A HYBIRD APPROACH FOR SECURE MESSAGE TRANSMISSION BY PAIRWISE KEY GENERATION IN VANET ENVIRONMENT

[1]Lakshmi Priya.S [2]Ramesh.G
[1]M.E Scholar, Department of IT, K.L.N College of Engineering, Pottapalayam
[2]Professor, Department of IT, K.L.N College of Engineering, Pottapalayam

ABSTRACT: Secret key generation by extracting the shared randomness in a wireless fading channel is a promising way to ensure wireless communication security. Previous studies only consider key generation in static networks, but real-world key establishments are usually dynamic. In this paper, for the first time, we investigate the pairwise key generation in dynamic wireless networks with a center node and random arrival users (e.g., roadside units (RSUs) with vehicles). We establish the key generation model for these kinds of networks. We propose a method based on discrete Markov chain to calculate the average time a user will spend on waiting and completing the key generation, called average key generation delay (AKGD). Our method can tackle both serial and parallel key generation scheduling under various conditions. We propose a novel scheduling method, which exploits wireless broadcast characteristic to reduce AKGD and probing energy. We conduct extensive simulations to show the effectiveness of our model and method.

I .INTRODUCTION

Establishing a pairwise secret key between two communication parties is crucial to securing wireless communication. Physical-layer key generation mechanisms that exploit reciprocal and spatial diversity properties of wireless fading channels have been proposed. Based on the reciprocity, the bidirectional channel states should be identical between two transceivers at a given instant of time. In a multipath or mobile environment, the channel states randomly fluctuate due to fading. Therefore, two legitimate parties can take advantage of this natural correlated random process to generate a shared key. Furthermore, the channel state observed at an eavesdropper is uncorrelated with the legitimate channel if the eavesdropper is more than half a wavelength away from legitimate parties. Existing research on physical-layer key generation mainly focuses on key generation rate (KGR) in static wireless networks. Most of the works discussed the KGR between two parties. The maximum KGR assuming no information loss on key generation procedure is bounded by the mutual information between two nodes. Theoretical studies about KGR are done. The studies of KGR considering practical communication condition are addressed.

In this paper, for the first time, we consider the key generation problem in dynamic wireless networks. In such case, using KGR to report the performance of the key generation is no longer appropriate because
1) the KGR of individual user pair is a changing quantity in dynamic wireless networks, affected by the entering and leaving of the key generation of other user pairs, and

2) the KGR cannot reflect the amount of time that user wait before doing the key generation and hence cannot report the status of service congestion in dynamic wireless networks. Thus, we focus on a different metric: the users' key generation delay. The key generation is a prestep before secure wireless communications. The delays that users suffer are their major concerned parameter.

The delay analysis of physical-layer key generation in dynamic networks is different from traditional delay analysis in wireless communication. First, in traditional delay analysis, service rate, which is denoted by the data transfer rate, is considered a constant. This is valid because using a time-division or frequency-division scheme on n user pairs reduces individual user pairs' data transfer rate to $1/n$, but the total data transfer rate remains unchanged. However, this basic assumption is no longer valid in key generation, where the service rate, which is denoted by KGR, depends on the number of users and channel probing scheduling (detailed in Section II-C). Second, to ensure that the keys generated on both sides are identical, a reconciliation process must be considered.

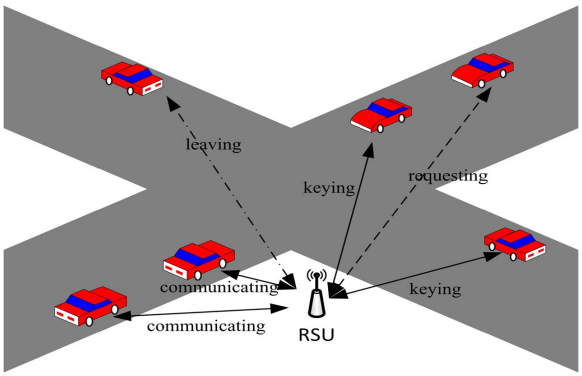

Fig. 1. Key generations in a dynamic wireless network.

In this paper, we consider the problem of pairwise key generation in dynamic wireless networks with a center node. We use the scenario of a roadside unit (RSU) with random arriving and leaving vehicles shown in Fig. 1 to exemplify our model and method. The arrival of vehicles is a stochastic process. We aim at calculating the average time a vehicle will spend on waiting and completing the key generation, called average key generation delay (AKGD). We propose the key generation model. Our model can tackle both serial and parallel key generation scheduling. We notice that, in the key generation model, each key establishment period has predictable time. We make use of such characteristic to develop a method based on a discrete Markov chain for calculating users' AKGD. Compared with our earlier work presented, we further propose a novel scheduling method, which exploits wireless broadcast characteristic to reduce AKGD and probing energy. We conduct simulations to show the effectiveness of our methods. .

Our main contributions are the following:

- We formulate the physical-layer key generation problem in dynamic wireless networks and analyze the delay.
- We propose the key generation model and develop a method to calculate AKGD.
- We propose a novel scheduling method, which exploits wireless broadcast characteristic to reduce AKGD and probing energy.
- We conduct extensive simulation to verify and evaluate our model.

II .RELATED WORK

An efficient identity-based batch verification scheme for vehicular sensor networks.
Author: Zhang.C, Lu. R. Lin and Shen. X.
Year: 2015
Identity-based cryptography/Batch signature verification scheme. This paper provides a basis for research in clustering schemes for Wireless Sensor Networks. One such problem is how to create an organizational structure amongst these nodes.

Anonymous credentials for privacy-preserving e-learning.
Author: Aïurme, E., Hage, H., & Onana, F. S. M.
Year: 2012
An E-learning system, Anonymous Credentials for E-learning Systems (ACES), ACES allows learners to provide anonymous credentials throughout the learning process, Anonymous Transcript or an Anonymous Degree. A novel approach for energy-aware management of sensor networks that maximizes the lifetime of the sensors while achieving acceptable performance for sensed data delivery. Missing sensor data might be a problem unless tolerated via the selection of redundant sensors.

Smart Cars and Smart Roads.
Author: Malik, J., Weber, J., Luong, Q. T., & Koller, D.
Year: 2009
Polynomial time approximation algorithm and optimal algorithm. Our simulation results show that multiple routing spanning trees significantly improve network reliability. The problem of constructing efficient routing trees and the problem of wake-up frequency assignment in a network with multiple routing trees.

SPARK: a new VANET-based smart parking scheme for large parking lots.
Author: Lu, R., Lin, X., Zhu, H., & Shen, X.
Year: 2009
A new smart parking scheme for large parking lots through vehicular communication. Highlight the design between energy and communication overhead savings in some of the routing paradigm. The common objective of trying to extend the lifetime of the sensor network, while not compromising data delivery.

Security issues and challenges of vehicular ad hoc networks (VANET).
Author: Samara, G., Al-Salihy, W. A., & Sures, R.
Year: 2010
The need for a robust VANET networks is strongly dependent on their security and privacy features. The connectivity among nodes can be highly ephemera. Vehicles travelling throw coverage area. A delay in millisecond makes the message meaningless; the problem is much bigger, where the application layer is unreliable, since the potential way to recover with unreliable transmission is to store partial messages in hopes to be completed in next transmission unreliable transmission is to store partial messages in hopes to be completed in next transmission.

AMOEBA: Robust location privacy scheme for VANET.
Author: Sampigethaya, K., Li, M., Huang, L., & Poovendran, R.
Year: 2007
Presented the problem of mitigating unauthorized tracking of vehicles based on their broadcast communications, to enhance the user location privacy in VANET. A safety message broadcast period, and vehicular network connectivity. Grouping vehicles to mitigate the location tracking of any

target vehicle. The group concept also provides robust anonymous access to prevent the profiling of LBS applications.

SPECS-Secure and privacy enhancing communications schemes for VANETs.
Author: Chim, T. W., Yiu, S. M., Hui, L. C., & Li, V. O.
Year: 2011
Presented a software-based solution which makes use of only two share secrets to satisfy the privacy requirement. RAISE protocol was proposed for vehicle- to-vehicle communications. The protocol is software-based. It allows a vehicle to verify the signature of another with the aid of a nearby RSU. It doesn't have authorized bloom filter. The initial verification is very low and the batch verification is high.

Secure communication scheme of VANET with privacy preserving.
Author: Hwang, R. J., Hsiao, Y. K., & Liu, Y. F.
Year: 2011
A secure communication and privacy preserving scheme of Vehicular ad-hoc network (VANET). Improves road safety and traffic conditions via the vehicle exchange the traffic information with other vehicles and some infrastructures. Problem in exchange messages are secure, trustworthy and protect user privacy. The transmission message must be well protected to ensure the integrity, confidentiality, anonymity and unlink ability.

PPGCV-Privacy preserving group communications protocol for vehicular ad hoc networks.
Author: Wasef, A., & Shen, X.
Year: 2008
It preserves the privacy of the users and provides conditional full statelessness property. GKMPAN has a partial statelessness property, which means that a node that missed certain number of group rekeying processes can compute the new group key.

Security issues and challenges of vehicular ad hoc networks (VANET).
Author: Samara, G., Al-Salihy, W. A., & Sures, R.
Year: 2010
The need for a robust VANET networks is strongly dependent on their security and privacy features. The connectivity among nodes can be highly ephemeral, Vehicles travelling throw coverage area. A delay in millisecond makes the message meaningless; the problem is much bigger, where the application layer is unreliable, since the potential way to recover with unreliable transmission is to store partial messages in hopes to be completed in next transmission.

III. PROPOSED SYSTEM:

Specific trust computation and trust derivation schemes are proposed based on analysis results. Finally, our design uses the combination of trust metric and QoS metrics as routing metrics to present an optimized routing algorithm. The routing metrics are obtained by combing the requirements on the trust worthiness of the nodes in the network and Key Generation Scheduling In the key generation, quantization and privacy amplification can be done locally at respective sides. While channel probing and information reconciliation need communication between the vehicle and RSU. When there are multiple vehicles in the system, scheduling is required to avoid interference. On the condition of equal priority, there are two scheduling policies can be used at queuing nodes in queuing theory serial serving, and processor sharing (Service capacity is shared equally among Customers).

They correspond to two key generation scheduling:

(1) **Serial Probing:** RSU probes the channel with vehicles one by one according to vehicles' arriving order.

(2) **Parallel Probing:** multiple vehicles share the channel using time-division method, RSU probes the channel with multiple vehicles in a round-robin way.

A method to calculate AKGD for both Serial and parallel probing, We will introduce a specific scheduling method by exploiting wireless broadcast characteristic in channel probing.

Analysis: In traditional queuing theory, service rate is considered as a constant. However, this assumption is no longer valid in key generation, where the service rate, denoted by KGR, depends on the number of vehicles and channel probing scheduling. Therefore, it is unable to use traditional queuing model to compute the AGKD.

Serial probing, consecutive channel probing measurements have small time separation and thus highly correlated. The correlated part provides little extra information and should be largely discarded in the final key in privacy amplification. On the other hand, for parallel probing as exemplified time separation between consecutive channel probing measurements is larger due to the insertion of the channel probing between RSU and the 2nd and the 3rd vehicles. The correlation of the measurements is lower and fewer correlated bits are discarded. The non-equal drop rate of correlated bits leads to non-equal KGR, and intuitively, parallel probing has higher KGR and smaller AKGD. We will show the correctness of the hypothesis in simulation by using proposed method to calculated AKG.

FLOW MODEL:

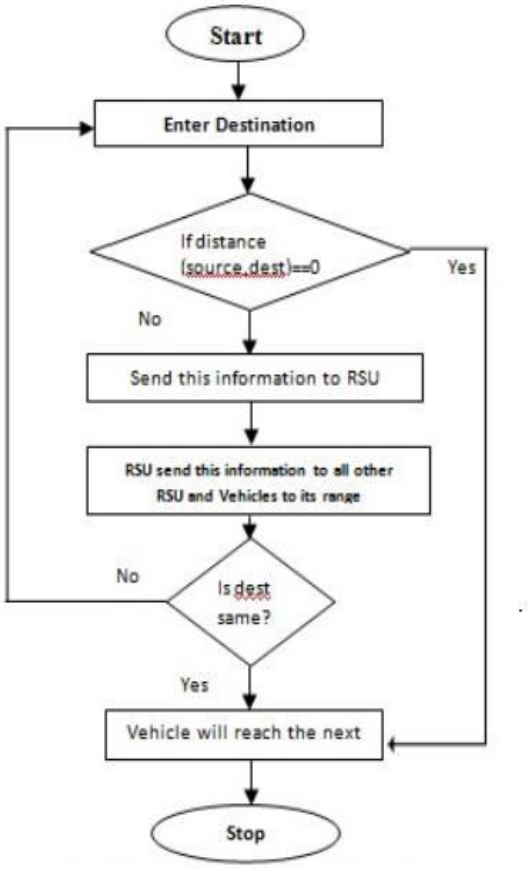

Fig.2.Flow Chart

According to the flowchart description when the process starts it will go to the next process which is enter destination after it reaches then it will go to the next condition (i.e)if the distance (source. dest)==0 this condition is "yes" then directly it will go to the last step (i.e)vehicle will reach the next if it is "no" that information will send to the RSU then that RSU send that information to all other RSU and Vehicles to its range then it will reach the next step Is the dust is same? if it is "no" it will reach the second step as enter destination if it is "yes" the vehicle will reach the next the last step is "stop" . The flowchart

implies that the destination is reached without any accident occurrence by means of knowing the speed, turning direction, location and real time traffic conditions. This can be done with the means of the Road side units and the On Board Units. Thus by knowing the destination and the road condition so that the vehicle senses the vehicle that is near and creates awareness for the driver and thus by the information given ,accidents are minimized and lives are saved.

IV.ALGORITHM:

In this section, we have suggested an algorithm to substantiate authenticity, confidentiality, access & availability during the transmission of vehicle related information. We have explained our proposed algorithm step-by-step in better way for better comprehensible. Table I shows description about notations which are used during the suggested Algorithm.

A. System Overview

In this section, we have described general scenario of current vehicle communication system which dictates basic idea behind for the same. Hence, it will be straightforward to understand actual framework. In this paper, we have assumed a vehicular ad-hoc network in which neighbors can communicate into the same direction only and with those vehicles which are available within the network range. Geographical positioning and timing related conditions are fulfilled with global positioning services receivers. To get the time instants either at receiving side or sending side, there is no any disturbance. All the vehicles have their unique identity number which is also known as vehicle identity. This vehicle identity can be a permanent for a particular vehicle during its life-cycle but it can also be destroyed if it is found as a malicious vehicle into the network.

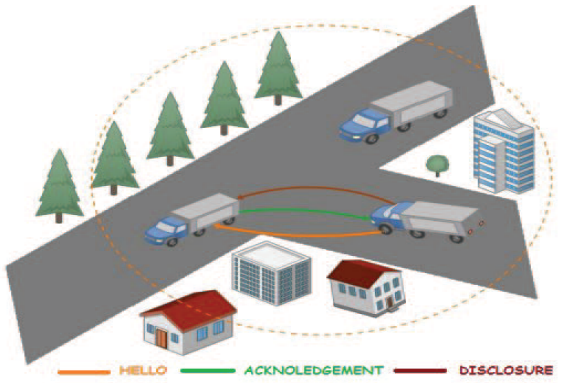

Fig.3.graphical overview of our proposed algorithm.

Vehicles have their own public key (*KX*) and private key (*K_X*) which are useful to encrypt or to decrypt the information either at sender side or receiver side. A private key (*K_ X*) is stored into the tamper-proof device which is installed in the vehicle. In the rule of encryption and decryption, we have considered the *Integrated Encryption Scheme (IES)* which is a compound encryption pattern which offers semantic security in contrast to an attacker. The security of the scheme is based on the *DiffieHellman problem*. *Discrete Logarithm Integrated Encryption Scheme (DLIES)* is one variety of *IES* which is applied especially in the cryptographic technique. Adversary may be either internal or external but internal vehicle as a adversary has more opportunities to masquerade into the system rather than external vehicle.

B. Secure Message Exchange Algorithm

We have described secure message exchange algorithm in details in which we have used concept of *HELLO ACKNOWLEDGEMENT- DISCLOSURE*. It means that user will send first *HELLO* message and another user will send

response to that user immediately after receiving message. Then finally, important information will be sent over public channel in encrypted format.

• In the first step, vehicle chooses time randomly to transmit *HELLO* message to other vehicles.

• Vehicle is able to send *HELLO* message at selected random time if and only if specific vehicle is belongs to same network range as well as speed difference between both (sender & receiver) vehicles must be less than or equal to threshold speed ($\Delta S \leq SY - SZ$). It is settled manually before the execution of protocol. There are two types of *HELLO* messages based on sender's originality. If sender is original *HELLO* message sender then some important details like sender's public key and message transmission time are stored into the *HELLO* message otherwise *HELLO* message includes message transmission time, message received time along with public key of current sender & previous sender.

• After receiving *HELLO* message at receiver side, receiver will send back one message to sender with some details like received public key as well as current time immediately for conformation. It means that specific message is received at particular time along with some important credentials.

• In last step, original sender will send another message as a *DISCLOSURE* message with such kinds of important credentials (Identity & signature of vehicle, current position and transmission time, etc.) in complex form.

Algorithm 1 Secure Message Exchange

Input: Encrypted message with public key and time-stamp

Output: Current position of vehicle

Step-1: Vehicle chooses any random time tY to transmit *HELLO* message.

Step-2: At time tY , vehicle X transmits *HELLO* message to all vehicles those are available into the network range and within the range of speed $\Delta S \leq SY - SZ$ as follows:

1) if sender is original source node then...

$HELLO = \_HELLO,KY , tY \_.$

2) if sender is not original source node then... $HELLO = \_HELLO,KY ,KX, tX, tXY.$

Step-3: Vehicle Z receives *HELLO* message from Y at $tY\ Z$ and sends *ACKNOLEDGEMENT* message to Y immediately.$ACKNOLEDGEMENT= \_ACKNOLEDGEMENT,KY , KZ, tY Z\_.$

Step-4: At time $t\_\ Y$, Y sends *DISCLOSURE* message to other vehicles.

Step-5: $DISCLOSURE = \_DISCLOSURE, IDY ,EKZ \_PY \_, t\_\ Y , SigY \_$

In proposed protocol, message is sent three times over communication channel to acquire actual position of other neighbour vehicle which are present to communicate with each other. First message is *HELLO* which is sent from one vehicle to all other vehicles. So message complexity will be $n(n-1)/2$ for *HELLO* message where n is number of vehicles. Second message is *ACKNOWLEDGMENT* which will be transferred only between receiver vehicle and sender vehicle. Thus, we can say that it is 1:1 vehicle communication. Last and third *DISCLOSURE* message is sent from sender to receiver only. It means that two vehicles participate in *DISCLOSURE* message communication. At last, total message complexity is $O(n2)$ which is quite similar to other secure positioning protocols message complexity in vehicular networks.

V.SIMULATION

The general process of creating a simulation can be divided into several steps:

1. Topology definition: to ease the creation of basic facilities and define their interrelationships, ns-3 has a system of containers and helpers that facilitates this process.
2. Model development: models are added to simulation (for example, UDP, IPv4, point-to-point devices and links, applications); most of the time this is done using helpers.
3. Node and link configuration: models set their default values (for example, the size of packets sent by an application or MTU of a point-to-point link); most of the time this is done using the attribute system.
4. Execution: simulation facilities generate events, data requested by the user is logged.
5. Performance analysis: after the simulation is finished and data is available as a time-stamped event trace. This data can then be statistically analyzed with tools like R to draw conclusions.
6. Graphical Visualization: raw or processed data collected in a simulation can be graphed using tools like Gnuplot, matplotlib or XGRAPH.

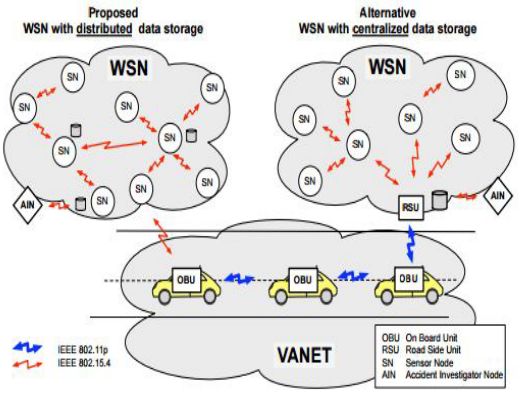

Fig.4.Architecture

VI.PERFROMANCE AND ANALYSIS

We have stipulated conjectural structure by using Linux platform with normal hardware system configuration as well as Network Simulator(NS) - 2 version was considered for implementation analysis. Each assessment was conducted 10 times, and later we have noted down the median of every used parameter. The packet delivery success ratio is around 98.00 %. We have obtained results after implementing a perceptive proposal by using the proposed algorithm concept. An end-toend delay with regard to sending throughput is 0.16 Sec and a processing time regarding forwarding throughput is 0.001Sec.

Transmitted messages are available with time-stamp & secret key in encrypted form. It will be available to only those vehicles which are belongs to network range as well as at-least speed difference must be less than or equal to threshold speed (ΔS). Hence, if anyone intercepts the message then also it will be hard to compute fake message simply. In our proposed algorithm, there are two mainly steps in which computation process is required. First one is *HELLO* message and other is *DISCLOSURE* message.

When sender vehicle sends *HELLO* message at that time it contains crucial information like public key of sender along with time-stamp of transmission message. After receiving acknowledgment from receiver, it sends *DISCLOSURE* message with important information like identity, signature and current position of sender vehicle in complex form. Acknowledgment will be sent to sender by receiver after receiving *HELLO* message. If acknowledgment is not acquired at sender side within sufficient time period

then sender will deduce that there should message loss or attack in communication channel. Hence, sender will send *HELLO* message with fresh generated public key and time-stamp once again. In addition to it, if message is stolen by any adversary vehicle then also it will not be auxiliary later because public key, private key and time-stamp is generated freshly for further communication. In such case, *DISCLOSURE* message is interrupted by adversary then also it will be difficult to get original information from encrypted data. After that, adversary cannot retrieve information without public key and private key at same computation time.

In this way, we can say that authentication is required to get real information in our proposed protocol. In addition to that, our proposed algorithm satisfies confidentiality of messages with complexity of it. Acknowledgment is sent to sender by receiver then it means that *HELLO* message is received within threshold time. Thus, access & availability are also fulfilled through this proposed algorithm. Finally, any vehicle can send its current position to other vehicles for different purposes with sanctification of authentication, confidentiality and access & availability. Hence, our proposed algorithm is useful to transmit current location to other vehicles securely. At last, we have done comparison among different message exchanging protocols with respect to security functionality such that authentication, confidentiality and access & availability.

VII.CONCLUSION

In this paper, we have explained obstacles regarding position of vehicle for V2V communication environment when vehicles send/receive important information firstly. Then, we have discussed different secure positioning protocols. Finally, we have suggested typical secure positioning algorithm for vehicles so that it can be helpful to send/receive actual current position to other neighbor vehicles (those are within network range).Proposed algorithm fulfills security requirements such that authenticity, confidentiality and access as well as availability.

VIII .REFERENCES

[1] Dias, Jo˜ao AFF and Rodrigues, Joel JPC and Zhou, Liang, *Cooperation advances on vehicular communications: A survey*, Vehicular communications,.

[2] Zeng, Yingpei and Cao, Jiannong and Hong, Jue and Zhang, Shigeng and Xie, Li, *Secure localization and location verification in wireless sensor networks: a survey*, The Journal of Supercomputing, Vol.64, No. 3, pp. 685–701, 2013.

[3] Blum, Jeremy J and Eskandarian, Azim and Hoffman, Lance J, *Challenges of intervehicle ad hoc networks*, Intelligent Transportation Systems, IEEE Transactions on, Vol.5, No. 4, pp. 347–351, 2004.

[4] Lin, Xiaodong and Sun, Xiaoting and Ho, Pin-Han and Shen, Xuemin, *GSIS: a secure and privacy-preserving protocol for vehicular communications*, Vehicular Technology, IEEE Transactions on, Vol.56, No. 6, pp. 3442–3456, 2007.

[5] Capkun, Srdjan and Hubaux, Jean-Pierre, *Secure positioning in wireless networks*, IEEE Journal on Selected Areas in Communications, Vol.24,
No. 2, pp. 221–232, 2006.
[6] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on PID controller," *IEEE Trans. Mobile Comput.*, vol. 12, no. 9, pp. 1842–1852, Sep. 2013.
[7] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254,
Jun. 2010.
[8] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 927–935.
[9] H. Taha and E. Alsusa, "Physical layer secret key exchange using phase randomization in MIMO-OFDM," in *Proc. IEEE GLOBECOM*,
Dec. 2014, pp. 1–6.
[10] F. J. Liu, X.Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. MILCOM*, Nov. 2011, pp. 538–542.
[11] I. Csiszar and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.
[12] L. Lai and S.-W. Ho, "Simultaneously generating multiple keys and multicommodity flow in networks," in *Proc. IEEE Inf. Theory Workshop*, Lausanne, Switzerland, Sep. 2012, pp. 627–631.
[13] C. Ye and A. Reznik, "Group secret key generation algorithms," in *Proc. IEEE ISIT*, 2007, pp. 2596–2600.
[14] R. H. Y. Louie, Y. Li, and B. Vucetic, "Practical physical layer network coding for two-way relay channels: Performance analysis and comparison," *IEEE Trans. Wireless Commun.*, vol. 9, no. 2, pp. 764–777, Feb. 2010.
[15] J. A. Fernandez, K. Borries, L. Cheng, and B. V. K. V. Kumar, "Performance of the 802.11p physical layer in vehicle-to-vehicle environments," *IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 3–14, Jan. 2012.
[16] C.-H. Ng and S. Boon-Hee, *Queueing Modelling Fundamentals: With Applications in Communication Networks*, 2nd ed. New York, NY, USA: Wiley, 2008.
[17] M. J. Neely, "Delay analysis for maximal scheduling in wireless networks with Bursty traffic," in *Proc. IEEE 27th INFOCOM*, 2008, pp. 385–393.
[18] F. Ishizaki and H. G. Uk, "Queuing delay analysis for packet schedulers with/without multiuser diversity over a fading channel," *IEEE Trans. Veh. Technol.*, vol. 56, no. 5, pp. 3220–3227, May 2007.
[19] R. Jin, X. Du, K. Zeng, L. Xiao, and J. Xu, "Delay analysis of physical layer key generation in multi-user dynamic wireless networks," in *Proc. IEEE ICC*, 2014, pp. 901–906.
[20] V. Sundarapandian, *Probability, Statistics and Queuing Theory*. New Delhi, India: PHI, 2009.
[21] D. Liu, J. Liu, Y. Mu, W. Susilo, and D. Wong, "Revocable ring signature," Journal of Computer Science and Technology, vol. 22, pp. 785-794, 2007.
[22] T. Zhou, R.R. Choudhury, P. Ning, and K.Chakrabarty,"Privacypreserving detection of Sybil attacks in vehicular ad hoc networks," IEEE Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, (MobiQuitous), pp. 1-8, 2007.