GLOBAL POSITIONING SYSTEM FORENSICS IN VEHICULAR AD-HOC NETWORKS

[1]BHAGYASHREE GADEKAR, [2]R.V. DHARASKAR, [3]V. M. THAKARE, [4]KOMAL SHARMA

[1]Research Scholar SGB Amravati University and Assistant Professor, Department of Computer Science, Priyadarshini Indira Gandhi College of Engineering, Hingna Road, Nagpur, Maharashtra, India.
[2]Director, MPGI Integrated Campus, Nanded, Maharashtra, India.
[3]Professor and Head, Computer Science, Faculty of Engineering & Technology, P. G. Department of Computer Science, Sant Gadge Baba Amravati University, Amravati, Maharashtra, India.
[4]Assistant Professor, Department of Computer Technology, Priyadarshini Institute of Engineering and Technology, Hingna Road, Nagpur, Maharashtra, India.
E-mail: bdharaskar@gmail.com, rvdharaskar@rediffmail.com, vilthakare@yahoo.co.in, komalmsharma@gmail.com

Abstract- Global Positioning Systems (GPS) have become more affordable and are now widely used in motor vehicles and in other frequently used applications. The principal purpose of vehicle tracking systems is generally to provide real-time information for efficient traffic control; they also serve an important security function along with enabling vehicles to alert each other with information like speed, position, acceleration and road conditions over short and medium range wireless networks called Vehicular Ad Hoc Network (VANET). By continuously displaying up-to-date location information and identifying vehicles that deviate from planned routes or cross specific boundaries, the GPS devices help protect assets that include the vehicles themselves and their high-value contents. As a consequence GPS are increasingly becoming an important source of evidential data for digital forensic investigations. The aim of this paper is to provide the guideline of recovering forensic data from widely used GPS devices. These devices are in-car navigators, Smart Phones, Digital Cameras, and so on. Evidentiary data can be gleaned from these devices to allow the recreation and tracing of the path taken before, during, and after a crime.

Keywords- GPS, Vehicular Ad Hoc Network, Indentifying Vehicles etc.

I. INTRODUCTION

Global Positioning System (GPS) networks have become a part of everyday life, possibly more than many realize. The positioning elements of GPS devices not only assist drivers in getting to their destination but also help with a large number of tasks. Vehicular Adhoc Networks uses the GPS devices in wide variety of applications such as Unmanned Arial Vehicles (U.A.V.) to operate autonomously, tracking of vehicle fleets, cargo, rental vehicles, bank cash vans etc. With the importance and ubiquity of tasks relying on GPS infrastructure it is worth considering the possible forensic implications of this technology. Devices receiving GPS information have access to precise location information as well as extremely accurate time data. It has already been established that in the case of automotive satellite navigation systems it is possible to retrieve historical location data based on the information received from GPS networks. The modern devices are equipped with much more inbuilt functionality such as Bluetooth, media players, calling facilities etc. which are proved to be very important sources of digital forensic investigation. We focus on the acquisition and subsequent analysis of source data from a range of GPS aware devices which can be there in a vehicle at the time of occurrence of the evidence. These devices can be PDAs, Smart phones also. Many of these GPS enabled devices make use of storage in the form of internal flash memory, external flash media and hard disks in order to store operational data, logs and other potentially significant data. In a forensic context, the extraction of log and user related information is at increased priority. The data recovered can be used to assist a diverse array of criminal and civil investigations. In particular dates, times and geographical positions may be valuable in reporting events of interest. GPS related research has focused on the forensic analysis of TomTom devices. Nutter, Garmin, Magellan, provided a detailed forensic account of identifying and extracting GPS location records and other data. Mobile smart phones and PDAs are the huge source of information widely used for forensic investigations.

2. Information that can be extracted from the GPS Devices

Depending on the manufacturer and model, GPS devices may contain some or all the following information:

- Track Logs
- Track Points
- Waypoints
- Routes (Google Map)
- Stored Location; Home, Office, etc…
- Security Location
- Recent Addresses (Longitude, Altitude)
- Call Logs (Missed, Dialed, Received)
- Paired Device History
- Incoming/Out Going Text Msg
- Videos, Photos, Audio

The above Information can prove to be very fruitful for the forensic analysis in Vehicular Ad hoc Networks.

3. Widely Used GPS Devices with respect to VANET forensic analysis

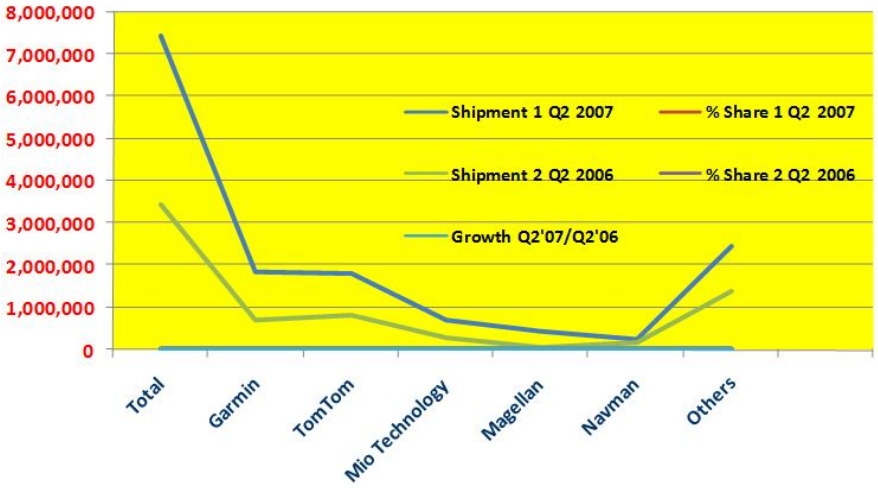

Fig. 1. Various GPS devices used in forensic analysis

1. Tom Tom:

TomTom are the most widely used GPS deviced since they provide for biking, hiking, and car navigation. Depending on the capabilities of the model, several different types of digital evidence can be located on these devices. In several TomTom models (Go 510, Go 910, Go 920 etc.) the facility of pairing mobile phone to the device is there and hence they can use the TomTom as a hands free kit. In this case the TomTom will store the Bluetooth MAC ID for up to five phones, erasing the oldest if a sixth phone is paired.

Depending on the phone model paired with the TomTom, there may also be files contains Call lists, contacts and text messages (sent & received) stored in the device for forensically analyzing TomToms is TomTology as

File Name	Purpose
\contacts\called.txt	Numbers called by the phone paired to the tomtom
\contacts\callers.txt	Numbers of phones which have called the phone paired to the tomtom
\contacts\contacts.txt	Details of numbers in the address book of the phone paired to the tomtom
\contacts\inbox.txt	Incoming text messages
\contacts\outbox.txt	Outgoing text messages
TTGO.bif	Device information (e.g. Serial number) and current home location
settings.dat	Name and MAC address of a paired phone, if one has been connected, wireless data settings and data provider if this has been set up, and home phone number information and owner information, if set10
\itn\	Directory containing itineraries, if any have been entered

Table. 1. Various file types

All the “on route” details can be retrieved from both live and unallocated space. It help us to retrieve the information about home, favorites and recent destinations, the last journey details as where the TomTom last had a GPS fix and also extract phone numbers of the paired mobile phone with deleted phone numbers, useful for potentially tracing a previous owner. As of 2012, TomTology has been superseded by TomTology2. This new program has the same functionality as TomTology but also deals with Garmins (live and deleted) and Navmans. It also include inbuilt mapping.

II. GARMIN

Zhe next modern GPS device which is widely used is Garmin. It also connects to a PC via a USB cable. It mounts itself as a Mass Storage Unit, similar to a USB Memory Stick. Navigation through the file system is possible after drivers for the unit have been loaded.Maximum of the Garmin files can be opened in normal text editors and the forensic related data including waypoints, date & time stamps, latitude & longitude coordinates and elevations can be extracted from the Current.gpx file located in the

\Garmin\GPX\ folder. All data of recent trips are stored in this file. Data can also be easily viewed via import feature of Google Earth. Google Earth can also import waypoints, tracks and routes from the unit. A slider bar in the program will show saved routes by date and time. When a specific waypoint is selected, a window will open that shows Latitude /Longitude Coordinates, Altitude, Speed, Heading and Date/Time (Zulu). With this data, raw or when viewed in Google Earth, entire trips can easily be reproduced giving exact time and locations for the GPS unit. It is unknown how many trips the unit is capable of storing or will store by default, but the Garmin Nuvi 260W test unit had 16 days of trip data stored to memory.

III. MAGELLAN

Magellan GPS device also connect to a PC via a USB cable. Some of its models such as Roadmate 1400 unit tested runs a version of Windows CE. Backup and restore functionality via a SD memory card slot can be extraced only if connected to PC. Magellan provides VantagePoint software to view map and waypoint data after connecting it to a PC. Google Earth also supports Magellan units via its import feature. Earth lists Explorist and Serial are the available import options.

4. Mobile Cell Phones/Smart Phones:
Mobile Cell phones are powered units that can compute the complexities of GPS data. These are very versatile devices that can be used to get wide variety of data for forensic analysis in VANET.

The availability of locational information in these devices is not always an intentional design choice, for example a device wirelessly connected to a Wi-Fi access point (AP) or cellular tower may record the service set identifier (SSID) or cellular id of the connected network [6]. Such recordings can be compared against available databases such as those offered by SkyHook and Google which match SSIDs and cellular IDs against physical locations.

The Multipathing errors caused by satellite signals being reflected off buildings creates multiple signals that the GPS must read and attempt to distinguish which signal should be used for position reporting. This can lead to an incorrect location that is recorded to a GPS log and shows the cell phone owner at a position other than where they had been. An Assisted GPS (AGPS) helps to negate this factor by relaying information to the cell phone and performing the GPS computations within the network.

Now a days most of the mobile phones has AGPS. These can record the paths travelled along with date/time, which can be very useful in forensic investigations under forensically sound conditions.

5. Digital Camera Images with GPS Information:
Recent digital cameras have built-in GPS receivers which it possible for the camera to record where exactly a photo was taken. This positioning information (latitude, longitude) can be stored in the Exif metadata header of JPEG files. Tools such as jhead can display the GPS information in the Exif headers. External GPS device can also be connected to the digital camera [8].

IV. FORENSICS EXAMINATION USING GPS DEVICE

4.1 General forensics examination Procedure in VANET:

VANET forensics is processes which contain 4 phases.
They are:

1. Collecting
2. Preserving
3. Analysis and Extracting
4. Presenting Digital artifacts and Documentation

4.1.1 Data Collection:
In this phase evidentiary value, digital data and storage media data are identified and collected.

4.1.2 Preservation:
Preservation phase involves the search, recognition, documentation, and collection of electronic-based VANET evidence. The Cryptographic hashing and checksums algorithm, documentations are all key component of the preservation phase.
It normally consist Securing and Evaluating the Scene after incident is occurred.

4.1.3 Analysis and Extracting:
By the use of various technologies the VANET forensic investigators will attempt to filter the GPS data which will be useful for proper analysis of the evidences.

Few of them include comparing cryptographic hash values of known good and known suspect files against a dataset.

4.1.4 Presentation and Documentation:
In the final phase of VANET forensics investigation the potential artifacts of evidentiary value are presented in a variety of forms.

4.2 GPS Devices and Preservation of Evidence:
In VANET, GPS have become an affordable and important source of evidential data for digital forensic investigations. GPS forensics SatNav (Satelite Navigation) Forensics, is the reliable and repeatable process of acquiring, examining and analyzing GPS devices for evidence of a criminal act or information of interest.

Evidentiary data can be collected from these devices to allow the recreation and tracing of the path taken before, during, and after a crime. Hybrid GPS devices equipped with a Bluetooth capability allow GPS devices to act as a handsfree device for mobile phones and therefore have the potential to contain much of the same data discovered during a mobile phone examination.

4.3 Satellite Navigation, GPS Devices and Data Collection:

More useful evidences are provided GPS Systems in cars and the more recent growth of such systems on Smart phones, PDAs, tablets, means that they can now be a useful evidence type in criminal cases.

The accuracy of a Satellite Navigation position depends on from how many satellites the device is currently receiving signals from. GPS receivers are a multi-channel device, which means they can receive a signal from multiple satellites at once. Higher the number of signals, greater is the accuracy of the positional data. When there is a fix on at least 6 satellites the data is accurate to within 20 meters, when the fix is on 10-12 satellites then the accuracy is typically within 5 meters.

The GPS consists of 24 earth-orbiting satellites so as to guarantee that there are at least 4 of them above the horizon for any point on earth at any time. There are normally 8 or so satellites which are "visible" to a GPS receiver at any given moment. When a Sat Nav is used in a built-up area and hemmed in by tall structures as tower and buildings, the satellite signals will often bounce off the building's exterior surfaces. These types of signals are called "multipath reflections" and may incorrectly report a device's location up to hundreds of metres away.

4.3.1. GPS Data Collection:

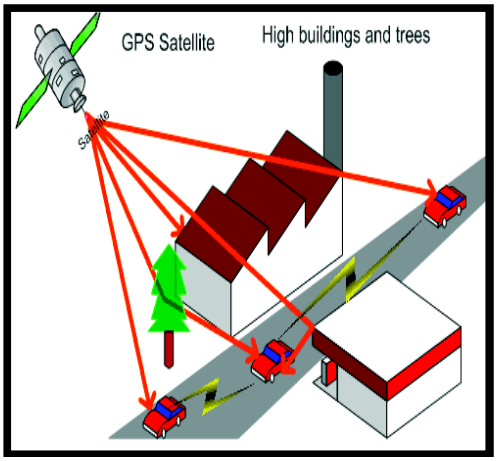

Fig 2: GPS communication in VANET

Step1: Normally, the satellite navigation system is supported by a number of ground stations that monitor the data sent by the satellites and transmit correct data back to the satellites. As the satellites orbit the earth they send out two different radio signals designated L1 and L2. L1 is set aside for civilian use and transmits data that can be read by civilian receivers to determine location. These signals contain three pieces of information called ephemeris data, almanac data, and pseudorandom code.

Ephemeris data contains the precise location of the satellite as well as the locations of all other satellites in the system. Almanac data includes the time and date of signal transmission, as well as the operational status of the satellite at the time of transmission. The last piece of information sent is the pseudorandom code, which is simply an identification code for the particular satellite that is transmitting the data signal.

Step2: All of this data is used by the GPS receiver to decipher the position of the receiver in relation to the satellites.

Step3: The GPS receiver collects the signals from the satellites and interprets them to give the user a fixed location.

In order to accurately evaluate data a GPS receiver needs to have either a two dimensional (2- D) or three dimensional (3-D) fix on orbiting satellites. A 2-D fix means that three satellites are being tracked and the GPS receiver can calculate latitude and longitude of the receiver as well as the user's movement. Having a fix on four or more satellites is considered a 3-D lock and adds the additional capability of calculating altitude. This system is based on line of sight and therefore some errors and coverage issues exist. Standard GPS receiver will not only place us on a map at any particular location, but will also trace our path across a map as we move. It can tell us:

1. The distance travelled
2. Total time of travel
3. Speed of travel
4. Average Speed of travel
5. A trail showing you exactly where you have travelled on the map and
6. The estimated time of arrival at destination if current speed maintained.

With the use of AGPS system the LBS maintains data on the network regarding the current location of satellites as well as estimates of future range and position of these satellites. This behavior of estimating satellite position is called "predictive ephemeris" and allows for a quicker initial 2-D, or 3-D, fix and more accurate position reporting. Since the network already knows which cellular tower the phone is operating from, it has a general idea where the user is located and can substantially decrease the

requirement for processing data by using predictive ephemeris that will reveal an accurate location. Almost all cell phones or service providers offer standalone GPS capabilities and the GPS functions of the cell phone might only operate with the aid of AGPS, this means the user must be within the provider's coverage area to gain any GPS data[7,11].

4.3.2 Forensic cases of GPS in VANET:

The types of devices discussed in the previous sections and Methodology of VANET forensic investigation used to investigate the cases and carry out forensics examination of GPS devices along with acquisition phase of an SD card. The first thing to consider are what type f case is there. The following are the most widely considered categories of cases in VANET:

1. Accidents/ Hit and Run
2. False Signals and Alarms
3. Missing rented vehicles and Bank cash-vans

Some of the common criteria for taking a case include:

- Whether it is a criminal or civil case.
- The impact on the investigating organization
- Whether the evidence is volatile or nonvolatile
- Legal considerations, such as the types of data that might be exposed
- The nature of the crime

A general case intake form needs to be completed when reviewing a potential case and determining whether to accept it. Among other issues, the form requests information to check for any conflict of interest between the concerned parties. This form confirms the understanding and agreement among the parties involved and sets the stage for everything else about the case, such as chain of custody and basic evidence documentation.

4.3.4: Forensic use of the collected data in VANET:

As discussed the nature of data as in section 2 and 3.3.2 the data collected by the processes discussed above we can find

- The Home location
- The Favourites
- The recent Destinations
- A list of addresses that have been entered manually
- The last journey that was plotted(if stored)
- The location of the Vehicle it last had a GPS Fix.
- Call Logs
- Waypoints
- Files updated /Deleted
- Call Log deleted
- Contacts
- GPRS data
- Google Earth/Map data
- And many more.

The above data can be analysed and investigated by using number of applications offered by vendors that are created for use by investigators to examine and retrieve forensic evidence from GPS devices. Applications such as Point 2 Point and Device Seizure offered by two prominent companies Paraben Corporation and Berla Corporation [12,14] are widely used. Device Seizure is an all-in-one application that can be used to examine data on multiple handheld devices, like cell phones, PDAs, and GPS units. This application captures device settings, maps, waypoints, tracks, and routes from the GPS along with saving this data and creating a *.GPS file that will incorporate all of the point data from the waypoints, tracks, and routes which can be used with Paraben's Point 2 Point. Point 2 Point is a software package that can be used in conjunction with the *.GPS file to display all recorded points in Google Earth to gain a map perspective of the locations where the GPS device had been taken. Berla Corporation [13] offers software applications by the name of Blackthorn and TomTology [15]. Blackthorn is specific to GPS analysis and will pull all relevant data pertaining to the data logs that include waypoints, tracks, and routes. This data can then be exported directly into Microsoft Excel so that it can be easily manipulated and placed into other applications. It also works in conjunction with Microsoft MapPoint and can plot all data points onto a map in a similar fashion as Paraben's Point 2 Point, in order to visualize the travels of the GPS device. TomTology is another software that is specific to the analysis of GPS units made by TomTom. TomTology essentially does what the other software packages do in that it records all of the pertinent data. All the above data sets can be viewed in Google Earth just as Specifically for the GPS forensics purpose, the applications mentioned above are created. These investigations are directly applicable to VANET forensics. There are other applications available that can be used to view stored GPS data, or to manipulate data in other applications or on the GPS. Some applications support "geotagging" which is a term for linking GPS data to digital photos. This is done by way of pairing up a GPS track log with the timestamps found on digital pictures.

Like the GPS devices that are specifically made to track and log the movement of a desired object, there are a number of services associated with tracking and logging. A couple of companies that offer such services are LandAirSea and LiveViewGPS. With these services an individual can deploy GPS tracking units on a fleet of vehicles, parents can track their children, or valuable assets can be tracked for security purposes. Some options with these services

are simply logging devices that can be purchased by a user and attached to the item they wish to have tracked. The device utilizes battery power and can be easily transferred from one item to another, and the data tracks can be downloaded to a computer for examination. Other devices offer the capability to hardwire a tracking device into a vehicle's power system in order to have sustained power to continuously log and track the vehicle position.

Another application that supports image modification is DeLorme's XMap. This has unique capabilities that refer GPS data with an image. XMap is a geographic information system (GIS) tool that allows users to capture, manage, and manipulate geographic data. A user can easily upload or download specific data points, such as waypoints, routes, and tracks, to or from the GPS device.

CONCLUSION

The digital forensic examination of GPS devices has been carefully researched and experimented with for their applicability to Vehicular Ad hoc networks. The reason of forensically carry out an investigation on a GPS devices is to test the feasibility of the forensic investigation of GPS devices as opposed to our standard forensic investigation of digital devices such as computer hard drive and their wide use in VANET. Due to the wide use of the GPS devices in our modern world, the forensic examination of such devices can be used to as a piece of irrefutable evidence in a court of law which can be used to solve some of the serious crimes in the VANETs such as Accidents (Hit-and- Run) Cases, False Warnings and Messages, Tracking of missing vehicle, etc. These investigations can prove themselves as boon to the Digital Forensic Investigations in VNET. We aimed for providing the guideline of recovering forensic data from widely used GPS devices.

We concentrated on most widely used GPS enabled devices which include in-car navigators such as TomTom, Garmin etc., Smart Phones, Digital Cameras, and so on. Evidentiary data which can be gleaned from these devices to allow the recreation and tracing of the path taken before, during, and after a crime are presented in a detailed fashion along with the most prominently used application software involved in forensic investigations in GPS and VANET.

REFERENCES

[1] http://www.forensicswiki.org/wiki/ Global_Positioning_System

[2] Chad Strawn, "Expanding the Potential for GPS Evidence Acquisition", Small Scale Digital Device Forensics Journal, VOL. 3, NO. 1, JUNE 2009 ISSN# 1941-6164

[3] http://www.forensic-access.co.uk/sat-nav-forensic-science-services.asp

[4] Peter Hannay, "Geo Forensics: Classes of Locational Data Sources for Embedded Devices", IACSIT International Journal of Engineering and Technology, Vol. 5, No. 2, April 2013

[4]. Beverley Nutter, "Pinpointing TomTom location records: A forensic analysis", Elsevier Digital Investigation Volume 5, issues 1–2, September 2008, Pages 10–18

[5] Smith, N. M. GPS gis and position tracking technology privacy and law enforcement. Retreived http://www.computerforensic-technician.com/wordpress/ gps-gis-and-position-trackingtechnology- privacy-and-law-enforcement/

[6] X. Wang, A. K. S. Wong, and Y. Kong, "Mobility tracking using GPS,Wi-Fi and Cell ID," in Proc. Information Networking (ICOIN), 2012 International Conference on, 2012, pp. 171-176.

[7] LaMance, J., Jarvinen, J., & DeSalas, J., " Assisted GPS: A low infrastructure approach", http://www.gpsworld.com/ gpsworld/article/articleDetail.jsp?id=12287

[8] Emerick, D. (2008, February 5). "Jobo announces GPS digital camera add-on" http://emerick.blogspot.com/ 2008_02_01_archive.html

[9]. Cusack, B. & Simms, M. (2011). Evidential Recovery from GPS Devices. Journal of Applied Computing and Information Technology Vol. 15, Issue 1. ISSN 2230-4398.

[10] GPS Passion. (n.d.). GPS explained, http://www.gpspassion.com/Hardware/explained.htm

[11] Köhne, A. & Wößner, M. (2007, March 4), "Sources of errors in GPS", http://www.kowoma.de/en/gps/errors.htm

[12] Paraben Corporation.. Device seizure v3.4. http://www.parabenforensics.com/catalog/product_info.php ?cPath=25&products_id=405

[13] Berla Corporation. Blackthorn. http://www.berlacorp.com/blackthorn.html

[14] Paraben Corporation.. Point 2 point v2.0. http://www.parabenforensics.com/catalog/product_info.php ?products_id=404

[15] Forensic Navigation. TomTology http://www.forensicnavigation.com/#/products/4527490520

[16] LandAirSea Systems. How GPS tracking works? http://www.landairsea.com/about/gps-tracking.html

[17] C. Valli and P. Hannay, "Geotagging Where Cyberspace Comes to Your Place," presented at the Proceedings of the 2010 International Conference on Security and Management, Las Vegas, 2010.

[18] LiveViewGPS. What will LiveViewGPS do for you? http://www.liveviewgps.com/

[19] DeLorme. XMap 6 GIS software suite http://www.delorme.com/xmap/

[20] Van Eijk, O., & Roeloffs, M. (2010). Forensic acquisition and analysis of the random access memory of tomtom GPS navigation systems, Digital Investigation 2010, 6 (3-4), 179-188.

★★★