Development of a Threat Model for Vehicular Ad-hoc Network based Accident Warning Systems

Niaz Morshed Chowdhury
University of Glasgow
Glasgow, Scotland
United Kingdom
n.chowdhury.1@research.gla.ac.uk

Lewis Mackenzie
University of Glasgow
Glasgow, Scotland
United Kingdom
lewis.mackenzie@gla.ac.uk

ABSTRACT

Accident Warning Systems (AWSs) use Vehicular Ad-hoc Networks to help avoid potential collisions and spread safety notifications amongst nearby vehicles. The development of such systems often assumes that the users are honest and therefore will participate as expected to maximize the intended benefit. In practice, however, attacks are a real possibility and require appropriate counter-measures to avoid a range of undesirable outcomes from reduced functionality to failure to maliciously induced traffic incidents. This paper examines the subject and identifies potential adversaries and the attacks that they might use. Finally, it proposes a threat model that presents a comprehensive picture of how security, privacy and trust issues in AWSs will be targeted and how they can be protected.

Keywords

Warning Systems, VANET, Threat Model

1. INTRODUCTION

Accident Warning Systems (AWSs) are developed for next generation vehicles that use Vehicular Ad-hoc Networks (VANETs) to avoid potential collisions and spread safety notifications amongst nearby vehicles [1]. The problem of designing efficient and effective warning systems has been widely studied but making such systems secure from potential attacks has yet to be seriously addressed. Although security is seen as one of the important issues in general networking, it has largely been overlooked in the AWS arena. There is sometimes an implicit assumption that a separate security system designed for generic wireless networks can be added to an AWS [12]; however, such an approach is unlikely to be adequate because of the unique nature of both the safety system itself and the potential threats.

For example, unlike most VANET applications that often handle confidential and sensitive data, AWSs are not generally concerned about data confidentiality. These systems willingly share data with other nodes so that they can operate cooperatively to prevent traffic accidents. The special nature of AWSs makes it necessary to develop a specific threat model by anticipating potential adversaries, their motivations and likely modes of attack.

SIN '14 September 09 - 11 2014, Glasgow, Scotland, United Kingdom

ACM 978-1-4503-3033-6/14/09:.$15.00.
http://dx.doi.org/10.1145/2659651.2659684

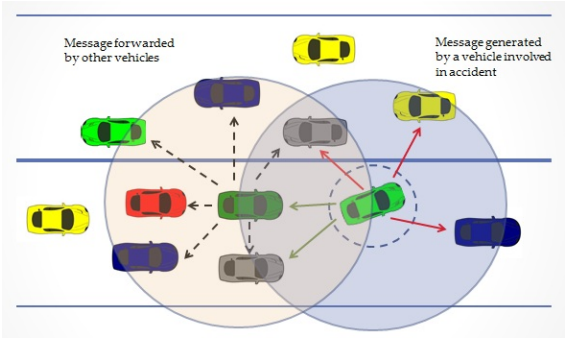

Figure 1: Accident Warning System (AWS)

In this paper, a threat model is presented through an in-depth analysis of security, trust and privacy issues in AWSs. The contribution is twofold: firstly, it presents a survey of possible adversaries and potential attacks on AWSs; and, secondly, it develops a threat model by ranking adversaries based on the level of potential damage associated with their likely types of intrusion.

The remainder of the paper is structured as follows: section 2 presents an overview of the system; sections 3 and 4 discuss adversaries and attacks respectively; section 5 outlines potential challenges; and section 6 presents the threat model; finally section 7 concludes.

2. OVERVIEW OF THE SYSTEM

The design process of a threat model requires a preliminary requirement analysis and component level description of the system. Such a study is presented in [4] and, for convenience, the main conclusions are briefly summarised in the next subsection.

2.1 System Architecture and Requirements

AWSs are collections of mobile nodes, each corresponding to a physical vehicle, whose purpose is to generate collision avoidance notifications that warn drivers before a potential

Figure 2: List of Adversaries based on their degree of threat.

accident takes place. These systems operate via a VANET with which they may be integrated to a greater or lesser degree. For the purposes of system design, collisions may be classified into several generic types: follow-up, pile-up, intersection, lane-change, forward-collision and collisions with object, human or animal. In order to tackle these various hazards, an AWS will use its associated VANET to send messages to containing information about locations and velocities of vehicles. In order to generate such information, individual vehicles need to be equipped with various devices including Global Positioning System (GPS) receivers, sensors to gather important data such as speed, acceleration and deceleration, presence of other vehicles in close proximity and possibly On Board Units (OBUs) to allow drivers to enter warnings of less time-critical hazards manually.

2.2 Message Pattern

Information that vehicles exchange is not confidential but rather visible to and accessible by everyone so that it can be used to identify potential hazards to as wide a relevant audience as possible. There are generally four types of AWS message used to disseminate information. These are: event-driven message, period warning, road-condition notification and emergency call-up. Event-driven messages are sent in response to an emergency situation that has arisen suddenly and unexpectedly such as an accident, an abruptly stopped vehicle and so on. These messages are the highest priority variants in any AWS and need to reach the targeted audience in the shortest possible time. Periodic warning messages are also high priority and require to be disseminated quickly: vehicles send these to warn others about their presence. Road-condition notifications inform other vehicles about scenarios such damaged or slippery surfaces, localised weather hazards etc. and are treated as low priority notifications. Emergency call-up is used in some AWSs to summon police, ambulance or mechanics after an incident takes place.

2.3 Interactions

These messages are typically small and open in nature. Senders want every recipient to which information might be relevant to read it and messages are forwarded repeatedly over a specific region. Unfortunately this has the potential to allow attackers to manipulate content and spread false information across the network. By its nature an AWS depends on accurate content and manipulation introduces not only the threat of the system failing to work as intended but even worse, the possibility of it actually causing accidents that would otherwise not have occurred.

3. ADVERSARIES

Potential attackers can be categorised according to the damage they might cause. Following section divides them into three classes and describes how they are going to operate in AWSs.

3.1 First Degree Threat

This category includes adversaries whose objective primarily involves breaching normal practice for temporary personal driving advantage. The aim is not to cause physical harm to others or direct monetary gain.

Dishonest Drivers

These are potential adversaries who inject false information into the network with a view to gaining advantage over other vehicles. For example, one might create the illusion of congestion to encourage other drivers to avoid a route one wishes to use freely.

Selfish Drivers

AWSs are cooperative system and every vehicle must comply with this principle. In order to make the system a success, it is assumed that all vehicles will share information and forward it to others, if necessary. It is, however, possible that some drivers may refuse to comply with this norm by disabling the forwarding of warning message either completely or partially. The impact of this behaviour may or may not cause system failure depending on its prevalence in particular area.

Pranksters

These are likely to be amateur hackers interfering with the system for amusement and, possibly, notoriety. Attacks could be carried out from the roadside deliberately feeding misleading instructions to vehicles. Most such individuals are intent on inconvenience rather than serious damage but, given the nature of motor vehicles, there is a danger of unintended serious harm.

On-board Passengers

Warning systems are often equipped with an OBU that helps drivers entering warning and road condition notification manually. Although the intention is to allow drivers to report potential hazards, where data entry is insecure, it may be possible for passengers to inject false notification into the network either through carelessness or for amusement.

3.2 Second Degree Threat

This category comprises adversaries that deliberately attack the system for monetary benefits but do not intend to cause physical harm. This includes misusing the system to rob others or trying to get personal information with a view to sell it.

Robbers
AWSs warn other vehicles about potential collisions. In an unsecured system where vehicles react automatically to such warnings, it would be possible to inject false information to bring a target vehicle to a halt in order to facilitate a robbery.

Sniffers
Although the warnings that AWSs disseminate are public and do not contain any personal information, monitoring a target individual's movement, driving pattern and vehicle information without consent, is a privacy violation that could be used against the victim.

Industrial Competitors
The MAC address of IEEE 802.11 contains a manufacturer identity field. This could in principle be used by an intruder to defame competitors by falsely associating deliberately engineered problems with their systems.

Watchers
This kind of adversaries encompasses everyone from a government secret service operative to a tabloid newspaper journalist to a criminal group attempting to monitor someone's regular movements and activities. The nature of these adversaries is different than sniffers as they explicitly try to defame or watch someone for their monetary or personal gain.

3.3 Third Degree Threat
This category comprises adversaries whose intention is to interfere with an AWS deliberately to cause harm to others.

Malicious Attackers
These attackers insert malicious information in the network or jam network channels to block information propagation in the network with a view to creating chaos for a variety of potential reasons such as affecting markets or creating diversions. Such an attack could easily lead to fatal accidents.

Terrorist/Activists
This group of adversaries can potentially manipulate data to create fatal accidents on motorways or in crowded city areas.

Abductors
An individual or a group who want to abduct someone can take advantage of this system. As drivers inject data regularly in the network, particularly in the form of periodic warning message, it leaves traces on their regular movement path. Abductors can make the use of those traces to predict someone's movement in advance to plot a physical attack in a planned and organized way.

Crazy Pranksters
For reasons previously mentioned, people pranking an AWS can cause physical injury or death even if unintentionally. Unfortunately there is reason to believe that some such individuals are capable of crossing the line into generating such outcomes deliberately for nihilistic pleasure.

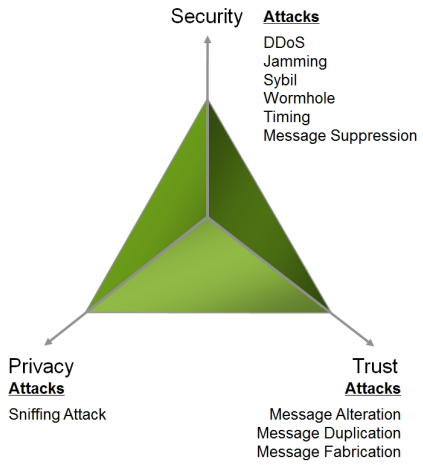

Figure 3: Possible Attacks associated with Security, Privacy and Trust.

4. ATTACKS
In this section, a comprehensive survey is presented of the various types of attack that can be used to target AWSs. Later in this paper connections will be established between these attacks and previously described adversaries to build the threat model.

Distributed Denial of Service (DDoS) Attack
DDoS is a type of denial-of-service attack on networks that is triggered by first compromising a number of *slave* or *zombie* devices and later using a trigger command to use their combined transmission power in an orchestrated flooding attack on some selected target [14]. The distributed nature of the attack makes it more difficult for the victim to block. Attacks of this type can make services unavailable during the course of the assault. The DDoS attack is considered one of the most dangerous attacks on networks [6].

Jamming Attack
Wireless networks are built upon a shared medium that allows potential adversaries to launch attacks easily. A jamming attack is a denial-of-service attack aimed at disabling this medium. For example an attacker may use a jamming device that emits a powerful RF signal to block a wireless channel so that legitimate users cannot get access [23, 21]. There are several jamming attack models such as constant jammer, deceptive jammer, dom jammer, reactive jammer and so on [15]. In an AWS an attack of this type would make vehicle information unavailable to other nodes. In a scenario where vehicles come to rely on AWSs to trigger automatic avoidance measures, this could easily result in collisions and serious harm.

Sybil Attack
This attack mode was first formally defined by [5] as the sending of message from one node with multiple spoofed identities. In a VANET ([3]) this amounts to a vehicle maliciously fabricating different identities to mislead others and generate false information. It is observed and argued that without a centralized authority, this attack is always possible and may go undetected [5, 7].

Wormhole Attack
This is an attack on various types of networks and considered one of the most difficult to counter [17]. According to [8], in a wormhole attack, a private tunnel is used to deliver apparently locally-originating packets to a remote destination. In this way a distant node can be made to appear at a location where it does not exist in reality. A wormhole attack can be performed even if the network provides confidentiality and authenticity.

Sniffing Attack
The aim here is simply to snoop on a target individual by collecting private information from the network [19]. There are several variants including content sniffing, phishing, location sniffing, identity sniffing etc. It has potential to create great threat on lives and properties should victims privacy is compromised.

Timing Attack
This attack particularly targets real-time applications. The attacker interferes with a legitimate message to engineer a deliberate delay [18]. Real-time applications that are time dependent can then be made to fail. This kind of attack is very difficult to detect as the attacker acts like a normal node.

Message Alteration, Duplication, Fabrication and Suppression Attacks
These form a group of attacks that have been identified as threats for VANETs [13] and target the relaying networks. In alteration, important information is altered during relay but in such a way that it still looks legitimate. In duplication a message is replicated by a relay to gain specific objectives. In fabrication, a message is generated that looks like it has been legitimately relayed rather than sourced by its creator. Finally, in suppression a relay simply discards a message it is supposed to forward allowing an attacker to block information from reaching intended recipients.

5. POTENTIAL CHALLENGES
AWS differ from other applications that might be expected to run on top of VANETs. They exhibit open behaviour where data must be visible and information about physical locations needs to be exchanged [11, 10]. Because of this special nature, defending against threats presents some important challenges.

Cooperative Systems
By its nature, an AWS is a cooperative distributed system operating locally with no centralised control. The basic conception relies on every node acting in a manner that is honest, helpful and cooperative because each is reliant for its safety on the received data. However, in practice adversaries can prey on a system organised in this way to achieve unethical and illegal benefits. It is easy to trigger attacks by using suitably prepared intruder vehicles to inject false or fabricated data into the network. A potential solution to this problem would be the use of an existing trust system, but that may create tension with a desire to preserve the personal privacy of the drivers.

Trust vs Privacy
Trust and privacy always have a somewhat uneasy relationship that becomes especially complicated in AWSs. Nodes depend on received data for important and safety critical decision-making and they need to know that such data is coming from a legitimate source. While a trust mechanism, by endorsing data, would remove many potential threats, in this situation, given the inherent location tracking, it would also compromise privacy and open drivers to snooping and even criminal targeting.

Non-confidential System
In an AWS the aim is to disseminate data to all vehicles who might be affected by the content. As a result, the source is not usually aware of the relevant audience and cannot use secure channels. This makes it easier for attackers to alter or fabricate data and disseminate false information that looks legitimate.

Decentralised Nature
The openness issue might be addressed if vehicles are provided with certificates issued by a trusted central authority. In this case only messages signed by their sources are to be trusted. However, the biggest challenge to doing this is the decentralized nature of the AWS which may not have access to a backbone network and thence a central server.

On consideration it can be seen that the above challenges are interconnected nature. As decentralized AWSs are cooperative system, they need to verify trust. Verifying trust, however, affects personal privacy that can be compromised because of the openness of the system. Nonetheless, the problem of openness is difficult to address unless the system is turned into a central authority controlled system.

6. THE THREAT MODEL
Potential adversaries and possible attacks have already been discussed along with different challenges that AWSs create because of their openness and cooperative behaviour. These considerations provide sufficient context for designing a realistic generic threat model for an AWS. Table 1 combines that information with a view to identify relationships between adversaries and attacks; and presents the threat model along with a discussion on possible countermeasure to safeguard the system from those attacks. The threat model is built in such a way that it divides the adversaries in the first place. This division provides clear understanding of the possible attackers who retain the maximum potential to make the system vulnerable. It also shows who often go undetected without leaving any trace of the system being misused. These adversaries have the potential to trigger attacks targeting security, privacy and trust aspects of the system that has also been shown in the model.

In order to protect AWSs from these attacks, the most suitable way is to look at the attack from the aspects they are targeting in the system. For example, dishonest-drivers and pranksters would be likely to use data-related attacks because the main objective is to fool people to gain temporary personal benefit or pleasure. Robbers and abductors would try to stop people in the middle of their way by giving false warning whilst terrorist and malicious attackers would

Degree	Adversary	Aspects	Possible Attacks
1^{st}	Dishonest Drivers	`Security` and `Trust`	*Alteration*, *Suppression* and *Duplication*
	Selfish Drivers	`Security`	*Suppression*
	Pranksters	`Security` and `Trust`	*Alteration* and *Suppression*
	On-board Passengers	`Trust`	*Fabrication*
2^{nd}	Robbers	`Privacy` and `Trust`	*Sniffing*, *Timing*, *Alteration* and *Fabrication*
	Sniffers	`Privacy`	*Sniffing*
	Industrial Competitors	`Security` and `Privacy`	*Sniffing*, *Jamming* and *Alteration*
	Watchers	`Privacy`	*Sniffing* and *Jamming*
3^{rd}	Malicious Attackers	`Security` and `Trust`	*Alteration*, *Fabrication*, *Dublication* and *Sybil*
	Terrorist/Activists	`Security` and `Trust`	*DDoS*, *Jamming*, *Alteration*, *Timing* and *Wormhole*
	Abductors	`Privacy` and `Trust`	*Sniffing* and *Alteration*
	Crazy Pranksters	`Security` and `Trust`	*Alteration* and *Fabrication*

Table 1: The Threat Model

create chaos by injecting malicious information. These behaviours indicate that the attacks would possibly make the use of trust issues and therefore, to protect AWSs from such attacks, establishment of trust system acts as a solution [18].

There are a number of approaches that help establishing trust such as key-based [20], reputation-based [2] and so on. These approaches, however, would require identifying the person involved in communication. As ASWs willingly and openly disseminate its location, revealing identify can cause severe threat. A potential solution to this problem would be using privacy-friendly trust system that recently became a prime research topic in trust [16] and data dissemination schemes are also following the same footsteps [9].

A trust system is, however, of little help in combating warning suppression attacks by both dishonest-drivers and selfish-drivers; and sometimes crazy pranksters. Selfish-node detection mechanism of Mobile Ad-hoc Networks can be introduced in VANET to fight against these adversaries [22]. Besides, security enforcement through monitoring vehicle communication behaviour offers partial solution to this problem. Another useful corrective measure that might help combat some threats would be OBUs that give drivers the opportunity to counter information discovered to be false. This might also help protect against long-term message alteration message and to cancel out accidental warnings.

7. CONCLUSIONS

This paper presents a threat model for AWSs that are developed for next generation vehicles. The main contribution of this paper is the identification of potential adversaries that might make warning systems vulnerable, the categorisation of such adversaries based on their degree of threat and their likely attacks they might mount to achieve their objectives. In future, this model should help in building trust systems and privacy friendly data dissemination schemes to address the potential vulnerabilities of AWS systems. Such solutions will be essential before such systems can safely be deployed in the field.

8. ACKNOWLEDGMENTS

This work is jointly supported by the Scottish Government through Scottish Overseas Research Student Award (SORSA) and the University of Glasgow through College of Science and Engineering Scholarship.

9. REFERENCES

[1] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan. A comprehensive survey on vehicular Ad Hoc network. *Journal of Network and Computer Applications*, pages 1–13, 2013.

[2] A. Bradai, W. Ben-Ameur, and H. Afifi. Byzantine resistant reputation-based trust management. In *9th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom)*, pages 269–278, 2013.

[3] C. Chen, X. Wang, W. Han, and B. Zang. A Robust Detection of the Sybil Attack in Urban VANETs. In *Proceedings of 29th IEEE International Conference on Distributed Computing Systems Workshops*, 2009.

[4] N. M. Chowdhury, L. M. Mackenzie, and C. Perkins. Requirement Analysis for Building Practical Accident Warning Systems based on Vehicular Ad-hoc Networks. In *11th IEEE/IFIP Annual Conference on Wireless On-demand Network Systems and Services (WONS)*, pages 81–88, 2014.

[5] J. Douceur. The sybil attack. In *In the proceedings of First International Workshop on Peer-to-Peer Systems*, 2002.

[6] L. Garber. Denial-of-service attacks rip the internet. *Computer Magazin*, July 2000.

[7] G. Guette and B. Ducourthial. On the sybil attack detection in vanet. In *In the proceedings of IEEE Internatonal Conference on Mobile Adhoc and Sensor Systems*, 2007.

[8] Y.-C. Hu and D. Johnson. Wormhole Attacks in Wireless Networks. *IEEE Journal on Selected Areas in Communications*, 24 (2):370–380, 2006.

[9] R.-J. Hwang, Y.-K. Hsiao, and Y.-F. Liu. Secure Communication Scheme of VANET with Privacy Preserving. In *IEEE 17th International Conference on Parallel and Distributed Systems (ICPADS)*, pages 654–659, 2011.

[10] F. J. Martinez, J.-C. Cano, C. T. Calafate, and P. Manzoni. A VANET Solution to Prevent Car Accident. In *Proceedings of Jornadas de Paralelismo*, Spain, 2007.

[11] T. Nadeem, P. Shankar, and L. Iftode. A Comparative Study of Data Dissemination Models for VANETs. In

Proceedings of IEEE Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, pages 1–10, San Jose, CA, USA, 2006.

[12] P. Papadimitratos, L. Buttyan, H. Holczer, and S. E. Secure vehicular communication systems: Design and architecture. *IEEE Communications*, 46:100–109, 2008.

[13] B. Parno and A. Perrig. Challenges in securing vechicular networks. In *In the proceedings of ACM SIGCOMM*, 2005.

[14] V. Paxson. An analysis of using reflectors for distributed denial-of-service attacks. *Computer Communication Review*, 31 (3), July 2001.

[15] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy. Denial of Service Attacks in Wireless Networks: The Case of Jammers. *IEEE Communications Surveys and Tutorials*, 13 (2):245–257, 2011.

[16] S. Ries, M. Fischlin, L. Martucci, and M. Muhlhauser. Learning Whom to Trust in a Privacy-Friendly Way. In *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 214–225, 2011.

[17] S. M. Safi, A. Movaghar, and M. Mohammadizadeh. A Novel Approach for Avoiding Wormhole Attacks in VANET. In *Proceedings of First Asian Himalayas International Conference on Internet*, 2009.

[18] I. A. Sumra, H. Hasbullah, J. lail, and R. Masood-ur. Trust and Trusted Computing in VANET. *Computer Science Journa*, 1 (1):29–51, 2011.

[19] B. S. Thakur and S. Chaudhary. Content sniffing attack detection in client and server side: A survey. *International Journal of Advanced Computer Research*, 2 (10):pp 7 – 10, 2013.

[20] J.-J. Wang, J.-P. Li, Y.-F. Li, and J. Peng. Review of Key-Based Dynamic Trust Authorization Mechanism. In *International Conference on Wavelet Active Media Technology and Information Processing (ICWAMTIP)*, pages 263–267, 2012.

[21] A. D. Wood, J. A. Stankovic, and S. H. Son. JAM: A Jammed-Area Mapping Service for Sensor Networks. In *Proceedings of 24th IEEE Real-Time Systems Symposium*, pages 286–297, 2003.

[22] L. Xu, Z. Lin, and Y. Ye. Analysis and Countermeasure of Selfish Node Problem in Mobile Ad Hoc Network. In *10th International Conference on Computer Supported Cooperative Work in Design*, pages 1–4, 2006.

[23] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In *Proceedings of ACM workshop on Wireless Security*, pages 80–89, 2004.