COMPARISON OF PRIVACY SCHEMES IN A MULTI-RADIO VANET

A Thesis

presented to

the Faculty of California Polytechnic State University,

San Luis Obispo

In Partial Fulfillment

of the Requirements for the Degree

Master of Science in Computer Science

by

Collin Kenner

December 2019
COMMITTEE MEMBERSHIP

TITLE: Comparison of Privacy Schemes in a Multi-Radio VANET

AUTHOR: Collin Kenner

DATE SUBMITTED: December 2019

COMMITTEE CHAIR: Bruce DeBruhl, Ph.D.
Professor of Computer Science

COMMITTEE MEMBER: Theresa Migler-VonDollen, Ph.D.
Professor of Computer Science

COMMITTEE MEMBER: Hugh Smith, Ph.D.
Professor of Computer Science
Intelligent vehicles are rapidly improving in functionality as they improve upon and incorporate new technologies. The addition of networking capabilities grants vehicles significant knowledge about the location and decisions of vehicles in the surroundings, and allows them to share perception information. However, adversarial listeners in the system may track vehicles by their communications resulting in a loss of user privacy. Past research has attempted to minimize privacy loss in single-radio environments through pseudonym changing schemes. We improved upon this research by comparing pseudonym schemes in a multi-radio environment.

Our simulation environment was created using the OMNeT++ networking and SUMO traffic simulators, with the Veins framework as an intermediary between the two. The OMNeT++ network software was extended using the INET framework to model WiFi traffic. This simulator was configured to test a variety of configurations for listener coverage and vehicle density. The data showed that the density-based privacy scheme offered improvement over the baseline timeout performance, while the blackout scheme posed no advantages.
ACKNOWLEDGMENTS

My thanks to:

- Joey Wilson for helping me to accomplish this surprisingly large endeavor. Your help and insights were of the utmost importance on all aspects of this project. You were an absolutely great teammate bro!

- My parents Brian and Kathleen who helped me to buckle down and focus when I was feeling discouraged, and went out of their way to let me use their home servers to host and view my data.

- Dr. Debruhl for keeping me motivated and providing me all of the resources I needed to gather data and develop ideas.

- My grandparents for letting me live with them and feeding me, so I was able to focus on school.

- All my friends who helped me throughout college.

- Andrew Guenther, for creating this template
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIST OF TABLES</td>
<td>x</td>
</tr>
<tr>
<td>LIST OF FIGURES</td>
<td>xi</td>
</tr>
<tr>
<td>CHAPTER</td>
<td></td>
</tr>
<tr>
<td>1 Introduction</td>
<td>1</td>
</tr>
<tr>
<td>2 Background</td>
<td>3</td>
</tr>
<tr>
<td>2.1 Intelligent Vehicle Definition</td>
<td>3</td>
</tr>
<tr>
<td>2.2 VANETS</td>
<td>5</td>
</tr>
<tr>
<td>2.2.1 VANET Overview</td>
<td>5</td>
</tr>
<tr>
<td>2.2.2 Security and Privacy</td>
<td>6</td>
</tr>
<tr>
<td>2.2.3 Pseudonym Certificates</td>
<td>6</td>
</tr>
<tr>
<td>2.2.4 Limitations of DSRC and Pseudonyms</td>
<td>7</td>
</tr>
<tr>
<td>2.2.5 Multi-Radio Protocol Awareness</td>
<td>7</td>
</tr>
<tr>
<td>3 Related Works</td>
<td>8</td>
</tr>
<tr>
<td>3.1 Agent Models and Game Theory</td>
<td>8</td>
</tr>
<tr>
<td>3.2 Existing Pseudonym Schemes</td>
<td>9</td>
</tr>
<tr>
<td>3.2.1 Timeout</td>
<td>9</td>
</tr>
<tr>
<td>3.2.2 Blackout</td>
<td>9</td>
</tr>
<tr>
<td>3.2.3 Density</td>
<td>10</td>
</tr>
<tr>
<td>3.2.4 Random Pseudonym Change</td>
<td>10</td>
</tr>
<tr>
<td>3.2.5 Synchronous Change Protocol</td>
<td>10</td>
</tr>
<tr>
<td>3.3 Defensive Model</td>
<td>11</td>
</tr>
</tbody>
</table>
4 Design
   4.1 Goal
   4.2 Requirements
   4.3 Simulation Parameters and Protocol Configuration
      4.3.1 Timeout
      4.3.2 Blackout
      4.3.3 Density
      4.3.4 Randomized Timeout
   4.4 Simulator Design
   4.5 Increased Computational Requirements
5 Implementation
   5.1 Simulator
      5.1.1 SUMO
      5.1.2 Randomizing Maps
      5.1.3 OMNeT++
   5.2 Network Model
      5.2.1 Mobility Sharing
      5.2.2 Radio Mediums and Loss Models
      5.2.3 Logging
      5.2.4 Analysis and Data Configuration
   5.3 Simulation Configurations
      5.3.1 Defensive implementations
      5.3.2 Timeout
      5.3.3 Blackout
      5.3.4 Density
5.3.5 Defensive Values ........................................ 33

5.4 Summary and Measure of Success ........................... 34

6 Error and Data Normalization ................................. 35

6.1 Data Normalization and Loss ............................... 35

6.1.1 Dataloss in the Attack .................................. 35

6.1.2 Normalization Reasoning ............................... 36

7 Analysis ......................................................... 38

7.1 Metrics Summary by Scheme ............................... 38

7.2 Timeout ....................................................... 40

7.2.1 Precision .................................................. 41

7.2.2 Recall ...................................................... 45

7.2.3 F1 .......................................................... 48

7.2.4 Associations .............................................. 52

7.2.5 Tradeoffs .................................................. 55

7.3 Density ......................................................... 56

7.3.1 Precision .................................................. 57

7.3.2 Recall ...................................................... 58

7.3.3 F1 .......................................................... 63

7.3.4 Associations .............................................. 64

7.3.5 Tradeoffs .................................................. 65

7.3.6 Blackout ................................................... 66

7.3.7 Precision .................................................. 67

7.3.8 Recall ...................................................... 69

7.3.9 F1 .......................................................... 72

7.3.10 Associations ............................................. 72
7.3.11 Tradeoffs ................................................. 74
7.3.12 Baseline Performance ............................... 74
7.4 Comparison ............................................... 75
8 Future Works ................................................ 82
  8.1 Simulator ................................................ 82
  8.2 Network Modeling ....................................... 82
  8.3 Data Collection ......................................... 83
9 Conclusion .................................................. 84
APPENDIX
  A .......................................................... 92
  A.1 Machines ............................................... 92
  A.2 Timeout ............................................... 93
  A.3 Blackout .............................................. 95
  A.4 Density ................................................ 98
# LIST OF TABLES

<table>
<thead>
<tr>
<th>Table</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.1</td>
<td>Timeout Scheme Variable Periods</td>
</tr>
<tr>
<td>4.2</td>
<td>Blackout Scheme Silence Duration</td>
</tr>
<tr>
<td>4.3</td>
<td>Density Scheme Vehicle Requirement</td>
</tr>
<tr>
<td>5.1</td>
<td>Simulator Versions</td>
</tr>
<tr>
<td>5.2</td>
<td>Mobility Coordinate Systems</td>
</tr>
<tr>
<td>5.3</td>
<td>Environmental Configurations for Each Defensive Scheme</td>
</tr>
<tr>
<td>7.1</td>
<td>Terminology for Simulation Result Analysis</td>
</tr>
<tr>
<td>A.1</td>
<td>Physical and Virtual Machine Information</td>
</tr>
</tbody>
</table>
LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1</td>
<td>On-board Vehicle Radio Protocols and Ranges</td>
<td>1</td>
</tr>
<tr>
<td>2.1</td>
<td>Society of Automotive Engineers (SAE) Automation Levels [1]</td>
<td>4</td>
</tr>
<tr>
<td>4.1</td>
<td>Single Simulation Flow</td>
<td>14</td>
</tr>
<tr>
<td>4.2</td>
<td>MultiRadio Vehicle Network Description File</td>
<td>18</td>
</tr>
<tr>
<td>4.3</td>
<td>Simulator Configuration</td>
<td>19</td>
</tr>
<tr>
<td>4.4</td>
<td>Sample Size Comparisons for Result Distributions</td>
<td>21</td>
</tr>
<tr>
<td>4.5</td>
<td>Script Flowchart for Simulation Automation</td>
<td>22</td>
</tr>
<tr>
<td>5.1</td>
<td>Map Translation to SUMO</td>
<td>25</td>
</tr>
<tr>
<td>5.2</td>
<td>Listener Configurations in Simulation</td>
<td>31</td>
</tr>
<tr>
<td>5.3</td>
<td>Node Traffic During Simulation</td>
<td>33</td>
</tr>
<tr>
<td>6.1</td>
<td>Overview of Loss for Different Listener Configurations</td>
<td>37</td>
</tr>
<tr>
<td>7.1</td>
<td>Timeout Scheme Dataset Heatmap</td>
<td>40</td>
</tr>
<tr>
<td>7.2</td>
<td>Timeout Scheme W2D Average Precision</td>
<td>42</td>
</tr>
<tr>
<td>7.3</td>
<td>Timeout Scheme D2D Average Precision</td>
<td>43</td>
</tr>
<tr>
<td>7.4</td>
<td>Timeout Scheme Average W2D Precision for Variable Listeners</td>
<td>44</td>
</tr>
<tr>
<td>7.5</td>
<td>Timeout Scheme Average D2D Recall</td>
<td>45</td>
</tr>
<tr>
<td>7.6</td>
<td>Timeout Scheme Average W2D Recall</td>
<td>46</td>
</tr>
<tr>
<td>7.7</td>
<td>Timeout Scheme Average Recall for Variable Listeners</td>
<td>47</td>
</tr>
<tr>
<td>7.8</td>
<td>Timeout Scheme Average D2D F1</td>
<td>49</td>
</tr>
</tbody>
</table>
7.34 1 Year Theoretical and Average predicted pseudonym Usage . . . . 79
7.35 Guessed Associations across all Schemes and Defensive Values . . 79
7.36 Guessed Associations over Total Pseudonyms . . . . . . . . . . . 80
7.37 Correct Associations across all Schemes and Defensive Values . . 81
A.1 Timeout W2D Recall for Variable Listeners . . . . . . . . . . . . . 93
A.2 Timeout W2D F1 Score for Variable Listeners . . . . . . . . . . . 94
A.3 Blackout Precision for Variable Listeners . . . . . . . . . . . . . 95
A.4 Blackout Recall for Variable Listeners . . . . . . . . . . . . . . . 96
A.5 Blackout F1 Score for Variable Listeners . . . . . . . . . . . . . 97
A.6 Density W2D Recall for Variable Listeners . . . . . . . . . . . . . 98
A.7 Density W2D F1 Score for Variable Listeners . . . . . . . . . . . 99
A.8 Density D2D F1 Score for Variable Listeners . . . . . . . . . . . 100
As intelligent technology begins to extend into our lives in more complete and invasive ways, the benefits are often mitigated by the risk of privacy exposure. Smart vehicles are not an entirely new phenomena, but despite several years the field is still under development. One of the largest questions facing designers is how to allow vehicles to act as entities on roads and make intelligent driving decisions based upon awareness of the surrounding world. Designers are forced to balance the performance of the vehicles with the privacy vehicles extend to users.

Malicious entities may attempt to track vehicles via Vehicle to Vehicle (V2V) mediums like Dedicated Short Range Communication (DSRC). In order to minimize the effectiveness of these attacks, many different approaches and systems have been designed. These systems focus primarily on components of V2V communication where vehicles broadcast information including location, direction, and speed. However, as more
radio devices are incorporated into vehicles, defenses need to account for the added vulnerability. A vehicle may be equipped with both Wifi and Bluetooth in addition to DSRC, and the majority of drivers also carry a smartphone while driving. Therefore, the actual range of wireless communication around a vehicle may be similar to what is seen in figure 1.1. While many defensive pseudonym have been proposed, their effectiveness in multi-radio environments is still relatively unexplored.

In this paper, we measure the performance of existing pseudonym privacy schema in a simulated multiradio Vehicular Ad Hoc Network (VANET), in addition to several modified schema. We then use the results to optimize schema configuration in vehicles operating with multiple radio protocols. As a means of measuring this performance, experiments were run using the OMNeT++ network simulator [2] and Simulation of Urban Mobility (SUMO) [3] traffic simulator with VEINS [4] as a bridge between the simulators. Each vehicle in the simulator broadcast over one DSRC device and a variable number of WiFi devices. The resulting network traffic was then processed using a multi radio attack [5] to determine the performance of each schema.

Chapter 2 of the paper covers the current approaches to intelligent vehicle design, the inclusion of vehicle communication through DSRC, and the limitations and defensive methods currently being considered for the system. In chapter 3, we explain design of the experimental design, defensive schemes, goals, and requirements, and in chapter 4 the system design, testing setup, and configuration for the simulator and vehicle network model are explained. The results of the experiments are analyzed in chapter 5, and the conclusions and future work are included in chapters 6 and 7.
Chapter 2

BACKGROUND

2.1 Intelligent Vehicle Definition

Although people have been developing driverless vehicles for nearly a century, testing methodologies as simple as radio controlled vehicles[6, 7], recent technological advancements in computation power and artificial intelligence have made fully autonomous vehicles much more feasible. The NHTSA breaks driving automation into 5 different levels where level 0 represents no driving automation in the vehicle, and level 5 represents a fully autonomous vehicle. At each level, the amount of required driver participation decreases. This can be seen in figure 2.1 from the NHTSA. They define fully autonomous to be the sustained and unconditional performance by an Automated Driving System(ADS) of the Dynamic Driving Task(DDT) or DDT fallback without any expectation that a user will respond to a request to intervene [8]. These definitions have set a firm standard of functionality that must be met by any evolving technology. There are multiple facets to this, vehicles must be able to make optimal decisions regarding the path they will take. They also need to have awareness of the surrounding world including other vehicles, pedestrians, and obstructions in the road. Utilizing this information, vehicles must make decisions to reach the destination while protecting both the safety of the driver and the people in the vicinity.

2.1.1 Evolution of Intelligent Vehicles

Recent years have seen a large increase in interest in the field of intelligent transportation systems(ITS). Autonomous vehicles(AV) may provide significant benefits
including independent mobility for non drivers like the elderly, reduced traffic congestion and parking demand, increased traffic safety, energy conservation, and pollution reduction [9].

Despite constant improvement in the transportation system, there are as many as 5.5 million crashes annually and over 100 billion dollars lost due to congestion [10]. Human driving skills and behaviors have become more regulated over the years through legislation, but small instances of human error or negligence can have drastic consequences. AV’s do not suffer as much from the limitations of human negligence. However, AV’s also possess several technical restrictions that must be dealt with for ideal implementation. Despite fast computation speeds, vehicle decision making still relies on the vehicles perception of the surrounding world. Current vehicle sensors can be broken down into active sensors such as Light Detection and Ranging (Lidar) and Radio Detection and Ranging (Radar), and passive sensors such as cameras [11].

In addition, vehicle decision making is often focused on threat assessment of incoming sensor input, path planning, and prediction. An extremely conservative vehicle driving slowly increases safety, but it will also likely reduce driving efficiency [12].

Figure 2.1: Society of Automotive Engineers (SAE) Automation Levels [1]
Therefore, vehicles operate the best in predictable environments where all vehicles are following the same operating rules. If a human element exists within the system, the vehicles must now account for inherently unpredictable behavior which decreases the safety of the system.

2.2 VANETS

2.2.1 VANET Overview

A Vehicular Ad Hoc Network (VANET) is a type of Mobile Ad Hoc Network (MANET). In a MANET there is no network infrastructure, and the network is continuously self-configuring. Nodes form temporary networks where they behave as both routers and endpoints [13]. Connections are created when vehicles are within communication range of each other and messages may be propagated through shared vehicle connections. In a VANET, both vehicles and roadside units operate as components of the network with V2V and Vehicle to Roadside (V2R) communications through DSRC. This information can be broken down into routine safety messages that include status information required for surrounding vehicles to make predictions about the movements of the sender, and event safety messages that indicate a break from the predictable routine behavior [14]. These safety messages provide vehicles with greater awareness of the surrounding road network. Rather than only reacting to sensor input provided, vehicles are also able to better predict the behavior of other entities.
2.2.2 Security and Privacy

Like any network, a VANET must deal with security and privacy. VANETS are susceptible to several attacks including Denial of Service (DOS), Black Hole, and Distributed Denial of Service (DDOS) [15]. While problematic in other networks, these attacks have the potential to be lethal in a driving situation where the vehicles are relying on the information to make decisions. Attackers need to be quickly isolated and removed from the network to prevent further damage. In this paper, we focused on attacks that center around eavesdropping, and we aimed to track vehicle movement within the network. Eavesdropping attacks occur when passive listeners throughout the network receive the security broadcasts of vehicles and use them to infer information about specific vehicle location and driving patterns [16]. One of the ways this is accomplished is through associating a type of signing certificate called a pseudonym with a vehicle.

2.2.3 Pseudonym Certificates

A pseudonym certificate is provided to vehicles, enabling them to operate safely, with disguised identity or pseudonymity, and location privacy. A vehicle will be given multiple valid certificates at any time through a trusted third party certificate authority (CA), so that it can switch certificates as often as is required. Each vehicle is given around 3,000 of these certificates for a 3 year period [17], but may request more if needed.

These pseudonyms function for multiple components of the V2V and V2R communication. They include public keys to be provided to receiving vehicles, verifying both the content and sender, psuedonymity, location privacy, and revocation using a Certificate Revocation List (CRL) [17].
2.2.4 Limitations of DSRC and Pseudonyms

The privacy provided by pseudonyms depends on how they are applied. Attackers targeting vehicular paths and identities will try to utilize safety information broadcast by a vehicle to associate past and current pseudonym certificates. An attacker trying to deanonymize a pseudonym will monitor network traffic in its region and link changed pseudonyms using the vehicle speed, direction, and location. This new pseudonym can then be linked to information gathered by other listeners to infer information about a vehicle’s route, and shared for any purpose. The protection afforded by changing pseudonyms occurs either when multiple vehicles are in close proximity and traveling in a similar direction or not within range of a listener. Changing pseudonyms in a group of vehicles forces an attacker to guess which new pseudonym is associated with the previous vehicle-specific pseudonym. Alternatively, changing outside a listening zone disconnects the vehicle from the last pseudonym that was seen by a listener.

2.2.5 Multi-Radio Protocol Awareness

In this paper, we expanded upon the evaluation of current vehicular network protocols to measure performance as the networks and surroundings become more complex through additional radio protocols. Given the above limitations on DSRC, there is a tradeoff between privacy and schema complexity, and we attempted to identify an optimal balance.
In this project, we expand both on the behavior of agents in an adhoc network, and the pseudonym protocols for optimal privacy. Vehicular agents must deal both with existence of passive listeners, and the existence of malicious agents in the network [18]. Recent works have shown methodologies for reduction of track-ability by use of caravaning where vehicles drive together in groups [19]. Vehicles do this by maintaining a short fixed distance as well as a predefined speed and direction. Sampigethaya et al. found that the necessity to broadcast data in a platoon is decreased, allowing for extended periods of silence. Lu et al. attempted to utilize preassigned social spots (PCS) to create mix zones where vehicles could change with other vehicles reducing the number of ineffective pseudonym changes that occur. Each of these more comprehensive systems targets the linkability of vehicle pseudonyms by attempting to confound an attacker’s ability to isolate a single vehicle. The following schemes were examined within the bounds of a single radio vehicle environment, but are unexplored within the bounds of a more complex radio network.

3.1 Agent Models and Game Theory

The advantage of a pseudonym change is maximized when done in a group or concurrently with multiple nearby vehicles. In his thesis, Nicholas Plewtong explored the cost of a vehicle changing pseudonyms without a surrounding group [21]. He treated mix zones as regions where vehicles may opt to participate and change their pseudonym. He found that as the cost of a pseudonym change increases, a vehicle
is less likely to participate in a pseudonym change. He also found that if vehicles which behave maliciously exist in the system, they will likely avoid participation in pseudonym change zones. Therefore, the expected benefit in these zones is lowered or lost entirely.

3.2 Existing Pseudonym Schemes

3.2.1 Timeout

The Timeout or periodic time change protocol is one of the simplest pseudonym changing methodologies, and revolves around changing pseudonyms at fixed time intervals. There is also an extended version of this protocol where the change strategy receives time slot specific pseudonyms[22] enabling a more synchronized pseudonym change. Eckhoff et al. attempted to build on this concept by allowing vehicles to swap pseudonyms with surrounding vehicles. He found that the mix of synchronous change periods and pseudonym swapping increased the privacy for nodes in close proximity.

3.2.2 Blackout

In the blackout protocol, considered in AMOeba[23], a vehicle enters a silent period where it does not broadcast any information following a pseudonym change. In this protocol, the silent period is some predefined amount of time used to reduce the trackability of the pseudonyms. An advantage of this schema is that it reduces an attacker’s ability to determine a vehicle’s pseudonym using predicted location from previous location, speed, and direction broadcasts. However, it also introduces a trade-off in safety, as the silent period can increase risk when vehicles are not communicating.
3.2.3 Density

The goal of a density-based-protocol is to reduce the likelihood that a vehicle will change it’s pseudonym when it is alone. Chaurasia and Verma explored how vehicles changing pseudonyms when in the vicinity of other vehicles improve their privacy. [24]. The concept relies on the requisite behavior that all vehicles are operating using the same precepts, and assumes that all vehicles within a sufficiently dense grouping of vehicles are likely to change their pseudonyms. If a vehicle enters a dense vehicle group inside a listening zone and changes pseudonyms, the link-ability of the vehicles may be reduced since a larger number of vehicles with similar coordinates, speed, and direction will can changed at the same time. A vehicle entering a dense grouping between mix zones could also trigger a change in pseudonyms, effectively reducing the ability to track the vehicle to the next listening zone.

3.2.4 Random Pseudonym Change

The random pseudonym change schema is an alternative to the periodic change model, which increases variability by randomizing time duration between pseudonym changes [25]. Pan et al. was able to probabilistically determine the likelihood of simultaneous pseudonym changes based upon the age of neighboring vehicles pseudonyms. In addition, he quantified the location privacy utilizing these probabilities.

3.2.5 Synchronous Change Protocol

A synchronous change protocol requires local vehicles to cooperate to simultaneously change pseudonyms when a minimum number of surrounding vehicles desire a change [22]. In this way, the protocol is reflective of the density based protocol. It reduces
the link-ability of pseudonyms within a particular listening zone by increasing the number of possible pseudonyms to associate. There are two primary weaknesses of this schema. An adversarial vehicle could broadcast a desire to change, but opt to not do so resulting in only the receiving vehicles changing pseudonyms. This issue could be addressed by adding a reputation component to the network where vehicles are assigned reputation based upon the reliance of their activity within the network [26]. The other limitation of a synchronous change protocol is the additional cost in network bandwidth.

3.3 Defensive Model

There already exist several surveys that examine the performance of many of these schemes within a single radio system [27, 28]. These works provide plenty of coverage of the privacy and defensive value of these schemes within a single radio system. Therefore, we attempt to build on this concept by exploring how defensive schemes perform when multiple radios exist in the network.
In the following chapter we explain the design of the defensive vehicle network where we test the different pseudonym schema. This includes the implementation of each of the defensive protocols that were used. We also outline the goals of the simulation, targets for the results, and the requirements for the defensive protocol to be successful.

4.1 Goal

The goal of our system is to mitigate an attacker's ability to derive pseudonyms from multiple Basic Safety Message (BSM) broadcasts and secondary radio traces. There are two types of changes that are considered when doing this. Pseudonym changes within the vicinity of listeners or listening zones and changes outside listening zones. Changes inside listening zones can be linked by attackers and thus the goal of privacy protocol is to minimize a vehicle's exposure by changing pseudonyms in conjunction with as many vehicles as possible [24]. Alternatively, vehicles may change pseudonyms within mix zones which fall outside of listener areas [29].

4.2 Requirements

Here we outline the system requirements for the simulator and testing model. There were several requirements to be considered:

- Cars should be modular and the system should support both single radio operation and multiple radio operation 4.4.
• system should allow for additional radio protocols to be added as needed.
• system should allow the addition of pseudonym schema that can be used to mitigate D2D associations.
• system should allow for the simulation of packet loss and radio interference for DSRC and WIFI protocols.

When picking defensive schema to test, we opted for models that had the potential to target components of the attack that were used previously [5]. Passive listeners are used to gather information about the vehicles passing between them and all vehicle information is stored to attempt to create associations between pseudonyms used. Similar attack concepts can be seen utilizing probabilistic association to determine the likelihood vehicle pseudonyms are associated [29, 30] where attackers explore given exit and enter events and determine the probability that a given vehicle entering a listening zone is the same vehicle that exited a different listening zone.

The first component of the attack attempts to link just pseudonyms by using association/disassociation. If pseudonyms are seen in different locations at the same time, it is assumed that they were disassociated. If a pseudonym was seen shortly after another pseudonym disappeared, it is assumed that the pseudonym is probably associated. Attempts to match observation zone exit and enter events are done to associate pseudonyms. Targeting this component of the attack was done by capitalizing on the fact that possible associations are ignored. Therefore, by reducing the number of positive associations that occur the success rate of this stage of the attack is reduced. To do this, we selected attacks that appear to break the conditions that are searched for. This criteria was met by the Density, Blackout, and Synchronous schemata. In addition, because the attack models all pseudonym associations as a matrix any new pseudonym that joins the system outside a listening zone will have no initial D2D associations. Therefore, the Timeout schema was also considered since it can enable changes outside listening zones.
The second component of the attack attempts to link Mac address to pseudonyms. Similar to the first component, associations are modeled using a matrix. However, in this part of the attack, the likelihood of an association is treated as a probability. Initially these probabilities were initialized to $\frac{1}{N+1}$ where $N$ is the number of possible identifiers, and it then uses boosting to determine which Wifi addresses are likely to be associated. Here we primarily targeted the linkability between listening zones. By increasing the number of pseudonyms that a Wifi address can be linked to we aim to decrease the probability that any pseudonym can be linked.

Figure 4.1: Single Simulation Flow
4.3 Simulation Parameters and Protocol Configuration

When simulating each of the defensive schemas, the goal was to try to examine a diverse running environment. Because of the time cost in data gathering, the number of environmental simulation parameters that we could change was somewhat minimal. In a realistic environment the operational map, protocol broadcast frequencies, and number of radios in the vehicle may differ from what we simulated with. We decided to focus primarily on two factors, vehicle density and quantity of listeners. Vehicle density was chosen because of the importance of more than one vehicle changing pseudonyms within a given time frame. If a vehicle was offered greater privacy by a simultaneous change, it would follow that a larger number of vehicles on the road would increase the likelihood that a change is done simultaneously and thus increase the privacy. The second consistent variable in simulation was the number of listeners. Our goal was to see how increasing the number of spaces in the map that are being eavesdropped on increases or decreases the success of the attack.

4.3.1 Timeout

When simulating the Timeout scheme, we opted to try to get a variation in the performance of different time periods. Specifically, we were interested in if increasing the frequency of changes increases privacy. When a vehicle is changing pseudonyms more frequently, the likelihood that the vehicle changes outside a region that is being listened to increases. Because the increased usage of pseudonyms adds overhead to the vehicle and the certificate authority an ideal performance in this protocol would be one that maximizes privacy while minimizing the number of changes needed. Therefore, in addition to the small time deltas we tested we also tested several incrementally larger deltas to see how vast the difference in privacy was.
Table 4.1: Timeout Scheme Variable Periods

<table>
<thead>
<tr>
<th>Timeout(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
</tr>
<tr>
<td>60</td>
</tr>
<tr>
<td>120</td>
</tr>
<tr>
<td>300</td>
</tr>
<tr>
<td>600</td>
</tr>
</tbody>
</table>

4.3.2 Blackout

The blackout scheme was more of an addition to the existing timeout scheme. We picked a fixed timeout delta and tested several varying silence periods after each change. These silence periods varied from very small to several broadcast periods. Our goal with these varying periods to allow vehicles changing near the edges of listening zones a measure of anonymity that might only have otherwise been achieved if they changed outside the listening zone.

Table 4.2: Blackout Scheme Silence Duration

<table>
<thead>
<tr>
<th>Blackout(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>15</td>
</tr>
</tbody>
</table>

4.3.3 Density

In the density scheme, computational requirements really limited our ability to run realistic simulations. A typical vehicle driving along a busy roadway may be surrounded by a large number of vehicles. However, since the simulator has to process the sending/receiving of every single transmission for both the sending and receiving vehicles, we were limited in our ability simulate large vehicle densities. This meant that density requirements that exceeded 5 vehicles may happen very infrequently. To account for this when using this scheme by requiring small numbers of surrounding vehicles to trigger a change. This may negatively affect the performance of this scheme since less vehicles are changing in a group.
4.3.4 Randomized Timeout

Similar to Blackout we tested this scheme more as an extension of Timeout rather than an independent scheme. By randomizing the timeout delta we expected to limit the predictability of pseudonym changes. We pick a maximum and minimum delta to prevent consistent and immediate changes and changes that are too long to be useful. When a pseudonym change occurs, a new delta will be selected between the minimum and maximum values.

4.4 Simulator Design

To test our multiradio schema we utilized a previously developed attack [5]. The attack takes a collection of DSRC and WIFI packets in a MongoDB collection as an input. These packets are read out and compared against an array of coordinates that represent listener locations to build a set of associations, possible associations, and disassociation’s for DSRC and WIFI.

In order to generate these packets we wanted to simulate network traffic as realistically as possible. To build on this we wanted to be able to model not just the existence of protocols within the network, but their behavior. This needed to include some packet structure, radio interference, collisions, and loss. The optimal simulator for these requirements was OMNet++ [2]. It was an open source simulator that included support for the projects required to model both Wifi and DSRC network stacks through INET [31] and Veins [4] respectively.
OMNet++ is a discrete event simulator based upon the Eclipse IDE [32]. The simulator uses Network Description (NED) files to define both network topology and component behavior. These description files allow for dynamic network topologies like VANETS by modeling network devices, components, and environments. Additionally, NED files model distance and location within each module. Each component within a NED file has a position within the “space” of that component. OMNet++ projects build on this by utilizing mobility modules which control how a node moves throughout the space. These network position and mobility values are used to calculate loss and interference of the packets between nodes. The network description file in figure 4.2 shows the multiradio vehicle with both network stack components, and the mobility component for DSRC.

![MultiRadio Vehicle Network Description File](image)

**Figure 4.2: MultiRadio Vehicle Network Description File**

The DSRC network stack was simulated through Vehicle in Network Simulation (Veins). Veins is a simulation framework that includes all of the required lower level protocol, radio models, and hardware to simulate DSRC communication [33]. It
communicates with SUMO using a TCP connection to model vehicle behavior and network activity as they drive. In addition, Veins provides Road Side Units (RSU’s) that can be modeled in whatever way is needed.

Utilizing Veins to simulate the DSRC traffic provided us with an additional benefit. Because Veins works with SUMO, we were able to use SUMO in a similar fashion to the original attack to generate traffic. Previous works took a generated SUMO map and generated WiFi and DSRC broadcasts at fixed time intervals. These recorded "packets" were then filtered out if further than a minimum distance from listeners. The remaining packets were saved and used as an input to the attack. The Veins/OMNeT++ simulation similarly took a generated SUMO map, and simulated DSRC network traffic using obstacle and distance based loss algorithms. The goal of the simulation was to reach as close to a realistic behavior as possible. We were able to leverage the random traffic generator functionality within SUMO to build pseudo

**Figure 4.3: Simulator Configuration**
non-deterministic traffic flow. By combining this with the ability to pick the spawning frequency of vehicles within the simulation we were able to achieve relatively dense traffic patterns.

Similar to Veins, INET is a simulation framework designed to simulate many of the protocols found in the internet stack [31]. It also possesses the capability to model both wired and wireless link layer protocols. It possesses the ability to communicate with SUMO to model vehicular networks through a Veins subframework. Selection of operating hardware allows for different levels of wireless simulation. INET also possesses its own mobility which can be used to model loss, interference, and node movement within the simulation space.

Simulation frameworks for dynamic networks like INET and Veins all require mobility to function. The interference and loss functions within the frameworks require the positions of the nodes. Both INET and Veins provided methods for updating mobility from SUMO, but unfortunately they were not designed to function together. Therefore, in order to simulate the desired behavior we set up both frameworks as independent networks and updated the mobility of one directly from the other. This required some low level changes to the framework that we will talk about later on in the implementation 5.2.1.

By utilizing OMNet++, Veins, and the INET frameworks, we were able to simulate a more complex network environment. Recording the activity within that network and saving to a database similar to Piersons enabled us to take the output of the new simulations and feed them directly into his attack. We record the scalar results of the attack along with some metadata gathered during simulation into a MySQL database [34]. An overview of the general simulation flow can be seen in 4.3.
4.5 Increased Computational Requirements

In order to generate traffic that was as realistic as possible, randomTraffic.py, a script included in SUMO for randomly generating vehicle traffic and spawn patterns was used. Each of these randomized traffic patterns was then used in simulation for each listener configuration shown in section 5.3. Because simulation results were stochastic, creating result distributions of sufficient sample size required significant computational time. The difference between sample sizes can be seen for the distributions in figure 4.4. Larger vehicle densities required longer to simulate, and gathering enough samples on a single computer was not really feasible.

![Sample Size Comparisons for Result Distributions](image)

**Figure 4.4: Sample Size Comparisons for Result Distributions**

There were several approaches we utilized to help gather the large sets of data required to analyze the simulations. During initial testing, we quickly discovered the time cost of manually running a simulation prevented our ability to effectively gather data. Depending on the number of vehicles, and amount of messages required for the simulator to process, a simulation could run in several minutes or 6 hours. We automated the iteration through each set of simulation configurations for any given generated map. Building on that, we wrote several scripts that allowed for automated running of each of the entire simulation process from traffic generation to running...
of the attack 4.5. Finally, multiple virtual machines were established to allow for simultaneous data gathering. These steps allowed for the gathering of much larger data sets.

Figure 4.5: Script Flowchart for Simulation Automation
For the reasons stated in 4.5, it was important in data analysis that large quantities of data were gathered for each of the configurations that needed to be tested. Optimally, a minimum of roughly 800-1000 data samples were desired for any given set of configuration parameters to produce distributions like in 4.4a. The run time of simulations for large vehicle densities greater than 300 varied from 6 to 18 minutes. In the worst case gathering 800 samples for a single configuration could take as long as 10 days. In order to mitigate this cost, simulations were distributed amongst 16 different machines shown in A.1.

5.1 Simulator

When selecting the simulator and framework versions, we utilized the latest version of OMNeT++ and it’s compatible version of INET. We opted to use Veins version 4.7.1 which included some level of WiFi integration using the veins_inet framework. This provided a frame of reference when updating the source code to allow the combination of the WiFi and DSRC network stacks. The versions of each of the simulators used can be seen in table 5.1. The SUMO simulator version also limited the simulation operating system to Ubuntu 16.04 instead of the newer Ubuntu 18.04 because of incompatibilities with the OSGEARTH library dependency.
Table 5.1: Simulator Versions

<table>
<thead>
<tr>
<th>Simulator</th>
<th>Version</th>
<th>Release Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>SUMO</td>
<td>0.32.0</td>
<td>2017-12-19</td>
</tr>
<tr>
<td>OMNeT++</td>
<td>5.4.1</td>
<td>2018-06-29</td>
</tr>
<tr>
<td>Veins</td>
<td>4.7.1</td>
<td>2018-06-05</td>
</tr>
<tr>
<td>INET</td>
<td>4.0.0</td>
<td>2018-06</td>
</tr>
</tbody>
</table>

5.1.1 SUMO

A single map of the town of San Luis Obispo was used in all simulations run through the SUMO environment. The OpenStreetMap API limits the size of map segments that can be downloaded. In this simulation, a map of roughly 0.03 degrees longitude by 0.02 degrees latitude was used which translated to a space close to 2 km by 1 km. The map seen below in figure 5.1 was the map used during the data collection for all of the data sets. This map was selected because it provided a fair amount of buildings for packet loss and noise simulation and the potential for grouping vehicles even with smaller vehicle densities during simulation. This allowed for additional measurements of the effectiveness of listener coverage in the map.

5.1.2 Randomizing Maps

Trip randomization was accomplished using the randomTrips.py script included with SUMO. The script takes 3 primary arguments, a start time, end time, and when vehicles enter and leave the simulation. The start and end times effectively show the length of the simulation, but because the paths of vehicles are randomized, the actual density seen in the simulation is always less than the amount of vehicles spawned in.
5.1.3 OMNeT++

The quantity of network traffic to be simulated here required a great deal of the visualization and logging information used needed to be turned off to speed up simulation time. In addition, because multiple configurations needed to be tested for any given SUMO traffic simulation, there was a need to recompile simulation settings before each simulation. During initial simulations, the graphical interface was used exclusively. This allowed for verification of proper handling of packets and behavioral interaction of the INET and Veins frameworks. The graphical interface also allowed for debugging and verification of vehicle and radio locations within the simulation map. Actual simulation was done using the terminal command environment. To maximize speed we also disabled the majority of system logging. The lack of graphical refresh and logging considerably sped up simulation time, but made for some difficulties during early simulation when bugs were still being caught.
5.2 Network Model

Vehicles in simulation are all implemented with the same radio configurations. They may be treated as vertices that are connected by edges representing connection through different radio protocols. They are each equipped with a single wave protocol radio. This radio handles the sending/receiving of all DSRC traffic. These DSRC radios broadcast a safety message to surrounding radios at a frequency of 1HZ. Additionally, each vehicle is equipped with two separate wlan interfaces from the INET framework for WiFi communication. Each of these WiFi interfaces function independently. UDP broadcasts are sent from each WiFi interface at a time that is randomly selected between 0 and 1s according to an exponential distribution. The listeners receive all messages from every vehicle on the map, and based upon distance, obstacles, and collisions it will decide whether it drops or keeps the packet. This is done through physical layer modules defined within the INET and Veins frameworks.

5.2.1 Mobility Sharing

Each module in a simulation exists at a location usually defined either at the start of the simulation or through a mobility module. These coordinates are different from the ones used in SUMO simulation. The default mobility module in OMNeT++ contains area constraint variables for the x, y, and z coordinate spaces. It also will record the last position of the object and its orientation at that time in the form of Coord and EulerAngle objects. In the default mobility module the area serves to limit where nodes move within the space during simulation. The differing mobility fields shown in table 5.2 needed to be taken into account during runtime to allow the system to actually model the network traffic.
Part of the Veins framework is functionality used to translate the SUMO coordinate system into the one used by Veins. Veins a set of x, y, and z coordinates to model vehicle location as well as a vehicle orientation, and speed value. Because the INET framework is not broadcasting safety information, the speed and orientation values were unimportant for network traffic. Additionally, while the INET mobility module operated with area constraints, the Veins mobility did not use any. The constraints of the simulation were defined by the size of the sumo map which was provided to the system at run time. Using the x, y, and z coordinates from Veins, we updated the location of the INET radio modules at the same time as we updated the Veins modules. The area constraints of the simulation were stored as global variables and used to update the nodes when they were initialized.

### 5.2.2 Radio Mediums and Loss Models

The radio models used in the simulation were what enabled loss and interference in the network. There are multiple different mediums and models to choose from. Some model operate purely on distance from the sending node while others operate based
upon obstacles within the simulation. Additionally, for DSRC radios, there is a de-
cider which decides when collisions occur and packets are dropped. The models used in our simulations were the SimplePathlossModel and Simple Obstacle Shadowing [35]. The obstacle shadowing model is used mainly to show radio loss in suburban or urban environments. The model will also allow packets that pass through buildings to be blocked based upon transmission strength and size of the building. The Simple Pathloss Model also causes packets to be discarded for not successfully arriving, but it assumes constant attenuation of the signal based upon signal strength and distance. As a means of verifying performance in an ideal scenario, we also attempted to simulate behavior with no loss models. Unfortunately, the lack of models in the system caused the required simulation runtime to jump from minutes to days, so the concept was quickly abandoned.

INET models also exist, however they did not appear to obviously port in the loss models which utilized the SUMO obstacles in the same way as Veins. Additionally, the radio medium used precluded the use of some models. The radio interface we used in simulation was the AckingMacWireless interface along with a given radio range. This particular WiFi model kept the traffic in a pattern that more closely resembled the ones used in Piersons attack.

5.2.3 Logging

To record the relevant vehicular data for tracking, it was relevant to have not only the pseudonym of the vehicle, but also its original identifier. Each vehicle opened two files when they were initialized. One of the files stored the received DSRC packet information for the vehicle, and the other stored the received WiFi packet information for the vehicle. The simulator also generated a file of vehicle identifiers to be used when creating the mongodb packets for the attack.
Packets were recorded at different points in the vehicle radios. DSRC packets were recorded at the application layer after the system had fully processed the packet. WiFi packets were recorded before being processed in the MAC layer. The different network layers in INET are stored in a special format called chunks. Chunks are processed by the system in a similar fashion to typical network headers, but the way they are read means that higher layers have no access to information from lower layers. Additionally, the way the data is stored in chunks means that it needs to be handled using the API provided for working with packets. The MAC address was the important feature for this particular attack so packets had to be recorded at or before the MAC layer chunk was processed out of the packet.

5.2.4 Analysis and Data Configuration

Simulation Results were stored in a MySQL database and several iterations were explored to get the minimum number of fields required to properly process the data. A website front end was created to allow for data visualization. The website used php for data processing and presented the data using a the JavaScript FusionGraphs graphing API. This allowed for a significant number of graphs to be generated dynamically as the incoming data changed. It also enabled us to observe the incoming data to tell when machines had finished simulations or were having issues.

5.3 Simulation Configurations

The simulation parameters discussed above sum up the majority of configuration decisions that were made. These decisions can be seen in the following tables. Each table shows the set of configuration parameters that were tested. The environment variables as seen below in table 5.3 were run for each of the defensive Schema for
each of the defensive values. This also held for any given randomly generated traffic pattern.

Table 5.3: Environmental Configurations for Each Defensive Scheme

<table>
<thead>
<tr>
<th>Parameter Definition</th>
<th>Simulation Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Listeners</td>
<td>5, 10, 15, 20</td>
</tr>
<tr>
<td>Vehicle Density in Simulation</td>
<td>50, 100, 150, 200, 250, 300</td>
</tr>
</tbody>
</table>

The listener configurations tested in the system were static regardless of traffic behavior. They were placed to get optimal map coverage based upon listener range and to minimize overlapping listening zones. In the five listener configuration 5.2a, listeners had little to no map coverage. Qualitative observation of simulations in the graphical environment showed that vehicles with shorter drive distances tended to not appear in more than a single listening zone. The ten listener configuration 5.2b showed better coverage with more vehicles passing through at least two listening zones.

The loss functions for network traffic are based on distance and obstacles. Thus, listeners placed with minimal surrounding buildings tended to receive traffic from all vehicles within range while listeners with multiple buildings tended to only see traffic from vehicles in the immediate vicinity. The 15 listener configuration 5.2c featured the least overlap between listeners while maximizing map coverage. However, certain vehicle placements could still occur in the bottom and top sections of the map resulting in a lack of visibility of these vehicles until they entered the visible range of listeners. Simulations with 15 listeners also began to show a noticeable slowdown from the slowdown of the 5 and 10 car listener configurations. The final configuration tested was the 20 listener configuration 5.2d, this listener configuration offered the best performance without overlapping listening zones. In order to get maximal coverage, ideally a listener would be placed at every single intersection within the map to avoid loss due to signals being obstructed by obstacles. The 20 listener placement allowed
almost complete visibility of vehicles outside of the urban obstacles and a fair amount of coverage within the urban environment as well.

5.3.1 Defensive implementations

The implementation of each of the defensive schema utilized different components of the simulation. During runtime, vehicles would periodically run a function that updates the vehicle position. Within this function, the system would check what
kind of defensive scheme the vehicle was supposed to be running. Additionally, the system would confirm whether or not the criteria for a pseudonym change for the given defensive scheme had been met.

5.3.2 Timeout

The timeout scheme set the delta for pseudonym switches at initialization from the system configuration files. The vehicle would also get the current value of the simulation timer. During movement updates which occurred roughly once a second, the vehicle would check the current simulation time with stored one. When a period of time greater than or equal to the delta value had passed, the vehicle would update both the pseudonym and its stored simulation timer value.

5.3.3 Blackout

The blackout scheme functioned in a similar fashion to the timeout scheme. However, the delta value that was stored in the system was the period of silence that occurred after a pseudonym change. Pseudonyms were changed every 300 seconds, and the vehicle would then set a system variable preventing it from broadcasting messages until the current value of the simulation timer was greater than the delta accepted by the system.

5.3.4 Density

The density scheme utilized a counter based upon received messages over a given period of time. If the number of received messages exceeded the criteria for a pseudonym change the vehicle would change pseudonyms. Additionally, in order to prevent the
vehicle from changing constantly while it was within a group of vehicles, a timeout period was added where the vehicle would not change. If the number of vehicles did not exceed the minimum criteria for a pseudonym change, the vehicle would reset the counter and continue operating with the old pseudonym until the criteria is met. During simulation, the period of time used for counting surrounding vehicles was roughly 1 second. In order for the vehicle to accept the message, the packet had to not be dropped, so only cars in the immediate vicinity as shown in figure 5.3 would increment the counter.

![Figure 5.3: Node Traffic During Simulation](image)

5.3.5 Defensive Values

The environment variables needed to be tested for every single defensive value. However, the defensive values that were tested in the simulation were much more dependent on the conditions that were able to be simulated. Because the computational requirements of simulating vehicle densities over 300 increased too quickly for feasible testing, the defensive schema values in tables 4.1, 4.2, and 4.3 had to reflect the environments that we could effectively simulate. The Blackout protocol had some flexibility, but because of the possible decrease in safety from no longer broadcasting traffic data we opted to test small periods of between 5 and 15 seconds. Given that
DSRC broadcasts occur every 1 second, this actually became a significant number of broadcasts that did not occur.

The Timeout protocol was also fairly diverse, and it was not dependent on any system parameters accept for the period of time between when a vehicle spawns and when it is removed from the simulation. We opted to test values ranging from 30 seconds to 10 minutes in order to see what the best performing time was. Periods longer than 10 minutes were not used because we found vehicles were leaving the simulation before ever actually making a single pseudonym change. The density scheme was actually the most limited of the schemes we tested. Because the number of vehicles in the simulation was not always high, we needed the vehicle to be able to change pseudonyms when less vehicles were present. Thus, we examined density expectations between 1 and 5 vehicles.

5.4 Summary and Measure of Success

Each Defensive Schema being tested was run using combinations of the environmental configurations in 5.3. Additionally, a given simulation run tested each configuration under all of the listener maps shown in 5.2. All results were compared against a baseline Timeout period of 300 seconds. We examined Precision, Recall, and f1 score looking for minimal performance compared to the baseline. Additionally, we examined pseudonyms used, and associations made to find which schemes resulted in the most pseudonyms being used.
During the course of a 3 month period of time, roughly 581 computer-days worth of simulation data was gathered by our 16 machines. Several initial datasets taken were ignored due to bugs in the simulator. Once these bugs were addressed, later simulations were grouped and organized by the machine the simulation was run on and the privacy schema being used.

6.1 Data Normalization and Loss

Initial simulations ran into issues where the attack would fail when configurations pushed the quantity of packets beyond certain limits. Upon closer examination, it was determined that it was likely due to one of the systems attempts to associate pseudonyms. The component of the system behaved similarly to the Softmax function where a probability distribution of association likelihood was created for identifiers. As the number of identifiers in the system and therefore in the distribution increased, the sum of the probabilities would exceed 1 and the system would crash.

6.1.1 Dataloss in the Attack

The loss of data due to the suspected floating point errors within our pseudo Softmax function showed up primarily within simulations that produced a significant amount of network traffic. These results were therefore skewed towards the lower density results because of the lack of data for larger simulations. At the smallest Listener
Configuration, we were able to collect the most consistent data with the least number of errors. As the vehicle density increased, small amounts of loss began to appear in the datasets. Additionally, as the Timeout defensive parameter in 6.1a increased, the number of errors increased proportionally. As the listener coverage increased to 10, this effect became more pronounced with each vehicle density group losing some more data as seen in 6.1b.

The effects of the loss in the attack really become pronounced in the 15 and 20 listener configurations. In 6.1c it can be seen that the loss of data in the higher vehicle densities is so severe that no meaningful analysis could be conducted. Finally in 6.1d, some simulation configurations had no data results. These initial results had so much data loss that they were pretty much unusable.

### 6.1.2 Normalization Reasoning

Observations about the pseudo softmax probabilities led to concerns that small errors in the floating point values stored in the distribution array may have slowly become significant as the data in the array increased. To solve this issue, we added a normalization component to the attack that divides each of the values in the probability array by the sum of the array. Since the probabilities we were concerned with were the largest ones anyways, this cleaned up the results without changing their actual relation to the rest of the distribution.
Figure 6.1: Overview of Loss for Different Listener Configurations

<table>
<thead>
<tr>
<th>Listener</th>
<th>Configuration</th>
<th>Loss</th>
<th>37</th>
<th>22</th>
<th>17</th>
<th>12</th>
<th>7</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a) 5 Listener</td>
<td>200</td>
<td>170</td>
<td>160</td>
<td>150</td>
<td>140</td>
<td>130</td>
<td>120</td>
<td>110</td>
</tr>
<tr>
<td>(b) 10 Listener</td>
<td>190</td>
<td>180</td>
<td>170</td>
<td>160</td>
<td>150</td>
<td>140</td>
<td>130</td>
<td>120</td>
</tr>
<tr>
<td>(c) 15 Listener</td>
<td>180</td>
<td>170</td>
<td>160</td>
<td>150</td>
<td>140</td>
<td>130</td>
<td>120</td>
<td>110</td>
</tr>
<tr>
<td>(d) 20 Listener</td>
<td>170</td>
<td>160</td>
<td>150</td>
<td>140</td>
<td>130</td>
<td>120</td>
<td>110</td>
<td>100</td>
</tr>
</tbody>
</table>

Note: Loss is measured in arbitrary units.
7.1 Metrics Summary by Scheme

In order to analyze the simulations, first we introduce some terminology for identification of the results. The results of any particular simulation could be broken down into several different scalar values. These values were then utilized to calculate other results. Several of these terms were direct definitions from the original attack [5] while others were added later to increase visibility into the modified simulator.

The w2d_prec and w2d_rec values were examined primarily as an addition to the results already provided by the attack. The original attack examined all network traffic passed to it as a complete system. In our simulator, some network traffic is being excluded due to loss and interference as discussed earlier. Thus in order to account for this, during simulation the total number of identifiers in the system was measured and recorded.
<table>
<thead>
<tr>
<th>Result Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>assoc_made</td>
<td>The number of W2D entries that meet the threshold such that the attack algorithm will conclude they are associations</td>
</tr>
<tr>
<td>correct_assocs</td>
<td>The number of correct associations from the above guessed associations</td>
</tr>
<tr>
<td>avg_prec</td>
<td>The average precision across all Wifi devices</td>
</tr>
<tr>
<td>avg_rec</td>
<td>The average recall across all Wifi devices</td>
</tr>
<tr>
<td>d2d_prec</td>
<td>The precision across the entire D2D matrix (all D2D associations)</td>
</tr>
<tr>
<td>d2d_rec</td>
<td>The recall across the entire D2D matrix (all D2D associations)</td>
</tr>
<tr>
<td>w2d_prec</td>
<td>The precision for W2D associations as calculated by $\frac{\text{correct_assocs}}{\text{assoc_made}}$</td>
</tr>
<tr>
<td>w2d_rec</td>
<td>The recall for W2D associations as calculated by $\frac{\text{correct_assocs}}{\text{total_identifiers}}$</td>
</tr>
</tbody>
</table>
7.2 Timeout

The dataset for Timeout was obtained from 150 computer-days of simulation. As discussed in earlier sections, it was tested within a variety of environmental configurations seen in section 5.3. The results were then compared using a 300 second timeout as a baseline for performance. This dataset was where the most data was gathered as we explored the minimum amount of data for meaningful analysis leading to several of the larger configuration sample sizes seen in 7.1.

![Figure 7.1: Timeout Scheme Dataset Heatmap](image)

Each of the squares represents the number of samples for a given value configuration in the heatmap. The value in the upper left hand corner is the average runtime for that particular set of configurations. The upper right hand value represents the
average precision as provided by the attack. The bottom left of each square was used primarily for debugging, it shows the number of successful simulations. It should be noted that simulations where the OMNeT++ simulator crashed could not be detected by the script and would not be included as failures. This can also be seen in the small differences in the number of simulations recorded for each configuration.

7.2.1 Precision

Precision for the Timeout scheme varies with vehicle density, number of listeners, and timeout duration. As seen in 7.2, W2D attack precision decreases with increased vehicle density, showing that pseudonyms are more difficult to link as the number of vehicles, and thus the number of possible pseudonyms, increases.

The D2D precision of the Timeout schema in 7.3 remained at 100% regardless of other configuration parameters. This proved to be true for all defensive schema including a saved dataset from Pierson’s experiment. There was little variation and as the number of simulations increased, the variation disappeared.

The timeout duration, however, doesn’t have as clear of a relation. While a timeout duration of 30 seconds has the least precision, timeout duration of 60 and 120 seconds have higher precision than 300 and 600 second timeout periods. This result doesn’t match the expected positive relationship between timeout and precision, and can be further examined through different listener configurations. Analysis of different listener configurations also shows that the behavior of the timeout scheme varies dramatically with the number of listeners observing pseudonym changes.

As the number of listeners increases, the gradient of the precision vs. vehicle density curve becomes more gradual. For example, the 600 second timeout precision for 5 listeners ranges from 0.58 to 0.44 over a vehicle density of 50 to 300 as shown in 7.4,
while precision for the same timeout duration only ranges from 0.22 to 0.19 when 20 listeners are present. Additionally, increasing the number of listeners decreases the precision quickly, a difference of about 50% when comparing the results for 5 listeners to that of 20 listeners. Both of these results can be explained by the increase in number of guessed associations as the listener coverage increases. As the number of listeners increases, so does the coverage and number of packets intercepted, causing more associations to be guessed, and an increase in recall but also incorrect associations proportionately.

The number of listeners also seems to affect which timeout value performs best. While 30 seconds is the best performing defensive timeout value in a layout with 5 or 10

Figure 7.2: Timeout Scheme W2D Average Precision
listeners, it is beat by timeout periods of 300 seconds and 600 seconds for scenarios with 15 or 20 listeners. The difference between the short and long period timeout precision increases as the coverage of the listeners increases. Observing the difference between 30 seconds and 300 seconds at a vehicle density of 100 from 5 listeners to 20 listeners, the difference changes from 0.05, to 0.05, -0.02, and finally -0.05. Timeout duration of 60 and 120 seconds behaves oddly, with a higher precision over all listener configuration, suggesting that the defensive ability of the timeout scheme is better towards extremes.

Figure 7.3: Timeout Scheme D2D Average Precision
Figure 7.4: Timeout Scheme Average W2D Precision for Variable Listeners

(a) 20 Listener

(b) 10 Listener

(c) 15 Listener

(d) 20 Listener
The timeout scheme has a strong negative correlation between timeout duration and d2d recall. This relationship is shown in 7.5 and 7.7, which represent the pseudonym recall values for any pseudonym changes which occur within listening zones. As pseudonyms are changed more frequently, the attack is able to detect less of the pseudonyms. This behavior is expected, since more frequent pseudonym changes means that there are likely to be more simultaneous pseudonym changes between cars, and between listening zones. As discussed earlier in the paper, changing pseudonyms between listening zones or concurrently with other cars creates confusion for the attack, which explains the negative correlation.
Figure 7.6: Timeout Scheme Average W2D Recall

D2D recall doesn’t appear to vary with vehicle density, however. As the vehicle density increases, there are more pseudonym changes and associations to be made, but the attack still detects the same proportion of pseudonyms. This is a characteristic of the attack, and shows that the performance of the Timeout scheme in terms of d2d recall is independent of vehicle density. In comparison, the W2D recall in 7.6 did vary with density. Additional graphs for the w2d recall for timeout can be seen in figure A.2. This measured recall when accounting for changes outside the zone of attack and awareness favored the faster timeouts like 30 with the slower timeouts coming last with variations of roughly 0.1.

The behavior of the correlation between timeout duration and recall varies depending
Figure 7.7: Timeout Scheme Average Recall for Variable Listeners

(a) 5 Listener
(b) 10 Listener
(c) 15 Listener
(d) 20 Listener
on the listener configuration. With only 5 listeners, nearly all of the pseudonym changes are detected within the listening zones at timeout duration of 300 seconds and 600 seconds, and there is a steep decrease in recall as the duration decreases to 120, 60, and 30 seconds. As the coverage by listeners increases, the behavior shifts and turns exponential for scenarios with 10, 15, or 20 listeners. In the 20 listener configuration, the average recall at 600, 300, 120, 60, and 30 seconds is approximately 0.96, 0.58, 0.38 and 0.28, a clear exponential decay. From this data, it would make sense that there is some maximum defensive asymptote which can be approached as the timeout duration is decreased. Increasing the number of listeners, and thus the coverage, reduces the recall of the attack over all timeout values.

7.2.3 F1

The D2D F1 score represents the harmonic mean of the D2D recall and precision discussed above. This is shown in figures 7.8 through 7.10d. As shown in the graphs, F1 score decreases as pseudonym change frequency increases, and also decreases as as the number of listeners increases. F1 score is decreased with shorter timeout periods since the recall is lowered, as discussed above.
Figure 7.8: Timeout Scheme Average D2D F1

Increasing the number of listeners decreases the F1 score due to the decreased precision. Again, the relationship between timeout duration and F1 score is approximately a decaying exponential, similar to that of D2D recall. Faster pseudonym changes offer a smaller margin of improvement when compared to changing between slower pseudonym change periods, such as 300 and 120 seconds. The higher defensive time-outs show the most interesting behavior as they change little across different listener configurations in figure 7.10. This behavior holds across the W2D F1 score where the 300 and 600 second timeouts varied by no more than 0.01.
Figure 7.9: Timeout Scheme Average W2D F1
Figure 7.10: Timeout Scheme F1 Score for Variable Listeners

(a) 5 Listener

(b) 10 Listener

(c) 15 Listener

(d) 20 Listener
7.2.4 Associations

Associations are broken down into the attempted associations by the attackers in figure 7.11, and the correct associations seen in figure 7.12. The associations being made with the Timeout scheme indicate a decaying behavior similar to a logarithmic graph. This was consistent across the correct and guessed associations. Additionally, when increasing the number of listeners in the simulation, the graphs show both a basic offset, and an increase in the variation between different defensive parameters.

In 7.11a the variation between different Timeout periods was not exceed 10%, and the overall number of guessed associations being made was less than 24% of the number of vehicles in the simulation. In comparison, 7.11d shows both a significant difference in performance of defensive protocols and an overall increase in guessed associations. Variation increased for the vehicle densities of 50 cars to 55% with the attack making at least two association guesses for each vehicle in the 30 second defensive scheme. At the 300 vehicle density, variation decreased to roughly 50%, and the number of guesses decreased to roughly 1.6 per vehicle.

The number of correct associations being seen on average followed a similar trend as the guessed associations at small listener configurations. Figure 7.12a shows the number of correct W2D guesses varied by roughly 12% across all Timeout periods at low vehicle densities. This variation dropped to roughly 9% as the density increased. As the number of listeners increased, the behavior of the graphs differs more from the guessed associations graphs in 7.11. This likely due to the increase in listener coverage drastically increasing the number of guesses the system makes while not improving the precision.
Figure 7.11: Timeout Scheme F1 Score for Variable Listeners

(a) Guessed Associations for 20 Listeners

(b) Guessed Associations for 15 Listeners

(c) Guessed Associations for 10 Listeners

(d) Guessed Associations for 5 Listeners

(e) Guessed Associations for 20 Listeners
Figure 7.12: Timeout Scheme F1 Score for Variable Listeners

(a) Correct Associations for 20 Listeners

(b) Correct Associations for 15 Listeners

(c) Correct Associations for 10 Listeners

(d) Correct Associations for 5 Listeners
7.2.5 Tradeoffs

The Timeout scheme can be broken down into its performance with different timeout periods. Faster timeout periods as seen in figures 7.11 through 7.14 change pseudonyms more frequently enabling an attacker to make more associations within listening zones. However it also decreases the overall recall as the vehicle changes outside of listening zones more often. In addition, due to the quantity of changes occurring within zones, the precision of attackers though this loss of precision is mitigated with the addition of more listening zones.

![Average Associations Made vs Vehicle Density](image)

**Figure 7.13: Timeout Scheme Guessed Association Average**

Slower Timeout periods provide a less drastic change in listener associations. Timeout periods of both 300 and 600 had roughly the same number of pseudonyms correctly associated. The average precision of the slower period performed less impressively
when less listener coverage existed, but when the number of listeners in the system increased the slower periods resulted in much worse precision for the attacker. In addition to this, slower periods have the benefit of being less costly in terms of certificate usage.

![Average Correct Associations vs Vehicle Density](image)

**Figure 7.14: Timeout Scheme Correct Association Average**

### 7.3 Density

The data from the density scheme was gathered from 88 computer days and is skewed towards lower vehicle densities, as shown in figure 7.15. This was primarily due to a lack of computational time for gathering all of the data. However, despite the noise induced by the lack of consistent sample sizes, the behavior of the scheme can be seen.
7.3.1 Precision

Despite a minimal amount of data, some trends are apparent in precision for the density-based pseudonym changing scheme. The data for precision is shown in figure 7.16. Precision has a negative linear association with vehicle density in all cases, and the slope of the line becomes less negative as the number of listeners increases. The behavior of this relationship is approximately equal to that of the standard 300
second timeout pseudonym change with regards to precision values relative to number of listeners and vehicle density. However, the density value required for a pseudonym change does not appear to have an effect on precision. While some slight variation exists at lower vehicle densities, the behavior across the different vehicle densities requirements was almost identical. At 5 listeners, there is an approximate range of 0.03 for precision of the density values given, 1 through 5. Unfortunately, no clear trend is visible which would state whether a higher or lower density value is better for a pseudonym change. At these lower densities where these differences are the largest, we took fairly large sample sets, so the results are likely not due to noise.

Interestingly, the number of listeners does greatly affect the attack precision on the Density protocol. At 5 listeners, the average precision of the attack was roughly 59% while the more comprehensive 20 listener system precision fell below 25%. However, despite the decreased performance, the attacker performed much more consistently across all vehicle densities at the 20 listener configurations.

7.3.2 Recall

Recall for the density scheme has a general negative correlation with vehicle density, but it maintains its consistent behavior across different density change requirements. In figure 7.17, it can be seen that the variation across different density change requirements is very small. These variations become more pronounced when looking at specific listening configurations which can be seen in A.4. the d2d recall shows behavior that was somewhat interesting in comparison. The average performance of the different Density protocols are very similar to the 300 second baseline, but the d2d recall of the density protocol showed a decreasing behavior as the density increased. For 5 listeners, d2d recall decreases from about 0.97 to 0.93. At 10 listeners, recall decreases from about 0.93 to 0.87. For 15 listeners, the data decreases from
Figure 7.16: Density Scheme Precision for Variable Listeners

(a) Precision for 5 Listeners

(b) Precision for 10 Listeners

(c) Precision for 15 Listeners

(d) Precision for 20 Listeners
approximately 0.87 to 0.83, and at 20 listeners the recall appears to decrease from 0.83 to 0.80. It’s interesting to note that the decrease in recall between listener values tends to level out when the vehicle density exceeds 150, and the slope of the line increases as listener numbers increase. Additionally, for higher listeners the amount of noise appears to increase among scheme density values. Regardless, at all listener numbers, the range in recall for varying scheme density values grows larger as vehicle density increases. This is likely because a higher vehicle density creates more frequent changes in the density-based pseudonym changing scheme.

![Figure 7.17: Density W2D Average Recall Across Listeners](image)

At lower vehicle densities, a pseudonym change is unlikely to occur for a higher threshold, causing the lower threshold density changes to occur much more frequently. This explains why higher threshold values are outperformed by lower threshold values at
low vehicle densities: at lower densities, the high threshold pseudonym changes never occur, and at higher vehicle densities the scheme is approximately equal regardless of threshold value. This also is why the graph appears to diverge at higher vehicle densities, since it is much more susceptible to noise inherent in the small data-set. Lower density thresholds have an advantage in triggering more frequently at lower vehicle densities, however this advantage decreases as vehicle density grows. The density scheme improves performance as the number of listeners grows. This is because a concurrent pseudonym change is more likely to occur within a listening zone, which creates confusion as discussed previously. As observed concurrent pseudonym changes become more frequent due to increased vehicle density and listener coverage, recall decreases. The same trends and improvements over basic timeout or blackout schemes are visible over the DSRC to DSRC and WiFi to DSRC datasets. The DSRC to DSRC dataset for recall is shown in figure 7.18.
7.3.3 F1

For the reasons discussed above in the precision and recall sections of 7.3.2, the F1 score decreases as vehicle density and number of listeners grows, and outperforms the standard 300 second timeout scheme. The average F1 score for the density scheme data is shown in figure 7.19 and can be compared to figure 7.9 to see an improvement of approximately 0.05 in reducing the F1 score.

While the density scheme performed on average better than the baseline timeout. The advantage primarily occurred when the number of listeners was smaller, with the density protocol performing roughly the same when 20 listeners were present in the system. This effect can be seen in figure A.7 where we show the average F1 performance for each listening configuration.

![Figure 7.19: Density Scheme F1](image)

Figure 7.19: Density Scheme F1
7.3.4 Associations

The increase in vehicles required for a change had little effect on either the number of guessed associations or the number of correct ones. The variation that can be seen is likely due to noise since it can be seen primarily in the higher densities. The difference between the guessed and correct pseudonyms was close for this scheme. At lower vehicle densities, the attacker is making guesses on roughly 64% of vehicles. As the vehicle density in the system increased to 300, the number of guesses being made by the attacker decreases to 55%.

![Graph showing density guessed associations](Image)

**Figure 7.20: Density Guessed Associations**

In both the guessed and correct association graphs, the trend of the associations being made for vehicle density represents a decaying line. However, the noise introduced
by lack of data makes further analysis necessary to be sure what kind of trend is happening.

![Figure 7.21: Density Correct Associations](image)

**Figure 7.21: Density Correct Associations**

### 7.3.5 Tradeoffs

The Density scheme performs very well in the simulation without some drawbacks seen in other schema. It does not introduce any danger to the system through silent periods, and it does not utilize pseudonyms as quickly as the smaller timeout periods.

This scheme also does not seem to show a large increase in performance based upon the density requirements for a pseudonym change. The variation in precision and recall for the attack for different vehicle densities was nominal. While we expected
the increase in vehicles required to change to reduce the precision and recall abilities of attackers, the results show that there may be little benefit to increasing the number of vehicles needed before a pseudonym change may occur.

### 7.3.6 Blackout

The blackout scheme is very similar to the timeout scheme, with an added period without any radio transmission after a pseudonym changes. Therefore, the blackout scheme was expected to perform similarly to the timeout scheme, with possible slight improvements as the blackout duration increased. The dataset was gathered from 185 computer days and is evenly distributed across vehicle densities, creating statistically significant data at lower densities. However, computational cost at larger densities limited the ability to gather significant data quantities as seen in 7.22. Noise from the smaller quantity of datapoints can be seen in the data below.
7.3.7 Precision

The precision was remarkably consistent among blackout durations of 5, 10, and 15 seconds. This can be seen in 7.23 through 7.24, which show the Wifi to DSRC association precision average across all listener configurations. In comparison to the timeout precision discussed earlier in analysis, the precision matches the 300 second data very closely. The precision for the variable defensive blackout periods remains almost identical only varying by roughly 3% at vehicle densities of 300. Blackout seems to have no apparent effect on precision.

Additionally, the shape of the line matches the shape of the standard timeout curve,
Figure 7.23: Average W2D Attack Precision for Blackout Scheme

including with variable vehicle densities and listener configurations. Figure A.3 shows the specific precision performance of each listener configuration. Similarly, the Blackout scheme showed no improvement on the timeout scheme for D2D precision. The average D2D precision of the attacker in this scheme remained at 100% regardless of the period of blackout or vehicle density.
Recall

Again, blackout seems to have minimal or negative effects on the trackability of vehicles. There is a small amount of variability between the 5, 10, and 15 second blackout curves in recall graphs, which can be attributed to noise. The shape and values of the curve matches the Wifi to DSRC recall graph of the simple timeout scheme for a value of 300 seconds. These results can be seen in figures 7.26 and 7.25 for both the D2D and W2D recall graphs. The recall for each listener and vehicle configuration can be found in figure A.4.

Figure 7.24: Average D2D Attack Precision for Blackout Scheme
Figure 7.25: Average W2D Attack Recall for Blackout Scheme
Figure 7.26: Average D2D Attack Recall for Blackout Scheme
7.3.9 F1

Since the recall and precision graphs for blackout are consistent with the timeout scheme for a period of 300 seconds, it makes sense that the F1 graph similarly follows. The W2D F1 score is shown in figure 7.27. The D2D F1 score was not shown here given that both recall and precision varied very minimally from 1. The F1 score for each listener configuration can be seen in A.5

![Average Association - w2d f1 score vs Vehicle Density](image)

Figure 7.27: Average F1 Attack Recall for Blackout Scheme

7.3.10 Associations

Finally, simulations show little to no difference in the number of guessed and correct associations for different blackout periods. The number of guessed associations follow a slightly decaying curve that remains mostly linear, while the number of correct
associations begins to taper more when the vehicle density exceeds 200. The number of correct associations relative to vehicle density and blackout period is shown in figure 7.29.

Figure 7.28: Blackout Guessed Associations Across All Listeners
7.3.11 Tradeoffs

The blackout scheme comes at a trade-off of decreased safety for longer periods by reducing the ability of vehicles to communicate. The results in this section show that blackout at low periods has little to no improvement to timeout effectiveness. Therefore, the blackout scheme appears to disproportionately decrease safety for an apparently nonexistent improvement in security.

7.3.12 Baseline Performance

As a means of comparing the schemes tested, we look only at the F1 score, and the number of guessed and correct associations. We do not consider implementation costs, infrastructure requirements, or safety implications. While these factors are
important and must be considered overall, we were primarily interested in the affects on privacy. The baseline we used as reference was the timeout scheme with a period of 300 seconds. This period was used in both of the other schemes for implementation of timeout mechanics that were required.

7.4 Comparison

The following figures 7.30 through 7.37 show the comparative performance of all of the defensive protocols. Each line represents a defensive value from one of the protocols tested. In order to get a general comparison, we are looking at average performance across all different listener configurations here.

![Average Association- w2d f1 score vs Vehicle Density](image)

Figure 7.30: F1 Score Value Comparison against Baseline
The timeout protocol with a period of 30 seconds shows the best performance across all listener configurations by a percentage difference of 70%\(\frac{(0.27-0.13)}{0.27+0.13} \times 100\) at lower vehicle densities and 92%\(\frac{(0.19-0.07)}{0.19+0.07} \times 100\) at the higher vehicle densities. Despite this overall advantage, the 1 vehicle density scheme actually provided lower attack precision at higher vehicle densities, and the variation between different schemes and the baseline is often less than 2%.

**Average Association-Attack Recall vs Vehicle Density**

Lines = Defensive Value(s) for the "Defensive Protocol"

---

**Figure 7.31: Recall Value Comparison against Baseline**

Recall is where the 30 second timeout performance reflects the F1 score. In figure 7.31, the recall of the 30 second timeout outperforms the second best density scheme by roughly 14% at lower densities, and 7% at higher vehicle densities. It should be noted though that while the recall of the density scheme decreased as vehicle density increased, the 30 second timeout did not show much variation. It can be seen that
while the 1 vehicle density scheme started out roughly comparable to the 300 second timeout baseline, and later provided roughly 3% reduction in attack recall.

Figure 7.32: Precision Value Comparison against Baseline

The pseudonym usage of each of the schemes is one of the more interesting things we found in this work. Each of the simulations we ran were 30 minutes long. The number of pseudonyms used by each vehicle can be roughly extrapolated by taking the number of vehicles in the simulation and the total number of pseudonyms used to see how many pseudonyms are used by each vehicle in a half hour period. In 2017, drivers spent on average 51 minutes a day driving vehicles or $51 \times 365 = 18615$ minutes per year. For each protocol, we calculate the average worst case theoretical pseudonym usage and the average usage from the simulations we measured. For the timeout protocols, the worst case change for vehicles is the timeout period. The
Blackout and Density protocols implement a basic timeout of 300 seconds to limit pseudonym usage, so we assume pseudonym usage based upon that. By looking at the predicted usage of these results and the theoretical calculations we can see the predicted 1 year pseudonym usage in figure 7.34.

Despite it’s optimal performance as measured by precision and recall, the 30 second timeout performed the worst in terms of guessed and correct associations. The attack consistently produced significantly more guessed and correct pseudonym associations for 30 second timeout period. Because the number of pseudonyms used by the defense, this still resulted in very low precision for the attacker. The average number of guessed pseudonyms over the total pseudonyms used can be seen in figure 7.36. A
comparison of the correct pseudonyms over the total pseudonyms in the system can be seen in the recall measured in figure 7.31. In this measurement, the 600 second timeout yielded the least correct associations with other schemes performing marginally worse.
Figure 7.36: Guessed Associations over Total Pseudonyms

Additionally, the density scheme utilized a much smaller quantity of pseudonyms for it’s performance against the attacker. The pseudonym usage of the 300 second timeout baseline in figure 7.33 maxed out in higher vehicle densities at around 309 pseudonyms used in a given simulation. The 1 vehicle density scheme required an additional 419 pseudonyms, and the 30 second timeout protocol required as many as 1300 pseudonyms.
Figure 7.37: Correct Associations across all Schemes and Defensive Values
To properly model a system as dynamic and large as a VANET is a significant challenge. The number of environmental variables that need to be accounted for increase with every attempt. These can include more accurate traffic modeling, inclusion of actual sensor data for traffic, and better systems for modeling loss and interference in the network.

8.1 Simulator

In order to properly model traffic in the system, an ideal simulator should allow for vehicle decision making based upon sensor data as well as network traffic. The simplified traffic model used in these simulations provided a solid model of general traffic flow, but vehicle decision making was still pretty more preordained. In addition to better modeling vehicles in traffic, utilizing some of the newer versions of OMNeT++ and Veins that have come out would allow for faster simulation which may allow for testing of larger vehicle densities in the network.

8.2 Network Modeling

The usage of both the INET and Veins frameworks enabled the separate implementation of each of their network stacks. However, neither frameworks were inherently designed to function together, even when implemented properly the actions taken by each network stack was completely separate. This led to difficulties in syncing be-
behaviors such as vehicles leaving the network. A better way to model the interaction between these two networks stacks will allow for better and more accurate simulation.

8.3 Data Collection

Without a doubt, the most painful component of the simulations were the computational and temporal requirements. The management and running of 16 machines was very time consuming. During the process, we wrote several scripts that helped to speed up the configuration and setup of these machines, but even a single machine going down could cost several hours to fix. This effect is compounded by the stochastic nature of the simulator. To produce statistically significant datasets required weeks of computation, and upon completion someone would have to manually restart the whole process. An implementation of a distributed system for simulation task designation and simulation automation is a must for future data collection.
A fully autonomous vehicle contains components that enable sensing, decision making, and network communication. Ideally, all of these components would be integrated into any simulation attempting to model vehicle behavior and its interactions with the surrounding world. In our simulation, we isolated the networking component of the vehicles and allowed for more simplistic modeling of vehicle traffic patterns using SUMO. We improved upon previous research into single-radio pseudonym privacy schemes by gathering thousands of computation hours of data for various schemes in multi-radio vehicles.

Our data was collected for the Timeout, Blackout, and Density privacy schemes over a range of vehicle density and listener coverage configurations. All simulation data was compared against an initial dataset gathered using the Timeout scheme with a period of 300 seconds.

The blackout scheme performed similarly to the baseline 300 second timeout in all configurations. Increasing the period of silence after a change had little effect on the attackers’ ability to associate identifiers. Silence comes at a cost, potentially reducing the safety for all vehicles in the vicinity. The concept for this idea is novel, but it does not perform well against this particular attack and only poses negative effects.

Lower timeout periods in the Timeout scheme offered considerable advantages when listener coverage was small. As listener coverage increased, the performance of shorter and longer timeout periods grew more similar. Although a faster pseudonym change offers performance benefits, it comes at a cost of increased pseudonym usage.
The Density scheme offered significant improvement over the 300 second timeout baseline used. The density scheme requires minimal software overhead, and uses no more pseudonyms than the baseline timeout scheme. We also found that the density protocol requires as little as a single additional vehicle to offer improvements.

The blackout scheme failed to outperform the timeout scheme baseline, but the density scheme showed promise as a means of maintaining user privacy in a multi-radio network. For future work, we recommend extending the simulator for a more realistic environment, measuring the effects of non-naive communication-based pseudonym schemes, and checking for improvements over different timeout period baselines.


[29] Levente Buttyán, Tamás Holczer, and István Vajda. On the effectiveness of changing pseudonyms to provide location privacy in vanets. In Frank Stajano, Catherine Meadows, Srdjan Capkun, and Tyler Moore, editors, *Security and


[33] Christoph Sommer. A multi-channel ieee 1609.4 and 802.11p edca model for the veins framework. 2012.


A.1 Machines

The virtual machines used to run simulations were all setup with the same configurations. Because there is little difference in their configuration, the virtual machine information is listed once in table A.1. However, the number of machines is also listed for clarification. A single machine was configured to run roughly 25 simulations for any given simulated configuration. Because of the length of time for a complete set of simulations for a dataset may vary from 5-20 days depending on the number of simulations run, simulation instances were run using the Linux terminal multiplexer screen [39]. Screen allows multiple terminal instances to be running even when detached from a user terminal.

<table>
<thead>
<tr>
<th>Machine Type</th>
<th># Machines</th>
<th>OS</th>
<th>Memory</th>
<th>Processors</th>
<th>HDD Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>1</td>
<td>16.04.6</td>
<td>8192 MB</td>
<td>4</td>
<td>300 GB</td>
</tr>
<tr>
<td>Physical</td>
<td>1</td>
<td>16.04.6</td>
<td>8192 MB</td>
<td>4</td>
<td>2 TB</td>
</tr>
<tr>
<td>Physical</td>
<td>1</td>
<td>16.04.6</td>
<td>32768 MB</td>
<td>8</td>
<td>100 GB</td>
</tr>
<tr>
<td>Virtual</td>
<td>14</td>
<td>16.04.6</td>
<td>8096 MB</td>
<td>3</td>
<td>20 GB</td>
</tr>
</tbody>
</table>
Figure A.1: Timeout W2D Recall for Variable Listeners

(a) Recall for 5 Listeners
(b) Recall for 10 Listeners
(c) Recall for 15 Listeners
(d) Recall for 20 Listeners

Figure A.2: Timeout W2D Recall for Fixed Listeners

(e) Recall for 5 Listeners
(f) Recall for 10 Listeners
(g) Recall for 15 Listeners
(h) Recall for 20 Listeners
Figure A.2: Timeout W2D F1 Score for Variable Listeners

(a) F1 Score for 20 Listeners

(b) F1 Score for 10 Listeners

(c) F1 Score for 15 Listeners

(d) F1 Score for 5 Listeners
A.3 Blackout Precision for Variable Listeners

(a) Precision for 20 Listeners

(b) Precision for 15 Listeners

(c) Precision for 10 Listeners

(d) Precision for 5 Listeners

Figure A.3: Blackout Precision for Variable Listeners

Legend:
- Lines = Association Model
- Dots = Blockout Estimation
- Error Bars = Standard Deviation

Average Association Model Efficiency vs. Blockout Efficiency

Average Blackout Estimation vs. Blockout Efficiency

A.3 Blockout
Figure A.4: Blackout Recall for Variable Listeners

(a) Recall for 5 Listeners
(b) Recall for 10 Listeners
(c) Recall for 15 Listeners
(d) Recall for 20 Listeners

Average Association - Blackout Recall vs Vehicle Density

(e) Recal for 15 Listeners
(f) Recall for 10 Listeners
(g) Recall for 5 Listeners

Average Association - Blackout Recall vs Vehicle Density
Figure A.5: Blackout F1 Score for Variable Listeners

(a) F1 Score for 5 Listeners

(b) F1 Score for 10 Listeners

(c) F1 Score for 15 Listeners

(d) F1 Score for 20 Listeners
Figure A.6: Density W2D Recall for Variable Listeners

(a) Recall for 5 Listeners

(b) Recall for 10 Listeners

(c) Recall for 15 Listeners

(d) Recall for 20 Listeners
Figure A.7: F1 Score for Variable Listeners

(a) F1 Score for 5 Listeners

(b) F1 Score for 10 Listeners

(c) F1 Score for 15 Listeners

(d) F1 Score for 20 Listeners
Figure A.8: Density D2D F1 Score for Variable Listeners

(a) D2D F1 Score for 5 Listeners
(b) D2D F1 Score for 10 Listeners
(c) D2D F1 Score for 15 Listeners
(d) D2D F1 Score for 20 Listeners

Legend:
- Line 1: Density F1 Score
- Line 2: Density F1 Score (with Error Bars)
- Line 3: Density F1 Score (with Error Bars)