ISSN No. 0976-5697

Volume 6, No. 2, March-April 2015

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Vehicular Ad-hoc Network (VANET) - Privacy and Security

Anil Kr.Panghal
CSE Deptt,
HCTM Technical Campus
Kaithal(Haryana)India

Sharda Rani
MCA Deptt
HCTM Technical Campus
Kaithal(Haryana)India

Poonam
CSE Deptt
GJUST
Hisar(Haryana)India

Abstract: Vehicular Ad-hoc Network (VANET) is the special instance of the Mobile Adhoc Network i.e. MANET. In VANET the mobile nodes are cars or vehicles, their average mobility rate is considerably greater, and the network they form is extremely dynamic. The emerging technology of vehicular ad-hoc network raises a number of technical problems that need to be addressed. Among those, challenges, security and privacy concerns are paramount for the wide adoption of vehicular ad-hoc network. So in this paper we are concerned with the challenges, security and privacy issue in the VANET and identify the silent feature of the VANET.

Keywords: VANET, MANET, Bootstrap, Mobility

I. INTRODAUCTION

Vehicular ad hoc networks (VANETs) are one of the fastest growing area of research in ad hoc networks. Inter-vehicle communication would indeed enable a huge number of applications, ranging from entertainment to traffic optimization and to be an important building block for in vehicle infotainment and safety applications [3]. A very important requirement for the success of Vehicular Networks is their reliability, various challenges, security and privacy issue. The build up of ad hoc network, the support of wireless access or wired backbone is not feasible. Ad hoc wireless network does not have any predefined infrastructure and all network services are configured and created on the fly. Thus it is obvious that with lack of infrastructural support and susceptible wireless link attacks, security in ad hoc network becomes inherent weakness [1].

II.KEY ISSUES AND CHALLENGES

Vehicles move at a fast rate, moving in and out of the reception area of other vehicles participating in the network. We can expect that a pair of vehicles can communicate for a limited amount of time. It is also expected that communication between nodes that have never before and will never interact again will be the norm. Thus vehicular networks are very different from existing mobile ad-hoc networks where communication between pairs of nodes can be of relatively long duration. Another challenge are the sheer scale of the network and the implementation of secure inter-vehicle communications faces are the opposing incentives of participating parties[1]. So some of the key issue and challenges in vehicular ad-hoc network are given below:-

A. Bootstrap:

Initially, only a small percentage of vehicles will be equipped with DSRC radios and little infrastructure will exist to support them. Thus, in developing applications for vehicular networks, we can only assume that a few other vehicles are able to receive our communications, and the applications must provide benefits even under these limited conditions (with increasing benefits as the number of DSRC-equipped vehicles increases).

B. Moblility:

Traditional sensor networks frequently assume a relatively static network, and even ad hoc networks typically assume limited mobility, often focusing on handheld PDAs and laptops carried by users. For vehicular networks, mobility is the norm, and it will be measured in miles, not meters, per hour. Also, the mobility patterns of vehicles on the same road will exhibit strong correlations. Each vehicle will have a constantly shifting set of neighbors, many of whom it has never interacted with before and is unlikely to interact with again. Please do not revise any of the current designations [3].

C. Roaming in Dangerous Environment:

Any malicious node or misbehaving node can create hostile attack or deprive all other nodes from providing any service.

D. Link Level Security:

In wireless environment the links are susceptible to attacks where eavesdropper can easily spoof the ongoing communication. As there is no protection like firewalls or access control in ad hoc network any node can become vulnerable to attacks coming from any direction or from any node. The results of such attacks include spoofing of the node's identity, tampering with node's credentials, leaking of confidential information or impersonating node. These types of attacks can easily compromise the basic security aspects like confidentiality, integrity, and availability and

privacy of the node.

E. Secure Routing:

The supported routing protocols within ad hoc network are more vulnerable to attacks as each device acts as a relay. Any tampering with routing information can compromise whole network. An attacker can insert rogue information within routing information or introduce denial of service type attack by replaying old logged or stored information. Also compromised node can route malicious information to other nodes, which can cause serious damage. However proposed routing solutions are capable to operate with dynamic topology but in terms of security measure they provide partial or no solution .Thus implementation of secure routing protocol is one of the challenges within ad hoc network.

F. Key Management:

In general, security goals in ad hoc networks are achieved through cryptographic mechanisms such as public key encryption or digital signature. These mechanisms are supported through centralized key management where trusted Certificate Authority (CA) provides public key certificate to mobile nodes so nodes can develop mutual trust between one another. Any tampering with CA can easily compromise the security of the entire network.

The proposed mechanisms used for identification such as shared secret, public key cryptography, third party authentication provide partial solution, as they are vulnerable or unable to scale. All proposed solutions require that the mobile users make proper usage of cryptographic keys. However goal of proper management and safekeeping of small number of cryptographic keys is difficult to achieve in ad hoc network due to random mobility of nodes where continuous connectivity is not maintained.

G. Incentives:

Successful deployment of vehicular networks will require incentives for vehicle manufacturers, consumers, and the government, and reconciling their often conflicting interests will prove challenging

III. VANET PRIVACY

Users of such networks have to be prevented from misuse of their private data by authorities, from location profiling and from other attacks on their privacy. On the other hand, system operators and car manufacturers have to be able to identify malfunctioning units for sake of system availability and security. These requirements demand an architecture that can really manage privacy instead of either providing full anonymity or no privacy at all [5][6].

Currently, there are some car-to-car network research projects which have operational prototypes, such as FleetNet, Carisma and VSC. However, only the VSC project dealt with security, where privacy has only been a minor issue. Out of the ongoing funded research projects, such as VSC-2, NOW, Prevent, Invent VLA, etc. only NOW and VSC-2 made considerable efforts to accommodate privacy so far. During our work, we found a couple of situations, where privacy should be discussed. As mentioned before, sometimes it is not desirable to achieve perfect privacy. But it has to be decided which degree of privacy is necessary under given circumstances and the system has to be designed accordingly. In the following we will give some examples for the problems we have to tackle in a widespread VANET [8].

H. An employer is overhearing the communications from cars on the company parking lot. After distinguishing which car-identifier belongs to which employee he automatically gets exact arrival and departure dates

I. A private investigator easily follows a car without being noticed by extracting position information from messages and hello beacons

J. Insurance companies gather detailed statistics about movement patterns of cars. In some cases individual persons may be charged for traffic accidents based on gathered movement patterns

K. Privacy Related Requirements:

After the previous sections, we now identify a number of requirements to achieve adequate privacy.

a. It is possible to use pseudonyms as identifiers instead of real-world identities.
b. It is possible to change these pseudonyms.
c. The number of pseudonym changes depends on the application and its privacy threat model. 4.Pseudonyms used during communication can be mapped to real-world identities in special situations.
d. A set of properties and/or privileges can be cryptographically bound to one or more pseudonyms.

This discusses only the primary requirements with respect to the VANET messaging system. There might be other important things to consider such as user interfaces and usability issues[6].

IV. SECURITY ISSUES

The use and integration of security mechanisms for warning messages and safety services is absolutely necessary within VANETs [10]. The ongoing Network On Wheels (NOW) project addresses a number of security issues in vehicular networks. The project adopts an IEEE 802.11 standard for wireless access and aim at implementing a reference system. The project addresses a number of security issues for VANET. VANET security should satisfy following points [2][6].

a. Authentication: Vehicle reactions to events should be based on legitimate messages (i.e., generated by legitimate senders). Therefore we need to authenticate the senders of these messages.

b. Verification of data consistency: The legitimacy of messages also encompasses their consistency with similar ones (those generated in close space and time) because the sender can be legitimate while the message contains false data.

c. Availability: Even assuming a robust communication channel, some attacks (e.g., DoS by jamming) can bring down the network. Therefore, availability should be also supported by alternative means.

d. Non-repudiation: Drivers responsible for accidents should be reliably identified; a sender should not be able to deny the transmission of a message. It may be crucial for investigation to determine the correct sequence and content of messages exchanged

before the accident.

e. ***Privacy:*** People are increasingly wary of enabling technologies. Hence, the privacy of drivers against unauthorized observers should be guaranteed.

f. ***Real-time constraints:*** At the very high speeds typical in VANETs, strict time constraints should be required.

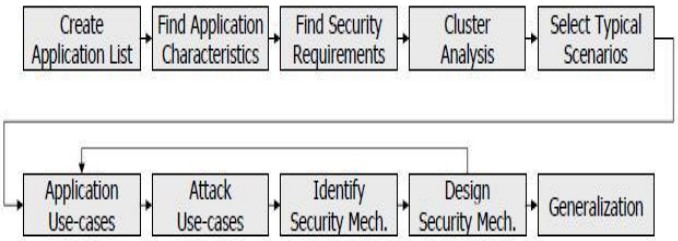

Figure. 1 Steps for Security Process [7]

The security issue also includes the following points against which security is needed, these points are given below [4]:-

a) ***Fake data transmission:*** The attacker sends false data to modify the behavior of other vehicles. An example would be sending fake accident warnings to free the road.

b) ***Masquerading:*** In this case, the attacker uses a fake identity to escape liability, and place the blame on someone else.

c) ***Tracking:*** The attacker here listens for messages coming from a targeted node, and is thus able to monitor the targets movements.

V. CONCLUSION

In this paper, we have elaborated on the various challenges, privacy and security issues in vehicular ad-hoc networks (VANETs). The challenges are the factor against the success of the VANET is measured and the area in which further research is needed. The Privacy is also an important factor for the public acceptance and Successful deployment of VANETs [3]. The security of the whole system is very much based on the security of the system platform in the vehicles. Security is one of the important factors for the success of future vehicular networks; hence its integration into the system has to be done very carefully making it an integral part of the system [9].

VI. REFERENCES

[1] L. Zhou and Z.J. Haas, "Securing Ad hoc Networ--ks", IEEE Networks, 13(6): 24-30, Nov/Dec 19 99

[2] Preetida Vinayakray-Jani, "Security within Ad h oc Networks" PAMPAS Workshop, Sept. 16/17 2002

[3] Kavita Taneja and R. B. Patel, " Mobile Ad hoc Networks: Challenges and Future" Proceedings of National Conference on Challenges & Opportunities in Information Technology (COIT-2007) RIMT-IET, Mandi Gobindgarh. March 23, 2007.

[4] Frank Kargl, "Vehicular Communications andVANETs" CCC Ulm, Ulm University.

[5] Cryptography and Network Security. Pearson Education International., 2006.

[6] F. D¨otzer. Privacy issues in vehicular ad hoc networks. Lecture Notes in Computer Science, vol. 3856, pp. 197-209, 2006.

[7] Stephan Eichler, "A Security Architecture Concept for Vehicular Network Nodes"

[8] M. Raya, P. Papadimitratos, and J.-P. Hubaux, "Securing vehicular communications," IEEE Wireless Communications, vol. 13, no. 5, pp. 8– 15, Oct. 2006

[9] B. Parno and A. Perrig, "Challenges in Securing Vehicular Networks," in Proceedings of the F ourth Workshop on Hot Topics in Networks (HotNets-IV), Nov.2005. [Online]. Available: http://www.ece.cmu.edu/ bparno.

[10] Ghassan , Abdalla,Mosa Ali Abu-Rgheff and Sidi Mohammed Senouci, **"** Current Trends in Vehicular Ad Hoc Networks" Mobile Communications Network Research, Portland ,2014.