IJETST- Vol.||02||Issue||02||Pages 1792-1799||February||ISSN 2348-9480 2015

Open access Journal International Journal of Emerging Trends in Science and Technology

An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications

Authors

Mr.K.Kamal Kishore[1],M.Suvitha[2]

[1]Assistant Professor, [2]PG Student

Dept.of IT, Adhiparasakthi Engineering College, Melmaruvathur

Email: *Kamalitapec@gmail.com, Suvitha.610@gmail.com*

ABSTRACT

Now a days people facing many problems because of traffic. To avoid this problem VANET is used here.In this group signature is used in VANETs to realized unauthorized authentication. In the existing system, group signatures is used and its suffers from long delay in the certificate revocation list (CRL) checking and process of signature verification, high message loss. In VANET in which roadside units (RSUs) are responsible for distributing group private keys and to managing vehicles in a localized manner. Then to avoid time consuming, hash message authentication (HMAC) is used here. The proposed work of this project is trinary partitioned black-burst-based broadcast protocol(3P3B) consists of two primary mechanisms. First, a mini distributed interframe space (DIFS) in a medium access control (MAC) sublayer is used to give higher access priority to the time critical emergency message as a higher priority and to communication channel compared with other messages. Second, a trinary is designed to iteratively partition the communication range into small sectors. In 3P3B outperforms benchmarks of the existing broadcast protocols in VANETs in terms of the packet delivery ratio, average message speed, message progress and communication delay.

Index terms—*Batch group signature, cooperation, hash message authentication code (HMAC), 3P3B, emergency message(EM)*

INTRODUCTION

A vehicular adhoc network (VANET) uses cars as mobile nodes in a MANET to create mobile network. VANET allowing cars at the distance of 100 to 300 meters of each other to connect. VANET is composed of three components: onboard units (OBU), roadside units (RSU)and trust authority (TA).Being aware of the traffic condition, such as vehicles in a position, speed, direction, safety. The goal is to achieve the HMAC, batch group signature verification and cooperative authentication. First ,the whole network is spilted into several domains. HMAC is used to replace the time consuming CRL checking and to ensure the integrity of messages before batch verification, reducing the number of invalid messages in the batch. It use cooperative authentication to improve the efficiency. It can meet the requirement of verifying 600 messages per second.

In this paper, a trinary partitioned black-burst-based broadcast protocol (3P3B) is proposed as an effective multihop broadcast protocol for time-critical EM dissemination in VANET. 3P3B it enables a speed and more reliable emergency message dissemination by shortening the channel access time and reducing the contention period jitter.

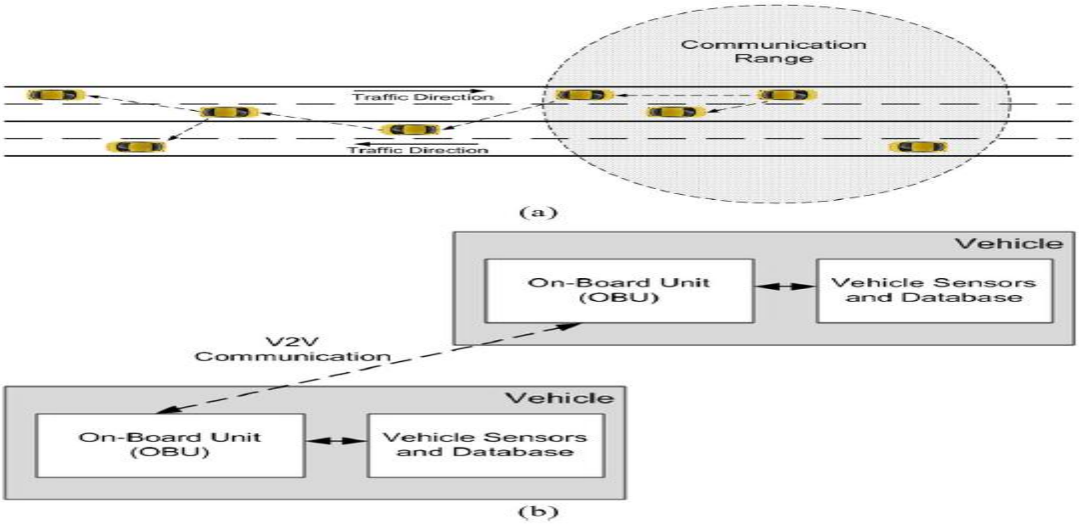

FIG 1. Architecture For Vanet Using V2v Communication

3P3B is composed of two main mechanisms.

The first mechanism is a mini distributed interframe space (DIFS) enhancement in a MAC sublayer. This is a channel to determine access mechanism which allows time-critical EMs to access a channel faster with low contention. Instead of waiting for the whole DIFS period, the time-critical EMs only wait for a fraction of DIFS to access the communication channel. So the mini-DIFS gives the time critical EMs as a higher priority. The second mechanism is a trinary partitioning, which is used to forwarding process. The next step is to select the farthest possible forwarder from the sender to forward the EM to the next hop with the largest progress range per hop. This can be done by the trinary partitioning mechanism.

The performance of 3P3B in terms of the average hop count and end-to-end delay. It provides high mobility and device portability that enable to connect network of node and communicate to each other. It allows the devices to maintain connections to the network and easily adding and removing devices in the network. User flexibility to design such a network at low cost and minimum time. Mobile ad hoc network consist large number of node and it form temporary network with dynamic topology. In this network without any central authority each node communicates with each other through radio channel. The performance of 3P3B, both analytical and simulation based evaluations are given in this paper. The results demonstrate that 3P3B attains more than 16% higher average dissemination speed compared with the efficient and robust benchmark protocols and maintains high communication reliability, which is greater than 95% of packet delivery ratio (PDR), even in a dense network. The rest of the paper is organized as follows: Section IIsummarizes the existing related work in the literature. The existing system model III and the proposed 3P3B are given in Section. Section IVdescribes the validation of the analytical models and the optimization of 3P3B. Performance analysis and comparisons with the existing state-of-the-art benchmark protocols are given I SectionIV. Finally, Section V concludes this paper.

RELATED WORK

A. A Distributed Key Management

Distributed key management is expected to facilitate the revocation of impropervehicles, system maintanence, and security policies, compared with the centralized key management assumedby the existing group signature schemes. In framework, eachroad side unit (RSU) acts as the distributed key for the group, where a new issue is that the semi-trust RSUs may becompromised. The develop security protocols for the scheme which are able to detect compromised RSUs and their colluding improper vehicles

B. Definition of group

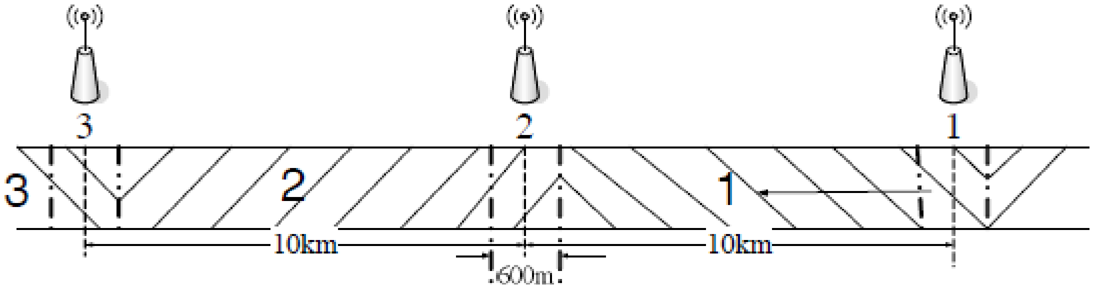

FIG 1: Group signature

These vehicles are getting keys from the same RSU form a group, as illustrated in Fig. 1, where the communication range of RSUs is 300 meters marked by the dashed lines. We assume that RSUs are only deployed at road segments entrances. In a highway scenario, RSUs are normally far away from each other. In the region out of the RSU coverage, vehicles in the same group can communicate with each other in an adhoc manner. In a city area, RSUs might overlap with each other.

C. Authentication with Privacy

Anonymous Signatures

The notion of anonymous signatures, introduced by Yang et al. and aims to achieve anonymity in the traditional settings of digital signatures, where the private key of a signer is used to produce signatures that are then verified using the Certificate revocation list (CRL).The verification procedure of a signature scheme requires as input the public key of the signer and the corresponding message. In the presence of system-wide known public keys there is hope to keep the signer anonymous as long as messages are not publicly disclosed. These ideas were formulated in assuming that signed messages have sufficiently high entropy to prevent otherwise unavoidable attacks, by which the anonymity adversary would guess the message and try out different public keys until the right public key allowing successful verification of the given signature is found.

The original definitions of anonymity for digital signatures from were simplified by Fischlin and adopted to address the potential exposure of secret signing keys. He also described a general transformation that adds the anonymity property to any unforgetable digital signature scheme, while the original work in showed more concrete constructions of anonymous signatures using number-theoretic constructions based on integer factorization and discrete logarithms. A slightly different concept for anonymous signatures was introduced independently in, where the assumption on high entropy of messages was traded against partial disclosure of signatures, i.e., by splitting the signature in two or more distinct components of which at least one is withheld. For these revised definitions of anonymity, provided several general transformations, achieving anonymity for arbitrary signature scheme and showed in addition a more concrete construction in the setting of bilinear maps.

The anonymity property of anonymous signatures differs, however, from the anonymity provided by group signatures in many ways. While group signatures aim is to protect anonymity of the signer against verifiers, yet allowing the latter to perform the verification procedure, unauthorized signatures lose their anonymity property as soon as the entire message-signature pair is revealed. This information, however, is required to perform the verification procedure.

D. Routing Protocol

This routing protocol utilizes the distance to select the forwarding nodes. The distance method uses the minimum distance from sender to receiver (one-hop distance) as the variable of discrimination between rebroadcasters and nonrebroadcasters. The method appeals to the intuition that if a node has received a message from another node very close to it, there is somewhat benefit in terms of additional coverage achieve by rebroadcasting. Nodes then should favour rebroadcasting when this distance is large.

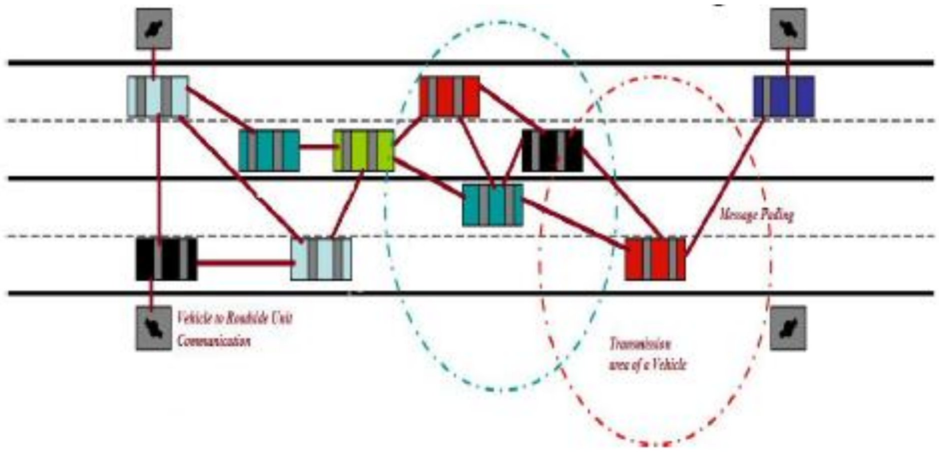
Message Fading
Vehicle to Roadside Unit Communication
Transmission area of a Vehicle

FIG 2: Transmission of routing protocol

E. Efficient and Reliable Broadcast in Intervehicle Communication Networks

a) simple flooding in which a node rebroadcasts a new message until it reaches all connected nodes in thenetwork

b) probability-based methods in which protocols can be further divided into two subclasses:

   I. a node rebroadcasts a message according to a predefined probability and it becomes a simple flooding

   II. a node decides whether to rebroadcast a message based on the number of the received copies during a certain period of time

c) an area-based method in which a node that can cover more additional area is selected to forward the received message from the source;

d) a neighbor knowledge method in which a node makes a forwarding decision according to the knowledge of its one-hop or two-hop neighbors

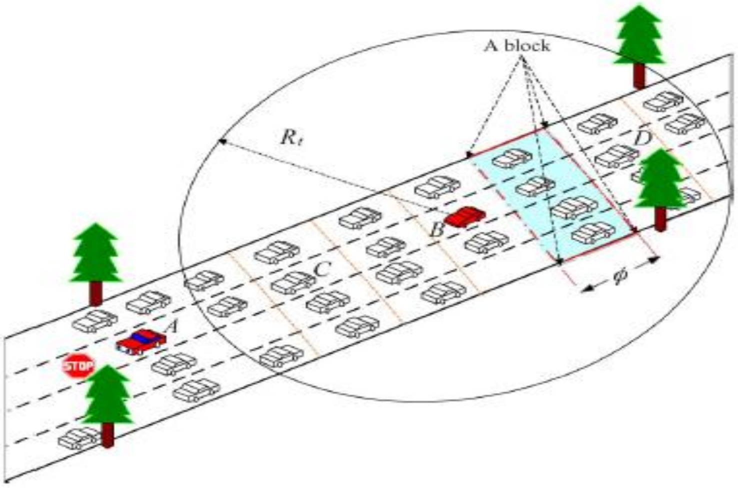

FIG 3: Blocks of highway

EXISTING SYSTEM

A vehicle should broadcast security related messages every 300 ms. In other words a vehicle has to verify 600 security related messages per second if there are about 180 vehicles in the communication range. The verification process of the group signature attached to the security related messages has to be efficient enough. To reduce the signature verification time employ batch group signature verification based on the properties of bilinear pairing operation, in which a large number of messages can be authenticated in a timely manner. If there exists a few invalid messages caused by wireless interference, packet loss they may introduce additional verification delay for rebatch and then lose their efficiency. Even if we do not count the rebatch time, the computation overhead of batch group signature verification. Attackers can easily get users private information, such as identity, tracing, if they are not properly protected in the existing system. In VANET, group signature is widely used for vehicles to achieve anonymous authentication since it allows any group member to sign a message on behalf of the group without revealing its real identity. When receiving a message from an unknown entity a vehicle has to check the certificate revocation list (CRL) to avoid communicating with revoked vehicles and then verify the sender’s group signature to check the validity of the received message.

ALGORITHM IMPLEMENTATION

In the existing system, RSA algorithm is used it is a symmetric key. It can be spiltted into multiple sectors and allocated the different key into each group .when the node is moving from one range to another range if it have the same key it searching for other access point. If any of the node does not get the proper signal and cannot connect to the access point they will be the attackers and throughout from out of range. So it may cause the long delay and loss of packet delivery ratio. To overcome this drawbacks AES algorithm is used in the proposed system.

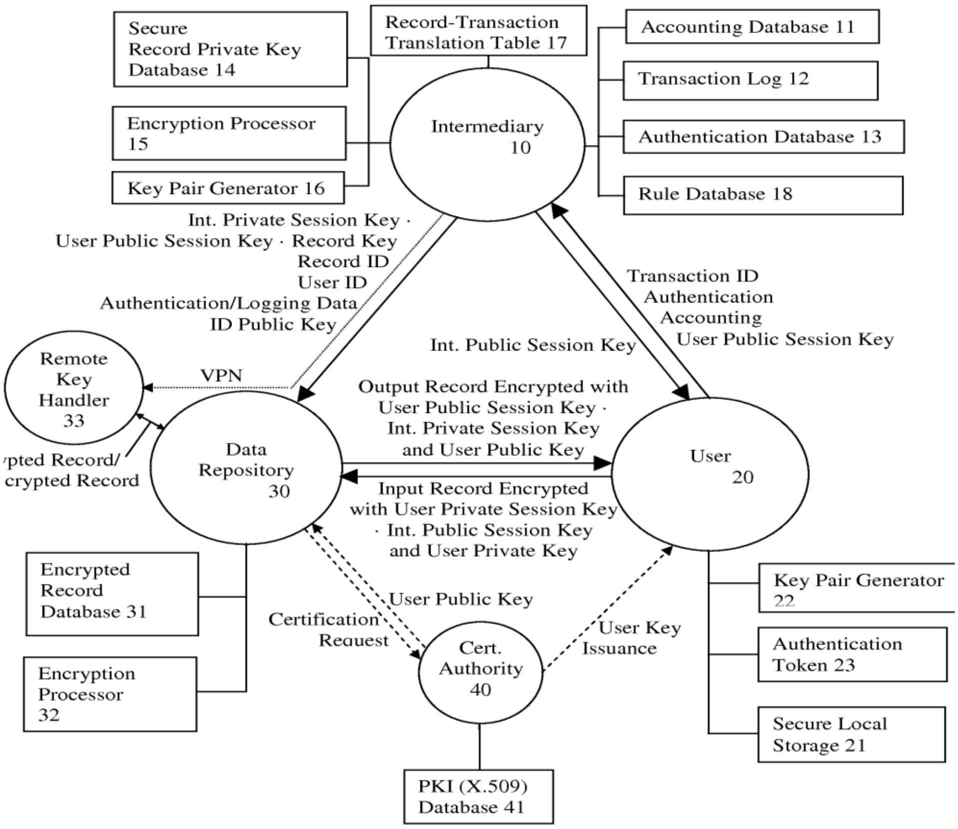

FIG 4. Block Diagram For Key Generation

One of the key is the private key and it will be kept secret and not shared with anyone. The other key is public key and it will not be kept secret and it can be shared with anyone. Data is encrypted by one of the keys and it can only be decrypted and recovered by using the other key. Techniques are used in this paper; they are group signature, HMAC and DSRC.

A dynamic group signature scheme

Γ=(GKg, (JoinM, JoinU), GSign, GVrfy, Open)

Key generation

Algorithm for the randomized group key generation algorithm GKg takes as input the security parameter as input

1^{κ}, $\kappa \in N$ *and*

returns a tuple (*gpk, gmsk, reg),*

where gpk is the group public key, *gmsk* is the group manager secret keyand *reg* is the registration list, which is initially empty.

Signature generation

The randomized group signing algorithm *GSign* takes as input a secret signing key *gsk[i]* and a message m and returns a group signature *σ.*

Signature verification

The deterministic group signature verification algorithm GVrfy takes as input the group public key gpk, a message m, and a candidate signature σ for m, and returns either 1 (to indicate that the signature is valid) or 0 (to indicate a failure).

Group signature scheme

Γ = (GKg, (JoinM, JoinU), GSign, GVrfy, Open) is correct if for all κ*, n* $\in N$*,*

all outputs (gpk, gmsk, reg) ← GKg(1^{κ}*),*

all outputs (reg[i], gsk[i]) ← (JoinM(gmsk,i), JoinU(gpk,i))

for any i $\in [1,n]$*, and all messages m* $\in \{0, 1\}^{*}$*:* *GVrfy(gpk, m, GSign(gsk[i],m))=1 and Open(gmsk, m, GSign(gsk[i],m), reg)= i.*

PROPOSED SYSTEM

The potential forwarders, who are in the outer partition, who are located in the second partition, will simultaneously broadcast a black burst B only during the first time slot and will first listen to the channel during the first time slot and then broadcast a black burst during the second time slot if they are no black-burst transmission during the first time slot.

The concept in the proposed system and show the reduction in compromising of node, secure connectivity, less memory usage, storage, computational and communicational efficiency than the existing system. The pairwise key establishment among nodes within the initialization phase.

Within the initialization phase, every node A broadcasts periodically a hello message.

This message is used to communicate the identifier of the node and of its seeds to the neighbours such as IDA (node identifier) and IDsx, IDsy (seed identifier)

- When a node B within the initialization phase receives a hello message, then it looks for shared seeds in the received set of seed IDs.
- If there are shared seeds, it randomly chooses a permutation factor(m) between 0 and 2µ and a seed among the shared seeds that are already used by the minimum number of links with other neighbors
- The goal of this routine is to decrease the number of unused seeds.
- The shared seed is transformed, using the seed and m as input of t().
- Node B executes f() with the new seed and MK to generate a pairwise key that will be used between the two nodes (A and B).
- The new key is identified by the identifier of the seed concatenated to the permutation factor.

- Then, node B replies to node A with an acknowledge message. This message contains: the identifier of node B , the seed, the permutation factor, and the MAC executed on the message (in order to prove the authenticity
- The cancellation of MK and of the seeds is required to protect the security of the network, since an opponent that owns MK and some seeds is able to generate all the corresponding keys.
- Although an attacker requires also t() and f() to generate new keys, since they are considered public, the security of the system is only based on the secrecy of MK and of the seeds.

CONCLUSION

The main aim of this project is proposed to 3P3B for the efficient time critical EM Dissemination in VANETs.Implement Trinary Partitioned Black-Burst-Based Broadcast Protocol for Time Critical Emergency Message Dissemination in VANETs for the efficient time- critical EM dissemination in VANETs. 3P3B employs trinary partitioning and mini-DIFS mechanisms. It is demonstrated through both analytical and simulation results that the proposed 3P3B outperforms the benchmark state-of-the-art protocols in terms of the average delay, average message dissemination speed, and average PDR.

REFERENCES

1. S.-B. Lee, G. Pan, J.-S. Park, M. Gerla, and S. Lu, "Secure incentives for commercial adissemination in vehicular networks," in *Proc. 8th ACMInt. Symp. MobiHoc*, Montreal, QC, Canada, Sep. 2007, pp. 150–159.
2. M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.
3. K. Mershad and H. Artail, "A framework for secure and efficient data acquisition in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*,vol. 62, no. 2, pp. 536–551, Feb.2013.
4. A.Wasef and X. Shen, "EMAP: Expedite message authentication protocol for vehicular ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 78–89, Jan. 2013
5. C. P. Schnorr, "Efficient signature generation by smart cards," *J. Cryptol* vol. 4, no. 3,pp. 161–174, 1991.
6. A. L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen, "Practical short signature batch verification," in *Proc. Top. Cryptol.—CT-RSA*, vol. 5473, *Lecture Notes in Computer Science*, 2009, no. 2009, pp. 309–324.
7. S. Frankel, R. Glenn, and S. Kelly, The AES-CBC cipher algorithm and its use with IPsec, RFC 3602, Sep. 2003.
8. D. Eastlake and P. Jones, US secure hash algorithm 1 (SHA1), RFC 3174, Sep. 2001.
9. X. Zhu, S. Jiang, L. Wang, H. Li, W. Zhang, and Z. Li, "Privacypreserving authentication based on group signature for VANETs," presented at the IEEE Global Telecommunications Conf., Atlanta, GA, USA, Dec. 2013, Paper WN-23.
10. K. A. Shim, "An efficient conditional privacy-preserving authenticationscheme for vehicular sensor networks," *IEEE Trans. Veh. Technol.*,vol. 61, no. 4, pp. 1874–1883, May 2012.
11. J. L. Huang, L. Y. Yeh, and H. Y. Chien, "AKABA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 60, no. 1, pp. 248–262, Jan. 2011 VANETs (R-OB-VAN)," in *Proc. 9th Int. Conf. ITS Telecommun.*, Lille, France, 2009, pp. 382–387.

12. M. Khabazian, S. Aissa, and M. Mehmet-Ali, "Performance modeling of message dissemination in vehicular ad hoc networks with priority," *IEEEJ. Sel. Areas Commun.*, vol. 29, no. 1, pp. 61–71, Jan. 2011
13. B. Yuanguo, L. X. Cai, S. Xuemin, and Z. Hai, "Efficient and reliable broadcast in intervehicle communication networks: A cross-layer approach," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2404–2417,Jun. 2010.
14. OMNeT++ Network Simulation Frame-work. [Online]. Available: http://www-.omnetpp.org
15. The Highway Code[Online].Available: https://www.gov.uk/browse/driving/highwaycode
16. M. Xiaomin, Z. Jinsong, and W. Tong, "Reliability analysis of one-hop safety-critical broadcast services in VANETs," *IEEE Trans. Veh. Technol.*, vol. 60, no. 8, pp. 3933–3946, Oct. 2011.
17. C. Xianbo, H. H. Refai, and M. Xiaomin, "A quantitative approach to evaluate DSRC highway inter-vehicle safety communication,"in *Proc. IEEE Global Telecommun. Conf.*, Washington, DC, USA, 2007,pp. 151–155
18. O. K. Tonguz, N. Wisitpongphan, J. S. Parikh, F. Bai, P. Mudalige, and V. Sadekar, "On the broadcast storm problem in ad hoc wireless networks,"in *Proc. 3rd Int. Conf. Broadband Commun. Netw. Syst.*, San Jose, CA, USA, 2006, pp. 1–11.
19. N. Wisitpongphan, O. K. Tonguz, J. S. Parikh, P. Mudalige, F. Bai, andV. Sadekar, "Broadcast storm mitigation techniques in vehicular ad hoc networks," *IEEE Wireless Commun.*, vol. 14, no. 6, pp. 84–94, Dec. 2007.
20. H. K. Chin and J. P. M. G. Linnartz, "Analysis of the RTS/CTS multiple access scheme with capture effect," in *Proc. IEEE 17th Int. Symp. Pers.,Indoor Mobile Radio Commun.*, Helsinki, Finland, 2006, pp. 1–5 *Chakkaphong Suthaputchakun* (M'13) received the B.Eng. degree.