Distributed Hardware Literature Review[1]

FOAM Protocol Research links

LPWAN (Low Power Wide Area Network)

Properties of LPWAN:

- Long Range
- Ultra low power operation
- Low Cost
- Scalability

Low Power Wide Area Networks: An Overview[2]

Raza, Usman, Parag Kulkarni, and Mahesh Sooriyabandara

This review paper presents the design goals and the techniques, which different LPWA technologies exploit to offer wide-area coverage to low-power devices at the expense of low data rates. We survey several emerging LPWA technologies and the standardization activities carried out by different standards development organizations. The success of LPWA technologies lies in their ability to offer low-power connectivity to massive number of devices distributed over large geographical areas at an unprecedented low-cost. This section describes the techniques LPWA technologies used to achieve these often conflicting goals.

[1] *add new research as noted in the syle guidlines in the appendix.*
[2] IEEE Communications Surveys & Tutorials 19.2 (2017)

LoRaWAN

LoRa Wide-Area Networks from an Internet of Things Perspective[3]

Alexandru Lavric, Valentin Popa

> The main contribution of the paper is the performance evaluation of the LoRa technology considering the requirements of IoT. In the first part of this paper LoRa technology is summarized by reviewing some aspects regarding the architecture and the security of the technology, meanwhile in the second part of the paper are presented some simulation scenarios.

FOAM Note: *This paper has great technical comparison charts between the different chip types.*

Understanding the limits of LoRaWAN[4]

Ferran Adelantado, Xavier Vilajosana, Pere Tuset-Peiro, Borja Martinez, Joan Melià-Seguí, Thomas Watteyne

> Low-power wide area networking technology offers long-range communication, which enables new types of services. Several solutions exist; LoRaWAN is arguably the most adopted. It promises ubiquitous connectivity in outdoor IoT applications, while keeping network structures and management simple.

Wireless position location: fundamentals, implementation strategies, and sources of error[5]

K.J. Krizman, T.E. Biedka, T.S. Rappaport

> This paper presents an overview of basic RF position location strategies which are feasible for ubiquitous deployment by cellular-type wireless system providers. Limitations on the practical ability to locate mobile RF transmitters and the effects of real world channel degradation on direction-finding and time difference of arrival systems are also discussed.

FOAM Note: *Appears to be a canonical paper on the subject*

[3] 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)

[4] IEEE Communications Magazine (Volume: 55 , Issue: 9 , Sept. 2017)

[5] 1997 IEEE 47th Vehicular Technology Conference. Technology in Motion

GPS-free Geolocation using LoRa in Low-Power WANs[6]

Bernat Carbonés Fargas, Martin Nordal Petersen

Internet of Things (IoT) has been growing over the last few years in multiple applications and due to the high need GPS for tracking capabilities, an innovative opportunity arises. This paper reports on a design and implementation of a LoRaWAN tracking system which is capable exploiting transmitted packages to calculate the current position without the use of GPS or GSM. This is done using the low power technology LoRa where the geolocation is calculated applying a multilateration algorithm on the gateways timestamps from received packages. The whole system consisted of an end-node, four gateways, a server and a java application to store the obtained data in a MySQL database.

The three most common methods used for performing the geolocation are **triangulation**, **trilateration** and **multilateration**.

Triangulation uses angles of incidence of the signal received from the transmitter. A triangle is defined with two of them and the end-node position is estimated applying trigonometric formulas.

Trilateration requires the distance between the transmitter and the receiver, which can be obtained from the time of arrival (TOA), the time of flight (TOF) or from the received signal strength indicator (RSSI). Therefore, it requires synchronization between the transmitter and the receiver. The position is the intersection of the three circles obtained from the different distances.

Multilateration is quite similar to trilateration; however, the main feature to compute the location is the time difference of arrival (TDOA). The transmitters are synchronized to each other, whereas the receiver does not need to be. Thus, the location in this technique is the intersection of at least two hyperbolas (three antennas required).

Secure verification of location claims[7]

Naveen Sastry, Umesh Shankar, David Wagner

With the growing prevalence of sensor and wireless networks comes a new demand for location-based access control mechanisms. We introduce the concept of secure location verification, and we show how it can be used for location-based access control. Then, we present

[6] 2017 Global Internet of Things Summit (GIoTS)

[7] WiSe '03 Proceedings of the 2nd ACM workshop on Wireless security

the Echo protocol, a simple method for secure location verification. The Echo protocol is extremely lightweight: it does not require time synchronization, cryptography, or very precise clocks. Hence, we believe that it is well suited for use in small, cheap, mobile devices.

FOAM Note: *Appears to be canonical. Need to closely revisit.*

Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey[8]

Liang Chen, Sarang Thombre, Kimmo Järvinen, Elena Simona Lohan, Anette Alén-Savikko, et al.

Internet of Things (IoT) connects sensing devices to the Internet for the purpose of exchanging information. Location information is one of the most crucial pieces of information required to achieve intelligent and context-aware IoT systems. Recently, positioning and localization functions have been realized in a large amount of IoT systems. [...] Security and privacy threats related to positioning in IoT have not been sufficiently addressed so far. In this paper, we survey solutions for improving the robustness, security and privacy of location-based services in IoT systems. First, we provide an in-depth evaluation of the threats and solutions related to both Global Navigation Satellite System (GNSS) and non-GNSS based solutions. Secondly, we describe certain cryptographic solutions for security and privacy of positioning and location-based services in IoT.

- Has Block diagram of GNSS threats to IoT positioning
- NON-GNSS BASED LOCALIZATION TECHNOLOGIES AND THEIR SECURITY THREATS
- SUMMARY OF STANDARD CRYPTOGRAPHY FOR LOCATION INFORMATION
- Distance-bounding and secure localization*

FOAM Note: *good attack vectors here*

Secure positioning of wireless devices with application to sensor networks[9]

S. Capkun, J.-P. Hubaux

[8]IEEE Access (Volume: 5)

[9]Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies.

So far, the problem of positioning in wireless networks has been mainly studied in a non-adversarial setting. In this work, we analyze the resistance of positioning techniques to position and distance spoofing attacks. We propose a mechanism for secure positioning of wireless devices, that we call verifiable multilateration. We then show how this mechanism can be used to secure positioning in sensor networks. We analyze our system through simulations.

FOAM Note: *These papers show an enormous amount of attack vectors, must revisit. Distance estimation v distance bounding?*

Verifiable Multilateration can also be performed with authenticated **distance estimation, instead of distance bounding.**

If the nodes are tightly synchronized, they can measure the signal time of flight to estimate their **mutual distance**. In the packets they send, nodes include timestamps of the times at which they sent the packets. Upon receiving a packet, each node registers the packet reception time, and estimates the distance based on the difference between the sending and the reception time.

Secure localization and location verification in wireless sensor networks: a survey[10]

Yingpei Zeng, Jiannong Cao, Jue Hong, Li Xie

In this paper, we present a survey of current work on both secure localization and location verification. We first describe the attacks against localization and location verification, and then we clas- sify and describe existing solutions. We also implement typical secure localization algorithms of one popular category and study their performance by simulations.

secure localization=sensors themselves need to get their correct locations

location verification=sensor nodes may be compromised and they may intentionally report false locations to the base. Thus, we need to verify the locations learnt from sensors.

So for secure localization, it can be measured by received signal strength indicator (RSSI), time of arrival (ToA), or time difference of arrival (TDoA)

For location verification, most of the solutions are about In-region solutions that try to verify that whether nodes (i.e., provers) are inside given regions. These all use distance bounding protocols

[10]2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems

FOAM Note: *Without synchronization can not get full geometry of network, why exactly though? Only one way* FOAM Note: *Excellent survey, need to revisit.*

Secure Location of Things (SLOT): Mitigating Localization Spoofing Attacks in the Internet of Things[11]

Pengfei Zhang, Sai Ganesh Nagarajan, Ido Nevat

> The rise of geo-spatial location-based applications for the Internet of Things introduces new location spoofing security risks. To overcome the threat of malicious spoofing attacks, we develop the Secure Location of Things (SLOT) framework which extends current state-of-the-art methods and is able to cope with such threats.

FOAM Note: *The algorithms developed here are for Ultra-Wideband (UWB) tech, not sure if they are applicable to LPWAN*

[11] IEEE Internet of Things Journal (Volume: 4 , Issue: 6 , Dec. 2017)

Distance Bounding Protocols

Location verification using secure distance bounding protocols[12]

D. Singelee, B. Preneel

> Authentication in conventional networks (like the Internet) is usually based upon something you know (e.g., a password), something you have (e.g., a smartcard) or something you are (biometrics). In mobile ad-hoc networks, location information can also be used to authenticate devices and users. We focus on how a provers can securely show that (s)he is within a certain distance to a verifier.

Distance Bounding: A Practical Security Solution for Real-Time Location Systems[13]

Adnan Abu-Mahfouz, Gerhard P. Hancke

> The need for implementing adequate security services in industrial applications is increasing. Verifying the physical proximity or location of a device has become an important security service in ad-hoc wireless environments. Distance-bounding is a prominent secure neighbor detection method that cryptographically determines an upper bound for the physical distance between two communicating parties based on the round-trip time of cryptographic challenge-response pairs.
>
> There are however some practical problems which limit the use of such protocols. There are three major attack scenarios: **distance fraud attacks, mafia fraud attacks and terrorist fraud attacks**

FOAM Note: *There is literature on Distance Bounding protocols, need to read more closely.*

[12] IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005
[13] IEEE Transactions on Industrial Informatics (Volume: 9 , Issue: 1 , Feb. 2013)

Wifi Location

SpotFi: Decimeter Level Localization Using WiFi[14]

Manikanta Kotaru, Kiran Joshi, Dinesh Bharadia, Sachin Katti

> This paper presents the design and implementation of SpotFi, an accurate indoor localization system that can be deployed on commodity WiFi infrastructure. SpotFi only uses information that is already exposed by WiFi chips and does not require any hardware or firmware changes, yet achieves the same accuracy as state-of-the-art localization systems.

I Am Alice, I Was in Wonderland: Secure Location Proof Generation and Verification Protocol[15]

Chitra Javali, Girish Revadigar, Kasper B. Rasmussen, Wen Hu, Sanjay Jha

> In this paper, we propose our novel solution for generating location proof for mobile users and verification of the location claim by application services.

[14] CCR August 2015

[15] 2016 IEEE 41st Conference on Local Computer Networks (LCN)

GPS Accuaracy Improvements

PRACTICAL, INEXPENSIVE, NANOSECOND TIME-ACCURACY USING GPS[16]

Scott Miller, Gene DuVall, Azmat Bhatty, James Edmonds

This paper investigates a method for achieving timing accuracy of approximately 3ns using low-cost, low-power components suitable for use in embedded systems. After developing an error model and a prototype costing $440 and consisting of an Oncore M12+ GPS receiver, an uncompensated 33MHz oscillator, and an Altera Cyclone Programmable Logic Device, testing indicated short-term frequency stability on the order of 1.5x10-15 seconds with the full system only consuming 1.7W from a 5V supply. Further testing is required to fully characterize this approach.

Clock Models, Metrics, and Testing[17]

Reid McGaughey

An introduction to clock models, metrics for gauging a clock's performance, and the various test setups for collecting these metrics. [and] the implementation and plant models for clocks, and how PTP interacts with these models. As part of the model discussion, we have discussed the disturbances that affect clocks, especially thermal drift and PDV. Clocks have noise processes other than additive white Gaussian noise, and metrics that provide insight into those noise processes provide further insight into the clock. Finally, we discussed the importance of unit testing and how purpose built timing test equipment can improve the development process.

[16]New Mexico Institute of Mining and Technology
[17]ODVA 2014 Industry Conference

Appendix

The following format may be used for referencing papers:

```
## title^[[published_location](url)]
_authors_

> Excerpt or abstract here.
additional comments as needed.
```

Make instructions for this document

Pandoc is a cross-platform application used for converting documents to other formats. The following will generate the pdf version of this document. Markdown is used for consistency, and ease of assembly.

```
pandoc 'Distributed Hardware Literature Review.md' --pdf-engine=xelatex
-o 'Distributed Hardware Literature Review.pdf'
```

Glossary

Words and their definitions should be included here alphabetically. Definitely include any domain specific words here, generic technical words may be included if this will improve readability of the document. Try to be succint where possible.

Attenuation

the reduction of the amplitude of a signal, electric current, or other oscillation.

Distance bounding

are cryptographic protocols that enable a verifier V to establish an upper bound on the physical distance to a prover P. They are based on timing the delay between sending out challenge bits and receiving back the corresponding response bits.

GPS

The Global Positioning System (GPS), originally Navstar GPS, is a satellite-based radionavigation system owned by the United States government and operated by the United States Air Force.

LoRa

LoRa (Long Range) is a patented digital wireless data communication technology developed by Cycleo of Grenoble, France, and acquired by Semtech in 2012.

LoRaWAN

LoRaWAN is the network on which LoRa operates, and can be used by IoT for remote and unconnected industries. LoRaWAN is a media access control (MAC) layer protocol but mainly is a network layer protocol for managing communication between LPWAN gateways and end-node devices as a routing protocol, maintained by the LoRa Alliance. Version 1.0 of the LoRaWAN specification was released in June 2015.[5] In basic terms, one can consider LoRaWAN to be a new WiFi to connect new IoT devices across every industry.

LPWAN

A low-power wide-area network (LPWAN) or low-power wide-area (LPWA) network or low-power network (LPN) is a type of wireless telecommunication wide area network designed to allow long range communications at a low bit rate among things (connected objects), such as sensors operated on a battery.

Multilateration (MLAT)

is the measurement of the difference in distance to two stations at known locations by broadcast signals at known times.

Wi-Fi

Wi-Fi is technology for radio wireless local area networking of devices based on the IEEE 802.11 standards. Wi-Fi is a trademark of the Wi-Fi Alliance, which restricts the use of the term Wi-Fi Certified

to products that successfully complete interoperability certification testing.