Security Policies and Mechanisms for Vehicular Delay Torlant Network

Zeshan Haider,
CoCoLab, PIEAS, Islamabad
luckier19@gmail.com

Shariq Aziz Butt
University of Lahore, Lahore
shariq2315@gmail.com

Adnan Muhammad
Institute of Telecommunication
University of Beira Interior
Covilha Portugal
admu05@ubi.pt

***Abstract*—**This article revision the literature related to Vehicular Delay Tolerant Network with focus on Cooperation. It starts by examining definitions of some of the fields of research in VDTN on security policies. An overview of VDTN on security policies cooperative networks is presented. A security policy is a high-level specification of the security properties that a given system should possess. It is a means for designers domain experts and implementers to communicate with each other, and a blueprint that drives a project from design through implementation and validation. We offer a survey of the most significant security policy models in the literature showing security may mean very different things in different contexts and we review some of the mechanisms used to implement a gievn security policy.

Keywords-component; Security policies Mechanism**, C**ooperative Networks, Vehicular Delay Tolerant Network ; Cooperation.

Introduction

This survey will present security policies and mechanisms on cooperation for Vehicular Delay Torlant Network.Security policy is a high level specification of the security policies. Security management is the ability to control access to the system and its services, while protecting the privacy of its legal users.

Many Organisations use the security policy to mean a colletion of content free statement.A security policy model is a succinct statement of the protection properties that a system, or generic type of system, must have. Its key points can typically be written down in a page or less. It is the document in which the protection goals of the system are agreed with an entire community, or with the top management of a customer. It may also be the basis of formal mathematical analysis.

In computer security, as in most branches of engineering, we learn more from the systems that fail than from those that succeed. MLS systems have been an e_ective teacher in this regard; the large expended in building systems to follow a simple policy with a high level of assurance
has led to the elucidation of many second- and third-order consequences of information flow controls.

Vehicular networks are promising in providing Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communication, thus allowing for many useful services on roads related to safety applications as well as entertainment applications. However, a number of constraints can impact the reliability of vehicular networks applications. The general constraints concern the high mobility, dynamic environment, security of communication,
and routing scalability. On the other hand, cooperation is vital and beneficial for services deployment in vehicular networks. We can imagine that cooperation in vehicular networks could be either implicit or explicit. The former concerns the efficiency of the MAC layer protocols in order to allow reliable multi-hop transfer between the nodes, and the efficient security mechanisms (mainly authentication and access control) that could allow the different vehicles (nodes) to communicate in a trusted manner and hence cooperate in relaying each others packets.[5].

What is security policy

Security engineering is about building system to remain dependable in the face of malice as well as error and mischance. As a discipline, it focuses on the tools, processes and methods needed to design, implement and test complete systems, and to adapt existing systems as their environment.[1]

Security and privacy are important to the wide deployments of delay tolerant networks. Without security and privacy guarantees, people are reluctant to accept such a new network paradigm. To address the security and privacy issues in delay tolerant networks, in this paper, based on ID-based ring signatures and Merkle hash tree techniques, we present a new efficient anonymous authentication mechanism. The newly proposed mechanism not only achieves good security properties, including authentication, anonymity and confidentiality, but also has strong robustness and high efficency.[2]

Access Control

As we have seen, security policies started primarily as coherent sets of constraints describing who could access what, and when. Even if our last few examples have shown more general scenarios, controlling access to resources tends to be the primary goal of many security policy models. It must be noted that pure access control is not the best mechanism when the policy requires state to be retained.

A delay tolerant network (DTN) is a store and forward network where end-to-end connectivity is not assumed and where opportunistic links between nodes are used to transfer data.

Security Attacks of Vehicular Networks. The application of vehicular ad hoc network (VANET) improves driving safety and traffic management. Due to the above applications, security attacks on VANET can be serious threats all the time. VANET is a special form of mobile ad hoc network (MANET). Hence any attacks exist on MANET also can be arisen on VANET. Moreover, some special attacks can be raised on VANET, which do not exist on MANET. Nevertheless, some characteristics of VANET can be positive effects and some can be negative effects on security issues. Before designing the security mechanism to defend attacks, the authors should take the positive effects and avoid the negative effects on the security of VANET. Furthermore, the authors class all possible attacks of VANET from every network layer. They also introduce the reason of forming every attack and the possible effect on VANET in detail. Therefore this chapter helps understanding the latent threats and the useful resources of security issues on VANET.[3]

Security and privacy Mechanisms for Vehicular Networks

Security and Autentication versus Cooperation

Cooperation between nodes in vehicular networks should be guaranteed in order to assure the correct service provision. Although cooperation in vehicular networks is important and beneficial to allow service access in a multihop distributed fashion, it could penalize the service access and the whole communication if malicious nodes could be involved in the communication. To assure secure and hence reliable cooperation, it should be ensured that only authorized users are granted network' s access. There are two main types of attacks could exist in vehicular networks and could allow non-cooperative behavior in such
Environment i) external attacks, where the attackers do not involve in the network, however they could carry out some attacks and malicious acts impacting the communication and the network and services performance, and ii)
internal attacks, where the attackers involve in the network and have legitimate service access, however they penalize the network performance through malicious and non cooperative acts. Consequently, efficient counter measures against these attacks need to be employed in order to ensure secure and reliable cooperation in vehicular
networks. These counter-measures includes authentication and access control that are vital counter-attack measures in vehicular networks deployments, allowing only authorized users to have connectivity. Although Authentication and access control can reinforce cooperation through prevention against external attackers, internal attackers could always exist even in the presence of effective authentication and access control mechanisms. Internal attackers are nodes that are authenticated and authorized to participate in the network; however, they can be harmful
nodes causing network and service performance degradation mainly through non cooperative behaviors (selfishness, greediness, and Denial-of-Services or DoS). Hence, there is a need for complementary mechanisms to authentication and access control.[5]

Security Requirement

In general, we look to secure the operation of vehicular coomunication system to design protocols that mitigate attacks and thwart deviations from the implemented protocols to the greatest possible extent.

Message autentication and integrity mechanisms protect messages from alteration and allow receivers to corroborate the node that creted the messages. If necessary, entity autentication can provide the evidance of the sender liveness.(that sender generated message recenetly).To prevent a sender from denying having sent a message non repudiation is needed. Access control and Authorization can detemine what each node is allowed to do in the network.in terms of implemented system functionality. Confidentaility can keep message content secret from unauthorized nodes.

Privacy and anonymity are required at least level of protection is achieved before the advent of VC system.In general VC systems should not allow disclousre of private user information. In particuler the identity of vehicular performing a VC specific action should be concealed. Anonmity with respect to an obserever. Depend on the set of involved vehiculers. An observer can’t determine among all vehicules in the set which vehicular performed an action. Moreover, any two actions by the same vehicule cannot be linked. But uder specific circumstances an observer could consider a vehicule more likely to perform an action.[4]

Secure Communication

The basic way for nodes to undertake secure communication is for them to sign messages digitally,after attaching a time stamp and signer’s location and certificate to the message. This way alteration replay, and relay attacks can be defeated.

Reducing the cost of security and privacy enhancing mechanism

Mechanisms have been proposed in the literatcure to reduce overhead and enhance robustness.

Mechanism1

At the sender side, the Cert Kv is computed only once Kv. Becasue CertKv remains unchanged throughout the puedo life time t. Note that notation here does n’t distinguish which method

is used for the certificate generation. For the same reason at the verifier side the Cert Kv is validated upon the first reception and stored even though the sender appends it multiple messages. For all subsequent receptions, if the Cert Kv has already seen. The verifier skips its validation. This optimization is useful because t >>r-1

Mechanism2

The sender appends its signature to all messages. But it appends the corresponding KvCert.only once every message.

Mechanism 2 can affect the protocol robustness. If the message carries Kv and Cert ca Ki+1 is not received. Then nodes in range V must wait for a messages before the pseudosym transmission while being unable to validate any message from V.This can be dangerous if vehicules are close to each other and moving at high relative speeds.

Mechanism3

To address the forementioned issue with mechanisms 2

The transmission of Kv i+1 Cert Kv i+1 is repeated for Bconsective messages when Kvi+1.is issued with B denoted as the puch period. Rather than distributing RLs of other regions. The CA validates certificates of visitng nodes.[4]

Conculsion

A security policy is a specification of the protection goals of a system. Many expansive failures are due to understand what the system security policy should have been. Technological protection mechanisms such as cryptography and smartcards may be more glamorous for the implementer, but technology-driven designs have a nasty habit of protecting the wrong things. At the highest level of abstraction, a security policy model has little if any reference to the mechanisms that will be used to implement it. At the next level down, a protection sets out what a given type of system or component should protect, without going into implementation detail, and relates the protection mechanisms to threats and evironmental assumptions. A security target gives a precise statement of what a given system or component will protect and how [6]. Especially at the highest levels the policy functions as a means of communication. it is a contract between the implementer and the client | something that both understand and by which both agree to be bound [7]. Security and anonymity are critical in many DTN implementations. Due to the unique disconnected nature of DTNs, traditional security solutions based on public key infrastructure are not suitable for these emerging networks [8].

References

[1] T. Jamal and P. Mendes, “Cooperative relaying in user-centric networking under interference conditions,” IEEE Communications Magazine, vol. 52, no. 12, pp. 18–24, dec 2014

[2] An efficient anonymous authentication mechanism for delay tolerant networks
Computers and electrical engineering archive volume issue 3 table of contents
Pages 435-441 Year of publication_2010-09-03 ISSN:0045-7906

[3] P. Mendes,W. Moreira, T. Jamal and Huiling Zhu, “Cooperative Networking In User-Centric Wireless Networks”, Springer Lecture Notes in Social Networks, User-Centric Networking: Future Perspectives, ISBN 978-3-319- 05217-5, May 2014.

[4] Security and Policy Mechanisms for Vehicular Networks. Panos papadimitratos
Ecole Polytechnique Federale de Lausanne.

[5] Cooperation in Autonomous Vehicular Networks Sidi Mohammed Senouci1, Abderrahim Benslimane2, Hassnaa Moustafa3 1Orange Labs, 2 Avenue Pierre Marzin, 22307, Lannion Cedex, France 2LIA/CERI University of Avignon, F 339 Chemin des Meinajaries BP 1228.

[6] T. Jamal and P. Mendes. Analysis of Hybrid Relaying in Cooperative WLAN. In Proc. of IFIP WirelessDays, Valencia, Spain, November 2013.

[7] T. Jamal, P. Mendes, and A. Zúquete, “RelaySpot: A Framework for Opportunistic Cooperative Relaying,” in Proc. of IARIA ACCESS, Luxembourg, Jun. 2011.

[8] T. Jamal and P. Mendes. “Cooperative Relaying for Dynamic Networks”, EU Patent, (EP13182366.8), August 2013.