Volume 2, No. 2, Mar-Apr 2011

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

CASE STUDY AND REPORT

Available Online at www.ijarcs.info

A Case Study of Security in Vanets

Siva Rama Krishnan S*
VIT University, Vellore, Tamil Nadu.
siva.s@vit.ac.in

Pavithra Balaji
VIT University, Vellore, Tamil Nadu.
pavithra@vit.ac.in

Gracia S
VIT University, Vellore, Tamil Nadu.
s.gracia@vit.ac.in

Sakthi Ganesh M
VIT University, Vellore, Tamil Nadu.
sakthiganesh.m@vit.ac.in

Abstract: The security of Vehicular ad-hoc network (VANETS) is a major concern these days. Many researchers have proposed various methods in security of the VANETS. In this paper, we identify certain drawbacks in existing methods and we propose new ideas to overcome the same.

Keywords: DSRC, VC, GPS, Radars, Laser-sensor.

I. INTRODUCTION

Vehicular Ad hoc Networks (VANET) is part of Mobile Ad Hoc Networks (MANET), this means that every node can move freely within the network coverage and stay connected, each node can communicate with other nodes in single hop or multi hop, and any node could be Vehicle and Road Side Unit. The vehicles use short range communication such as Dedicated Short Range Communication (DSRC), Bluetooth or Zigbee. The major challenge for VANETS is that the vehicles are mobile and the speed of each vehicle differs. So the time for connectivity is very limited and within this time constraint we need to implement the security methods.

A. Security Threats in VANETS

The various attacks against the messages are:

[a] Denial of Service Attack

This attack happens when the attacker takes control of a vehicle's resources or jams the communication channel used by the Vehicular Network, so it prevents critical information from arriving. It also increases the danger to the driver, if it has to depend on the application's information.

[b] Message Suppression Attack

An attacker selectively dropping packets from the network, these packets may hold critical information for the receiver, the attacker suppress these packets and can use them again in other time. The goal of such an attacker would be to prevent registration and insurance authorities from learning about collisions involving his vehicle and/or to avoid delivering collision reports to roadside access points.

[c] Fabrication Attack,

An attacker can make this attack by transmitting false information into the network, the information could be false or the transmitter could claim that it is somebody else.

[d] Alteration Attack,

This attack happens when attacker alters an existing data. It includes delaying the transmission of the information, replaying earlier transmission, or altering the actual entry of the data transmitted.

[e] Replay Attack,

This attack happens when an attacker replay the transmission of an earlier information to take advantage of the situation of the message at time of sending. Basic 802.11 security has no protection against replay. It does not contain sequence numbers or timestamps. Because of keys can be reused, it is possible to replay stored messages with the same key without detection to insert bogus messages into the system. Individual packets must be authenticated, not just encrypted. Packets must have timestamps. The goal of such an attack would be to confuse the authorities and possibly prevent identification of vehicles in hit-and-run incidents.

[f] Sybil Attack,

This attack happens when an attacker creates a large number of pseudonymous, and claims or acts like it is more than a hundred vehicles, to tell other vehicles that there is jam ahead, and force them to take alternate route. A Sybil attack depends on how cheaply identities can be generated, the degree to which the system accepts inputs from entities that do not have a chain of trust linking them to a trusted entity, and whether the system treats all entities identically.

B. Attacks on Vanet

Attacker's model: To classify the capacities of an attacker, we have defined three dimensions:

[a] Insider vs. Outsider. The insider is an authenticated member of the network that can communicate with other members. This means that he possesses a certified public key. The outsider is considered by the network members as an

intruder and hence is limited in the diversity of attacks he can mount (especially by misusing network-specific protocols).

[b] Malicious vs. Rational. A malicious attacker seeks no personal benefits from the attacks and aims to harm the members or the functionality of the network. Hence, he may employ any means disregarding corresponding costs and consequences. On the contrary, a rational attacker seeks personal profit and hence is more predictable in terms of the attack means and the attack target.

[c] Active vs. Passive. An active attacker can generate packets or signals, whereas a passive attacker contents himself with eavesdropping on the wireless channel.

II. ANALYSIS OF EXISTING SECURITY METHODS IN VANETS

Frank Kargl et al. in [1] proposed an idea to develop a future proof security solution for vehicular communication (VC) to prevent sending of bogus messages to other vehicles. Their approach was to analyze a large set of informally specified applications. From these applications typical representatives were selected that would cover the requirements of a whole cluster of applications. Later, they proposed to develop a security solution for this particular subset of applications so that it covers the requirements of all applications that have been considered. In this paper, the authors have applied cluster analysis as part of their security engineering process to find the security requirements of VANET applications.

A. Critical Review

In this paper, it may not be appropriate to choose a cluster-centric application as the representative, since the application security requirement at the boundary of the cluster may vary. They have also mentioned that whenever a security mechanism is designed it may result in additional attack vector and there would be a loop-back mechanism implemented which goes to attack use case. This kind of technique leads to processing delay.

B. Proposed Solution

A common security framework can be designed for various applications since these applications tend to change periodically according to user requirements and also it is a tedious task to write an attack use-case for each new application encountered.

Pandurang Kamat et al. in [2] proposed a security framework for vehicular networks, using Identity-Based Cryptography (IBC) that provides authentication, confidentiality, message integrity, non repudiation and pseudonymity. They present a pseudonym generation mechanism that exploits the implicit authentication provided by IBC to generate unforgettable, authenticated pseudonyms. Using these pseudonyms the vehicles engage in anonymous communication. The non-repudiation is also provided as a Trusted Authority (TA) only can reconstruct the true identity of a vehicle from its pseudonym to settle disputes or provide accountability.

C. Critical Review

In this paper, the use of pseudo ids may create problems, as there would be a lot of false ids at bulk posing to be the actual pseudonyms.

D. Proposed Solution

The solution which we have proposed to solve the above problem is to link up the electronic number plate (ELP) with the pseudonyms.

Ghassan Samara et al. in [3] discussed about the challenges and attacks in VANETs. They also talk about how message must be encrypted by session key obtained from the Certificate Authority. They also propose to decrease the overhead on the receiving vehicle for verifying the signature, by making use of a list in TPD containing the certificates of vehicles of the last 100 vehicles that made a successful communication, each certificate can be identified by a 16 byte fingerprint (the size of one AES block) the total for the memory consuming is 1600 byte, 10 minutes is the life time for each signature in the list, so when new message arrives, the vehicle will search in the list, if the certificate is there, no need for verifying the vehicle signature.

E. Critical Review

In this paper, the authors discussed about the size of the certificate list which has certain tradeoffs. For example, if verifying signatures will happen more frequent for the same vehicles, the certificate buffer size increases, resulting in slower search. The number of the certificates will be higher, and the signature for each vehicle needs to be verified again.

F. Proposed Solution

We can make use of the public key infrastructure where the verification by each vehicle may be done using the vehicle's certificates and its own private key.

Robert K. Schmidt et al. in [4] propose a framework for behavior analysis of other vehicles in the vicinity. They are combining the output of multiple behavior analysis modules and then each vehicle is assigned a trustworthiness value which may be additionally exchanged among all vehicles, building up reputation. Based on this information, vehicles are classified into trustworthy, untrustworthy or neutral. The authors also talk about beacon packets, which give the global information such as speed and the direction. Using these beacons, each vehicle will know about surrounding. The authors also use VEhicle Behavior Analysis and Evaluation Scheme (VEBAS). By using this scheme, the authors refer to all observable information on a vehicle, in particular its past, present and even future movements and its communication activities. The basis of the behavior analysis along with the beacons will contain vehicle position and movement information.

G. Critical Review

The authors in this paper deal with rating parameter which is evaluated for each component, starting with the behavior analysis module as a basis for the evaluation of behavior and then, the aggregation and aging of the outputs of the modules are calculated. The local and global rating is calculated and these are exchanged as reputation information

in terms of recommendations. Finally, its aggregation outputs the called the aggregated trust is calculated. This proposed model requires some storage for a long duration and processing time. Since in VC, there are constraints such as transmission range and time of connectivity, we need to build-up the security within that time limit.

H. Proposed Solution

We may make use of the beacons by which we can know the speed, location etc., and we can build a security framework by integrating GPS and vehicle sensors.

Xiaonan Liu et al. in [5] have designed an intelligent transport system. The ITS (intelligent transport system) includes two big function modules. Information processing application system and Road condition information transferring system. The main task of the road condition information transferring module is in charge of the information exchange of the car inside, car to car and car to road. The authors in this paper suggest that each node needs to keep a certificate revocation list (CRL) of revoked certificates. However, a digital signature can be verified by any node given that it knows the public key of the signing node. This makes digital signature scalable to large numbers of receivers. Only a total number of n public/private key pairs need be maintained in a network of n nodes. Here the authors make use of the Public Key Infrastructure solution, where each vehicle will be assigned a public/private key pair.

I. Proposed Solution

The better solution for the above paper might be that each vehicle would store its key information in online space. The key can also contain electronic number plate and random number generated by any key management technique

Gongjun Yan et al. in [6] in this paper deal with a method which enhances position security in VANET. To achieve local and global position security, they are using the on-board radar to detect neighboring vehicles and to confirm their announced coordinates. The authors main contribution is to show that by using GPS and radar-provided information one can ensure the validity of position information in the VANET by detecting and isolating malicious. The authors say that the observer vehicle stores position data in a time series to form a movement history of the observed vehicles. The movement history can help determine whether new received data is valid or not. They isolate vehicles which send invalid data. This isolation can help to prevent a large number of position-based attacks, Sybil attacks, and some combinations of position and Sybil attacks.

J. Critical Review

In the above paper the authors use radars. But Radar transmission range is limited. So the location data may not be precise. The authors also propose to fit radar in the rear and front of the car. This would become a costly affair as radar is expensive.

K. Proposed Solution

In the above paper the authors can use a Sensor laser is much simpler than radar and also is less expensive. This sensor laser can also interact with the GPS.

III. CONCLUSION

In this review paper, we analyzed various methods related to security in VANETs and we proposed new solutions for the existing methods.

In our future work we would implement our new methods in a real time scenario.

IV. ACKNOWLEDGEMENTS

We would like to sincerely thank our honorable Vice-Chancellor, Dr. Raju for his motivation and support. We also like to express our gratitude and sincere thanks to Prof H.R.Vishwakarma, for his guidance. Finally, we thank Dr. S.Sankaran, Scientist-G, NGRI, Hyderabad, who has been of immense support all through our efforts.

V. REFERENCES

[1] Frank Kargl, Zhendong Ma, and Elmar Schoch, “Security Engineering for VANETs”, SEVECOM project report, European Commission e-Safety initiative, contract no. IST-027795.

[2] Pandurang Kamat, Arati Baliga, and Wade Trappe, “An Identity-Based Security Framework For VANETs”, *VANET’06,* September 29, 2006, Los Angeles, California, USA. ACM 1595935401/06/0009.

[3] Ghassan Samara, Wafaa A.H. Al-Salihy and R. Sures, “Security Issues and Challenges of Vehicular Ad Hoc Networks (VANET)”, UNIVERSITY OF SALFORD,.August 09,2010 at 12:58:19, IEEE Xplore.

[4] Robert K. Schmidt, Tim Leinm¨uller, Elmar Schoch, Albert Held and G¨unter Sch¨afer, “Vehicle Behavior Analysis to Enhance Security in VANETs”, Telematics/Computer Networks Research Group, Technische Universit¨at Ilmenau, Germany.

[5] Xiaonan Liu, Zhiyi Fang and Lijun Shi, “Securing Vehicular Ad Hoc Networks”, 1-4244-0971-3/07/$25.00 ©)2007 IEEE.

[6] Gongjun Yan, Gyanesh Choudhary, Michele C. Weigle, and Stephan Olariu, “Providing VANET Security Through Active Position Detection”, VANET’07, September 10, 2007, Montréal, Québec, Canada. ACM 978-1-59593-739-1/07/0009