Chapter 1

Conclusion and Future Work

Traditionally being a law enforcement application, digital forensics has recently found its way to academia and is today among the most active research areas. Digital forensics, however, is rapidly evolving and has recently given raise to the more intelligent discipline of computational forensics. In this thesis, we focused on a particular application of computational forensics, namely criminal surveillance and tracking. The main goal of this research is to investigate how to passively (and clandestinely) track a target, who we assume to be a suspect that may have been associated to either a crime that already took place, in which case we consider offline tracking (also known as trace reconstruction), or a crime that is expected to take place, in which case we consider online tracking. While in online tracking, the tracking process takes place in real-time, in offline tracking, the tracking process takes place after the fact (post hoc), where in the latter case any available trace associated to a target suspect is collected and forensically analysed. In online tracking, we emphasise that the tracking process should be passive such that the target is not aware of it. This mere requirement greatly contributes toward the novelty of our research since passive tracking has rarely been thoroughly investigated in the literature, and, evidently, is more difficult than active tracking as it adds the additional requirement of maintaining clandestinity throughout the whole tracking process. In contrast, when tracking a target actively, the target is aware of the tracking, sometimes is even cooperatively involved. While developing our online and offline tracking algorithms, we also considered different environments and scenario settings. Roughly, the thesis can be divided into three main parts:

- *Part 1: Pedestrian tracking.* In this part, we considered online tracking of individuals in real-time by observing signal emissions from any wireless devices they may possess. However, due to humans' limited mobility, we assumed a small tracking scene (such as the size of a neighbourhood or similar venues).

- *Part 2: Vehicular tracking.* We extend the tracking scene to consider vehicles, which have much rapid (but more constrained) mobility patterns than pedestrians. In this case, our tracking scene is restricted to a city size area. We consider both online (with mobility prediction) and offline forensic tracking.
- *Part 3: Multimodal tracking.* In this part, we further extend the tracking scene and consider a combination of parts 1 and 2. In multi-modal tracking we try to track the targets over a large metropolitan area assuming that target entities may opt to use different modes of transportation such as vehicular and other public transportation means (buses, trains etc.). We only considered offline tracking because it is more applicable in the real world, where online multi-modal tracking may be infeasible or unrealistic having such large tracking area.

In this final chapter, we discuss how this thesis can be extended and provide ideas for future work that we believe would be interesting to investigate. In appendix A, we already provide a study on the feasibility of carrying out live forensics on modern intelligent vehicles as an example of such extensions.

1.1 Offline Pedestrian Forensic Tracking

As discussed above, throughout the thesis, we developed and proposed various forensic tracking algorithms for three different tracking environments: pedestrian (chapter **??**), vehicular (chapters **??** and **??**) and multi-modal (chapter **??**). While we investigated both online and offline forensic tracking in the vehicular setting, we only considered online forensic tracking in the pedestrian setting and only offline forensic tracking in the multi-modal setting. Thus, a logical extension to this thesis is to consider the missing scenarios, namely offline pedestrian forensic tracking and online multi-modal forensic tracking. However, it is clear that the online forensic tracking in a multi-modal setting (for a sufficiently large, realistic) scenario becomes very quickly unmanageable, so we doubt its relevance and feasibility. Offline pedestrian forensic tracking, on the other hand, may be more interesting and certainly would have more applications than the online one. This kind of tracking is, nevertheless, more challenging than the offline vehicular forensic tracking due to the unpredictability of pedestrian movement and thus will need more careful modelling in order to reconstruct the traces accurately.

1.2 Advanced Bayesian-based Trace Reconstruction

In chapter **??** we discussed the Bayesian approach for trace reconstruction, then in chapter **??** we demonstrated how to use simple Bayesian inference for this purpose

in a vehicular setting. However, in chapter **??**, we only considered the worst case scenario, where we do not have any external information about the scene in which the target's (incomplete) traces were obtained. In that case, simple Bayesian inference was sufficient and probably the only option. However, if we happen to have access to more information about the scene, we will have more variables and then the more powerful Bayesian Networks (with their dynamic and fuzzy extensions) can be used. It will, therefore, be interesting to create such scenarios and develop a Bayesian Network to investigate how accurately traces can be reconstructed, but we note that for a large number of variables, Bayesian networks become exponentially complex, as discussed in chapter **??** (with their dynamic and fuzzy extensions, complexity grows even faster).

1.3 Tracking based on Social Networking

This thesis has been exclusively concerned with the physical tracking of targets from online passive tracking to offline tracking and trace reconstruction. The contributed algorithms carried out the tracking based on physical observations, but sometimes such physical traces may not be available/accessible due to resource constraints. In this case, a logical tracking may be pursued instead. The theory of *social networking* seems to provide an interesting tool for this purpose. In this theory, individuals are represented by nodes that are connected to each other by ties, such as friendship, business etc., forming a network of interconnected nodes. This network can then be analysed in many ways and various hypotheses can be made based on connections between the nodes. Recent work [**?**] used such approach to investigate child sex trafficking networks and the result seems promising. Similar approach can be used for different forensic purposes and would make an interesting extension to the work presented in this thesis.

1.4 Crime Reconstruction

The main contribution of this thesis is the investigation of how to reconstruct traces belonging to particular individuals, considering different environments and settings. While this will certainly assist in most criminal investigations (as we discussed extensively in chapter **??** and throughout the thesis), trace reconstruction is *not* synonym to the more general field of crime reconstruction. Also known as crime scene reconstruction, crime reconstruction is the process of reconstructing the sequence of the events leading to a crime by making hypotheses based on evidence collected from the crime scene or obtained by external sources. Traditionally, these evidence were mainly biological substances that were inadvertently left by the offenders at the crime scene

and later found by police investigators. While such substances still provide significant evidence in most criminal investigations, today digital evidence and traces are also common leftover pieces of evidence. Crime reconstruction is not confined to the reconstruction of events that took place before or during the crime, but also in most cases considers the events that occurred after or as a result of the crime, which also usually provide significant evidence. Therefore, trace reconstruction can indeed be considered a subset of crime reconstruction. Clearly, then, it would be interesting to investigate other aspects of crime reconstructions that can complement trace reconstruction.

1.5 Multi-modal Trace Reconstruction System

In chapter **??** we proposed a complete multi-modal trace reconstruction system. Although we provided a theoretical complexity evaluation of the reconstruction algorithm and showed that it is both optimal and complete, it was not possible to actually implement and practically test this system due to resource and time constrains. The reconstruction algorithm uses several mobility models, which we especially proposed and tailored for forensic analysis. These models resemble other existing mobility models except that they are simpler since in our scenario we are not concerned about the various microscopic details that conventional mobility models usually take great care to describe precisely. This, however, does not mean that these models do not need to be evaluated independently, but such evaluation will have to be undertaken alongside the evaluation of our multi-modal trace reconstruction system since they are part of it. In other words, we developed these models especially to be used with our trace reconstruction system, and as such they cannot replace the normal mobility models in applications where the conventional mobility models are usually used (e.g. for evaluating protocols) because they would not generate precise node mobility traces, rather they would only generate the time delay that simulated nodes would generally take in traversing a particular area or route. This behaviour, however, is useless in most mainstream (non-forensic) applications using mobility models. Thus, we felt that evaluating these mobility models (which, for the sake of distinction, we called "mobility delay models") without actually using them in an implementation of our trace reconstruction system, has little value as they may not be used elsewhere. Therefore, an immediate extension to this thesis is to implement our multi-modal trace reconstruction system and evaluate it in practice, but this will likely take quite sometime given the detailed structure of the system. We believe that this system has the potential of going beyond academic research to find its way to the real world and be an important tool which law enforcement can use in real modern criminal investigations.

1.6 Live Vehicular Forensics

In appendix **??**, we showed that significant evidence can be extracted from modern intelligent vehicles due to the rich set of sensors they are equipped with. We considered each sensor individually and discussed the evidence that can be obtained from them. A possible extension to this work is to characterise and fuse such sensor data sources. Most of this data is, however, volatile, thus it would be interesting to investigate what kind of non-volatile data[1] that common vehicular systems preserve and store in-memory. Our expectation is that most of such data is not relevant to the forensic behavioural analysis of individuals. However, some automotive functions may be capable of storing useful information as part of their normal operation, possibly with user interaction. For example, most navigation systems maintain history records of previous destinations entered by the user in addition to a *favourite locations* list and a *home* location bookmark configured by the user; such data and configurations are likely to be non-volatile and can be easily retrieved at later times. Moreover, these systems may also contain information on *intended* movement, which is of particular interest if it can be communicated to investigators in real-time, that will enable anticipating target movements. Finally, it will also be interesting to investigate counter-forensics mechanisms, which may also be relevant in some cases (for example, investigating whether hired vehicles have been tampered with in anticipation of industrial espionage).

1.7 Final Remarks

In this thesis, we investigated and studied a computational forensic discipline that we believe has significant relevance to modern crime investigation and prevention technologies, we call this discipline "forensic tracking". Forensic tracking and surveillance is the process of investigating and reconstructing the location of a target (or targets) for forensic purposes. Like conventional tracking, forensic tracking can either be online or offline. We studied and elaborated in both types while considering different environments and settings. We proposed algorithms for passive online pedestrian and vehicular forensic tracking, then proceeded to consider vehicular offline forensic tracking and finally concluded with offline multi-modal forensic tracking, which is the most challenging as it combines both vehicular and pedestrian settings. This thesis demonstrate the practical importance and relevance of forensic tracking and surveillance and envisions that this discipline will become an integral part of modern criminal investigations, while still posing interesting academic research for years to come.

[1] Data captured by the Event Data Recorder (EDR) is non-volatile, but it is not always interesting or relevant for forensic investigations; see appendix **??**.