Assessing Mobile Device Location Behavior to Enable Building Mobile Ad Hoc Networks of Trusted Nodes

A Dissertation
Presented in Partial Fulfillment of the Requirements for the
Degree of Doctor of Philosophy
with a Major in Computer Science
in the College of Graduate Studies
University of Idaho
by

Karen Hammer Thurston

Major Professor: Daniel Conte de Leon, Ph.D.
Committee Members:
Lori Baker-Eveleth, Ph.D.
Frederick Sheldon, Ph.D.
John Shovic, Ph.D.
Department Administrator: Terence Soule, Ph.D.

December 2021

Authorization to Submit Dissertation

This dissertation of Karen Hammer Thurston, submitted for the degree of Doctor of Philosophy with a Major in Computer Science and titled "Assessing Mobile Device Location Behavior to Enable Building Mobile Ad Hoc Networks of Trusted Nodes," has been reviewed in final form. Permission, as indicated by the signatures and dates below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor: _____Date: _____
Daniel Conte de Leon, Ph.D.

Committee Members: _____Date: _____
Lori Baker-Eveleth, Ph.D.

_____ Date: _____
Frederick Sheldon, Ph.D.

_____ Date: _____
John Shovic, Ph.D.

Department Administrator: _____ Date: _____
Terence Soule, Ph.D.

Abstract

***Context*—**Mobile computing and communication devices are ubiquitous and can form mobile ad hoc networks (MANets). This may be particularly useful when device density may provide communications when Cellular, WAN, or LAN infrastructure is unavailable.

***Problem*—** Trust is subjective in the sense that the trustor determines the evaluation criteria on which to judge a potential trustee. Assessing the trust of MANet nodes is an ongoing research problem. Previous mobile ad-hoc network (MANet) trust research focuses on the behavior of nodes already operating in a MANet or on recommendations of other nodes. Previous trust research does not consider node location behavior as a potential avenue for measuring trust before allowing a node to join the MANet.

***Solution*—**This dissertation provides an objective metric for calculating node trust based on the capability, commitment, and consistency of node geographic behavior. In this dissertation, I describe an approach to measure node behavior defined as repeated and lasting physical presence in geographic locations to calculate a trust value. The approach measures node presence at geographic locations for at least a minimum duration repeatedly over time as defined by a MANet operator. This approach provides a way for MANet operators to qualify node behavior prior to deploying the node in a MANet, and to monitor node behavior to ensure conformance to MANet manager's expectations for that behavior.

***Contributions*—**

1: Created a novel method for building trust based on location behavior of mobile nodes (MACH-T).

2: Designed, implemented, and tested an algorithm and corresponding software implementation for MACH-T.

3: Designed and performed six experiments for evaluating MACH-T and evaluated MACH-T's performance under difference scenarios using real location data in the first five experiments and synthetic data in the sixth.

***Results*—**I found that MACH-T can build a useful and reliable trust measure, and corresponding confidence measure, based on mobile node location data. MANet operators could use MACH-T to measure trust of mobile nodes based on location behaviors.

Acknowledgements

The formulation of this research proposal has been possible because of the support from many sources, and I wholeheartedly acknowledge my indebtedness to all of them.

I express my deepest sense of gratitude and appreciation to my major professor Daniel Conte de Leon, Ph.D. for his encouragement, guidance and support in undertaking and proceeding with this research. I extend my heartfelt gratitude towards the members of my dissertation committee, Lori Baker-Eveleth, Ph.D., Frederick Sheldon, Ph.D., and John Shovic, Ph.D. for their valuable advice during the research, for reviewing this dissertation and for providing insightful feedback.

I wish also to acknowledge my former manager, Center Executive Officer and Vice-President at the University of Idaho, Charles Buck, Ph.D. for supporting my enrollment in the graduate program while I was an administrator at the University of Idaho. My sincere thanks go to Susan Branting and Arleen Furedy, also at the University of Idaho, Computer Science Department, for providing administrative support during my graduate studies. Many thanks to a former colleague and University of Idaho professor, Robert Rinker, Ph.D., and Nancy Ripplinger, M.S., also a former colleague and North Idaho College professor who hired me for my first faculty position at North Idaho College which gave me additional confidence and experience teaching which I plan to continue after earning my Ph.D.

I gratefully acknowledge the support from the University of Idaho staff employee benefits and the Senior Scholar program which both partially funded my graduate studies. I also gratefully acknowledge the support for my studies from my former employer, North Idaho College in Coeur d'Alene, Idaho, and my current employer, Long Beach City College in Long Beach, California.

From my days as a graduate student at California State University, Sacramento, working on an M.S. degree in Computer Science which I completed in 1992, I also gratefully acknowledge the late Richard H. Thayer, Ph.D., who encouraged me to enroll in a Ph.D. program. His encouragement planted a seed.

Finally, I am grateful to Microsoft Research and researchers from the University of Rome Tor Vergata for their public research datasets which provided real data for my research.

Dedication

To my late parents John and Margaret Hammer

To my husband John Thurston, my greatest support

To my children William, Shelby, Ian and son-in-law Pasquale

To my grandchildren Reid, Sloane, Siena, Pasquale Luca, and Baby Mastantuono

In God I Have Put My Trust

Psalms 56:4

Table of Contents

List of Figures

List of Tables

Chapter 1:
Introduction

1.0 Context

Ensuring adequate emergency communications during widespread emergencies or during system outages is an unsolved challenge. Whether a natural disaster causes system outages, or cyber-attacks or other actions or events restrict access to Cellular or other telecommunications infrastructure, the possibility of device-to-device communication may be a viable alternative.

The ability of communities to disseminate important messages in the event of widespread outages in the telecommunications infrastructure depends on the preparation and availability of reliable backup methods. Amateur radio operators are a typical source of backup communications in many communities, but they have limited resources and reach.

These are just a few of the motivating reasons for investigating ways to ensure only trusted nodes join device-to-device mobile ad hoc networks that could serve as backups to existing communication infrastructure.

Building and maintaining dedicated and resilient emergency response and public service networks is expensive, and although network sharing is a common approach to reduce costs and increase resiliency, it is often constrained by limited resources. Ubiquitous and high-density mobile communication devices such as smart phones can provide alternative communication infrastructure by forming mobile ad hoc networks (MANets).

In 2012, Li, et al. [1] listed various uses for MANets including

> *…both civilian and military applications, ranging from emergency disaster rescue personnel coordinating efforts after a hurricane, earthquake or brush fire to soldiers exchanging information for situational awareness on the battlefield as well as personal and home area networking, real-time traffic alert propagation via vehicular networks, and Cyber Physical System (CPS).*

In 2014 Deville, et al. [2] studied how mobile phone data could provide insights into population density to inform which locations are candidates for mobile ad hoc network services.

1.1 Problem

Establishing trust in mobile devices and their services prior to using the devices as network nodes is an unsolved problem but has been the subject of study from the time mobile devices first began to proliferate, in the early part of the twenty first century. Trust is the basis for security and privacy of communications. Like trust in human relationships, attributes comprising device trust are complex and not easily measured. As it relates to security, trust can be considered a prerequisite or a result of security as in "trustworthy". Semantics can be argued either way.

Guo, Chen, and Tsai [3] presented a survey and classification of trust computation models in 2017. They also pointed out several gaps in trust research. One subtopic area, within the topic of trust, for which a marked lack of published research results appears to exist, is when there are several distinct trust metrics contributing to one overall trust value. Their survey pointed to other researchers [4], [5], [6], [7] focused on social and distributed (peer-to-peer) types of trust in prior years between 2012 and 2016.

Govindan and Mohapatra [8] in 2011 contended that node trust computations are simpler in static networks because node behavior is predictable after enough observations, but mobile node trust computations are hard when the location is constantly changing.

Gligor and Wing [9], also in 2011 argued for a "general theory of trust" based on "human expectations and mental models of trust without relying on false metaphors and analogies with the physical world." They also claimed that trustworthiness should factor in computational correctness and a behavior trust primitive.

The problem of measuring trust in mobile ad hoc networks (MANets) has not been systematically addressed using an approach that mirrors how humans measure trust. Section 2.1 Related Work provides a chronology and analysis of previous trust research in MANets.

1.2 Solution

The solution in this dissertation proposes to consider adherence to expected behaviors in physical presence as a necessity for establishing trust prior to joining a node to a MANet. Similarly to the way adherence to expected financial behaviors are used to calculate credit scores, expected proximate physical presence is a key component in successful MANet

formation and operation. **This dissertation demonstrates that mobile node behaviors are predictable because even mobile nodes carried by humans or mounted in taxicabs, for example, exhibit average behaviors such as spending predictable time periods in a predictable number of specific locations. This dissertation also demonstrates that such predictability may be successfully used to calculate device trust. Nodes earn trust ratings by abiding to an expected location behavior: nodes with high capability, consistency, and commitment earn higher trust ratings than nodes with low capability, consistency, and commitment.**

The ability to calculate a trust value for a mobile node based on its historical geographic movement patterns will determine its value to a MANet when its past behavior is relied on as an indicator of future behavior. Once mobile nodes can be relied on to be in a particular place at a particular day and time, a trust overlay network operator can oversee the formation of such a network at such times and for purposes as they may be needed.

To use an analogy, in the consumer loan process, a lender checks the credit score of someone applying for a loan before trusting that the applicant will pay back the loan. Human expectations in this case involve expected financial behaviors usually measured today by a credit score. The higher the credit risk, the lower the credit score, and the higher the interest rate. If the credit score is lower than a threshold, the loan application may be declined altogether. My own father, a "plenty tough Army Sergeant" Gilliam [10] during World War II was fond of saying to me and my siblings as children, "In God we trust, all others pay cash!" MANet operators should also have some sense of the behavior of a node prior to allowing it to join a MANet or their expectations of the node's presence will not be met.

The solution presented in this dissertation builds on work from Guo, Chen, and Tsai [3] who evaluated trust computation models in 2017 as compositions of *trust composition, trust propagation, trust aggregation, trust update,* and *trust formation.* This solution falls closer to their classifications as *trust formation* and *trust update*. Furthermore, the solution presented in this dissertation was built to support the concepts of "capability", "commitment", and "consistency" as described by Hacker [11] in 2014. Hacker described that "high trust" is the result of a person or organization considering another person or organization to be capable, committed, and consistent in their behavior [11]. Although this solution does not use human

or device recommenders to contribute to trust ratings, the empirical data considers the same factors discussed by Hacker [11]. This is because the mobile nodes have human operators, and the nodes reflect the behaviors of those humans even though humans are not directly involved in the trust determination.

Table 1.1 shows a mapping that I developed between the trust classification design dimensions from Guo, Chen, and Tsai's [3] to the human behavior dimension by Hacker [11]. This mapping shows full coverage between the computing and human behavior domains and is one of the pillars for the solution described in this dissertation which assigns measurable attributes to each trust dimension.

Table 1.1 Trust Classification Model Component Mapping to Human Behavior Trust Components

Trust Classification Design Dimension in the Computing Domain [3]	**Trust Dimension in the Human Behavior Domain [11]**
Quality of Service	Capable: Presence of GPS trace data collected frequently over time, capable of communicating with GPS satellites or other devices providing geolocation data
Centralized	Consistent: Centralizing allows for comparison to others and to self to determine consistency in behavior
Static weighted sum	Consistent: Repeated conformance to expected set of population average geographic location behaviors or to an ideal set of geographic location behaviors
Event + time-driven	Committed: Visits to the same geographic locations over time shows commitment
Multi-trust	Capable: Many dimensions contribute to overall trust

In MANets, the five characteristics of trust defined by Cho, et al. [12] in 2010 are that it is dynamic, subjective, not necessarily transitive, asymmetric (need not be reciprocal), and context dependent. These characteristics define a relationship between cooperating nodes in a MANet. The approach described in this dissertation exhibits three of the five trust properties as defined by Cho et al. [12] and shown in **Table 1.2**.

Table 1.2 Trust Property Mapping to MACH-T Approach

Cho [12] Trust Property	**MACH-T Approach**
Dynamic	MANet operator updates trust calculations periodically, as desired
Subjective	MANet operator chooses trust evaluation parameters
Not necessarily transitive	Nodes in a MANet need not trust a node trusted by a node it trusts. MACH-T defines trust from the MANet operator perspective.
Asymmetric (need not be reciprocal)	Nodes in MANet need not trust a node trusting it. MACH-T defines trust from the MANet operator perspective.
Context dependent	MACH-T node trust is calculated on its geographic context (location behaviors)

1.3 Contributions

Three major contributions are described in this dissertation:

Contribution 1: Created a novel method for measuring mobile device trust based on location behavior.

Contribution 2: Designed, implemented, and tested an algorithm and corresponding software implementation for measuring mobile device trust.

Contribution 3: Designed and performed six experiments for evaluating the MACH-T approach and algorithm for the case of personal and taxi-mounted mobile device GPS traces.

Six experiments described in this dissertation tested two hypotheses:

- Hypothesis 1: Location behaviors in personal mobile devices can be quantified, measured, and used to assign trust values.
- Hypothesis 2: Location behaviors in vehicle-mounted mobile devices can be quantified, measured, and used to assign trust values.

These experiments are not an effort to determine if the unexpected or outlier behavior is malicious, only that it is unexpected and therefore not trustworthy, based on a given, and adjustable, definition of expected behavior.

The MACH-T algorithm described in this dissertation provides an approach and method for calculating trust for personal and vehicle-mounted mobile device nodes plus a

confidence value on the resulting adjusted trust value. MACH-T translates the trust attributes of capability, commitment, and consistency into the following measurable data:

- Capability: Data availability, longevity, and density.
- Commitment: Repeated visits within a small perimeter for a minimum duration.
- Consistency: Repeated visits to a small number of locations.

1.6 Author's Related Publications

Included as Chapter 3:

K.H. Thurston, D. Conte de Leon. "MACH-T: A Behavior-based Mobile Node Trust Evaluation Algorithm for Building Ad hoc Mobile Networks." Submitted to 2022 Hawaii International Conference on System Sciences

Included as Chapter 7 (copyright notice in **Figure 11-1**):

K.H. Thurston, D. Conte de Leon. "MACH-2K Architecture: Building Mobile Device Trust and Utility for Emergency Response Networks." Proceedings of the 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW), Monterey, CA, USA, November, 2019, IEEE, DOI: 10.1109/MASSW.2019.00004

Included as Chapter 8 (copyright notice in **Figure 11-2**):

K. Thurston and D. C. de Leon, "The healthcare IoT Ecosystem: Advantages of Fog Computing Near the Edge," in 2018 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). IEEE, 2018, pp. 51–56.

1.7 Institutional Review Board Determination

The University of Idaho's Institutional Review Board determined this research is not human subjects research (Project 20-206, reference number 11508, determination letter dated January 25, 2021) because the datasets used were anonymized, gathered in the past (nothing more current than 2014), and were publicly available. Where the term "subjects" is used in this dissertation it should be assumed to mean "subject devices" or "mobile devices".

1.8 Organization of this Dissertation

The rest of this dissertation is organized as follows. Chapter 2 presents Background and Related Work. Chapter 3 describes the MACH-T trust algorithm and the first Geolife dataset experiment. Chapter 4 describes a second and third MACH-T experiment using different trust parameters with the same Geolife dataset. Chapter 5 describes a fourth and fifth MACH-T experiment using the Roma Taxi dataset and ideal behaviors rather than observed population average behaviors. Chapter 6 describes a trust modeling approach using the MACH-T algorithm. Chapter 7 describes MACH-2K, a MANet architecture. Chapter 8 provides a survey of edge computing in healthcare settings. Chapter 9 discusses final results and future work. Chapter 10 contains a full list of cited references. An Appendix includes copyright notices.

Chapter 2:
Background and Related Work

2.0 Chapter Introduction

The subject of trust has been addressed in many disciplines including sociology, economics, philosophy, psychology, organizational management, and autonomic computing in industrial and system engineering [12].

In a survey of various trust management schemes for MANets, Cho, et al. [12] found that "*no work clearly addresses what should be measured to evaluate network trust*". The survey cited 125 research papers. For individual node trust metrics, Cho, et al. [12] proposed future research to include measuring both social reputation and quality of service.

In a book titled Security Metrics: Replacing Fear, Uncertainty and Doubt, published in 2007, Jacquith [21] quotes a former boss who said, "Trust is good, control is better". To control system variables such as which nodes are allowed to join the MANet, trust must be measurable. As former US president Ronald Reagan once quoted Vladimir Ilyich Lenin, "Trust, but verify." In other words, observe or measure whether trust is warranted.

2.1 Related Work

How to determine trust in individual nodes in a mobile ad-hoc network (MANet) is an open research problem. Comprehensive searches of research databases found no research that uses historical location behavior as an indicator of MANet node trust. The related work cited below focuses either on the viability of mobile ad hoc networks or on trust as a measure of a node's behavior as it operates in a network.

Through the years, beginning in 2001, interesting studies focusing on network node trust have contributed to this research topic, and the following paragraphs provide a chronological overview of research showing the problem of trust in computing is an ongoing problem.

Computing hardware can be manufactured to be trustworthy as prescribed by the Trusted Platform Module (TPM), a standard of the Trusted Computing Group, first released in 2001. The latest version (2.0) of this standard was released in 2015 as ISO/IEC 11889:2015. It has been adopted by a large number of manufacturers of various hardware components,

including mobile devices. Segall [14] describes the modules as small inexpensive chips with limited security functions that are the Root of Trust for a device, most useful for remotely identifying or authenticating a machine, protecting secrets or data through hardware protection, and verifying a machine's state or attestation.

Various architectures for MANets have proposed a layer to oversee the management of the MANet. The term "Trust Overlay Network" as defined by Zhou, et al. [15] in 2006 originally proposed metrics for determining reputation of nodes in an established MANet.

Cho, et al. [12] cited 125 different research papers in their 2010 survey on trust management for mobile ad hoc networks. Their work included a discussion of trust terminology including trust management which encompasses trust establishment, trust update, and trust revocation; reputation management; and recommendation. Cho reported that "in the literature, the terms trust and trustworthiness "seem to be used interchangeably without clear distinction." Cho cites research from Josang et al. [16] and Gambetta [17] which defines a "level of trust" as the "belief probability varying from 0 (complete distrust) to 1 (complete trust)…that the trustees will behave as expected." Additionally, research by Solhaug [19] defines "trustworthiness as the objective probability that the trustee performs a particular action on which the interests of the trustor depend."

Cho, et al. [12] assumed ad hoc networks without centralized infrastructure must rely on local trust evidence in node to node interactions.

Among the various MANet trust management research cited by Cho, et al. [12] is research from Kamvar et al. [18] who proposed a reputation based trust calculation in peer-to-peer networks where they assign "each peer a unique global trust value, based on the peer's history of uploads." The purpose was to "decrease the number of downloads of inauthentic files in a peer-to-peer file-sharing network." This particular research was the only one found to use a metric related to the specific context of the application to measure trust. One of the five trust characteristics defined by Cho, et al. [12] is that it is context dependent.

Also cited by Cho, et al. [12] is research from Solhaug et al. [19] who defined trust management as "a special case of risk management with a particular emphasis on

authentication of entities under uncertainty and decision making in cooperation with unknown entities.

Also cited by Cho, et al. [12] is research from Li et al. [20] and Li et al. [21] who combined reputation-based frameworks using direct observation of nodes in a network and opinions of intermediate nodes to determine the trust between nodes without prior interactions.

Cho, et al. [12] also cites Yunfang [22] who proposed two ways to evaluate trust: policy-based and reputation-based. Where policy-based relied on signed credentials based on "strong and objective security schemes such as logical rules and verifiable properties for access control" reputation-based trust used numerical and computational mechanisms to evaluate trust which would then be disseminated among entities.

Cho, et al. [12] also cite Li and Singhal [23], who classified trust management into evidence-based and monitoring-based. Evidence-based would rely on challenge/response processes such as those used with public key, and monitoring-based would be based on observations of node behavior in the network such as packet dropping, packet flooding, or reputation reports from other nodes.

Cho, et al. [12] also cite Aivaloglou et al. [24] who classified trust frameworks as either certificate-based or behavior-based. The certificate-based trust framework would rely on pre-deployment knowledge of trust, either by the certificate-authority itself, or by another node.

Finally, Cho, et al. [12] do not explore how to validate trust models even though they assert *"In general, validation of trust models is difficult, given the inherent subjectivity in the trust metric, but it is also critical."*

Saied, Olivereau, Zeghlache, and Laurent [25] assumed nodes were trustworthy prior to joining a network and they proposed a "bootstrapping" period in their 2013 research to test the trustworthiness of nodes based on artificially induced node interactions, including requests for assistance between nodes.

In a book published in 2013 titled Modeling Trust Context in Networks, Sibel Adali [26] discusses the issue of identity by stating that identity and authentication are important for security. In citing Nissenbaum's 2004 research [27] he notes that identities on networks result

in “disembodiment” and that identity not being “tied to … physical presence” is a barrier to establishing trust.

A NIST publication at the end of 2015 described a proof-of-concept implementation of the Trusted Platform Module configured to know the current location of the hardware to enforce geolocation restrictions for purposes of restricting computing devices outside of national borders, for example, but not to track the geographic locations of a moving hardware device over time [28].

With the new 5G cellular technology rollouts, Lu, et al. in 2018 [29] studied ways to offload cellular network traffic to device-to-device networks using femtocell technology to augment the macro cellular infrastructure in a Heterogeneous Cellular Network (HCN). In Lu, et al., trust only depends on authorization, key authentication, prior social interactions, or device-to-device performance in an already formed network, not on historical device location behaviors or other measurable attributes.

Behavioral scientists Eagle and Pentland [30] have shown predictability in human behaviors they term “eigenbehaviors” which can predict with a high degree of certainty where someone will be in the future, based on past behavior [30]. This dissertation demonstrates an approach, although not based on the same eigenbehavior method, to predict the location of mobile devices carried by human operators based on past behavior, and to use calculated values to assign trust to a device to be deployed as a node in a MANet.

A recent patent application by Agarwal [31] proposes using geolocation and timing for issuing a one-time password for authentication purposes but does not address the issue of network node trust over time.

While trust has been the topic of many investigations, the approach in this dissertation is unique and most closely draws on the eigenbehavior concept [30] of predictable human behavior which in this dissertation is extended to mobile devices. While Eagle and Pentland were focused on predictability in human behavior, and created a measure for human behavior, their work did not explore the relationship between predictability and trust. Their work does mention human interactions and relationships as one aspect of human behavior but did not explore trust in those interactions or relationships. The MACH-T solution focuses on

calculating a value for trust which can be used for a specific purpose: building a MANet of trusted nodes, that is, trusted in the sense of location persistence.

The MACH-2K architecture described in Chapter 7 of this Dissertation describes an overlay network architecture that would be centrally managed. Nodes would either be in the network because they are trusted based on their geographic behavior, or they would not be in the network because their trust value was below a threshold. Nodes would not have access to trust values of other nodes but would trust any node in the network because the MANet operator (the trust authority) deemed them trustworthy.

Chapter 3:

MACH-T: Behavior-based Trust of Personal Mobile Devices

3.0 Chapter Introduction

This chapter proposes an approach for assessing trust of personal mobile device nodes based on their location behaviors prior to joining and while joined to a MANet.

This chapter provides the following contributions supporting Hypothesis 1:

Contribution 1: Create a novel method for measuring trust based on location behavior.

Contribution 2: Design, implement, and test an algorithm (MACH-T) and corresponding software implementation for measuring trust.

This chapter also provides the personal mobile device experiment description and results:

Contribution 3: Design and perform two experiments for evaluating the MACH-T approach and algorithm for the case of personal and taxi-mounted mobile device GPS traces.

Hypothesis 1: Location behaviors in personal mobile devices can be quantified, measured, and used to assign trust. **The results of this experiment indicate the hypothesis is true.**

I designed, developed, and implemented a process and toolset for calculating the MACH-T trust value based on raw GPS trace data. This process is described in **Figure 3-1** (data stores are represented with boxes, and processes in italic typeface).

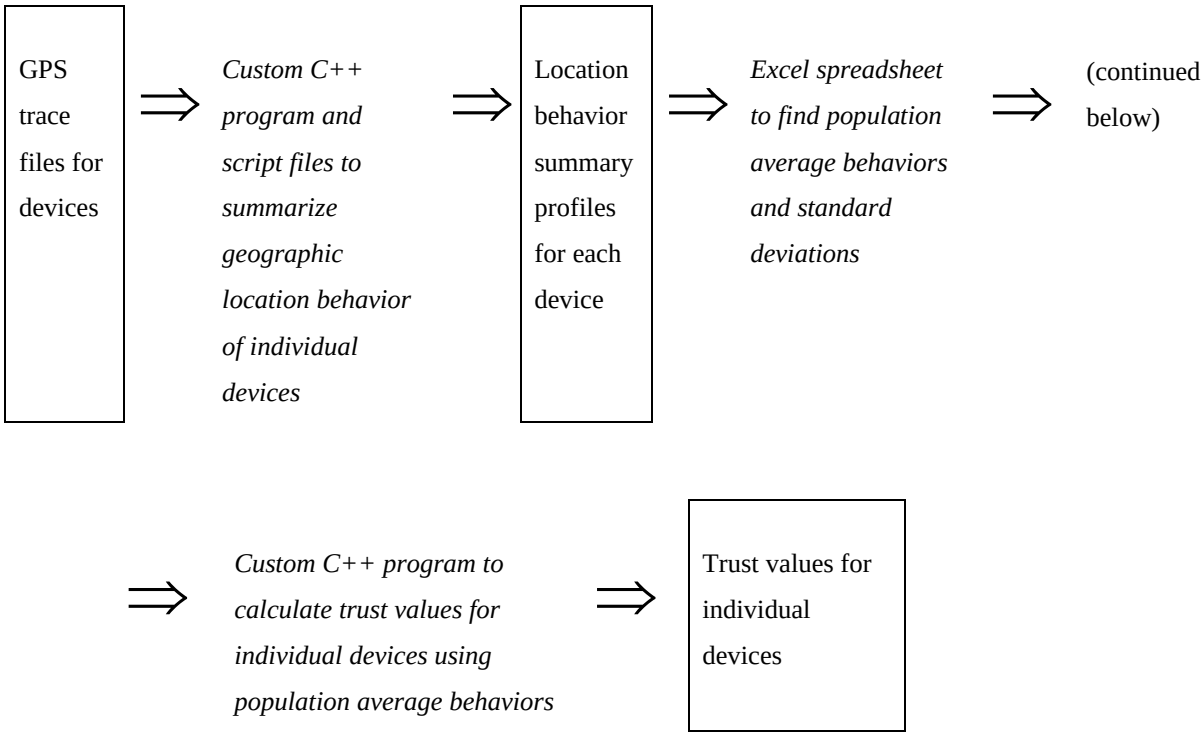


Figure 3-1 Geolife Data Analysis Workflow

A compressed version of this chapter has been submitted to the 2022 Hawaii International Conference on System Sciences and is currently under review.

3.0.1 Abstract

MACH-T is a novel behavior-based algorithm for mobile ad hoc network node trust building. MACH-T uses historical mobile node geographic location traces to incrementally calculate node trust values based on the concepts of geographical node capability, commitment, and consistency. Motivation for this work is to increase resiliency in community and public service networks. Resiliency may be economically enhanced by building new ad hoc networks of private mobile devices and joining these to public service networks at specific trusted points. Resiliency in such ad hoc networks relies on security which is in turn built on trust. By first establishing trust, message confidentiality, privacy, and integrity may be implemented by well-known cryptographic means. In this article, we describe the MACH-T

algorithm for automatically evaluating the trust of ad hoc network nodes. We also describe our experiments and results from evaluating MACH-T using real GPS traces from the Microsoft Research Geolife project. Our results show that MACH-T can successfully build a reliable trust value and corresponding confidence value based on learnt patterns of time spent in certain qualifying geographic locations.

Keywords: algorithms, trust, trust building, emergency response networks, network resiliency, spatio-temporal data mining, location history, Internet of Things, mobile ad hoc network (MANet).

3.1 Introduction

Mobile devices have become ubiquitous. Wireless capabilities for device-to-device communication are varied and currently available in most mobile devices. Applications such as FireChat and BluetoothChat have seen widespread use in areas where cellular service has been interrupted or is non-existent [32]. These applications assume a binary trust determination based on human mobile device users or owners knowing each other a priori.

Such trust determinations are well-suited for network applications that involve human intervention such as chat applications or human-to-human messaging applications. However, requiring a priori trust determination is not possible in many interesting applications. For example, (1) unknown or ad hoc IoT device message forwarding, (2) messaging to, from, within, or across ad hoc networks with thousands or more devices or nodes, (3) emergency response message forwarding and delivery, (4) community service message forwarding and delivery.

This paper investigates using geographical behavior patterns of mobile devices to build trust for mobile nodes in ad hoc networks based solely on device geographical behavior, when device owner authorization is given. We used real mobile device GPS traces form the Microsoft Geolife dataset [33], [34], [35], [36], to analyze and discover predictable geographical behaviors. These behaviors were used as the basis for constructing a generic trust evaluation algorithm, MACH-T. MACH-T was then evaluated against the Geolife dataset showing very promising results.

We envision a future system where builders and managers of ad hoc networks would be able to:

1. Select certain geographic areas of interest for building a MANet (Mobile Ad hoc Network),
2. Automatically assign trustworthiness for subscribing ad hoc mobile nodes within those geographic areas (MACH-T),
3. Create trust groups and select desired trustworthiness and trust confidence thresholds for joining different trust groups or network action or message types, and
4. Initiate messages with destinations to, or forwarded by, nodes on the MANet, depending on the message type and trusted MANet groups, which may have different trust level requirements.

This article describes our approach, algorithm, experiments, and results toward enabling point 2 above by using a node's geolocation behavior patterns as provided, with device owner's permission, to a central device trust determination authority. Using MACH-T, a system could be built to enable operators to request trust determination information from a mobile node trust determination authority. Only the resulting trust value, but not the source traces, would be shared with MANet operators ensuring the privacy of device users or owners. In a previous article, we described the overall architecture of a system that would enable such MANets called MACH-2K [32]. In this article, we describe the MACH-T algorithm for trust determination that would enable such resilient MANets to be built.

The rest of this chapter is organized as follows: Section 3.2 describes related work, Section 3.3 describes the Geolife dataset, Section 3.4 describes our methods, Section 3.5 describes our results, and Section 3.6 presents our conclusions.

3.2 Related Work

Other researchers have investigated trust for mobile ad hoc networks. However, we found no academic reports describing an approach in which trust is built based on actual historical geographical behavior plus context-sensitive requirements established by network managers such as requirements for presence in a geographic location.

Guo, Chen, and Tsai [3] presented a survey and classification of trust computation models. They also pointed out several gaps in trust research [3]. One subtopic area, within the topic of trust, for which a marked lack of published research results appears to exist, is when there are several distinct trust metrics contributing to one overall trust value. Guo, Chen, and Tsai found only four papers in this area: [37], [38], [39], [40]. However, [37], [38], [39], [40] focused on social and distributed (peer-to-peer) types of trust building. By contrast, the algorithm and results we describe in this article contribute new knowledge in the subtopic area of multi-attribute trust formation. Our research also has the potential for leading into developing Trust as a Service (TaaS), another approach needing further research as suggested by Guo, Chen, and Tsai [3].

Within the Guo, Chen, and Tsai [3] trust model classification, one model, which they call "*Class 5: QoS + social / distributed / static weighted sum / event + time-driven / multi-trust*" would fit the closest to the MACH-T model presented in this article. Our model differs from Guo et. al. Class 5, in that it does not have a social attribute component since these attributes tend to assume direct involvement by humans as an essential portion of the trust computation. In addition, our trust formation model is intended to be automatic and centralized rather than manual and distributed.

Also, Guo, Chen, and Tsai's [3] evaluated trust computation models as one of: *trust composition, trust propagation, trust aggregation, trust update,* and *trust formation.* Our approach falls closer to their classifications as trust formation and trust update. Furthermore, MACH-T is built to support the concepts of "capability", "commitment", and "consistency" as described by Hacker [11]. Hacker writes that high trust results from one person or device considering another person, organization, or device to be capable, committed, and consistent in their behavior [11]. Although our approach does not use human or device recommenders to directly contribute to trust ratings, the empirical data we analyzed considers the same factors discussed by Hacker [11]. This is because the mobile nodes we analyzed have human operators and we assume devices reflect the behaviors of those humans even though, in our case given the desired functionality, we need humans not to be directly involved in the trust determination. **Table 3.1** shows a mapping of the trust classification design dimensions from Guo, Chen, and

Tsai's [3] to the human behavior dimension by Hacker[11] where we show full coverage between the computing and human behavior domains.

Saied, Olivereau, Zeghlache, and Laurent [25] assumed nodes were trustworthy prior to joining a network and they propose a "bootstrapping" period to test the trustworthiness of nodes based on artificially induced node interactions, including requests for assistance between nodes [25]. In contrast, our work proposes using actual historical geographic behavior to incrementally build mobile device (node) trust.

Table 3.1 Trust Computation Model Component Mapping to Human Behavior Trust Components

Trust Classification Design Dimension in the Computing Domain	**Trust Dimension in Human Behavior Domain**
Quality of Service	Capable (presence of GPS trace data collected over time, capable of communicating with GPS satellites)
Centralized	Consistent (centralizing allows for comparison to others and to self)
Static weighted sum	Consistent (trust increases with conformance to expected set of behaviors)
Event + time-driven	Committed (visits to same locations over time shows commitment)
Multi-trust	Capable (many dimensions contribute to overall trust)

3.3 Dataset

This section describes the dataset we used for our analysis and initial experiments.

The Geolife dataset from Microsoft Research [33] collected GPS traces from 182 subjects mostly between April 2007 and August 2012. The average subject's data spanned 6.2 months (standard deviation of 1 year, 2.4 months). Microsoft's statistics for the dataset are 17,621 trajectories with a total distance of more than 1.29 million kilometers and 50,176 hours. The sampling rates vary from 1 to 5 seconds and between 5-10 meters per point. The data was mostly gathered in and around Beijing, China, with some traces in the United States and Europe. The Geolife dataset also included transportation modes for some of the subjects (walk, bike, bus, car and taxi, train, airplane, and other) but we did not use this data attribute in our analysis.

Table 3.2 provides the data format of the detail records in the GPS trace files. The first six records in each file were header records which we did not use. We used Field 5: *Number of days since fixed date* for calculations involving the date as a number instead of using Field

6: *Date* and Field 7: *Time*. We discarded Field 3 (always 0) and Field 4: *Altitude* since they were not relevant to our research. **Figure 3-2** shows two sample GPS trace detail records.

Table 3.2 Geolife GPS Trace File Detail Record Data Format (as Shown in the Geolife User Guide)

Field 1	Latitude in decimal degrees.
Field 2	Longitude in decimal degrees.
Field 3	All set to 0 for this dataset.
Field 4	Altitude in feet (-777 if not valid).
Field 5	Date - number of days (with fractional part) that have passed since 12/30/1899
Field 6	Date as a string
Field 7	Time as a string

39.906631, 116.385564, 0, 492, 40097.5864583333, 2009-10-11, 14:04:30

39.906554, 116.385625, 0, 492, 40097.5865162037, 2009-10-11, 14:04:35

Figure 3-2 Example Geolife GPS Trace Data Records

3.4 Methods

In summary, the process for analyzing the dataset is shown below.

- Process GPS trace files for all days for each subject device (node)
- Accumulate qualifying locations and write detail records for each qualifying location to file for each subject device (node)
- Qualifying locations determined by subjective definition of trust: How long a subject device is required to stay in a location for the location to qualify, how many total days and hours for which there are trace records and how many of the days and hours qualify for the minimum stay in a location
- Locations determined by desired zoom level using the OpenStreetMaps.org tile system
- Write one summary record with summary data and trust values: MACH-T(U), Confidence, and MACH-T(A)

3.4.1 Input file processing of stationary activity

The first step in our evaluation methodology was to analyze the GPS traces of the Geolife dataset from Microsoft Research [33] to determine average behavior which we then considered as the basis for desired behavior. Assuming and anticipating that most subjects

would spend at least one hour in only a handful of unique locations over time, such as home, work, school, places of worship, shopping, and recreation, we compiled the total hours and number of times a subject visited the same location for at least one hour. The GPS traces we analyzed recorded the movement of mobile devices.

We used these trace data focusing on the times when devices were stationary or at least within a square area approximately 469 meters on each side for at least one hour. We assumed that most mobile devices carried by human owners or operators will not be mobile for more than a fraction of a 24-hour period. Even in more congested areas with long commutes compared to other regions such as the Los Angeles basin in California, USA, where average commute times are 31 minutes each way, or about 1 hour per day, commute time accounts for only 4.2% of one 24-hour day [41]. Even with an extra round trip per day for an additional hour for purposes other than work, only 8.2% of the day may be spent traveling at most. Considering the purpose for our trust calculations is to form mobile ad hoc networks, devices that are confined to a limited geography while connected to the network would likely be more useful to the network.

Because the dataset we used was not recent, we did not restrict analysis to any given date range within all dates in the data which ranged from April 2007 to the end of July 2012.

3.4.2 Data Processing

We conducted our detailed analysis by writing and executing a C++ program to read each of the trace files for each subject to record one or more locations for each subject for any continuous time in the location of at least one hour in duration. For any two trace records where the time interval between any two GPS trace records was longer than 10 minutes we did not add that time to the accumulated time in one location, assuming the GPS tracking application was either disabled or lost contact with the GPS satellite. We did add intervals longer than 10 minutes to the total of all trace intervals for a subject as an indicator of the total time span during a day from the first trace to the last. Assuming a MANet may rely on devices being able to respond to messages within a short time, we chose 10 minutes, but this value could be smaller or larger depending on the needs of the MANet operator. The 10-minute requirement also increased the confidence value of the calculated trust value.

The C++ program converted latitude and longitude input values in the GPS trace files to x,y tile coordinates using the OpenStreetMaps.org [42] conversion algorithm pseudocode shown in **Figure 3-3** which uses a spherical pseudo-Mercator projection providing non-overlapping relatively square locations approximately 469 meters on each side at the latitude of Beijing, China.

```
numTiles = 2 ^ 16//zoom level 16
xTile = numTiles * ((Lon + 180) / 360)
    lat_rad = deg2rad(Lat)
    yTile = (numTiles * (1 - (log(tan(lat_rad) + 1/cos(lat_rad)) / Pl)) / 2)
```

Figure 3-3 Conversion Formula from GPS Coordinates to Tile Coordinates

Initially, we did not convert the GPS coordinates to x,y tile coordinates but instead used a circular shape with a radius of 500 meters to group the locations. We realized using the center of a circle of a specified radius would result in overlapping circles for some locations which was less desirable than non-overlapping relatively square tile locations. The tiles become smaller at more northern latitudes due to the curvature of Earth, but the spherical pseudo-Mercator projection does not adjust for this factor. Because most of our data points were near Beijing, China or at a similar latitude, we used the tile size of 469 meters on each side as a constant size. The Open Street Maps documentation does not provide standard measurements for on the ground distances between tiles at various zoom levels. To estimate this distance, we used the GeoFabrick Tile Calculator web resource [43] and a Windows application called GPSprune [44]. Future versions of our C++ program could adjust for latitudes to calculate the appropriate tile size.

Figure 3-4 shows the web page from the GeoFabrick Tile Calculator [43] for tile (53945,24810,16). The value 16 is the zoom level. The northeast corner of the tile (indicated by the solid black arrow in the image) is the point represented by the longitude and latitude coordinate pair (116.32874, 40.00238), shown in the lower right corner of the image. To get a close approximation of the length of a side of a tile at zoom level 16 we found the longitude and latitude coordinates (116.32323, 40.00238), for the northwest corner of the neighboring tile to the West (53944, 24810, 16) and used the online distance calculator from the US Federal Communications Commission website [45] to calculate the distance between the two points, which is shown in **Figure 3-5**.

To verify the consistency of the scale of the OpenStreetMap tiles we used the GPSprune Windows application program [44] which allowed us to display the same location as the web page map but also had a scale displayed on the map and a built-in distance calculator. The estimated distances between the same two pairs of GPS coordinates resulting from using GPSprune [44] and the FCC Online distance calculator [45] in were consistent at 469 meters as shown in **Figure 3-6**.

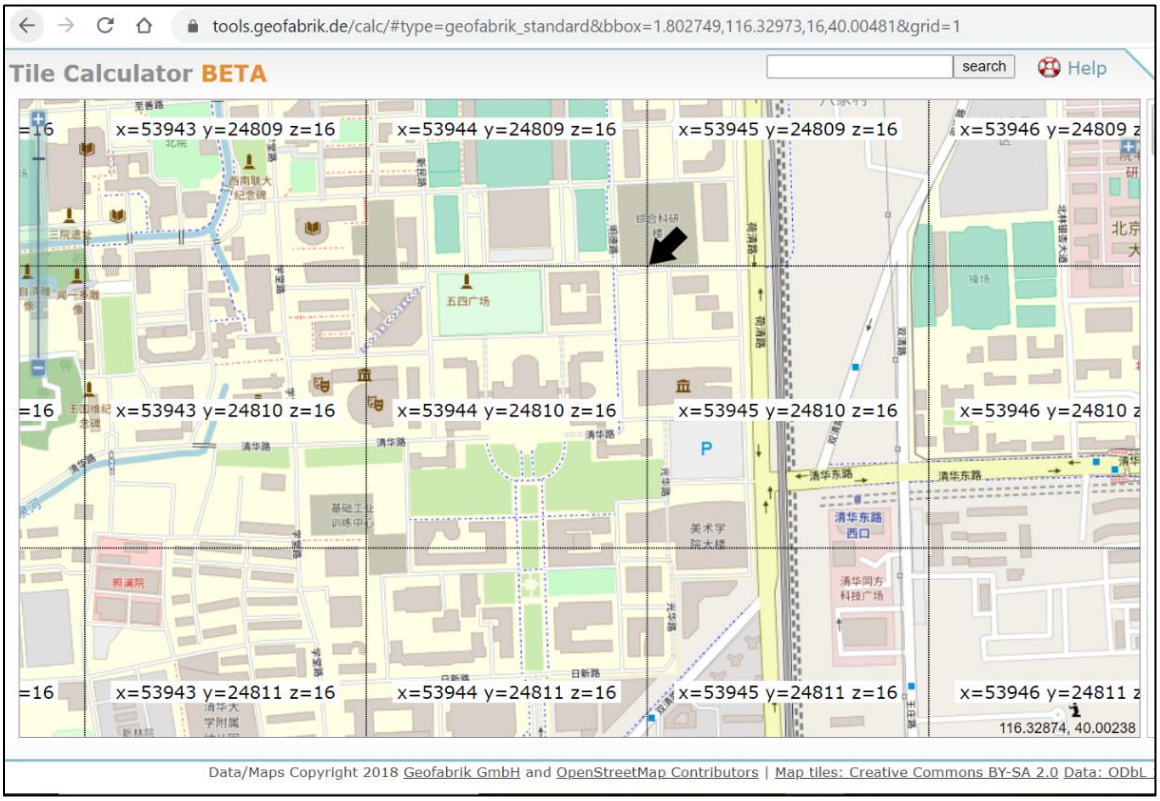


Figure 3-4 Webpage [43] Showing Tiles (53945, 24810, 16) and (53944, 24810, 16)

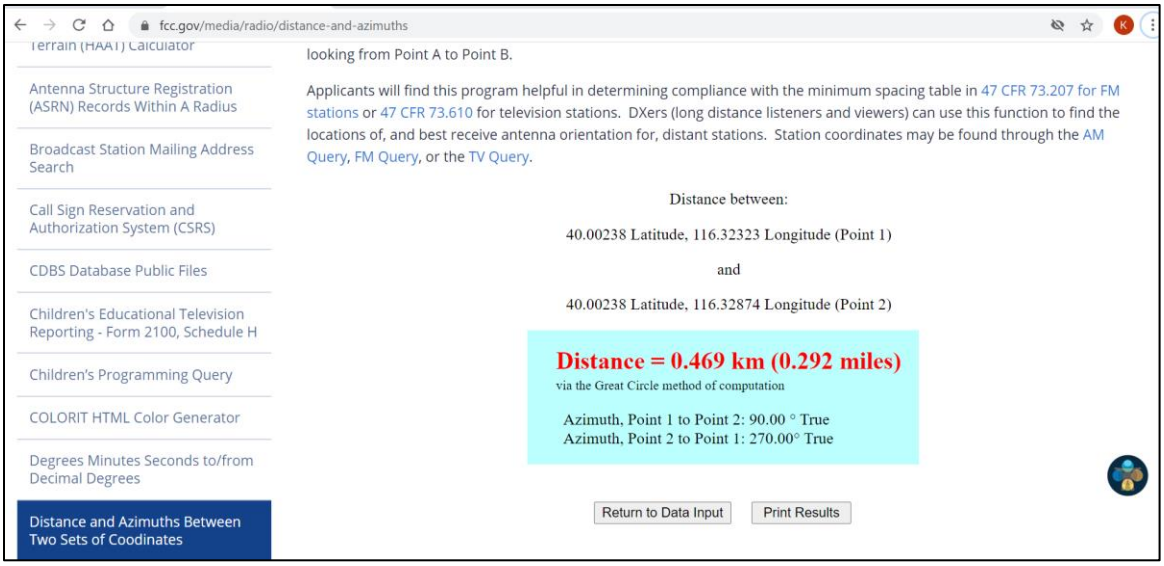


Figure 3-5 U.S. FCC Online Distance Calculator [45]

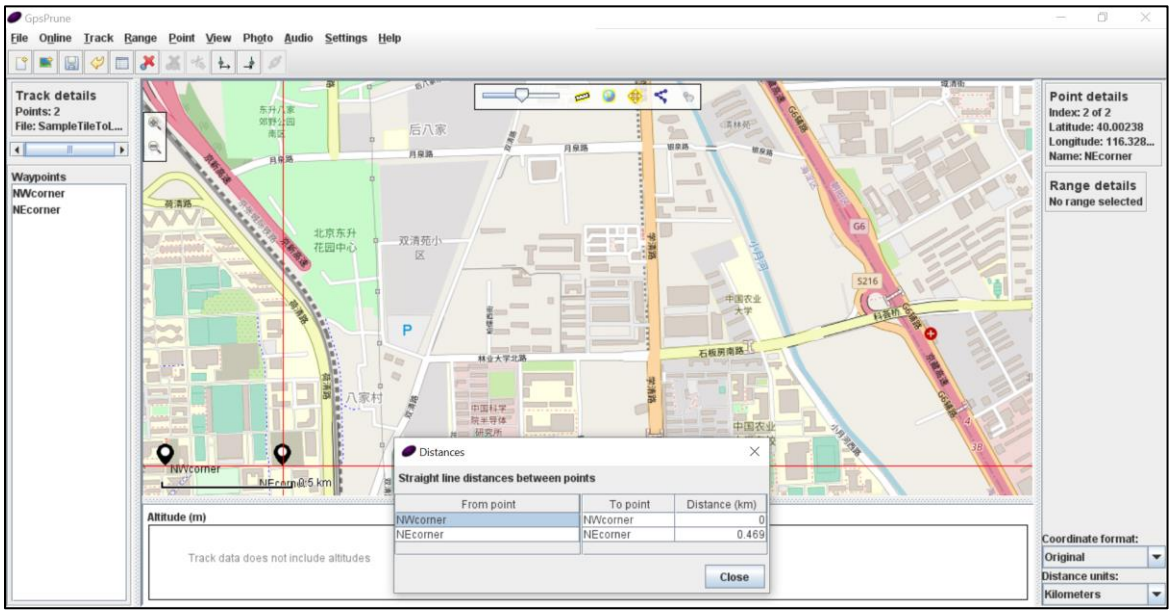


Figure 3-6 GPSprune [44] Map Showing Distance Between Two Test Points (one side of a tile)

After choosing the zoom level of 16, resulting in square tiles with a side of about 469 meters, we decided to require at least one continuous hour in the same location to mark that location as a trust qualifying location. Multiple occurrences over any number of days of at least one hour in each location were accumulated for total time in each location. Repeatable time in each qualifying location, as defined by a tile, was used as a key factor in determining the attributes of capability, commitment, and consistency for establishing trust.

3.4.3 Output File Record Formats

Table 3.3 shows the data format for detail records we calculated for each subject. We initially tracked the hour of the day and the day of the week when nodes were at a location but decided to discard that information to simplify the results. In addition to the detail records, we also created a header record to store the run-time parameters of zoom level (16), required time in location (3600 seconds), and program name (mach2ktile.exe). We compared summary data for each subject to establish averages and standard deviations from the average.

Table 3.3 Qualifying location record detail for each subject

Location Attribute	Description
xTile	X tile coordinate (Open Street Maps zoom level 16) for qualifying location (≥ 1 hour)
yTile	Y tile coordinate (Open Street Maps zoom level 16) for qualifying location (≥ 1 hour)
Hour	Beginning hour of the day (not used currently)
DOW	Day of the week (not used currently)
Freq	Number of times ≥ 1 hour in location
Hours Duration	Total number of hours in location
Trace Count	Number of trace records for location (for determining confidence in the MACH-T value)
First Date	First/oldest date in location
Last Date	Last/most recent date in location

Table 3.4 shows the summary data calculated for each subject stored in a header record of the subject's qualifying locations file containing the detailed location data shown in **Table 3.3**. We used the summary header data to calculate the population averages and standard deviations for the coefficient values in the MACH-T trust algorithm formulas described in **Figure 3-7** and **Figure 3-8**. Summary data values used to calculate the coefficients are preceded by **(C)** and data values preceded by **(T)** contribute to the MACH-T calculation. Values preceded by **(F)** are used in the Confidence Formula.

Table 3.4 List of Summary Behavioral Attributes for Each Mobile Node Used in MACH-T

Attribute	Description
First-Last Date	**(F)** First to last date for all GPS trace records (date range)
Total Days (TD)	**(C) (F)** Total days in all GPS trace records
Total Hours (TH)	**(C) (F)** Total hours in all GPS trace records
Total Locations (TL)	**(C)** Total locations in GPS trace records (not unique locations, count incremented each time a location changed) (one location is one tile given by the x,y coordinate at the northwest corner)
Qualified Locations (QL)	**(C)** Qualifying locations ($\geq$ one hour) for all GPS trace records
Tot qualified hours (QH)	**(C)** Total qualified hours (sum of hours in all qualified locations)
Total qualified days (QD)	**(C)** Total number of days with qualifying locations
QH / TH %	Percentage qualifying hours to total hours
Min xTile	Minimum X tile coordinate (at zoom level 16)
Min yTile	Minimum Y tile coordinate (at zoom level 16)
Max xTile	Maximum X tile coordinate (at zoom level 16)
Max yTile	Maximum Y tile coordinate (at zoom level 16)
#1 loc%	Percentage of qualifying hours in most visited location
#2 loc%	Percentage of qualifying hours in second most visited location
#3 loc%	Percentage of qualifying hours in third most visited location
#4 loc%	Percentage of qualifying hours in fourth most visited location
#5 loc%	Percentage of qualifying hours in fifth most visited location
#6 loc%	Percentage of qualifying hours in sixth most visited location
Subject	Subject number (000-181)
QH / QD	**(T)** Ratio of qualified hours to total qualified days (“Capability”)
QL / QD	**(T)** Ratio of qualified locations to total qualified days (“Capability”)
QD / TD	**(T)** Ratio of qualified days to total days (“Commitment”)
QL km^2	Area in km^2 of qualified locations (QL*.469*.469 km^2)
QL perimeter km^2	Area in km^2 using per of all qualified locations ((Max xTile - Min xTile +1)*.469)* ((Max yTile - Min yTile +1)*.469)
QL km^2 / QL perim. km^2	**(T)** Ratio of qualified locations area to perimeter area (“Consistency”)
QL / TL	**(T)** Ratio of qualified locations to total locations (“Consistency”)
QH / TH	**(T)** Ratio of qualified hours to total hours (“Commitment”)
MACH-T_U Trust Value	Calculated trust value before applying confidence adjustment
MACH-T_A Trust Value	Calculated trust value after applying confidence adjustment
Total Trace Records	**(F)** Total number of GPS trace records for all trace files for a subject
Max Interval	Longest number of seconds between two trace records (if longer than 10 minutes, interval was not counted for qualifying purposes)
Max Interval HHMMSS	End time of longest trace record interval
Min Interval	Shortest number of seconds between two trace records (records with the same time stamp were discarded)
Cumm Trace Secs	Cumulative interval in seconds between trace records
Traces/Day	Average number of traces per day for a subject
Avg Interval	Average trace interval (Cumulative Trace Secs/Trace Count)
Tot Qual Trace Count	Total trace record count for all qualifying locations

3.4.4 Trust Formulas

The formula in **Figure 3-7** has six weighting factors, equally weighted at 16.66% in our experiment, to calculate one trust rating for each subject. A MANet operator might adjust these weights for each factor depending on the needs of a planned ad hoc network. The general formula indicates a vector of weights, W_1 to W_6.

As a prequalification for applying the formula, the subject had to pass three tests, or we assigned zero as the trust value. See **Table 3.4** for descriptions of the terms QH, QD, QL, TD, QL km^2, QL perimeter km^2, TL, and TH.

QD $\geq$ 1 (at least one qualified day—days with at least one qualified location, "Capability" metric)

QL >1 (at least two qualified locations—locations with at least one visit $\geq$ one hour, "Consistency" metric)

QL perimeter km^2 < 1000km^2 (area encompassing all qualified locations must be less than or equal to 1000 km^2, "Consistency" metric).

The **MACH-T$_U$** unadjusted trust formation formula, shown in **Figure 3-7**, has three additional terms where values in the denominator could potentially be zero: TD (total days), TL (total locations), and TH (total hours). We do not check for zero values in these terms before applying the formula because the QD and QL values would be zero and result in a trust value of zero without applying the formula.

$$\textbf{MACH-T}_U = [W_1 * \frac{\frac{QH}{QD}}{\left(\frac{\overline{QH}}{\overline{QD}}\right)+1\sigma}] + [.W_2 * \frac{\frac{QL}{QD}}{\left(\frac{\overline{QL}}{\overline{QD}}\right)+1\sigma}] + [W_3 * \frac{\frac{QD}{TD}}{\left(\frac{\overline{QD}}{\overline{TD}}\right)+1\sigma}] +$$

$$[W_4 * \frac{\frac{QL\ km^2}{QL\ perimter\ km^2}}{\left(\frac{\overline{QL\ km^2}}{QL\ permimeter\ \ km^2}\right)+1\sigma}] + [W_5 * \frac{\frac{QL}{TL}}{\left(\frac{\overline{QL}}{\overline{TL}}\right)+1\sigma}] + [W_6 * \frac{\frac{QH}{TH}}{\left(\frac{\overline{QH}}{\overline{TH}}\right)+1\sigma}]$$

Figure 3-7 MACH-TU Trust Algorithm Formula

Additionally, we adjusted the final trust (**MACH-T$_A$**) to account for the confidence level from the trace data using the formula in **Figure 3-8**. The higher the density and volume of data, the higher the confidence value, with a maximum value of 1.0. Density evaluation uses

the first two factors: Density of trace records per hour and the hours per day. Volume evaluation uses the third factor: the number of days of data as a percentage of the desired number of days of data, with a maximum value of 1.0. When simplified the formula is shown in **Figure 3-9**.

$$\textbf{MACH-T}_{\textbf{A}} = \textbf{MACH-T}_{\textbf{U}} * \frac{\frac{\text{Total Trace Records}}{\text{TH}}}{\text{Desired Trace Records per hour}} * \frac{\text{TH}}{24 * \text{Days in Date Range}} * \frac{\text{TD}}{\text{Desired Number of Days}}$$

Figure 3-8 Formula for Confidence-Adjusted Trust Algorithm Value MACH-T(A)
(Confidence determined by the volume and density of data available for trust evaluation)

Simplifying the formula in **Figure 3-8** results in the formula in **Figure 3-9**. The value cannot exceed 100% or 1.0.

$$\textbf{MACH-T}_{\textbf{A}} = \textbf{MACH-T}_{\textbf{U}} * \frac{\text{Total Trace Records} * \text{TD}}{\text{Desired Trace Records per day} * \text{Days in Date Range} * \text{Desired Number of Days}}$$

Figure 3-9 Simplified Formula for Confidence-Adjusted Trust Algorithm Value MACH-TA

Table 3.5 describes numerators for each term in the unadjusted trust formula. The denominators for each term are the average plus one standard deviation of the same ratio in the numerator. If the node's numerator value is $\geq$ the average + 1σ of all nodes in the population, this factor will increase the MACH-T_U value more than if the value is less than the average + 1σ.

Table 3.6 describes the terms in the Confidence formula.

Table 3.5 MACH-T Formula Term Descriptions

MACH-T_U Formula Term	**Description**
$[W_1 * \frac{\frac{QH}{QD}}{\left(\frac{\overline{QH}}{QD}\right) + 1\sigma}]$	The ratio of qualified hours (number of hours $\geq$ one hour in the same location) to qualified days (number of days with at least one qualified location) is an indication of a node's capability to be present. If a node has no qualifying days, the trust value is zero and the formula is not used.
$[W_2 * \frac{\frac{QL}{QD}}{\left(\frac{\overline{QL}}{QD}\right) + 1\sigma}]$	The ratio of qualified locations (number of locations with $\geq$ one hour in the same location) to qualified days is an indication of a node's capability to be present. If a node has < 2 qualifying locations, the trust value is zero and the formula is not used.
$[W_3 * \frac{\frac{QD}{TD}}{\left(\frac{\overline{QD}}{TD}\right) + 1\sigma}]$	The ratio of qualified days to total days (number of GPS trace days) is an indication of a node's commitment to action over time. If TD is zero, the node has no GPS trace data and the formula is not used.
$[W_4 * \frac{\frac{QL\ km^2}{QL\ perimter\ km^2}}{\left(\frac{QL\ km^2}{QL\ permimeter\ \ km^2}\right) + 1\sigma}]$	The ratio of qualified location area in km^2 to the perimeter are in km2 is an indication of a node's consistency in behavior. Visiting just a small number of total locations indicates high suitability for a MANet since a node's presence is highly predictable within a given location.
$[W_5 * \frac{\frac{QL}{TL}}{\left(\frac{\overline{QL}}{TL}\right) + 1\sigma}]$	The ratio of qualified locations to total locations is an indication of a node's consistency in behavior. If a node's qualifying locations are a large percentage of all the node's locations, it is an indication of a node's consistency in behavior and high suitability for a MANet since a node's availability is highly predictable.
$[W_6 * \frac{\frac{QH}{TH}}{\left(\frac{\overline{QH}}{TH}\right) + 1\sigma}]$	The ratio of qualified hours to total hours is an indication of a node's commitment to be available for MANet operation.

Table 3.6 MACH-T Confidence Formula Term Descriptions

Confidence Formula Term	Description
$\frac{\frac{\text{Total TraceRecords}}{\text{TH}}}{\text{Desired Traces Records per hour}}$	**Trace record density per hour.** This term determines the ability of a node to communicate at a desired rate when the node is communicating. It does not reflect a node's ability to be available on any given day. Maximum confidence in the MACH-T value would be for subjects with trace records at a desired rate such as every 5 seconds (12 per minute or 720 per hour) for all days and hours within the start and end date range for which they had trace records. This term could alternatively be constrained to the average traces per qualified hour. More traces during the time a subject is in a location for at least one hour indicates less opportunity to stop the trace application, leave the area, and return later to restart and record another trace record. Depending on the desired confidence level, a MANet operator may choose a maximum trace interval between individual trace records before assuming a trace segment has ended. In our experiment we chose to restart the time and trace counter if a trace interval was longer than 600 seconds or 10 minutes. Because our zoom level defined areas of approximately 469 meters on a side, during ten minutes it would be possible for a subject to leave the area and return at a later time to record another trace which could be interpreted as being in the same place, but the subject would need to stay very close to the area to accomplish such a feat and would require much effort to do so.
$\frac{\text{TH}}{24 * \text{Days in Date Range}}$	**Trace record density per day.** The total possible hours during the days when traces were recorded represents the maximum possible trace data for a given trace day. Traces representing a high percentage of all possible hours during days when traces were recorded will have a higher confidence and indicate a node's ability to be present within a 24-hour period. Periods when a subject was not using the GPS trace application increases the potential for malicious behavior.
$\frac{\text{TD}}{\text{Desired Number of Days}}$	**Trace record volume for date range.** The total days (TD) in the trace data as a percentage of the desired days reflects a node's ability to be present within a date range but does not reflect frequency of communication during an average day. The denominator in this factor is 30 days for this experiment. This term in the Confidence formula is limited to a value of 1.0 if TD exceeds the Desired Number of Days.

3.5 Analysis and Results

3.5.1 Analysis of Geolife GPS Traces

Although each subject created GPS trace data on their own schedule and at days and times of their own choosing, our results nevertheless confirmed observable and repeatable behavioral norms for most of the subjects for visits of at least one hour to the same geographic location visited by the subject over time. Of the 21 trusted subjects (subjects with MACH-T values greater than zero) in our sample of 182 total subjects, each spent an average of 99% of their qualifying time (at least one hour in a location) in only six locations compared to only 46.7% of qualifying time for untrusted subjects. Trusted subjects also spent over 7.5% of their trace hours in one or more qualifying places for at least one hour compared to 3.5% for untrusted subjects.

The following seven tables show results of analyses of the Geolife GPS trace files for 182 subjects. **Table 3.7** lists the totals, averages, minimums, maximums, standard deviations, and modes for the summary data for all 182 subjects. We discovered some of the subjects (82, 84, 140, 142, 153, and 163) recorded traces in Seattle, Washington at the Microsoft Corporate campus, and we decided to analyze the data along with the data traces from Beijing, China. These subjects also recorded locations in Beijing, China, and all were assigned zero MACH-T values due to their QL perimeter km^2 values larger than 1000 km^2 which we chose as an arbitrary bound. **Table 3.8** shows the coefficient values calculated for using in the MACH-T trust formula. The trust coefficients shown in **Table 3.8** were calculated using the values from **Table 3.7**.

Table 3.7 Observed Population Statistics for Geolife Subjects

Statistic	Total Days (TD)	Total Hours (TH)	Total Locations (TL)	Qualified Locations (QL)	Total Qualified Hours (QH)	Total Qualified Days (QD)
Total	18670	41937.2	915622	447	1568.3	686
Average	102.6	230.4	5030.9	2.5	8.6	3.8
Minimum	1	0.1	3	0	0	0
Maximum	2153	3686.9	126342	22	92.89	36
Standard Deviation (σ)	249.4	450.0	12825.6	3.9	16.1	6.3
Mode	8	68.3	386	0	0	0

Table 3.8 Calculated Trust Formula Coefficients from Geolife Subject Statistics

Calculated Trust Formula Coefficients	**QH/ QD**	**QL /QD**	**QD /TD**	**QL km² / QL perimeter km²**	**QL/ TL**	**QH/ TH**
Averages: $\overline{QH/QD}$, $\overline{QL/QD}$, $\overline{QD/TD}$, $\overline{QL/TL}$, $\overline{QH/TH}$ **and** $\left(\overline{\frac{QL\ km^2}{QL\ permimeter\ km^2}}\right)$	1.17	0.45	0.06	0.16	0.001	0.039
Averages + 1σ	2.49	.93	0.17	0.51	0.003	0.102

Table 3.9 shows the MACH-T(A) values for each of the 21 trusted subjects that are greater than zero. The table lists the six formula factors for each subject in descending MACH-T(A) value order. The coefficients representing the "Average + 1σ" values in two cases resulted in trust values slightly greater than 1.0.

Table 3.9 Trusted Subjects in Descending MACH-T Order

Subj.	**QH/ QD**	**QL/ QD**	**QD/ TD**	**QL km² / QL perimeter km²**	**QL/ TL**	**QH/ TH**	**MACH-T_U**	**CONFI-DENCE**	**MACH-T_A**
35	3.259	0.350	0.270	0.025	0.004	0.208	1.108	0.195	0.216
104	1.494	1.000	0.070	0.011	0.003	0.025	0.552	0.286	0.158
7	1.744	0.750	0.074	0.004	0.001	0.022	0.414	0.375	0.155
23	3.444	0.333	0.353	0.200	0.001	0.220	1.113	0.099	0.111
119	1.762	0.500	0.178	0.006	0.002	0.054	0.590	0.186	0.110
1	3.610	0.750	0.056	0.016	0.002	0.069	0.665	0.163	0.108
16	2.158	0.833	0.118	0.003	0.003	0.078	0.694	0.105	0.073
92	2.356	0.571	0.045	0.004	0.002	0.049	0.481	0.152	0.073
40	2.276	0.800	0.185	0.082	0.002	0.082	0.688	0.055	0.038
8	1.224	1.000	0.088	0.045	0.002	0.028	0.504	0.067	0.034
23	1.938	0.107	0.072	0.014	0.000	0.049	0.310	0.104	0.032
96	3.638	0.214	0.125	0.083	0.001	0.187	0.811	0.034	0.027
50	2.815	0.571	0.137	0.004	0.001	0.078	0.600	0.040	0.024
179	2.472	0.500	0.085	0.027	0.001	0.072	0.521	0.040	0.021
125	1.745	0.833	0.105	0.037	0.001	0.057	0.520	0.040	0.021
85	3.381	0.368	0.044	0.005	0.000	0.072	0.483	0.038	0.018
155	1.624	1.000	0.071	0.004	0.003	0.063	0.602	0.027	0.016
34	1.215	1.000	0.030	0.002	0.001	0.026	0.389	0.042	0.016
44	1.220	0.750	0.056	0.006	0.001	0.037	0.407	0.031	0.013
78	1.224	0.800	0.050	0.004	0.002	0.062	0.474	0.016	0.008
82	1.785	0.833	0.063	0.009	0.001	0.047	0.455	0.007	0.003

Table 3.10 Sample of Untrusted Subjects in Descending QL Perimeter km2 Order, TRUST=0

Sub.	QH/ QD	QL/ QD	QD/ TD	QL perimeter km^2	QL km^2 / QL .perimeter km^2	QL/ TL	QH/ TH	MACH-T_U	CONFIDENCE
142	1.846	0.875	0.051	92237500	0.000	0.001	0.037	0.000	0.010
128	2.038	0.647	0.008	18900400	0.000	0.000	0.016	0.000	0.041
140	0.957	0.800	0.013	18691400	0.000	0.000	0.009	0.000	0.013
144	3.309	0.842	0.031	6062560	0.000	0.000	0.060	0.000	0.073
153	1.309	0.842	0.009	2680660	0.000	0.000	0.007	0.000	0.057
115	1.421	0.667	0.016	1846810	0.000	0.000	0.017	0.000	0.014
163	1.397	1.000	0.016	1763110	0.000	0.000	0.010	0.000	0.011
25	1.528	0.667	0.008	1391510	0.000	0.000	0.013	0.000	0.061
42	1.615	1.000	0.033	874739	0.000	0.001	0.021	0.000	0.042
22	3.650	0.545	0.151	603470	0.000	0.001	0.100	0.000	0.136

Table 3.10 lists the six formula factors for 10 sample untrusted subjects and their calculated unadjusted trust value, ordered by descending QL perimeter km^2. This table also lists the TD, QD, and QL values since these values disqualified many of the subjects from being trusted. The data show many subjects with zero trust with $\geq$ 1000 QL perimeter km^2 area, or less than two qualifying locations (QL), or less than 1 qualified day of GPS trace data (QD). Other subjects with zero trust had < 30 total days (TD) of GPS traces. Confidence factors for untrusted subjects were on average higher than the confidence for trusted subjects.

Table 3.11 shows some data (TH, TL, and QH) used in intermediate calculations in ascending subject order for a sample of 10 subjects.

Although tile coordinates (Min x Tile, Min y Tile, Max x Tile and Max Y Tile) were not used as trust criteria in this experiment, we did analyze the data looking for most frequently visited locations and show results in **Table 3.12**. Future MANet operators looking for nodes in a specific location could select trusted nodes based first on their trust and then on their consistent and long-term presence in desired locations or willingness to be present if requested.

Table 3.11 Summary Subject Data in Ascending Subject Order

Subj	First - Last Date		TH	TL	QH	Min x Tile	Min y Tile	Max x Tile	Max y Tile
000	20081023025304 -	20090705025307	840.4	6322	18.9	53928	24791	54894	26803
001	20081023055305 -	20081214235553	208.7	1463	14.4	53940	24792	53947	24815
002	20081023124523 -	20090322035816	614.4	5699	27.2	52933	24828	53946	25413
003	20081023175854 -	20090705025307	1850.1	22186	92.8	53928	24791	54894	26803
004	20081023175852 -	20090729060736	2020.2	17150	32.3	53925	24802	54901	26779
005	20081024041230 -	20090319043602	252.7	1772	21.3	53439	24807	53950	28628
006	20081023065939 -	20081211043153	109.2	2469	0.0	---	---	---	---
007	20081025142200 -	20081215095900	320.4	3124	7.0	53903	24789	53919	24832
008	20081024114834 -	20081212042153	129.3	1826	3.7	53939	24816	53949	24821
009	20081024101535 -	20081214045729	303.3	1190	21.6	53944	24809	53947	24811

Table 3.12 Most Frequently Visited Locations by Trusted Subjects in Descending QD/TD Order

Subj,	Min xTile	Min yTile	Max xTile	Max yTile	QH/ QD	QL/ QD	QD/ TD	MACH-T_U	CONFI-DENCE	MACH-T_A
023	52487	28499	52491	28502	3.444	0.333	0.353	1.113	0.099	0.111
035	53939	24803	53950	24825	3.259	0.350	0.270	1.108	0.195	0.216
040	53945	24816	53951	24822	2.276	0.800	0.185	0.688	0.034	0.027
119	53957	24796	53974	24834	1.762	0.500	0.178	0.590	0.105	0.073
050	53916	24811	53952	24839	2.815	0.571	0.137	0.600	0.055	0.038
096	53943	24808	53944	24825	3.638	0.214	0.125	0.811	0.163	0.108
016	53903	24791	53945	24828	2.158	0.833	0.118	0.694	0.027	0.016
125	53939	24808	53953	24816	1.745	0.833	0.105	0.520	0.040	0.024
008	53939	24816	53949	24821	1.224	1.000	0.088	0.504	0.186	0.110
179	53940	24789	53944	24810	2.472	0.500	0.085	0.521	0.286	0.158
007	53903	24789	53919	24832	1.744	0.750	0.074	0.414	0.040	0.021
017	53943	24806	53959	24818	1.938	0.107	0.072	0.310	0.040	0.021
155	53947	24811	53978	24832	1.624	1.000	0.071	0.602	0.067	0.034
104	53938	24809	53972	24829	1.494	1.000	0.070	0.552	0.038	0.018
082	53947	24798	53962	24831	1.785	0.833	0.063	0.455	0.152	0.073
001	53940	24792	53947	24815	3.610	0.750	0.056	0.665	0.016	0.008
044	53944	24791	53960	24820	1.220	0.750	0.056	0.407	0.007	0.003
078	53944	24793	53983	24817	1.224	0.800	0.050	0.474	0.375	0.155
092	53940	24803	53975	24828	2.356	0.571	0.045	0.481	0.031	0.013
085	53939	24794	53974	24833	3.381	0.368	0.044	0.483	0.042	0.016
034	53933	24771	53968	24838	1.215	1.000	0.030	0.389	0.104	0.032

Although specific individual tile coordinate data in **Table 3.12** does not contribute to the trust ratings of any subjects, we did identify the most frequently visited locations by trusted subjects by calculating the MODE of the x,y minimum and maximum tile coordinates and then selecting the trusted subjects with qualified locations in this range. The coordinate range is from (53939, 24803) to (53944, 24825) which is a perimeter area of 6 * 23 tiles or 138 * 0.469 km * 0.469 km or 30.4 km^2. Fifteen subjects qualified (rows with shading), and five subjects visited the locations more than 10% of the days in their trace files (QD/TD values greater than 0.10 for the shaded rows).

Finally, one other metric which we considered adding to the trust formula was the number of total hours in qualifying locations as a percentage of all qualifying hours in the GPS trace history for a trusted subject. We show this data in **Table 3.13** to validate the results of the trust algorithm. Trusted subjects spent an average of 99% of their qualifying time (at least

one hour in a location) in only six locations and 87% in only three locations compared to only 47% and 43% respectively of qualifying time for untrusted subjects. Trusted subjects also spent over 7.5% of their trace hours in one or more qualifying places for at least one hour compared to only 3.5% for untrusted subjects. These results are encouraging because they show the potential for concentrated node presence in small numbers of repeatable locations, a requirement for forming a reliable MANet for community and disaster response.

Table 3.13 Percentage of Qualifying Hours in Top Six Most Visited Locations by 21 Trusted Subjects

Subject	#1 loc%	#2 loc%	#3 loc%	#4 loc%	#5 loc%	#6 loc%	Total loc 1-6%	Total loc 1-3%	MACH-T_A
035	57.6	12.1	10.7	9.0	4.6	4.2	98.2	80.4	0.216
104	17.6	15.4	14.4	13.4	11.0	10.2	81.9	47.3	0.158
007	67.7	16.5	15.8	0.0	0.0	0.0	100.0	100.0	0.155
023	69.1	13.8	12.2	4.9	0.0	0.0	100.0	95.1	0.111
119	49.2	28.2	14.2	8.4	0.0	0.0	100.0	91.6	0.110
001	74.4	14.2	11.4	0.0	0.0	0.0	100.0	100.0	0.108
016	42.0	19.7	16.5	13.2	8.6	0.0	100.0	78.2	0.073
092	62.3	15.9	14.0	7.8	0.0	0.0	100.0	92.2	0.073
040	30.9	25.3	22.5	21.4	0.0	0.0	100.0	78.6	0.038
008	42.2	30.0	27.8	0.0	0.0	0.0	100.0	100.0	0.034
017	49.9	48.3	1.8	0.0	0.0	0.0	100.0	100.0	0.032
096	90.5	7.5	2.0	0.0	0.0	0.0	100.0	100.0	0.027
050	73.8	11.3	7.5	7.4	0.0	0.0	100.0	92.6	0.024
179	37.9	37.1	25.0	0.0	0.0	0.0	100.0	100.0	0.021
125	31.6	21.8	19.2	16.3	11.1	0.0	100.0	72.5	0.021
085	39.6	34.1	18.2	2.6	2.1	1.7	98.3	91.9	0.018
155	48.1	26.0	25.9	0.0	0.0	0.0	100.0	100.0	0.016
034	18.5	18.4	17.1	17.0	14.7	14.4	100.0	53.9	0.016
044	46.4	29.5	24.1	0.0	0.0	0.0	100.0	100.0	0.013
078	41.5	23.2	18.8	16.5	0.0	0.0	100.0	83.5	0.008
082	33.7	27.9	16.8	12.2	9.4	0.0	100.0	78.4	0.003

3.6 Discussion

3.6.1 Analysis

Our analysis did not consider any geographic location as more desirable than any other location, but builders of mobile ad hoc networks would likely impose an additional capability factor for this attribute to find mobile devices in specific locations. Selection of a desired geographic location could be one of the dynamic weighted sum variables used at run time to calculate trust.

We also removed the hour of the day and the day of the week values from our results in order to simplify the results, but these values would be potential additional terms in the trust formula for networks operating only at certain hours of the day or days of the week. The day of the month and the month of the year could also be specified and contribute to the trust rating.

Additionally, we did not restrict the age of GPS trace data to a range of dates in the recent past. Some data was collected as far back as 2007 and we considered that data equally with more current data from 2012. MANet operators may decide to impose a period for collecting behavior data such as for example the most recent past 30. Behavior data in the recent past could be weighted more heavily than data in the distant past, but long term consistent desirable behavior should be weighted heavily as it supports all fundamental aspects of trust.

3.6.2 Threat Model and Mitigations

To address the resiliency of the MACH-T algorithm to potential cyber-attacks, we describe each type of cyber-attack as described by Guo, Chen, and Tsai [3] in **Table 3.14** and describe how MACH-T mitigates such types of attack.

Table 3.14 Cyber Attack Types and MACH-T Mitigation

Attack Type	Description	Mitigation
Self-Promotion and Ballot Stuffing	A malicious node increases its own trust level, or one or more nodes unjustifiably increase the trust of another node	MACH-T is not susceptible to ballot stuffing because it does not use recommenders. MACH-T instead uses empirical behavior observed by independent means rather than by recommendations of other nodes in the network. Self-promotion while following expected location permanence patterns would require the nodes to be at repeatable locations, forcing an attacker to fully follow the expected location behaviors.
Bad Mouthing	A malicious node reduces the trust of another node	MACH-T is not susceptible to this attack because it uses a centralized authority independent of recommenders to establish trust. Mobile nodes must independently demonstrate their behavior over time to the central authority to build trust.
On-off Attack	A malicious actor turns on and off the trace recording application with the purpose of masking unexpected behaviors or visited locations.	The confidence value is a measure of the density and length of the received data traces used for the trust value. If a malicious actor were to selectively disable the trace recording application at times when it was in or traveling to unexpected locations the confidence value would decrease because the density and volume of traces over time would decrease.
Opportunistic Service Attack	A malicious node provides good service to gain trust opportunistically especially when it senses its reputation is dropping. With a good reputation/high trust, it can effectively collude with other bad nodes to perform bad-mouthing and ballot-stuffing attacks.	This attack would fall within the previous category of On-Off Attacks. MACH-T is not vulnerable to bad-mouthing and ballot-stuffing attacks because it does not use peer-based reputation but instead uses individual location patterns. Because trust parameters are subject and can be dynamic, a malicious node would need inside knowledge of the parameters at any given time.
Spoofing/ GPS Spoofing	A mobile device could potentially physically attach itself to another unsuspecting mobile node or to a person or vehicle on which the already trusted device is mounted in order to gain trust and be admitted to the MANet.	This attack would be detectible by a trusted node detecting an unknown device in the proximity of the trusted node that remains proximate continuously. This would be an unusual occurrence and the tag along or piggy backing node could be physically removed and possibly destroyed. This type of attack would be expensive and not scalable. GPS spoofing would also be very expensive and would have national security consequences.

3.6.3 Threats to Validity

The analysis in this article stems from one dataset. We calculated average and standard deviation values to use during our trust formation formula design. However, some of these

values are not known to be common to other datasets. Future work is needed to determine if behaviors of human operated mobile devices can be predicted based on constant ratios across multiple datasets, although we did design the MACH-T formula with the intent of parametrizing it further. Ensuring behavioral data sources are trustworthy is an additional factor to consider as we evaluate additional datasets if such are available.

3.7 Conclusions

Experimental results show GPS traces provide sufficient data to automatically and incrementally calculate mobile device trust based on a device's most frequently visited locations. In our experiment, and for the subjects we deemed to be trustworthy, over 99% of trusted devices spent all of their stays of one hour or more in only six locations which for the average subject in the dataset had GPS traces spanning 6.2 months (standard deviation of 1 year, 2.4 months).

Future work could involve date ranges from the more recent past, or additional prorations to assign higher trust formation values to more recent date ranges.

Before ad hoc networks can become secure and resilient, trust will need to be measurable and dynamic. Historical and geographical behavior analysis appears to be a promising avenue for providing the basis for trust formation in mobile ad hoc network devices.

3.7.1 Supplementary Materials

The source code and results of our analysis are available online at https://github.com/CenterForSecureAndDependableSystems/MACH2K.

Chapter 4:
MACH-T: Behavior-based Trust of Personal Mobile Devices with Varied Behavior Expectation Parameters

4.0 Chapter Introduction

The two experiments described in this chapter are also based on the Geolife dataset. The first experiment in Chapter 3 required a node to stay in one location for one hour (3600 seconds). These two experiments compare stay requirements of 20 minutes (1200 seconds) and 60 minutes (3600 seconds).

Several changes in the C++ program parameters changed the results from the first experiment:

1) Removed the requirement for a node to stay within a 1000km^2 area.
2) Reduced the requirement for three qualifying locations to one qualifying location.
3) Stopped processing a trace file for one day when more than 10 minutes elapsed between trace records. The first experiment continued to process the trace file but didn't add the duration of time in the location. This change resulted in many fewer total locations for each subject and the total population in the second experiment.
4) Removed the requirement for 30 days of trace data, and instead made the desired number of days in the confidence formula equal to the days in the date range for all trace records.

This second experiment using the 60 minute time requirement resulted in 49 trusted subjects instead of 21 as in the first experiment.

This chapter provides the same contributions as Chapter 3 supporting Hypothesis 1:

Contribution 1: Create a novel method for measuring trust based on location behavior.

Contribution 2: Design, implement, and test an algorithm (MACH-T) and corresponding software implementation for measuring trust.

This chapter also provides the personal mobile device experiment description and results:

Contribution 3: Design and perform two experiments for evaluating the MACH-T approach and algorithm for the case of personal and taxi-mounted mobile device GPS traces.

Hypothesis 1: Location behaviors in personal mobile devices can be quantified, measured, and used to assign trust. **The results of this experiment indicate the hypothesis is true.**

4.1 Analysis and Results

4.5.1 Analysis of Geolife GPS Traces

For this experiment, the software no longer used the 1000 km^2 boundary or 30 days of data requirement (only one day was required), and the subjects (82, 84, 140, 142, 153, and 163) with traces in Seattle, Washington Microsoft Corporate campus had very low or zero MACH-T(A) trust scores. These restrictions were removed to demonstrate the subjective nature of trust. Also, because the volume of data in the Geolife dataset was much larger than the Roma Taxi dataset, removing the 30 day requirement for the second two Geolife experiments provided a similar set of parameters for comparing the results of the analysis of the two datasets.

Table 4.1 shows the number of trusted subjects (out of a total of 182 subjects) for each set of parameters with information about time spent in qualifying locations (visits of at least 20 or 60 minutes). Trusted subjects are defined as having a MACH-T(A) value greater than zero. The first Geolife experiment resulted in fewer trusted subjects, 21, because of the boundary and number of days required.

Table 4.1 Distribution of Total Qualifying Time Over Qualified Locations for Trusted Geolife Subjects

Number of Locations	20 Minute Minimum Stay (129 trusted subjects)	60 Minute Minimum Stay (49 trusted subjects)
1	54.7%	80.9%
2	72.8%	96.2%
3	80.7%	99.2%
4	85.7%	99.8%
5	89.4%	100%
6	91.9%	100%

Although more subjects achieved MACH-T(A) trust scores above zero with the shorter time in place, more locations qualified. The 20 minute minimum stay analysis showed 90.4% of qualified time spent in the first six qualified locations compared with 100% of the 60 minute stay analysis achieved in the first five qualified locations. The implication for a MANet operator is that shorter minimum stay time requirements yield more potential qualified locations but longer minimum stay time requirements provide more certainty for placing a node at a location.

All of the untrusted subjects (MACH-T(U) values equal to zero) in both experiments had no qualifying locations.

The following ten tables show results of analyses of the Geolife GPS trace files for 182 subjects. Tables 4.2 and 4.3 list the totals, averages, minimums, maximums, standard deviations, and modes for the summary data for all 182 subjects. The first three columns of the two tables contain dataset data that does not change based on the two different minimum stay requirements.

Table 4.2 Observed Population Statistics for Geolife Subjects (20 minute minimum stay)

Statistic	Total Days (TD)	Total Hours (TH)	Total Locations (TL)	Qualified Locations (QL)	Total Qualified Hours (QH)	Total Qualified Days (QD)
Total	10634	9288	485154	836	706.3	908
Average	58.4	51.0	2665.7	4.6	3.9	5.0
Minimum	1	0.03	1	0	0	0
Maximum	1245	1286.5	99104	69	51.1	65
Standard Deviation (σ)	129.1	125.7	8765.3	8.3	6.8	8.9
Mode	6	7.7	58	0	0	0

Table 4.3 Observed Population Statistics for Geolife Subjects (60 minute minimum stay)

Statistic	Total Days (TD)*	Total Hours (TH)*	Total Locations (TL)*	Qualified Locations (QL)	Total Qualified Hours (QH)	Total Qualified Days (QD)
Total	10634	9288	485154	82	164.9	94.0
Average	58.4	51.0	2665.7	.5	.91	.52
Minimum	1	0.03	1	0	0	0
Maximum	1245	1286.5	99104	5	14.65	8
Standard Deviation (σ)	129.1	125.7	8765.3	.87	2.1	1.1
Mode	6	7.7	58	0	0	0

***Same values as the 20 minute minimum stay analysis**

Tables 4.4 and 4.5 show the coefficient population average values calculated for using in the MACH-T trust formula denominators. The trust coefficients are based on the values from Tables 4.2 and 4.3.

Table 4.4 Calculated Trust Formula Coefficients from Geolife Subject Statistics (20 minute minimum stay)

Calculated Trust Formula Coefficients	QH/ QD	QL /QD	QD /TD	QL Km^2 / QL perimeter km^2	QL/ TL	QH/ TH
Averages: $\overline{QH/QD}$, $\overline{QL/QD}$, $\overline{QD/TD}$, $\overline{QL/TL}$, $\overline{QH/TH}$ **and** $\left(\overline{\frac{QL\ km^2}{QL\ permimeter\ km^2}}\right)$	.554	.767	.116	.239	0.006	0.096
Averages + 1σ	1.095	1.453	0.28	0.646	0.024	0.207

Table 4.5 Calculated Trust Formula Coefficients from Geolife Subject Statistics (60 minute minimum stay)

Calculated Trust Formula Coefficients	QH/ QD	QL /QD	QD /TD	QL Km^2 / QL perimeter km^2	QL/ TL	QH/ TH
Averages: $\overline{QH/QD}$, $\overline{QL/QD}$, $\overline{QD/TD}$, $\overline{QL/TL}$, $\overline{QH/TH}$ **and** $\left(\overline{\frac{QL\ km^2}{QL\ permimeter\ km^2}}\right)$	0.460	0.252	0.012	0.163	0.000	0.019
Averages + 1σ	1.359	0.675	0.048	0.523	0.001	0.072

Tables 4.6 and 4.7 show the MACH-T(A) values for the top 10 subjects with MACH-T(A) values greater than zero. The table lists the six formula factors for each subject in descending MACH-T(A) order. Some MACH-T(U) values are slightly greater than 1.0 but all MACH-T(A) values are less than 1.0.

The grey and yellow shaded MACH-T(U) and Confidence values are in the highest ten values for each. The highest MACH-T(A) values do not necessarily always correspond with the highest MACH-T(U) or Confidence values. Confidence values are the same for subjects with MACH-T(U) values greater than zero whether there is a 20 minute or a 60 minute minimum stay requirement since Confidence is based on the density of the data, not the data values.

Table 4.6 Top 10 of 129 Subjects with MACH-T(A) > 0 in Descending MACH-T(A) Order
(20 minute minimum stay)

Subject	QH/QD	QL/QD	QD/TD	km^2 Density	QL/TL	QH/TH	MACH-T (U)	Confidence	MACH-T (A)
151	0.9622	2.0000	1.0000	1.0000	0.0645	0.5795	2.1545	0.0664	0.1430
160	0.5883	1.0000	0.6667	0.1429	0.0230	0.3584	1.0918	0.1251	0.1366
143	0.8208	1.0000	1.0000	1.0000	0.0256	0.3750	1.5775	0.0713	0.1125
137	0.4622	1.0000	1.0000	1.0000	0.0143	0.2193	1.3178	0.0818	0.1078
41	0.5893	0.9032	0.2199	0.0008	0.0011	0.0468	0.3759	0.2448	0.0920
48	1.0892	2.0000	0.3333	0.2500	0.0050	0.2032	0.8703	0.0977	0.0850
77	0.54194	1.0000	0.5000	1.0000	0.0500	0.2514	1.3075	0.0433	0.0567
141	2.6519	5.0000	0.0385	0.0735	0.0154	0.1147	1.2547	0.0432	0.0542
123	1.5267	2.0000	0.2500	0.5000	0.0141	0.2729	1.0718	0.0464	0.0497
25	0.5978	0.6957	0.2434	0.0000	0.0018	0.0699	0.3897	0.1210	0.0472

Table 4.7 Top 10 Geolife Subjects with MACH-T(A) > 0 in Descending MACH-T(A) Order
(60 minute minimum stay)

Subject	QH/QD	QL/QD	QD/TD	km^2 Density	QL/TL	QH/TH	MACH-T (U)	Confidence	MACH-T (A)
123	1.1458	1.0000	0.2500	1.0000	0.0070	0.2048	3.2206	0.0464	0.1493
41	1.1089	1.0000	0.0142	0.1818	0.0001	0.0057	0.5157	0.2448	0.1262
50	1.4672	1.0000	0.0357	1.0000	0.0004	0.03034	1.0113	0.0714	0.0722
23	3.5831	0.6667	0.1429	0.3333	0.0007	0.1955	1.7813	0.0358	0.0637
13	1.3592	1.0000	0.0110	1.0000	0.0004	0.0169	0.8783	0.0645	0.0566
159	1.2754	0.2500	0.3077	1.0000	0.0039	0.2073	2.7299	0.0206	0.05615
16	2.3956	1.0000	0.0571	0.0155	0.0024	0.1457	1.4731	0.0361	0.0532
30	2.5593	1.0000	0.0113	1.0000	0.0005	0.0418	1.1006	0.0424	0.0467
8	1.5494	1.0000	0.0333	1.0000	0.0012	0.0551	1.1949	0.0389	0.0465
179	1.1167	1.0000	0.0222	1.0000	0.0005	0.0196	0.9075	0.0439	0.0399

Table 4.8 and **Table 4.9** list the six formula factors for 10 sample subjects with the lowest MACH-T(A) values and their calculated unadjusted trust value, ordered by descending MACH-T(A) values. The data show many subjects with very low trust with much less than one qualified day per total days (QD/TD) of GPS trace data and had correspondingly low confidence values as a result. Subject 56, in particular, in **Table 4.8** (20 minute minimum stay) had a high MACH-T(U) value of 1.1278 but a very low confidence resulting in a very low MACH-T(A) value. Subjects 51 and 101 in **Table 4.9** (60 minute minimum stay) had two of the ten highest MACH-T(U) values but the very low confidence factor resulted in two of the ten lowest MACH-T(A) values.

Table 4.8 Lowest 10 Geolife Subjects with MACH-T(A) > 0 in Descending MACH-T(A) Order
(20 minute minimum stay)

Subject	QH/QD	QL/QD	QD/TD	km^2 Density	QL/TL	QH/TH	MACH-T (U)	Confidence	MACH-T (A)
146	0.3939	1.0000	0.1250	1.0000	0.0164	0.1238	0.7263	0.0010	0.0007
118	0.3494	1.0000	0.2500	1.0000	0.0111	0.1810	0.8029	0.0008	0.0006
56	1.8122	4.0000	0.0435	0.3333	0.0161	0.1753	1.1278	0.0006	0.0006
139	0.3611	1.0000	0.0625	1.0000	0.0097	0.0636	0.5893	0.0008	0.0005
114	0.3547	1.0000	0.0625	1.0000	0.0010	0.0255	0.4972	0.0007	0.0003
111	0.6225	1.0000	0.0286	1.0000	0.0006	0.0123	0.5049	0.0004	0.0002
174	0.3746	1.0000	0.0462	0.0200	0.0064	0.0460	0.2924	0.0006	0.0002
134	0.3696	1.0000	0.0345	0.3333	0.0043	0.0462	0.3512	0.0005	0.0002
58	0.3702	1.0000	0.1765	0.0026	0.0083	0.0915	0.4148	0.0002	0.0001
55	0.4876	1.0000	0.1111	1.0000	0.0180	0.1456	0.7614	0.0001	0.0001

Table 4.9 Lowest 10 Geolife Subjects with MACH-T(A) > 0 in Descending MACH-T(A) Order (60 minute minimum stay)

Subject	QH/QD	QL/QD	QD/TD	km² Density	QL/TL	QH/TH	MACH-T (U)	Confidence	MACH-T (A)
168	1.1364	1.0000	0.0154	1.0000	0.0002	0.0140	0.8191	0.0131	0.0108
3	1.1565	0.6667	0.0135	0.0000	0.0004	0.0239	0.4739	0.0205	0.0097
140	1.0975	1.0000	0.0042	1.0000	0.0001	0.0069	0.7431	0.0117	0.0087
82	1.4258	0.7500	0.0548	0.0055	0.0008	0.0790	0.8754	0.0064	0.0056
51	3.6636	0.7500	0.0889	0.0000	0.0045	0.4009	2.6217	0.0019	0.0051
92	1.2861	1.0000	0.0096	1.0000	0.0008	0.0210	0.9320	0.0045	0.0042
101	3.1211	1.0000	0.0513	1.0000	0.0032	0.1864	2.0943	0.0020	0.0041
142	1.2536	1.0000	0.0097	1.0000	0.0002	0.0159	0.8250	0.0038	0.0031
104	1.3435	1.0000	0.0291	0.0045	0.0023	0.0628	1.0449	0.0026	0.0027
163	1.4746	1.0000	0.0037	0.0000	0.0001	0.0076	0.4717	0.0050	0.0023

Table 4.10 and **Table 4.11** show the subjects with the highest Confidence values in descending Confidence value order. Five of the subjects for the 20 minute stay have MACH-T(A) values above zero while only two subjects for the 60 minute minimum stay also have MACH-T(A) values above zero due to having MACH-T(U) values equal to zero. Confidence can reduce the MACH-T(U) value but not increase it since the Confidence is the ratio of actual traces over the maximum possible over all possible days in the trace range of days. None of the highest confidence values for either minimum stay requirement corresponded to subjects with one of the ten highest MACH-T(U) values. Also, none of the ten lowest Confidence values for either of the stay requirements had either MACH-T(U) or MACH-T(A) in the top ten highest values.

Table 4.10 Geolife Subjects with highest Confidence values in Descending Confidence Order (20 minute minimum stay)

Subject	QH/QD	QL/QD	QD/TD	km² Density	QL/TL	QH/TH	MACH-T (U)	Confidence	MACH-T (A)
41	0.5893	0.9032	0.2199	0.0008	0.0011	0.0468	0.3759	0.2448	0.0920
124	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1729	0.0000
160	0.5883	1.0000	0.6667	0.1429	0.0230	0.3584	1.0918	0.1251	0.1366
156	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1215	0.0000
25	0.5978	0.6957	0.2434	0.0000	0.0018	0.0699	0.3897	0.1210	0.0472
120	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1078	0.0000
48	1.0892	2.0000	0.3333	0.2500	0.0050	0.2032	0.8703	0.0977	0.0850
88	0.3861	1.0000	0.1765	0.0083	0.0050	0.0491	0.3612	0.0937	0.0338
169	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0926	0.0000
137	0.4622	1.0000	1.0000	1.0000	0.0143	0.2193	1.3178	0.0818	0.1078

Table 4.11 Geolife Subjects with highest Confidence values in Descending Confidence Order (60 minute minimum stay)

Subject	QH/QD	QL/QD	QD/TD	km^2 Density	QL/TL	QH/TH	MACH-T (U)	Confidence	MACH-T (A)
41	1.1089	1.0000	0.0142	0.1818	0.0001	0.0057	0.5157	0.2448	0.1262
124	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1729	0.0000
156	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1215	0.0000
25	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1210	0.0000
120	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1078	0.0000
169	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0926	0.0000
88	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0882	0.0000
160	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0834	0.0000
137	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0818	0.0000
50	1.4672	1.0000	0.0357	1.0000	0.0004	0.0303	1.0113	0.0714	0.0722

Although tile coordinates (Min x Tile, Min y Tile, Max x Tile and Max Y Tile) were not used as trust criteria in these experiments, data analysis included looking for most frequently visited locations (mode) and the results are shown in **Table 4.12**. Future MANet operators looking for nodes in a specific location could select trusted nodes based first based on their trust and then on their consistent and long-term presence in desired locations or willingness to be present if requested.

Table 4.12 Most Frequently Visited Locations by Subjects with MACH-T(A) Values > 0

Most Frequently Visited Locations(Mode)	**20 Minute Minimum Stay (129 trusted subjects) 10 square tile area (2x5 tiles)**	**60 Minute Minimum Stay (49 trusted subjects) 18 square tile area (3x6 tiles)**
minXtile	53944	53945
minYtile	24812	24813
maxXtile	53945	53947
maxYtile	24816	24818

4.2 Discussion

4.2.1 Analysis

Repeating the Geolife dataset analysis with two different criteria for minimum duration of stay in a location demonstrated how changing definitions of trust can change a trust rating. It also demonstrated the capability of the MACH-T approach to measure trust on mobile nodes based on the fit to expected location behaviors. The 20 minute minimum stay parameter provided many more qualifying locations and many more subjects with MACH-T(A) values

greater than zero (129 versus 49). The average number of qualified locations for the 20 minute stay was 4.6 versus 0.5 for the 60 minute stay requirement. However, the average MACH-T(A) value for the 20 minute stay was 0.0153 (standard deviation 0.0250) and for the 60 minute stay was nearly double at 0.0279 (standard deviation 0.0281). Longer minimum stay requirements resulted in higher trust values.

4.3 Conclusions

Experimental results show GPS traces provide sufficient data to programmatically and incrementally calculate mobile device trust based on a device's visited locations. Because the MACH-T(U) formula can be adjusted by changing coefficients or removing some terms altogether, MANet operators can determine their desired node behavior and then measure node behavior according to the fit of mobile device nodes behavior to the desired or expected (baseline) behavior.

4.3.1 Supplementary Materials

The source code and results of our analysis are available online at https://github.com/CenterForSecureAndDependableSystems/MACH2K.

Chapter 5:

MACH-T: Behavior-based Trust of Taxi-Mounted Mobile Devices

5.0 Chapter Introduction

The two experiments documented in this chapter analyze the Roma Taxi dataset. These two experiments compare stay requirements of 10 minutes (600 seconds) and 20 minutes (1200 seconds). Instead of using population average behavior as algorithm coefficients, a set of ideal coefficients were used to determine the trust values.

The program parameters for the two experiments in this chapter were the same as for the two Geolife dataset experiments described in Chapter 4.

This chapter provides the same three contributions as Chapters 3 and 4 but supports Hypothesis 2 instead of Hypothesis 1:

Contribution 1: Create a novel method for measuring trust based on location behavior.

Contribution 2: Design, implement, and test an algorithm (MACH-T) and corresponding software implementation for measuring trust.

Contribution 3: Design and perform two experiments for evaluating the MACH-T approach and algorithm for the case of personal and taxi-mounted mobile device GPS traces.

- Hypothesis 2: Location behaviors in vehicle-mounted mobile devices can be quantified, measured, and used to assign trust values. **The results of this experiment indicate the hypothesis is true.**

5.1 Dataset

This section describes the dataset we used for our analysis and experiments.

The RomaTaxi dataset from Bracciale, et al. [46] is a publicly available dataset. The researchers collected GPS traces from 291 taxi-mounted GPS tracker Android devices during a six-month period from October 2013 through April, 2014, in Rome, Italy. They made the first four days of data from February, 2014 available for public download. The average

subject's data spanned 2.46 days (standard deviation of 1.091 days). The sampling rates averaged 15.164 seconds (standard deviation of 1.104 seconds). The data was mostly gathered in central Rome, Italy. The researchers stated their focus was on an 8km x 8km area (or 64 km^2) in the center of Rome. The average geographic area traveled in this analysis of the dataset was 63km^2 for subjects with MACH-T(A) values greater than zero with a 20 minute stay requirement. Some subjects traveled far outside the focus area as in the case of trusted subjects in the 10 minute stay requirement analysis with an average area covered of 98.2km^2. Untrusted subjects in both analyses traveled even farther, a maximum of 1,166km^2 in the 10 minute stay analysis.

Researchers who collected the data stated they collected traces every 7 seconds, but the dataset download contained traces only every 15 seconds.

Table 5.1 provides the data format of the detail records in the Roma Taxi GPS trace files which were in semicolon-separated fields. **Figure 5-1** shows three example Roma Taxi GPS trace records.

Table 5.1 Roma Taxi GPS Trace File Detail Record Data Format

Field 1	Taxi Number (Subject)
Field 2	Date: YYYY-MM-DD
Field 3	Time: HH:MM:SS
Field 4	Unused field
Field 5	"POINT("
Field 6	Latitude
Field 7	Longitude
Field 8	")"

```
156;2014-02-01 00:00:00.739166+01;POINT(41.8836718276551 12.4877775603346)
187;2014-02-01 00:00:01.148457+01;POINT(41.9285433333333 12.4690366666667)
297;2014-02-01 00:00:01.220066+01;POINT(41.8910686119733 12.4927045625339)
```

Figure 5-1 Example Roma Taxi GPS Trace Data Records

5.2 Methods

Because the plan was to use the same C++ software used for the prior experiments to analyze the GPS traces, the data records first needed to be converted to the same format as the Geolife records. Writing a preprocessor program provided a way to convert the raw Roma Taxi Data which was contained in a single file into multiple GPS trace files in the same format as

the Geolife records. The Geolife records were stored in one or more files for each date. The preprocessor for the Roma Taxi dataset created one file per date from the single file provided in the download. **Figure 5-2** shows the workflow for the Roma Taxi processing. Data stores are represented with boxes, and processes in italic typeface.

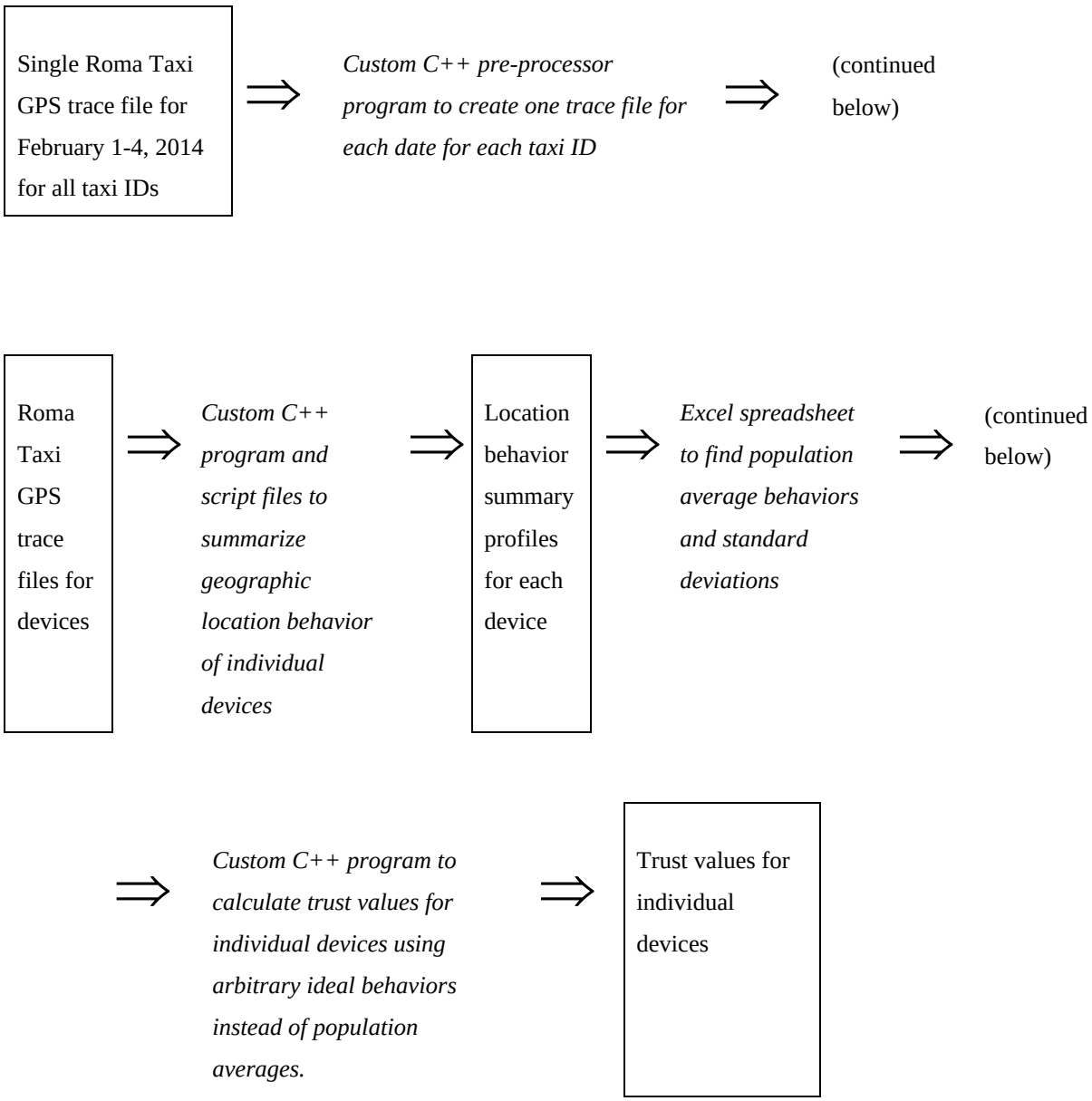


Figure 5-2 Roma Taxi Data Analysis Workflow

Once the raw Roma Taxi data was converted into the same format as the Geolife records, the same C++ software was used to analyze the data. The trust parameters for length of stay were set at 10 minutes for the first experiment and 20 minutes for the second. In

addition, the Confidence parameter was set to 240 traces per hour (one every 15 seconds) based on the actual Roma Taxi data.

Because the OpenStreetMap.org tile sizes vary based on latitude, the similar latitudes of Rome (approximately 41 degrees North) and Beijing (approximately 40 degrees North) justified keeping the same OpenStreetMap.org tile area constant at 0.469km for zoom level 16.

5.3 Analysis and Results

The Roma Taxi dataset spans four days in February 2014, concentrated in mostly a small geographic area less than 100km^2. Due to this relatively smaller area compared to the Geolife dataset, the resulting behavioral data shows more repeated location visits than the Geolife dataset. Results show behavioral consistency for visits of at least 10 minutes (600 seconds) or 20 minutes (1200 seconds) to the same geographic location visited by the subjects over time. When requiring 60-minute minimum stays, trusted subjects in the Geolife dataset spent 100% of qualified hours in the first five qualified locations (see **Table 4.1**), while trusted subjects in the Roma Taxi dataset spent 94.7% and 98.6% percent of qualified hours in the 10 minute and 20 minute stay experiments, respectively. The shorter time requirement caused more locations to qualify and therefore the first six qualified locations did not account for all qualified locations for the trusted subjects.

Table 5.2 shows the number of trusted subjects (out of a total of 291 subjects) for each length of stay requirement. Trusted subjects are defined as having MACH-T(A) valued greater than zero.

Table 5.2 Distribution of Total Qualifying Time Over Qualified Locations for Roma Taxi Trusted Subjects

Number of Locations	10 minute Stay (274 trusted subjects)	20 Minute Minimum Stay (259 trusted subjects)
1	46.4%	54.4%
2	66.5%	76.2%
3	78.7%	88.0%
4	86.3%	94.1%
5	91.4%	97.2%
6	94.7%	98.6%

More subjects achieved MACH-T(A) trust scores above zero with the shorter required minimum stay (274 versus 259). The 10 minute minimum stay analysis showed 94.7% of qualified time spent in the first six locations compared with 98.6% of the 20 minute stay

analysis. The implication for a MANet operator is that shorter time requirements yield more potential locations but longer time requirements provide more certainty for placing a node at a location. The Roma Taxi dataset shows much less difference between the 10 and 20 length of stay requirements than the difference between the Geolife 20 minute and 60-minute results (see **Table 4.1**).

Table 5.3 and **Table 5.4** list the totals, averages, minimums, maximums, standard deviations, and modes for the summary data for all 291 taxi subjects.

Table 5.3 Observed Population Statistics for Roma Taxi Subjects (10 minute minimum stay)

Statistic	Total Days (TD)	Total Hours (TH)	Total Locations (TL)	Qualified Locations (QL)	Total Qualified Hours (QH)	Total Qualified Days (QD)
Total	716	3110	115688	1662	1240.6	572
Average	2.46	10.7	397.6	5.71	4.26	1.97
Minimum	1.0	0.0	1.0	0.0	0.0	0.0
Maximum	4.0	30.9	1574.0	19.0	16.57	4.0
Standard Deviation (σ)	1.09	6.89	286.98	3.586	3.304	1.096
Mode	3.0	9.0	326.0	6.0	0.0	1.0

Table 5.4 Observed Population Statistics for Roma Taxi Subjects (20 minute minimum stay)

Statistic	Total Days (TD)	Total Hours (TH)	Total Locations (TL)	Qualified Locations (QL)	Total Qualified Hours (QH)	Total Qualified Days (QD)
Total	*	*	*	981	958.9	503.0
Average	*	*	*	3.37	3.3	1.73
Minimum	*	*	*	0.0	0.0	0.0
Maximum	*	*	*	11.0	14.57	4.0
Standard Deviation (σ)	*	*	*	2.31	2.85	1.09
Mode	*	*	*	3.0	0.0	1.0

***Same values as the 20 minute stay analysis**

Table 5.5 contains the coefficient values arbitrarily set as ideal coefficients. The trust coefficients are not based on the values from **Table 5.3** and **Table 5.4** as they were with the Geolife experiment. The Roma Taxi experiments did not use the population average behavior as the ideal behavior but instead chose the values to use in the MACH-T(U) formula.

Table 5.5 Ideal Trust Formula Coefficients from Roma Taxi Subject Statistics
(10 and 20 minute minimum stay)

Trust Formula Coefficients	QH/ QD	QL /QD	QD /TD	QL km^2 / QL perimeter km^2	QL/ TL	QH/ TH
Arbitrary Ideal Values →	6.0	2.0	1.0	0.064	0.004	0.5

Table 5.6 and **Table 5.7** contain the MACH-T(A) values for the top 10 subjects with MACH-T(A) values greater than zero. The table lists the six formula factors for each subject in descending MACH-T(A) order. Some MACH-T(U) values are slightly greater than 1.0 but all MACH-T(A) values are less than 1.0 for the 10 minute stay requirement, but some of the values are greater than 1.0 for the 20 minute stay requirement. A MANet operator can determine the value of MACH-T(A) sufficient for inclusion in a MANet. A higher value denotes higher trust.

The grey and yellow shaded MACH-T(U) and Confidence values are in the highest ten values for each. The highest MACH-T(A) values (shaded in green) do not necessarily always correspond with the highest MACH-T(U) or Confidence values. Confidence values are the same for subjects whether there is a 10 minute or a 20 minute stay requirement since Confidence is based on the density of the data, not the data values.

Table 5.6 Top 10 Trusted Roma Taxi Subjects in Descending MACH-T(A) Order (10 minute minimum stay)

Subject	QH/QD	QL/QD	QD/TD	km^2 Density	QL/TL	QH/TH	MACH-T (U)	Confidence	MACH-T (A)
99	6.4824	8.0000	1.0000	0.0058	0.0292	0.6437	1.3226	0.4148	0.5486
356	4.9968	9.0000	1.0000	0.0256	0.0495	0.5531	1.3372	0.3700	0.4947
300	4.7952	10.0000	1.0000	0.0101	0.0385	0.5287	1.3170	0.3736	0.4920
243	4.1952	4.0000	1.0000	0.0082	0.0128	0.4454	0.8428	0.5835	0.4918
186	4.4568	8.0000	1.0000	0.0952	0.0440	0.4882	1.2283	0.3771	0.4632
96	3.9728	3.3333	1.0000	0.0051	0.0105	0.4410	0.7839	0.5618	0.4404
252	3.1472	4.3333	1.0000	0.0079	0.0121	0.3559	0.7598	0.5423	0.4120
171	3.8232	8.0000	1.0000	0.1429	0.0325	0.4387	1.1391	0.3611	0.4113
157	2.7528	5.0000	1.0000	0.0500	0.0151	0.3219	0.7814	0.5252	0.4104
316	2.9600	4.3333	1.0000	0.0077	0.0155	0.3610	0.7637	0.5066	0.3869

Table 5.7 Top 10 Trusted Roma Taxi Subjects in Descending MACH-T(A) Order (20 minute minimum stay)

Subject	QH/QD	QL/QD	QD/TD	km^2 Density	QL/TL	QH/TH	MACH-T (U)	Confidence	MACH-T (A)
308	4.4232	1.0000	1.0000	1.0000	0.0046	0.4880	3.3084	0.3715	1.2292
70	3.4164	0.5000	1.0000	1.0000	0.0024	0.4964	3.1518	0.3818	1.2033
151	1.3080	3.0000	1.0000	1.0000	0.0103	0.1626	3.5179	0.3325	1.1696
212	1.6656	1.0000	1.0000	1.0000	0.0056	0.3920	3.2424	0.3510	1.1382
141	1.9584	1.0000	1.0000	1.0000	0.0041	0.2271	3.1343	0.3538	1.1090
48	1.2936	1.0000	1.0000	1.0000	0.0033	0.1603	3.0587	0.3335	1.0201
269	1.9176	2.0000	0.3333	1.0000	0.0016	0.0885	2.9562	0.2991	0.8843
356	4.0776	6.0000	1.0000	0.0170	0.0330	0.4514	2.3471	0.3700	0.8684
244	0.4320	1.0000	1.0000	1.0000	0.0034	0.0627	3.0074	0.2877	0.8652
186	2.6520	5.0000	1.0000	0.1250	0.0275	0.2905	2.2206	0.3771	0.8374

Table 5.8 and **Table 5.9** list the six formula factors for 10 sample subjects with MACH-T(U) values equal to zero, ordered by descending Confidence values. The data show all subjects with zero trust with no qualified hours and small numbers of traces (in the Trace Count column) resulting in low but not zero Confidence values. Because many of the untrusted subjects in the 20 minute stay experiment were trusted in the 10 minute stay experiment, the subjects listed in the tables are different. The Confidence values in the 10 minute stay experiment are also significantly lower because many of the trusted subjects with higher Confidence values were applied to much lower MACH-T(U) values resulting in MACH-T(A) values greater than zero.

Table 5.8 Sample of Roma Taxi Subjects with MACH-T(U) = 0 in Decreasing Confidence Order (10 minute minimum stay)

Subject	QH/QD	QL/QD	QD/TD	km^2 Density	QL/TL	QH/TH	MACH-T (U)	Confidence	Trace Count
324	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0462	532
132	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0461	531
60	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0431	248
41	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0401	231
122	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0397	457
358	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0177	102
279	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0175	101
294	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0128	148
215	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0122	70
320	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0109	63

Table 5.9 Sample of Roma Taxi Subjects with MACH-T(U) = 0 in Decreasing Confidence Order (20 minute minimum stay)

Subject	QH/QD	QL/QD	QD/TD	km^2 Density	QL/TL	QH/TH	MACH-T (U)	Confidence	Trace Count
221	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.2651	1527
181	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1882	1084
88	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1569	904
56	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1444	832
79	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.1128	1300
341	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0885	1530
89	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0742	1710
343	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0648	746
62	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0530	916
80	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0488	562

Although tile coordinates (Min x Tile, Min y Tile, Max x Tile and Max Y Tile) were not used as trust criteria in this experiment, the data for the most frequently visited locations (mode) is in **Table 5.10**. MANet operators looking for nodes in a specific location could add a term or replace one of the terms in the MACH-T(U) formula with a term specifying minimum time spent in a specific geographic location.

Table 5.10 Most Frequently Visited Locations by Roma Taxi Subjects with MACH-T(A) Values > 0

Most Frequently Visited Locations (mode)	**10 Minute Minimum Stay (274 trusted subjects) 256 square tile area (8 x 32 tiles)**	**20 Minute Minimum Stay (259 trusted subjects) 174 square tile area (6 x 29 tiles)**
minXtile	35036	35038
minYtile	24347	24350
maxXtile	35043	35043
maxYtile	24378	24378

The 10 minute minimum stay requirement produced a larger geographic area of most frequently visited locations than the 20 minute stay requirement. **Figure 5-3** and **Figure 5-4** show the tile area (orange rectangle) on a map for the 10-and 20-minute stay subjects using the Geofabrik tile overlay tool [43]. Although the mapping used tiles at zoom level 16, the image shown at zoom level 12 allowed the complete rectangle to fit on one web page. The map areas reflect a boundary area of frequent locations, but the coverage is not 100% of all possible tiles in the areas. For trusted subjects, the density or coverage of tiles visited to total square tile area was 15.3% (standard deviation 26.4%) for the 10-minute stay requirement and 23.9% (standard deviation 34.4%) for the 20-minute stay requirement. Although the 20-minute stay area is smaller, there is higher coverage of tiles.

The area on the map in **Figure 5-3** (10-minute stay) extends further north and west than the map in **Figure 5-4** (20-minute stay). The total area covered by the 256 tiles in the 10 minute stay experiment is an 8 by 32 tile area or 55.2km^2 or approximately 56.2% of the 98.2km^2 total area covered by the traces for trusted subjects. The total area covered by the 174 tiles in the 20 minute stay experiment is a 6 by 29 tile area or 38.3km^2 or approximately 60.7% of the 63.1km^2 total area covered by the traces for trusted subjects. The 20 minute stay requirement produced fewer trusted subjects and a smaller geographic area of most visited locations, but a higher concentration of stays in the total qualifying area covered by trusted subjects. A MANet operator would prefer the higher concentration for better node coverage.

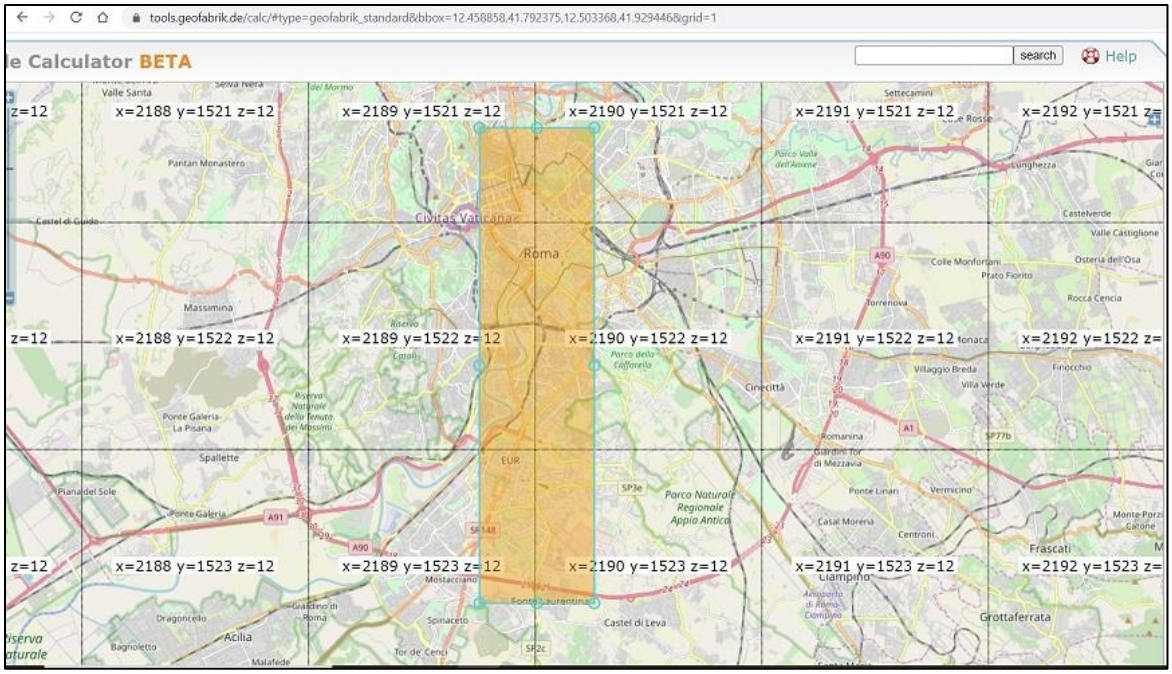


Figure 5-3 Geographic Area Covered by Trusted Roma Taxi Subjects with MACH-T(A) > 0 (10 minute stay)

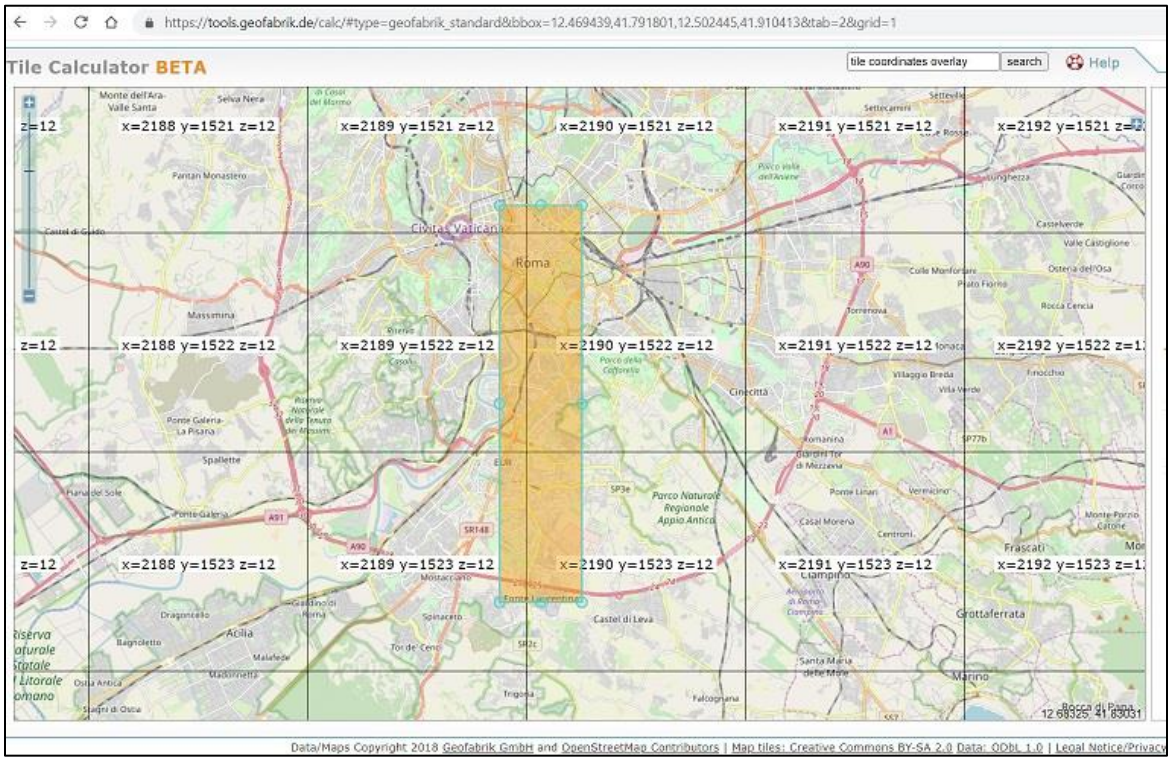


Figure 5-4 Geographic Area Covered by Trusted Roma Taxi Subjects with MACH-T(A) > 0 (20 minute stay)

5.4 Discussion

The Roma Taxi dataset provided another real-world dataset to validate the methods used for the Geolife dataset. The Roma Taxi dataset had 291 subjects versus the 182 subjects in the Geolife dataset. The Roma Taxi dataset contained only four days of data whereas the Geolife dataset covered a much longer period (almost five years) although the average subject's data spanned just over six months. The Roma Taxi dataset was confined to a much smaller geographic area and was comprised of a homogenous type of mobile user, a taxi. Geolife subjects were individuals with smart phones and their behavior was more varied based on the daily activities of the owners of the devices. The Geolife subjects were not employed in the same occupation as were the subjects in the Roma Taxi dataset, which also contributed to the variety in activities. **Table 5.11** shows a variety of statistics for the two datasets.

Although the two datasets contained GPS traces for vastly different population types, the resulting MACH-T(U) values were generally between zero and 1.0 and showed a somewhat normal distribution indicated by the median, mode, and average values being close in value. The Confidence values were skewed to the low range and reduced the MACH-T(U) values giving the resulting MACH-T(A) values. **Figure 5-5** through **Figure 5-10** show the distribution histograms for the MACH-T(U), Confidence, and MACH-T(A) values for the Geolife 60-minute stay second experiment (from Chapter 4) and the Roma Taxi 10-minute experiment.

Table 5.11 Comparison of Geolife and Roma Taxi Dataset Statistics and Subject Devices

Statistic	**Geolife Dataset (population average coefficients)**	**Roma Taxi Dataset (arbitrary ideal coefficients)**
Number of subjects	182	291
Range of dates for all GPS Traces	Up to 5 years	Up to 4 days
Total number of trace days for all subjects	10,634	716
Average number of trace days for all subjects	58.4	2.5
MACH-T(U) Coefficients	20 minute stay: QH/QD=1.077, QL/QD=1.380, QD/TD=0.281, QL km^2 density=0.648 QL/TL=0.024, QH/TH=0.207 60 minute stay: QH/QD=1.360, QL/QD=0.675, QD/TD=0.048, QL km^2 density=0.523 QL/TL=0.001, QH/TH=0.072	10 and 20 minute stays: QH/QD=6.0, QL/QD=2.0 QD/TD=1.0 QL km^2 density=0.064 QL/TL=0.004 QH/TH=.5
Number of trusted subjects	20 minute stay: 129 60 minute stay: 49	10 minute stay: 274 20 minute stay: 259
Average number of total locations for all subjects	20 minute stay: 2,666 60 minute stay: 2,666	10 minute stay: 398 20 minute stay: 398
Average number total locations for trusted subjects	20 minute stay: 3,652 60 minute stay: 6,658	10 minute stay: 420 20 minute stay: 434
Highest MACH-T(U) value for all subjects	20 minute stay: 2.7369 60 minute stay: 3.2206	10 minute stay: 2.8388 20 minute stay: 23.9035
Highest Confidence value for all subjects (Confidence depends on data density, not on trust parameters. Values are the same for each stay length.)	20 minute stay: 0.2448 60 minute stay: 0.2448	10 minute stay: 0.5835 20 minute stay: 0.5835
Highest MACH-T(A) value for all subjects	20 minute stay: 0.1430 60 minute stay: 0.1493	10 minute stay: 0.5486 20 minute stay:
Average MACH-T(U) value for subjects with MACH-T(A) > 0	20 minute stay: 0.6066 60 minute stay: 1.1542	10 minute stay: 0.7184 20 minute stay: 1,2292
Average Confidence value for subjects with MACH-T(A) > 0	20 minute stay: 0.0255 60 minute stay: 0.0285	10 minute stay: 0.2348 20 minute stay: 0.2359
Average MACH-T(A) value for subjects with MACH-T(A) > 0	20 minute stay: 0.0156 60 minute stay: 0.0279	10 minute stay: 0.1751 20 minute stay: 0.3401

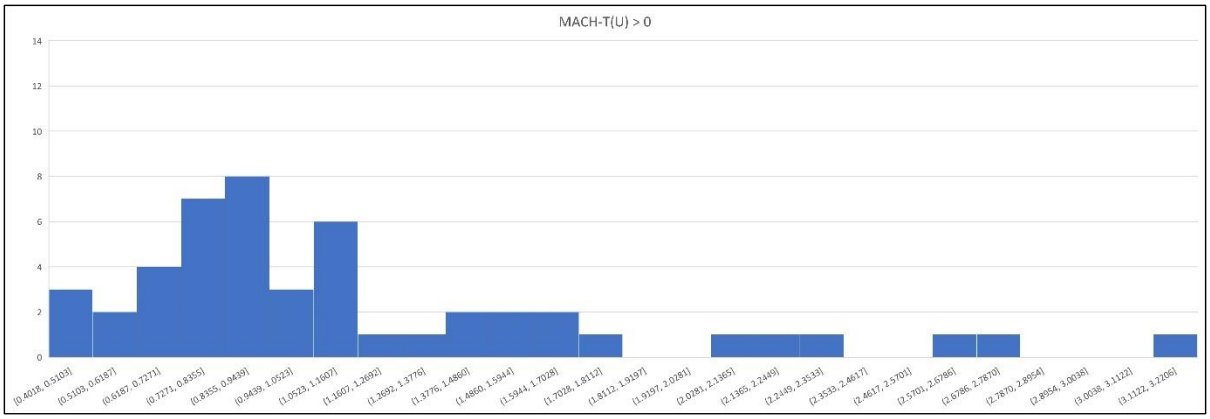


Figure 5-5 Distribution of Geolife MACH-T(U) Values (60 minute stay)

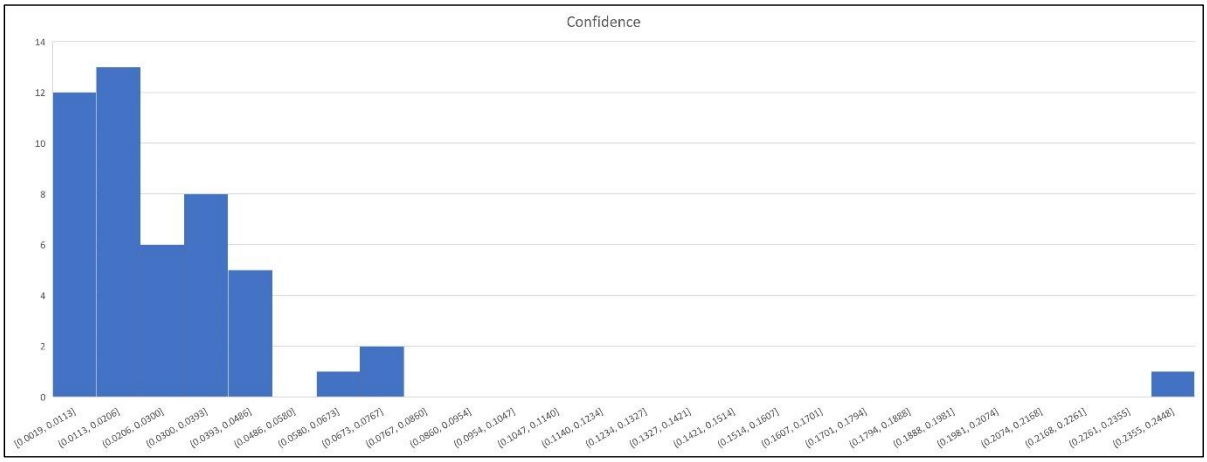


Figure 5-6 Distribution of Geolife Confidence Values (60 minute stay)

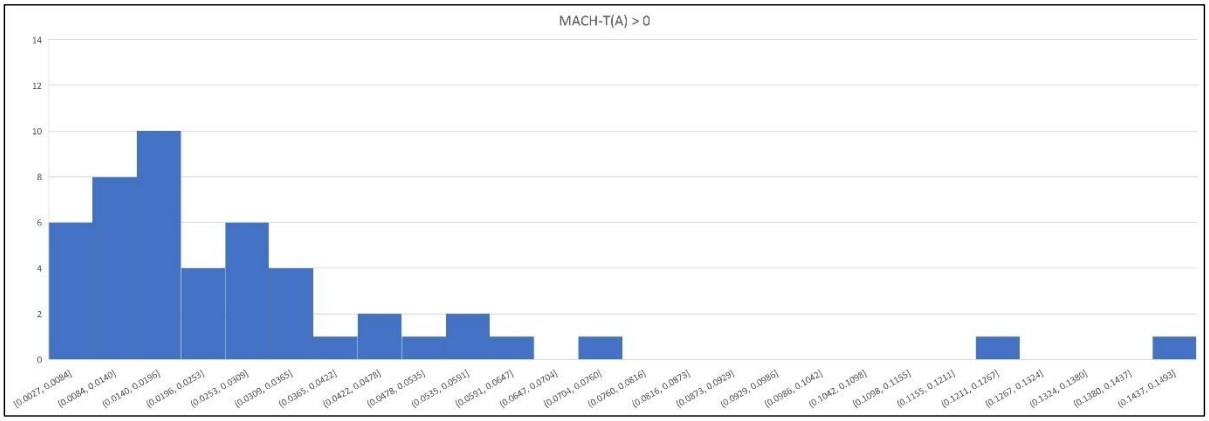


Figure 5-7 Distribution of Geolife MACH-T(A) Values (60 minute stay)

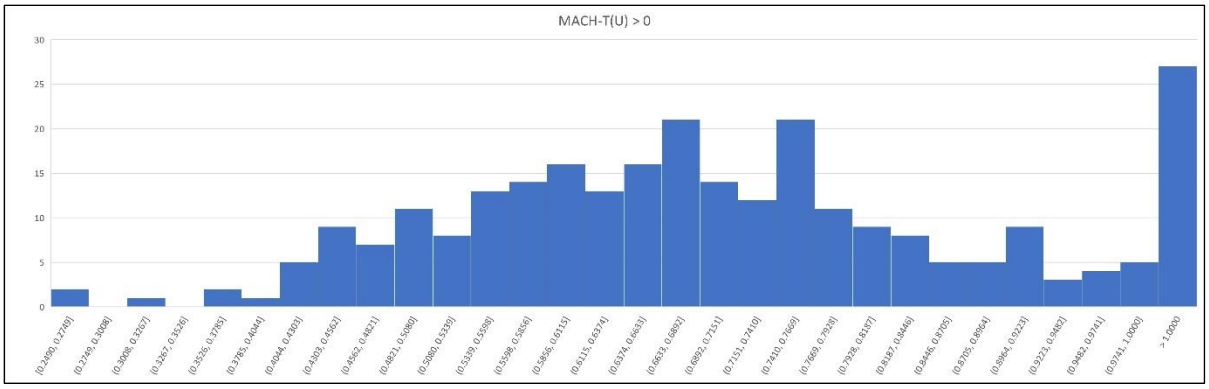


Figure 5-8 Distribution of Roma Taxi MACH-T(U) Values (10 minute stay)

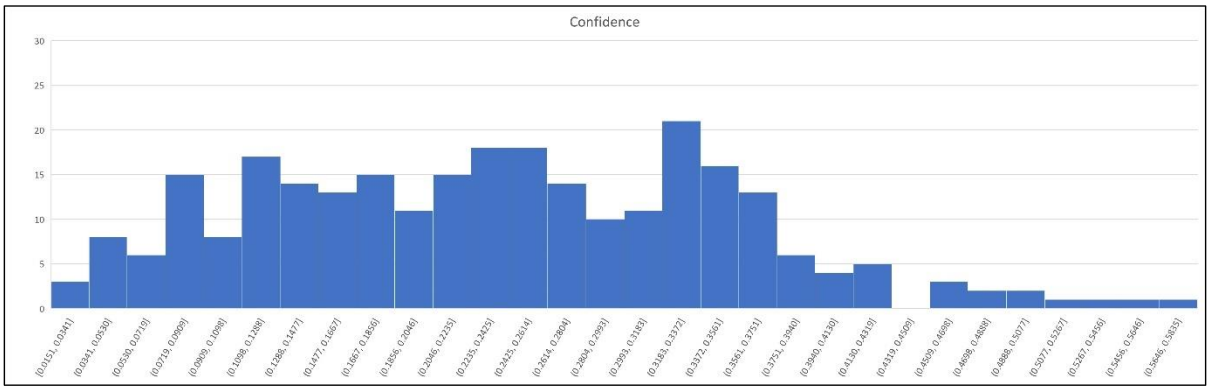


Figure 5-9 Distribution of Roma Taxi Confidence Values (10 minute stay)

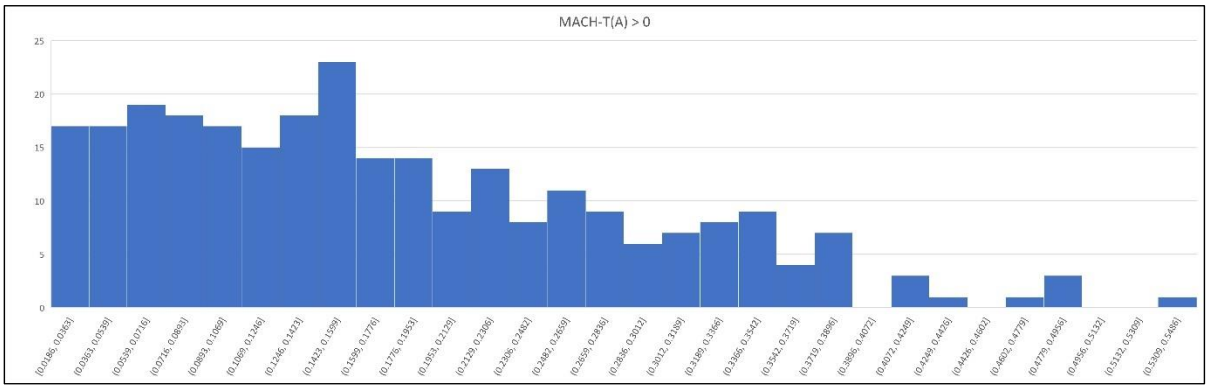


Figure 5-10 Distribution of Roma Taxi MACH-T(A) Values (10 minute stay)

5.5 Conclusions

Experimental results show GPS traces provide sufficient data to programmatically and incrementally calculate mobile device trust based on a device's most frequently visited locations.

The value at which a MANet operator would deem a subject “trusted” would depend on the MANet operator’s needs. The MACH-T algorithm provides a method to distinguish behavior of nodes based on their geographic location behavior patterns.

5.5.1 Supplementary Materials

The source code and results of our analysis are available online at https://github.com/CenterForSecureAndDependableSystems/MACH2K.

Chapter 6:
MACH-T: Trust Modeling and Analysis

6.0 Chapter Introduction

This chapter demonstrates an approach for modeling trust of mobile nodes by creating location behavior data for ten hypothetical personal mobile node subjects to represent ten different combinations of MACH-T(U) trust and Confidence (or density and volume of data).

This chapter provides the hypothetical node experiment description and results of modeling the effect of changing different aspects of location behavior expectations on the MACH-T(U), Confidence, and MACH-T(A) values. This experiment uses an Excel spreadsheet in place of the custom C++ software implementation to analyze the hypothetical node value.

This chapter provides the same contributions as Chapter 3 supporting Hypotheses 1 and 2:

Contribution 1: Create a novel method for measuring trust based on location behavior.

Contribution 2: Design, implement, and test an algorithm (MACH-T) and corresponding software implementation for measuring trust.

Hypothesis 1: Location behaviors in personal mobile devices can be quantified, measured, and used to assign trust.

Hypothesis 2: Location behaviors in vehicle-mounted mobile devices can be quantified, measured, and used to assign trust values.

The results of this experiment show mobile devices capable of recording GPS traces may be modeled, quantified, and measured to assign trust values.

6.1 Data Description

Table 6.1 shows ten different combinations of unadjusted trust (MACH-T(U) and Confidence values modeled in the Excel spreadsheet for each hypothetical node.

Table 6.1 Hypothetical Node Unadjusted Trust (MACH-T(U) and Confidence Approximations (One Day Data Volume)

Conformance to subjective trust parameters	**High Confidence**	**Medium Confidence**	**Low/No Confidence**
High Trust	**Node 1** MACH-T(U) ≈ 1.0 Confidence=1.0	**Node 2** MACH-T(U) ≈ 1.0 Confidence=0.5	**Node 3** MACH-T(U) ≈ 1.0 Confidence=0.25
Medium Trust	**Node 4** MACH-T(U) ≈ 0.5 Confidence=1.0	**Node 5** MACH-T(U) ≈ 0.5 Confidence=0.5	**Node 6** MACH-T(U) ≈ 0.5 Confidence=0.25
Low Trust	**Node 7** MACH-T(U) MACH-T(U) ≈ 0.25 Confidence=1.0	**Node 8** MACH-T(U) ≈ 0.25 Confidence=0.5	**Node 9** MACH-T(U) ≈ 0.25 Confidence=0.25
No Trust			**Node 10** MACH-T(U) = 0.0 Confidence = 0.0

Table 6.2 and **Table 6.3** show the various created behavioral values and resulting MACH-T(U), Confidence, and MACH-T(A) values. The ideal population behaviors of the nodes were arbitrarily chosen and can be adjusted to observe the resulting MACH-T(U), Confidence, and MACH-T(A) values. The Confidence value can be calculated with either one day of data volume required, or 30 days.

The blue shaded columns are the variable values input by the user and represent the expected behavior. The light green shaded columns are the calculated intermediate MACH-T formula terms, and the dark green shaded columns are the final MACH-T(U) and MACH-T(A) values. The yellow shaded columns contribute to and are the resulting Confidence values. The grey shaded columns are information only.

Table 6.2 Hypothetical Nodes' Input Values in Ascending Node Order

A	B	C	D	E	F	G	H	I	J	K	L	M	T
COLUMN LEGEND: **Yellow:** Calculated confidence values **Green:** Calculated trust values **Blue:** Data entry **Grey:** Informational	**First Date Time**	**Last Date Time**	**Poss. Days**	**Ideal % of Days with Traces**	**TD (:D*:E) /100**	**Ideal Qualified Hours per Total Days (TD)**	**Ideal Qualified Locations (QL)**	**TL (:H/:R)**	**TH (:L/:S)**	**Trace Hours per day (:J/:F)**	**QH (:G*:F)**	**QD (:L/:N)**	**Subject Node**
High Trust High Confidence	20140301 000000	20140401 235959	32	100	32	6	6	1500	768	24	192.0000	32.0000	**1**
High Trust Medium Confidence	20140301 000000	20140401 235959	32	50	16	6	6	1500	384	24	96.0000	16.0000	**2**
High Trust Low Confidence	20140301 000000	20140401 235959	32	25	8	6	6	1500	192	24	48.0000	8.0000	**3**
Medium Trust High Confidence	20140301 000000	20140401 235959	32	100	32	3	3	1500	768	24	96.0000	32.0000	**4**
Medium Trust Medium Confidence	20140301 000000	20140401 235959	32	50	16	3	3	1500	384	24	48.0000	16.0000	**5**
Medium Trust Low Confidence	20140301 000000	20140401 235959	32	25	8	3	3	1500	192	24	24.0000	8.0000	**6**
Low Trust High Confidence	20140301 000000	20140401 235959	32	100	32	1.5	1	1000	768	24	48.0000	32.0000	**7**
Low Trust Medium Confidence	20140301 000000	20140401 235959	32	50	16	1.5	1	1000	384	24	24.0000	16.0000	**8**
Low Trust Low Confidence	20140301 000000	20140401 235959	32	25	8	1.5	1	1000	192	24	12.0000	8.0000	**9**
No Trust No Confidence	20140301 000000	20140401 235959	32	0	0	0	0	0	0	0	0.0000	0.0000	**10**

Table 6.3 Hypothetical Nodes' Calculated Trust and Confidence Values in Ascending Node Order

A	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG
		MACH-T(U) Formula Terms							100% Traces per day=		100% Traces per day=			
									5760		5760			
COLUMN LEGEND: **Yellow:** Calculated confidence values **Green:** Calculated trust values **Blue:** Data entry **Grey:** Informational	Subject Node	Term 1 ((QH/QD) /AA)*.1666	Term 2 ((QL/QD) /AB)*.1666	Term 3 ((QD/TD) /AC)*.1666	Term 4 ((QL km^2 /QL perim km^2) /AD)*.1666	Term 5 ((QL/TL) /AE)*.1666	Term 6 ((QH/TH) /AF)*.1666	MACH-T(U)	CONFIDENCE AF/(AB*D) One Day Data Volume	MACH-T(A) One Day Volume	CONFIDENCE (AF/(AB*D))*TD/30 30 Days Data Volume (maxTD/30 = 1.0)	MACH-T(A) 30 Day Volume	Trace Cnt (15 seconds between traces)	Traces per Hour
		6.0000	2.0000	1.0000	0.0645	0.0040	0.2500							
High Trust High Confidence	1	0.1666	0.1666	0.1666	0.1666	0.1666	0.0833	0.9163	1.0000	0.9163	1.0000	0.9163	184320	240.0000
High Trust Medium Confidence	2	0.1666	0.1666	0.1666	0.1666	0.1666	0.0833	0.9163	0.5000	0.4582	0.2667	0.2443	92160	240.0000
High Trust Low Confidence	3	0.1666	0.1666	0.1666	0.1666	0.1666	0.0833	0.9163	0.2500	0.2291	0.0667	0.0611	46080	240.0000
Medium Trust High Confidence	4	0.0833	0.0833	0.0833	0.0833	0.0833	0.0417	0.4582	1.0000	0.4582	1.0000	0.4582	184320	240.0000
Medium Trust Medium Confidence	5	0.0833	0.0833	0.0833	0.0833	0.0833	0.0417	0.4582	0.5000	0.2291	0.2667	0.1222	92160	240.0000
Medium Trust Low Confidence	6	0.0833	0.0833	0.0833	0.0833	0.0833	0.0417	0.4582	0.2500	0.1145	0.0667	0.0305	46080	240.0000
Low Trust High Confidence	7	0.0417	0.0417	0.0417	0.0417	0.0417	0.0208	0.2291	1.0000	0.2291	1.0000	0.2291	184320	240.0000
Low Trust Medium Confidence	8	0.0417	0.0417	0.0417	0.0417	0.0417	0.0208	0.2291	0.5000	0.1145	0.2667	0.0611	92160	240.0000
Low Trust Low Confidence	9	0.0417	0.0417	0.0417	0.0417	0.0417	0.0208	0.2291	0.2500	0.0573	0.0667	0.0153	46080	240.0000
No Trust No Confidence	10	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0	0.0000

6.2 Data Analysis

When observing the final MACH-T(A) value resulting from the adjustment of the MACH-T(U) with the Confidence value when 30 days of data are desired, some lower trust MACH-T(U) values result in a higher MACH-T(A) when the Confidence is high. Node 4 had a higher MACH-T(A) value than nodes 2 and 3 and Node 7 had a higher MACH-T(A) value than nodes 3, 5, and 6. **Table 6.4** shows the same nodes sorted in descending MACH-T(A) order for the 30-day Confidence calculation, illustrating this point.

Another interesting item to note is the TD (Total Days) value is used both in calculating MACH-T(U) and in the Confidence calculation. Adjusting this value impacts both the QD/TD (percentage of Qualified Days to Total Days) and the density and volume of trace records calculation for Confidence.

Table 6.4 Hypothetical Nodes' Calculated Trust and Confidence Values (Descending 30 Day Data Volume MACH-T(A) order)

A	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG
		MACH-T(U) Formula Terms							100% Traces per day=		100% Traces per day=			
									5760		5760			
COLUMN LEGEND: **Yellow:** Calculated confidence values **Green:** Calculated trust values **Blue:** Data entry **Grey:** Informational	Subject Node	Term 1 ((QH/QD) /AA)*.1666	Term 2 ((QL/QD) /AB)*.1666	Term 3 ((QD/TD) /AC)*.1666	Term 4 ((QL km^2 /QL perim km^2) /AD)*.1666	Term 5 ((QL/TL) /AE)*.1666	Term 6 ((QH/TH) /AF)*.1666	MACH-T(U)	CONFIDENCE AF/(AB*D) One Day Data Volume	MACH-T(A) One Day Volume	CONFIDENCE (AF/(AB*D))*TD/30 30 Days Data Volume (maxTD/30 = 1.0)	MACH-T(A) 30 Day Volume	Trace Cnt (15 seconds between traces)	Traces per Hour
		6.0000	2.0000	1.0000	0.0645	0.0040	0.2500							
High Trust High Confidence	1	0.1666	0.1666	0.1666	0.1666	0.1666	0.0833	0.9163	1.0000	0.9163	1.0000	0.9163	184320	240.0000
Medium Trust High Confidence	4	0.0833	0.0833	0.0833	0.0833	0.0833	0.0417	0.4582	1.0000	0.4582	1.0000	0.4582	184320	240.0000
High Trust Medium Confidence	2	0.1666	0.1666	0.1666	0.1666	0.1666	0.0833	0.9163	0.5000	0.4582	0.2667	0.2443	92160	240.0000
Low Trust High Confidence	7	0.0417	0.0417	0.0417	0.0417	0.0417	0.0208	0.2291	1.0000	0.2291	1.0000	0.2291	184320	240.0000
Medium Trust Medium Confidence	5	0.0833	0.0833	0.0833	0.0833	0.0833	0.0417	0.4582	0.5000	0.2291	0.2667	0.1222	92160	240.0000
High Trust Low Confidence	3	0.1666	0.1666	0.1666	0.1666	0.1666	0.0833	0.9163	0.2500	0.2291	0.0667	0.0611	46080	240.0000
Low Trust Medium Confidence	8	0.0417	0.0417	0.0417	0.0417	0.0417	0.0208	0.2291	0.5000	0.1145	0.2667	0.0611	92160	240.0000
Medium Trust Low Confidence	6	0.0833	0.0833	0.0833	0.0833	0.0833	0.0417	0.4582	0.2500	0.1145	0.0667	0.0305	46080	240.0000
Low Trust Low Confidence	9	0.0417	0.0417	0.0417	0.0417	0.0417	0.0208	0.2291	0.2500	0.0573	0.0667	0.0153	46080	240.0000
No Trust No Confidence	10	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0	0.0000

6.3 Discussion

By using an Excel spreadsheet to create hypothetical nodes with varying degrees of location trace behavior, the spreadsheet user can quickly see how changing any aspect of node location behavior or desired location behavior changes the resulting MACH-T(U), Confidence, and MACH-T(A) values. The spreadsheet can uncover the subtle relationships between the various behavioral attributes when the user can change one value and see how it changes one or more of the MACH-T(U), Confidence, and MACH-T(A) values, sometimes unexpectedly. For example, a node qualifying in more locations would at first seem to be a more trusted node, but if the locations are geographically dispersed, causing the total perimeter area to increase beyond the desired total perimeter area , the resulting trust will be lower.

Chapter 7:
MACH-2K Architecture: Building Mobile Device Trust and Utility for Emergency Response Networks

7.0 Chapter Introduction

This chapter presents a published paper proposing an architecture for building and managing a mobile ad hoc network (MANet) of trusted nodes.

Researching and composing the paper cited below provided background for continued research into a solution for calculating and assigning trust values to MANet nodes.

K.H. Thurston, D. Conte de Leon. "MACH-2K Architecture: Building Mobile Device Trust and Utility for Emergency Response Networks." Proceedings of the 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW), Monterey, CA, USA, November, 2019, IEEE, DOI: 10.1109/MASSW.2019.00004

7.0.1 Abstract

In this article, we introduce the MACH-2K trust overlay network and its architecture. MACH-2K's objectives are to (a) enhance the resiliency of emergency response and public service networks and (b) help build such networks in places, or at times, where network infrastructure is limited. Resiliency may be enhanced in an economic manner by building new adhoc networks of private mobile devices and joining these to public service networks at specific trusted points. The major barrier to building resiliency by using private devices is ensuring security. MACH-2K uses device location and communication utility patterns to assign trust to devices, after owner approval. After trust is established, message confidentiality, privacy, and integrity may be implemented by well-known cryptographic means. MACH-2K devices may be then requested to forward or consume different types of messages depending on their current level of trust and utility.

7.1 Introduction

7.1.1 The Problem

Building and maintaining dedicated and resilient emergency response and public service networks is expensive. Using shared networks is a common approach to reduce costs.

However, ensuring adequate emergency communications in cases of widespread emergencies or dependent system outages while using shared networks is a major unsolved challenge. Hence, the problem we focus on, in this article, is how to provide adequate emergency and public service communications using networks of trusted nodes in a manner that is resilient to major emergencies or outages and also efficient and cost-effective.

7.1.2 Proposed Solution

With the ubiquitous and world-wide availability of smartphones and other mobile devices with wireless communication capability, we see a cost-effective and untapped opportunity to create mobile ad hoc networks to support or enhance emergency response and public service communication networks. Such hybrid networks may also enable additional public service use cases beyond emergency communications for emergency response personnel. They may also enable direct communication with the public. However, one of the major problems with building such ad hoc networks is the problem of security and privacy of the communications which comes from the lack of trust in each device. This novel Trust Overlay Network named MACH-2K, we use 2K as an alternative name for TON, relies on the history of mobile node location, movement patterns, timing, and communication performance to calculate and assign trust and utility values for individual devices. Such trust and utility are intended to fully enable: (1) Emergency mobile communications for first responders; (2) Emergency public broadcasts when other networks are unavailable or degraded; (3) Backup communication when primary networks are at capacity such as in crowded public areas; (4) More reliable communication within under-served geographies such as rural or remote areas or countries without adequate mobile network infrastructure; (5) Distributed fog network gateways for gathering data from, and providing over the air updates to distributed sensors.

7.1.3 Contribution

The contribution described in this article is the architecture of MACH-2K. The MACH-2K system provides the means for calculating trust based on patterns of location occurrence and communication utility of private devices. These trust ratings would allow public organizations to build and manage a hybrid network that may offer a high level of resiliency in a cost effective manner. Such a hybrid network (partly fixed, partly ad hoc) may be used to

provide emergency response and public service communications in a resilient and cost-effective manner.

7.1.4 Outline of this Article

The remainder of this paper is organized as follows: Section 7.2 introduces related terminology. Section 7.3 describes the system entities of the MACH-2K architecture. Section 7.4 describes the MACH-2K mode of operation. Section 7.5 describes the MACH-2K services. Section 7.6 describes the MACH- 2K message types. Section 7.7 describes related research and applications. Section 7.8 introduces plans for furthering this work. Acknowledgements and a complete list of References follow.

7.2 Background

Today, many emergency response communication systems rely on trusted and dedicated private radio towers and public communication infrastructure. Cellular network infrastructure is also used for emergency response. In the event of widespread emergencies or disasters, dedicated emergency response communication infrastructure and wide-area sections

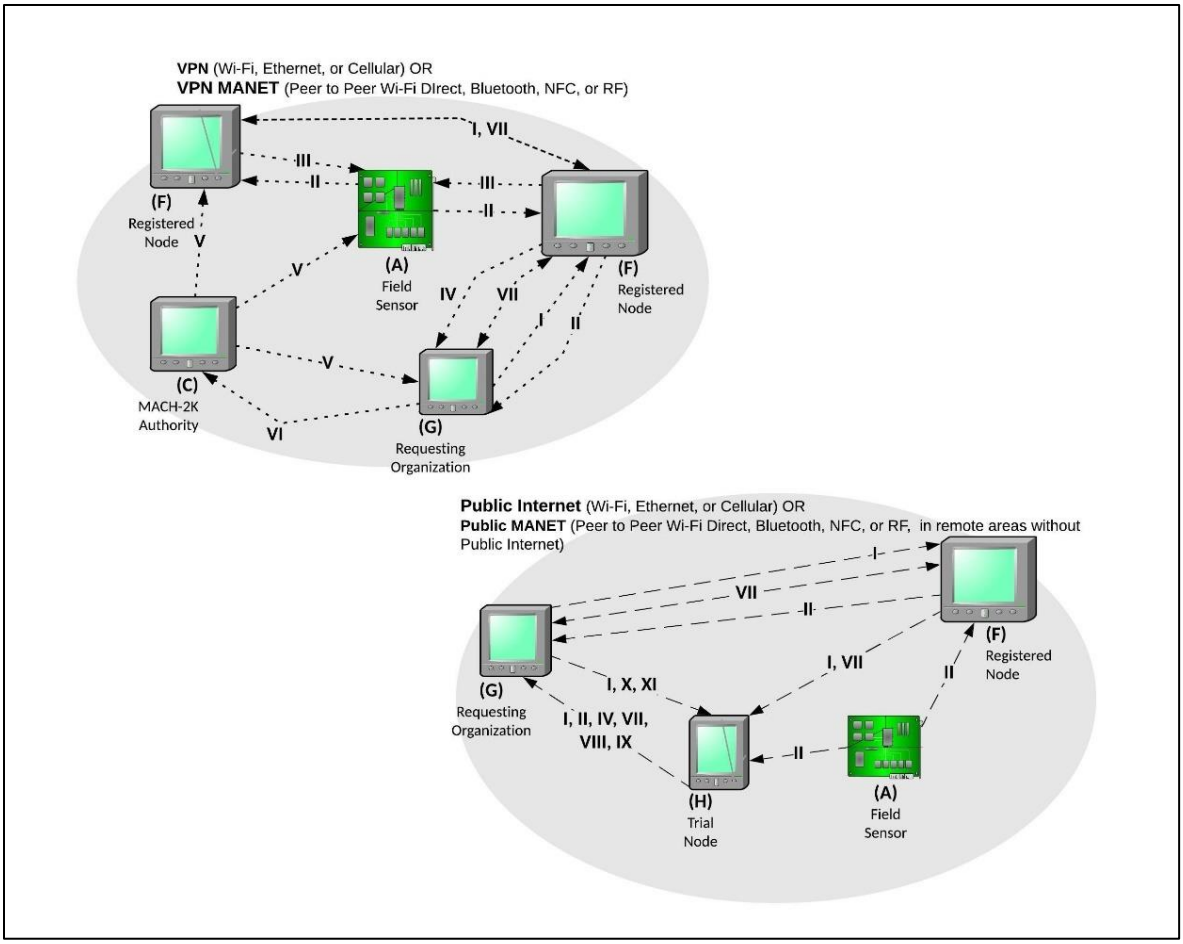


Figure 7-1 MACH-2K System Architecture Diagram

of the cellular network may quickly become unavailable or heavily congested. In some scenarios, limited numbers of portable radios provide backup systems. However, these systems require specialized equipment and trained personnel to operate and provide limited resumption of communications. Such reduced or removed communication capabilities may result in inadequate or delayed emergency response. We argue that mobile ad hoc networks may be configured and managed and need not be purely ad hoc or opportunistic. As long as patterns of geographic and time appearance and message forwarding reliability can be inferred and a trust value assigned, based on such patterns, then nodes may be trusted to be members of a reliable hybrid network. In this case, network nodes might be smart phones, tablets or other computers with wireless communication capabilities such as micro-controller units found on field sensors. Although mobile ad hoc networks are by their nature dynamic structures, they do not require anonymity or spontaneity and need not be self-configuring. Requiring a trial period of node observation in order to gather the unique movement and communication history

of a node would allow for calculating trust. Given the ability to apply behavioral analysis to nodes prior to granting them access to the network, the behavior of a node during a trial period can be analyzed to determine if the behavior profile fits closely enough to a predefined ideal profile of time in a geographic location, and the ability to correctly receive, process, and respond to network messages in a timely manner. Similarly to how people develop trusted relationships over time, nodes would develop trust as their behavior became known to an organization building a MANet using MACH- 2K. Most current access control systems rely on a binary definition of trust.

7.3 MACH-2K System Entities

Figure 7-1 shows the interactions of the system entities with network messages and system management data in the network environments included in the MACH-2K architecture. Below we describe each of the entities.

A. Field Sensor: A node providing environmental data to or receiving control data from other nodes, including over the air updates to its executable software.

B. Field Sensor Owner: The owner of a Field Node, can be the same as the Requesting Organization.

C. MACH-2K Authority: Issues certificates for Registered Nodes.

D. Message Creators: Alias for the various entities allowed to create messages.

E. Node Owner: The owner of either a Trial Node or a Registered Node.

F. Registered Node: Nodes achieving the required MACH- 2K rating as defined by the Requesting Organization using the network in a specific geographic area.

G. Requesting Organization: The organization requesting network participants determines the desired geography, density, the number of mobile and stationary field sensor nodes, and the required timeliness and accuracy of messages. The Requesting Organization is the owner of at least one Registered Node.

H. Trial Node: Nodes requesting registration. The Trial Node Location Zone History is tracked for a trial period after which it is compared to Requesting Organization Location Zone requirements to determine if it is similar enough to be included as a Registered Node.

The Trial Node communication history determines if its message integrity meets requirements. Trial Nodes are not permitted to send messages to Registered Nodes, but at the end of the trial period in a public Internet or public MANet, their message history is compared against message history maintained at the Requesting Organization and if the message history achieves the threshold of required messages correctly received, the Trial Node receives a MACH-2K rating and certificate and is upgraded to a Registered Node.

7.4 MACH-2K Operation

The MACH-2K architecture calculates the MACH-2K trust rating of nodes requesting to join the network as registered nodes. A trial period for each node establishes the pattern of individual node travel through various locations and assesses various factors including the messages logged by the node during the trial phase. This could be accomplished by a mobile application installed on the trial node. The MACH-2K network architecture uses a VPN for node to node and field sensor to node communication enabled by WiFi, Ethernet, or cellular Internet connectivity if available, or WiFi direct, Bluetooth, or radio frequency MANet if not. The trial process will use a software application implemented for web and mobile platforms. The MANet communication will require a secure mobile application which can be updated via the Internet or MANet VPN. Updates to the mobile application will include revisions to MACH Trust certificates and other security data in addition to other software enhancements.

The MACH-2K architecture switches mobile nodes from Cellular or WiFi to MANet peer-to-peer as node densities and proximities support MANet communications, and when other options are not available. The system will compile history of the location and timing of MANet communication to inform of the viability of MANet communications in any given geographic area or location zone.

7.5 MACH-2K Services

7.5.1 Mobile Node Services

The MACH-2K Mobile application software will implement the following services:

1. Create Message: Requesting Organizations, Node Owners, and Field Sensors may create Broadcast, Node to Node, Field Sensor Environmental Data, or Field Sensor Over the Air Update messages.

2. Decrypt Message: A node will use its private key to decrypt a message.

3. Encrypt Message: A node will use a public key to encrypt a message to another node, and its private key to sign a message.

4. Query MACH Certificate: The MACH certificate will include MACH ratings of registered nodes. The certificate will provide a level of trust in node to node communication. The MACH-2K Authority will share certificate information widely to eliminate the risk of a single point of failure of the authority node.

5. Query MACH Value: The MACH value is a component of the MACH certificate issued to a registered node.

6. Update Locations Visited: The mobile app will use geotags and timestamps for start and end times to update node location history.

7. Collect Sensor Data: Registered nodes will collect sensor data at various locations.

7.5.2 Management Services

The MACH-2K management application software will implement the following services:

1. Create MACH-2K Certificate: The MACH-2K Authority will use node trial period history and registered node history to create and update the MACH-2K Certificate.

2. Create Message: Requesting Organizations, Node Owners, and Field Sensor Owners may create Broadcast, Node to Node, Field Sensor Environmental Data, or Field Sensor Over the Air Update messages.

3. Issue MACH-2K Certificate to Registered Node: The MACH-2K Authority will be the sole issuer of MACH- 2K certificates but will share the certificate data to all registered nodes to avoid spoofing.

4. Log Node Communication: Save node communication history.

5. Log Node Location: Save node location history.

6. Manage Location Zone: Requesting Organizations designate standard location areas such as postal ZIP codes, smaller areas such as postal Carrier Routes, major streets or highways, or public locations such as schools or commercial locations.

7. Register Trial Node: Nodes initially register for a trial period prior to becoming registered nodes.

8. Set required MACH-2K value for Registered Nodes: Each Requesting Organization determines the qualifying MACH-2K values for registered nodes.

9. Update MACH-2K Value: MACH-2K values can change over time and the system will update when required.

10. Upgrade Trial Nodes to Registered Nodes: At the conclusion of a trial period, nodes may be upgraded to registered nodes if they qualify.

11. View Current and Historic Node Information: Node Owners and Requesting Organizations will be able to view node location and message history.

12. View Field Sensor data: Field Sensor Owners will be able to view Field Sensor data.

13. View Node Coverage Map: Requesting Organizations will be able to view node coverage for given Location Zones.

14. View Node MACH-2K Values: The MACH-2K Authority and Requesting Organizations will view MACH-2K values for multiple nodes at a summary or detail levels, and Node Owners will be able to view node detail for their node.

15. Verify Trial Node Field Sensor Data: The trial period required for nodes will include verification of data collected by trial nodes from field sensors.

7.6 MACH-2K Message Types

I. Broadcast: A message defined by the Requesting Organization to be sent to all registered and trial nodes. Such messages are information only, and not to be used for updating

Field Sensor control software. The message may be relayed by any registered node to any other registered or trial node and only relayed from a trial node back to the requesting organization.

II. Field Sensor Environmental Data: Environmental data sent to Trial Nodes and Registered Nodes from field sensors.

III. Field Sensor Over the Air (OTA) Update: Updates to Field Sensor software sent by Requesting Organization to Registered Nodes to deliver to Field Sensors.

IV. Location Zone Data: Geographic areas defined by the Requesting Organization to be used to determine if a Trial Node qualifies to be a Registered Node. Also used to periodically recalculate and update MACH2K trust ratings of nodes.

V. MACH-2K Certificate: Certificate containing unique identity and MACH-2K ratings for registered nodes and Field Sensors.

VI. MACH-2K Values: Values from node location history, travel, timing, and communication history from node logs, for creating MACH-2K certificates.

VII. Node to Node: A message category describing communication between any two nodes. The message may originate from a Registered Node or a Field Sensor but not a Trial Node. In addition to a unique communication between only two nodes, a Node to Node Message can be a relayed Broadcast message, a Field Sensor Environmental Data message, or a Field Sensor Over the Air (OTA) Update message.

VIII. Account Data: Each node in the system provides identifying data upon registering as a trial node or as a requesting organization. Account data could also include billing or compensation details.

IX. Registration Request: The Trial Node registration process creates a message to a Requesting Organization.

X. Registration confirmation: The Requesting Organization confirms the Trial Node Registration Request.

XI. Trial Node Upgrade: At the conclusion of the Trial Node trial period, the Requesting Organization sends a message to the Trial Node to notify of the upgrade to a Registered Node or to advise the upgrade was denied.

7.7 Related Work

Research on trust in mobile peer-to-peer and ad hoc networks is an emerging topic. The literature covering peer-to- peer and ad hoc networks first focused on the enabling technology. Later on it focused on efficiencies and optimizing approaches. Then, within the last few years, there has been some focus on trust and security. However, the latter with a primary focus on anonymous or opportunistic mobile, peer-to-peer, or purely ad hoc networks. Such focus fails to acknowledge the fact that most mobile devices follow the usage and location patterns of their owners and that such patterns, combined with communication utility measures, may be used to build trust over time. Such trust may then be used to establish secure and managed networks as an overlay over hybrid (ad hoc and infrastructure) networks. We did not find in the literature, even after an extensive literature search and review, descriptions of approaches for planning and management of ad hoc networks for public service use. Such planning and management would be a requirement to enable use of such networks for emergency response and public service in a reliable and resilient manner. In addition, authentication and security are dependent on trust. We describe in this section work that is related and likely complementary of the MACH-2K approach.

7.7.1 Security and Trust in Mobile Ad Hoc Networks

Strayer et al. [47] proposed a radio-integrated content sharing networking paradigm which provides security. It also includes content request history to determine content utility which is similar to the MACH-2K concept of node utility based on movement and communication history. Vasudeva and Sood [48] surveyed methods for protecting ad hoc networks against Sybil attacks. Talasila, Curtmola, and Borcea [49] proposed collaborative Bluetooth-based location authentication on smart phones. Coon [50] modeled trust in random wireless networks and explored the idea of node relative locations and interaction history, particularly in 5G networks where peer-to-peer file sharing is a practical possibility. Several authors used social ties of node owners to assign trust in anonymous networks [51], [52], [53] and [54]. Guo, Chen, and Tsai [3] provided a comprehensive survey of trust computation

methods for service management in IoT systems. Other authors [53], [54], [55], [56], and [57] also investigated trust. By contrast with these previous works, the MACH-2K architecture focuses on building trust based on location history and utility with the purpose of enhancing the reach and resiliency of emergency response or public service networks in a cost-effective manner.

7.7.2 Emergency and Disaster Response

Several authors have investigated approaches to mobile network configuration and management for emergency operations. For example, Kuada and Bannerman [58], DiFelice, Bedogni, and Bononi [59], Lakshmi and Ibe [60], Krug, Schellenberg, and Seit [61], Kanchanasut et al. [62], and Aschenbruck et al. [63]. However, these works do not appear to consider security and trust as an integral part of the network design, planning, and operation.

7.7.3 Peer-to-Peer Protocols and Applications

Ciobanu et al. [64] and Casetti et al. [65] identify WiFi, WiFi Direct, and Bluetooth as the best commercial and readily available layer two wireless protocols for peer-to-peer wireless networks. For vehicular networks, 802.11p, physical layer for Dedicated Short Range Communication (DSRC) and Qualcomm's LTE-V2X, also known as C-V2X or PC5, are the usual options but neither is currently ubiquitous [66], [67], [68], [69], [70], and [71]. LTE-V2X may see faster adoption rates due to the ubiquity of cellular infrastructure. Masini et al. [66] state in reference to LTE-V2X: "for the first time in history, a cellular system allows direct communication between peers". GoTenna is a commercial enterprise marketing a 2-watt a Multi-Use Radio Service (MURS) radio and antenna that pairs with a smart phone using Bluetooth. It achieves greater communication range than is possible with the smart phone alone. The company sells the MURS version of its platform to consumers to use in forming ad hoc mesh networks when out of range of cellular infrastructure. GoTenna recently released a professional vRange version it sells primarily to military, first responder, and emergency operations organizations. The ProX product uses VHF (142-175MHz) and UHF (445-480MHz) radio frequencies broadcasting from 0.5W up to 5W of power. Range is up to 4 miles on the ground and up to 69 miles if the antenna is elevated above any ground obstacles. A mobile app provides end to end encryption of messages but assumes all nodes are known ahead of joining the group and the application does not manage access to the app other than

authenticating the user with a user name and password. The app also has a mapping feature which shows the location of all GoTenna nodes active on the network. Several consumer mobile applications have attempted to deploy mobile peer-to-peer communications with various degrees of success. FireChat, available for Android in the Google Play Store, may be used by groups of people to communicate without using the cellular network. Bluetooth Chat, also available for Android has high ratings but it only uses Bluetooth which works at very short ranges of a few meters. For sensor to mobile device communication, though, Bluetooth relaying of data could be proven useful. These applications do not provide mechanisms for evaluating the trust or utility of nodes in the network. By contrast, the latter are key features of the MACH- 2K architecture.

7.7.4 Distributed Processing

Le [72] proposed approaches for efficiently sharing compute loads among mobile peers. Teng et al. [73] and Shah et al. [74] proposed using mobile nodes in vehicles to distribute over the air updates to smart city devices or collect sensor data from sparse and widely distributed devices. Kim, et al. [75] described an approach for how to maintain node densities using positioning algorithms for minimal power consumption. These distributed processing architectures could benefit from the MACH-2K trust and utility features.

7.7.5 Other Uses of Location Data

VANET (Vehicular Ad hoc NETwork) research has focused on predictable node locations such as on roadways but other predictable locations are proposed to be equally likely for MANet nodes such as schools, businesses, churches, event venues, and other public gathering places where node owners may already be known to each other and have a level of trust through social ties [66]. Zumigo Corp. is an example of a commercial data broker of consumer location data. Zumigo has purchased consumer location data from cellular providers and used the data successfully to reduce credit card and other fraud [76] . Marin, Dobre, and Xhafa [77] tracked a group of volunteers over three months working in an academic setting and collected location and interaction data over the period. Marin, Dobre, and Xhafa concluded that there are clear patterns of node mobility and communication emerged from their analysis. Other authors also explored location and social factors when determining routing in mobile ad hoc networks [51], [52], and [78].

7.8 Future Work

The next step in this research project will be to implement the MACH-2K architecture in a prototype system. First, within a simulated environment and, on a later stage, potentially using volunteers as a source of mobility and communication history data within specific geographies.

Acknowledgments

We would like to thank the State of Idaho for partially funding this research work. Also thanks to the University of Idaho's personnel that ensures our research infrastructure and support services are available on a day-to-day basis. We would also like to thank the program committee and chairs and the reviewers for their help improving this paper. The opinions expressed in this paper are not those of the State of Idaho.

Chapter 8:
Survey of IoT Fog Computing Near Healthcare IoT Edge Devices—Another Use Case for MANets

8.0 Chapter Introduction

This chapter presents a published paper surveying and discussing the advantages and disadvantages of a fog computing layer in proximity of IoT network edge devices for processing healthcare information. The importance of geographic location and real-time response requirements are similar to the requirements for MANets. The NIST Fog Computing Conceptual model (NIST 500-325) [79] lists six essential characteristics of fog computing, of which the first five are also essential to MANets, and the sixth, "scalability and agility" improves the quality. The two additional features listed below and the additional five attributes all apply equally to MANets.

(1) Contextual location awareness and low latency,

(2) Geographical Distribution,

(3) Heterogeneity,

(4) Interoperability and Federation,

(5) Real-time interactions,

(6) Scalability and agility of federated fog-node clusters.

Two additional features are often associated with fog [79]:

(1) Predominance of wireless access,

(2) Support for mobility.

In addition, according to NIST 500-325 [79], fog nodes need to support one or more of the following attributes:

(1) Autonomy,

(2) Heterogeneity,

(3) Hierarchical clustering,

(4) Manageability,

(5) Programmability.

Given the similarity between fog and MANets, issues of trust in MANets also apply to fog. One paper on fog-based MANets provided a background discussion of trust research, but itself focused on a novel routing protocol to conserve energy, and a security measure to generate anonymous identification for message source nodes [80]. None of the background research cited addressed the geographic location behavior of nodes prior to joining the MANet.

Additionally, a 2018 industry survey identified insufficient authentication/ authorization of IoT devices as one of the top ten IoT vulnerabilities [81].

Researching and composing the paper cited below provided background for continued research into a solution for calculating and assigning trust values to MANet nodes.

K. Thurston and D. C. de Leon, "The healthcare IoT Ecosystem: Advantages of Fog Computing Near the Edge," in 2018 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE). IEEE, 2018, pp. 51–56.

8.01 Abstract

Abstract— The IoT (Internet of Things) provides numerous opportunities for the connected healthcare industry, especially in the distributed cloud environment known as fog which resides in a middle architectural layer adjacent to edge devices. This tutorial provides an overview of recent research and industry advances focusing on connected health technologies: fog concepts and architectures; development and lifecycle frameworks; security vulnerabilities, threats and best practices; and connected medical device regulations.

8.02 KEYWORDS

IoT, connected health, fog computing, edge computing, gateways, service-oriented architecture, middleware, cloud operating systems, secure software engineering, secure systems development

8.1 Introduction

Multiple industries are building systems of networked physical devices commonly known as the Internet of Things (IoT) or the Industrial Internet of Things (IIoT). The term 'IoT' was first used by Kevin Ashton in 1999 in a presentation to Proctor and Gamble executives. Since then, hardware and software IoT solutions, both proprietary and open source have been deployed in a wide range of industries for numerous purposes. Agriculture, architecture and construction, automotive, consumer electronics, education, energy, fitness, health care, manufacturing, public safety, recreation, retail, smart cities, smart homes, telecommunications, transportation, utilities and wearables are some examples.

David King, in an interview for Automation World in August, 2016 provides context for the fog computing aspect of IoT: "…Cisco created the term fog computing years ago to describe a layer of computing at the edge of the network that could allow pre-processed data to be quickly and securely transported to the cloud" [82].

Researchers Chiang, et al. [83] identify research opportunities related to fog: "Filling the technology gaps in supporting IoT will require a new architecture—fog—that distributes computing, control, storage, and networking functions closer to end user devices."

Fog computing has many advantages, including reduced latency, local control and the resulting increased security, reliability, fault tolerance, lower data transfer and storage costs, extensibility, distributed computing, heterogeneity management, and support for hardware/software maintenance [84].

Unfortunately, fragmented or non-existent standards efforts have created silos of proprietary systems, resulting in a heterogeneous environment that is difficult to secure. In fact, IoT system security has not been a priority due to lack of any requirements to comply with any existing security standard other than standards that may already exist for individual system hardware or software components.

Because the healthcare industry must protect human life as well as personal privacy, system confidentiality, integrity and availability, security is a top requirement. Section 8.2 reviews recent healthcare IoT fog research and case studies with a summary of the security and privacy risks addressed or acknowledged in each. Section 8.3 includes a summary of fog

conceptual models and reference architectures and components and introduces the NIST Fog Computing Conceptual Model [79] and the OpenFog Consortium reference architecture (an IEEE draft standard) [85]. Section 8.4 discusses security vulnerabilities. Section 8.5 reviews the FDA medical device safety evaluation plan [86] of which the National Evaluation System for health Technology (NEST), is a part and Section 8.6 concludes the paper with a summary of the security concerns and open research questions for healthcare fog computing environments.

8.1.1 Approach and Methodology

The goal of this tutorial is to introduce fog computing for the healthcare IoT ecosystem. The search of the literature using 'healthcare fog' as the search term at lib.uidaho.edu which searches multiple literature databases yielded a variety of papers referenced in Section II.

In addition to research papers, industry sources including white papers, web sites, podcasts and product literature provided substantial background information for this tutorial.

8.2 Healthcare IoT Fog Research and Case Studies

Healthcare applications span a wide range of functions, from intensive care to health monitoring of healthy individuals for preventive health and public health purposes.

Stakeholders for healthcare IoT include patients and their families, healthcare professionals, provider organization staff and management, insurance payers, and regulatory agencies such as the United States Food and Drug Administration (FDA).

Connected healthcare applications must be highly secure in a hospital or clinical setting but may have lower levels of security if they are for informational purposes for personal fitness tracking, for example.

Steele and Clarke [87] propose an IoT public health information system. Although their research does not identify a fog layer as such, their proposed architecture includes local processing on a mobile device connected to sensors which meets the definition of a fog layer. Mobile devices communicate with an anonymizing network layer. The researchers address privacy concerns with anonymous networks such as MIX and Onion routing.

Ni et al. [88], Al-Shaqi [89], and Frontoni [90] address IoT systems in three separate papers for independent living of older adults. Although mobile phones are discussed as data collection devices, fog architectural layers are not explicitly noted. Privacy and security concerns are addressed in one paper by proposing less revealing binary sensors in place of cameras and microphones. User managed access is another suggested solution to privacy concerns.

Akrivopoulos [84] discusses using Bluetooth Low Energy (BLE) to communicate with a patient's smart phone acting as a fog gateway providing proxies for security updates, encryption or deep packet inspection and threat detection.

Sood and Mahajan [91] propose an IoT fog-based healthcare framework for disease tracking.

Verma and Sood [92] present a fog assisted IoT enabled disease diagnosis framework.

Rahmani, et al. [93] have built a smart eHealth gateway to demonstrate the power of fog computing.

The OpenFog Consortium [94] presents several case studies including one for patient monitoring in a fog based IoT environment.

8.3 IoT Fog Conceptual Models and Reference Architectures

The fog layer in IoT architectures is a distributed, sometimes ad hoc and frequently mobile network cloud of devices acting as intelligent gateways for physical devices. This layer provides many advantages, including reduced latency; local control; increased security, reliability, and fault tolerance; lower data transfer and storage costs; extensibility; distributed computing; heterogeneity management; and support for hardware and software maintenance [84].

A simple architecture diagram in **Figure 8-1** with three layers represents a typical IoT architecture: Physical layer, middle layer, and cloud or enterprise layer. The physical layer consists of sensor and/or actuators, the middle layer includes simple data aggregation and basic compute and transport functions, while the cloud or enterprise layer can perform the most

sophisticated analysis. This model does not identify a fog layer with more sophisticated features.

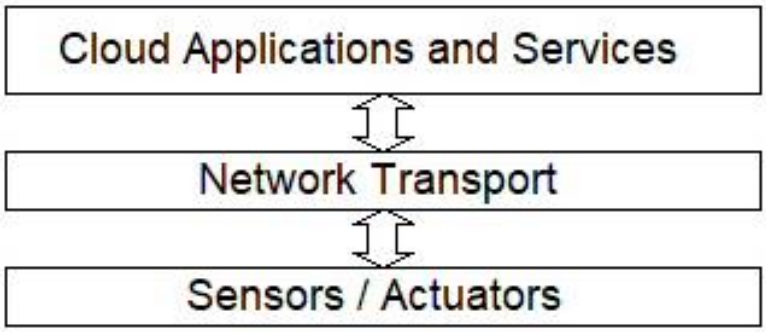


Figure 8-1 IoT Architecture without a Fog Layer and All Applications in the Cloud

Modifying the diagram to show fog layer features is shown in **Figure 8-2**.

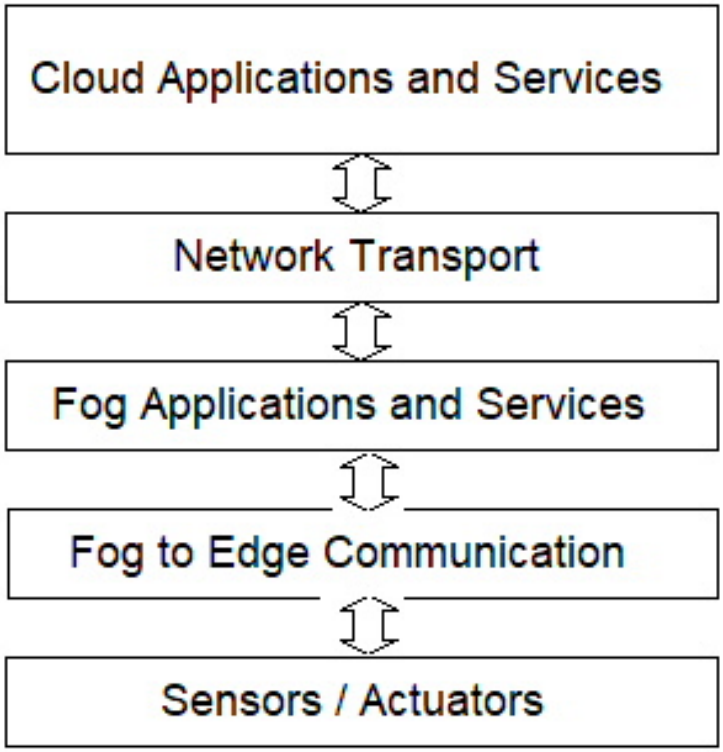


Figure 8-2 IoT Architecture Showing the Fog Layer with Applications and Services

8.3.1 Fog Conceptual Model

NIST special publication 500-325 describes a conceptual model of fog computing.

From the publication abstract:

Managing the data generated by Internet of Things (IoT) sensors and actuators is one of the biggest challenges faced when deploying an IoT system. Traditional cloud-based IoT systems are challenged by the large scale, heterogeneity, and high latency witnessed in some cloud ecosystems. One solution is to decentralize applications, management, and data analytics into the network itself using a distributed and federated compute model. This approach has become known as fog computing. This document presents the conceptual model of fog and mist computing and how they relate to cloud-based computing models for IoT. This document further characterizes important properties and aspects of fog computing, including service models, deployment strategies, and provides a baseline of what fog computing is, and how it may be used [79].

The NIST publication lists six essential characteristics of fog computing:

1.Contextual location awareness, and low latency
2. Geographical Distribution
3. Heterogeneity
4. Interoperability and Federation
5. Real-time interactions
6. Scalability and agility of federated, fog-node clusters.

Two additional features are often associated with fog:

Predominance of wireless access

Support for mobility

In addition, fog nodes need to support one or more of the following attributes:

Autonomy
Heterogeneity
Hierarchical clustering
Manageability
Programmability

NIST describes fog deployment models as paralleling traditional cloud deployment models which include Private, Community, Public, and Hybrid.

NIST also addresses the differences between fog and edge computing:

Fog is multi-layered and decouples and meshes hardware and software functions whereas edge computing executes specific applications in a fixed location.

Fog is hierarchical, but edge is limited to small numbers of peripheral devices. The peripheral edge is also referred to as the IoT network.

8.3.2 Fog Computing Reference Architecture

The OpenFog Consortium says this about fog architectures:

> *Fog architectures selectively move compute, storage, communication, control, and decision making closer to the network edge where data is being generated in order solve the limitations in current infrastructure to enable mission-critical, data-dense use cases.*

They consider their reference architecture document to be

> *the baseline to developing an open architecture fog computing environment. It is the first step in creating standards to enable interoperability in IoT, 5G, Artificial Intelligence, Tactile Internet, Virtual Reality and other complex data and network intensive applications* [94].

The key benefits they cite are:

Containerization
Virtualization
Orchestration
Manageability
Efficiency

Their key architectural pillars are:

Security
Scalability

Openness
Autonomy
RAS(Reliability, Availability, Serviceability)
Agility
Hierarchy
Programmability

They also stress as does the NIST group, that fog computing is different from edge computing:

Fog works with the cloud, but the edge excludes the cloud.

Fog is hierarchical, while the edge is limited to a few layers at most.

8.3.3 Sensors, Actuators, and Edge Devices

Most IoT edge nodes consist of sensors and maybe actuators, an embedded processor microcontroller with or without an operating system, a connectivity module and an energy source [95].

For personal health devices (PHDs), sensing devices need to consider human comfort and compatibility with activities of daily life. Low power requirements and long battery life are also desirable.

Connectivity that relies on proprietary readers can be expensive at scale. Antennas featuring Bluetooth Low Energy (BLE) or very low cost Near Field Communication (NFC) can be connected with fog nodes such as a smart phone or dedicated gateway processor performing user authentication, data collection and aggregation, analysis, and communication with a centralized cloud when necessary.

The Eclipse IoT Working Group, AGILE IoT, IEEE, and the Open Mobile Alliance co-sponsored an online survey between January 24 and March 5 of 2018 of 502 IoT developers [96].

Although the survey title indicates only developers were surveyed, the actual breakdown of job titles is as follows:

Developer: 30%

Architect: 16%

Development Manager: 12%

Researcher: 10%

Independent Consultant:8%

Other: 7%

Executive: 6%

Product Manager: 5%

Student: 4%

Role in sales and/or business development: 1%

Not currently employed: 1%

Testing: 1%

Survey results for the top processor hardware are mostly ARM and Intel processors. Unfortunately, 28% of those surveyed did not know the hardware platform, which can be explained by the wide range of job titles surveyed.

Don't know: 28%

Arm Cortex-M3 / Arm Cortex-M4: 26

Other 32-bit MCU: 24%

Arm Cortex-M0 / Arm Cortex-M0+: 21%

Arm cortex-M7: 20%

16-bit MCU: 19%

8-bit MCU: 18%

Survey results of the top operating systems for the IoT are:

Linux, over 71%, and Windows, FreeRTOS (now owned by Amazon AWS), and No OS/bare metal each have about 20% share.

Most respondents use more than one OS accounting for responses totaling more than 100%.

The same survey surveyed usage of the various messaging/networking protocols (multiple responses account for the total above 100%):

MQTT: 63%

HTTP: 54%

Websockets: 35%

HTTP/2: 25%

COAP: 22%

AMQP: 18%

The most commonly used network/connectivity protocols are:

TCP/IP: 63%

Wi-Fi: 53%

Ethernet: 48%

Bluetooth/Bluetooth Smart: 38%

Cellular: 36%

UDP/IP: 32%

Zigbee: 22%

LPWA: 21%

Serial RS-232/RS-485: 18%

8.3.4 Fog Devices

Fog devices, known as nodes, provide CPU power, memory, and data storage sufficient to perform data analysis and other functions too resource intensive for IoT edge devices in order to improve response time and save on bandwidth, processing, and storage in the cloud. They are small compute devices such as mobile phones, tablets, laptops, and network gateways. The fact that mobile devices are already ubiquitous in the environment presents the capability for massive sensor data collection, analysis, and even control without the need for massive hardware and telecommunications deployments. Software will enable this vision.

Fog devices, with their more ample resources, will also provide mitigation of security vulnerabilities.

Figure 8-3 shows fog devices as part of the overall telecommunications infrastructure (diagram created for conference presentation, was not part of original paper).

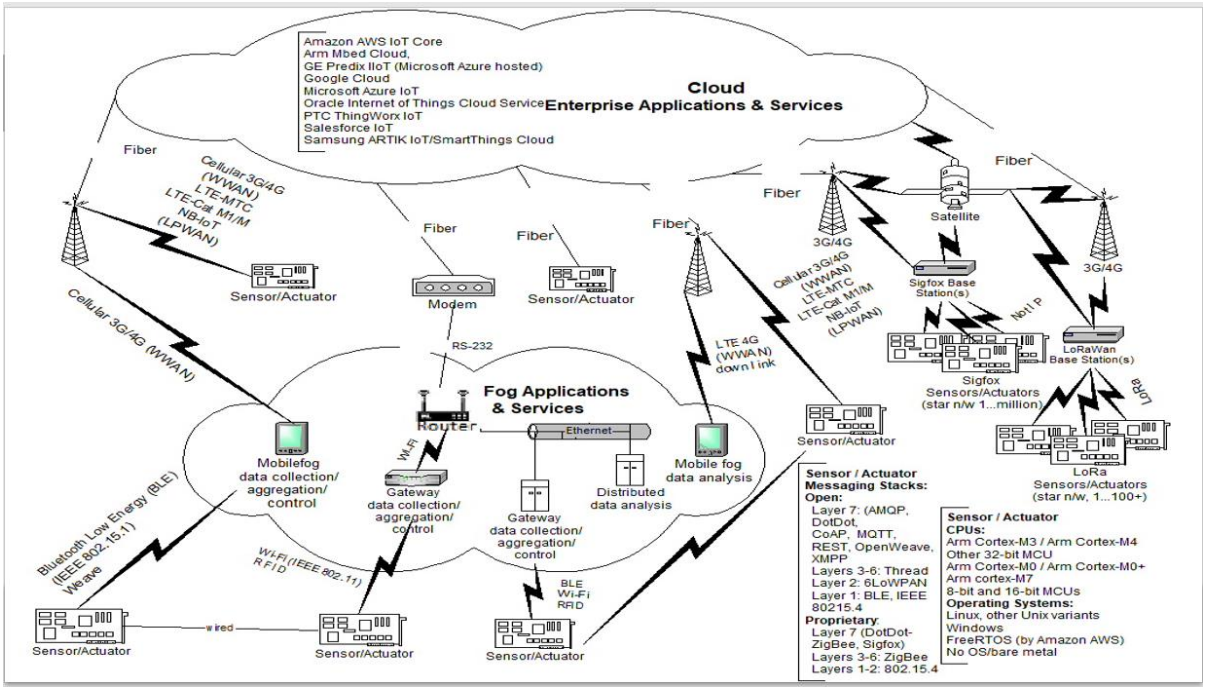


Figure 8-3 Fog Devices Integrated with Telecommunications Infrastructure

8.4 IoT Vulnerabilities

The Open Web Application Security Project (OWASP) organization has published their list of top 10 vulnerability types for IoT systems [97].

1. Insecure Web Interface
2. Insufficient Authentication/Authorization
3. Insecure Network Services
4. Lack of Transport Encryption/Integrity Verification
5. Privacy Concerns
6. Insecure Cloud Interface
7. Insecure Mobile Interface
8. Insufficient Security Configurability
9. Insecure Software/Firmware
10. Poor Physical Security

8.4.1 NIST National Vulnerability Database

Searching the NIST National Vulnerability Database [98] using the keywords 'medical' and 'patient' reveals a recently growing number of vulnerabilities as shown in **Figure 8-4** and **Figure 8-5**.

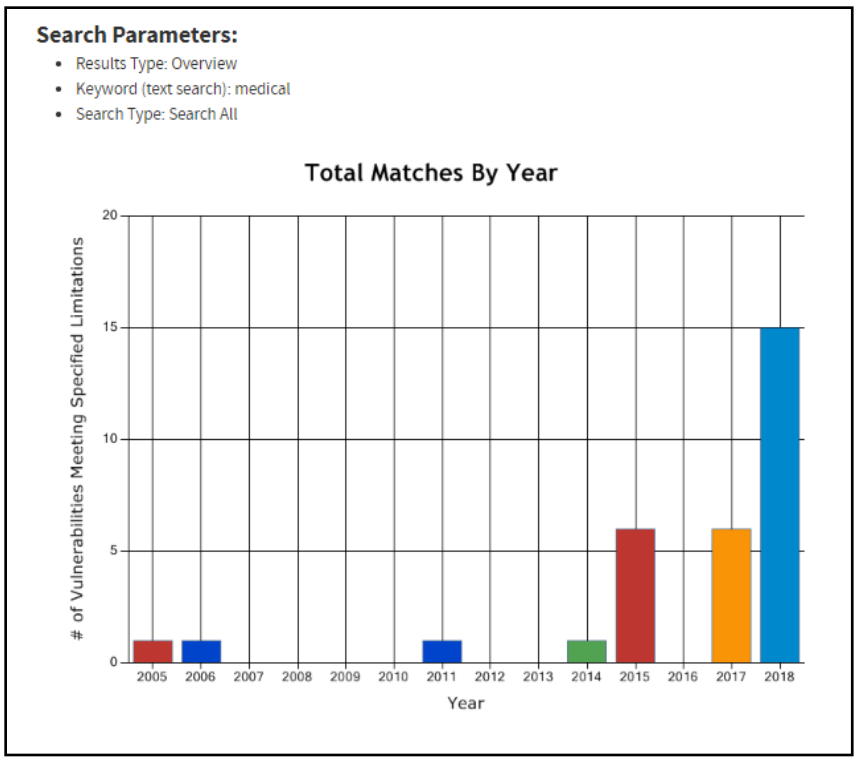


Figure 8-4 Number of Vulnerabilities Found using the Search Term ”medical”

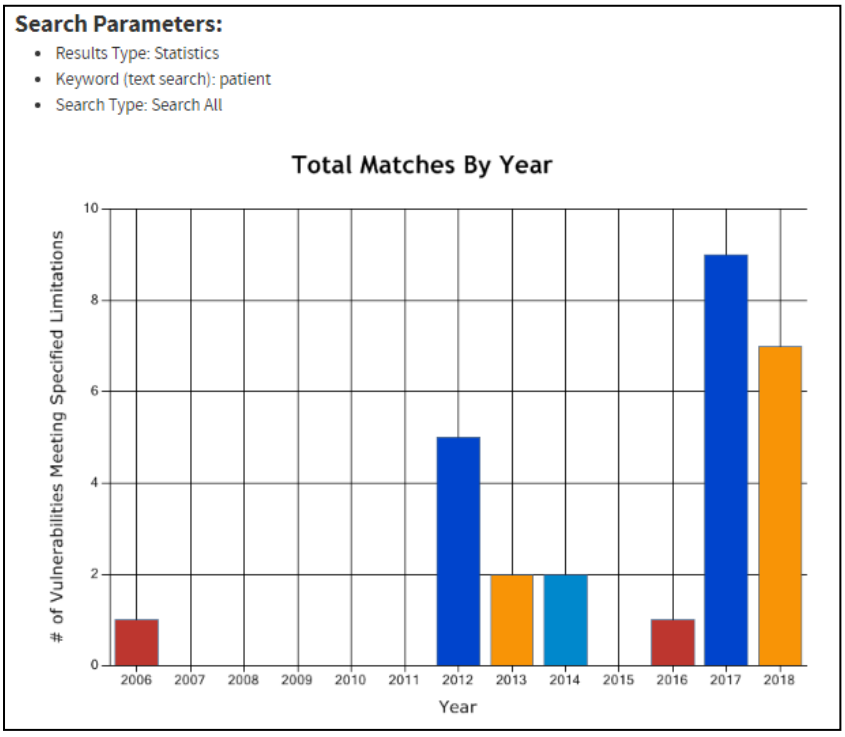


Figure 8-5 Number of Vulnerabilities Found using the Search Term “patient”

The “medical” search results were mostly for IoT devices, while the “patient” search results were mostly for information systems. The results suggest the increase in the number of networked medical devices is associated with an increasing number of vulnerabilities.

The number of vulnerabilities is small, but when considering the large numbers of devices that can be affected by each vulnerability, there exists the potential for thousands of potential breaches.

8.5 IoT Standards and Regulations

The healthcare industry is unique in its formation of a voluntary network of partners to consolidate medical device data for evaluating medical devices for regulatory purposes. A public-private partnership between the FDA and the Medical Device Innovation Consortium (MDIC) resulted in a grant creating the National Evaluation System for health Technology Coordinating Center (NESTcc) [99].

From the NESTcc.org website:

> *A Planning Board convened by the Duke-Margolis Center for Health Policy in late 2015 envisioned NEST as a voluntary network of data partners able to efficiently consolidate RWE [Real World Evidence] to inform medical device evaluation and support regulatory decision-making throughout the total product life cycle (TPLC).*
>
> *In September 2016, FDA awarded a grant for the NEST Coordinating Center (NESTcc) to the Medical Device Innovation Consortium (MDIC). MDIC is a 501(c)(3) public-private partnership with the objective of advancing regulatory science of medical devices for patient benefit. The selection of a third-party entity was important given the need for NESTcc to establish relationships and agreements between partners in a neutral, objective manner and to solicit a balanced representation from stakeholders.*

The FDA published the Medical Device Safety Action Plan in 2018. Among its five goals is cybersecurity:

> *1. Establish a robust medical device patient safety net in the United States*

2. Explore regulatory options to streamline and modernize timely implementation of postmarket mitigations

3. Spur innovation towards safer medical devices

4. Advance medical device cybersecurity

5. Integrate the Center for Devices and Radiological Health's (CDRH's) premarket and postmarket offices and activities to advance the use of a TPLC approach to device safety [86].

The ISO/IEEE 11073 Personal Health Data (PHD) group of standards addresses interoperability among PHDs [100].

8.6 Conclusion and Future Research

Chiang and Zhang predict future research will determine how fog interacts with the cloud and which functions are performed in the fog layer [101].

Fog computing for connected healthcare is a promising technology that will bring improved security, reduced latency, and possibly lower cost mobile cellular service to consumers as healthcare and other industries seek to leverage the scalability of mobile edge computing or distributed cloud also known as fog computing.

Australian telecommunications provider, Vodafone, has recently made data plans available at no cost to consumers participating in a cancer research project (Dream Lab) that uses the processing power of consumer smart phones while phones are plugged into chargers (usually overnight) [102]. Future research would extend this model to gather and process data from IoT edge devices.

Chapter 9:
Final Results and Future Work

9.0 Chapter Introduction

MACH-T can build a reliable trust value and corresponding confidence value based on learned patterns of time spent visiting geographic locations for a configurable minimum time duration. Geographic location information in GPS trace files is the source of data for calculating trust values. Such trust values will be useful for MANet operators desiring to build networks of trusted nodes where the trust is measurable prior to admitting a node to a MANet.

Research and study of prior work on the subject of trust by Guo et al. [3] and Hacker [11] in both computer science and human behavior, led to the contribution in this dissertation of an algorithm that maps trust attributes in the computer science domain with attributes in the human behavioral science domain. This mapping, shown in **Table 9.1**, provided the foundation for a trust algorithm, MACH-T.

Table 9.1 Trust Classification Model Component Mapping to Human Behavior Trust Components

Trust Classification Design Dimension in the Computing Domain [3]	**Trust Dimension in the Human Behavior Domain [11]**
Quality of Service	Capable: Presence of GPS trace data collected frequently over time, capable of communicating with GPS satellites or other devices providing geolocation data
Centralized	Consistent: Centralizing allows for comparison to others and to self to determine consistency in behavior
Static weighted sum	Consistent: Repeated conformance to expected set of population average geographic location behaviors or to an ideal set of geographic location behaviors
Event + time-driven	Committed: Visits to the same geographic locations over time shows commitment
Multi-trust	Capable: Many dimensions contribute to overall trust

The MACH-T algorithm provides the ability to parameterize trust calculations based on the history of a node's capability, commitment, and consistency as shown by a node's

- capability to visit geographic locations and record GPS traces,
- commitment to visit locations within a small perimeter for minimum time durations or at relative time (time-of-day, time-of-week, or time-of-month), and
- consistency to repeatedly visit a small number of geographic locations.

Because trust is context dependent, the MACH-T trust algorithm provides a level of assurance of success in building a MANet. That is, it reduces the risk of failure in building a MANet because the trusted nodes are capable of communicating as evidenced by their GPS trace history, the nodes are committed to visiting a small number of geographic locations for at least a minimum duration as defined by the MANet operator, and over time the nodes visit the same small number of locations. Additionally, the volume and density of node GPS traces provides a Confidence factor which can decrease the unadjusted trust value, MACH-T(U), resulting in an adjusted trust value, MACH-T(A).

The context of geographic presence over time is relevant to MANet formation in the same way that a medical degree and a history of successfully treating patients would be trust criteria for a medical doctor. The different contexts require different trust parameters.

Using two publicly available datasets, one from Microsoft Research (the Geolife dataset) and one from University of Rome, Tor Vergata researchers (the Roma Taxi dataset), this dissertation documented five experiments to calculate trust values based on the behavioral attributes of the subject mobile devices and also on the subjective definition of trust in each experiment.

In addition, a trust modeling spreadsheet demonstrated the ability to model various node trust attributes to learn how various behaviors and subjective trust parameters can change the resulting calculated trust value.

9.1 Discussion

Three instances of geographic location for authentication were found in the literature:

One is the Trusted Platform Module chip which includes a GPS locator to restrict certain computer hardware from operating outside specific geographic areas [14].

Another, no longer used, was the practice of cell phone companies selling user data to credit card companies to allow the credit card companies to know if a cell phone belonging to the card holder was present during a transaction using the credit card. Courts determined the cell phone companies violated cell phone users' privacy rights and the practice stopped [76].

A third, Social media site Nextdoor.com validates new members by first requiring them to enter a verification code they receive by postal mail at their home physical address. Their actual physical presence in the neighborhood authenticates their identity [103]. Someone could impersonate a neighbor but would need to intercept the postcard in order to do so. This physical "man-in-the-middle" attack is not scalable.

In the six experiments described in this dissertation, the MACH-T method of trust assessment resulted in a trust metric indicating if a mobile device was behaving in a trusted way, as defined by a MANet operator. In all six experiments, the MACH-T(A) adjusted trust value ranged from zero, considered untrusted to a positive value. A MANet operator would determine at what value above zero a mobile node should be considered to be trusted and allowed to join a MANet.

Previous research on trust in mobile ad hoc networks has not focused on individual node geographic location history as a means of calculating a trust value based on such behavior which can be classified as a type of non-peer based reputation measure. All previous research focused on node communication ability or recommendation of neighbor nodes.

As reported by Chen and Chang [104] in their research on technology acceptance, the International Telecommunication Union reported in 2010 that mobile cellular subscriptions per 100 inhabitants reached 116.1 in developed countries. This high level of mobile communication adoption indicates acceptance by the public of mobile cellular communication as a trusted means of communicating within the definition of trust proposed in this dissertation. That is, the mobile cellular communication network is capable of sending and receiving data without error, is committed to sending and receiving data because it is available at all times and is consistent because the communications are correct over time. Any lack of trust in the mobile device hardware itself by the general public has not been a barrier to communicating on the cellular infrastructure and it does not logically follow that it would be a barrier to communicating device-to-device in mobile ad hoc networks.

Because mobile devices exist in the physical world and are typically carried by people or vehicles, MACH-T can be a viable and useful method for assessing trust in mobile devices themselves which is necessary for security and vice versa,

9.2 Risks to Proposed Solution

The proposed method includes a confidence factor for calculating node trust and depends on having GPS traces collected frequently (every few seconds) over a span of days, weeks, or months. Geographic behavior over time provides the basis for assigning trust values. Without enough nodes of similar type such as smart phones carried by human operators, the proposed solution cannot use average geographic behavior to measure one node against the average behavior for that type of node, but an ideal behavior profile can instead be used.

Various threats to the MACH-T method such as ballot stuffing, bad mouthing, on-off attacks, opportunistic behavior, and spoofing have been addressed and are mitigated with the MACH-T approach.

The experiments in this dissertation used the OpenStreetMaps.org tile method of dividing the globe into distinct areas or tiles at zoom level 16. At that zoom level, and at the latitude of GPS traces in the experimental datasets, the tiles measure approximately 469km on a side. Potentially, if a mobile device stays in a location near the borders of two or four adjacent tiles, the GPS trace information may not accurately report on the mobile device's ability to stay in one location for a minimum amount of time. The error would be on the side of distrust in the device since the device may not stay in just one tile for the minimum time duration. Reducing the zoom level would be one way to remedy this problem, especially if the buildings in a locale tended to overlap more than one tile. A MANet operator would need to learn the specifics of a geography to determine the appropriate zoom level for using the MACH-T algorithm.

Implementation risks such as the reliability and correctness of GPS trace data must be considered although this risk is beyond the scope of the proposed solution. Harris describes how GPS data is vulnerable to spoofing and jamming in a paper published in 2021 [105] . This proposed method uses GPS traces but other means for ensuring physical presence in a location could be used such as Bluetooth or Near Field Communication beacons placed at a location or detection by other trusted MANet nodes.

9.3 Future Work

Before ad hoc networks can become secure and resilient, trust will need to be measurable and dynamic. Historical and geographical behavior analysis appears to be a promising avenue for providing the basis for trust formation in mobile ad hoc network devices.

Future work may determine if behaviors of personal or other types of mobile devices such as non-taxi vehicle-mounted devices can be predicted based on constant ratios across multiple datasets. Google.com location history files represent one source of data [106]. Ensuring behavioral data sources are trustworthy is an additional factor to consider when evaluating additional datasets if such are available.

Recent formation of networks of stationary devices such as the Amazon Sidewalk network which uses Wi-Fi and LoRa communication channels to connect Amazon Alexa and Ring doorbell devices to form non-cellular networks is an interesting development [107].

Consumers who opt out of using their devices in such a network could present challenges to network connectivity. MANet nodes of smart phones could potentially provide coverage for gaps in such a network.

GoTenna corporation's MURS radio which integrates with mobile devices using Bluetooth communication can boost the reach of a Bluetooth enabled device from 100 meters to many miles depending on the terrain and interference from structures such as buildings or trees [108]. Combining a GoTenna radio with a smart phone would provide extended reach for smart phones.

Apple corporation's FindMy network uses millions of iPhone devices to cooperatively provide location information for a lost device and report the location to the device owner. Users can opt out of this feature which uses the NFC, Bluetooth, and Wi-Fi communications capability of iPhones to communicate device-to-device without active participation by the phone owner. Recently they have included a new ultra-wideband U1 chip in their iPhone 11 and 12 models. The device-to-device communication capability has recently been expanded to Apple's AirTag devices which are small hardware devices with NFC capabilities that can be attached to personal property to help find the property through the FindMy network in case of loss [109].

Amazon corporation announced a mid-June product launch resulting from a new partnership with Tile, a manufacturer of devices predating and similar to the Apple AirTag. The Tile devices will integrate with the Amazon Sidewalk network [110].

Samsung phones support Samsung's GalaxyFind network with similar capabilities to the Apple FindMy network [111].

In a May 2021 article published in the Wall Street Journal, reporter Christopher Mims summarizes these new technologies:

> *Yes, perfect strangers are using slivers of our bandwidth, as our devices send out and listen to little chirrups of radio chatter that don't pertain to us. And you're now able to leverage the radios and internet connection of countless devices owned by other people, too* [107].

MANets may someday soon also leverage the availability of multitudes of mobile devices owned by people who will have options for device-to-device communications, eliminating the total dependence on cellular infrastructure. Using geographic location history MANet operators will have the ability to calculate the trust value of all mobile nodes in the MANet which will assure the capability, consistency, and commitment of nodes towards the successful operation of the MANet.

Chapter 10: References

[1] Li, W., Parker, J., & Joshi, A. (2012). Security through collaboration and trust in MANETs. *Mobile Networks and Applications*, *17*(3), 342-352.

[2] Deville, P., Linard, C., Martin, S., Gilbert, M., Stevens, F. R., Gaughan, A. E., ... & Tatem, A. J. (2014). Dynamic population mapping using mobile phone data. Proceedings of the National Academy of Sciences, 111(45), 15888-15893.

[3] J. Guo, R. Chen, and J.P. Tsai. "A survey of trust computation models for service management in internet of things systems." Computer Communications 97 (2017): 1-14. http://dx.doi.org/10.1016/j.comcom.2016.10.012

[4] F. Bao, I.R. Chen, Dynamic trust management for internet of things applications. In Proceeding of Self-IoT '12: Proceedings of the 2012 international workshop on Self-aware internet of things, San Jose, CA, USA, September 2012, ACM Press: ISBN 978-1-4503-1753-5

[5] I.R. Chen, F. Bao, J. Guo, Trust-based service management for social internet of things systems, IEEE Trans. Dependable Secure Comput. (2016), in press, doi: 10. 1109/TDSC.2015.2420552 .

[6] Z. Chen , R. Ling , C.M. Huang , X. Zhu , A scheme of access service recommendation for the social internet of things, Int. J. Commun. Syst. 29 (4) (2016) 694–706.

[7] M. Nitti , R. Girau , L. Atzori , Trustworthiness management in the social internet of things, IEEE Trans. Knowl. Data Manage. 26 (5) (2014) 1253–1266 .

[8] Govindan, Kannan, and Prasant Mohapatra. "Trust computations and trust dynamics in mobile adhoc networks: A survey." *IEEE Communications Surveys & Tutorials* 14, no. 2 (2011): 279-298.

[9] Gligor, V., & Wing, J. M. (2011, March). Towards a theory of trust in networks of humans and computers. In *International workshop on Security Protocols* (pp. 223-242). Springer, Berlin, Heidelberg.

[10] Gilliam, H. (1987). “Who’s Who on Mt. Tamalpais”, San Francisco Chronicle.

[11] S. Hacker. Who DO You Trust? Quality progress 47.8 (2014): 24.

[12] Cho, J. H., Swami, A., & Chen, R. (2010). A survey on trust management for mobile ad hoc networks. *IEEE communications surveys & tutorials*, *13*(4), 562-583.

[13] Jaquith A. Security metrics. Upper Saddle River, NJ: Pearson Education; 2007.

[14] Segall, A. (2016). *Trusted Platform Modules: Why, when and how to use them*. The Institution of Engineering and Technology.

[15] Zhou, R., & Hwang, K. (2006, April). Trust overlay networks for global reputation aggregation in P2P grid computing. In *Proceedings 20th IEEE International Parallel & Distributed Processing Symposium* (pp. 10-pp). IEEE.

[16] A. Josang and S. LoPresti, "Analyzing the Relationship between Risk and Trust," *Proc. 2nd Int'l Conf. Trust Management*, LNCS, Springer-Verlag, 2004, pp. 135-145.

[17] D. Gambetta, "Can We Trust Trust?" *Trust: Making and Breaking Cooperative Relations*, Basil Blackwell, Oxford, 1990, pp. 213-237.

[18] S. D. Kamvar, M. T. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks," *Proc. 12th Int'l Conf. on World Wide Web*, New York, NY, 20-23 May 2003, pp. 640–651.

[19] B. Solhaug, D. Elgesem, and K. Stolen, "Why Trust is not proportional to Risk?" *Proc. 2nd Int'l Conf. on Availability, Reliability, and Security*, 10-13 Apr. 2007, Vienna, Austria, pp. 11-18.

[20] R. Li, J. Li, P. Liu, H. H. Chen, "An Objective Trust Management Framework for Mobile Ad Hoc Networks," *Proc. IEEE 65th Vehicular Technology Conf.*, 22-25 Apr. 2007, pp. 56-60.

[21] J. Li, R. Li, and J. Kato, "Future Trust Management Framework for Mobile Ad Hoc Networks: Security in Mobile Ad Hoc Networks," *IEEE Commun. Mag.*, vol. 46, no. 4, Apr. 2008, pp. 108-114.

[22] F. Yunfang, “Adaptive Trust Management in MANETs,” *Proc. 2007 Int’l Conf. on Computational Intelligence and Security*, Harbin, China, 15-19 Dec. 2007, pp. 804-808.

[23] H. Li and M. Singhal, “Trust Management in Distributed Systems,” *Computers*, vol. 40, no.2, Feb. 2007, pp. 45-53.

[24] E. Aivaloglou, S. Gritxalis, and C. Skianis, “Trust Establishment in Ad Hoc and Sensor Networks,” *Proc. 1st Int’l Workshop on Critical Information Infrastructure Security, Lecture Notes in Computer Science*, vol. 4347, pp. 179-192, Samos, Greece, 31 Aug. – 1 Sep. 2006, Springer.

[25] Y.B. Saied , A. Olivereau , D. Zeghlache , M. Laurent , Trust management system design for the internet of things: a context-aware and multi-service approach, Comput. Secur. 39 (2013) 351–365.

[26] Adali, S. (2013). *Modeling trust context in networks*. Springer Briefs.

[27] H. Nissenbaum, Will security enhance trust online, or supplant it? in *Trust and Distrust in Organizations*, ed. by R.M. Kramer, K.S. Cook. Russell Sage Foundation Series on Trust (Russell Sage Foundation, New York, 2004), pp. 155–188.

[28] Bartock, M., Souppaya, M., Yeluri, R., Shetty, U., Greene, J., Orrin, S., ... & Scarfone, K. (2015). Trusted geolocation in the cloud: Proof of concept implementation. *Publication NISTIR, 7904*.

[29] Lu, D., Huang, X., Zhang, G., Zheng, X., & Liu, H. (2018). Trusted device-to-device based heterogeneous cellular networks: a new framework for connectivity optimization. IEEE Transactions on Vehicular Technology, 67(11), 11219-11233.

[30] Eagle, N., & Pentland, A. S. (2009). Eigenbehaviors: Identifying structure in routine. Behavioral Ecology and Sociobiology, 63(7), 1057-1066.

[31] Agarwal, Gaurav. "Time and location based authentication credentials." U.S. Patent Application 15/920,973, filed September 19, 2019.

[32] K.H. Thurston, D. Conte de Leon. MACH-2K Architecture: Building Mobile Device Trust and Utility for Emergency Response Networks. Proceedings of the 2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW), Monterey, CA, USA, November, 2019, IEEE, DOI: 10.1109/MASSW.2019.00004

[33] Microsoft Research. (2012, August 9). GeoLife GPS trajectories. Retrieved July 3, 2020, from GeoLife: Building social networks using human location history http://research.microsoft.com/en-us/downloads/b16d359d-d164-469e-9fd4-daa38f2b2e13/

[34] Yu Zheng, Lizhu Zhang, Xing Xie, Wei-Ying Ma. Mining interesting locations and travel sequences from GPS trajectories. In Proceedings of International conference on World Wild Web (WWW 2009), Madrid Spain. ACM Press: 791-800.

[35] Yu Zheng, Quannan Li, Yukun Chen, Xing Xie, Wei-Ying Ma. Understanding Mobility Based on GPS Data. In Proceedings of ACM conference on Ubiquitous Computing (UbiComp 2008), Seoul, Korea. ACM Press: 312-321.

[36] Yu Zheng, Xing Xie, Wei-Ying Ma, GeoLife: A Collaborative Social Networking Service among User, location and trajectory. Invited paper, in IEEE Data Engineering Bulletin. 33, 2, 2010, pp. 32-40.

[37] F. Bao, I.R. Chen, Dynamic trust management for internet of things applications. In Proceeding of Self-IoT '12: Proceedings of the 2012 international workshop on Self-aware internet of things, San Jose, CA, USA, September 2012, ACM Press: ISBN 978-1-4503-1753-5

[38] I.R. Chen, F. Bao, J. Guo, Trust-based service management for social internet of things systems, IEEE Trans. Dependable Secure Comput. (2016), in press, doi: 10. 1109/TDSC.2015.2420552 .

[39] Z. Chen , R. Ling , C.M. Huang , X. Zhu , A scheme of access service recommendation for the social internet of things, Int. J. Commun. Syst. 29 (4) (2016) 694–706.

[40] M. Nitti , R. Girau , L. Atzori , Trustworthiness management in the social internet of things, IEEE Trans. Knowl. Data Manage. 26 (5) (2014) 1253–1266 .

[41] California Average Commute Time by County. Available online: https://www.indexmundi.com/facts/united-states/quick-facts/california/average-commute-time#map

[42] OpenStreetMaps.org. Available online: https://wiki.openstreetmap.org/wiki/Main_Page

[43] Tile Calculator Beta. Available online: https://tools.geofabrik.de/calc/#2/43/7&type=Geofabrik_Standard

[44] GPSprune. Available online: https://activityworkshop.net/software/gpsprune/download.html

[45] Distance and Azimuths Between Two Sets of Coordinates. Available online: https://www.fcc.gov/media/radio/distance-and-azimuths

[46] L. Bracciale, M. Bonola, P. Loreti, G. Bianchi, R. Amici, A. Rabuffi, CRAWDAD dataset roma/taxi (v. 2014-07-17), 2014, doi: 10.15783/C7QC7M. (accessed November 15, 2020).

[47] T. Strayer, S. Nelson, A. Caro, J. Khoury, B. Tedesco, O. DeRosa, C. Clark, K. Sadeghi, M. Matthews, J. Kurzer, P. Lundrigan, V. Kawadia, D. Ryder, K. Gremban, and W. Phoel, “Content sharing with mobility in an infrastructure-less environment,” Computer Networks, vol. 144, pp. 1–16, 2018. [Online]. Available: https: //doi.org/10.1016/j.comnet.2018.07.021

[48] A. Vasudeva and M. Sood, “Survey on sybil attack defense mechanisms in wireless ad hoc networks,” Journal of Network and Computer Applications, vol. 120, pp. 78–118, 2018. [Online]. Available: https://doi.org/10.1016/j.jnca.2018.07.006

[49] M. Talasila, R. Curtmola, and C. Borcea, “Collaborative Bluetooth based location authentication on smart phones,” Pervasive and Mobile Computing, vol. 17, pp. 43–62, 2015. [Online]. Available: https://doi.org/10.1016/j.pmcj.2014.02.004

[50] J. P. Coon, “Modelling trust in random wireless networks,” in 11th International Symposium on Wireless Communications Systems (ISWCS-2014), August 2014, pp. 976–981. [Online]. Available: https://doi.org/10.1109/ISWCS.2014.6933495

[51] R. Gupta, N. Krishnamurthi, U. Wang, T. Tamminedi, and M. Gerla, “Routing in mobile ad-hoc networks using social tie strengths and mobility plans,” in IEEE Wireless Communications and Networking Conference (WCNC-2017), March 2017, pp. 1–6. [Online]. Available: https://doi.org/10.1109/WCNC.2017.7925620

[52] J. Zhang, H. Huang, C. Yang, J. Liu, Y. Fan, and G. Yang, “Destination-aware metric based social routing for mobile opportunistic networks,” Wireless Networks, March 2019. [Online]. Available: https://doi.org/10.1007/s11276-018-01907-2

[53] F. Liu, X. Li, Y. Ding, H. Zhao, X. Liu, Y. Ma, and B. Tang, “A social network-based trust-aware propagation model for p2p systems,” Knowledge-Based Systems, vol. 41, pp. 8–15, 2013. [Online]. Available: https://doi.org/10.1016/j.knosys.2012.12.005

[54] C. Selvaraj and S. Anand, “Peer profile based trust model for p2p systems using genetic algorithm,” Peer-to-Peer Networking and Applications, vol. 5, no. 1, pp. 92–103, March 2012. [Online]. Available: https://doi.org/10.1007/s12083-011-0111-9

[55] X. Zhang, “Efficient and quality-aware data access in mobile opportunistic networks,” Ph.D. dissertation, Pennsylvania State University, May 2016. [Online]. Available: https://etda.libraries.p su.edu/catalog/q811kj61g

[56] A. K. Saha, “Cross layer techniques to secure peer-to-peer protocols for location, adjacency, and identity verification,” Ph.D. dissertation, University of California, Riverside, 2006. [Online]. Available: http: //alumni.cs.ucr.edu/_saha/

[57] L. Lilien, Z. Kamal, V. Bhuse, and A. Gupta, “Opportunistic networks: The concept and research,” in Proceedings of the International Workshop on Research Challenges in Security and Privacy for Mobile and Wireless Networks (WSPWN 2006). Springer, 2006. [Online]. Available: https://doi.org/10.1007/978-0-387-71058-7 5

[58] E. Kuada and B. Bannerman, “Opportunistic rescue network for disaster management,” in 2017 IEEE AFRICON, September 2017, pp. 917–922. [Online]. Available: https://doi.org/10.1109/AFRICON.2017.8095604

[59] M. Di Felice, L. Bedogni, and L. Bononi, “The emergency direct mobile app: Safety message dissemination over a multi-group network of smartphones using wi-fi direct,” in Proceedings of the 14th ACM International Symposium on Mobility Management and Wireless Access, ser. MobiWac-2016. ACM, 2016, pp. 99–106. [Online]. Available: https://doi.org/10.1145/2989250.2989257

[60] R. Lakshmi Narayanan and O. C. Ibe, “6-joint network for disaster relief and search and rescue network operations,” in Wireless Public Safety Networks 1, D. Cˆamara and N. Nikaein, Eds. Elsevier, 2015, pp. 163–193. [Online]. Available: https: //doi.org/10.1016/B978-1-78548-022-5.50006-6

[61] S. Krug, S. Schellenberg, and J. Seitz, “Impact of traffic and mobility patterns on network performance in disaster scenarios,” in Proceedings of the 10th ACM MobiCom Workshop on Challenged Networks, ser. CHANTS ’15. New York, NY, USA: ACM, 2015, pp. 9–12. [Online]. Available: https://doi.org/10.1145/2799371.2799388

[62] K. Kanchanasut, T. Wongsaardsakul, M. Chansutthirangkool, A. Laouiti, H. Tazaki, and K. R. Arefin, “Dumbo ii: A v-2-i emergency network,” in Proceedings of the 4th Asian Conference on Internet Engineering, ser. AINTEC ’08. ACM, 2008, pp. 37–38. [Online]. Available: https://doi.org/10.1145/1503370.1503380

[63] N. Aschenbruck, M. Frank, P. Martini, and J. Tolle, “Human mobility in manet disaster area simulation,” in Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, November 2004, pp. 668–675. [Online]. Available: https://doi.org/10.1109/LCN.2004.64

[64] R.-I. Ciobanu, C. Negru, F. Pop, C. Dobre, C. X. Mavromoustakis, and G. Mastorakis, “Drop computing: Ad-hoc dynamic collaborative computing,” Future Generation Computer Systems, vol. 92, pp. 889–899, 2019. [Online]. Available: https://doi.org/10.1016/j.future.2017.11.044

[65] C. E. Casetti, C. F. Chiasserini, Y. Duan, P. Giaccone, and A. Perez Manriquez, “Data connectivity and smart group formation in wi-fi direct multi-group networks,” IEEE Transactions on Network and Service Management, vol. 15, no. 1, pp. 245–259, March 2018. [Online]. Available: https://doi.org/10.1109/TNSM.2017.2766124

[66] B. M. Masini, A. Bazzi, and A. Zanella, “A survey on the roadmap to mandate on board connectivity and enable v2v-based vehicular sensor networks,” Sensors, vol. 18, no. 7, 2018. [Online]. Available: https://doi.org/10.3390/s18072207

[67] M. Green, A. Thomas, A. Chachich, W. Fehr, and N. Deshmukh Towery, “Fhwa white paper on mobile ad hoc networks,” US Federal Highway Administration, Tech. Rep., January 2018, fHWA-HRT-18-027. [Online]. Available: https://www.fhwa.dot.gov/publications/research/ear/18027/index.cfm

[68] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang, “Vehicle-to-vehicle communications: Readiness of v2v technology for application,” US National Highway Traffic Safety Administration, Tech. Rep., 2014. [Online]. Available: https://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V 2V-Technology-for-Application-812014.pdf

[69] S. Chen, J. Hu, Y. Shi, Y. Peng, J. Fang, R. Zhao, and L. Zhao, “Vehicle-to-everything (v2x) services supported by lte based systems and 5g,” IEEE Communications Standards Magazine, vol. 1, no. 2, pp. 70–76, 2017. [Online]. Available: https: //doi.org/10.1109/MCOMSTD.2017.1700015

[70] P. Choi, J. Gao, N. Ramanathan, M. Mao, S. Xu, C.-C. Boon, S. A. Fahmy, and L.-S. Peh, “A case for leveraging 802.11p for direct phone-to-phone communications,” in Proceedings of the 2014 International Symposium on Low Power Electronics and Design, ser. ISLPED-2014. New York, NY, USA: ACM, 2014, pp. 207–212. [Online]. Available: https://doi.org/10.1145/2627369.2627644

[71] O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. Lin, and X. Liu, “Internet of vehicles: Motivation, layered architecture, network model, challenges, and

future aspects," IEEE Access, vol. 4, pp. 5356–5373, 2016. [Online]. Available: https: //doi.org/10.1109/ACCESS.2016.2603219

[72] M. Le, "Universal mobile service execution framework for device-to-device collaborations," Ph.D. dissertation, Utah State University, May 2018. [Online]. Available: https://digitalcommons.usu.edu/etd/7032

[73] H. Teng, Y. Liu, A. Liu, N. N. Xiong, Z. Cai, T. Wang, and X. Liu, "A novel code data dissemination scheme for internet of things through mobile vehicle of smart cities," Future Generation Computer Systems, vol. 94, pp. 351–367, 2019. [Online]. Available: https://doi.org/10.1016/j.future.2018.11.039

[74] R. C. Shah, S. Roy, S. Jain, and W. Brunette, "Data mules: Modeling and analysis of a three-tier architecture for sparse sensor networks," Ad Hoc Networks, vol. 1, no. 2, pp. 215–233, 2003. [Online]. Available: https://doi.org/10.1016/S1570-8705(03)00003-9

[75] Y. Kim, K. Bok, I. Son, J. Park, B. Lee, and J. Yoo, "Positioning sensor nodes and smart devices for multimedia data transmission in wireless sensor and mobile p2p networks," Multimedia Tools and Applications, vol. 76, no. 16, pp. 17 193–17 211, August 2017. [Online]. Available: https://doi.org/10.1007/s11042-016-3794-3

[76] S. Krouse, "Five ways companies use your cellphone location data," July 2018, wall Street Journal. [Online]. Available: https://www.wsj.com/arti cles/5-ways-companies-use-your-cellphone-location-data-1531659600

[77] R. Marin, C. Dobre, and F. Xhafa, "Exploring predictability in mobile interaction," in Third International Conference on Emerging Intelligent Data and Web Technologies, September 2012, pp. 133–139. [Online]. Available: https://doi.org/10.1109/EIDWT.2012.29

[78] P. Martinez-Julia and A. F. Skarmeta, "Beyond the separation of identifier and locator: Building an identity-based overlay network architecture for the future internet," Computer Networks, vol. 57, no. 10, pp. 2280–2300, 2013. [Online]. Available: https://doi.org/10.1 016/j.comnet.2012.11.020

[79] Michaela Iorga, Larry Feldman, Robert Barton, Michael J. Martin, Nedim S. Goren, and Charif Mahmoudi. 2018. Fog Computing Conceptual Model. https://doi.org/ 10.6028/NIST.SP.500-325 NIST-SP 500-325.

[80] Fang, Weidong, Wuxiong Zhang, Jinchao Xiao, Yang Yang, and Wei Chen. "A source anonymity-based lightweight secure AODV protocol for fog-based MANET." *Sensors* 17, no. 6 (2017): 1421

[81] Open Web Application Security Project. 2014. OWASP: Top Ten IoT Vulnerabilities. https://www.owasp.org/index.php/Top_IoT_Vulnerabilities Accessed: 30 Sep. 2018.

[82] D. Greenfield, "Fog Computing vs. Edge Computing: What's the Difference? | Automation World", Automationworld.com, 2016. [Online]. Available: https://www.automationworld.com/fog-computing-vs-edge-computing-whats-difference. [Accessed: 30- May- 2018].

[83] M. Chiang, B. Balasubramanian, and F Bonomi, eds., "FOG FOR 5G AND IoT", Wiley Series on Information and Communication Technology, 2017.

[84] O. Akrivopoulos, I. Chatzigiannakis, C. Tselios and A. Antoniou, "On the Deployment of Healthcare Applications over Fog Computing Infrastructure", in 2017 IEEE 41st Annual Computer Software and Applications Conference, Torino, Italy, 2017.

[85] "IEEE SA - 1934 - IEEE Draft Standard for Adoption of OpenFog Reference Architecture for Fog Computing", Standards.ieee.org, 2018. [Online]. Available: https://standards.ieee.org/develop/project/1934.html. [Accessed: 30- May- 2018].

[86] U.S. Food & Drug Administration, "Medical Device Safety Action Plan: Protecting Patients, Promoting Public Health", U.S. Food & Drug Administration, 2018.

[87] R.Steele and A. Clarke, "The Internet of Things and Next-generation Public Health Information Systems", *Communications and Network*, vol. 05, no. 03, pp. 4-9, 2013.

[88] Q. Ni, A. García Hernando and I. de la Cruz, "The Elderly's Independent Living in Smart Homes: A Characterization of Activities and Sensing Infrastructure Survey to Facilitate Services Development", *Sensors*, vol. 15, no. 5, pp. 11312-11362, 2015.

[89] R. Al-Shaqi, M. Mourshed and Y. Rezgui, "Progress in ambient assisted systems for independent living by the elderly", *SpringerPlus*, vol. 5, no. 1, 2016.

[90] E. Frontoni, R. Pollini, P. Russo, P. Zingaretti and G. Cerri, "HDOMO: Smart Sensor Integration for an Active and Independent Longevity of the Elderly", *Sensors*, vol. 17, no. 11, p. 2610, 2017.

[91] S. Sood and I. Mahajan, "A Fog-Based Healthcare Framework for Chikungunya", *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 794-801, 2018.

[92] P. Verma and S. Sood, "Cloud-centric IoT based disease diagnosis healthcare framework", *Journal of Parallel and Distributed Computing*, vol. 116, pp. 27-38, 2018.

[93] A.M. Rahmani, T.N. Gia, B. Negash, A. Anzanpour, I Azimi, M. Jiang, and P. Liljeberg, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach", *Future Generation Computer Systems*, vol. 78, part 2, pp. 641-658 (2018

[94] "Resources|OpenFogConsortium", Openfogconsortium.org, 2018. [Online]. Available: https://www.openfogconsortium.org/resources/#use-cases. [Accessed: 31- May- 2018].

[95] K. Konstantinos, T. Orphanoudakis, and T. Dagiuklas, "Evaluation of IoT-based Distributed Health Management Systems", ACM Proceedings of the 20th Pan-Hellenic Conference on Informatics, p. 9, 2016.

[96] "IoT Developer Survey 2018", Slideshare.net, 2018. [Online]. Available: https://www.slideshare.net/kartben/iot-developer-survey-2018. [Accessed: 31- May- 2018].

[97] "OWASP Internet of Things Project - OWASP", Owasp.org, 2018. [Online]. Available: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project. [Accessed: 31- May- 2018].

[98] "NVD - Search and Statistics", Nvd.nist.gov, 2018. [Online]. Available: https://nvd.nist.gov/vuln/search. [Accessed: 31- May- 2018].

[99] "About MDIC | Medical Device Innovation Consortium (MDIC)", Mdic.org, 2018. [Online]. Available: http://mdic.org/about-us/. [Accessed: 31- May- 2018].

[100] "IEEE 11073-20601-2014 - IEEE Health informatics--Personal health device communication - Part 20601: Application profile- Optimized Exchange Protocol", Standards.ieee.org, 2018. [Online]. Available: https://standards.ieee.org/findstds/standard/11073-20601-2014.html. [Accessed: 31- May- 2018].

[101] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities - IEEE Journals & Magazine", Ieeexplore.ieee.org, 2018. [Online]. Available: http://ieeexplore.ieee.org/document/7498684/. [Accessed: 31- May- 2018].

[102] A. van Dorn. 2016. “The Dream Lab”, *The Lancet Oncology* vol. 17, no. 2 (February 2016). https://doi.org/10.1016/S1470-2045(16)00033-4

[103] Free website allows city residents to 'talk' to neighbors. (2014). *Dayton Daily News (Dayton, Ohio. 1987)*.

[104] Chen, K. Y., & Chang, M. L. (2013). User acceptance of ‘near field communication’ mobile phone service: an investigation based on the ‘unified theory of acceptance and use of technology’ model. *The Service Industries Journal*, *33*(6), 609-623.

[105] Harris, M. (2021). Military Tests that Jam and Spoof GPS Signals are an Accident Waiting to Happen. *IEEE Spectrum*, *58*(2), 22-27.

[106] McCallum, S. C., & Patterson, Z. (2021). *Google Location History Data and its Potential for Activity Space Research* (No. TRBAM-21-01464).

[107] Mims, C. (2021). EXCHANGE --- Keywords: Thanks for Powering Our Wireless Network --- Amazon and Apple are using your devices for their vast end-run around satellite and cable companies. *Wall Street Journal*

[108] Flamm, Matthew. (2019). CONSTANT CONTACT; Brooklyn startup GoTenna helps first responders stay connected in the harshest conditions. *Crain's New York Business*, *35*(25), 3.

[109] Albergotti, R. (2021, April 20). With AirTags, Apple launches a new product - and invites antitrust scrutiny. *Washington Post*, NA. https://link.gale.com/apps/doc/A659086417/AONE?u=mosc00780&sid=bookmark-AONE&xid=81ed04f7

[110] Amazon Sidewalk has set a mid-June launch for its Tile partnership, following's Apple's announcement of its AirTag competitor. (2021). In *The Business Insider (Blogs on Demand)*. Newstex LLC.

[111] Tofel, K. (2021, April). Why Apple AirTags Will be a Hit: This is no Ordinary Bluetooth Tracker. In *Stacey On IoT*. https://staceyoniot.com/why-apple-airtags-will-be-a-hit-this-is-no-ordinary-bluetooth-tracker/ [Accessed 9-August-2021]

Chapter 11:

Appendix: Copyright Notices

ACM Copyright and Audio/Video Release

Title of the Work: The Healthcare IoT Ecosystem: Advantages of Fog Computing Near the Edge

Author/Presenter(s): Karen Thurston:University of Idaho Coeur d'Alene;Daniel Conte de Leon:University of Idaho
Type of material: Full Paper

Publication and/or Conference Name: CHASE '18: ACM/IEEE International Conference on Connected Health: Applications, Systems and Engineering Technologies Proceedings

I. Copyright Transfer, Reserved Rights and Permitted Uses

* Your Copyright Transfer is conditional upon you agreeing to the terms set out below.

Copyright to the Work and to any supplemental files integral to the Work which are submitted with it for review and publication such as an extended proof, a PowerPoint outline, or appendices that may exceed a printed page limit, (including without limitation, the right to publish the Work in whole or in part in any and all forms of media, now or hereafter known) is hereby transferred to the ACM (for Government work, to the extent transferable) effective as of the date of this agreement, on the understanding that the Work has been accepted for publication by ACM.

Reserved Rights and Permitted Uses

(a) All rights and permissions the author has not granted to ACM are reserved to the Owner, including all other proprietary rights such as patent or trademark rights.

(b) Furthermore, notwithstanding the exclusive rights the Owner has granted to ACM, Owner shall have the right to do the following:

(i) Reuse any portion of the Work, without fee, in any future works written or edited by the Author, including books, lectures and presentations in any and all media.

(ii) Create a "Major Revision" which is wholly owned by the author

(iii) Post the Accepted Version of the Work on (1) the Author's home page, (2) the Owner's institutional repository, (3) any repository legally mandated by an agency funding the research on which the Work is based, and (4) any non-commercial repository or aggregation that does not duplicate ACM tables of contents, i.e., whose patterns of links do not substantially duplicate an ACM-copyrighted volume or issue. Non-commercial repositories are here understood as repositories owned by non-profit organizations that do not charge a fee for accessing deposited articles and that do not sell advertising or otherwise profit from serving articles.

(iv) Post an "Author-Izer" link enabling free downloads of the Version of Record in the ACM Digital Library on (1) the Author's home page or (2) the Owner's institutional repository;

(v) Prior to commencement of the ACM peer review process, post the version of the Work as submitted to ACM ("Submitted Version" or any earlier versions) to non-peer reviewed servers;

(vi) Make free distributions of the final published Version of Record internally to the Owner's employees, if applicable;

(vii) Make free distributions of the published Version of Record for Classroom and Personal Use;

Figure 11-1 ACM Copyright Notice (Page 1 of 4)

(viii) Bundle the Work in any of Owner's software distributions; and

(ix) Use any Auxiliary Material independent from the Work.

When preparing your paper for submission using the ACM TeX templates, the rights and permissions information and the bibliographic strip must appear on the lower left hand portion of the first page.

The new ACM Consolidated TeX template Version 1.3 and above automatically creates and positions these text blocks for you based on the code snippet which is system-generated based on your rights management choice and this particular conference.

Please copy and paste the following code snippet into your TeX file between \begin{document} and \maketitle, either after or before CCS codes.

```
\copyrightyear{2018}
\acmYear{2018}
\setcopyright{acmcopyright}
\acmConference[CHASE '18]{ACM/IEEE International Conference on
Connected Health: Applications, Systems and Engineering
Technologies}{September 26--28, 2018}{Washington, DC, USA}
\acmBooktitle{ACM/IEEE International Conference on Connected Health:
Applications, Systems and Engineering Technologies (CHASE '18), September
26--28, 2018, Washington, DC, USA}
\acmPrice{15.00}
\acmDOI{10.1145/3278576.3278595}
\acmISBN{978-1-4503-5958-0/18/09}
```

ACM TeX template .cls version 2.8, automatically creates and positions these text blocks for you based on the code snippet which is system-generated based on your rights management choice and this particular conference.
Please copy and paste the following code snippet into your TeX file between \begin{document} and \maketitle, either after or before CCS codes.

```
\CopyrightYear{2018}
\setcopyright{acmcopyright}
\conferenceinfo{CHASE '18,}{September 26--28, 2018, Washington, DC, USA}
\isbn{978-1-4503-5958-0/18/09}\acmPrice{$15.00}
\doi{https://doi.org/10.1145/3278576.3278595}
```

If you are using the ACM Microsoft Word template, or still using an older version of the ACM TeX template, or the current versions of the ACM SIGCHI, SIGGRAPH, or SIGPLAN TeX templates, you must copy and paste the following text block into your document as per the instructions provided with the templates you are using:

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with

Figure 11-1 ACM Copyright Notice (Page 2 of 4)

credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

CHASE '18, September 26–28, 2018, Washington, DC, USA
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-5958-0/18/09…$15.00
https://doi.org/10.1145/3278576.3278595

NOTE: Make sure to include your article's DOI as part of the bibstrip data; DOIs will be registered and become active shortly after publication in the ACM Digital Library. Once you have your camera ready copy ready, please send your source files and PDF to your event contact for processing.

☑ A. Assent to Assignment. I hereby represent and warrant that I am the sole owner (or authorized agent of the copyright owner(s)), with the exception of third party materials detailed in section III below. I have obtained permission for any third-party material included in the Work.

☐ B. Declaration for Government Work. I am an employee of the National Government of my country and my Government claims rights to this work, or it is not copyrightable (Government work is classified as Public Domain in U.S. only)

Are any of the co-authors, employees or contractors of a National Government? ○ Yes ◉ No

---

II. Permission For Conference Recording and Distribution

* Your Audio/Video Release is conditional upon you agreeing to the terms set out below.

I hereby grant permission for ACM to include my name, likeness, presentation and comments in any and all forms, for the Conference and/or Publication.

I further grant permission for ACM to record and/or transcribe and reproduce my presentation as part of the ACM Digital Library, and to distribute the same for sale in complete or partial form as part of an ACM product on CD-ROM, DVD, webcast, USB device, streaming video or any other media format now or hereafter known.

I understand that my presentation will not be sold separately as a stand-alone product without my direct consent. Accordingly, I give ACM the right to use my image, voice, pronouncements, likeness, and my name, and any biographical material submitted by me, in connection with the Conference and/or Publication, whether used in excerpts or in full, for distribution described above and for any associated advertising or exhibition.

Do you agree to the above Audio/Video Release? ◉ Yes ○ No

III. Auxiliary Material

Do you have any Auxiliary Materials? ○ Yes ◉ No

IV. Third Party Materials

In the event that any materials used in my presentation or Auxiliary Materials contain the work of third-party individuals or organizations (including copyrighted music or movie

Figure 11-1 ACM Copyright Notice (Page 3 of 4)

excerpts or anything not owned by me), I understand that it is my responsibility to secure any necessary permissions and/or licenses for print and/or digital publication, and cite or attach them below.

(•) We/I have not used third-party material.
( ) We/I have used third-party materials and have necessary permissions.

V. Artistic Images

If your paper includes images that were created for any purpose other than this paper and to which you or your employer claim copyright, you must complete Part V and be sure to include a notice of copyright with each such image in the paper.

(•) We/I do not have any artistic images.
( ) We/I have any artistic images.

VI. Representations, Warranties and Covenants

The undersigned hereby represents, warrants and covenants as follows:

(a) Owner is the sole owner or authorized agent of Owner(s) of the Work;

(b) The undersigned is authorized to enter into this Agreement and grant the rights included in this license to ACM;

(c) The Work is original and does not infringe the rights of any third party; all permissions for use of third-party materials consistent in scope and duration with the rights granted to ACM have been obtained, copies of such permissions have been provided to ACM, and the Work as submitted to ACM clearly and accurately indicates the credit to the proprietors of any such third-party materials (including any applicable copyright notice), or will be revised to indicate such credit;

(d) The Work has not been published except for informal postings on non-peer reviewed servers, and Owner covenants to use best efforts to place ACM DOI pointers on any such prior postings;

(e) The Auxiliary Materials, if any, contain no malicious code, virus, trojan horse or other software routines or hardware components designed to permit unauthorized access or to disable, erase or otherwise harm any computer systems or software; and

(f) The Artistic Images, if any, are clearly and accurately noted as such (including any applicable copyright notice) in the Submitted Version.

☑ I agree to the Representations, Warranties and Covenants

DATE: **09/21/2018** sent to kthurston@uidaho.edu at **13:09:29**

Figure 11-1 ACM Copyright Notice (Page 4 of 4)

IEEE COPYRIGHT AND CONSENT FORM

To ensure uniformity of treatment among all contributors, other forms may not be substituted for this form, nor may any wording of the form be changed. This form is intended for original material submitted to the IEEE and must accompany any such material in order to be published by the IEEE. Please read the form carefully and keep a copy for your files.

MACH-2K Architecture: Building Mobile Device Trust and Utility for Emergency Response Networks
Karen H. Thurston
2019 IEEE 16th International Conference on Mobile Ad Hoc and Sensor Systems Workshops (MASSW)

COPYRIGHT TRANSFER

The undersigned hereby assigns to The Institute of Electrical and Electronics Engineers, Incorporated (the "IEEE") all rights under copyright that may exist in and to: (a) the Work, including any revised or expanded derivative works submitted to the IEEE by the undersigned based on the Work; and (b) any associated written or multimedia components or other enhancements accompanying the Work.

GENERAL TERMS

1. The undersigned represents that he/she has the power and authority to make and execute this form.
2. The undersigned agrees to indemnify and hold harmless the IEEE from any damage or expense that may arise in the event of a breach of any of the warranties set forth above.
3. The undersigned agrees that publication with IEEE is subject to the policies and procedures of the IEEE PSPB Operations Manual.
4. In the event the above work is not accepted and published by the IEEE or is withdrawn by the author(s) before acceptance by the IEEE, the foregoing copyright transfer shall be null and void. In this case, IEEE will retain a copy of the manuscript for internal administrative/record-keeping purposes.
5. For jointly authored Works, all joint authors should sign, or one of the authors should sign as authorized agent for the others.
6. The author hereby warrants that the Work and Presentation (collectively, the "Materials") are original and that he/she is the author of the Materials. To the extent the Materials incorporate text passages, figures, data or other material from the works of others, the author has obtained any necessary permissions. Where necessary, the author has obtained all third party permissions and consents to grant the license above and has provided copies of such permissions and consents to IEEE

You have indicated that you DO wish to have video/audio recordings made of your conference presentation under terms and conditions set forth in "Consent and Release."

CONSENT AND RELEASE

1. In the event the author makes a presentation based upon the Work at a conference hosted or sponsored in whole or in part by the IEEE, the author, in consideration for his/her participation in the conference, hereby grants the IEEE the unlimited, worldwide, irrevocable permission to use, distribute, publish, license, exhibit, record, digitize, broadcast, reproduce and archive, in any format or medium, whether now known or hereafter developed: (a) his/her presentation and comments at the conference; (b) any written materials or multimedia files used in connection with his/her presentation; and (c) any recorded interviews of him/her (collectively, the "Presentation"). The permission granted includes the transcription and reproduction of the Presentation for inclusion in products sold or distributed by IEEE and live or recorded broadcast of the Presentation during or after the conference.
2. In connection with the permission granted in Section 1, the author hereby grants IEEE the unlimited, worldwide, irrevocable right to use his/her name, picture, likeness, voice and biographical information as part of the advertisement, distribution and sale of products incorporating the Work or Presentation, and releases IEEE from any claim based on right of privacy or publicity.

Figure 11-2 IEEE Copyright Notice (Page 1 of 3)

BY TYPING IN YOUR FULL NAME BELOW AND CLICKING THE SUBMIT BUTTON, YOU CERTIFY THAT SUCH ACTION CONSTITUTES YOUR ELECTRONIC SIGNATURE TO THIS FORM IN ACCORDANCE WITH UNITED STATES LAW, WHICH AUTHORIZES ELECTRONIC SIGNATURE BY AUTHENTICATED REQUEST FROM A USER OVER THE INTERNET AS A VALID SUBSTITUTE FOR A WRITTEN SIGNATURE.

Karen H. Thurston — **Signature**

22-10-2019 — **Date (dd-mm-yyyy)**

Information for Authors

AUTHOR RESPONSIBILITIES

The IEEE distributes its technical publications throughout the world and wants to ensure that the material submitted to its publications is properly available to the readership of those publications. Authors must ensure that their Work meets the requirements as stated in section 8.2.1 of the IEEE PSPB Operations Manual, including provisions covering originality, authorship, author responsibilities and author misconduct. More information on IEEE's publishing policies may be found at http://www.ieee.org/publications_standards/publications/rights/authorrightsresponsibilities.html Authors are advised especially of IEEE PSPB Operations Manual section 8.2.1.B12: "It is the responsibility of the authors, not the IEEE, to determine whether disclosure of their material requires the prior consent of other parties and, if so, to obtain it." Authors are also advised of IEEE PSPB Operations Manual section 8.1.1B: "Statements and opinions given in work published by the IEEE are the expression of the authors."

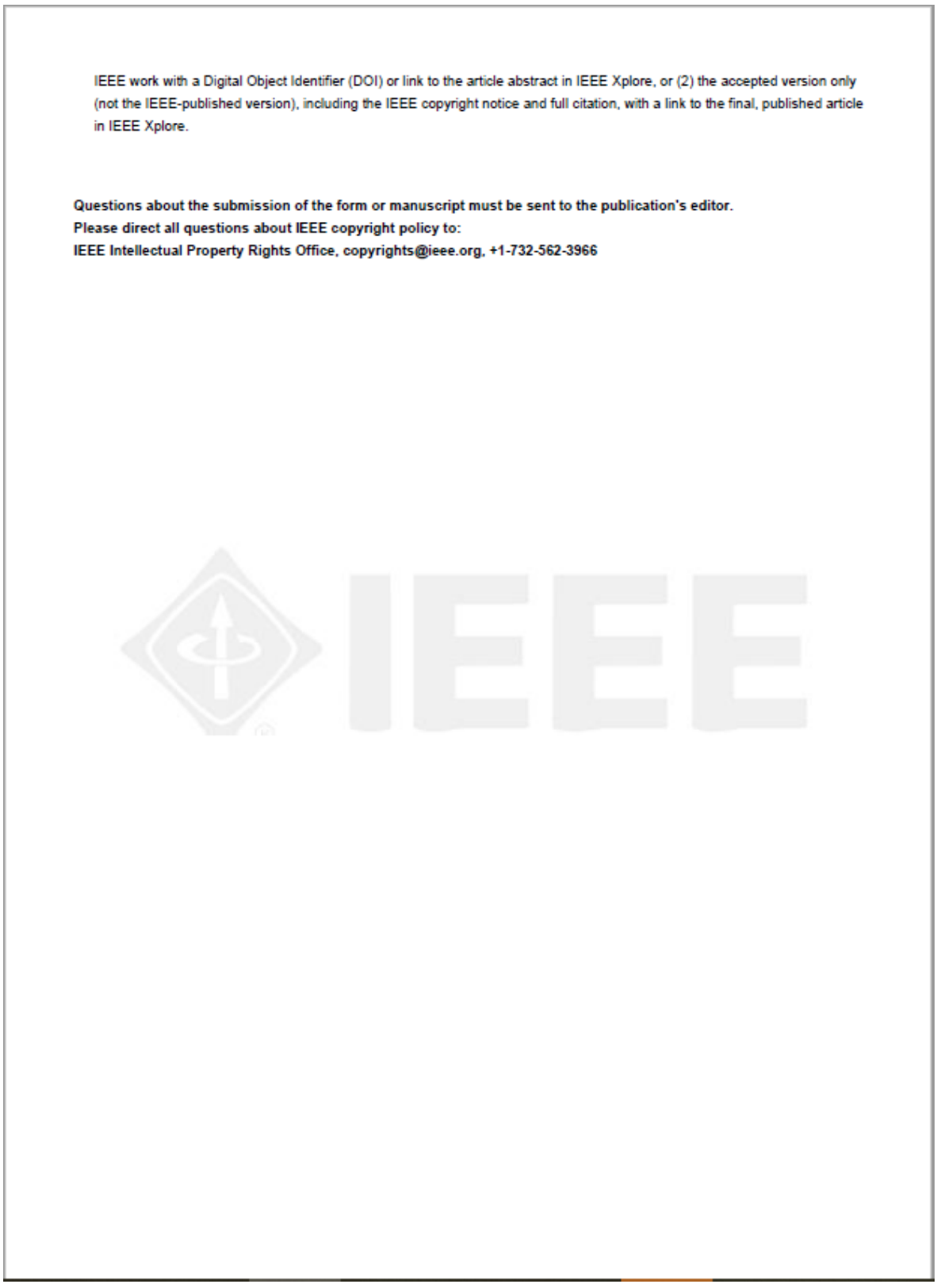
RETAINED RIGHTS/TERMS AND CONDITIONS

- Authors/employers retain all proprietary rights in any process, procedure, or article of manufacture described in the Work.
- Authors/employers may reproduce or authorize others to reproduce the Work, material extracted verbatim from the Work, or derivative works for the author's personal use or for company use, provided that the source and the IEEE copyright notice are indicated, the copies are not used in any way that implies IEEE endorsement of a product or service of any employer, and the copies themselves are not offered for sale.
- Although authors are permitted to re-use all or portions of the Work in other works, this does not include granting third-party requests for reprinting, republishing, or other types of re-use.The IEEE Intellectual Property Rights office must handle all such third-party requests.
- Authors whose work was performed under a grant from a government funding agency are free to fulfill any deposit mandates from that funding agency.

AUTHOR ONLINE USE

- **Personal Servers**. Authors and/or their employers shall have the right to post the accepted version of IEEE-copyrighted articles on their own personal servers or the servers of their institutions or employers without permission from IEEE, provided that the posted version includes a prominently displayed IEEE copyright notice and, when published, a full citation to the original IEEE publication, including a link to the article abstract in IEEE Xplore. Authors shall not post the final, published versions of their papers.
- **Classroom or Internal Training Use.** An author is expressly permitted to post any portion of the accepted version of his/her own IEEE-copyrighted articles on the author's personal web site or the servers of the author's institution or company in connection with the author's teaching, training, or work responsibilities, provided that the appropriate copyright, credit, and reuse notices appear prominently with the posted material. Examples of permitted uses are lecture materials, course packs, e-reserves, conference presentations, or in-house training courses.
- **Electronic Preprints**. Before submitting an article to an IEEE publication, authors frequently post their manuscripts to their own web site, their employer's site, or to another server that invites constructive comment from colleagues. Upon submission of an article to IEEE, an author is required to transfer copyright in the article to IEEE, and the author must update any previously posted version of the article with a prominently displayed IEEE copyright notice. Upon publication of an article by the IEEE, the author must replace any previously posted electronic versions of the article with either (1) the full citation to the

Figure 11-2 IEEE Copyright Notice (Page 2 of 3)



IEEE work with a Digital Object Identifier (DOI) or link to the article abstract in IEEE Xplore, or (2) the accepted version only (not the IEEE-published version), including the IEEE copyright notice and full citation, with a link to the final, published article in IEEE Xplore.

Questions about the submission of the form or manuscript must be sent to the publication's editor.
Please direct all questions about IEEE copyright policy to:
IEEE Intellectual Property Rights Office, copyrights@ieee.org, +1-732-562-3966

Figure 11-2 IEEE Copyright Notice (Page 3 of 3)