DEMO: Demonstrating a Trust Framework for Evaluating GNSS Signal Integrity

Xihui Chen[†*], Carlo Harpes[♯], Gabriele Lenzini[†], Miguel Martins[♯], Sjouke Mauw[†], Jun Pang[†]

[†]University of Luxembourg, Luxembourg [♯]itrust consulting s.à r.l., Luxembourg

ABSTRACT

Through real-life experiments, it has been proved that spoofing is a practical threat to applications using the free civil service provided by Global Navigation Satellite Systems (GNSS).

In this paper, we demonstrate a prototype that can verify the integrity of GNSS civil signals. By *integrity* we intuitively mean that civil signals originate from a GNSS satellite without having been artificially interfered with. Our prototype provides interfaces that can incorporate existing spoofing detection methods whose results are then combined into an overall evaluation of the signal's integrity, which we call *integrity level*. Considering the various security requirements from different applications, integrity levels can be calculated in many ways determined by their users. We also present an application scenario that deploys our prototype and offers a public central service – *localisation assurance certification*. Through experiments, we successfully show that our prototype is not only effective but also efficient in practice.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection*

Keywords

GNSS signal; signal integrity; spoofing

1. INTRODUCTION

The free access to the civil localisation service of Global Navigation Satellite Systems (GNSS) has been popularising numerous location-based applications which have penetrated into people's daily life from leisure activities, such as geo-social networks, to safety-critical products, such as driverless cars. However, different from military signals, civil GNSS signals are neither signed nor encrypted. This leads to the problem that their originators cannot be authenticated. Besides this, due to the weak strength when transmitted in the open air, they can be easily taken over by false signals. Such attacks are called *spoofing* [4]. It has been demonstrated by a number of scientific experiments (e.g., see [3]) that receivers can be fooled by spoofed signals to calculate wrong locations.

Navigation message authentication is considered as an effective method to prevent spoofing attacks. However, this is not feasible in the near future due to the difficulties to upgrade the current GNSS infrastructure. Although the European GNSS – Galileo is planning to offer authenticated civil services, it is not free and also not accessible to everybody. In the literature, a number of methods have been proposed aiming to *detect spoofing* instead of *preventing spoofing*. A spoofing detection method usually makes use of an observable feature of GNSS signals that should be present when they are not spoofed. The absence of the feature will lead to an alarm of spoofing. Otherwise, a claim of signal integrity will be issued. For instance, as integrous signals have signal strength smaller than -153.5 dBW, given a signal with a larger power the corresponding spoofing detection method will conclude that the signal is spoofed.

Spoofing detection methods explore two inference rules. For instance, when signal strength is used, they are formulated as follows:

$$\textit{signal strength} \leq -153.5\ dBW \rightarrow \textit{the signal received is integrous};$$
$$\textit{signal strength} > -153.5\ dBW \rightarrow \textit{the signal received is spoofed}.$$

Meanwhile, these inference rules can also be interpreted as the causal relations between the precedents and the conclusions, e.g., whether the strength is smaller than -153.5 dBW and whether the signal is integrous, respectively.

However, these inference rules do not capture the correct causal relations between observed features and signal integrity. For example, signal strength is a physical attribute of GNSS signals. Its value is measured by a certain sensor which takes signals as input. Therefore, if the received signal is integrous then its strength is smaller than the threshold (-153.5 dBW). However, "the observation that the signal strength is larger than the threshold implies that the signal is integrous" is a false statement. Moreover, after having studied several spoofing detection methods, we concluded that additional conditions are required to express the causal relations, as some observed features are not only caused by the current signal but are also related to past signals. For instance, users' future locations can be predicted based on their current positions and other information such as direction and velocity. An existing spoofing detection method makes use of the distance between the locations calculated and the predicted ones. Once the distance is small enough, it will claim integrity of the signal. In fact, the integrity of the current signal only cannot enforce the small distance. We also need to ensure the correctness of the prediction which is decided by the integrity of the past signal used to calculate the past position.

The impacts of environmental noise on attributes of signals are not fully addressed in the literature. The noise caused by natural facts such as reflection can lead to significant variance in the

*Supported by the National Research Fund, Luxembourg (SECLOC 794361).

CCS'13, November 4–8, 2013, Berlin, Germany.
ACM 978-1-4503-2477-9/13/11.
http://dx.doi.org/10.1145/2508859.2512492.

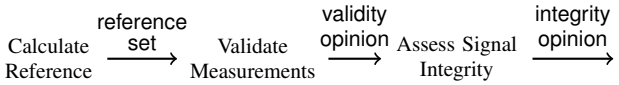

Figure 1: Main steps to derive an integrity opinion.

measurements of some attributes. Thus, some expected observable features can be violated even if the signal is not spoofed. A qualitative conclusion, as usually given by the existing spoofing detection methods, cannot capture uncertainty in such cases.

We proposed a trust framework [1] to evaluate the integrity of GNSS signals. Informally, a received signal is integrous if it has originated from a GNSS satellite without having been artificially interfered with. Our framework provides a formal characterisation of spoofing detection methods and the causal relationships used by them. Subjective logic is exploited to infer signal integrity from observations and it can capture the uncertainty caused by unpredictable environmental noise. This leads to a quantitative opinion on signal integrity. Subsequently the quantification allows us to develop meaningful algorithms to combine the outputs of different spoofing detection methods.

Our contributions. We develop a prototype based on the trust framework [1] to provide a general software structure to make use of existing spoofing detection methods. It takes the measurements of attributes of received signals as input and outputs an overall conclusion on the signal integrity. We take into account the diversity of users' security requirements and provide a customisable evaluation process. For instance, users can cater the evaluation according to the quality of their localising devices and ever-changing environment. To demonstrate the marketing potentials of our prototype, we implemented a public service – *location assurance certification*. With extensive experiments, we show that our prototype is not only effective but also efficient in practice.

2. TRUST FRAMEWORK OVERVIEW

We give a brief introduction to our trust framework [1]. Fig. 1 shows the three steps in the framework to use a spoofing detection method to check signal integrity. Intuitively, a spoofing detection method takes a measurement of an attribute of a received signal (e.g., signal strength) as input and outputs its assessment on the signal's integrity which is in the form of a *subjective logic opinion*. A subjective logic opinion expresses the belief of an agent on the truth of a (multiple) proposition(s) [2]. For instance, $w_x^A = (b, d, u, a)$ is the opinion of A on the truth of x, where b, d and u describes A's belief, disbelief and uncertainty, respectively; and a is the *a priori* probability that x is true. Furthermore, we have $b + d + u = 1$ and the *expectation probability* of x being true is calculated as $b + a \cdot u$.

A spoofing detection method first calculates a set of predicted values for an attribute if the signal is integrous, called *reference set*. Subsequently, it will check whether the measurement of the attribute of the received signal is in the reference. If it is, the measurement is valid. The output of this step is called *valid opinion* which in fact expresses the belief on the presence of an observable feature. Its calculation captures the impact of environmental noise. The last step clarifies the causal relationship between the observation of a received signal and its integrity. For example, with regards to signal strength, the causal relation is '$the\ received\ signal\ is\ integrous \rightarrow signal\ strength \leq -153.5\ dBW$'. We also identify another type of spoofing detection methods whose causal relationships contain past signals' integrity in the precedent. For example, in the inertial spoofing detection, the causal relationship can be formulated by $if\ referred\ past\ signals\ and\ current\ signal\ are\ integrous \rightarrow the\ calculated\ location\ is\ close\ to\ the\ predicted\ location$. These

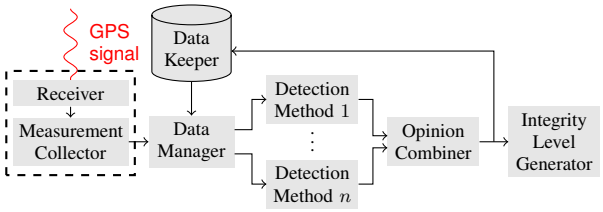

Figure 2: The components of the prototype.

relationships show that the reasoning of signal integrity based on observed features is *abductive* but not *deductive*. The output of this step is called *integrity opinion*.

Given multiple spoofing detection methods, for a received signal, we will obtain multiple integrity opinions. They are different from each other due to the various features of signal attributes in detecting spoofed signals. Thus, an overall integrity opinion is necessary to resolve the difference. To combine the different integrity opinions, three algorithms are proposed to meet the various security requirements of applications – Veto, Consensus and Combined. The Veto algorithm returns the opinion which indicates the largest probability of spoofing. It gives conservative results and can be used in safe-critical applications. However, false alarms of spoofing are quite possible due to the abrupt changes on signal attributes caused by environmental noise. The Consensus algorithm makes use of the *fusion* operation on subjective logic opinions. Intuitively, it ensures that the integrity opinions with less uncertainty are more important in the combined opinion. Compared with the Veto algorithm, the Consensus algorithm generates fewer false claims of spoofing but may output more false claims of integrity, especially in the case where attackers have more power to tune signal attributes. The Combined algorithm aims to reach a balance between false alarms of spoofing and false claims of integrity. It returns the consensus of *VETO opinions* which indicate large probabilities of spoofing with small uncertainty. When VETO opinions do not exist, the Consensus algorithm will be used.

3. PROTOTYPE

We have developed a prototype based on the trust framework. It collects the measurements of received GPS (Global Positioning System) signals from receivers in real time and returns the signal integrity to users in terms of *integrity levels*.

Our prototype allows a user to customise the integrity evaluation process according to the real-time environment in order to obtain more reliable results. First, a user can disable some spoofing detection methods in certain cases when they are likely to calculate incorrect integrity opinions. For instance, when driving in a forest, a user wants to stop using detection methods relying on signal strength due to the significant fluctuations caused by trees. Second, a user can choose the algorithm to combine integrity opinions from different spoofing detection methods according to the service he is requesting. Last, a user can notify our prototype of the type of his receiver. This is necessary because receivers may differ in terms of computation power and antennas. The variants lead to different measurements of some attributes even for the same signal. In our prototype, we make a simple classification – professional and commercial-off-the-shelf, and assign different values to the *a priori* parameters used during the evaluation process.

We show in Fig. 2 the components of our prototype. Upon receiving a signal, the receiver calculates its location. Meanwhile the *measurement collector* (MC) starts gathering the values of the attributes measured by the receiver during localisation and subsequently send them to the *data manager* (DM). We organise and

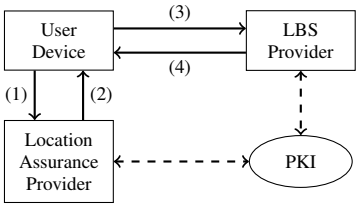

Figure 3: Location Assurance Provider

record the measurements in the form of XML (Extensible Markup Language) due to its simplicity and generality. The preference of a user to customise the integrity evaluation is also added, including the spoofing detection and combination algorithms to run. The DM prepares and distributes the input for each spoofing detection method. Besides the measurements of signal attributes, other information is also included in the inputs, such as the integrity opinions of related past signals and parameters to calculate reference sets. All such information is stored and managed by the *data keeper* (DK). Integrity opinions are calculated by spoofing detection methods and then sent to the *opinion combiner* (OC) which calculates the overall integrity opinion according to the user's requirement contained in the XML file. In the end, the combined integrity opinion is transformed into an *integrity level* between 1 to 5 which is intuitive and easy for users to understand. Specifically, a signal is labelled by integrity level i if the expectation probability of the integrity opinion is between $0.2 \cdot (i-1)$ and $0.2 \cdot i$.

Note that MC should be installed on the device equipped in the receiver so as to have access to the measurements of signals (see the dashed rectangle in Fig. 2). The other components can be deployed and run on remote agents. However, the communication between them should be well designed as users' locations are acknowledged as an important piece of private information.

4. LOCATION ASSURANCE PROVIDER

To demonstrate our trust framework for evaluating GNSS signal integrity, we present an implementation of a public service – *location assurance certification* based on our prototype in practice. *Location-based services* (LBS) are services customised according to users' locations. Delivering a service calculated with a wrong location will lead to security concerns such as privacy leakage. Take location-based local friend search as an example. Users send requests to LBS providers for the list of friends who are close to them in order to have a common activity. By feeding a user's device with false locations, attackers can learn the locations of any friends of the user which should not be revealed according to the user's real location. To fight against such attacks, only to protect users' device from malware is not sufficient because spoofing is still possible.

We have implemented a trusted central server called *location assurance provider* (LAP) based on our prototype to evaluate signals' integrity and issue a certificate on their integrity levels (called *location assurance certificate*). The certificate is then sent to the LBS provider who will verify and adjust its policy (e.g., stop or continue) to deliver the service according to the integrity level. Fig. 3 shows the main steps for a user to request an LBS using location assurance certification. Before sending a request to the LBS provider, the user device first collects the measurements of received signals and contacts the LAP to evaluate their integrity (step (1)). Upon receiving the location assurance certificate (step (2)), the user sends an LBS request together with the certificate (step (3)) to the LBS provider. The provider checks the validity of the certificate and returns the service catered in terms of the integrity level attached (step (4)). To accomplish the scheme, a public key infrastructure (PKI) is required to manage the LAP's public key. Besides the LAP we also implement an Android application which runs on users' mobile devices. In fact, the application works as the measurement collector (MC in Fig. 2) and takes charge of communicating with the LAP. We use a 3G telecommunication network to establish the connection with the LAP. According to our test, the average transition time of a message is about 2 seconds.

Table 1: Computation time of a request.

# users	100	200	300	400	500
avg. time (s)	0.1	0.7	2.5	2.6	3.7

We test the efficiency and effectiveness of the LAP in terms of computation time and numbers of false conclusions. The LAP is run on a virtual machine with 4G RAM and an Intel Xeon E5-2640 processor. Tab. 1 shows the average computation time for a request when different number of users send requests concurrently – it increases when the number of requests gets large. This is because for a request, the LAP needs two operations on the database (read parameters and store integrity opinions) which takes about 90% of the computation time. However, even with the current setting, for 500 requests, we need less than 4 seconds which is still acceptable. More efficient database techniques can improve the parallelism of the computation. Fig. 4 shows the distributions of integrity levels of four spoofing detection methods[1] and our three integration algorithms on a dataset of signals which contains about 18% of spoofed signals. We can see that the integrity opinions vary over the different detection methods and the Combined algorithm gives the results with the minimum number of false alarm and false claims.

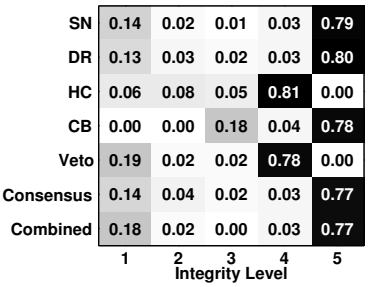

Figure 4: Integrity opinions

5. CONCLUSION

We have developed a software prototype to evaluate the integrity of GNSS signals. It offers a general framework to exploit existing spoofing detection methods. With this prototype, we implemented a public service – location assurance certification and illustrated the marketing potentials of our prototype through experiments.

6. REFERENCES

[1] X. Chen, G. Lenzini, M. Martins, S. Mauw, and J. Pang. A trust framework for evaluating GNSS signal integrity. In *Proc. 26th IEEE Computer Security Foundations Symposium (CSF)*, pages 179–192. IEEE Computer Society, 2013.

[2] A. Jøsang. Subjective logic (book draft). `http://folk.uio.no/josang/papers/subjective_logic.pdf`, 2012.

[3] M. Mixon. Todd Humphreys' research team demonstrates first successful GPS spoofing of UAV. `http://www.ae.utexas.edu/news/archive/`, 2012.

[4] J. S. Warner and R. G. Johnston. A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing. *Journal of Security Administration*, 25(19), 2002.

[1]SNR, DR, CB and HC are short for signal-to-noise ratio, Doppler ratios, clock bias and height comparison, see [1] for more details.