A Literature Survey on Security Challenges in VANETs

Ahmad Yusri Dak, Saadiah Yahya, and Murizah Kassim

***Abstract*—This paper presented a literature survey on security challenges in Vehicle Ad-hoc Networks (VANETs). Many researches on Mobile Ad-Hoc Networks (MANETs) have been done where VANETs routing protocol has taken as a new protocol exist in the network. This protocol or system allows cars to talk to each other where a wireless device sends information to nearby vehicles. More and more technique using VANETs also has been published but yet no comparison has been made between them to look further on the security issues. This research discussed the security issues such as confidentiality, authenticity, integrity, availability and non-repudiation aimed to secure communication between vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). It discussed and analyzed literature on the possible security attacks from 13 researchers that address security and privacy concern in VANETs. Statistics on the relationship between security services versus the technique to encounter the possible attacks is tabulated. Five security services with security attacks and techniques also have been presented. This paper can serve as a reference in building the new technique for VANETs.**

***Index Terms*—Vehicle ad-hoc networks (VANETs), mobile ad-hoc networks (MANETs), security, technique.**

I. Introduction

Vehicular networks are emerging as a new promising field of wireless technology which aims to deploy vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) for safety and non-safety applications. It provides the ability of vehicle to communicate among nearby vehicle and road-side unit (RSUs) as shown in Figure 1. When RSU receives a message from vehicle, it authenticates the message to ensure no malicious message. The Autonomous Server (AS) is responsible for security related issues between vehicle and RSU. Based on wireless fundamental concepts, Wireless Ad-Hoc Network (WANET) has many categories such as wireless mesh networks, wireless sensor networks and Mobile Ad-Hoc Networks (MANETs) as shown in Figure 2. VANETs is a subset of MANETs with a unique characteristic of dynamic nature or node mobility, frequent exchange information, real time processing, self-organizing, infrastructure less nature, low volatility and distance. It is considered the first commercial vehicles of MANETs. In VANETs, security and privacy are identified as major challenge.

Manuscript received August 1, 2012; revised September 2, 2012.

Ahmad Yusri Dak is with the Department of Computer Technology and Networking and Malaysia Institute of Transport (MITRANS), Universiti Teknologi MARA, Malaysia (e-mail: yusri@tmsk.uitm.edu.my).

S. Yahya is with the Computer Sciences at MARA University of Technology, Malaysia.

M. Kassim is with Faculty of Electrical Engineering, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia.

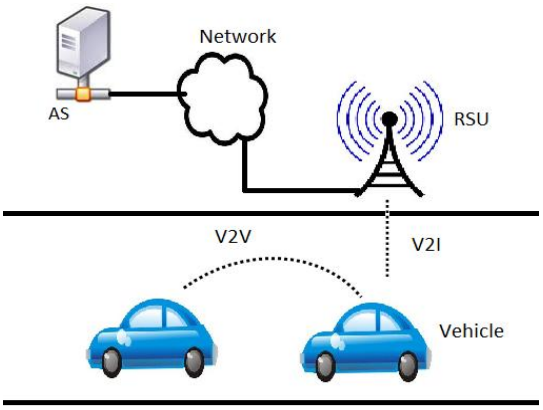

Fig. 1. V2V and V2I communication.

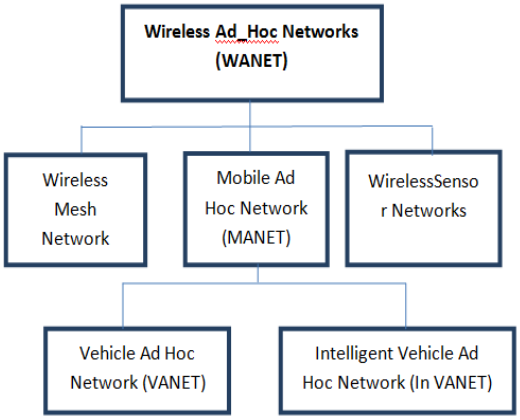

Fig. 2. Structure of WANETs.

This research discusses the security issues such as confidentiality, authenticity, integrity, availability and non-repudiation aim to secure communication between V2V and V2I. The privacy issues are concerned with protecting and disclosing driver's personal information such as name, location, plate number and many more. This paper has discussed and analyzed the possible of security attacks from 13 researchers that address security and privacy concern in VANETs. The analysis concludes that a research gap in the area of security in VANETs. In Section 3, a study on the relationship between securities services versus the technique proposed to encounter the possible attacks is presented

II. Possible Attacks in VANETs

There are a numbers of possible attacks in VANETs. The purpose of these attacks is to create problem for users to access the system or phising some information. Derived are some definition of attacks.

A. Sybil Attacks

Sybil attack is the creation of multiple fake nodes broadcasting false information. In Sybil attack, a vehicle

install with On Board Unit(OBU) sends multiple copies of messages to other vehicle and each message contains a different fabricated identity. The problem arises when malicious vehicle is able to pretend as multiple vehicle and reinforce false data. There are several technique proposed to encounter Sybil attack in VANETs such as statistical and probability, signal strength and session keys [1]-[6]. However, each of these schemes has advantageous and disadvantageous due to dynamic characteristics, weather conditions and system design. One of the interesting method proposed by [1] and [4] are based on statistical and probability algorithm integrated with signal strength as an input data. The different between received signal strength and estimate signal strength is claimed by positionaire calculated. It is analysed by AS using statistical and probability algorithm. A framework to detect Sybil attacks in nodes has been proposed using Certificate Authority (CA) [2], [3]. Two main steps involve in the proses are system initialization and attacks detection where public key and private key are used during system initialization to sign in the message.

B. Node Impersonation

Node impersonation is an attempt by a node to send modified version of message and claims that the message comes from originator for the unknown purpose. An algorithm technique to detect and isolate node impersonation using greedy algorithm that is Detection of Malicious Vehicle(DMV) and Outlier Detection algorithm has been proposed to overcome this problem [7]-[9]. The schemes used RSU to detect and observe an abnormal behaviour of nodes. The proposed scheme increases the trust value of the node if the vehicle is trusted. The identity(ID) of the vehicle will be reported to the relevant Certificate Authority (CA) as malicious if distrust value is higher than threshold value.

C. Sending False Information

Sending False Information can be described as sending the wrong and fake information purposely by one node to another to create chaos scenarios. This scenario may create misinterpretation of the actual scenario. False information is sent by attackers to vehicle for selfish reasons. For example, attacker might send false report on congestion, accident or road block in order to clear the road. A scheme has been proposed to detect the compromised nodes that may misbehave using different kinds of technique [2], [3], [5], [7], [10]-[12]. One of the schemes is a group signature which relies on password access. It can be applied to sign message so that when another vehicle receives a message, it only check the authentication of the message. However, this scheme is not practical since group members always will change frequently especially in a city networks.

D. ID Disclosure

The nodes are able to disclose the identity in the network and track the location of the target nodes. Observer monitors the target nodes and sends a virus to the neighbours of the target nodes. When the neighbours of the attacker are attacked by virus, then they take the ID of the target nodes as well as target's nodes current location [2][3][7][10]. A technique to deal with privacy preserving scheme such as identity disclosure has been proposed to prevent vehicle from being tracked by identifying keys that are used. Al-Hawi et al.[10] is used pseudonyms as an exchange mechanism to encrypt and hide vehicle's unique identity such as driver's name, plate number and location. The pseudonyms used the Public Key Infrastructure to sign the message and this make it difficult to track.

E. DoS and DDoS Attack

The attacker attacks the communication medium or network's nodes to cause the channel or some problem to networks or nodes. The vehicle is unable to access the networks and result in devastation and overtiredness of the nodes and network's resources. None of the reseachers are focusing on DoS and DDoS attack in VANETs as up to date.

III. Security Services in MANET

Security is an important issue for ad hoc networks, especially for security sensitive applications. To secure an ad hoc network, we need to consider the following attributes as criteria to measure security which include availability, confidentiality, integrity, authentication and non-repudiation.

A. Availability

The availability deals with network services for all nodes comprises of bandwidth and connectivity[13]. In order to encounter the availability issues, prevention and detection technique using group signature scheme has been introduced[10]. The scheme is focusing on availability of exchanging the messages between vehicles and RSUs. When the attack causes network unavailability, the proposed technique still survives due to interconnection using public and private keys between RSUs and vehicles.

B. Confidentiality

Confidentiality ensures that classified information in the network can never disclosed to unidentified entities[14]. It also prevents unauthorized access to confidential information such as name, plate number and location. The most popular technique, pseudonyms are used to preserved privacy in vehicular networks [2][3]. Each vehicle node will have multiple key pairs with encryption. Messages are encrypted or signed using different pseudo and these pseudo has not linked to the vehicle node but relevant authority has access to it. Vehicle need to obtain new pseudo from RSUs before the earlier pseudo expires.

C. Authentication

Authentication is the verification of the identity between vehicles and RSUs and the validation of integrity of the information exchange. Additionally, it ensure that all vehicles are the right vehicle to communicate within network. Public or private keys with CA are proposed to establish connection between vehicles, RSUs and AS [8], [12]. On the other hand, password is used to access to the RSUs and AS as authentication method [10].

D. Integrity

Data integrity is the assurance that the data received by nodes, RSUs and AS is the same as what has been generated during the exchanges of the message. In order to protect the integrity of the message, digital signature which is integrated with password access are used [10].

E. Non-Repudiation

Ensures that sending and receiving parties cannot deny ever sending and receiving the message such as accident messages. In certain fields, non-repudiation is called auditability whereby RSUs and vehicles can prove have been receive and sent respectively.

IV. Analysis of Attacks

Listed in Table I, Table II and Table III are analysis of attacks based on previous researches. Based on the statistics four most attacks have been identified as listed in Table I.

TABLE I: Analysis of Security Attacks in VANETs.

Authors	Sybil Attacks	Node Imper'	Sending False Info'	ID Disc'
Daeinabi A. and Rahbar A.G.,2011 [8]		√		
Li and Joshi, 2009 [9]		√		
Xiao B et al, 2006 [1]	√			
Zhou T. et al, 2011 [2]	√		√	√
Zhou T et al,2010 [3]	√		√	√
W.W.Neng et al, 2008 [7]			√	√
Grover J. et al, 2010 [4]	√			
Hao Y. et all, 2011 [5]	√		√	
Mainak G. et al, 2009 [10]			√	√
Park S. et al, 2009 [6]	√			
Al-Hawi F. et al, 2010 [11]		√		√
G. Mainak et al, 2009 [12]			√	

TABLE II: Analysis of Security Services in VANETs on Availability and Authenticity.

Problem statement	Availability		Authenticity	
		Technique		Technique
Daeinabi A. and Rahbar A.G.,2011 [8]			√	Threshold value & CA
Li and Joshi, 2009 [9]			√	Outlier detection algorithm
Xiao B et al, 2006 [1]			√	
Zhou T. et al, 2011 [2]			√	CA/PKC
Zhou T et al,2010 [3]			√	PKC
W.W.Neng et al, 2008 [7]			√	CA/ Symmetric crypto
Grover J. et al, 2010 [4]			√	CA/ Symmetric Crypto
Hao Y. et all, 2011 [5]			√	CA/ digital signature
Mainak G. et al, 2009 [10]	√	Group Signature		Digital signature – secret signing key
Park S. et al, 2009 [6]			√	Digital certificates
G. Mainak et al, 2009 [12]			√	Digital Certificate

TABLE III: Analysis of Security Services in VANETs on Confidential, Integrity and Non-Repudiation.

Problem statement	Confidentiality (Privacy)		Integrity		Non-repudiation	
		Technique		Technique		Technique
Zhou T. et al, 2011 [2]	√	Pseudonyms				
Zhou T et al,2010 [3]	√	Pseudonyms				
W.W.Neng et al, 2008 [7]	√	Session keys				
Grover J. et al, 2010 [4]	√	Session keys: Pairwise & group keys.			√	Digital Signature with sequence number
Hao Y. et all, 2011 [5]	√	Group signature/ private key				
Mainak G. et al, 2009 [10]	√	Group public key	√	Digital signature with password		
Park S. et al, 2009 [6]	√	Timestamp				
Al-Hawi F. et al, 2010 [11]	√	Pseudonyms			√	ID Based signature

TABLE IV: Secure Routing Protocol.

Security Problem	Security attacks	Technique
Availability	Interruption	Group Signature
Authentication	Fabrication	Certificate Authority(CA)
Integrity	Modification	Digital Signature with password
Confidentiality	Interception	Encryption and decryption
Non-repudiation		Sequence number, Digital Signature

V. Conclusion

This paper has briefly introduced Vehicular Ad Hoc Networks and challenges associated with security attacks and security services. It also deeply dig out the security gap for DoS and DDoS that never been explorer previously as in Table I. Various techniques has been identified and discussed by researchers to solve security issues as depicted in Table II and Table III. Five security services with security attacks and techniques has been analysed and tabulated in Table IV according to its security problem.

Acknowledgements

This research is sponsored in part of grant from Malaysia Institute of Transport(MITRANS), Malaysia Logistic Council(MLC) and Ministry of Higher Education(MOHE),

Malaysia for the grant no. 100-RMI/GOV 16/6/2(8/2011)

REFERENCES

[1] B. Xiao, B. Yu, and C. Gao, "Detection and localization of sybil nodes in VANETs," *B. Proceedings of the 2006 Workshop on Dependability Issues in Wireless ad Hoc Networks and Sensor Networks*, 2006, pp. 1-8.

[2] Z. Tong, R. R. Choudhury, N. Peng, and K. Chakrabarty, "P2DAP-sybil attacks detection in vehicular ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 22, no. 3, 2011, pp. 582 - 594.

[3] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of sybil attacks in vehicular ad hoc networks," *Mobiquitous*, Aug. 2009

[4] G. Jyoti, S. G. Manoj, and L. Vijay, "A novel defense mechanism against sybil attacks in VANET," in *Proceedings of the 3rd International Conference on Security of Information and Networks (SIN '10). ACM*, New York, NY, USA, pp. 249-255. 2010.

[5] H. Yong, C. Yu, Z. Chi, and S. Wei, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 3, pp. 616 - 629, 2011.

[6] S. Park, B. Aslam, D. Turgut, and C. C. Zou, "Defense against sybil attack in vehicular ad-hoc network - based on roadside units support," in *Proceedings of the IEEE Military Communications Conference (MILCOM'09)*, Boston, MA, vol. 18, no. 21, October, 2009.

[7] W. W. Neng, M. H. Wueh, and M. C. We, "Anovelsecure communication schemein vehicular ad hocnetworks," *Computer Communications Archive*, vol. 31, no. 12, pp 2827-2837, July 2008.

[8] D. Ameneh and P. R. A. Ghaffar, "Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks," accepted for publication in *Springer Multimedia Tools and Applications*, *Special Issue on Secure Multimedia Communications in VANET*.

[9] L. Wenjia and J. Anupam, "Outlier detection in ad hoc networks using dempster-shafer theory," *10th International Conference on Mobile Data Management'2009*, pp. 112- 121, 2009.

[10] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," *Proceedings of the Mobile Networking for Vehicular Environments (MOVE) workshop in conjunction with IEEE INFOCOM*, Anchorage, Alaska, May 2007.

[11] F. A. Hawi, C. Y. Yeun, and M. A. Qutayti, *The 4th International Conference on Information Tecnology, ICIT 2009*, pp. 3-5 October 2009.

[12] M. Ghosh, A. Varghese, A. Kherani, and A. Gupta, "Distributed misbehavior detection in VANETs," *WCNC 2009, IEEE Wireless Communication and Networking Conference, Budapest, Hungary, IEEE Press*, April 2009.

[13] M. Kassim, R. A. Rahman, and R. Mustapha, "Mobile ad hoc network (MANET) routing protocols comparison for wireless sensor network," in *Proceedings of IEEE International Conference on System Engineering and Technology, ICSET*, no. 5993439, pp. 148-152, 2011.

[14] M. H. M. Zaharuddin, R. A. Rahman, M. Kassim, "Technical comparison analysis of encryption algorithm on site-to-site IPSec VPN," in *Proceedings of International Conference on Computer Applications and Industrial Electronics, ICCAIE 2010*, art, no. 5735013, pp. 641-645, 2010.

Ahmad Yusri Dak received B. Eng degree and MSc (Information Technology) from Universiti Teknologi MARA (UiT), Shah Alam, Malaysia in 1997 and 2003. He is currently working toward the Ph. D degree with Department of Computer Technology and Networking and Malaysia Institute of Transport (MITRANS), Universiti Teknologi MARA, Malaysia. His current research interest includes information security, computer networking and wireless networks.

S. Yahya is a Professor of Computer Sciences at MARA University of Technology, Malaysia. S. Yahya was born at Kuala Lumpur Malaysia in 1956. S. Yahya has graduated with Bachelor of Science with Education (Hon) double majoring in Chemistry and Mathematic 1982 from University of Science Malaysia. S. Yahya later earned a post graduate Diploma in Microprocessor & Applications and Master of Computer Studies from University of Essex UK respectively in 1986 and 1987. S. Yahya finally received her PhD in Computer Science specializing on computer networking from Putra University Malaysia in 1989. She has been lecturing in the University for 27 years in the area of networking, Information Technology security, and Information Technology management. She has published 10 (7 main author and 3 co-author) academic books in the area of computer sciences and IT , written 10 refereed journal and 64 refereed international proceedings in the area of computer networking. She is actively doing research in the area of computer networking and IT and currently has completed 17 researches. Seven of those researches has participated in innovation, invention, and design competition at university and international level and won numerous medals (1 gold, 5, silver, 4 bronze and a Special Award: best presenter). Prof Dr S. Yahyainvolves in many important academic committees at the faculty and the university and is also active with co-curricular activities at the University Particularly for the Faculty of computer and mathematical sciences. Prof Dr S. Yahya has been the head of Network Application and Communication SIG, and an advisor for networking student's union society at the faculty. Prof Dr S. Yahya has been appointed as advisor and chief of panel examiners for many industries and agencies such as Malaysian Board of Higher School of Examination, University of Selangor, Islamic College University of Selangor, and OUM. Prof Dr S. Yahya is committee member of Internet Security Malaysia. Prof Dr S. Yahya is married and a mother of four grown children.

M. Kassim currently is pursuing her PhD study in Computer Engineering at Universiti Kebangsaan Malaysia, Bangi, Malaysia. She is a lecturer from Faculty of Electrical Engineering, Universiti Teknologi MARA. M. Kassim received her Diploma in Computer Science in 1992, BSc (Hons) in Data Communications and Networking in 2003 and MSc in Information Technology in 2007 from the Faculty of Mathematics and Computer Science, Universiti Teknologi MARA (UiTM), Malaysia. She has experienced in the technical and project management during her services in the Centre for Integrated Information System CIIS, the core IT centre for UiTM for 15 years. She work in various network project implementations and managements for 13 years, as project manager in development the university smartcard applications and system for three years and database design and structure for a year. She joined the academic since January 2009 and has published about 20 papers in refereed international proceedings in the area of computer networking and engineering. She is actively doing research in the area of computer engineering and currently has completed 3 researches. Her research interest includes Network Traffic Management, Network Security, Contactless Smartcard Applications, MIFARE Technology Applications, Protective Management System, E-Content Management and Development and WEB-Based applications development. Ms. Kassim also recently a member of IEEE Computer Section Malaysia and member of the International Association of Computer Science and Information Technology (IACSIT) organization.