UNIVERSITY OF TARTU
Faculty of Science and Technology
Institute of Computer Science
Computer Science Curriculum

Alice Cooper

Type Inference for Fourth Order Logic Formulae

Master's Thesis (30 ECTS)

Supervisor(s): Axel Rose, MSc
May Flower, PhD

Tartu 2023

Type Inference for Fourth Order Logic Formulae

Abstract:
Many interpreting program languages are dynamically typed, such as Visual Basic or Python. As a result, it is easy to write programs that crash due to mismatches of provided and expected data types. One possible solution to this problem is automatic type derivation during compilation. In this work, we consider study how to detect type errors in the WHITESPACE language by using fourth order logic formulae as annotations. The main result of this thesis is a new triple-exponential type inference algorithm for the fourth order logic formulae. This is a significant advancement as the question whether there exists such an algorithm was an open question. All previous attempts to solve the problem lead lead to logical inconsistencies or required tedious user interaction in terms of interpretative dance. Although the resulting algorithm is slightly inefficient, it can be used to detect obscure programming bugs in the WHITESPACE language. The latter significantly improves productivity. Our practical experiments showed that productivity is comparable to average Java programmer. From a theoretical viewpoint, the result is only a small advancement in rigorous treatment of higher order logic formulae. The results obtained by us do not generalise to formulae with the fifth or higher order.

Keywords:

List of keywords

CERCS:

CERCS code and name: `https://www.etis.ee/Portal/Classifiers/Details/d3717f7b-bec8-4cd9-8ea4-c89cd56ca46e`

Tüübituletus neljandat järku loogikavalemitele

Lühikokkuvõte:

One or two sentences providing a basic introduction to the field, comprehensible to a scientist in any discipline.

Two to three sentences of more detailed background, comprehensible to scientists in related disciplines.

One sentence clearly stating the general problem being addressed by this particular study.

One sentence summarising the main result (with the words “here we show´´ or their equivalent).

Two or three sentences explaining what the main result reveals in direct comparison to what was thought to be the case previously, or how the main result adds to previous knowledge.

One or two sentences to put the results into a more general context.

Two or three sentences to provide a broader perspective, readily comprehensible to a scientist in any discipline, may be included in the first paragraph if the editor considers that the accessibility of the paper is significantly enhanced by their inclusion.

Võtmesõnad:

List of keywords

CERCS:

CERCS kood ja nimetus: `https://www.etis.ee/Portal/Classifiers/Details/d3717f7b-bec8-4cd9-8ea4-c89cd56ca46e`

Fix hiphenization

Contents

1 Introduction

One is where and when one claims to be - this is the underlying principle of the majority of today's location-based services. However, this principle is preceded by a series of implicit premises, one of which is a hinted belief in the honesty of the subject when it comes to accurately reporting their location. Having this trust delegated, the reliance on a trusted third party, frequently an atomic entity, is still subject to tampering, repudiation, inaccuracy, punctual and single failure, or any other kind of Byzantine behaviour. Strategic interactions between rational agents often end up supporting this trust. One party provides a location-based service, and another party makes use of it for its individual benefit, providing an allegedly non-tampered time-conscious piece of location claim. This interaction appears to be one of a non-zero-sum game, that can be observed in most GPS-based services, mapping platforms, navigation systems, mobility and ride-hailing apps, among many others. If driven by the reasoning goal of extracting correct information from the interacting system, users are logically motivated to report an accurate location. The services, having the higher goal of not losing users due to their reported malfunctioning or inaccuracy, are thus motivated to provide maximized quality when operating and consuming the location claims.

This paradigm is now ubiquitous, which may lead to its fallacious use in other very distinct scenarios. The trust levels required to testify to one's location evidences remain unmeasurable in modern arrangements, and those scenarios are, therefore and inversely, the ones that fundamentally require verifiable Proof-of-Location to assert a particular state or derive a conclusion. The concept of location-based authentication or authorization in adversarial environments that rely on information gathered in a trustless setup eventually materializes into services requiring, for instance, a digital certificate as proof that a given user is within a particular geographical area, to enable certain functionalities or assert liability. Some examples are location-based access control, review, or reward systems, social networks, augmented reality games, social or criminal charges. Security against geo-tampering or location spoofing in a relatively trustless environment is needed to achieve the required integrity. In the era of endemic disinformation, with AI generated content made available at unprecedented scales, combating the scourge of false facts may be the duty of every socially and morally concerned individual. Enforcing, providing, and contributing to tamper-proof, integrous and censorship resistant (location) information, in today's chaotically data driven world, may preemptively demand for a collective and decentralized effort.

The basic infrastructural concept of a Proof-of-Location system is somewhat understood, and theoretical or experimental solutions have been delivered throughout the years. These solutions have evolved parallel with their trust assumptions, beginning with a fully trusted setup and progressively shifting towards modern requirements for operational decentralization, of resources, power, and profit. Most recent attempts contemplate the need for a permissionless means of reaching consensus between a quorum of witnesses

that can attest to one's presence at a given point in space and at a given moment in time. These concepts take shape with a combination of tools: wireless technologies as short-range message-exchanging means, cryptographic protocols as confidentiality, integrity, or authentication enablers, and distributed ledgers as publicly trusted record keepers.

The quest for a solution that could make this kind of location-based services as prevalent and ubiquitous shall aim to address a set of design challenges. These challenges are, among others, the solution's flexibility and deployability, preferably by making use of existing infrastructure, and the solution's security and privacy, obeying the modern cryptographic standards and requirements, to guarantee envisioned levels of integrity and resiliency to attacks. This thesis, aiming to address these matters, delivers the following contributions:

1. An overview of the alternative location-based services' paradigm, including the underlying premises and the strategic interactions between rational agents, along with a review of the state of the art in the field. The review is discriminated in terms of trust levels, from fully trusted to permissionless environments, and, consequently, in terms of infrastructure, from centralized to decentralized.

2. The design and implementation of a proof-of-concept that can be deployed in a permissionless manner, using existing technology, ultimately set to attest to one's existence at a given point in space and time. The proof-of-concept is specifically based on the use of routing protocols for multi-hop mobile ad hoc networks to set up a mesh network of witnesses that can assert one's presence in a given geographical area.

The structure of the work is as follows. In Chapter 2, an introduction to the underlying concepts and hypotheses is provided, together with a mention to the technology involved in the practical implementation. Chapter 3 examines similar work discriminated in terms of trust levels. In Chapter **??**, a general overview of the requirements for the proposed solution is given. Chapter **??** details the architecture's design, implementation, and evaluation. Finally, Chapter **??** presents the conclusion and recommendations for future work.

2 Background

This section introduces not only the underlying concepts that sustain the work, but also the technology involved in implementing the proposed practical solution. First, in Section 2.1, we state the Proof-of-Location problem, its participants, and common threat models. Section 2.2 reviews the concept of Wireless Mesh Networks and related routing protocols for establishing nearby witnessing. Lastly, Section 2.3 introduces the permissionless consensus problem and its role in obtaining a location proof in a trustless environment.

2.1 Proof-of-Location

The problem of attesting to one's location is a fundamental act of metaphysical reasoning that happens everywhere, at every moment. Unconsciously and unwittingly, we do claim to be somewhere at an indiscriminated point in time, and we do expect others to believe in us. However, this act is grounded on informal and implicit levels of trust that are not often explicitly asserted, as liability is usually not categorically assigned. When it does happen, trust is usually delegated to a third party or distributed between multiple parties, that may be able to testify to one's presence, synchronously, at the very same location. The act of witnessing is, therefore, a regular yet fundamental part of our interactions with physical reality. When we do claim our presence at an event, assert our location to a service provider, or even state our alibi to authorities, as defense in a criminal charge, a protocol for location attestation is implicitly followed. Some may require a physical interaction of any kind, while others may find digitalized and infrastructural means to gather the required location proof [1].

A digital Proof-of-Location can then be defined as an electronic certificate that assuredly attests one's relative position in both space and time [2]. The relativity of the attestation is, nevertheless, a non-trivial matter. It is, in fact, a complex and multi-faceted process that requires the simultaneous existence of various untrusted or semi-trusted parties, especially in an environment with no individual honesty guarantees. According to Nasrulin et al. [3], a Proof-of-Location protocol may be considered secure if complete, spatiotemporally sound, non-transferable and tamper-evident. Consequently, the system that materially backs the implementation of such a protocol is expected to provide fault-tolerance, reliability, and availability guarantees. More advanced protocols may also explore the possibility of providing privacy and anonymity assurances [4], as well as the possibility of being used in a fully trustless environment [2]. Following is the conceptualization of the common entities of a Proof-of-Location protocol.

2.1.1 Parties Involved

The general act of witnessing alludes to the simultaneous spatiotemporal existence of a set of entities with distinct roles. The majority of the protocols convey a clear contrast between these roles, highlighting the relative dynamism that differentiates those entities.

In comparable terms, highly dynamic entities do not maintain a fixed geographical location for long periods of time. They are often observed in movement, thereby repeatedly starting and finishing communication procedures with neighbouring entities. On the other hand, static entities are expected not to engage in frequent position changes, expressing continuous and fairly invariable communication availability around a fixed point in space as time passes [3]. The act is, however, only completed with another type of entity from whom neither the relative staticity nor the relative dynamism frankly matters. These protocol parties are often external and asynchronous to the witnessing process, but they do effectively take a non-negligible part in incentivizing and giving significance to the witnessing act.

Concisely and in concrete terms, these location-proof arrangements expect the existence of a *prover* that engages in any communication protocol with nearby participants, the *witnesses*, with the goal of gathering a verifiable Proof-of-Location claim, to be later presented to a *verifier*, therefore convincing it of one's existence within a geographical area, at a given moment [5].

Prover. A prover is a dynamic entity, both in movement and availability terms, that is expected to be able to communicate with the witnesses, to gather a proof of its location, and to be later able to provide a location claim to the verifier. Communication with nearby witnesses is thought to happen wirelessly, using any short-range message transmission means. Provers are also expected to be associated with a verifiable but desirably private identity, often as a pseudonym.

Witness. A witness is an entity that is expected to be able to communicate with the prover via the same short-range communication channel and to provide it with a verifiable piece of location attestation. These parties are envisioned to seldomly change their absolute location and maintain a relatively stable neighbouring list of nearby witnesses. These references aim at attaining the figurative creation of coverage zones as strongly connected graphs that form the boundaries of the atomic units of a polygonal mesh. Witnesses are also expected to be fictitiously identified, usually by a pseudonym.

Verifier. A verifier is an external entity that is able to receive a location claim from a prover and verify its validity. Although possible and predicted for trusted setups, in a trustless environment and with the general assurances of a permissionless protocol, verifiers shall not have the need to communicate directly with the witnesses. Verifiers'

identity is also of no measurable importance for the protocol, as the interaction with the prover is usually asynchronous and external to the witnessing process.

Should I introduce formal definitions, like [3]:
Definition 1 (Proof-of-Location). A Proof-of-Location is a verifiable digital certificate that attests the presence of a prover σ at location l and time t and is signed by an authorised witness ω.
And for Completeness, Spatio-Temporally soundness, non-transferability, tamper-evidence...?

2.1.2 Common Threat Models

Like with any technology that involves the collection and processing of sensitive and tamper-prone location data, Proof-of-Location systems must be designed and implemented with a keen awareness of the threat landscape. The threat models of these systems are very often intricately multisided, encompassing a diverse range of actors, motives, and attack vectors. In this context, it is crucial to understand not only the technical mechanisms of Proof-of-Location systems, but also the broader factors that shape their security and privacy risks.

Some common scenarios that may affect the security of Proof-of-Location systems are, for instance, malicious provers that may attempt to forge location claims, or witnesses that may attempt to collude with other entities to falsify the information. Adversary efforts may also be observed in the form of baleful provers, or witnesses, that may try to respectively impersonate other peers. Sybil attacks are also on the horizon of possible threats, often employed to disrupt the operation of the system by flooding it with fake participants [3]. Other works have also considered semi-honest adversaries that, despite following the protocol rules, may try to learn additional information from the messages exchanged [5].

2.2 Wireless Mesh Networks

The envisioned fourth industrial revolution has set the track for modern advancements in achieving a global web of pervasive connectivity between all sorts of machines [6, 7]. New means of radio and wireless communication have been pushing for the technological heterogeneity of protocols, architectures, devices, and consequent performance levels, in order to find their design suitability for different coverage or range scenarios, transmission or bandwidth rates [8]. Additionally, requirements for more complex, adaptable, and resilient topologies have captured broad interest, in both academic and industry domains.

The development of new hardware architectures, protocols, and applications started gaining momentum and branched their way forward to support the popularisation of Wireless Mesh Networks (WMNs). In mesh topologies (see Figure 1), network nodes

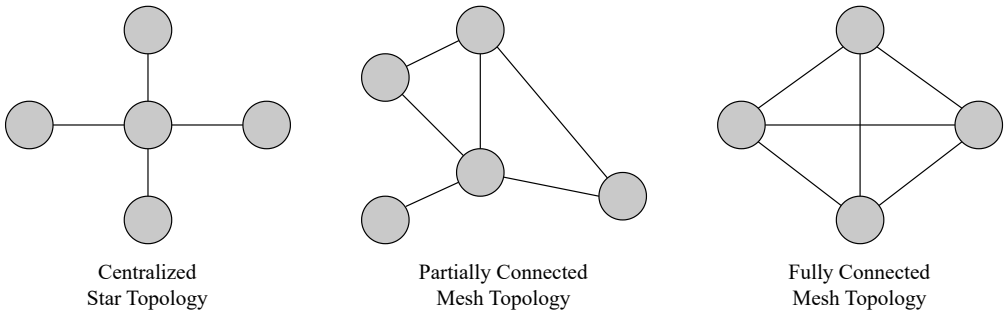

Figure 1. Examples of different topologies of a computer network. Starting on the left, the star topology shows all the nodes connected to a central hub. To the right, examples of mesh topologies depict the direct and decentralized connections between the nodes.

are directly and dynamically connected in a non-hierarchical way. This trait eventually allows for many-to-many communications between the devices to efficiently route data from a generic source to a generic destination. The infrastructure nodes that make up the mesh are expected to dynamically self-organize and configure themselves, resulting in beneficial distributed effects on the overall fault tolerance, ease of deployment, and workload allocation [7, 8]. WMNs follow these principles with the particularity of being made up of radio nodes that communicate via any sort of wireless technology.

Some of the most common wireless technologies that have been, throughout the years, ported to WMNs are Bluetooth, LoRa and IEEE 802.11. The first two are prominent solutions for the extremities of the mesh networking spectrum, with Bluetooth under the short-range realm of Personal Area Networks (PANs), and LoRa under the Low Power, Wide Area (LPWA) scenario. Downsides of these technologies are, respectively, the limiting coverage range for one-hop neighborhoods, or the low bandwidth rates [7]. Hence, IEEE 802.11 became the most flexible and widely used, being the basis for the Wi-Fi standard, which, at the beginning of the last decade, saw an amendment that mainly targeted mesh networks — the IEEE 802.11s WLAN Mesh Standard [9]. The novelty came with the introduction of routing mechanisms operating at the ISO/OSI Layer 2, allowing for compatible information delivery in the layers above. The dynamic establishment of a topology for IEEE 802.11s-based mesh networks relies on the phased transmission of beacon messages that allow for the discovery, synchronization, and maintenance of the links between the peers. IEEE 802.11s has a default routing protocol, the Hybrid Wireless Mesh Protocol (HWMP), which is based on a series of flooding procedures for both proactive and reactive path finding and selection [10]. However, this protocol is not strictly enforced by the standard and has been replaced by other more popular solutions. One notable example is the Better Approach To Mobile Ad-hoc Networks (B.A.T.M.A.N.) routing protocol.

This thesis will explore the concept of WMNs and their potential for serving as the infrastructural topology that enables the relatively short-ranged wireless exchange of messages between the participants of a Proof-of-Location protocol. The following sections will present the B.A.T.M.A.N. routing protocol, OpenWRT and other relevant tools that will be later used to implement the proof-of-concept.

2.2.1 B.A.T.M.A.N. Routing Protocol

The Better Approach To Mobile Ad-hoc Networks (B.A.T.M.A.N.)[1] is a proactive routing protocol for WMNs that operates not at the network layer but at the data link layer, asserting the reliability of radio links using routing metrics and a distance-vector approach [11]. Its newer wireless version, *batman-adv*, has gained traction and popularity and eventually made itself available in the Linux kernel.

Route discovery is preemptively replaced with neighbour discovery, and each infrastructural node is instructed to calculate its potential best next-hop, significantly reducing the overhead of requiring each peer to be aware of the whole network topology. Its version V introduced a throughput metric to evaluate the links' quality and routing choices, replacing the version IV packet loss based metric, deemed unsuitable for larger network sizes [11].

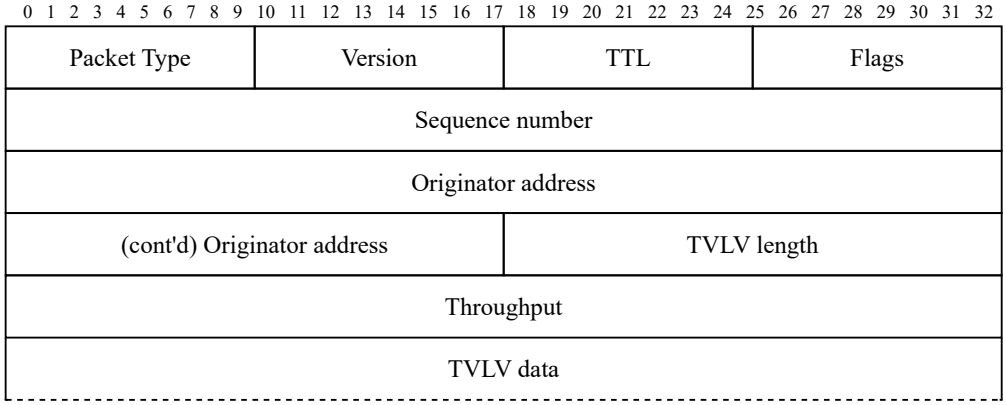

Figure 2. OriGinator Message version 2 (OGMv2) packet format [7, 12]. These messages are broadcasted with a collision avoidance delay mechanism defaulting to 1 second. The packets contain, among other fields, the originator's MAC address and throughput metric values, measured in units of 100 kbit/s.

The discovery of neighbouring nodes is accomplished with the capture of broadcasted OriGinator Messages (OGMv2, see Figure 2), that feature a collision avoidance delay mechanism, the detection of new or duplicate messages, and other fields for throughput

[1] `http://www.open-mesh.org/`

measurement and gateway discovery. The Echo Location Protocol (ELP) handles the received messages and ranks the discovered neighbours. The OGM flooding protocol, on the other hand, enables mesh routing procedures that, simultaneously but independently, allow for estimating the quality of the individual links [7]. Additionally, the protocol facilitates OGM aggregations as an effort to reduce the overhead of sending many short-sized frames. Nevertheless, there is still a quest for optimizations that would allow for more efficient use of multiple interfaces. An implementation of a subset of the Internet Control Message Protocol (ICMP) is also made available, allowing, for instance, the use of the *ping* command to test the connectivity between nodes [11].

Building on the previous, the B.A.T.M.A.N. routing protocol has been, through multiple initiatives, successfully blended into the OpenWRT project, which will also be employed in the proof-of-concept. The following section will present OpenWRT and other relatable tools.

2.2.2 OpenWRT, QEMU, and Raspberry Pis

The OpenWRT project[2] is a Linux distribution for embedded devices, which, in the context of this thesis, will serve as the host operating system for running the proof-of-concept solution. The project is based on the Linux kernel, encapsulating several of its libraries and packages, and is designed to be used on resource-constrained devices. OpenWRT features not only a writable root filesystem and automation build tools with integrated cross-compiler toolchain, but also a package management system that allows for the installation of additional software. The project also provides extensive configuration options for networking capabilities, which includes enabling mesh networking support through the B.A.T.M.A.N. routing protocol.

To facilitate the development and testing of the proof-of-concept, the QEMU[3] emulator will be used. QEMU is a generic and open-source machine virtualizer that, through its versatile set of features, allows for the full-system emulation of a wide range of hardware and software. The emulator will run the OpenWRT-generated images and spawn multiple virtual machines. These machines will simulate the various protocol participants by establishing, with the help of the network emulation tools, a fully connected mesh network. The intention is to ease and accelerate the development process by allowing for testing the proof-of-concept in a controlled environment, without the management, maintenance, and deployment hustle of physical devices. Later, the solution will eventually be deployed on a set of Raspberry Pis[4], the most widely used single-board computers for developing IoT solutions.

Specify later the type of PIs...

[2] https://openwrt.org/
[3] https://www.qemu.org/
[4] https://www.raspberrypi.org/

2.3 Permissionless Consensus

Long has been the time when consensus was still on the verge of being considered such a fundamental problem of distributed systems. Generally defined by Lamport et al. [13, 14], consensus means reaching an agreement between multiple parties in the potential presence of faulty individuals. As per multi-agent systems, interacting over computer networks, consensus is thought to be the result of a coordination effort, that eventually leads the parties to agree on some value at a given moment. However, the evolution of the consensus problem has been invariably limited by a set of strong assumptions. The well-known Byzantine-Fault-Tolerant multiparty consensus systems, that have been designed over the years, are usually meant to work only with a set of known participants, being them faulty or not [15].

The other side of the coin is the permissionless consensus challenge, consisting of achieving agreement in an environment where the parties are unknown and untrusted [16,17]. The relative openness and lack of any kind of central authority are other intrinsic particularities of this type of networks, which inevitably adds complexity to the problem. The participants are not only unknown and untrusted but can also join or leave the network at any time, freely choosing if they care to participate in the consensus protocol. Nevertheless, the problem of permissionless consensus is still seen as a special case of the general consensus definition, but under more meticulous trust assumptions.

Further in this thesis, we will evaluate the different high-level Proof-of-Location protocols and draw a parallel between the evolution of their trust levels and the ultimate need for a low-level permissionless consensus algorithm that allows for establishing decentralized and time-conscious agreement, in an eventual trustless setup, between the multiple witnesses. The next subsections will briefly review some of the most relevant aspects and proof units that give practicality to the roots of the problem.

2.3.1 Proof-of-X

The solution is, nonetheless, unsettled and the scientific community has been reasoning about the need for permissionless consensus when there are already well known and established consensus protocols that work in trusted environments [15, 18]. However, even those protocols have their own limitations, not only in terms of trust, fault-tolerance, centrality, permissions, or bottlenecks, but also in terms of scalability [18], despite assuring deterministic finality [19]. The need for permissionless consensus is then justified by the fact that permissioned protocols are not compatible with the requirements of the new generation of distributed systems, especially in the context of Blockchain networks. These requirements include dealing with today's sparse networks of anonymously and dynamically participating devices, without interrupting consensus and while battling the disruption of the system, typically by subverting it with many pseudo-entities — the so-called Sybil attacks [20, 21]. Fundamentally, the permissionless consensus problem

is the need for a consensus protocol that can be run in a distributed and decentralized environment, where the participants are unknown and untrusted, and where the network is bigger, sparser and unpredictably less reliable.

Technically, permissionless environments allow for larger networks that depict lower connectivity between the participants. Operationally, everything is expected to happen in an asynchronous or partially synchronous fashion, and the number of transactions is predicted to be smaller than in the permissioned counterparts. Participation is free, and the governance is not centralized, but rather distributed and public. The identity of the participants is secured or semi-secured as it often relies on pseudonymity for protecting the nodes' identity, enabling, at the same time, full transparency concerning the rest of the network's content and operation [22]. Expectedly, the goal of permissionless consensus, as for any consensus protocol, is to reach agreement on a single value, or a set of values. However, due to the nature of the protocols, the values that are agreed upon end up establishing the serialization of the transactions, and so establishing time consciousness and total order of the events [20].

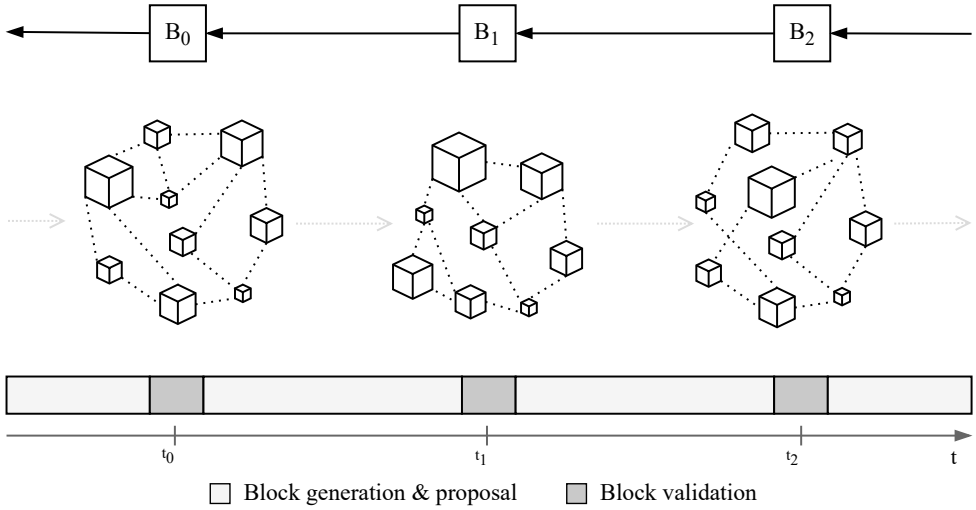

Figure 3. An illustration of the permissionless consensus building phases. From the bottom to the top, the asymmetric arrow of time discretizes the block generation and proposal phase, followed by the block validation, along with frequent network topology changes and the consequent time conscious serialization of the blocks.

Also described by Xiao et al. [21], very concisely, the way to achieve an operating protocol, as seen in the mainstream Blockchain networks, is by first generating the agreeable value, in this particular case, a block and its proof, proposing and disseminating the information to the network, followed by the eventual validation and acceptance of the block by the majority of the nodes. This is the approximate moment of probabilistic

finality, when consensus is ultimately reached (See Figure 3). During the whole process, a fair and somewhat predictable incentive mechanism is also needed, that rewards participants for their honest effort in reaching consensus, and punishes the ones that are not behaving correctly. These incentives are of major importance in this very context of permissionless consensus and all these building phases form the basis of the inner functioning of Bitcoin itself [16], replicated with some variations in other networks [17, 21]. The following is a short introduction to some relevant proof units that feature in the most popular Blockchain systems.

2.3.2 Proof-of-Work and Proof-of-Stake

Without discrediting the previous attempts, the first practical permissionless consensus algorithm was proposed by Nakamoto in [16]. It is a Proof-of-Work consensus protocol that resembles a replicated state machine where the independent participants reach agreement not only about transactional values, but also about their order - naturally forming the underlying structure of what is now known as a Blockchain. The focus shifted for decentralized systems and after Proof-of-Work many other consensus mechanisms have been proposed, relying on different consensus units.

In the classical Nakamoto consensus protocol, the generation of a block, to be proposed for further network agreement, complies with the unit of computational work needed to create, or rather find, a verifiable proof of the effort spent on assembling the block [16]. This essentially requires brute forcing the search for a cryptographic hash value for the aggregation of the block information with a nonce. This value has to satisfy a difficulty threshold (See Procedure 1), which gets adjusted dynamically over time, to maintain the network overall requirement for the block generation interval [20, 21].

Procedure 1: BlockGeneration

Input: Transaction Merkel Tree Root, Hash of the last Block, Timestamp, Other.
Result: new $Block$.

$BlockHeader \leftarrow$ Transaction Merkle Tree Root
    | Hash of the last Block
    | Timestamp
    | Other;

`// the preceding zero bits in` $target$ `depict the mining difficulty`
while $Hash(BlockHeader \mid nonce) \geq target$ **do**
    Increment $nonce$;

`// append transactional data`
return new $Block$;

One can then exercise the reasoning line and extrapolate the previous block generation

mechanism to a *Proof-of-Something* pseudo-random competition in which an entity in possession of a higher amount of a certain resource, either computational power, or stake, or certain currency, or, for instance, a higher amount of storage space, guarantees a higher probability of leading the block generation and proposal, and consequently winning the acceptance by the majority. This is the essence of Proof-of-Stake, as a derivative of the Proof-of-Work mechanism. Here, stake is a traceable and verifiable amount of a certain unit, token or currency, that is owned by a certain entity who wishes to participate in the consensus protocol. The stake works as a form of collateral that is used to guarantee everyone's honesty, in an attempt to reduce the Sybil attack likelihood. And, respectively as in Proof-of-Work with computational power, the higher the stake, the higher the probability of leading the block generation and proposal.

Idealized and inspired by Proof-of-Stake, extending or adapting Proof-of-Work became a popular trend in the Blockchain community. The main idea is to replace the computational power with some other resource, that is more scarce, or more valuable, or more verifiable, or more traceable, to combine multiple resources, or even to add extra requirements to pure Proof-of-Work [21]. Not that every one of the options has a considerable potential for entirely solving the permissionless consensus problem, but each one of them may tackle different use cases where consensus needs to be reached, and where different resources are available to make the agreement happen [23, 24]. Nonetheless, the design of these consensus mechanisms shall aim for a protocolar choice between a set of properties that form a trilemma: Security, Scalability, and Decentralization. Briefly put, relaxing the security requirements may allow for more scalability, both of which, consequently, have hands tied with decentralization. These trade-offs are of practical consideration when defining the network goals and use cases [21]. Further dissection of various classes of Proof-of-Stake based protocols, diverging alternatives to the classic Nakamoto consensus, and comparisons between them can be found in [20, 21, 23–25].

With all the above in mind, we will proceed to review some of the proposed Proof-of-Location solutions, discriminated by trust levels. Aiming at achieving spatiotemporal agreement among the witnesses, we will reason about the applicability of one of these lower-level permissionless consensus protocol, in the context of a fully decentralized and trustless environment.

3 Related Work

This section presents a nuanced description of the current state of the Proof-of-Location problem, spanning the spectrum of its trust levels, from fully trusted to permissionless environments. Furthermore, it encompasses an assessment of the typical infrastructural scenarios, detailing the progressive shift from centralized to decentralized systems. The organization of the section is as follows. Section 3.1 outlines the starting point in a trusted and centralized setting. Section 3.2 details the progressive shift towards distributed and decentralized protocols. Section 3.3 presents the most recent developments in the Proof-of-Location problem, which ultimately target permissionless and fully trustless setups. Finally, alternative strategies to the prevailing Proof-of-Location protocols, which this thesis mainly addresses, are presented in Section 3.4.

3.1 Trusted and Centralized Architectures

The establishment of not just the concept, but also the need for a new kind of systems that, in simple terms, would allow for attesting and prove some device's location, dates back to the early beginnings of this century.

Waters and Felten, in [26], attempt at pioneering the design of a location-proving system by proximity that simultaneously ensures integrity and privacy. The system model assumes a fully trusted setup, fundamentally composed by two entities, a *verifier* and a *device*. The latter is implicitly thought to be managed by an untrusted user, but hypothesised and expected to be tamper-resistant, and thus trusted by the *verifier*. The motivation behind this scenario is oriented towards practical situations in which, for instance, trusted parties lend their equipment to users and want to verify, or monitor, the equipment's location, such that it remains inside some pre-established location boundaries. The authors explicitly mention the lending of computers by universities and the wish that those devices to not leave the campuses. Home arrest monitoring systems have, as well, the need for ensuring that the ankle device, and so the person in charge, does not escape a certain location.

Faced with the design and coverage unadaptability of GPS-based location systems, which do not structurally aim at serving as Proof-of-Location enablers, the authors identify the need for small wireless networks, covering a relatively short-ranged area, via a *location manager*, acting as an access point. This *location manager* is either set up, or distinctively trusted by the *verifier*. Round-trip and signal propagation latency are the metrics used, respectively, for determining the proximity of the *device* to the *location manager* and for protecting against proxy attacks — when a proxy device is placed near the *location manager* and serves as signal repeater for the original *device* that is somewhere else, outside the coverage area. Concretely, the work targets Wireless LAN network operators and their existing access points' infrastructure, to serve as *location managers*. A Public Key Infrastructure (PKI) is also proposed in order to delegate the

atomic responsibility of authenticating and managing their identities to a trusted third party. Finally, the authors set down the seeds for extending their proximity proof system to a secure and moderately accurate positioning proof mechanism, with the possibility of using multiple *location managers* and a triangulation algorithm.

The Proof-of-Location track was inevitably unfogged with this primordial work and location proofs were soon to be fully demystified and categorically defined. Sariou and Alec, in [27], concisely introduce the primitive concepts around Proof-of-Location and some desired properties of an inherently secure system. However, the key contribution of their work was the delineation of a set of example applications that would benefit from Proof-of-Location protocols. These include, but are not limited to, costumer reward systems for physical stores, location-authenticated business review systems, location-restricted web content delivery, voter's physical presence verification, among many others.

Further protocols took inspiration from this groundwork and started shaping the landscape. Graham and Gray, in [28], propose a Proof-of-Location scheme called SLVPGP that removes the need for the *location manager* to be trusted by the central *verifier*, delegating the trust to tamper-resistant modules. VeriPlace, by Luo and Hengartner [1], is a complex and expensive privacy-aware location proof architecture that distributes responsibility among three types of trusted entities, taking the first step at avoiding dedicated tamper-resistant hardware. It specifically targeted the integration with Yelp[5], a public crowd-sourced reviews system for businesses. Another worth mentioning piece of work is from Javali et al. [29], still in a centralized and trusted stand, that adds robustness to the previous protocols by simplifying, in theoretical and practical terms, with trusted and existing Wi-Fi infrastructure, the Proof-of-Location generation process. Finally, the work of Akand et al. [30] is a more recent solidification attempt in the design of centralized but provably secure Proof-of-Location systems that protect against geo-tampering attacks.

The next section will report the emergence of the first relatively distributed Proof-of-Location protocols, taking a step further in the direction of fully decentralized and trustless systems.

3.2 Progressively Distributed and Decentralized Protocols

VeriPlace had already profiled and templated an inherently distributed architecture with built-in privacy awareness, taking a first infrastructural step towards defending against proxy attacks, without the need for trusted hardware [1]. The whole setup is especially tangled and consequently resourceful for the levels of trust it assumes, but it definitely settled the ground for the next generation of Proof-of-Location schemes.

The following evolutionary stage of these protocols aims at flexing and distributing

[5] `https://www.yelp.com`

trust, resources, power, and responsibility, with the hope of achieving more resilient, fault-tolerant, and scalable systems. APPLAUS, by Zhu and Cao [31], delivers one of the first distributed protocols that combines the location proof and location privacy problems. It uses Bluetooth enabled mobile devices that communicate with nearby participants, during the proof generation process. The protocol asserts certain bond levels between the *prover*, *verifier*, and *witnesses*, all of them known to a trusted Certificate Authority (CA), disregarding, on the other hand, the need for a fully trusted location proof server to store the historic location records. The claim is that, by statistically changing the pseudonyms for each device and by following a user-centric privacy model, the protocol can effectively generate privacy preserving location proofs and store them in a trustless manner. STAMP [32] and PROPS [33] are two contemporaneous works that take the same witnessing approach as APPLAUS, but follow the path of convincing the *verifier* by presenting several shares of a composite location proof, based on group signatures. Both of them try to more profoundly tackle the *prover*'s and *witnesses*' privacy concerns, but may admittedly fail at preventing collusion scenarios between them. Gambs et al. argue that the reliance on a trusted third party may be an unavoidable requirement, even if against the authors' principles of location sovereignty, especially when one wants to entirely prevent unbounded collusion attacks [33]. SPARSE, by Nosouhi et al. [34], avoids the typical distance-bounding mechanism and the *witness* picking process by the *prover*, as done in the previous works, with the goal of protecting against those collusion attempts, at best, in relatively crowded and decentralized witnessing situations. At this point, all these schemes have assumed the common goal of protecting the identity of the involved parties, but they have not yet tackled the additional problem of keeping the location information proportionally private from whoever needs to verify it. Dupin et al. [5] theoretically propose a Secure Multi-Party Computation (SMPC) based protocol that is provably resilient against any semi-honest participant. Their solution could still benefit from the classical distance-bounding mechanisms [5], but it is highly resourceful and practically infeasible, as it relies on expensive and complex cryptographic primitives and assumes directional antennas [35].

On the horizon of these solutions was still the high level need for detaching Proof-of-Location protocols from any kind of trusted central authority, for both identity and information management. This goal has naturally met, along the way, Blockchain technology. The next section will finally present the most recent developments in achieving decentralized, trustless, and infrastructure-independent Proof-of-Location schemes.

3.3 Fully Trustless Environments

Inspired by the solution proposed by Zhu and Cao [31], Amoretti et al. [2] dive into the definition of a novel decentralized and infrastructure-independent approach that allies together short-range communication technology and Blockchain-based storage

and information verification. The authors propose the establishment of a distributed overlay network of linked nodes that, at the same time, wirelessly provide or request location proofs from nearby nodes, and verify or store propagated proofs, via any typical lower-level Blockchain protocolar agreement, achieving, thus, permissionless consensus. Their solution is claimed to be one of the very first at protecting against the main location-based-systems' attacks, with the help of a fully decentralized and Blockchain inspired peer-to-peer scheme, which assures both integrity and user privacy. Real-world performance evaluation and the possibility for integrating higher-level incentive mechanisms were set as future work prospects. Both Amoretti et al. [2] and Nasrulin et al. [3] contemporaneous works illustrate practical constructs that take advantage of the tamper and censorship resistent nature of Blockchain technology. The latter tries, as well, to formalize the main security and spacio-temporal requirements that such a decentralized Proof-of-Location protocol shall present, ending up implementing a proof-of-concept, based on a permissioned Blockchain framework, to specifically solve supply chain tracking challenges.

Further efforts that build upon the above-mentioned solutions are the ones proposed by Wu et al. [36] and Nosouhi et al. [37]. The first follows the path of Amoretti et al. [2] and tries to enable, on top of it, user-defined hierarchical privacy protection, with the help of Zero-Knowledge proofs. The proposed protocol finds a bridge between the typical Proof-of-Location set of entities and the usual Zero-Knowledge proof participants. The suggested *zk-PoL* protocol aims so at allowing the *prover* to convince the *verifier* that one was at a specific location, at a certain point in time, but with a granular privacy preserving disclosure of the location proof details. The obvious motivation of the mechanism is to solve spam, traceability, and privacy concerns of publicly storing raw location information, especially within decentralized and public ledgers. Therefore, the scheme is, to a great degree, centred in the privacy assurances and not in the infrastructural aspects of the potential decentralization that it is built upon. Nevertheless, it sets a promising starting point for the introduction of privacy preserving technology in the realms of trustless Proof-of-Location protocols. Optimizations and faster proof mechanisms are kept in the outlook and waiting to be explored. Nosouhi et al. [37] stress out a different proximity checking mechanism, to protect against the still unsolved *prover* and *witnesses* collusions, while committing, as well, to privacy preserving location proof generation and storage, using public and decentralized Blockchain technology. Their work has also an original integration of an incentive mechanism that rewards collaborative participants, in order to more strongly prevent the main known attacks. This sets an unprecedented track for the incorporation of these Proof-of-Location protocols into the digital and decentralized economy that already runs, via Smart Contracts, on Blockchain networks like Ethereum [17, 37].

Minding all the above, Pournaras [38] proposes the complementing concept of Proof-of-Witness-Presence as a key element in an augmented democracy approach to smart city

development. This concept involves validating the accuracy of data collected through participatory crowd-sensing, by requiring physical presence at locations of interest. The author argues that this approach can foster greater citizen engagement and participation in public spaces, and can be incentivized through Blockchain consensus and a crypto-economic design. Acknowledging the limitations of current localization methods such as GPS, it is suggested the need for more advanced and secure location certificates, based on complex social proofs. The Proof-of-Witness-Presence model envisioned by Pournaras may rely on token curated registries and a supplemental fully trustless Proof-of-Location protocol that, for instance, FOAM[6] tries to deliver. The next paragraph will be fully dedicated to this last piece of work.

3.4 Alternative Strategies

[6] https://foam.space/

References

[1] W. Luo and U. Hengartner, "Veriplace: a privacy-aware location proof architecture," in *Proceedings of the 18th SIGSPATIAL International Conference on Advances in Geographic Information Systems*, pp. 23–32, 2010.

[2] M. Amoretti, G. Brambilla, F. Medioli, and F. Zanichelli, "Blockchain-based proof of location," in *2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, pp. 146–153, IEEE, 2018.

[3] B. Nasrulin, M. Muzammal, and Q. Qu, "A robust spatio-temporal verification protocol for blockchain," in *Web Information Systems Engineering–WISE 2018: 19th International Conference, Dubai, United Arab Emirates, November 12-15, 2018, Proceedings, Part I 19*, pp. 52–67, Springer International Publishing, 2018.

[4] W. Li, H. Guo, M. Nejad, and C.-C. Shen, "Privacy-preserving traffic management: A blockchain and zero-knowledge proof inspired approach," *IEEE access*, vol. 8, pp. 181733–181743, 2020.

[5] A. Dupin, J.-M. Robert, and C. Bidan, "Location-proof system based on secure multi-party computations," in *Provable Security: 12th International Conference, ProvSec 2018, Jeju, South Korea, October 25-28, 2018, Proceedings*, pp. 22–39, Springer, 2018.

[6] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer networks*, vol. 47, no. 4, pp. 445–487, 2005.

[7] A. Cilfone, L. Davoli, L. Belli, and G. Ferrari, "Wireless mesh networking: An iot-oriented perspective survey on relevant technologies," *Future Internet*, vol. 11, no. 4, p. 99, 2019.

[8] M. L. Sichitiu, "Wireless mesh networks: opportunities and challenges," in *Proceedings of World Wireless Congress*, vol. 2, p. 21, 2005.

[9] G. R. Hiertz, D. Denteneer, S. Max, R. Taori, J. Cardona, L. Berlemann, and B. Walke, "Ieee 802.11 s: the wlan mesh standard," *IEEE Wireless Communications*, vol. 17, no. 1, pp. 104–111, 2010.

[10] S. Bari, F. Anwar, and M. Masud, "Performance study of hybrid wireless mesh protocol (hwmp) for ieee 802.11 s wlan mesh networks," in *2012 international conference on computer and communication engineering (ICCCE)*, pp. 712–716, IEEE, 2012.

[11] D. Seither, A. König, and M. Hollick, "Routing performance of wireless mesh networks: A practical evaluation of batman advanced," in *2011 IEEE 36th Conference on Local Computer Networks*, pp. 897–904, IEEE, 2011.

[12] "Open-mesh. originator message version 2 (ogmv2)." `https://www.open-mesh.org/projects/batman-adv/wiki/OGMv2`. Accessed: 2023-02-16.

[13] M. Pease, R. Shostak, and L. Lamport, "Reaching agreement in the presence of faults," *Journal of the ACM (JACM)*, vol. 27, no. 2, pp. 228–234, 1980.

[14] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," in *Concurrency: the works of leslie lamport*, pp. 203–226, Springer, 2019.

[15] M. Castro, B. Liskov, *et al.*, "Practical byzantine fault tolerance," in *OsDI*, pp. 173–186, 1999.

[16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[17] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[18] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The honey badger of bft protocols," in *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*, pp. 31–42, 2016.

[19] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong consistency," in *Proceedings of the 17th International Conference on Distributed Computing and Networking*, pp. 1–10, 2016.

[20] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2019.

[21] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A survey of distributed consensus protocols for blockchain networks," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 2, pp. 1432–1465, 2020.

[22] Y. Xiao, N. Zhang, J. Li, W. Lou, and Y. T. Hou, "Distributed consensus protocols and algorithms," *Blockchain for Distributed Systems Security*, vol. 25, p. 40, 2019.

[23] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Expert Systems with Applications*, vol. 168, p. 114384, 2021.

[24] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021.

[25] C. Natoli, J. Yu, V. Gramoli, and P. Esteves-Verissimo, "Deconstructing blockchains: A comprehensive survey on consensus, membership and structure," *arXiv preprint arXiv:1908.08316*, 2019.

[26] B. Waters and E. Felten, "Secure, private proofs of location," *Department of Computer Science, Princeton University, Tech. Rep. TR-667-03*, 2003.

[27] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in *Proceedings of the 10th workshop on Mobile Computing Systems and Applications*, pp. 1–6, 2009.

[28] M. Graham and D. Gray, "Protecting privacy and securing the gathering of location proofs-the secure location verification proof gathering protocol.," in *MobiSec*, pp. 160–171, Springer, 2009.

[29] C. Javali, G. Revadigar, K. B. Rasmussen, W. Hu, and S. Jha, "I am alice, i was in wonderland: secure location proof generation and verification protocol," in *2016 IEEE 41st conference on local computer networks (LCN)*, pp. 477–485, IEEE, 2016.

[30] M. R. Akand, R. Safavi-Naini, M. Kneppers, M. Giraud, and P. Lafourcade, "Privacy-preserving proof-of-location with security against geo-tampering," *IEEE Transactions on Dependable and Secure Computing*, 2021.

[31] Z. Zhu and G. Cao, "Applaus: A privacy-preserving location proof updating system for location-based services," in *2011 Proceedings IEEE INFOCOM*, pp. 1889–1897, IEEE, 2011.

[32] X. Wang, A. Pande, J. Zhu, and P. Mohapatra, "Stamp: Enabling privacy-preserving location proofs for mobile users," *IEEE/ACM transactions on networking*, vol. 24, no. 6, pp. 3276–3289, 2016.

[33] S. Gambs, M.-O. Killijian, M. Roy, and M. Traoré, "Props: A privacy-preserving location proof system," in *2014 IEEE 33rd International Symposium on Reliable Distributed Systems*, pp. 1–10, IEEE, 2014.

[34] M. R. Nosouhi, S. Yu, M. Grobler, Y. Xiang, and Z. Zhu, "Sparse: privacy-aware and collusion resistant location proof generation and verification," in *2018 IEEE Global Communications Conference (GLOBECOM)*, pp. 1–6, IEEE, 2018.

[35] Z. Yang, C. Jin, J. Ning, Z. Li, A. Dinh, and J. Zhou, "Group time-based one-time passwords and its application to efficient privacy-preserving proof of location," in *Annual Computer Security Applications Conference*, pp. 497–512, 2021.

[36] W. Wu, E. Liu, X. Gong, and R. Wang, "Blockchain based zero-knowledge proof of location in iot," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–7, IEEE, 2020.

[37] M. R. Nosouhi, S. Yu, W. Zhou, M. Grobler, and H. Keshtiar, "Blockchain for secure location verification," *Journal of Parallel and Distributed Computing*, vol. 136, pp. 40–51, 2020.

[38] E. Pournaras, "Proof of witness presence: Blockchain consensus for augmented democracy in smart cities," *Journal of Parallel and Distributed Computing*, vol. 145, pp. 160–175, 2020.

Appendix

I. Glossary

II. Licence

Non-exclusive licence to reproduce thesis and make thesis public

I, **Alice Cooper**,
*(*author's name)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to

   reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

   Type Inference for Fourth Order Logic Formulae,
   *(*title of thesis)

   supervised by Axel Rose and May Flower.
   *(*supervisor's name)

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Alice Cooper
dd/mm/yyyy