, we can achieve α <<0, and obtain

$$FAR \ge 2^{-D(P_{Q_0}||P_{Q_1})} \tag{9}$$

$$H_S = D(P_{Q_0} \,||\, P_{Q_1}) \ge -\log FAR \tag{10}$$

Therefore, spatial entropy can be computed using attacker's FAR from Eqn. (10), which gives a theoretical lower bound of the uniqueness measure.

iii. System Information Entropy

Information entropy or information density is an indicator for quantitative information capacity of each location feature. High information entropy indicates a large potential value space of geotag. The potential information density mostly depends on the coverage of Loran transmitters as well as the grid size of the parameter. Technically speaking, the information used to compute a geotag can be estimated based on the potential information capacity of location features. However practically, if an attacker knows an authorized user's location, an attack can be performed and the effective information is reduced.

We assume the location-based parameters uniformly and independently distributed. Applying Eqn. (2), the total information entropy or geotag size in geoencryption system can be interpreted as follows

$$H = \sum_{i=1}^{N_P} (\log n_i - H_{T_i}) \tag{11}$$

N_P is the total number of location-based parameters while n_i is the possible occurrences of each individual parameter after quantizing the parameter with a particular grid size. Temporal entropy, H_T, increases FRR, degrades the reliability of the system, and reduces the total system information entropy. However, if the grid size chosen is large enough to overbound random noise and seasonal variations of the location parameters, temporal entropy can be reduced to zero.

IV. Experimental Results & Analysis

In this section, we validate and evaluate the mathematical framework of information measure using real Loran signals. Two data sets are collected to measure temporal entropy and spatial entropy. Actual Loran data is helpful for the evaluation of the information theoretic approach because there are many practical concerns that are hard to predict and model mathematically.

A. Temporal Entropy Measure

One of the error sources of Loran signals is additional secondary factor (ASF) that is the extra delay in propagation time due to the signals travel over a mixed path; partially over land with various conductivities and partially over seawater path. This delay is a significant and can introduce a position error of hundreds of meters [10]. ASF represents one of the largest error sources in Loran and many researchers have been observing and studying its characteristics in order to model its seasonal variation and provide an overbound error for Loran users. In order to observe this seasonal variation, the data set to estimate the temporal entropy should be long enough.

A seasonal monitor station, equipments of that provided by Alion Science & Technology shown in Fig. 2, has been set up at Stanford University to study the ASF characteristics in the west coast. A Locus E-field antenna and Locus SatMate 1030 receiver are used to continuously log Loran location-based parameters. A GPS receiver is used to train the Loran receiver clock. The surveyed GPS antenna position is used as a reference for ASF corrections. The Loran receiver averages the parameters every minute.

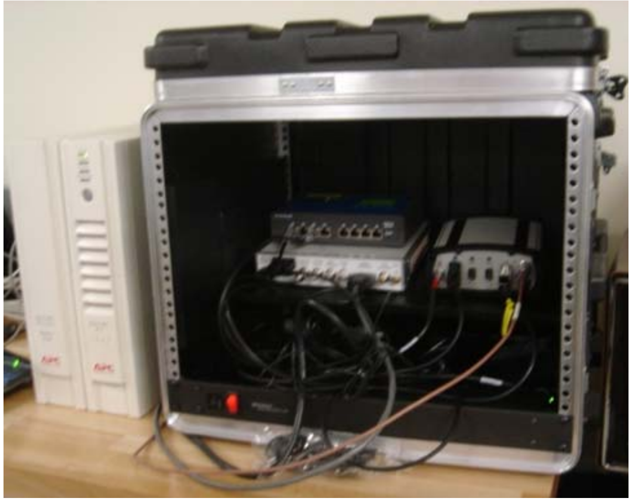

Fig. 2. Stanford Seasonal Monitor Station

We use 90-day data to investigate the temporal entropy. The raw data of TOA with zeros mean, ECD and SNR from Loran west coast chain is plotted in Fig. 3. Loran west coast chain, Group Repetition Interval (GRI) 9940, includes four stations: Fallon, George, Middletown and Searchlight. Middletown is the closest station to Stanford University. The ASF seasonal variation is observed in the TOA plot on the left.

We use TOA measurements from Middletown as an example to conduct the evaluation of consistency. Due to the seasonal change of ASF, the standard deviation of the measurements increases with time and doesn't follow Gaussian distribution. The histogram of the TOA measurements with zero mean is plotted in Fig. 4. The standard deviation for 90-day measurements is approximately 12.19 meters. The red curve is Gaussian distribution constructed using the measured standard deviation.

To measure temporal entropy accurately, it is necessary to remove this seasonal varying bias first. Many factors affect ASF, including conductivity of soil, temperature, humidity, local weather, etc. Therefore, ASF varies both temporally and spatially, and this raises the difficulty modeling ASF over CONUS. The temporal component comes from all time varying aspects; while the spatial component takes into account the non-uniform ground conductivity and topography [11]. From previous study and observation of seasonal monitor data, winter has the worst variations. East coast has significantly greater variation than the west coast.

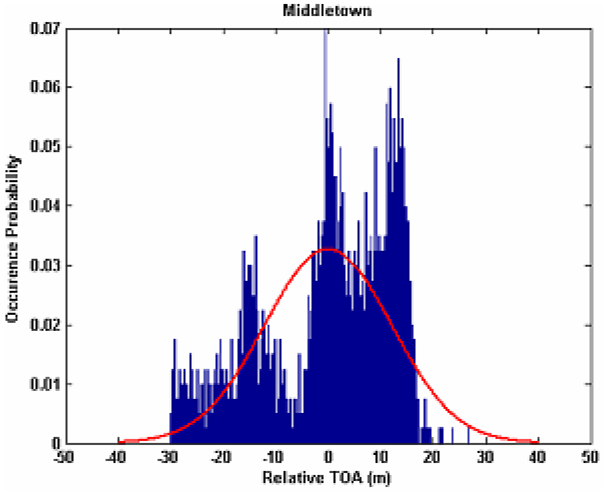

Fig. 3. Histogram of TOA from Middletown

Many methodologies have been developed to mitigate ASF. Here we just demonstrate two simple ideas: time difference and "previous day is today's correction". Time difference (TD) is to the difference in TOAs between secondary stations and the master station; thus master station is used as a reference to remove the ASF bias. The tradeoff using TD is that the total information entropy to compute the geotag is

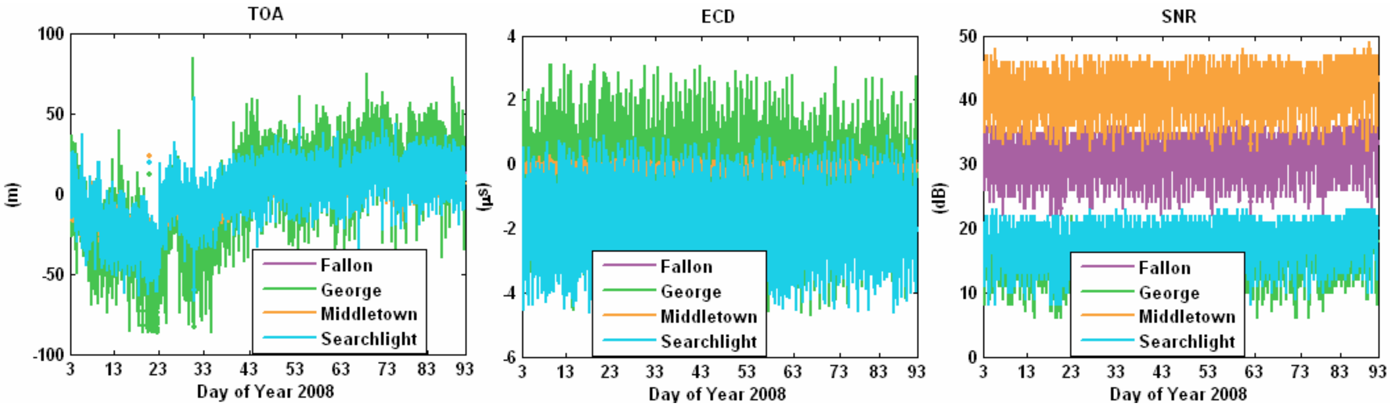

Fig. 4. Stanford Seasonal Monitor Data

reduced since we lose the TOA information from the master station. In another words, using TD can achieve high reliability or better user performance but results in less information entropy or shorter geotag. The second method is to use the previous day's ASF measurements as today's correction. This requires either the user receiver constantly monitors Loran data or a reference station that is nearby the users broadcasts previous day's ASF as a correction via a data channel. The histograms of corrected Middletown TOA using the above methods are plotted in Fig. 5.

The standard deviation of TD is 3.83 meters while the other correction method results in a standard deviation of 8.55 meters. Both methods don't remove ASF completely. TD method has spatial decorrelation due to the different propagation paths of master and secondary stations. Previous day's correction suffers from the temporal decorrelation of ASF because previous day's ASF is different from today's ASF. If the ASF corrections from Loran reference stations can be updated more frequently or broadcasted in real time, the temporal decorrelation can be reduced.

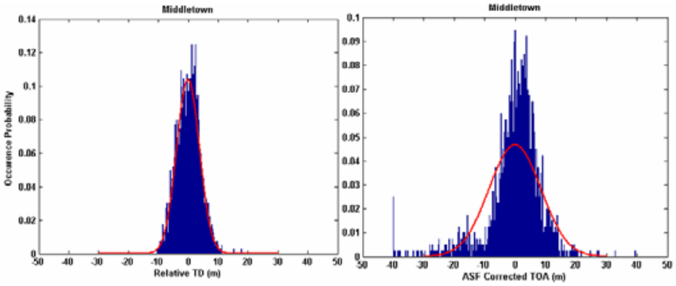

Fig. 5. Histograms of Corrected Middletown TOA.
TD (Left); "Previous day is today's correction" (Right).

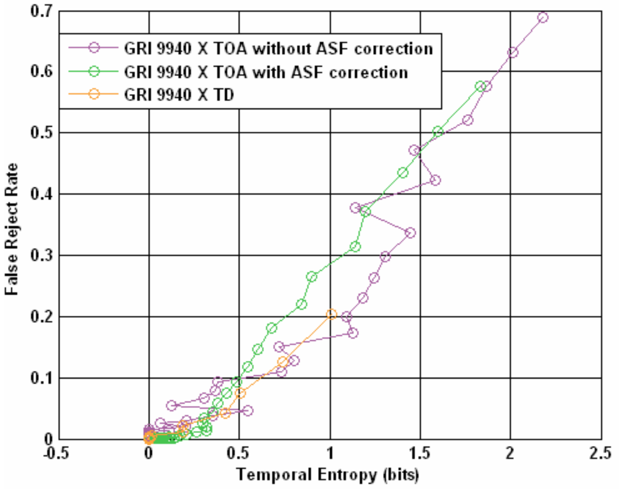

Fig. 6. FRR v.s. Temporal Entropy

Fig. 6 illustrates how FRR varies with temporal entropy of three scenarios: TOA without ASF variation, TOA corrected using previous day's ASF correction and TD of Middletown. Each maker represents a different grid size, which decreases from left to right, ranging from 100 to 10 meters. For the same grid size, TD has smaller temporal entropy than the ASF corrected TOA.

B. Spatial Entropy Measure

Key length, which is derived from secrecy of information, is sometimes used as a metric to judge the security of a cryptographic system if the protocol has been proved no analytic attacks. In geoencryption system, information entropy provides an upper limit of geotag only if the attackers have no a priori information about the user's location information. We consider the worst scenario here that the attackers not only know where the user is located but also have hardware device to receive the Loran signals and compute a geotag. Since there is no physical boundary to distinguish authorized user and attacker, there is a probability that the attackers achieve a right geotag by staying as close as possible to the user. This approach replies on a probabilistic mapping from the attackers' locations to that of the user, called "parking lot" attack. In this case, the information entropy is not a valid metric for the system security but spatial entropy.

As mentioned earlier, spatial entropy quantifies the uniqueness of location-based parameters as the parameters de-correlate as a function of physical distance. It also measures the difficulty in parking lot attack. It is necessary to examine the decorrelation distance, which is defined as the minimum distance to distinguish one location from another.

Another set of Loran data was collected using Locus H-field antenna and SatMate 1030 at 21 different locations in a parking structure at Stanford University. We collected data for 5 minutes at each location. A diagram with the numbered test locations, represented as red pushpin markers, is illustrated in Fig. 7.

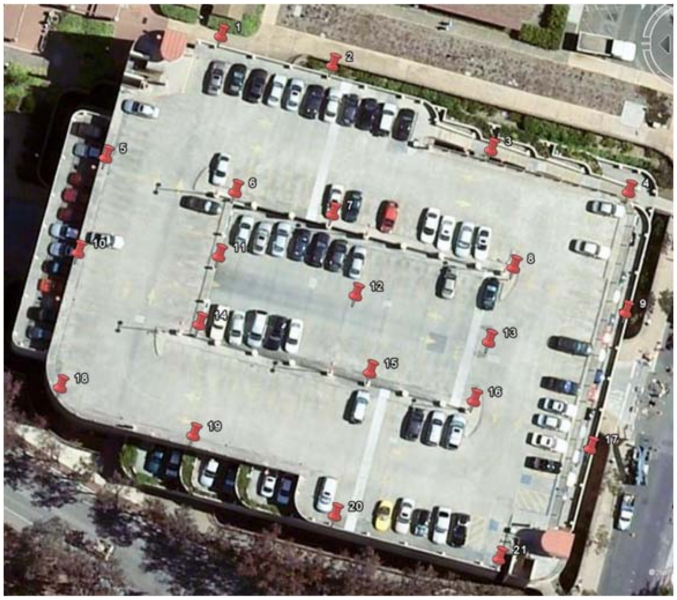

Fig. 7. Roof of Mitchell Building in Stanford University

We consider the center point, location 12, as the master location or authorized user's location and observe how the location-based parameters de-correlate as the antenna moves away from the master location. Applying Eqn. (13) discussed in previous section, we can compute the spatial entropy of all the location features. Fig. 8 illustrates the spatial entropy of TD of Middletown. As the closest station to Stanford campus, high SNR of Middletown makes the location features decorrelate quickly. To take into account seasonal variations, overbounded standard deviations and grids intervals are applied to quantize the location parameters. Since we have authenticated Loran signals and tamper resistant device, the attackers cannot project or interpolate their locations to the users'. All they can do is to rely on the mapping probability and perform trials and errors. The dark blue region has spatial entropy zero bit, and this implies that the attackers can easily achieve a correct geotag anywhere in this region. The upper left area has spatial entropy somewhere from 0 to 12 bits. The attackers need to try a number of attempts in order to receive a correct geotag. Three locations seem to be secure with spatial entropies above 40 bits. Each attempt requires at least 20 seconds considering the authentication time, discussed previously in [3]. For instance, if the spatial entropy of a location is 12 bits, attackers need to spend 22.75 hours to finish the trials of 2^{12} different attempts.

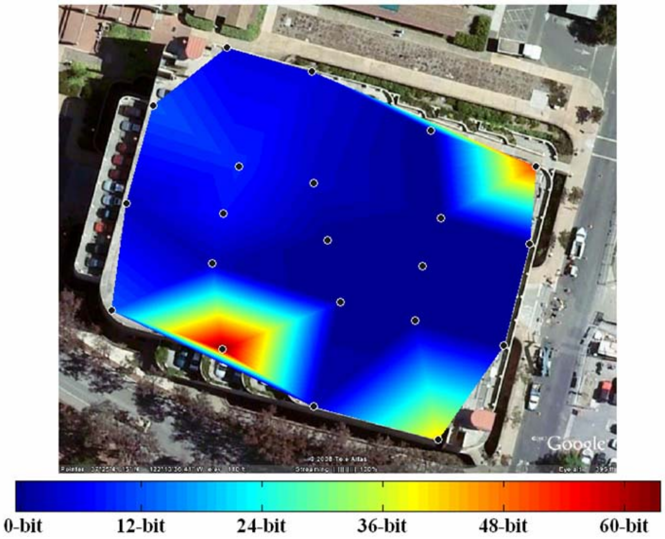

Fig. 8. Estimated Spatial Entropy of TD from Middletown

High SNR parameters provide high spatial decorrelation. From the measurements, we also validate the uniqueness of different location features: TD has the highest spatial decorrelation; ECD has the least; SNR is very sensitive to the environmental change.

C. Location Information Measure

Information entropy is an indicator for quantitative information capacity of each location feature. High information entropy can potentially result in a longer geotag as well as a higher security level of the system. In this section, we use information theoretic approach to provide an upper bound on the geotag over CONUS.

From Eqn. (11), it is easy to tell high information content requires large number of occurrences n_i but low temporal entropy H_{Ti}, where i represents each location feature. Intuitively, if the temporal entropy is equal to the information entropy, the parameter cannot be used to compute a geotag. As a feature becomes more accurate, location information content increases.

Overbounded grid sizes of location features can be obtained using the standard deviation models discussed previously. We use the signal strength model of 26 Loran stations, developed by Dr. Ben Peterson, and assume constant noise floor for each GRI [12]. The grid size, which is limited by the expected user performance, FRR, can be computed using the estimated standard deviation of location feature and desired FRR. With overbounded grid intervals, the temporal entropy is low thus the total information content only depends on location information density. With uniform and independent distribution of location-based parameters, we can analyze the availability of information entropy over CONUS. The availability contour plot is shown in Fig. 9. The FRR of 0.0001 for each location parameter is chosen to compute the grid size. The location parameters used are TD, ECD and SNR. More parameters result in higher total system entropy but degrade the user performance as overall FRR goes higher. The information entropy varies spatially because the station coverage and availability are different for each location. In this analysis, we only use the stations with SNR higher than 3 dB, which is a lower limit for receivers to demodulate Loran messages properly and authenticate successfully, discussed previously in [4]. For instance, a user at Stanford University can achieve a 66-bit theoretical system entropy with overall FRR approximately 0.001.

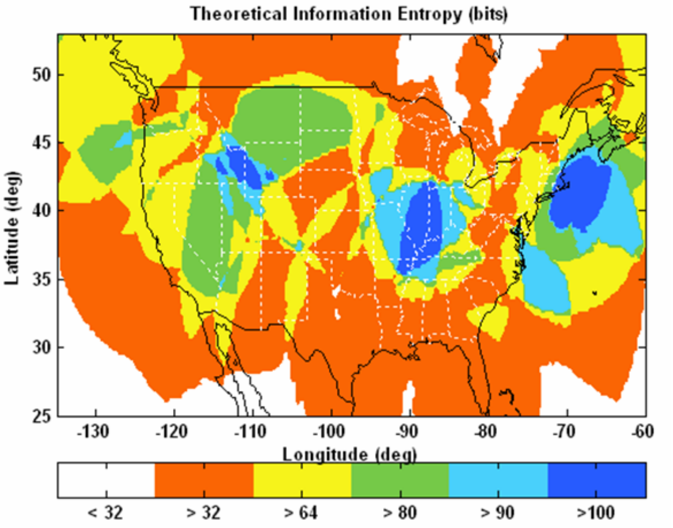

Fig. 9. Available Location Information Entropy

V. Conclusion

In this paper, we have presented an information theoretic approach to measure location information content. We have demonstrated the information measure using two different data sets with the developed mathematical framework: temporal entropy for consistency, spatial entropy for uniqueness and information entropy that limits geotag size.

Two basic methods are introduced to mitigate the seasonal ASF effects: time differencing correction and "previous day is today' correction". In addition, we validate the temporal entropy can be traded off between spatial entropy and information entropy by varying the grid sizes. The standard deviation models of location features are used to estimate an upper bound of grid interval sizes to achieve zero temporal entropy if ASF seasonal variations have been corrected. Furthermore, the preliminary result shows spatial entropy of 12 to 60 bits can be achieved when the decorrelation distance is 40 meters. One typical measure of cryptographic attack difficulty is time. Converting the spatial entropy to time, 12-bit and 60-bit are equivalent to 22.75 hours and 2.5×10^{11} years, respectively.

In this study, we also examine and compare the consistency and uniqueness of different location-based parameters using collected Loran data. Different location parameters provide different strength and information content. Future work includes studying the correlation between different location based parameters as high correlation coefficient reduces the total information entropy, investigating more usable location-based parameters to generate a more robust geotag and developing algorithms to improve the system performance.

ACKNOWLEDGMENT

The authors would like to thank Mitch Narins of the FAA, Loran Program Office for supporting this effort. In addition, we would like to thank Prof. Dan Bohen of Stanford University, Dr. Greg Johnson, Ruslan Shalaev and Christian Oates from Alion Science & Technology for providing us the Stanford Seasonal Monitor data collection equipments. Finally, thanks go to US Coast Guard (USCG) Loran Support Unit (LSU) for the use of their equipment in our testing.

REFERENCES

[1] L. Scott, D. Denning, "Location Based Encryption & Its Role In Digital Cinema Distribution", *Proceedings of ION GPS/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, S. Lo, and P. Enge, "Geoencryption Using Loran", *Proceeding of ION NTM 2007*.

[4] D. Qiu, "Security Analysis of Geoencryption: A Case Study using Loran", *Proceeding of ION GNSS 2007*.

[5] International Loran Association (ILA), "Enhanced Loran (eLoran) Definitions Document", January 2007. Available at the ILA website.

[6] T. Cover, Elements of Information Theory. John Wiley & Sons, Inc. 2001.

[7] S. Kullback, Information theory and statistics. John Wiley & Sons, NY. 1959.

[8] M.S. Roulston, "Estimating the errors on measured entropy and mutual information". Physica D, 125, 285-294.

[9] C. Cachin, "Entropy Measures and Unconditional Security in Cryptography". Ph.D Thesis.

[10] S. Lo, R. Wenzel, G. Johnson, and P. Enge, "Assessment of the Methodology for Bounding Loran Temporal ASF for Aviation". *Proceeding of ION NTM 2008*.

[11] P. Swaszek, G. Johnson, R. Hartnett, and S. Lo, "An Investigation into the Temporal Correlation at the ASF Monitor Sites". *Proceedings of ILA 36th Annual Meeting 2007*.

[12] Loran-C Signal Specification. Available at the navigation center website.