International Journal of Scientific & Engineering Research, Volume 4, Issue 8, August 2013
ISSN 2229-5518

Wireless Device Localization Using Vehicular Ad-hoc Network

Joseph John, Lakshmi K S

Abstract— With the advance in wireless technology and the increase in use of wireless devices the need for technologies and tools to localize or locate wireless devise has become important, especially in law and order. This paper presents a novel idea to localize a wireless device using VANETs.

Index Terms— VANET, Beaconing, GPS, localization, Road side unit, MAC address.

1 Introduction

Network security has become an important law and order issue of this decade. The economic and human cost involved in it is unprecedented. Last year alone 30 million people in India and 431 million people globally were victims of technology related crimes. Billions of dollars are spent globally to counter network related attacks. There are meant tools and technology invented and used today for this counter attack. Surveillance tool is one such tool that plays a major role in fighting this crime wave. Surveillance tool are used to locate and localize a device so that we can find its position in a map. Many surveillance tools have been proposed and designed to locate a device in a infrastructure network but not much have been done to locate a device once it leaves the network this infrastructure network, i.e., when the device 'go out of range'. Once a crime has been committed no culprit will stay in the scene of crime. So it is essential we find an efficient method to track down a device once it goes out of the network. This paper proposes an idea in this matter.

2 Basic Idea

There are many existing technologies and tools to find the malicious device by analysing the traffic in a network. We can find its IP, MAC id and other details using these technologies. The problem arises when the device leaves the network or go out of range (from now on we will call this network with infrastructure as infra-network to distinguish it from VANET which is an ad-hoc network). The idea behind this paper is to extend the methods, ideas and algorithms used in infra-network to an ad-hoc network and use this ad-hoc network to locate the device once it leaves the infra-network. The ad-hoc system used here is VANET.

VANET stands for Vehicular Ad-hoc Network. It is an adhoc network with vehicles as the nodes. These vehicles are intelligent enough to communicate with neighbouring vehicles or nodes. Nodes in VANET can also communicate with RSUs or Road Side Units. They are deployed on the road, positioned in such a manner that vehicles driving past it can communicate with it. RSU [1] can collect and relay in formations to vehicles. The communication in efficiency in VANET nodes mainly speed of the vehicle (node speed) and the density of vehicle (node density), but we will see that both are not a problem in this proposed system.

Usually when we refer to VANET it has nodes coming and going out of it regularly. In a moving traffic we cannot be sure of the number of vehicles that will communicate with a specific node at a specific time, i.e., the number of nodes is not predefined, but in this system we use a predefined number of nodes. The idea is that once a command is given to locate a device a set of prearranged and pre-programmed VANET nodes are deployed. These nodes communicate only with each other and not with other vehicles. These nodes are responsible for the localization of the malicious device. If we allow it to communicate with other random vehicles or enable addition of the accuracy of surveillance may increase but this increase in accuracy comes with communication overhead. So it is advisable to use a predetermined number of VANET nodes. Another advantage is that node density and node speed is not a big issue when we use a predetermined number of nodes. The number nodes can be determined by the cost factor and the efficiency in communication between VANET nodes.

The whole procedure of device localization can be divided into four steps

- Identifying the device and its MAC address
- Relaying the information to the VANET
- Locating the device using VANET
- Plotting the device

Each step is explained in detail, in the sections below.

3 Identifying the device and its MAC address

As mentioned above this proposed idea is to locate a device which has committed a crime and then left the infra-network. So we need to find which device committed the crime in the infra-network before we can pass it into VANET.

- *Joseph John is currently pursuing masters degree program in network engineering in Mahatma Gandhi University, India. E-mail: josephjohn2010@gmail.com*
- *Laskshmi K S is currentlyworking as Assisstant professor in Rajagiri School of Engineering and technology,India. E-mail: lakshmiks@rajagiritech.ac.in*

Every device that can communicate has a unique MAC id associated with it. So if we find the MAC id of the device we can identify the device itself. One method to find the MAC id of devices communicating in an infra-network is by analysing the traffic and the traffic pattern in the access points. Once the analysis is complete we can identify all the devices which are present but more importantly in this case, which were present. By comparing the traffic corresponding to each MAC id we can locate the malicious mobile device. There are many tools to find a device in an infra-network using this traffic analysis method. 'The digital marauders Map' [2] is one such tool. Tools like Marauder's Map give detail explanation about how to capture the traffic, analyse it, locate the devise and plot it on to a map, in an infra-network. The Marauders Map also specifies three localization algorithms to efficiently locate the device in n infra-network. But like many other tools it fails to explain what to do when the device leaves an infra-network.

So we do here is, we use available methods such as the Marauders Map to find the information about malicious device, by analysing the information in the infra-network where the crime has been committed. We mainly need only the MAC id of the malicious device. Once we get this MAC id we relay this information to the VANET. Then VANET use this information to locate the device.

4 RELAYING THE INFORMATION TO THE VANET

Once the MAC id has been found out we need to relay it to every node of the VANET. For this we can use SMS or technologies similar to it.

The infra-network admin can do this relaying of the information but its better we employ a central agency, like the cyber cell, to do it so as to ensure that people don't exploit it with vicious intend. In almost all cases it has been found that the method used to control or limit exploitation itself becomes a medium for exploitation. By employing a central command centre and proper protocols we can ensure this exploitation never happens. In Kerala for example all cyber and mobile tracking is headed by the cyber cell of that state. So we can use this same cyber cell as the central authority which can relay the information to the VANET.

To ensure safe and responsible usage of this proposed idea we can program the VANET nodes in such a way that it tries to locate a device only if it receives information from a particular device (or number if it's SMS) or group of device. As mentioned before in this VANET the number of nodes interacting is predefined and known beforehand. There is no new addition of VANET nodes once the devices are deployed. So we can manually program the devices from which the VANET nodes are supposed to receive instructions. The advantage is that new commanding device can be added and deleted as the need arises.

We can also prioritize the devices; instructions from one device can be given priority than other. For example if a commanding device from two different districts is relaying an instruction to the same VANET, at the same instant we can give priority to the district which is geographically nearer to it. Or the priority can be based on the nature of the crime. Tracking down of a device used to assist a terrorist should be given more priority than a device used for uploading a pirated movie. The priority can also be on the basis of the authority relaying the information. For example defence organizations like army or intelligence agency should be given more importance than local police. So depending on different model we can use the system in manner which suits the situation most.

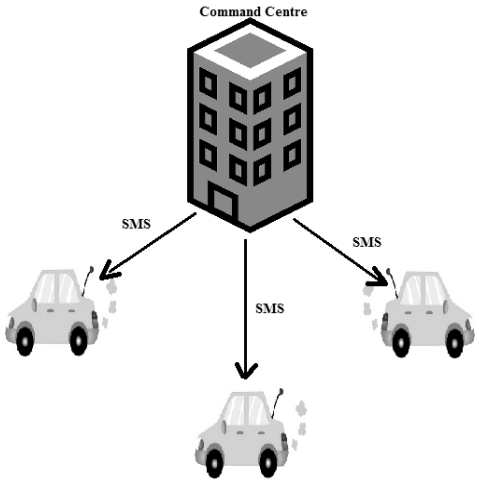

Fig. 1 Relaying information

5 LOCATING THE DEVICE USING VANET

Once the instruction is received through a central authority, the VANET is deployed in a geographical area. Then each VANET node search for the malicious device. How the search is done is explained below. The VANET nodes are positions in such manner that if the malicious mobile device is present in that geographical area it will be located by more than and VANET node when the search is done. The location or localization of the device has three main steps:

- Communication between VANET nodes
- Probe for the device
- Use the collected information to locate the device

5.1 Communication between VANET nodes

So as to properly locate a device each VANET node must know where the other nodes are. This location information has more importance in case of VANET because the nodes are constantly moving. So each node must be updated with the location of other nodes in a constant periodic time interval. There are four main method of communication in VANET-Beaconing, Geobroadcast, Unicast routing and information aggression [3],[4] .The method of VANET communication that is best suited in this scenario is Beaconing. In beaconing method each node informs every other node about its position and related details periodically. The period is determined in advance.

As you can imagine communication overhead may be a little high for this method of communication compared to other mentioned above. But a neighbouring node must know immediately if the malicious device has been located by any VANET node and also the position of the VANET node when it located the malicious device. The latter is essential because in locating the malicious device arc algorithms are used and to implement the arc algorithms the position data of each VANET nodes should be available to all other nodes in real time. The details about that will be explained in the next segment.

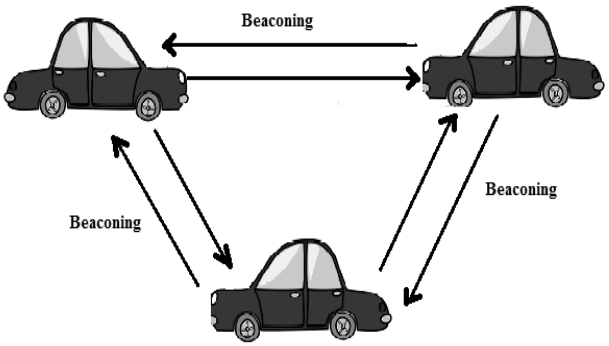

Fig. 2 Communication between VANET nodes

5.2 How to probe for the device

The malicious device can be probed by using sending a 'disassociation' signal with the MAC id of the malicious device as the destination address.

Each VANET node already knows the MAC id from the SMS instruction received. Once the malicious device receives the disassociation signal it gets disconnected from any network it is connected to at that instance. As soon as the malicious device get disconnected from a network it will have send a probe signal to identify the various network connections available. These probe signals will also reach one or more nodes of the VANET.

Once we get probe request with source MAC id as that of the malicious device we can confirm that the device is somewhere in the range of the VANET node. When the node identify that the malicious device is in its vicinity in informs all other nodes about the discovery.

Fig. 3 Disassociation signal

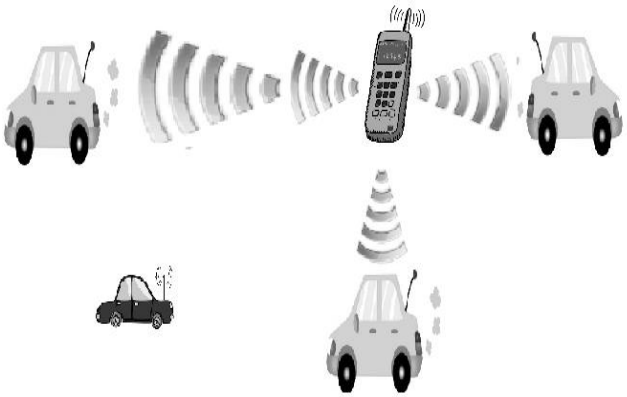

Fig. 4 Probe signal

5.3 How to use the collected information to locate the device

Once more than one VANET node has identified the device can use any of the available arc algorithms to locate the device [2]. As the number of nodes involved in the arc computation increase the accuracy of localization increase. So it is essential we position the VANET nodes in such a way that it the network probe request sent by the malicious device reach maximum VANET node.

There are many algorithms available to calculate the position of a mobile device in an infra-network if we know the details of the position of access points, with which it has communicated. We can extend these algorithms to VANET by taking the VANET nodes as the access points and implementing the arc algorithm on the basis of the position VANET nodes. There are two methods by which this calculation can be carries out.

One is to calculate the position in real time. This requires electing a leader node to do the calculations. The advantage

of this method is that we get the position of the malicious device fast. But the problem is that location accuracy may be compromised. This is because the network probe request from the malicious device may reach different node at different instance. So the signal may reach some VANET nodes after the leader node carries out the computation to find the malicious device. So as the number of nodes involved decreases the localization accuracy also decreases. But if we wait to make sure all nodes which have located the device are involved in the calculation, the malicious device may have moved to some other location and the position we calculated will be a faulty one. Also as the calculation is done by the VANET nodes themselves, the computation power of the nosed should be high and this will result in higher cost.

The second method is to relay the position of the VANET nodes that received communication from the malicious device, to the command centre. The command centre can carry out the localization computation without involving the VANET node. The advantage is that we can decrease the computation capacity of VANET nodes thereby decreasing cost. We can also ensure that all nodes which received communication from malicious device can be used for computation. Another advantage is that only the command centre has knowledge about the final position of the malicious device, this increases security.

Both methods involves transmission of the VANET node position between the nodes as well as the transmission of positions to the command centre The location is specified using longitudes and latitudes using GPS.

6 PLOTTING THE DEVICE

Once the calculation is complete instead of a specific longitude and latitude we get a set of longitudes and latiyudes. From that set we select an optimal point to locate it on a map. For plotting the device onto a map, using longitude and latitude, we will use Google map API.

7 IMPROVEMENT

The proposed method has a lot of avenues of improvement. One such area is the automatic positioning of the VANET nodes. When a VANET node has located the device and relays it position to other nodes, these other nodes can position themself such that more devices can locate the device. This job can also be done by the command centre by instructing the node to move to a more strategically advantageous position. Another method is to select a leader node so that it can instruct on changing positions.

Another method is to setup RSUs. These RSUs can help in things like malicious device location, better communication between VANET nodes etc. One other area of interest is the signal range of the VANET nodes. Many studies have been already carries about how to increase the Wi-Fi range and some of them has been already implemented [5], [6]. But there is no use of just increasing the range of the VANET nodes. This is because the disassociation signal may reach the malicious device if the range of VANET node is increased but if the Wi-Fi in the malicious device does not have much range then the network probe device may never reach the VANET nodes.

8 CONCLUSION

This paper proposes an idea on how to locate a malicious device outside an infrastructure network. This is idea if implemented will not replace the existing methods used to localize a mobile device, but it will work alongside it. The paper proposes some innovative methods in VANET implementation and more improvements can be made as the VANET technology advances.

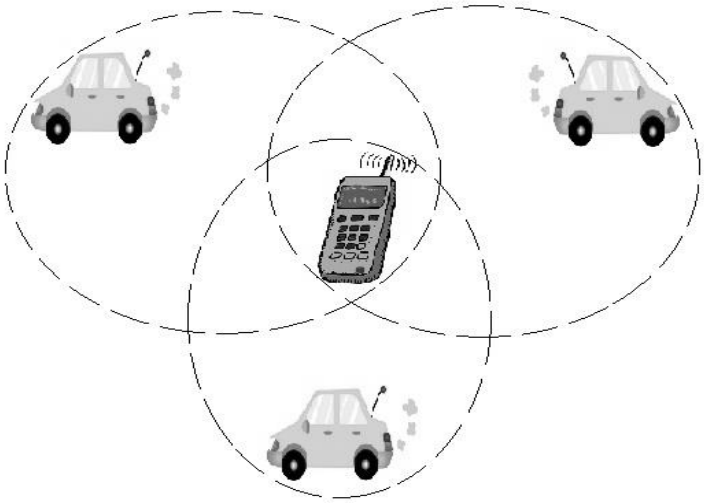

Fig. 5 Plotting the device

REFERENCES

[1] Enhancing VANET Connectivity Through Roadside Units on Highways Sok-Ian Sou and Ozan K. Tonguz, Member, IEEE, October 2011

[2] The Digital Marauder's Map:A WiFi Forensic Positioning Tool Xinwen Fu, Member, IEEE, Nan Zhang, Member, IEEE, Aniket Pingley, Wei Yu, Member, IEEE, Jie Wang, Member, IEEE, and Wei Zhao, Fellow, IEEE,2012

[3] Communication Patterns in VANETs, Elmar Schoch, Frank Kargl, and Michael Weber, Ulm University Tim Leinmüller, DENSO AUTOMOTIVE Deutschland GmbH

[4] Unicast Communication in Vehicular Ad Hoc Networks: A Reality Check,Mate Boban, Ozan K. Tonguz, and João Barros,December 2009

[5] WiLDNet: Design and Implementation of High Performance WiFi Based Long Distance Networks,Rabin Patra ,Sergiu Nedevschi ,Sonesh Surana Anmol Sheth,Lakshminarayanan Subramanian,Eric Brewer

[6] Very Long Distance Wi-Fi Networks,Rob Flickenger,Steve Okay,Ermanno Pietrosemoli,Marco Zennaro and Carlo Fonda