Security and Privacy in Vanets

Akshay Goswami, Roopali Goel

Abstract*— *Technologies have both advantages and disadvantages. Now a day's a vehicle can be tracked by its location, traffic status and position based on transmission of signals, when vehicles communicated to other vehicles.

In the above paper, we discuss the different aspects of security and privacy measures in VANET'S. Vanet communication can be enhanced to provide optimized working of security and privacy measures, for flexible communication between interconnected vehicles..

I. INTRODUCTION

Vanet (vehicular ad-hoc networks) allows transmission of signals related to traffic, accidents and location between vehicle to vehicle (V-2-V network communication) and road-side-infrastructure (V-2-I network communication). These functions provide location based service, reduction of traffic conjunction, accident details and safety. [1]

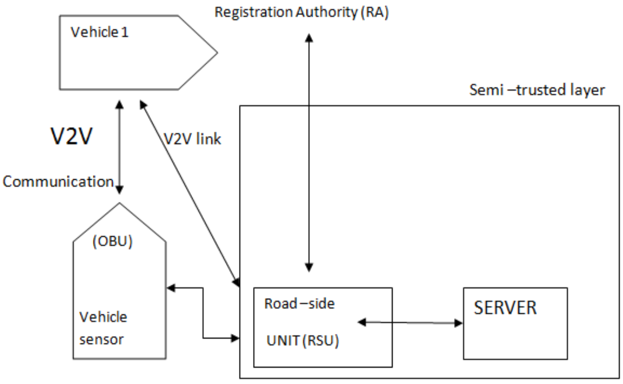

Figure 1: Illustrates the inter-vehicle or vehicle-to-infrastructure communication.

II. SAFETY OF VANET'S

As this wireless networks are essential for safety precautions of vehicle and equally are their security and threat concern.

Vanet's system should:

1) Information received is correct.
2) Source of message is not fake or fallacious.
3) Signal or node transmitted by sender cannot be tracked, part of a privacy concern.
4) Program should be robust.

III. SECURITY FACTORS IN VANETS

Signals or nodes transmitted by vehicle can be misjudged or mislead by any fabrication attacker. The attacker can send fallacious message to the network, these attacks include warnings, fake messages.

A. *Entity identification*

This enables the process to identify whether a participants is unique or should transmit different node. Moreover, identification does not itself conclude that entity testify that it is the actual identity-this requisite is called entity authentication. Vehicle to vehicle (V-2-V) warning requires identification of the sender to enable message routing and forwarding. In any case, if a regular vehicle transmits a message as if it's a police vehicle, then there should be an identification that authorizes the user, in this aspect the VANET security can be breached.

B. *Non-repudication*

Non-repudication assures the fact that sender or receiver cannot deny their nodes transmitted and received. In this way , nodes transmitted by any malicious attacker must be held responsible for his actions and cannot deny.

In group communication Non-repudication is generally not required, because the emitting node could possibly belong to any of the group members. In infrastructure to vehicle communication (I-2-V) and vehicle to infrastructure communication (V-2-I) warning, Non-repudication of root is required, so in this sense fallacious message warning can be culpable to the sender's node. Non-repudication is not presently needed, but would will be in future, currently the accidents caused only due to human driver. Moreover in future needs there would be visualized application that would automate driving task.

C. *Integrity*

Message transmitted should not be tainted or corrupted. Integrity promises the detection of malicious attack or system failures.

D. *Confidentiality*

Confidentiality is significantly needed in V-2-V communications. First the vehicle should be registered with RSU (road-side-unit). The RSU provide vehicle with symmetric key. Key acquired by vehicle is used to establish links between vehicle to vehicle (V-2-V).

In this way, communication between groups of vehicles engages. But sometimes these groups are too big for RSU range, in this aspect confidentiality is breached. This problem can be facilitate in dividing RSU's sectors into 'splits'. Now a split consists of a group of vehicles which communicate to each other. As on, the next split's key can be computed by vehicle. Thus now, the vehicle can perform inter-group communication and only one time registration is performed by RSU. [2]

Manuscript published on 30 August 2012.

***** Correspondence Author (s)
Akshay Goswami I.I.L.M (U.P), INDIA.
Roopali Goel, working as a Assistant Professor in the department Of CSE In IILM-AH L, Greater Noida ,U.P , India

IV. PRIVACY ISSUES IN VANET

Though the advantages of vehicular ad-hoc networks (vanet's) provides significant intersection between vehicles, but deals with privacy and security concerns also.

A. Anonymity:

Network would certainly miscarry if anonymity is being introduced in whole network for different vehicles. [3]

Any message or alert without known name, identity or source can end up with road accidents , crashes and traffic jams. There should be a way so that VANET's network should be secured and rules out anonymity.

B. Linkability:

It allows a road – side – unit (RSU) to distinguish signatures issued by OBU's in the path to maintain their anonymity. By linkability, RSU is able to recognize OBU's signatures for future extensions without tracing identity of OBU's [3]

C. Restricted credential usage:

As discussed in "distributed certificate architectures for VANET's by BABER ASLAM & cliff C.ZOU , if a user wants to use a service in service area then payment can be delivered to the provided server without showing user's account or vehicle information. Payment for the service used can be carried out by on-board payments device in the vehicle. The temporary credentials involved in pursuing the service can be use as privacy and security attributes in vehicular ad-hoc networks (VANET's). [4]

V. CONCLUSION

Above paper discusses necessity and importance of security and privacy in vehicular ad-hoc networks (VANET's).

A secured connection is important between vehicles and service provider entity, non-rededication, integrity, confidentiality are essential factors in a secured connection.

VI. APPENDIX

A. Abbreviations:

- VANET - Vehicular ad-hoc network
- GPA - Global Passive Adversary
- OBU - On-Board Unit
- RSU - Road Side Unit
- V2V - Vehicle-to-Vehicle
- V2I - Vehicle-to-Infrastructure
- IVC - Inter-Vehicle Communication

REFERENCES

[1] Krishna sampigetnaya*, leping huang+, mingyanLi* , Radha roovendran* , kanta matsura+ , kaary sezaki+ University of Tokyo, Japan *University of Washington , Seattle In CARAVAN: providing location privacy for VANET's.

[2] Jose' mariade Fuentes , Ana Isabel Gonzalez- tables Arturo ribagarda Department of computer science University of carlos of Madrid (Spain) in overview of security issues in vehicular ad-hoc network.

[3] Hang dok1, Huirang fu1, rubeen edievarria2 , and Hesivi weerasingne1
1 Oakland university , Rochester
2 university of Illinois at Chicago , IL , USA In privacy issues of vehicular ad-hoc network.

[4] Babur aslam and cliff c.zoo in distributed certificate architecture for VANET's.

[5] Aijaz, A., Bochow, B., Dötzer, F., Festag, A., Gerlach, M., Kroh, R., et al. (2006). Attacks on Inter-Vehicle Communication Systems - An Analysis. International Workshop on Intelligent Transportation. Hamburg, Germany: IEEE Communications Society.

[6] Kargl, F., Papadimitratos, P., Buttyan, L., Müter, M., Schoch, E., Wiedersheim, B., et al. (2008). Secure vehicular communication systems: implementation, performance, and research challenges. IEEE Communications Magazine , 46 (11), 110-118.

[7] Papadimitratos, P., Gligor, V., & Hubaux, J.-P. (2006). Securing Vehicular Communications - Assumptions, Requirements, and Principles. Workshop on Embedded Security in Cars (ESCAR), (pp. 5-14). Berlin, Germany.

[8] J.-P. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," IEEE Security & Privacy, vol. 2, no. 3, pp. 49–55, 2004.

[9] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in IEEE Wireless Communications and Networking Conference (WCNC), 2005, pp. 1187–1192.

[10] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis," in Proc. of the ACM Workshop on Wireless mobile applications and services on WLAN hotspots (WMASH), 2003, pp. 46–55.

[11] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Towards modeling wireless location privacy," in Proc. of the Workshop on Privacy. Enhancing Technologies (PET), 2005.

[12] F. Bai, N. Sadagopan, and A. Helmy, "IMPORTANT: A framework to systematically analyze the impact of mobility on performance of routing protocols for adhoc networks," in Proc. of the IEEE Infocom, 2003, pp. 825–835.

Ms. Roopali Goel is working as a Asst. prof in the department of CSE in CET-IILM-AHL Greater Noida, UP, India. She is also pursuing her M.Tech in CS(final year) from Jamia Hamdard University Delhi. Her area of interest is Cloud Computing and Wireless Networks.

Mr. Akshay Goswami is currently pursuing B.tech in CSE (3rd year) from CET-IILM-AHL Greater Noida (India). His area of interest are Network security, robotics and Artificial intelligence.