https://doi.org/10.3311/PPtr.14955

Periodica Polytechnica Transportation Engineering, 48(4), pp. 377–383, 2020

Recent Developments on Security and Privacy of V2V & V2I Communications: A Literature Review

Evangelos Mitsakis[1], Iliani Styliani Anapali[2*]

[1] Center for Research and Technology Hellas (CERTH), Hellenic Institute of Transport (HIT), 6th km Charilaou-Thermi Rd., 57001, Thermi, Thessaloniki, Greece
[2] Department of Transportation and Hydraulic, Faculty of Rural and Surveying Engineering, Aristotle University of Thessaloniki, 54124, Thessaloniki, Greece
[*] Corresponding author, e-mail: iliani.anap@gmail.com

Received: 09 September 2019, Accepted: 19 November 2019, Published online: 05 April 2020

Abstract

In the recent years Intelligent Transportation Systems and associated technologies have progressed significantly, including services based on wireless communications between vehicles (V2V) and infrastructure (V2I). In order to increase the trustworthiness of these communications, and convince drivers to adopt the new technologies, specific security and privacy requirements need to be addressed, using Vehicular Ad Hoc Networks (VANETs). To maintain VANET's security and eliminate possible attacks, mechanisms are to be developed. In this paper, previous researches are reviewed aiming to provide information concerning matches between an attack and a solution in a VANET environment.

Keywords

V2V, V2I, Vehicular Ad Hoc Networks (VANETs), privacy, security

1 Introduction

Cooperative Intelligent Transport Systems (C-ITS), also known as Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Everything (V2X) communications, utilize technologies that allow inter-vehicle communication, exchanging information with road-side infrastructure and with other road users. C-ITS deal with transportation issues, improves road safety by contributing to reduced number of accidents, decreased congestion, improved handling of the travel demand, supporting eco-friendly choices of transportation and optimal use of the already existing capacity of transport networks.

The main concern about these communications is the trustworthiness and integrity of the information provided, in order to verify the authenticity of the messages, and the confidentiality of the data, to ensure that measurements made by a sensor are not intercepted by a third party. Securing mechanisms are developed to protect users' privacy, as a privacy violation can discourage users from adopting this new technology.

VANET is a security framework concerning V2V, V2I and hybrid communications, created by applying the principles of Mobile Ad Hoc Networks (MANETs), and includes On-Board Units (OBUs) and Road Side Units (RSUs) (Sucasas et al., 2016). On Board Units (OBU) are installed on vehicles and operate on a principle of Dedicated Short Radio Communications (DSRC). They consist of sensors that collect, process and exchange data via channels (Durech et al., 2016; Monteuuis et al., 2017). Road-Side Units (RSU) are mostly located at intersections and their operation extents the telecommunication operation by providing additional data packages to the drivers (Durech et al., 2016; Monteuuis et al., 2017). In the near future more vehicles are expected to be equipped with OBUs, and more RSUs will be deployed, enhancing V2V and V2I communication. Moreover, every vehicle in VANET should be equipped with a Global Positioning System (GPS) or a Differential Global Positioning System (DGPS) receiver, in order to precise its location (Durech et al., 2016; Yang et al., 2004).

Vehicle-to-Vehicle communication is the exchange of data between two or more vehicles without the support of RSUs (Monteuuis et al., 2017). V2V communication includes the exchange of collision warning messages, road obstacle warning, cooperative driving, intersection

Cite this article as: Mitsakis, E., Anapali, I. S. (2020) "Recent Developments on Security and Privacy of V2V & V2I Communications: A Literature Review", Periodica Polytechnica Transportation Engineering, 48(4), pp. 377–383. https://doi.org/10.3311/PPtr.14955

collision warning, and lane modification assistance (Durech et al., 2016). The most common message is the Basic Safety Message (BSM). A BSM contains information about the state of the vehicle, such as acceleration, speed, position, brake system status and transmits it multiple times per second (Jae and Seng., 2016). V2I is the exchange of information between vehicles and infrastructure (Monteuuis et al., 2017), and are responsible for traffic monitoring.

Following the introduction, the paper is structured as follows: Section 2 refers to security and privacy requirements that need to be addressed; Section 3 lists the attacks and challenges in VANET; Section 4 suggests security and privacy preserving mechanisms; Section 5 proposes solutions to the attacks and challenges and Section 6 concludes this paper.

2 Security and privacy requirements

To guarantee the success of VANET, it is important to list the security and privacy requirements that need to be addressed. Security requirements increase the security of processing and data exchange, while privacy requirements increase the trustworthiness between the system and the traders with the system. The studies reported in (Jae and Seng, 2016; Sucasas et al., 2016; Hasrouny et al., 2017; Agarwal, 2017; Asuquo et al., 2018) investigate and establish them in detail.

2.1 Security requirements

1. Authentication. Receivers accept messages only by legitimate senders, in order to protect the system from malicious users and false data (Agarwal, 2017). An authenticated origin is verified by certificates and pseudonyms (Hasrouny et al., 2017).
2. Confidentiality. Confidentiality is a set of rules aiming to limit access on certain resources by unauthorized users (Hasrouny et al., 2017), and protect data from eavesdroppers. Confidentiality mainly uses encryption techniques based on secure key management system (Agarwal, 2017).
3. Traceability and Revocability. For security reasons, real identity of the vehicles must stay hidden from third parties, but at the same time must be traceable from specific authorities, in order to revoke them in case of misbehavior (Hasrouny et al., 2017). A Trust Authority keeps a revocation list including those OBUs cannot be trusted.
4. Efficiency. The computational overhead should be decreased to keep low channel delays and ensure high efficiency of the scheme (Hasrouny et al., 2017).

2.2 Privacy requirements

1. Short-term linkability. When an OBU provides two or more data packages in a short period of time δt, the receivers should be able to link the massages with the source in order to address the risk of Sybil attack.
2. Long-term unlinkability. The messages transmitted cannot be linked with the originator's identity, so sensitive information such as sender's location, direction etc., remain hidden, ensuring drivers' privacy.
3. Forward unlinkability. After a vehicle is included in TA's revocation list, its future messages are still untraceable (Sucasas et al., 2016).
4. Anonymity. Anonymity is used to preserve users' identity and actions hidden from third-parties. It is usually achieved with pseudo-anonymous identities (Hasrouny et al., 2017).
5. Pseudonymity. Privacy and anonymity is achieved with pseudo-identities, temporary and anonymous keys, giving drivers' the opportunity to access certain services, while staying untraceable. A Trusted Third-Party, usually the CA, is the only authority that can link every pseudonym with the real identity and in case of misbehaving revoke the malicious vehicle.
6. Accountability - Non-reputation. Entities cannot deny any previous or current message transmission (Monteuuis et al., 2017).
7. Location Privacy. All information concerning vehicles' trajectories, present or past location, points of interest etc., must be protected from other entities (Asuquo et al., 2018).

3 Attacks and challenges

Before adopting any security architecture, such as VANET, one must acknowledge the risks associated with message transmission via wireless communications. Several studies investigated the risks of VANET (Raw et al., 2013; Samara et al., 2010; Chauley, 2016; Lim and Manivannan, 2016; van der Heijden, 2010; Dak et al., 2012; Hasrouny et al., 2017).

Authors in (Hasrouny et al., 2017), suggest four main attack categories:

1. Wireless interface, including:
   - Location Tracking. The attacker outlines driver's characteristics and tracks his/hers location.
   - Denial of Service (DoS). The attacker disrupts or overloads the communication channel by transmitting high numbers of messages.
   - Sybil Attack. The attacker impersonates as multiple vehicles, sending the same message, commonly resulting in road traffic.

- Malware. The attacker sends spam messages to overload the communication connection, causing delays and consuming network bandwidth.
- Man in the Middle (MiM). The attacker invades the communication of two vehicles, impersonalizing each one of them to alternate the message content.
- Brute force Attack. The attacker obtains sensitive information including passwords, identification numbers, cracks encrypted data, or tests network security.
- Black Hole Attack. The attacker intercepts or retains the data packet, transmitting it delayed or at another location.

2. Hardware and software, including:
   - Injection of erroneous messages (bogus info). The attacker intentionally transmits false messages.
   - Message Suppression or Alteration. The attacker changes message content.
   - Usurpation of the identity of a node (Spoofing or Impersonation or Masquerade). The attacker impersonalizes another vehicle.
   - Tampering Hardware. The attacker tries to get or put special data in the network.
   - Routing Attack. The attacker drops a data packet or disrupts the routing.
   - Cheating with position info (GPS spoofing) and Tunneling attack. The attacker generates false position information.
   - Timing attack. The attacker adds timeslots, creating delays.
   - Replay attack. The attacker sends previously generated messages in new connections.
3. Sensors input in vehicles, including:
   - Illusion attack. The attacker deceives vehicles' sensors, causing incorrect sensors' readings and false warning messages.
   - Jamming attack. The attacker violates VANET's radio frequencies.
4. Threats to infrastructure, including:
   - Unauthorized access. The attacker accesses the network without permission, spying the transmitted data.
   - Session hijacking. The attacker controls the session between nodes.
   - Reputation (loss of event traceability). The attacker causes denial of communication.

4 Security and privacy preserving mechanisms

Many mechanisms are developed to achieve security and privacy in vehicular communications and to ensure the trustworthiness of the system and the authentication of the messages transmitted. The proposed security architectures address the necessities and potential risks involved in VANET environment and specifies when and where to apply security controls. Authors in (Jae and Seng, 2016; Sucasas et al., 2016; Durech et al., 2016; Monteuuis et al., 2017; Rigazzi et al., 2017; Hasrouny et al., 2017; Asuquo et al., 2018), suggest multiple schemes and their constituent parts.

1. Anonymous Certificates. Transmitted messages are signed with anonymous certificates, issued by the Certificate Authority (CA), preserving the real identity of the origin. CA is the only entity that tracks vehicles via serial numbers, matches them with the anonymous certificates and revokes them in cases of misbehaving. The disadvantage of the procedure is the efficiency reduction of the revocation mechanism, and the scalability problem caused by the high communication frequency between vehicles and CA (Raya and Hubaux 2005).
2. Public Key Infrastructure (PKI). PKI consists of:
   - Certificate Authority (CA), authenticates vehicles, issues digital certificates and provides vehicles with public/secret key pairs to sign their messages (Raya and Hubaux 2005). The private key is used to sign an outgoing message, while the public key is used by the receiver to verify the trustworthiness of the sender. CA is also responsible for the revocation mechanism in case of misbehaving or corrupted entities.
   - Certificate Revocation List (CRL), includes the revoked certificates cannot be trusted. The receivers accept data packets after checking if the corresponding certificate is not published in the CRL, or else deny them (Raya et al., 2006; Rigazzi et al., 2017).
   - Root CA, a trusted party, authenticates entities' identities (Hasrouny et al., 2017).
   - Registration Authority (RA) or Enrollment Authority (EA), certified by the Root CA, issues certificates, and protects Root CA from attackers. RA activates or initializes OBUs. Only when a vehicle holds the enrollment certificate, is able to request pseudonym certificates (Jae and Seng, 2016).

- Certificate database, includes issued and revoked certificates.
- Certificate store, located on each vehicle, stores issued certificates and private keys.

The disadvantage of PKI architecture is the scalability problem, as research is required to recover the keys.

3. Pseudonym/Vehicular Public Key Infrastructure (PPKI/VPKI) (Rigazzi et al., 2017; Jae and Seng, 2016). PPKI or VPKI is a PKI architecture scheme with the additional security authority concerning traceability. Vehicles' real identity is replaced by pseudo-identities, thus creating a Pseudonym or else Vehicular PKI. PPKI/VPKI includes:
   - Root CA, responsible for the Long Term Certification Authority and the Pseudonym Certification Authority.
   - Pseudonym CA (PCA), which issues pseudonyms and CRLs to registered vehicles.

This approach suggests that every vehicle, owns a pair of public/private key and short-term certificates including some pseudonyms. After a small period of time the pseudonyms expire and the vehicles communicate with the PCA to renew them, resulting in communication overhead.

4. Group Signature Schemes. The members of a group have several private keys, but share only one public key. A receiver acknowledges the group's signature, but at the same time the identity of the sender is undistinguished. Group signature may replace the large volume of pseudonym certificates, but causes computational problems (Sucasas et al., 2016).
5. Clustering cooperative approach. Vehicles organize in groups with a group leader, responsible for gathering and delivering message packages, jeopardizing his privacy in order to maintain other group members' identity hidden. The disadvantage of the scheme is that the group leader sacrifices his privacy (Sucasas et al., 2016).
6. Pseudo-identity scheme. Vehicles are equipped with a pseudonym and a secret key, issued by the Trust Authority (TA). A receiver accepts messages after the verification of the public parameters of the TA. Vehicles only contact the TA to renew their pseudonyms periodically, to avoid traceability. The TA should not provide a large set of pseudonyms to the vehicles, in order to keep the revocation mechanism efficient in case of misbehavior, but also should not provide a small set of pseudonym, in order to avoid communication overhead between vehicles-TA, achieving autonomy of the system. TA is the only participated authority, responsible for the credential generation, credential distribution, misbehavior detection, and anonymity revocation. It is the only party that can link the serial number of the OBUs with the credentials and track the vehicles. The revocation event occurs after reporting and investigating possibly misbehaving or malicious vehicles. A transmitted message is signed with the private key and bears the pseudo-identity, securing the issue of anonymity. Only the TA can link a pseudo-identity to the real identity/ serial number of an OBU (Sucasas et al., 2016).
7. Digital signature scheme. Every vehicle is provided with a pair of long-term, cryptographic keys, one secret and one public. The CA issues a long-term certificate for the public key. Vehicles' Hardware Security Module (HSM) is responsible for storing the secret keys, generating digital signatures and managing the cryptographic keys' operations. Digital signature schemes use the pseudo-anonymous identification, in order to protect the real identity of the vehicles. To create a pseudonym, a vehicle first sends the public key to the CA, via secure channel, and then the CA signs the public key and generates a set of pseudonyms for each vehicle. When a pseudonym change occurs, the vehicle can no longer utilize the past pseudonym. The frequency of the pseudonym change depends on the security level needed (Durech et al., 2016).

To transmit a message, the sender uses its secret key to create a digital signature. In this way a cryptographic number is created. Cryptographic number, attached to the message and the certificate, which is connected with the public key, are send to the receiver vehicle. The receiver validates the certificate and the digital signature attached to the message, using its public key.

5 Proposed solutions to the attacks and challenges

5.1 Complete PKI communication

In PKI vehicles need to communicate frequently with the appropriate entities responsible for registration, pseudonym and digital certificates, public/private keys and revocation mechanisms.

Authors in (Monteuuis et al., 2017), suggest the SCOOP@F PKI protocol to achieve complete end-to-end communication between vehicles and PKI entities. Its constituent parts are:

- Root CA (RCA), a trusted party responsible for the Long Term Certification Authority and the Pseudonym Certification Authority.

- The Long Term Certification Authority (LTCA), issues Long Term Certificates (LTC), validates the Pseudonym Certificates, having the role of a security manager.
- The Pseudonym Certification Authority (PCA), responsible for the delivering, the monitoring and the use of Pseudonym Certificates.
- The Distribution Center (DC), responsible for the update of trust information, such as the Certificate Revocation List (CRL).
- The LifeCycle Management Center and the Manufacturer, responsible for vehicles' registration within the LTCA and vehicles' connection with a PKI certification authority.

PKI security mechanism constitutes from request and responses between vehicles-PKI entities, aiming to provide certificates. This type of communication includes the following stages:

- Initialization. The manufacturer generates a pair of public and private key to ensure sender's authentication, associates the public key with a unique identity, sends a registration request, and finally the LTCA accepts the request and add it to the database.
- Long Term Certificate (LTC) request and response. LTC request is sent to the LTCA.
- Pseudonym Certificate (PC) request and response. PC request, attached with the LTC, is sent to the PCA.
- Certificate Revocation List / Trusted Service Status List (TSL) request and response. CRL includes those certificates that are revoked and shall not be trusted, and the Trusted Service Status List (TSL) includes those certificate authorities that can be trusted. A vehicle may obtain these lists, by sending CLR and TSL requests to the Distribution Center.

5.2 Communication overhead elimination

As mentioned in Section 4, in PPKI/VPKI approach every vehicle owns a pair of public/private keys, short-term certificates and some pseudonyms. When the pseudonyms expire, vehicles communicate with the PCA to renew them.

In (Rigazzi et al., 2017), a method to minimize the frequency of the communication and reduce the results of the communication overhead, with a Bloom Filter compression is suggested. A bloom filter is a probabilistic data structure used to test whether an element is a member of a set. There are two possible matches, false positives and false negatives, representing the probability of "possibly in set" or "definitely not in set".

In standard CRL the certificates are identified with an ID and an optional expiry date field, while in Compressed CRL (C^2RL) a single Bloom filter of fixed size is carried by the entries field, succeeding in remaining the size constant as the number of revoked certificates increases.

The CRL size decreases the amount of data disseminated causing computational problems. CRL's overhead could be eliminated with the use of the bloom filter compression, resulting in Compressed Certificate Revocation List (C^2RL) (Rigazzi et al., 2017).

C^2RLs are issued by the RCA and delivered to the connected PCA. The PCA sends the C^2RL to the RSUs, which validate the attached signature. RSUs sign the C^2RL, and then it transmits to the connected vehicles, verifying the authenticity. In this way, malicious vehicles can be easily tracked, by checking if the certificates attached in the messages are contained in the filter transmitted in the latest C^2RL (Rigazzi et al., 2017).

5.3 Location privacy preserving

Researchers in (Asuquo et al., 2018), establish two privacy preserving authentication schemes that address location privacy in vehicular network:

- Symmetric Key Authentication Schemes (SKAS). In SKAS, a single cryptography key is used by both the sender and the receiver in the process of the encryption, to achieve message authentication. Receivers use their key to verify the messages transmitted.
- Asymmetric Key Authentication Schemes (AKAS). Public Key Cryptography (PKC) or digital signatures are utilized for signing and message verification. A public key is used for message encryption and a private one for decryption. AKAS can be either Public Key Infrastructure (PKI)-based or Identity (ID)-based authentication. ID-based authentication, which depends on ID-based crypto-systems, the real identity of vehicles is used to sign and verify digital signatures, reducing communication overheads and simplifying the process of managing certificates.

5.4 Attacks solutions

Attacks and challenges listed in Section 3, encounter with many security controls, and mostly with security and privacy mechanism analyzed in Section 4.

1. Wireless Interface. To eliminate wireless interface risks, it is of primary importance to secure OBUs location and identity. Pseudonyms, anonymous changing keys or group signature are mainly

used. Digital certificates and signatures in association with confidential key communication and short-lived changing keys are used to resist to Man in the Middle, Malware and Spamming, and DoS attacks. Sybil attacks may be encountered with temporary certificates, PKIs, anonymous certifications, and pseudo-identity mechanisms (Hasrouny et al., 2017).

2. Hardware and Software. Group and Digital signature schemes are the proposed solutions for message tampering, message saturation, replay attack, node impersonation, masquerading, and routing attacks. Researchers recommend VPKI, group communications use for Spoofing and Forgery attack. The majority of the attacks could be abated with time stamping techniques and cryptographic certificates, symmetric cryptography and authenticated identities (Hasrouny et al., 2017).
3. Sensors input in vehicles. Jamming attack is surpassed by switching transmission channel or switching between different wireless technologies, while for GPS Spoofing, Faking Position or Illustration attack, digital signature with positioning system is suggested (Hasrouny et al., 2017).
4. Threats to infrastructure. For unauthorized access CRL's digital certificates, certified and disposable keys are used. Moreover, to preclude traceability, authenticated and verified sensors, or audit logs, remote activation and deactivation of nodes are proposed (Hasrouny et al., 2017).

6 Conclusion

In this paper, a literature review about the recent developments on secure V2V and V2I communication has been presented. The paper discusses the current architecture mechanisms that can be used to enhance the trustworthiness of the transmitted messages and overcome the disadvantages. Several threads concerning VANET security framework exist, and additional research needs to be done to enhance the robustness of the scheme from potential attacks.

References

Agarwal, P. (2017) "Technical Review on Different Applications, Challenges and Security in VANET", Journal of Multimedia Technology & Recent Advancements, 4(3), pp. 21–30.

Asuquo, P., Cruickshank, H., Morley, J., Ogah C., P., A., Lei, A., Hathal, W., Bao, S., Sun, Z. (2018) "Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges and Countermeasures", IEEE Internet of Things Journal, 5(6), pp. 4778–4802. https://doi.org/10.1109/jiot.2018.2820039

Chauley, N. K. (2016) "Security Analysis of Vehicular Ad Hoc Networks (VANETs): A Comprehensive Study", International Journal of Security and Its Applications, 10(5), pp. 261–274. https://doi.org/10.14257/ijsia.2016.10.5.25

Dak, A. Y., Yahya, S., Kassim, M. (2012) "A Literature Survey on Security Challenges in VANETs", International Journal of Computer Theory and Engineering, 4(6), pp. 1007–1010. https://doi.org/10.7763/ijcte.2012.v4.627

Durech, J., Franekova, M., Holecko, P., Bubenikova, E. (2016) "Modelling of Security Principles Within Car-To-Car Communications in Modern Cooperative Intelligent Transportation Systems", Information and Safety-Related Systems, 14(1), pp. 49–88. https://doi.org/10.15598/aeee.v14i1.1279

Hasrouny, H., Samhat, A. E., Bassil, C., Laouiti, A. (2017) "VANet security challenges and solutions: A survey", Vehicular Communications, 7, pp. 7–20. https://doi.org/10.1016/j.vehcom.2017.01.002

van der Heijden, R. (2010) "Security Architectures in V2V and V2I Communication", In: 13th Twente Student Conference on IT June 21st, Enschede, Netherlands, pp. 1–10.

Jae, J. K., Seng, P. H. (2016) "Study on the privacy-preserving vehicular PKI in autonomous driving environments", Contemporary Engineering Sciences, 9(13), pp. 619–625. https://doi.org/10.12988/2016.6449

Lim, K., Manivannan, D. (2016) "An efficient protocol for authenticated and secure message delivery in vehicular ad hoc networks", Vehicular Communications, 4, pp. 30–37. https://doi.org/10.1016/j.vehcom.2016.03.001

Monteuuis, J. P., Hammi, B., Sallés, E., Labiod, H, Blancher, R., Abalea, E., Lonc, B.(2017) "Securing PKI Requests for C-ITS Systems", In: 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, pp. 1–8. https://doi.org/10.1109/icccn.2017.8038492

Rigazzi, G., Tassi, A., Piechocki R. J., Tryfonas, T., Nix, A. (2017) "Optimized Certificate Revocation List Distribution for Secure V2X Communications", In: 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall), Toronto, ON, Canada, pp. 1–7. https://doi.org/10.1109/vtcfall.2017.8288287

Raw, R. S., Kumar, M., Singh, N. (2013) "Security Challenges, Issues and Their Solutions for VANET", International Journal of Network Security & Its Applications (IJNSA), 5(5), pp. 95-105. https://doi.org/10.5121/ijnsa.2013.5508

Raya, M., Hubaux, J. P. (2005) "The security of vehicular ad hoc networks", In: Proceedings of the 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN '05, New York, NY, USA, pp. 11–21. https://doi.org/10.1145/1102219.1102223

Raya, M., Jungels, D., Papadimitratos, P., Aad, I., Hubaux, J. P. (2006) "Certificate revocation in vehicular networks", Laboratory for computer Communications and Applications (LCA), School of Computer and Communication Sciences, EPFL, Ecublens, Switzerland, pp. 1–10.

Samara, G., Al-Salihy, W. A. H. Sures, R. (2010) "Security Analysis of Vehicular Ad Hoc Networks (VANET)", In: 2010 Second International Conference on Network Applications, Protocols and Services, Kedah, Malaysia, pp. 55–60.
https://doi.org/10.1109/netapps.2010.17

Sucasas, V., Mantas, G., Saghezchi, F. B., Radwan, A., Jonathan, R. (2016) "An autonomous privacy-preserving authentication scheme for intelligent transportation systems", Computers & Security, 60, pp. 193–205.
https://doi.org/10.1016/j.cose.2016.04.006

Yang, X., Liu, J., Vaidya, N. H., Zhao, F. (2004) "A vehicle-to-vehicle communication protocol for cooperative collision warning", In: The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, 2004. MOBIQUITOUS 2004, Boston, MA, USA, pp. 114–123.
https://doi.org/10.1109/mobiq.2004.1331717