Granting Privacy and Authentication in Mobile Ad Hoc Networks

Balmahoon R, Peplow R (Prof)
Computer Engineering
University of Kwazulu Natal, King George V Avenue, Glenwood, Durban, 4041
Tel: +27 74 338 1192, Fax: +27 86 5857443
email: 207503590@stu.ukzn.ac.za, roger@ukzn.ac.za

Abstract- In recent times, MANETs have gained considerable exposure. The importance of MANETs cannot be overlooked as the computing world is becoming more portable and compact. Their ease of use and convenience make them ideal for emergency type situations. There are security issues in MANETs which arise due to their characteristics and a main issue is the unavailability of a central registration authority. An interesting classification of MANETs is Vehicular Ad Hoc Networks (VANETs). This type of network allows for communication between vehicles and promotes safety on roads. It is essential that the vehicle's identity is hidden in order to prevent tracking; however the certificate authority (CA) needs to know the real identity of the vehicle for legal reasons. There is thus a need for both privacy and authentication.

Privacy is implemented in the form of an anonymous identity or pseudonym, and ideally has no link to the real identity. Authentication ensures that the real identity can be verified. Privacy and authentication are conflicting tenets of security as the former hides a user's identity and the latter ensures a user's identity is known and certified. This paper proposes a novel approach for granting both privacy and authentication in VANETs.

Index Terms—VANET, pseudonym, privacy, authentication

I. INTRODUCTION

In recent decades, the cost and complexity of wireless communication has dropped dramatically while the usage has risen equally dramatically. During 2002, the number of mobile phone subscribers exceeded the number of fixed line phone subscribers, marking a significant event in the history of wireless communications [1]. The growth of wireless network devices has given rise to a new field of networking; that of Ad-hoc networks where the fundamental paradigm shift is that these networks have no formal or predefined structure or generally, any central administration or coordination functions that are normally the hallmark of the more historic wired and structured networks [2].

Ad-hoc networks may be wired or wireless but the lack of organised structure means that nodes can add to or remove themselves from the network at any time [2]. Further, the lack of structure may mean, particularly in wireless networks that two nodes that wish to communicate may be out of signal range of one another and so intermediate nodes may be expected or requested to route the communication packets between the two end nodes [3]. Where Ad Hoc Networks are composed of mobile nodes that enter and leave groups, they are termed Mobile Ad-hoc Networks (MANETs). A growing field within this class is that of Vehicular Ad-hoc Networks (VANETs) which, as explained by Boukerche [4], allow for vehicles to exchange time-critical information that helps improve the safety on roads. The VANET can be used for information transfer between vehicles and much has been written by Boukerche [4] and others in [5] [6] [7] [8] [9] [10] on the various scenarios where vehicles may obtain value from communication. Messages warning of icy road conditions, accidents, congestion etc., are all potentially extremely useful and could reduce accidents.

However, one needs to be sure that the messages are valid and that the network will not be used maliciously. One could for example conceive of a situation where all traffic is informed of a major accident on a motorway and advised to divert to a different route whereas the sender is merely trying to keep a section of the motorway free so that they can use it as a race track. One method of reducing the likelihood of such malicious use is to ensure that all nodes are registered with some central authority so that nodes caught sending erroneous and malicious messages can be determined and held accountable. According to Aboudagga et al. [11], this means that every node should be registered with a central authority. It also means that nodes must identify themselves as the source of all their messages and anonymous message sources should not be permitted or accepted.

This registration and identification however opens up a different problem in that message senders can now be traced and this lack of privacy may result in many nodes being unwilling to send messages at all. It could also allow other nodes to track the sender for nefarious purposes. Examples from Kargl [12] and Weerasinghe et al. [13] discuss how a vehicle may be tracked by developing location profiles. Thus it can be seen that there is a need for all messages to be traceable [14], so the sender can be held accountable for the messages and yet at the same time, it should not be possible for any node to identify the source of any message or to track a node through multiple messages.

This paper is organised as follows: Section II provides an introduction to VANETs. This is where VANET concepts and the network operation are explained. Section III discusses privacy in VANETs. Section IV develops and presents the solution, which caters for both authentication and privacy. The paper is concluded in Section V.

II. VANET INTRODUCTION

Sumra et al. [15] defines the focus of VANETs as fulfilling users' requirements on the road and making their journey safe and comfortable. VANETs make it possible to send warnings about environmental hazards (e.g., ice on the pavement), traffic and road conditions (e.g., emergency braking, congestion, or construction sites), and local (e.g., tourist) information to other vehicles [16]. Once it is known that there is a traffic jam, road closure or accident ahead, a driver may safely avoid the route and save time. Communication between vehicles is therefore suitable because vehicles are able to distribute warnings to other vehicles. Padmadas et al. [8] state that the minimal configuration and quick deployment of VANETs make them suitable for emergency type situations. Messages can also be sent from vehicles to summon for help if needed and to also inform authorities of dangerous behaviour on roads. In another paper by Papadimitratos et al. [17], VANETs are said to assist to make roads safer and offer convenience.

A vehicle is the basic entity module of the vehicular network [15]. VANETs are made up of vehicles (which are equipped with On Board Units (OBUs) and road-side infrastructure units (RSUs). Vehicles may communicate with other vehicles (vehicle to vehicle communication) or with RSUs (vehicle to roadside communication). This is illustrated in figure 1 below. OBU's have on-board sensory, processing and wireless communication modules [18]. The RSUs (road side units) are fixed entities and the vehicles are the moving entities.

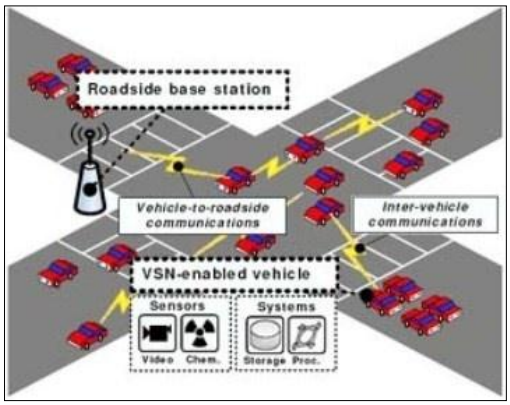

Figure 1-1 – Typical VANET Scenario [19]

The communication in VANETs can either be between vehicles as 'one-hop' or vehicles can act as routers, retransmitting messages and communicating in a 'multi-hop' method [20]. This means that nodes can communicate directly with another vehicle or can pass messages through a series of vehicles.

III. PRIVACY IN VANETS

Pseudonyms are false names and are used to hide the user's permanent or true identity, which in effect preserves privacy [21]. Chaurasia et al. [22] maintain that the pseudonym functions to obtain and sustain anonymity. It allows for a vehicle to interact with other vehicles anonymously. Pseudonyms are ephemeral and distinct pseudonyms hide their relation to each other and to the user's true identity [22]. In terms of VANETs, using a pseudonym for a vehicle means that the vehicle a message originated from cannot be determined. The purpose of pseudonyms is so that the vehicle's identity would be different for each conversation and it would not be possible to determine what identity the same vehicle will have at a later time.

Nodes should ideally be allowed to keep their correspondence private so that confidential information is not leaked to the rest of the network [23]. The same sentiments are shared by Fonseca et al. [24] who further state that the driver's privacy should be respected. Implementing privacy will ensure that the user's real identity is not known and any other vehicle will not be able to determine which vehicle messages originated from. It further allows for vehicles to send messages without fear of being tracked or monitored by malicious users

In VANETs, knowing the source of a message implies that the vehicle the message was sent from is known. If the vehicle's permanent identity is used for sending messages, it allows an eavesdropper to identify all messages sent by the vehicle thus violating privacy [25]. Allowing for the link between a vehicle and the messages sent by the vehicle to be this straight forward could be problematic. Gerlach [26] explains that if the vehicle's permanent identity is not masked it would be possible for malicious nodes analyzing packets in a certain area to create detailed location profiles of vehicles. This problem is also highlighted as a concern by Weerasinghe et al. [13] and others in [25] [27]. Problems could further arise if a vehicle is targeted for an attack. A vehicle whose permanent identity is known could be travelling with a low fuel reserve and request for help, but because the vehicle's identity is known an attacker monitoring communication in the network will be aware that there is a vulnerable vehicle on a road and could follow the vehicle until it has run out of fuel and possibly attack the occupants and steal all valuable items in their possession. The vehicle occupants could then be stranded without a means of contacting the authorities. However, if the vehicle's permanent identity is hidden from all other vehicles and can only be seen by the authorities then only authorized personnel will know which vehicle has requested help and would be able to assist accordingly. Therefore, for the safety of vehicle occupants it is necessary that the permanent vehicle identity is kept secret from other vehicles and known only to the relevant authority. Identity resolution must thus be supported with anonymity [28].

Authentication is employed to ensure that vehicular communication is trusted and secure [29]. A certificate is an electronic document that uses a digital signature to bind a public key to an identity [30], ensuring authenticity of the certificate's owner. The CA is the trusted authority in the network, and is responsible for handing out the initial authoritative information: the certificate. Certified pseudonyms are essential for providing privacy and authentication [31]. Certified pseudonyms are identified by certificates that have been produced by an identity authority (namely the CA), which binds a pseudonym to a public key. The pseudonym has been certified by the CA and it is therefore considered trusted. The certified pseudonym is different from any pseudonym, as pseudonyms are merely a false name and are not authenticated in any way.

IV. SOLUTION

We can see that the desire for privacy is directly in conflict with the need for authentication and certification that can only come about through the registration with a trusted third party or CA. Without this registration, no node would be likely to trust the communications from any other node as there would be no way of tracing a node that gave out false information. Hence in a situation where Alice is sending some message to Bob, Bob needs to receive a certificate with Alice's message that would guarantee that Alice is a registered, authenticated vehicle and can be traced by the CA if the need arises. This certificate must have been signed with the CA's private key so that on receipt, Bob can use the CA's public key to check the certificate. If the certificate can be validated with the CA's public key then it can only have been produced by the CA and then the content of the certificate could be used to verify the registration status of Alice. However, to protect Alice's (and Bob's) privacy, each message sent by Alice should appear as if it comes from a different vehicle; Alice needs pseudonyms. However, this pseudonym must contain some information that would allow the CA, and only the CA to determine Alice's true identity. Thus Alice's permanent or true identity should not be readable by any other vehicles; it should appear as unintelligible information. Further, the certified pseudonym needs to be signed by the CA, ensuring it has a trusted signature. This caters for both authentication and privacy, but there is still an issue. This becomes very difficult to implement in a VANET because there could often be times when the mobile node is out of range of the CA and thus the CA cannot sign this pseudonym certificate. Pseudonyms will thus need to be produced and certified while the node is offline.

The obvious approach is to have the CA always available to generate a pseudonym whenever required but since this is not practical, it makes sense to have some proxy for the CA always available at the node. For this to work, the proxy would have to be a part of the node yet must be implemented in such a manner that it would be impossible for the node to interfere with its operation or to even examine its operation. The proxy should therefore be tamper-proof. It is necessary because the proxy would be in possession of confidential CA information and allowing for the node or any other node to access the proxy would compromise the system's security. The proxy would have to be secure in terms of keeping private information confidential and be immune to any attacks. The proxy would be required to produce the certified pseudonyms and therefore has to have the ability to perform cryptographic computations. The proxy needs to also be a part of a VANET which at times will contain the CA as an available node and at other times not. Proxies need to receive updates, etc. from the CA and therefore need online access to the CA.

A convenient method to ensure that each OBU is equipped with a proxy for the CA is to make use of smart cards. Smart cards are small plastic devices that contain non-volatile memory and microprocessor components, capable of performing very large cryptographic computations [32]. Contact based smart cards, which are used in bank cards, credit cards and SIM cards for mobile telephones, are those referred to [33]. These smart cards are rendered useless upon being tampered with and this protects confidential information contained within them [34]. When physically tampered with, the information stored on the smart card is destroyed. ChunXiao et al. [34] implement PKI functionality on a smart card. Here, a SIM card generates dynamic passwords for authentication, using a security algorithm that has been embedded in the SIM card; this is convenient as a user does not need to carry separate authentication devices. Li et al [35] use SIM cards to produce digital signatures; this is achieved by combining hash functions and an asymmetric encryption algorithm. Satisfying the requirements of a tamper proof proxy, capable of complex cryptographic computations and able to keep information secure, smart cards are thus highly suited for the task of proxy to the CA.

Since physically damaging the proxy will render it useless, tampering with another vehicle's proxy is not a useful option. Vehicles may however be prone to being hijacked or broken into and entire OBU's may be stolen. As soon as an OBU is stolen the CA needs to be made aware so that the unit can be blacklisted. The OBU can then be considered useless and the proxy is disabled and cannot be used. This is similar to the common blacklisting protocol followed when a mobile telephone is stolen. Furthermore, removing the OBU from a vehicle should immediately render it dysfunctional. Such a system could be used by providing each OBU with a code that would need to be entered every time the OBU is powered up. This is very similar to the approach used in many car radios. This means that if the vehicle battery is disconnected or the OBU is disconnected, the code has to be re-entered on the next power up. If a thief gets hold of the OBU it is essentially useless without the PIN and pointless to steal. This is also similar to the authentication used in a mobile telephone.

Utilizing these smart cards as proxies allows for the user to always have verifiable certificates for the pseudonyms produced irrespective of the vehicle's proximity to the CA. This is because the CA's proxy is always 'on-board' the vehicle. The CA's proxy, which has the same level of authority as the CA, is able to issue certificates to users. The proxy would be able to produce certified pseudonyms when required, avoiding the need to wait until the vehicle is in the vicinity of the CA, or for the CA to use large amounts of memory to store a list of pseudonyms for each vehicle.

The main CA requires a public-private key pair separate from the proxies. Should there be a single public-private key pair used by both the main CA and proxies, it would not be possible to distinguish between what has been signed by the main CA and what has been signed by its proxies. The main CA is the main authority and performs greater functions than that of the proxy and therefore requires its own identity. It is essential however that a user is not able to determine which proxy produced a particular proxy signature. By embedding the same public-private key pair in every proxy, all proxies will produce a signature using the same private key. It will therefore not be possible to determine which proxy created the signature, aiding with privacy. There therefore needs to be two public-private key pairs that belong to the CA; a main key pair and a secondary key pair. The main CA holds both key pairs while all proxies hold

only the secondary key pair. The main CA is identified by the CA's primary public-private key pair (PU_{CA1} ,PR_{CA1}), and the proxy is identified by the CA's secondary public-private key pair (PU_{CA2}, PR_{CA2}). The pseudonym produced by the proxy is therefore signed with PR_{CA2}.

The proxy's certificate which combines authentication, privacy and traceability is shown in high level below:

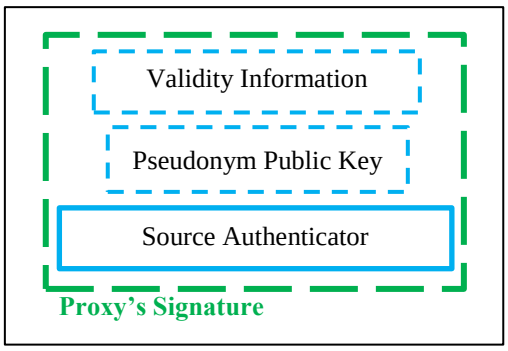

Figure 2 - High Level overview of Proxy Certificate

The attributes needed to verify validity of the proxy's certificate are the Timestamp and Lifespan. The Timestamp indicates the time at which the proxy certificate was created and the Lifespan indicates the duration of the proxy certificate validity. Each time the proxy generates a pseudonym, a public-private key pair is also generated. The vehicle's pseudonym for a specific time is identified by the public key corresponding to that pseudonym. The vehicle's pseudonym public-private key pair is denoted by (PU_V, PR_V), where PU_V is the pseudonym's public key and PR_V is the pseudonym's private key.

The permanent certificate of the vehicle shown above as the source authenticator (contains the vehicle's permanent identity and validity information). This is fixed data and will not change over a long period of time, even though pseudonyms will be changing. While undergoing a traffic analysis attack, the same sequence of bits would be observed in each certificate sent from the vehicle if the permanent identity were not somehow masked. Therefore, to ensure privacy, some sort of variation of the permanent certificate needs to be introduced. A timestamp is used to make the message look different. It will also provide information as to when the permanent identity was used for the current proxy certificate. A different timestamp will be used with each pseudonym as they would be produced in different times. The vehicle's permanent identity and timestamp for variation are implemented in the source authenticator as follows:

$$Source\ authenticator = E_{PU_{CA1}}(Permanent\ Certificate\ ||\ Timestamp) \quad (1)$$

Where:
- $E_{PU_{CA1}}$ = Encryption with the CA's primary public key, PU_{CA1}
- $Permanent\ Certificate$ = The vehicle's permanent identity that has been certified by the CA
- $Timestamp$ = The time at which the proxy's certificate is created.

The vehicle's permanent identity is known and traceable by the main CA only. The certificate containing the vehicle's permanent identity which is handed to the proxy from the CA looks as follows:

$$Permanent\ Certificate = E_{PR_{CA1}}(ID_V\ ||Timestamp_{Perm}||Lifespan_{Perm}) \quad (2)$$

Where:
- $E_{PR_{CA1}}$ = Encryption with the CA's primary private key, PR_{CA1}
- ID_V = The vehicle's permanent identity
- $Timestamp_{Perm}$ = Time that the permanent certificate was created
- $Lifespan_{Perm}$ = Lifespan of the permanent certificate

The permanent certificate in equation (2) is used by the main CA to trace the source of the pseudonym. When a node behaves maliciously or is in distress and requires assistance, the CA attempts to trace a vehicle's identity.

The resultant proxy certificate is a combination of equation (1), the proxy certificate's validity information and pseudonym public key. The proxy certificate is therefore as follows:

$$Proxy\ Certificate = E_{PR_{CA2}}(Validity_{Proxy}\ ||\ PU_V\ ||\ Source\ authenticator) \quad (3)$$

Where:
- $E_{PR_{CA2}}$ = Encryption with the CA's secondary private key, PR_{CA2}
- $Validity_{Proxy}$ = The validity information for the proxy certificate. It is made up of $Timestamp_{Proxy}$ and $Lifespan_{Proxy}$ which are the time that the proxy's certificate was created and the lifespan of the proxy's certificate respectively.
- PU_V = The pseudonym public key

A. Protocol Analysis

Considering the scenario where a message from Carol (Alice's pseudonym) is broadcast to other nodes and Dale (Bob's pseudonym) chooses to reply to Carol, the following transactions will take place:

Alice's OBU generates the pseudonym (Carol) and a public private key pair for Carol (PU_{V_C}, PR_{V_C}). A timestamp is combined with Alice's permanent certificate and both are encrypted using the CA's primary public key, to result in Alice's authenticator:

$$Alice's\ Authenticator = E_{PU_{CA1}}(Alice's\ Permanent\ Certificate\ ||\ Timestamp)$$

The proxy generates validity information ($Validity_{Proxy}$) for the proxy certificate and creates Carol's certificate:

$$Carol's\ Certificate = E_{PR_{CA2}}\ (Validity_{Proxy}\ ||\ PU_{V_C}\ ||\ Alice's\ Authenticator)$$

The hash of the message to transmit and the message timestamp are signed with PR_{V_C} to produce Carol's signed hash:

$$Carol's\ signed\ hash = E_{PR_{V_C}}(h\ (message)||\ timestamp_M)$$

Carol's certificate, signed hash and original message are combined and transmitted:

$$Transmitted\ Message = Carol's\ certificate||Carol's\ signed\ hash||message$$

This transmitted message is broadcast to each node in the area. Since all nodes have access to PU_{CA2} Carol's certificate can be verified.

Upon receiving the transmitted message, Bob does the following:

Bob uses PU_{CA2} to verify the signature on Carol's certificate. Upon verification, Bob can see the following:

$$D_{PU_{CA2}}(Carol's\ certificate) = Validity_{Proxy}\ ||\ PU_{V_C}\ ||\ (Unintelligible\ Information)$$

Where: $D_{PU_{CA2}}$ = Performing a decryption or 'unwrapping' operation (in this case verifying the proxy's signature), using PU_{CA2}

Only $Validity_{Proxy}$ and PU_{V_C} can be read by Bob. If Carol's certificate is valid, PU_{V_C} is considered authentic and valid and is used to verify the signature on Carol's signed hash:

$$D_{PU_{V_C}}(Carol's\ signed\ hash) = h\ (message)||timestamp_M$$

Bob can then read Carol's message hash and view the message timestamp. The hash of the message in plaintext is calculated and if both hashes match, the message was indeed created by Carol.

Thereafter assuming Bob wanted to reply, Bob's OBU generates a public private key pair for Dale (PU_{V_D}, PR_{V_D}). Bob's Authenticator and Dale's certificate are created in the same way Alice's Authenticator and Carol's certificate were created. The only difference is that the original message sent as part of the transmitted message would be wrapped with PU_{V_C}, allowing only Carol to read the message.

The steps above demonstrate that the protocol caters for both authentication and privacy. All proxies are considered trusted and are able to provide authentic pseudonyms which protect the user's real identity, while also ensuring that the CA can trace the vehicle if necessary.

V. CONCLUSION

The goal was to determine if it is possible for a node to produce pseudonyms for itself that would carry the authority of the CA while being traceable by the CA, and would be completely anonymous. The solution achieves this by making use of an on board proxy to produce certified pseudonyms as and when needed, which copes well in the absence of the CA. This is because access to the CA is not needed to produce certified pseudonyms. The proxies are implemented using smart cards as they have remarkable abilities of performing cryptographic computations and keeping private information confidential. They have been used widely in the mobile phone industry as SIM cards and have been highly reliable. These smart cards are damaged when physically tampered with, hence allowing for confidential information to remain private. The proxy mainly functions to produce certified pseudonyms. The proxy certificate functions to certify the pseudonym's public key and provides traceability by embedding in it the source authenticator.

VI. REFERENCES

[1] Samuel C Yang, "Toward a Wireless World," IEEE Technology and Society Magazine, 32 - 42, 2007.

[2] Charles E. Perkins, "Ad Hoc Networking: An Introduction," Nokia Research Centre, 2000.

[3] Patrick McDanial, and Thomas F. La Porta Heesook Choi, "Privacy Preserving Communication in MANETs,".

[4] A Boukerche, *Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks* , 1st ed.: Wiley-IEEE Press , 2009.

[5] Thomas Nowey, Christian Mletzko Klaus Plobl, "Towards a Security Architecture for Vehicular Ad Hoc Networks," in *Proceedings of the First International Conference on Availability, Reliability and Security*, 2006.

[6] Many, *VANET Vehicular Applications and Inter-Networking Technologies*, 1st ed., Hannes Hartenstein and Kenneth P. Laberteaux, Eds. West Sussex, United Kingdom: John Wiley and Sons Ltd, 2010.

[7] Jean-Pierre Hubaux, Srdjan Capkun, and Jun Luo, "The Security and Privacy of Smart Vehicles," in *IEEE Computer Society*, 2004, pp. 49 - 55.

[8] Sudipto Das, Security Issues in MANETs, www.cs.ucsb.edu/~sudipto/talks/Security.pps.

[9] Yvonne Gunter and Hans Peter Großmann, "Usage of Wireless LAN for Inter-Vehicle Communication," in *8th International IEEE Conference on Intelligent Transportation Systems*, Vienna, 2005, pp. 296 - 301.

[10] Yunpeng Wang, Zhenguo Yi, Daxin Tian, and Haiying Xia, "Safety Message Transmitting Method for Vehicle Infrastructure Integration," in *6th Advanced Forum on Transportation of China*, Beijing, 2010.

[11] Nidal Aboudagga, Mohamed Tamer Refaei, and Mohamed Eltoweissy, "Authentication Protocols for Ad Hoc Networks: Taxonomy and Research Issues," in *MSWiM*, Montreal, 2005.

[12] Frank Kargl, "Inter-Vehicular Communication," Ulm University, Habilitation Thesis 2008.

[13] Hesiri Weerasinghe, Huirong Fu, and Supeng Leng, "Enhancing Unlinkability in Vehicular Ad Hoc

Networks," in *IEEE International Conference on Intelligence and Security Informatics*, 2011, pp. 161 - 166.

[14] Tat Wing Chim, S. M. Yiu, Lucas C. K. Hui, and Victor O. K. Li, "Security and Privacy Issues for Inter-vehicle Communcations in VANETs," in *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks Workshops*, 2009, pp. 1 - 3.

[15] I.A Sumra, H Hasbullah, I Ahmad, and J.-L bin Ab Manan, "Forming Vehicular Web of Trust in VANET," in *Saudi International Electronics, Communications and Photonics Conference*, 2011, pp. 1 - 6.

[16] Panagiotis Papadimitratos et al., "Secure Vehicular Communication Systems: Design and Architecture," *IEEE Communications Magazine: Topics in Automotive Networking*, pp. 100 - 114, November 2008.

[17] P Papadimitratos, G Calandriello, J.-P Hubaux, and A Lioy, "Impact of Vehicular Communications Security on Transportation Safety," in *IEEE INFOCOM Workshop*, Laussane, 2008, pp. 1- 6.

[18] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy, "On the Performance of Secure Vehicular Communication Systems," *IEEE Transactions on Dependabe and Secure Computing*, vol. 8, no. 6, pp. 898 - 912, November 2011.

[19] Bruce Sterling. (2007, June) Turning cars into wireless network nodes. [Online]. http://www.wired.com/beyond_the_beyond/2007/06/turning_cars_in/

[20] Wai Chen, Ratul K. Guha, Taek Jin Kwon, John Lee, and Irene Y. Hsu, "A Survey and Challenges in Routing and Data Dissemination in Vehicular Ad Hoc Networks," in *IEEE International Conference on Vehicular Electronica and Safety*, Columbus, 2008, pp. 328 - 333.

[21] Alan Lawson, "Adopting a pseudonym can preserve privacy," Butler Group Review, 2003.

[22] Brijesh Kumar Chaurasia and Shekhar Verma, "Optimizing Pseudonym Updation for Anonymity in VANETs," in *IEEE Asia-Pacific Services Computing Conference*, 2008, pp. 1633 - 1637.

[23] Surabhi Mahajan and Prof Alka Jindal, "Security and Privacy in VANET to reduce Authentication Overhead for Rapid Roaming Networks," *International Journal of Computer Applications*, vol. 1, no. 20, pp. 17 - 21, February 2012.

[24] E Fonseca, A Festag, R Baldessari, and RL Aguiar, "Support of Anonymity in VANETs - Putting Pseudonymity intp Practice," in *WCNC Proceedings*, 2007, pp. 3402 - 3407.

[25] Florian Schaub, Zhendong Ma, and Frank Kargl, "Privacy Requirements in Vehicular Communication Systems," Ulm University, Germany, 2009.

[26] Matthias Gerlach. (2012) Assessing and Improving Privacy in VANETs. [Online]. http://wenku.baidu.com

[27] Frank Kargl, Bjorn Wiedersheim, Zhendong Ma, and Panos Papadimitratos, "Privacy in Inter-Vehicular Networks: Why simple pseudonym change is not enough," in *The Seventh International Conference on Wireless On-demand Network Systems and Services*, 2010, pp. 176 - 183.

[28] Ghassan Samara, Wafaa A.H. Al-Salihy, and R. Sures, "Security Analysis of Vehicular Ad Hoc Networks," in *Second International Conference on Network Applications, Protocols and Services*, 2010, pp. 55 - 60.

[29] Many, *Vehicular Networking: Automotive Applications and Beyond*, 1st ed., M Emmelmann, B Bochow, and Kellum C C, Eds. Wiltshire, Great Britain: John Wiley and Sons, 2010.

[30] CREN and DLF, "Digital Certificate Infrastructure," Washington, 2002.

[31] José María de Fuentes, Ana Isabel González-Tablas, and Arturo Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks," in *Handbook of Research on Mobility and Computing*.

[32] Steve Petri, "An Introduction to Smart Cards," SSP,.

[33] Deep Vardhan Bhatt, "Analysing the behaviour for a Smart Card based model for secure communication with remote computers over the internet," University of Pretoria, Pretoria, Master of Engineering Dissertation 2010.

[34] CardLogix Corporation. (2010) Welcome to Smart Card Basics. [Online]. http://www.smartcardbasics.com/

[35] Quanle Li, Junwei Zou, and Xiaoying Zhang, "The E-Bank Digital Signature Solution Based on PKI-SIM Cards," in *Proceedings of ICCTA 2009*, 2009, pp. 900 - 902.

Reevana Balmahoon received her undergraduate degree in Computer Engineering in 2010 from the University of Kwa Zulu Natal and is presently studying towards her Master of Science degree at the same institution. Her research interests include information security, data communications and mobile networks.