ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #35366

Privacy and Security in Pervasive and Ubiquitous Computing

Dr. Abdelrahman Elleithy, William Paterson University

Dr. Elleithy is an Assistant Professor in the Department of Computer Science at William Paterson University, Wayne, New Jersey since September 2017. His research interests include wireless sensor networks, mobile communications and network security. He has published many research papers in international journals and conferences in his area of expertise.

Dr. Elleithy has worked as a Visiting Assistant Professor of Computer Science at Texas A&M University between August 2014 to August 2016 and as a lecturer of the same department from September 2016 to June 2017.

Dr. Elleithy received the BS, MS, and Ph.D. degrees in computer science from the University of Bridgeport in 2007, 2008 and 2013 respectively.

Dr. Elleithy is a member of the technical program committees of many international conferences. He served as a member of the technical program committee of the Annual International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering virtual conferences 2010 – 2014 and the technical program committee of 2016 Annual IEEE Connecticut Conference on Industrial Electronics, Technology & Automation.

Dr. Elleithy is a member of several technical and honorary societies. He is a Member of IEEE, Association of Computing Machinery (ACM), and the honor society of UPE.

Privacy and Security in Pervasive and Ubiquitous Computing

Camila Paulette Murillo Infante, Natalia Zaytseva, Jacob Maizel, Anthony Martinez,
Abdelrahman Elleithy

William Paterson University of New Jersey
Wayne, NJ, USA
murilloc1@student.wpunj.edu, zaytsevan@student.wpunj.edu, maizelj@student.wpunj.edu,
martineza62@student.wpunj.edu, elleithya@wpunj.edu

Abstract— **With ubiquitous computing, individuals are always surrounded by technology, which has become an essential part of their daily routines. Ubiquitous computing, also known as pervasive computing, is a concept where computing is available anytime and anywhere. It is supported using any device, any location, and any format. With technology being intertwined in human lives, the problem arises when we start to discuss the user's privacy and security in pervasive/ubiquitous computing environments. There are many ways in which a user's privacy and security can be at risk. This paper will examine these privacy and security issues and discuss techniques that could solve these problems. Our research results show that the average of finding a pseudonym in our controlled experiment is 0.012694%. With these results, we conclude that the possibility of tracking a single pseudonym consistently in an area of a half square mile is virtually impossible.**

Keywords—Ubiquitous, Privacy, Security, Location Privacy

I. Introduction

One of the significant concerns with technology is data access and availability to other unknown parties. Ubiquitous computing provides access to computational resources anywhere and anytime[1]. This concept can be perceived as an overreach of technology into people's lives. Having surrounding individuals, from the moment they open their eyes in the morning to the second they close their eyes at night, has its pros and cons.

On the bright side, having unlimited access provides insights and information/statistics about the user's daily lives that we could never obtain before. Examples include how many steps a person walks, average heart rate, heart rhythm, or how many deep REM hours. By allowing this information to be gathered on smart devices at home and wearable devices on the body, a person entrusts the service providers with information about their lives' habits, behavior, and interests.

This personal information is valuable to marketing companies, bad actors, and data miners looking to re-sell this information. For example, marketing companies like to see if a person is getting into running to sell them shoes. Bad actors would like to see locations' habits, and data miners want to know what searchers are conducted on Amazon to target clients with ads strategically. Thus, being always connected to the ubiquitous computing environment is an enormous challenge to data privacy.

This paper will examine privacy and security issues then discuss techniques that could solve these problems. There is a problem with the generalized anonymity for location. Within anonymous communications, one person sends data to the recipient, and neither of whom can be traced back to because of the Mix networks' anonymity. This method works with a lower margin of error on a larger scale area, such as a city, but when the area becomes smaller, it is easier to track the sender and recipient. To prevent performance's degradation, an application called a Mix zone is implemented.

II. Problem Identification

With technology becoming so intertwined in human's lives, we have inversely become too dependent on technology. This dependence has exposed us to privacy concerns ranging from the most straightforward information, such as one's name, to having sensitive and personal details of one's life. This information is all stored within cell phones, but with technology, allowing for syncing data across multiple devices within an individual's possession. Information that is stored within one device is available on all other synced devices. Syncing devices comes with many benefits since it is intended to create ease for the user but can allow for the user's information to be exposed if, by chance, one device is compromised.

Bad actors can use the data that they have obtained and steal the user's identity. "Stajano notices that while researchers are busy thinking about the killer applications for pervasive computing, cyber-criminals, and computer villains are already considering new, ingenious attacks that are not possible in traditional computing environments"[2]. Large businesses can use personal information to sell to third party entities such as advertisers. These advertisers would then use personal information and manipulate what the user browsers on the internet.

III. Related Work

The location privacy issue is because location information is collected and stored in the database. Previous research has introduced Mist as a way to address this issue. Mist is a communication infrastructure that aims to preserve privacy in pervasive computing environments[3]. This is achieved by separating location from the identity, allowing authorized users of the system to access services while protecting their location privacy. Pankaj Bhaskar and Sheikh Iqbal Ahamed's research states that Mist works through a privacy-preserving hierarchy of specialized routers that form an overlay network. The network provides private communication by routing packets in a hop-by-hop, handle-based routing protocol[4]. This allows the transmission to be untraceable to any unintended parties.

A. *Identity Privacy*

The issue with identity privacy occurs due to that the user's interaction history is being collected. It is essential that intrusive technology cannot spy on users by tracing them and by recording their acts. Laurent Bussard, Yves Roudier, and Refik Molva state that the solution to this issue is to authenticate entities based on their interaction history, which is made of credentials proving that some interaction occurred[5]. Certification is provided after any exchange to declare what happened in a previous exchange. To support identity privacy, issuers of the credentials should not be able to trace the users by the credentials that were delivered to them, and a credential has to be created in a way that does not allow the issuer to recognize the credential when it is presented[3]. The technique that Laurent Bussard, Yves Roudier, and Refik Molva proposed is to use blind signature mechanisms to ensure that the credentials are untraceable.

B. *Location Privacy*

In today's environment, full of pervasive computing, the user's location is used to power many different services. The location provides much more information than just where the user is located. Past locations' trends can be analyzed and data mined to figure out a frightening amount about the user and their life's details. Companies can easily take advantage of this detailed information and use it to target ads, recommend services, or even sell this information to 3rd party buyers. If this valuable data was somehow intercepted and landed in bad actors' hands, terrible things could happen. Thus, it is crucial to find a solution to protect users' location privacy while still allowing them to utilize the useful services that run off location data, i.e., Google Maps.

One solution to meet this requirement is a concept called Mix Networks and Mixed Nodes. A mix network is a store-and-forward network that offers anonymous communication facilities[6]. The network contains regular messaging routes and has particular Mix nodes that will prevent bad actors from trace the message from source to destination without the mix nodes, even if they can monitor every link in the chain. The mix nodes add a layer of anonymity by collecting n packets, mixing them, and creating unlinkability between incoming and outgoing messages. A Mix zone is a group of users within a spatial region with no application callbacks registered. Within a Mix zone, applications do not receive any user location information, so their identities are mixed. The more people within a Mix zone, the higher the assurance level is that their identities and information are anonymized; this is called the anonymity set. This concept will allow for pseudonyms to be used instead of real names. It will enable people using those pseudonyms to move freely under anonymity without the risk of being meticulously being tracked step by step by their location data.

C. *Information Privacy*

There is an exponential increase in ubiquitous and pervasive sensors being deployed in every walk of life. These systems store information indefinitely. It is more crucial now than it ever has been to set up boundaries to prevent this data from being a privacy nightmare and losing user trust. The information space model is a theoretical model of information spaces. Information space is a semantic structure to create privacy control policies with[7]. Within these systems, the user provides access to bits of the information space to user agents. The agent is software designed to protect the user and deliver to them the information required. The information spaces supply storage for important privacy-related factors. Space has owners with the ability to set information permissions, such as viewing specific information or modifying it.

Three operations can be carried out to resources in information space: Reading and writing, Promotion (the act of making information gathered more accurate) and Demotion (opposite of Promotion), and aggregation, which means combining information to find out more[7]. By using privacy tagging, it allows for more decentralization, as well as the ability to distribute both data and privacy controls to an information space simultaneously. A privacy tag has three parts: a space handle to determine which information space the object in question belongs to, a privacy policy set by space owners, and a privacy policy list showing an object's lifetime stats[7]. The information space model supplies us with a potential solution for the rampant data privacy issues of 2019 by using a permission hierarchy to determine who has access to certain information and preventing people without that permission from gaining access.

IV. Proposed Solution

The most concerning problem is the lack of communication and location privacy between wireless devices. We will be expanding the related works we have come across called *Location Privacy in Pervasive Communication* by Alastair R. Beresford and Frank Stafano and in *Mix Zones: User Privacy in Location-aware Services* by Alastair R. Beresford and Frank Stafano. In their research, they focused on the use of Mix Networks and Mix Nodes "To protect the privacy of our location information while taking advantage of location-aware services"[6].

A. Mix Networks and Mix Nodes

The primary purpose of Mix networks and Mix nodes is to shroud the user in anonymity. This is achieved by having the "Mix node collects n equal-length packets as input and reorders them by some metric before forwarding them"[6]. This network uses communication nodes and blank or dummy nodes, Mix nodes, to interfere with any party trying to get information from the source[6]. This way, communication bounces around *n* nodes in multiple iterations near impossible to trace the source. The Mix nodes act as a buffer to interfere with the trackers and not pinpoint the communication. This works with a user's location, as in a Mix network, the location is bounced from node to node and cannot be pinpointed.

Any information is difficult to single out, and any packets that users send and receive from outside the servers are almost impossible to be traced back to the user. This process makes it nearly impossible for any conceivable method to trace it back to the output source since the mix nodes interfere with anyone or anything trying to pinpoint the source.

B. Pseudonyms and Mix Zones

There is a problem with this generalized anonymity for location. Within anonymous communications, one person sends data to the recipient, and neither of whom can be traced back to because of the Mix networks' anonymity. This method works with a lower margin of error on a larger scale, such as a city, but when the area becomes smaller, such as a mall, it is easier to track the sender and recipient[8]. To prevent this, an application called a Mix zone can be implemented.

Mix zones is a connected spatial region of a maximum size where none of the users are registered for any application callback like alerts or offers[6]. These mix zones would be used along with pseudonyms that hide the identity of the actual recipient. If the user assumes a different pseudonym every time they enter a Mix zone, the zone cannot distinguish one from the other no matter how often they enter and leave. On the other hand, if the Mix zone is larger than the distance it takes for one user to walk in a period between updates, then the anonymity would be broken as the direction the user is taking would indicate their path[9].

Another problem with this is when the user works in a company that must know the user's identity. To solve this, application zones are used. An application zone is an area where applications are registered with a middleware, allowing users to be identified and connected to the area they belong in[8]. As a Mix zone is a large area, it can fit multiple application zones, overlapping and allowing the application zone users to be identified. The outside users that are there, not for that registered zone, are anonymous.

For large areas where there are multiple users in a zone, the extent that a single individual can be tracked is limited. A bad actor can only go so far by knowing that an *n* number of users entered a Mix zone and that an n number of users left. For a bad actor to track any distinct individual, they cannot distinguish one person's path from the other, or even if it was the same person or a third party. However, in a zone where there are fewer users congregated or fewer options for a user to divert into a different direction, like a hallway, then the user can be tracked[8]. After all, people walking down a hallway are unlikely to turn around and go back, so tracking that user from one point to another is relatively easy.

C. *Our Intended Method*

A mix network contains mix nodes, Mix zones, and use pseudonyms. The Mix nodes bounce information, data, communication, and location among an n number of nodes that tracking the user is near impossible. Mix zones allow users not to be identified within a particular area and pairing that with pseudonyms enables users to be anonymous even when logging into some application. By changing the pseudonym with every new mix zone, tracking becomes even more difficult as the user goes through zones.

Statistical models can simulate this type of network layout and show how intricate and difficult it is to track a user. By calculating the number of Mix nodes, the arrangement of the number of packets they transfer, the number of people entering and exiting a Mix zone, and the pseudonyms they used all in one day, the result would show how efficient this technique would be.

V. Mathematical Model

We are using Python's statistical packages as the programming language. With the solution proposed, we base our findings on the population. We will be basing all these calculations on the population densities of the following seven cities of varying population densities; New York, NY, Newark, NJ, Seattle, WA, Los Angeles, CA, Savannah, GA, Chicago, IL, and Nashville, TN.

Variables

The population size, we based on the population density of each city. It was decided that the population density would change from population by a square mile to population by a square half-mile, or 2640 square feet. This was done because of the size that is required of a Mix zone. A Mix zone must be large enough to fit enough of the population, and it must be small enough that someone can walk the whole length of it within one time period. The average human walking speed is around three miles per hour[10], meaning that someone can walk three-fourths of a mile within 15 minutes. Of course, this is assuming that they walk straight through, so we believe that fifteen-minute intervals for a half-mile in a city where people don't just walk through is a good assumption.

Adding to that is the population change. Each square half-mile has a specific population that is always changing every time the zone updates. This means that people come and go from the zone at a certain amount. We assumed that a fifteen-percent change below and above the population density number that we have found would sufficiently simulate people's comings and goings. A range of thirty percent of the population is increasing and decreasing with each time update.

Going along with this is the use of pseudonyms and zones. Ther are Mix zones and application zones. Because of an application zone's nature, it is not meant for any anonymity and is not needed in the calculations. It is assumed that every person has a device that is then connected to the Mix zone under a pseudonym. We also assume that each person possesses a middleware that allows all the applications on their device to share a pseudonym so that there is one pseudonym for each person. We also assume that each person only has one device in which they can be tracked with on their person to make one middleware needed.

Deciding how many Mix nodes depended on how much of the population would be used for each node. The cities with the larger population would have more mix nodes and a smaller mix node influence than the cities with smaller populations. The nodes can only redirect a certain number of communications per node, which is why the number of them is affected by the population. We have then decided that there would be nine mix nodes for every real node to be a useable mix network.

Tables 1 and 2 contain all the information and numbers found and calculated for the mathematical model to work. In Table 1, "Population/sq mi", "population / 0.5 sq mi", and "mix zone population" refer the the populations that we are using for each city. The "Grid area sq ft" refers to the size of influence that each real node has, leading to the "Number of Grids" or the number of nodes in the 0.5 square mile area that is the Mix zone. The "Real Nodes," "Dummy nodes," and "All Nodes" refer to the number of nodes that we will be using in our calculations. In Table 2, "Population" refers to each city's population in the half square mile. The "Nodes" refer to the number of nodes in that area. The "Lower Limit" refers to the fifteen percent below the population's limit to simulate people coming and going from the area. In comparison, the "Upper Limit" refers to the fifteen percent above the limit. The "Range" refers to the population change between those fifteen-percent limits or the thirty-percent population change that we will be using.

To simulate the people entering and leaving cities, we randomized the number of populations within the thirty-percent range that we have decided on before. We use this randomized number to dictate the people for the time update. We then use this randomized population number to randomize the pseudonyms that we will use to simulate one's tracking.

A. Numerical Results

After inputting the variables into the python code and running it, we get Table 3, divided into two because of its size. Table 4 refers to the numbers that we had received when the code was executed. The top row labeled one through 10 refers to the number of times that we had run the code or the number of tests that we have done. Table 4's cells that contain 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10 those columns have the results of "finding" a particular pseudonym in the ones that were examined. The total number of pseudonyms that we created is in the columns labeled 1-all, 2-all, 3-all, 4-all, 5-all, 6-all, 7-all, 8-all, 9-all, 10-all. The "found" pseudonyms refer to the one number that we had set the program to look for in all twelve-time updates. These results, however, do not include the changing of the pseudonyms. We had "found" the pseudonyms that were the same through-out the twelve-time updates, but that is not to say that it is the same pseudonym. Due to the changing nature of the population, and with a new pseudonym being made for each new entry into the Mix zone, the "found" pseudonym does not mean that it found the needed pseudonym. That does not include the nodes that were diverting attention, with multiple nodes containing the same pseudonym as a fake while the real one is much less likely to be found.

Table 4 contains the percentages that each test result ended up being, while the "Total" column contains the averages that each city ended up. In the end, the average overall number of cities for finding a particular pseudonym comes out to be 0.012694% or around 0.013% on average. Statistically, this number means that it is doubtful to get the wanted pseudonym in all the other pseudonyms and nodes, almost to the point that it is impossible to be found.

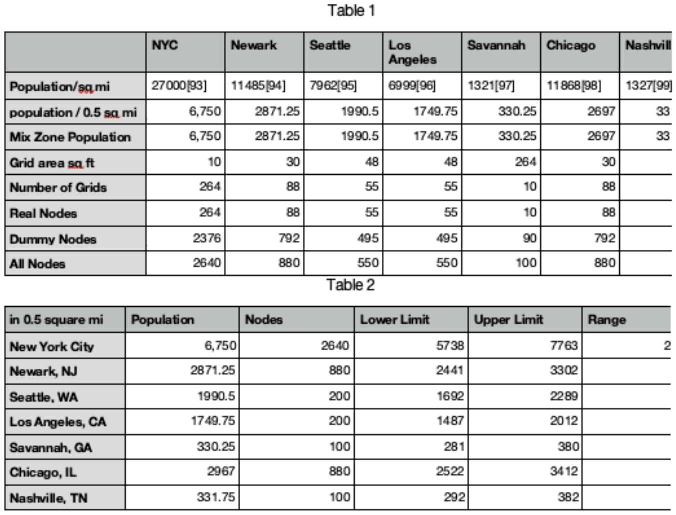

Table 1

	NYC	Newark	Seattle	Los Angeles	Savannah	Chicago	Nashvill
Population/sq mi	27000[93]	11485[94]	7962[95]	6999[96]	1321[97]	11868[98]	1327[99]
population / 0.5 sq mi	6,750	2871.25	1990.5	1749.75	330.25	2697	33
Mix Zone Population	6,750	2871.25	1990.5	1749.75	330.25	2697	33
Grid area sq ft	10	30	48	48	264	30	
Number of Grids	264	88	55	55	10	88	
Real Nodes	264	88	55	55	10	88	
Dummy Nodes	2376	792	495	495	90	792	
All Nodes	2640	880	550	550	100	880	

Table 2

in 0.5 square mi	Population	Nodes	Lower Limit	Upper Limit	Range
New York City	6,750	2640	5738	7763	2
Newark, NJ	2871.25	880	2441	3302	
Seattle, WA	1990.5	200	1692	2289	
Los Angeles, CA	1749.75	200	1487	2012	
Savannah, GA	330.25	100	281	380	
Chicago, IL	2967	880	2522	3412	
Nashville, TN	331.75	100	292	382	

Table 1 and Table 2

Source: Adapted from[11] and[12]

B. *Real World Vs. Controlled Experiment*

What we had done would be classified as a controlled experiment where almost all of the variables were assumed and set by us based on real possibilities. In actuality, it would be much harder to track any pseudonym that the tracker wants. The first thing that is different in the real world was that this experiment did not include the possibilities of large numbers of population changes during various events. An example would be the New Year's Ball Drop in New York City on December 31st. This ball drop attracts the attention of thousands of people, and the population density during that time increases exponentially, especially in an area like times square. Whereas on average, people would be sitting a few feet apart or walking by, in this event, people are standing shoulder to shoulder over a large area. There are an estimated one million people in Times Square during the Ball Drop[17]. This dense number of people in this area would negatively affect the ability to track a certain pseudonym at the time. Then there are the vacations that people go on during the months that school is out, so the population during the summer months fluctuates even more than we used. Any events like a famous Broadway show or a concert for a touring star also affect these numbers.

Another thing we assumed was the number of pseudonyms that each person uses in a Mix zone. This becomes a little more complicated as we assumed that each person uses a middleware application for all their devices, but that is not the norm. Nowadays, almost everyone has multiple devices on their person, each with their one location services. With this, a person can use a middleware service for each device and, assuming that each person has, on average, three devices in total, this means that there would be three pseudonyms for each person. This makes it three times more difficult on average for a tracker to get a pseudonym. All of this is assuming that each person uses a middleware application at all. If a person does not use a middleware application, then a pseudonym is made for each application that requires a location on their phone. Applications like social media, GPS, and search engines would have their pseudonym. This means that each person will have so many more pseudonyms than we assumed. For example, assume that a person has three devices; a phone, a music player, and a fitness watch. Each one has its location service, so that is automatically three pseudonyms right there.

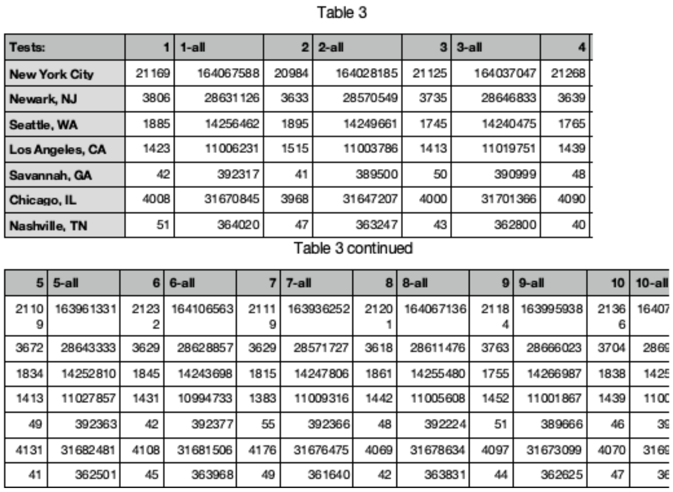

Table 3

Tests:	1	1-all	2	2-all	3	3-all	4
New York City	21169	164067588	20984	164028185	21125	164037047	21268
Newark, NJ	3806	28631126	3633	28570549	3735	28646833	3639
Seattle, WA	1885	14256462	1895	14249661	1745	14240475	1765
Los Angeles, CA	1423	11006231	1515	11003786	1413	11019751	1439
Savannah, GA	42	392317	41	389500	50	390999	48
Chicago, IL	4008	31670845	3968	31647207	4000	31701366	4090
Nashville, TN	51	364020	47	363247	43	362800	40

Table 3 continued

5	5-all	6	6-all	7	7-all	8	8-all	9	9-all	10	10-all
21109	163961331	21232	164106563	21119	163936252	21201	164067136	21184	163995938	21366	16407
3672	28643333	3629	28628857	3629	28571727	3618	28611476	3763	28666023	3704	2869
1834	14252810	1845	14243698	1815	14247806	1861	14255480	1755	14266987	1838	1425
1413	11027857	1431	10994733	1383	11009316	1442	11005608	1452	11001867	1439	1100
49	392363	42	392377	55	392366	48	392224	51	389666	46	39
4131	31682481	4108	31681506	4176	31676475	4069	31678634	4097	31673099	4070	3169
41	362501	45	363968	49	361640	42	363831	44	362625	47	36

Table 3: Source: Adapted from[13] and[14]

A fitness watch would not have many application services needed to keep track of the phone and overall service location. This means that the watch has two pseudonyms. Next would be the music player. No matter what kind, nowadays, most would have at least three location services. One for itself, one for the music library connection, and one for any type of Bluetooth connection. That is another three pseudonyms. Then there is a phone. It also has three connections, one for general location, one for location services, and one for Bluetooth connections. It also has location services for any social media or service engines that each person has. Assume that a person has three social media applications and one search engine application, then the phone has seven pseudonyms. Combining them, this person has twelve pseudonyms. If all people have twelve pseudonyms, then the ability to track a pseudonym becomes twelve times harder.

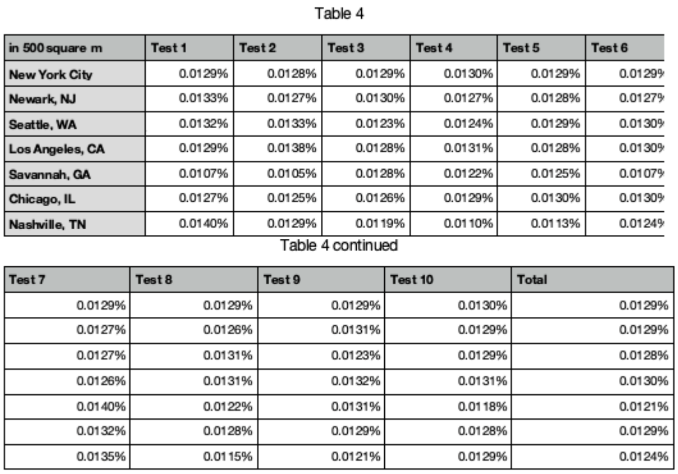

Table 4

in 500 square m	Test 1	Test 2	Test 3	Test 4	Test 5	Test 6	Test 7	Test 8	Test 9	Test 10	Total
New York City	0.0129%	0.0128%	0.0129%	0.0130%	0.0129%	0.0129%	0.0129%	0.0129%	0.0129%	0.0130%	0.0129%
Newark, NJ	0.0133%	0.0127%	0.0130%	0.0127%	0.0128%	0.0127%	0.0127%	0.0126%	0.0131%	0.0129%	0.0129%
Seattle, WA	0.0132%	0.0133%	0.0123%	0.0124%	0.0129%	0.0130%	0.0127%	0.0131%	0.0123%	0.0129%	0.0128%
Los Angeles, CA	0.0129%	0.0138%	0.0128%	0.0131%	0.0128%	0.0130%	0.0126%	0.0131%	0.0132%	0.0131%	0.0130%
Savannah, GA	0.0107%	0.0105%	0.0128%	0.0122%	0.0125%	0.0107%	0.0140%	0.0122%	0.0131%	0.0118%	0.0121%
Chicago, IL	0.0127%	0.0125%	0.0126%	0.0129%	0.0130%	0.0130%	0.0132%	0.0128%	0.0129%	0.0128%	0.0129%
Nashville, TN	0.0140%	0.0129%	0.0119%	0.0110%	0.0113%	0.0124%	0.0135%	0.0115%	0.0121%	0.0129%	0.0124%

Table 4: Source: Adapted from[15] and[16]

VI. Conclusion

Our research results show that the average of finding a pseudonym in our controlled experiment is 0.012694%. This ratio indicates that it is almost impossible to find the pseudonym that of interest to an attacker. This percentage becomes smaller when the time updates change the person who possesses the pseudonym due to them leaving, and another person comes. Practically the number decreases significantly. With other parameters that add to the number of pseudonyms that each person possesses and adds to the number of pseudonyms in an area, this percentage becomes almost negligible. With these results, we can conclude that the possibility of tracking a single pseudonym consistently in an area of a half square mile is virtually impossible.

References

[1] A. Rashid et al., Ubiquitous Data Mining. International Journal of Creative Research Thoughts, vol 6, Issue 2, April 2018.

[2] F. Stajano, Security for Ubiquitous Computing: Halsted Press, 2002.

[3] Campbell, J. Al-Muhtadi, P. Naldurg, G. Sampemane, M. D. Mickunas, "Towards Security and Privacy for Pervasive Computing," Proceedings of International Symposium on Software Security, 2002.

[4] Pankaj Bhaskar and Sheikh Iqbal Ahamed. 2007. Privacy in Pervasive Computing and Open Issues. In Proceedings of the Second International Conference on Availability, Reliability, and Security, ARES 2007, The International Dependability Conference - Bridging Theory and Practice. 147–154.

[5] L. Bussard, Y. Roudier, R. Molva, "Untraceable secret credentials: trust establishment with privacy," Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, 14- 17 March 2004, pp.122-126.

[6] A. R. Beresford, F. Stajano, "Location Privacy in Pervasive Computing," Pervasive Computing, IEEE, Volume 2, Issue 1, Jan-Mar 2003, pp. 46-55

[7] J. Xiaodong, J. A. Landay, "Modeling privacy control in context-aware systems," Pervasive Computing, IEEE, Volume 1, Issue 3, July-Sept. 2002, pp. 59-63.

[8] A. R. Beresford, F. Stajano, "Mix Zones - User Privacy in Location-aware Services," International Workshop on Pervasive Computing and Communication Security, IEEE, Mar 2004.

[9] A.Pfitzmann, M. Köhntopp (2001) Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology. In Federrath H. (eds) Designing Privacy Enhancing Technologies. Lecture Notes in Computer Science, vol 2009. Springer, Berlin, Heidelberg.

[10] E. Cronkleton, "Average Walking Speed: Pace, and Comparisons by Age and Sex." Healthline, Healthline Media, March 14th. 2019, www.healthline.com/health/exercise-fitness/average-walking-speed.

[11] New York City Population. (2019-07-07). Retrieved 2019-12-14, from http://worldpopulationreview.com/us-cities/new-york-city/

[12] Newark Population. (2019-10-29). Retrieved 2019-12-14, from http://worldpopulationreview.com/us-cities/newark/

[13] Socrata. "Population Density of Seattle, WA. "Open Data Network, www.opendatanetwork.com/entity/1600000US5363000/Seattle_WA/geographic.population.density?year=2017.

[14] Los Angeles Population. (2019-10-29). Retrieved 2019-12-14, from http://worldpopulationreview.com/us-cities/los-angeles/

[15] Socrata. "Population Density for Chicago, IL."Open Data Network, www.opendatanetwork.com/entity/1600000US1714000/Chicago_IL/geographic.population.density?year=2017.

[16] Nashville Population. (2019-10-29). Retrieved 2019-12-14, from http://worldpopulationreview.com/us-cities/nashville/

Admin. "Times Square NYE." *Times Square NYE | Times Square NYC*, April 7th. 2017, www.timessquarenyc.org/times-square-new-years-eve.