# Cooperative and Automated Vehicles Misbehaviour Detection

## COMS7003 Research Report 1

ABSTRACT: Cooperative Intelligent Transport Systems are the next step in road transport but brings many security risks. This research report looks at three threats involving misbehaving C-ITS stations and presents some academic and industry research into the same. With that in mind, the author devised system for detecting misbehaving C-ITS stations is described.

**Anthony Carrick**

*Table of*
# Contents

# Introduction

Cooperative Intelligent Transport Systems allowing vehicles to communicate their status and road conditions to each other hope to improve the driving experience, safety and efficiency of vehicles whether autonomous or manually piloted. However, complex technology with such potential, particularly wireless, is open to malicious modification, hacking, or even unintentional misbehaviour through fault. This research report introduces three threats involving misbehaving C-ITS stations and then provides a high-level look at some of the academic and industry research into misbehaviour detection. Finally, I propose a multi-technology, layered approach to detecting and reporting misbehaving vehicles with changing Pseudonym Certificates. Where appropriate I have tried to relate the research to the Australian environment.

# Electronic Threats from Misbehaving C-ITS Systems

## Masquerade

One threat to the validity and authenticity of C-ITS communications and systems is that of an ITS station masquerading as another, or as another kind of station than it is. [1] Because Vehicle to Vehicle messages may not provide a way to determine their validity, a vehicle may act on the information received, before it has it has in able to its validity (if it even can). A non-emergency vehicle masquerading as an emergency vehicle could lead to vehicle collisions as several vehicles adjust their road positions to give way to the non-existent emergency vehicle. In the short term, most of the current research is applying C-ITS to human-driven vehicles, particularly in Australia [2] (in the pilot programs in the Illawarra region), but in the longer-term C-ITS technology could be applied to autonomous vehicles which, unlike humans looking out the window, cannot visually verify the warning.

## False Advice

Without needing to compromise a C-ITS station enough to masquerade as another, it would be theoretically possible to broadcast valid but false ITS messages. [1] One interesting way such an attack could be achieved is by modifying the C-ITS station itself, creating false inputs such the station (correctly) creates false outputs. [3]. An example of this would be modifying the accelerometers or brake pads to give the C-ITS computers the impression of a different speed than is occurring. This would cause the on-board C-ITS unit to broadcast a valid and perfectly signed message, but with technically invalid content. Therefore, other vehicles could be made to brake or change their heading unnecessarily, posing several safety risks in urban environments. By totally detaching the C-ITS technology from the vehicle, more sophisticated attacks could be carried out by combining multiple C-ITS units, for example on a truck!

## Threats to Data Availability

An interesting kind of threat within C-ITS systems is known as “black holes”, named after the astronomical phenomena. In this context, of course, only communications are affected! According to the ETSI, a black hole attack utilizes several adjacent C-ITS stations each

refusing to relay messages from other stations beyond the affected area. [1] Such an attack could be malicious, caused by deliberate tampering or the existence of malware of unsuspecting users' vehicles or Road-Side-Units; or accidental if an equipment failure causes a station to be unable to transmit or reprocess received messages. It is this author's belief that a black hole attack would be of limited risk to public safety but a medium risk to traffic flow. Any messages originating far enough away that they need to be relayed to be received most probably aren't directly impacting on a vehicle's direct speed and heading. However, the absence of these messages may impact routing and navigation choices, leading to traffic congestion.

## Misbehaviour Detection Research

Most of the initial research seems theoretical currently and surprisingly, cited research into C-ITS, VANETs, and misbehaviour detection has been going for number of years, beginning around 2005 with *The Security of Vehicular Ad hoc Networks* by Maxim Raya and Jean-Pierre Hubaux making the foundational observation that anonymous vehicles could be de-identified simply by tracking them to their owner's residence [4]. Though after their initial research paper into VANET (before the C-ITS term) security issues, the detection of misbehaviour itself doesn't present a research topic until 2008. One interesting approach by G Yan et al involving actively corroborating a vehicle's location with onboard radar to help mitigate Sybil attacks. [5] (A Sybil attack is where a malicious entity forges many false identities to deceive other users [6], often to create the impression of a larger number road users [5].)

Specifically, on the topic of misbehaviour detection, Rens W. van der Heijden *et al* classify misbehaviour detection in their research Survey into either *Data-centric* or *Node-centric* misbehaviour detection [7]. Data-centric detection tries to detect a misbehaving station by analysing received data and correlating it with already known data about the road conditions. For example, if I am travelling at 60kph, the station reporting a traffic jam must be wrong. Node-centric detection aims to detect bad stations by its lack of correct behaviour (forwarding on CAM messages) or its trust-worthiness according to neighbouring stations on the road, participating in some trust-voting system. However, it's important to note that a trust-based system may be vulnerable to Sybil attacks if a malicious node is trying to evade detection.

An interesting example of a form of Node-Centric misbehaviour detection is that of a Watchdog [8], where a relatively trusted node monitors surrounding nodes and makes sure they are forwarding packets to other nodes while finding more reliable routing paths in an attempt to mitigate Black Hole Attacks. Sergio Marti *et al*'s research into this idea out of Stanford University is certainly promising as they have built simulations of their concepts, calculating the gains and losses and have covered potential mechanisms for the malicious defeat of their system. Promising as it may be, and though it was referenced in Rens W. van der Heijden *et al* 2016 [7] Survey, the Watchdog research wasn't intended for C-ITS itself, rather mobile ad hoc networks generally, and it seems difficult to apply it to *moving* networks. Even if it could be refined, Australia's low traffic density outside of metropolitan centres would make the deployment of Watchdog nodes rather expensive to cover the needed distances.

A seemingly simple data-centric detection mechanism was identified by researchers at DaimlerChrysler AG and TU Berlin [9]. They note that a legitimate emergency braking event should come from a previously known node (a vehicle in front) and data should be plausible (no ice in warm conditions). They also propose that a car or another car on the same road didn't need to brake then the event may be false. Further, they describe a layered approach to evaluating data by combining it with onboard sensor data as well as its logical plausibility. Their approach should work reasonably well in Australia as our roads are relatively predictable. Interestingly they also didn't agree with Marti et al's Watchdog idea with fast moving nodes, such as on highways, due to speed of processing.

## Detecting Misbehaving C-ITS Stations

As discussed above, there is a raft of research being done on detecting misbehaving C-ITS stations, onboard or road-side units, and in a limited fashion, some of this can be done in each vehicle while some would have to be done within infrastructure. The problem is that with changing anonymous Pseudonym Certificates (or Authorisation Ticket), it's difficult or impossible to identify the Enrolment Certificate (actual vehicle) which is misbehaving. In this section, I propose the C-ITS and SCMS systems use a combination of detection and reporting to reduce the impact of misbehaving vehicles (or stations impersonating vehicles or RSUs).

- Car is issued some number of Pseudonym Certificates which it uses to sign any messages in the field.
- Car misbehaves but signed its false cooperative awareness messages.
- Another car detects this (in real-time or afterwards) and reports it to the SCMS
- A number of other cars report this AT as misbehaving.
- With enough reports of misbehaviour, the SCMS will match the AT to the EC and blacklist it, refusing to provide new ATs. *Refusal to provide new ATs is the limit of the exiting TCA and ETSI proposal so far.* [10]
- The misbehaving vehicle will no longer acquire new ATs (at least until a service)
- The other road users will have to try to detect any residual misbehaviour or cooperatively blacklist known bad ATs before their eventual expiry.

### On-Board Detection

As highlighted above, node-centric detection mechanisms are less viable in Australia due to the distances between cities and timing issues within fast-moving networks. A better approach would be to have individual road-users use data-centric mechanisms to detect neighbouring misbehaving vehicles; though depending on the misbehaviour, it might not be detected until after. Some methods could be cross-referencing with real-world conditions, other road-users [4], or implausible characteristics.

Since Australia is Australia is following the European approach [2] of having expiring Pseudonym Certificates (and gathering a bunch to use for a time period) rather than relying their revocation if compromised, a misbehaving station will still be able to participate until its batch of ATs expire. One way around this is for road-users to vote amongst themselves reporting suspected misbehaviour. However, this won't work very well in areas a low population density or if the misbehaving vehicle changes its AT every few minutes. Potentially,

the SCMS could report previously detected misbehaving vehicles to other road-users even based on the known ATs so they aren't fooled before expiry.

## Conclusion

C-ITS and the SCMS (systems) are certainly coming to Australia in the near to medium term future, with Transport Certification Australia researching this for the Australian market. The security and reliability of the system is of upmost importance as this report has identified some of the potential threats. To help mitigate these threats, various standards bodies, academic researchers as well as government and industry groups are currently researching misbehaviour detection in mobile networks, and this report has introduced a few of them. As well as threats and a research report, I have also proposed a possible system to help detect errant C-ITS stations.

# Bibliography


[1] ETSI Technical Committee Intelligent Transport System (ITS)., "Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)," ESTI, Valbonne, 2010.

[2] Transport Certification Australia Limited, "Discussion Paper: Towards a national vision for a secure, connected future through Cooperative Connected Transport Systems (C-ITS)," Transport Certification Australia Ltd, Melbourne, 2016.

[3] Working Group 5 of the C-ITS Platform, "C-ITS Platform WG5: Security & Certification," smartmobilitycommunity.eu, Brussels, 2016.

[4] M. Raya and J.-P. Hubaux, "The Security of Vehicular Ad Hoc Networks," in *3rd ACM workshop on Security of ad hoc and sensor networks*, New York, 2005.

[5] G. Yan, S. Olariu and M. C. Weigle, "Providing VANET security through active position detection," *Computer Communications,* vol. 31, no. 12, pp. 2883-2897, July 30 2008.

[6] J. R. Douceur, "The Sybil Attack," in *Peer to Peer Systems First International Workshop*, Cambridge, MA, 2002.

[7] R. W. v. d. Heijden, S. Dietzel, T. L. ¨ller and F. Kargl, "Survey on Misbehavior Detection in Cooperative Intelligent Transportation Systems," Cornell University Library, Cornell, 2016.

[8] S. Marti, T. J. Giuli, K. Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, New York, 2000.

[9] T. Leinmuller, A. Held, G. Schafer and A. Wolisz, "Intrusion Detection in VANETs," in *12th IEEE International Conference on Network Protocols*, 2004.

[10] Transport Certification Australia Limited, "Key Decisions to Progress Australian Deployment of a SCMS," Transport Certification Australia Limited, Melbourne, 2018.

[11] Transport Certification Australia Limited, "Cooperative Intelligent Transport Systems (C-ITS)," 2017. [Online]. Available: http://tca.gov.au/documents/2016-17_TCA_Annual-Report_CITS.pdf. [Accessed 04 09 2018].