A Survey on VANET Security: Issues, Challenges and Solutions

Ankit vasava[1] Prof Karishma Chaudhary[2] ,Prof. Tushar Raval[3]

[1] ME Student, Computer engineering, L.D. College of Engineering, Gujarat, India
[2] Assistance professor, Computer engineering, L.D. College of Engineering, Gujarat, India
[3] Associate professor, Computer engineering, L.D. College of Engineering, Gujarat, India

ABSTRACT

Vehicular Ad-hoc Network (VANET) is an foundation less system. It gives upgrade in security related systems and solace while driving. It empowers vehicles to share data with respect to security and movement investigation. The extent of VANET application has expanded with the current progresses in innovation and improvement of keen urban communities over the world. VANET give a mindful framework that has major affect in improvement of movement administrations and in decreasing street mishaps. Data partook in this framework is time touchy also, requires strong and snappy framing system associations. VANET, being a remote specially appointed system, fills this need totally however is inclined to security assaults. Exceedingly powerful associations, delicate data sharing and time affectability of this system, make it an eye-getting field for assailants. This paper speaks to a writing study on VANET with essential worry of the security issues and difficulties with it. Highlights of VANET, engineering, security necessities, assailant sort and conceivable assaults in VANET are considered in this study paper..

Keyword: - *VANET , Architecture of VANET*

1. TITLE-Introduction

Vehicular Ad hoc network consist of mobile nodes (vehicles embedded with sensors), fixed infrastructure (Road Side Access Point) and wireless interconnection to allow them to talk with each other. The most important service provided by these networks is driving safety. Almost 1.3 million people die in road accidents and additional 20-50 millions are injured worldwide. Road Traffic crashes ranked as 9th leading cause of death [1]. Some survey shows that 60% of accidents can be avoided if the driver gets the warning even before half a second of the accident [2]. VANET are subset of ad-hoc network working over vehicular domain. VANET has emerged as a solution and become a key component of Intelligent Transportation System (ITS). Main objective of ITS is improving traffic efficiency and providing better road safety. VANET serves the purpose by sharing road safety information, information related to traffic analysis, normal data (files, audio, video etc.) using uninterrupted internet connectivity.

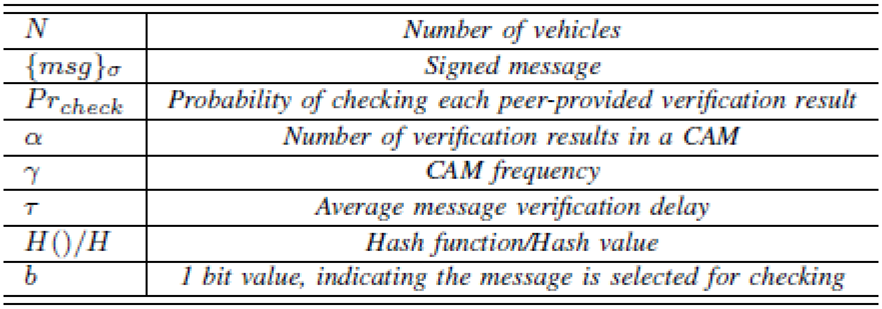
VANET differs from other ad-hoc wireless networks of this same class in these terms :

- High processing power
- Large storage capacity
- Energy sufficiency (as work over battery of vehicle).
- Predictable movement of nodes (as vehicles are bound to follow a certain path along the road).

2. Scaling VANET Security Through Cooperative Message Verification

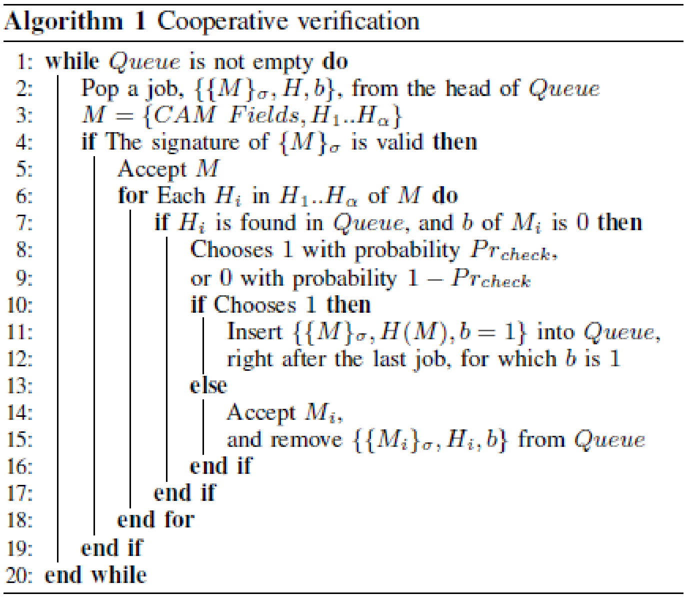
This scheme extends the traditional V2V message verification, leveraging neighboring peers to reduce validation delays without compromising the achieved security (and privacy). The basic idea is to augment each (safety) message with brief identifiers of previously validated messages. These identifiers indicate the corresponding messages have been verified by the sender. This is exactly where nodes can benefit from each other: accepting a message can help verifying the messages (received and queued) the identifiers in this message point to. In addition, to counter misbehavior, each node probabilistically selects a subset of the received identifiers and verifies by itself the signatures of the corresponding messages. Revocation would be triggered if any misbehavior is identified. Table I summarizes notation used in this method.

TABLE I: Notation



N	*Number of vehicles*
$\{msg\}_\sigma$	*Signed message*
Pr_{check}	*Probability of checking each peer-provided verification result*
α	*Number of verification results in a CAM*
γ	*CAM frequency*
τ	*Average message verification delay*
$H()/H$	*Hash function/Hash value*
b	*1 bit value, indicating the message is selected for checking*

Message Generation and Reception: The format of a signed CAM in our scheme is changed into:
fMg_ = fCAM Fields; H1::H_g_: (1)
Except the hashes, H1::H_, we assume the rest of the fields are as defined in the standard . H1::H_ are the hashes of latest verified CAMs (based on the timestamps of the CAMs, not the times of reception or verification). For Example , a vehicle, V , caches locally the hash values of the latest verified CAMs (for which V performed signature verifications, not cooperatively verified as described below) and includes them in its own (sent) CAMs. Every time a node receives a CAM, it generates a job based on the CAM. Here, we consider the processing of a received CAM as a job. The format of the job is defined as follows:
ffMg_; H(fMg_); b = 0 or 1g: (2)
The field b indicates the CAMs are selected for probabilistic checking. In case b is set to 1 for a job, the corresponding CAM cannot be verified through cooperative verification (peer provided hashes): the signature of this CAM must be verified. For each new job, b is set to 0. We assume a single thread for cryptographic verification in
each OBU: a CAM received when the thread is busy needs to be queued. To increase efficiency, we randomly select the inserted position in the queue for each new job. This way, we reduce the probability that nearby receivers verify the same CAM roughly simultaneously. The verification of CAMs that sent from a node does not need to follow the sending order, as long as they are verified before they expire. Cooperative Verification: Queue processing at a node is done according to Algorithm 1. When the queue is not empty, the node pops the first job from the queue, and accepts the CAM if the signature is valid. The hashes, H1::H_, are used to verify the CAMs (for which b = 0) in the queue. For each cooperatively verified CAM, there is a probability Prcheck,that the CAM will be checked by validating the signature. If so, b is set to 1 and it is inserted after the last job with b = 1(i.e., before the first job that b = 0). Otherwise, the CAM is accepted and removed from the queue.



```
Algorithm 1 Cooperative verification
while $Queue$ is not empty do
    Pop a job, $\{\{M\}_\sigma, H, b\}$, from the head of $Queue$
    $M = \{CAM\ Fields, H_1..H_\alpha\}$
    if The signature of $\{M\}_\sigma$ is valid then
        Accept $M$
        for Each $H_i$ in $H_1..H_\alpha$ of $M$ do
            if $H_i$ is found in $Queue$, and $b$ of $M_i$ is 0 then
                Chooses 1 with probability $Pr_{check}$,
                or 0 with probability $1 - Pr_{check}$
                if Chooses 1 then
                    Insert $\{\{M\}_\sigma, H(M), b = 1\}$ into $Queue$,
                    right after the last job, for which $b$ is 1
                else
                    Accept $M_i$,
                    and remove $\{\{M_i\}_\sigma, H_i, b\}$ from $Queue$
                end if
            end if
        end for
    end if
end while
```

FIG -2: Cooperative verification algorithm

this demonstrated how their cooperative message verification scheme could enable secure VC at network densities even double compared to those prior approaches could be workable for. Though this is achieved by trading off a tiny vulnerability window, they showed this can be harmless. In addition, their scheme is orthogonal to all prior optimizations and could complement them.

3. A New Anti-Jamming Strategy for VANET

DoS attacks to VANET can aim at different layers with variations of three basic techniques: buffer overflow at Network Layer and above, protocol violation at Mediu Access (MAC) layer, and signal inference by a radio emitter, called jammer, at Physical (PHY) layer. Jamming-style DoS attacks target at MAC and PHY layers, either by squelching the channel continually/randomly to block senders, namely active jammers, or by corrupting the data to target receivers upon sensing channel busy, called reactive jammers. The dominant way to defend against a jamming attack is retreat strategy: Channel Surfing to switch on another channel when the current frequency is blocked and Spatial Retreat to move on another location if the area involves interference. Recently, competition strategy is proposed for transceivers to alleviate jamming effects by adjusting their transmission powers and/or error correction codes. For example, Pelechrinis et al developed an Anti-jamming RE-Enforcement System (ARES). ARES loops back jamming measures to tune the carrier sense threshold, dramatically improved the throughput of various 802.11 wireless networks .

3.1 VANET SECURITY METRICS

Figure 1 illustrates a base to derive VANET security metrics Vehicles choose between two highway paths to reach a particular Destination: Normal Route and Alternate Route. When Normal Route gets congested due to ransportation dynamics, vehicles without VANET would still head towards the congested road segment as that was usually the shortest; those vehicles equipped with OBE will be informed by nearby RSE and/or neighboring vehicles to take the Alternate Route. If a jammer attacks the area where the two paths split, VANET denies its service to deliver the warning information in time to prevent the downstream vehicles from heading to the congested road segment. The jammer also effectively stops the warning messages from those vehicles stuck in the congested road segment to propagate, rendering VANET useless. A sophisticated jammer could inject false messages, telling the downstream vehicles that Alternate Route gets congested and luring more vehicles into the congested road segment.

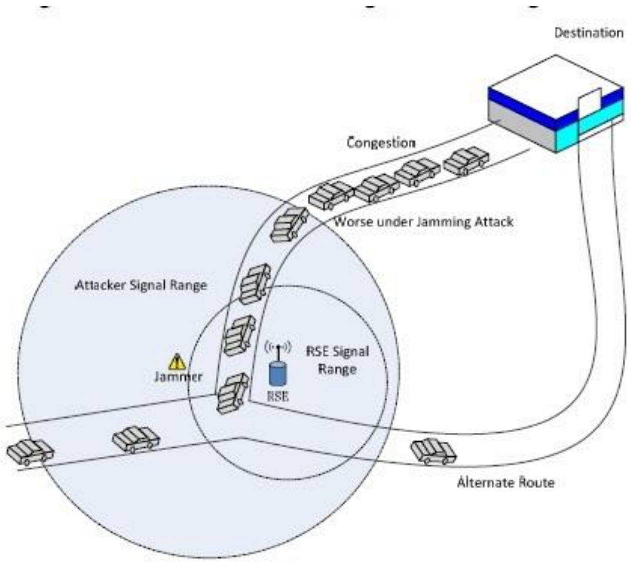


FIGURE 1: jammer Attack Scenario

3.2 Metrics Directed Defense

The sample VANET security metrics defined above direct a new defense class, Hideaway Strategy: upon detecting a jamming attack, a node stops sending signals and keeps silent until the jammer moves away. We anticipate that Hideaway defends VANET against active jammers effectively. A hybrid with Retreat Strategy would work against both active and reactive jammers. As Hideaway is a countermeasure, detection is out of the scope in this paper. Figure 2 shows a typical VANET architecture. It contains vehicles equipped with Onboard Equipment (OBE) moving in the infrastructure of Roadside Equipment (RSE) placed along the Field of a transportation environment following traffic operation.

.

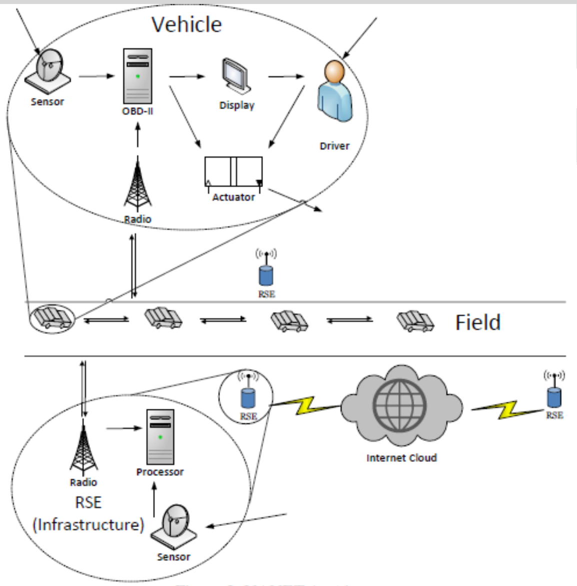


Figure 3: VANET Architecture

Fig -2 VANET Architecture.

OBEs communicate with each other and with RSEs via radio across the Field; RSEs communicate among themselves via the Internet. OBE has sensors such as lidar to detect potential collision with cars not equipped with OBEs while RSE has sensors such as cameras. The processor in OBE includes OBD-II to sense the car's own movement such as brake. Vehicle's actuator is affected by many factors including driver's reaction to the messages on display.

4. CONCLUSIONS

VANET being a wellbeing data sharing medium, needs secure and safe environment. VANET has wide scope for assaults because of its exceedingly powerful nature, remote medium of correspondence and every now and again evolving topology. Security issues and difficulties identified with VANET have high effect on productive usefulness of the system. Today, VANET are as a rule broadly sent because of its improving highlights of giving sheltered, secure and comfort driving. VANET, highlights of VANET, need of security in VANET are the hotly debated issues identified with the present situation. In this paper, we have done a writing study about different sorts of assaults, their preventive measures, kind of assailants what's more, some current security solutions for assaults in VANET.

6. REFERENCES

[1]. Road Crash Statistics- Association for Safe International Road Travel. Available:
http://asirt.org/initiatives/informing-road-users/road-safety-facts/roadcrash-statistics.

[2]. Maxim Raya et al., “The Security of Vehicular Ad Hoc Networks”,
SASN’05, Nov 7 2005, Alexandria, Virginia, USA, pp. 11-21

[3]. “Scaling VANET Security Through Cooperative Message Verification”
Hongyu Jin and Panos Papadimitratos
Networked Systems Security Group, KTH Royal Institute of Technology, Sweden
fhongyuj, papadimg@kth.se
www.ee.kth.se/nss

[4]. “A New Anti-Jamming Strategy for VANET Metrics-Directed Security Defense”
Ikechukwu K. Azogu, Michael T. Ferreira, Jonathan A. Larcom, Hong Liu*
Department of Electrical & Computer Engineering University of Massachusetts Dartmouth Dartmouth, Massachusetts, USA {U_IAzogu, MFerreira, JLarcom, HLiu@UMassD.edu}

[5] International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016
“VANET Security: Issues, Challenges and Solutions”
Rashmi Mishra , Akhilesh Singh , Rakesh Kumar