The security threats and logics to mitigate them in VANETs

Prof. Rituparna Chaki, University of Calcutta and
Visiting Professor of AGH University of Science & Technology

The progress and improvements of distributed networks have played a decisive role for researchers to consider new solutions for various VANET applications as: transportation, highway safety, driving assistance, disaster management system, and lots more. With the recent advancement in networking domain VANET is capable to serve many kind of remote monitoring and sharing those information by avoiding a huge resource installation cost. In order to achieve these goals a huge amount of information is needed to be shared through network. Sometimes it also includes private information like health related data of a person in case of remote healthcare or current location information in case of driving assistance etc. All this information is time sensitive and require robust and quick deployable network connections. In case of VANET, nodes (vehicles) are very dynamic in nature and frequently they can join and leave a network. So, node registration and maintenance of a neighbor table is becoming very complex. Hence, for this scenario, recognition of authenticate user is the first important issues. Information send by an authenticate user can also be manipulated. Sybil attack is a very common attack in case of VANET. It is the creation of multiple fake nodes broadcasting false information. A vehicle with On Board Unit(OBU) sends multiple copies of messages to other vehicle and each message contains a different fabricated identity. The problem arises when malicious vehicle is able to pretend as multiple vehicle and reinforce false data. In this way the network become congested. Another way is to send modified version of message and claims that the message comes from originator for the unknown purpose. This is called Node impersonation. A wrong and fake information purposely can be send by one node to another to create chaos scenarios. This scenario may create misinterpretation of the actual scenario. False information is sent by attackers to vehicle for selfish reasons. Some nodes are able to disclose the identity in the network and track the location of the target nodes. Some of the attackers use observer for monitoring the target nodes and send a virus to the neighbors of the target nodes. When the neighbors' of the attacker are attacked by virus, then they take the ID of the target nodes as well as target’s nodes current location. The attacker can also attacks the communication network to cause some problems to network or network's nodes. The nodes are unable to communicate, thus resulting in wastage of the nodes and network's resources.
Given the huge potential of VANETs as aides in disaster management, the need of the day is to investigate the threats and possible security measures to mitigate them.