A Research On Authentication System Based On Space

Caixia Wang

School of Software, University of Science and Technology Liaoning, China

aswcx1980@126.com

Abstract

A system and methods for location based authentication using medium earth orbit (MEO) and low earth orbit (LEO) satellites are presented. Location of a client device is authenticated based on at least one client received MEO satellite signal received from at least one MEO satellite at the client device and at least one client received LEO satellite signal received from at least one LEO satellite at the client device.

Keywords

Space; signals; low and medium; earth; orbit.

1. Introduction

A significant fraction of power of satellites signals such as a Global Navigation Satellite System (GNSS) signal may be lost in urban and indoor environments where satellites signals are frequently blocked. Blocking satellite signals weakens coverage in urban and indoor environments, and loss of power degrades performance in low signal to noise ratio (SNR) environments. Degraded performance in low SNR environments may prevent or minimize an ability of an authentication system to validate that a position computation or an assertion based on a position is bona fide.

2. A method for location based authentication using medium earth

A method for location based authentication using medium earth orbit (MEO) and low earth orbit (LEO) satellites, the method comprising: receiving at a server a client MEO signal signature comprising samples over an MEO signature time period of at least one client received MEO satellite signal received at a client device from at least one MEO satellite footprint of at least one MEO satellite; constructing a server MEO signal signature comprising samples over the MEO signature time period of at least one server received MEO satellite signal received from the at least one MEO satellite; comparing the client MEO signal signature and the server MEO signal signature to provide an MEO comparison result; receiving at the server a client LEO signal signature comprising samples over an LEO signature time period of at least one client received LEO satellite signal received at the client device from at least one LEO satellite footprint of at least one LEO satellite; constructing a server LEO signal signature comprising samples over the LEO signature time period of at least one server LEO satellite signal of the at least one LEO satellite; comparing the client LEO signal signature and the server LEO signal signature to provide an LEO comparison result; and authenticating that the client device is at an asserted location based on the MEO comparison result and the LEO comparison result to authenticate the asserted location of the client device.

A server client data module operable to: receive a client MEO signal signature comprising samples over an MEO signature time period of at least one client received MEO satellite signal received from at least one MEO satellite; and receive a client LEO signal signature comprising samples over an LEO signature time period of at least one client received LEO satellite signal received from at least one LEO satellite; a server data module operable to: construct a server MEO signal signature comprising samples over the MEO signature time period of at least one server received MEO satellite signal received from the at least one MEO satellite; and construct a server LEO signal signature comprising samples over the LEO signature time period of at least one server LEO satellite signal of the at least one LEO satellite; and a comparison module operable to: compare the client MEO signal

signature and the server MEO signal signature to provide an MEO comparison result; and compare the client LEO signal signature and the server LEO signal signature to provide an LEO comparison result.

3. system for authenticating an asserted location based

Fig. 1 is an illustration of communication system (system) for authenticating an asserted location based on satellite signals according to an embodiment of the disclosure. The system may comprise MEO satellites , and , orbiting in a medium earth orbit (MEO) , LEO satellites , and , orbiting in a low earth orbit (LEO) , an optional terrestrial broadcast station (terrestrial source), a client comprising a satellite receiver 200, an authentication server comprising a satellite receiver 200, and a host network .

In one embodiment, an MEO satellite signal from at least one of the MEO satellites , , and in MEO and an LEO satellite signal from at least one of the LEO satellites , and in LEO are combined.

In another embodiment, the MEO satellite signal from at least one of the MEO satellites in the MEO and the LEO satellite signal from at least one of the LEO satellites in LEO are augmented by coded terrestrial signals from the terrestrial source .

The LEO satellites may comprise, for example but without limitation, satellites from the Iridium(TM), Iridium(TM) NEXT, GlobalStar constellations, or other satellite that may be utilized for position, navigation, or timing related applications.

The MEO satellites may comprise, for example but without limitation, a Global Navigation Satellite System (GNSS) satellite, a Global Positioning System (GPS(TM)) satellite, a Globalnaya Navigatsionnaya Sputnikovaya Sistema (GLONASS(TM)) satellite, a BeiDou Navigation System (COMPASS(TM)) satellite, a Galileo(TM) satellite, or other satellite that may be utilized for position, navigation, or timing related applications.

The terrestrial source may comprise a cell phone base station, a wireless or wired access point, or other terrestrial source.

The MEO satellite signal from the MEO satellite can be processed at the client receiver module 200 of the client to determine location , velocity and time of the client . The LEO satellite signal from the LEO satellite (e.g., Transit Satellite Navigation) can also be processed to yield estimates of location , velocity and time of the client.

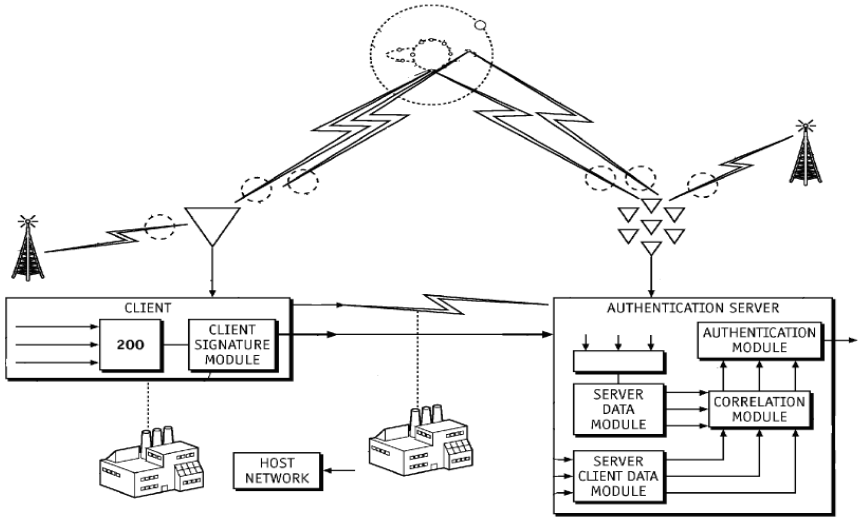


FIG. 1 is an illustration of communication system (system)

The location of the client may be estimated using measurements made available from the MEO satellite signal from at least one of the MEO satellites and the LEO satellite signal from at least one of the LEO satellites . The estimates of the location are based on a minimum set of signal sources. System applies to similar systems with a few MEO satellites plus a few LEO satellites, with or

without a high quality user clock. Any suitable mathematical technique may be used to estimate the location based on, for example, a minimum set of signal sources.

System enables space based authentication indoors and downtown. System is configured to work with sparse sets of visible satellites; one MEO satellite and one LEO satellite are sufficient. If one MEO satellite and one LEO satellite are visible, then the system is capable of instantaneously estimating and authenticating location in two dimensions if a third dimension (e.g., altitude) is known and the user equipment has a clock with adequate accuracy.

The client signature module is configured to construct a client MEO signal signature comprising samples over an MEO signature time period of at least one client received MEO satellite signal . The client signature module is also configured to construct a client LEO signal signature comprising samples over an LEO signature time period of at least one client received LEO satellite signal . The client signature module is also configured to construct a client terrestrial signal signature comprising a client terrestrial time window of at least one client received terrestrial signal . The client received MEO satellite signals , the client received LEO satellite signal , and the client received terrestrial signal may be collectively referred to as client received signals , , herein. Also, the client MEO signal signature , the client LEO signal signature , and the client terrestrial signal signature may be collectively referred to as signature signals , a client signature set , or location signatures herein.

The authentication server is configured to receive or estimate the signature signals , and (client signature set) for the location . The authentication server may receive the client signature set via a wired communication link , a wireless communication channel , a combination thereof, or estimate the client signature set locally at the authentication server . The authentication server may comprise the satellite receiver 200 (server receiver module 200), a server client data module , a server data module , a correlation module , and an authentication module .

The server receiver module 200 may also be configured to receive at least one MEO satellite signal at the authentication server (server device) to provide at least one server received MEO satellite signal . The server receiver module 200 is also configured to receive at least one LEO satellite signal at the server device to provide the at least one server LEO satellite signal . The server receiver module 200 may also be configured to receive at least one terrestrial signal at the server device to provide the at least one server received terrestrial signal . The server LEO satellite signal, the server received MEO satellite signal, and the server received terrestrial signal may be collectively referred to as server received signals, , herein.

The client received LEO satellite signal may comprise two client received LEO satellite signals received from two of the LEO satellites and . The server LEO satellite signal may comprise two server received LEO satellite signals from the two of the LEO satellites and .

The server client data module is configured to receive the client MEO signal signature comprising samples over an MEO signature time period of at least one client received MEO satellite signal received from at least one of the MEO satellites . The server client data module is also configured to receive a client LEO signal signature comprising samples over an LEO signature time period of at least one client received LEO satellite signal received from at least one LEO satellite. The server client data module may also be configured to receive a signal signature comprising a time window of at least one client received terrestrial signal received from at least one terrestrial source.

The authentication module is configured to authenticate the location of the client device based on the MEO comparison result and the LEO comparison result . In one embodiment, the authentication module is configured to authenticate the location of the client device based on the MEO comparison result , the LEO comparison result , and the terrestrial comparison result . The authentication module is also configured to generate an authentication message indicating an authentication decision. In at least one embodiment, the authentication module may be configured to generate an authentication message that may be used by another module to make the authentication decision and may further assist in carrying out the appropriate action associated with that decision which may comprise,

without limitation, granting the client device access to a protected resource and rejecting the client device access to a protected resource.

4. Illustration of an exemplary flow chart showing a client location-based authentication process according to an embodiment of the disclosure

The various tasks performed in connection with the process may be performed by software, hardware, firmware, a computer- readable medium having computer executable instructions for performing the process method, or any combination thereof. The process may be recorded in a computer- readable medium such as a semiconductor memory, a mag¬netic disk, an optical disk, and the like, and can be accessed and executed, for example, by a computer CPU such as the processor modules 1406/1432 in which the computer-read- able medium is stored.

It should be appreciated that process may include any number of additional or alternative tasks, the tasks shown in FIG. 2 need not be performed in the illus¬trated order, and process may be incorporated into a more comprehensive procedure or process having additional functionality not described in detail herein. In some embodi¬ments, portions of the process may be performed by different elements of the systems 100, 600, and 1400 such as: the client 126, the authentication server 128, etc. Process may have functions, material, and structures that are similar to the embodiments shown in FIGS. Therefore common features, functions, and elements may not be redundantly described here.

Process may begin by receiving at least one client received MEO satellite signal at a client device from at least one MEO satellite . The at least one MEO satellite may comprise, for example but without limitation, a Global Navigation Satellite System (GNSS) satellite, a Glo¬bal Positioning System (GPS™) satellite, a Globalnaya Navi- gatsionnaya Sputnikovaya Sistema (GLONASS™) satellite, a BeiDou Navigation System (COMPASS™) satellite, a Galileo™ satellite, or other satellite that can be used to sup¬port positioning, navigation, or timing related applications.

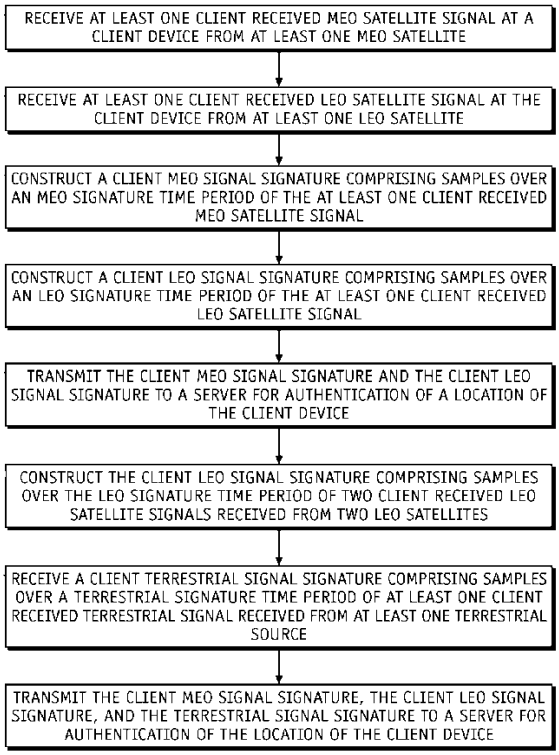
Process may then continue by receiving at least one client received LEO satellite signal at the client device from at least one LEO satellite .

Process may then continue by constructing a client MEO signal signature comprising samples over an MEO signature time period of the at least one client received MEO satellite signal .Process may then continue by constructing a client LEO signal signature comprising samples over an LEO signature time period of the at least one client received LEO satellite signal.

Process may then continue by transmitting the client MEO signal signature and the client LEO signal signa- ture to a server for authentication of a location of the client device .Process may then continue by constructing the client LEO signal signature comprising samples over samples over the LEO signature time period of two client received LEO satellite signals received from two LEO satellites .Process may then continue by receiving a cli¬ent terrestrial signal signature comprising samples over a client terrestrial time period of at least one client received terrestrial signal received from at least one terrestrial source.Process may then continue by transmitting the client MEO signal signature, the client LEO signal signature, and the terrestrial signal signature to a server for authentica-tion of the location of the client device .

In this manner, embodiments of the disclosure pro¬vide protection against spoofing and counterfeiting such as proximate and offshore attacks, and strong coverage in urban and indoor environments where satellites signals are fre¬quently blocked. Embodiments of the disclosure provide an authentication system that allows adequate received signal strength for a navigation satellite signal to be received at a client device located in a low signal-to-noise-ratio (SNR) environment such as indoors and downtown.

While at least one example embodiment has been presented in the foregoing detailed description, it should be appreciated that a vast number of variations exist. It should



5. Conclusion

Many financial transactions utilize mobile devices such as cell phones or laptops such as the client indoors or downtown. Such financial transactions may occur on platforms that are low cost and operating in obstructed signal environments. Two criteria may be important to a design of such a cost effective satellite based authentication system. First, data should be available from the satellite receiver 200 included in the cell phone. Second, the satellite based authentication system should operate with the client received signals , , and that are expected where cell phone users congregate indoors and downtown.

References

[1] Surface Reconstruction by a Gauss Kernel Integration Approach[A]. 2014 7− (th) International Conference on Signal Processing Proceedings[C]. 2014

[2] Kunihiro Sato,Atsuhiko Sugita,Masakazu Morimoto,Kensaku Fujii. Reconstruction of Full-Color Images with a RGB Time-Sharing Holographic Display System[A]. Proceedings of 20th Congress of the International Commission for Optics[C]. 2013

[3] RBF Neural Networks and Cross Validation-based Signal Reconstruction for Nonlinear Multi-functional sensor[A]. Proceedings of 2010 9th International Conference on Signal Processing(ICSP'2010)[C]. 2010

[4] MENG Xiangwei. Sampling and Reconstruction of Bandpass Signal[A]. Proceedings of 2013 3rd International Conference on Signal Processing(ICSP'2013) Volume [C]. 2013

[5] Ch.R.Koenig,D.H.Mueller,K.D.Thoben. Detection and Reconstruction of Impact Loads within Fibre Reinforced Polymers with an Estimation of Its Damage Relevance[A]. Abstract Proceedings of the International Conference on Experimental Mechanics 2013 (ICEM 2013)[C]. 2013