Sumra *et al.LGU (IJECI)* 2018

LGU (IJECI)
ISSN: 2522-3429 (Print)
ISSN: 2616-6003(Online)

LGU International Journal for
Electronic Crime Investigation

Research Article Vol. 2 issue 1 January-March 2018

A Survey on Attacks and Detection Mechanisms in VANET

Irshad Ahmed Sumra[1], P.Sellappan[2], Azween Abdullah[3]

Department of Information Technology Malaysia University of Science and Technology (MUST), Malaysia. isomro28@gmail.com

Abstract:

Vehicular ad hoc network (VANET) has grown to be foremost up and coming talented and rapidly uprising network or matrix in modern vehicles and this matrix is termed as mobile ad hoc network (MANET). This matrix consists of important and intelligent nodes (vehicles) and certain computing devices named as road side unit (RSU) which are responsible for the communication of vehicles with other vehicles and with RSU as well. Vehicles can communicate with other vehicles on the roads to avoid road accidents and traffic jams on busy roads to save valuable time. This communication is done with the help of unauthentic means of wireless medium which makes the communication possible through air using certain waves like radio waves of high frequency. Because of its immense essence, these matrices are vulnerable to assaults which might cause life threatening circumstances and innocent lives may be lost. If there is any fault in the matrix it can cause serious damage to lives of innocent people so to avoid such significant and serious instances, it is important and necessary that there must be some tools and methods regarding to safety which can observe and find out attacks or assaults like this in the matrix. The purpose of this study is to discuss assaults on VANET and to describe methods to find out the presence of such assaults and to suggest the ways to secure vehicular matrix. Certain and common types of assaults are categorized and discussed and the consequences of such assaults are also explained. This paper also discusses the possible expositions and pros and cons of these expositions.

Keywords: intrudes and intruders, presence of attacks or assaults and attackers, roadside unit, safety, safety measurements, wireless medium, radio waves.

Introduction

Vehicle Ad Hoc Network which is termed as VANET is a certain kind of mobile ad hoc matrix that is responsible for the communication between nodes or vehicles and certain computing devices named as roadside units. Ad hoc networks are spontaneous self-organization of matrix nodes. It must not be necessarily connected to the internet and is usually formed by hybrid wireless matrix and mesh matrix. Every node that is present in the matrix must be installed with onboard circuits (OBC), which helps to accumulate and transmit the nodes' wireless communications, small sensors, embedded systems, and Global Positioning System (GPS). The nodes can then communicate and transmit messages not only to other nodes on the matrix but also to roadside units (RSU), as in traffic signals, which assists in improving the driving experience and ensures the safety of the driver.

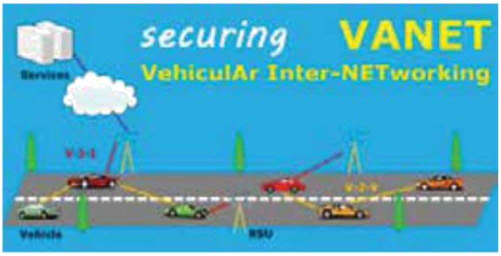

Fig.1 Architecture of VANET

VANET has been becoming one of the uprising technologies in daily routine situations like it is used to find out the traffic jam on a certain road, proper scanning of traffic and administration of traffic. For example if on some busy road there happened to occur an accident, a vehicle (node) that is connected to VANET matrix can send a message to all the other vehicles (nodes) that are connected to same VANET matrix about the accident and deliver them a message to choose an alternate way to travel. Similarly, if traffic is jammed somewhere, a node can deliver a message to other nodes about the traffic jam and intimate them to choose an alternate route. These are the basic routine usage of VANET which may address safety issues but VANET is not limited to this basic routine usage, there are some other applications vitally important that VANET addresses, for example, nodes in this matrix broadcast and share information at all the times, define the facility and utility about the payments, calculates the payments according the two usage and many other things like this. So these applications demand the nodes to communicate and share the information with other nodes, with users of the matrix and with the structure of matrix and the Internet, which results the VANET to be grown and this makes VANET an Internet of Vehicles (IoV). The Internet of Vehicles (IoV) is a collection of multiple matrices which includes inter vehicle matrix (in which nodes communicate with each other V2V), an intra-vehicle matrix (like automotive functions inside the node), and vehicular mobile Internet.

VANET has some distinguished aspects like ability of nodes to be moved freely and easily, its capability of forming new and frequent ad-hoc matrices and topologies that support this feature, of its being capable of judging the moving nodes. For these abilities to be fulfilled there must be distinguished algorithms that can fully and reliably work in such environments for the fulfilment of VANET aspects described above. Safety is a major and most vital concern when dealing with nodes in VANET. The three major components nodes, people and RSU must work together in predicted routine in order to provide a healthy environment. If they are not working in predicted manner then it means safety is breached by an attacker. Safety also means that private data of the user must be confidential. So if safety is compromised it can cause to life threatening risks. But so far, progress on the technology on the issue of safety is has been made but very little.

The first study on the subject of safety was done by by Isaac et al. He proposed certain methods in case of assaults in VANET, but major issues were not solved. In the ending of decade 2000’s, methods were started to be proposed regarding safety. In some of searches during these periods, assaults on safety in VANET were discussed in detail and idea of some systems to find out the presence of intrudes and intruders was proposed. Also presented was the idea to build systems to lower the risk of assaults.

1. Safety Applications in VANET

Mobile ad hoc network MANET has proposed contemporary and advanced safety measurements which if taken risk of compromise on security and safety can be lowered. Problems in VANET can be the deficiency of main spots, for a node to be moved freely and easily, frequent and consecutive correspondence of wireless connection, to be able to work with mutual cooperation, deficiency of a vivid boundary of protection. The major and specialized aspects of VANET are the ones which make above mentioned problems more difficult to resolve. Details of the problems are discussed here:

1.1 Privacy

Vehicular ad hoc network (VANET) has motivated fascination in academic as well as in industry environment. Once these matrices have been deployed in vehicular nodes they might yield a fresh and new driving experience for drivers. But whenever communication happens in an open environment like VANET it challenges the security and privacy. Both privacy and security compromises and it affects the matrix of vehicles.

If the security has to be provided to the VANET user then privacy would have to be sacrificed. Because the matrix controller authorities may have to have information from the drivers of the vehicular nodes during any event but users demands to hide their personal data like their identification, location access and other sensitive data. So to resolve this conflict i.e.; to stop the vehicular nodes from being tracked by unauthorized jurisdictions and for legal jurisdictions to find out the actual identification of VANET user, there must present a suitable system.

1.2 Scalability

Scalability means the addition of more and more nodes into the VANET matrix without the need of changing previous existing components of the matrix. This matrix of vehicular nodes must be scalable in order to meet its modern criteria. Detailed interfaces of scalable components should be provided by manufacturers. Currently, amount of automobiles is roughly about 1.5 billion, may be more than that. And for those nodes which are connected to VANET is about to exceed 1.5 million and is increasing day by day. Till present, none of the international jurisdiction is delivering the safety measurements and methods to matrices like this, for it is a daring and difficult job to provide a systematize mandate for matrix of vehicular nodes. To provide a suitable and feasible solution for this, native jurisdictions must sit together to define systematize rules regarding safety in network.

1.3 Mobility

The nature of matrix of cars as nodes is such that one node interacts with another node a few times, sometimes only one time so topology of the matrix varies frequently. Nodes are usually noticeable if they move with velocity between 18 to 22 meter per seconds but in reality nodes move with velocity greater than the noticeable velocity in mobile matrix of nodes. So there is a frequent disconnection in association of nodes in the matrix. And this disconnection in the association of nodes is even higher if the nodes are moving in antiparallel orientation, here connection keeps itself only for a fraction of time. Nodes usually are connected for a small interval of time and after that probably they never communicate with one another. This issue creates problems for the VANET system. But the nature of topology of VANET is more foreseeable when it is compared against the nature of MANET.

1.4 Hard-delay constraints

Most of the implementations in VANET must be quick respond generating implementations, they must respond to any situation in a real time. If they do not response back in any case of tragedy or accidental events or in emergency situations, then results can be drastically awful. In addition such implementations must be assault proof. All most all the authors suggest that safety implementations must especially emphasis on intercepting the assaults. To stop the assault is better than to find the assault. But the identification of assault is also important in implementations in certain situations like when any employee who knows the security procedure details of matrix tries to assault the matrix.

1.5 Acquiescence

Most of the algorithms and set of rules and regulations of VANET suppose that nodes will distribute and propagate the information to other nodes. And if it happens creates again a challenge for the safety and security for the matrix and matrices become easier for assaults as in wrong information can be sent from one node to another resulting threats and damages for nodes in the matrices. So most of the safety methods depend upon the acquiescence of nodes because more sensitive data is needed in order to stop and find the presence of assaults.

Second safety issue that is present more in MANET but less in VANET is a lucid boundary of protection. Unlike other security systems, security systems in matrices of vehicular nodes are not consisted of some fix points like it happens in guided matrices, but roadside unit is responsible for the safety in VANET like collecting node data and suggesting resolutions to the problematic events. The safety methods in VANET are more efficient than the safety methods of MANET because of some components provided by RSU and this has been already proposed in many literature reviews.

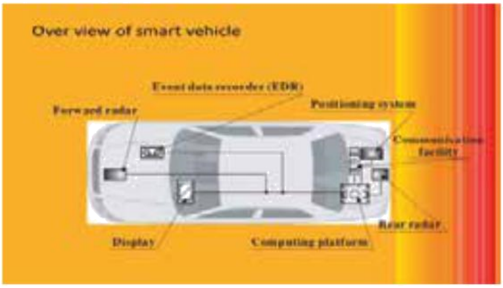

Fig.2 Smart vehicle of VANET

Since the very beginning of the history of VANET and MANET, many different solutions methods and tools have been suggested. Many of these methods were acceptable and adjustable for MANET but largely they seems not fit for VANET because this matrix is highly dynamic in nature contrary to previous matrix. So authors have been trying to propose methods with variations in previous models. Also included the research to protect the matrix from intruders in order to maximize the safety measurements. Previously made safety methods were limited in its working and in the diagnosis of intruders, limited to certain types of intruders, but modification in those methods can result in identification of every kind of intruders like inside intruders who is more dangerous than the outsider intruder. The Internet of Things (IoT) is getting popular day by day. Internet of things is the interconnection of many computing gadgets and matrices enabling them to send and receive and share data even though the types of matrices are different for different electronic devices. These interconnected systems can be embedded systems as well. This can be helpful in many fields such as in home systems, electronic health care systems, embedded sensor networks, doctor patient interaction, alarm systems, automatic lighting, transport systems, ecommerce and many more. And numbers of devices that are interconnected are increasing day by day and in nearest future this number of devices will reach above 25 billion in number. But most of the devices are automobiles and vehicular nodes forming internet of vehicles. Internet of things includes many applications like recognition; transmit messages to other nodes, and setting the rules and regulations for the transmission of messages from node to node. But most devices and applications lack safety methods and procedures. So, some types of assaults are presented in this paper in the following:

1.6 Inter-vehicle-attacks

Inter node communication means the communication between one node and the other node. Nodes have to share information, transmit messages and communicate with each other at all the times. For instance if a node comes across some busy read where the traffic is jam then this node has to transmit a alarming message to all the other nodes particularly in that area. Similarly, if some road accident has occurred at some place then a node which is present there must communicate this message to other nodes in the surrounding region about the accident. Other messages for transmission could be about the slowing down the velocity of the node, change the lane of the road, to stop on the traffic signal, giving alerts about the bad condition of roads etc. so nodes have to communicate with each other if they are connected to the matrix of nodes.

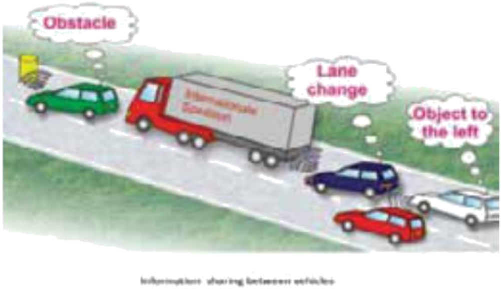

Fig.3 Vehicle to vehicle (V2V) Communication

But intruders can take the advantage of this protective communication. For example, if the intruder is present in node C which is at the last of node A and node B, it can generate false message to node A to slow down while at the same time to node B to fasten its velocity causing an accident between node A and node B. so there must present some more strong methods regarding safety of the matrix against intruders and for the safety of human life.

2. Intra-vehicle attacks: Intra-vehicle communication means the communication of the node within the node. One component of the node transmits the messages to other components of the same node. Advanced vehicular nodes have built in embedded sensors in order to examine the road state, distance between nodes, the presence of any barrier or hurdle, awareness of the fire, to accelerate or retard the velocity of the node,

the interface to exhibits the messages, and an On-Board Unit (OBU) that comprises of node-to-node and road-to-node transmission organization. Assaults within a node like dogging an internal sensor may be dangerous for the node and the surroundings as well. For instance, an assault in the inside system of the node like automatic handling of the node which includes automatic control of steering and horns, automatic speed of the node, information about the fuel etc. can be very harmful for the node and surroundings. In addition, if the node is connected to the internet they there are more chances for a vehicle to be assaulted by an intruder. But these kinds of assaults are not a part of our study.

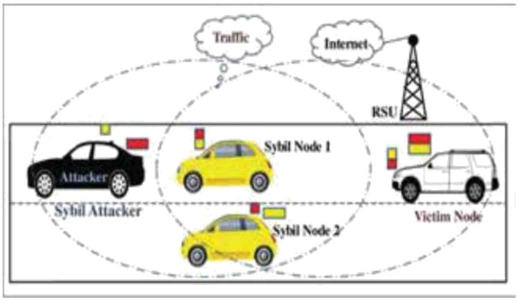

Fig.4 Vehicle to roadside unit (V2R) Communication

2. ATTACK TYPES AND SOLUTIONS

As the growth and expansion of VANET is increasing, the chance of safety concerning issues on moving nodes has been multiplied. Here is presented some of the well-known assaults on the matrix of moving nodes, their categorization with respect to their ambitions and procedures is also discussed.

2.1 Sybil attack

Sybil attack is regarded very hazardous assault in VANET. This kind of assault is concerned with the associating of more than one identity to a single node. A single node can have more than one identity. Because of this, other vehicular nodes in the matrix assume the information is coming from multiple nodes in the mesh or matrix. And they follow the information. The person who makes an assault changes the behavior of the network according to his wish. For instance, assaulter can deliver a message of a busy road to other moving nodes in the matrix, all the other nodes assume that this data is coming from multiple nodes but actually, it is coming from a single node which has more than one identity. These type of assaults are more challenging to be caught. Whenever a node is connected to the matrix it is given a unique identity which is different from the identities of the other moving nodes, so in Sybil assault a node starts to have multiple identities it means they become more than one node in the matrix. And other nodes assume that they are different node in the matrix. These assaults can be made stop by improving the sensor condition of the moving nodes. So the correct information about the node and the position of the node can be received.

2.2 Refusal of Service Assault

Refusal of service assaults is concerned with inaccessibility of certain legal services of a node in the matrix. If a person who assaults the system starts to send the solicitations in amount more than a system can handle then this type of assault is more likely to happen.

Communication is the key of the moving nodes matrix and sending right messages between nodes is the key of trusted communication. If communication breaks for any reason, whole matrix can be destroyed. So if more requests generated by the person who is assaulting the matrix are coming to the system, it may be hard for the system to handle and responded back to these requests in time, so load on matrix increases and communication link goes down. Now nodes cannot deliver the messages of busy roads or about the accidents to other nodes and the purpose of assaulter is fulfilled. The solution to stop this assault is to define a limit of the number of messages a node can send in a unit time to the matrix system. If the number of messages exceeds the maximum limit then it means node is the assaulter.

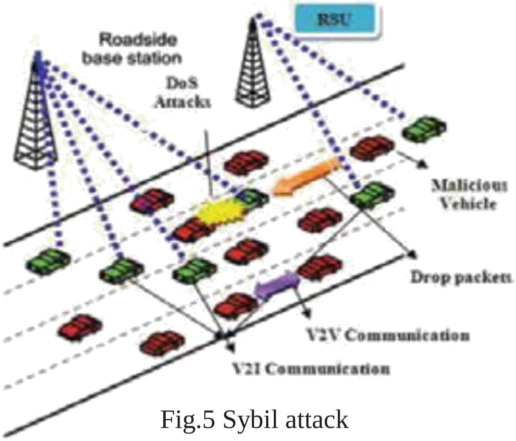

Fig.5 Sybil attack

2.3 Black hole Attack

While refusal of service assault is concerned with making communication link down between the nodes in the matrix, there is also another important sort of assault that can change the behavior of the matrix according to his own wish. In a black hole assault, the person who assaults the matrix enforces other nodes in the matrix to send the information through the assaulter node. All the useful information is now starts to deliver between vehicular nodes through the node of the assaulter. This sort of assault can be made stop if a node that is sending the information can monitor the node who is receiving the node. By monitoring each other these assaults can be minimized.

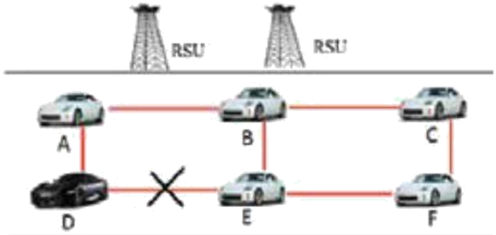

Fig.6 Black hole Attack

2.4 Worm hole attack

A wormhole assault is not carried out by a single node rather it is a combination of two or more than two nodes that are responsible for such assaults. These combinations of nodes claim that they are aware of the shortest route to any target. The purpose of the assaulter is to change behavior of the matrix so that he can gather and handle massive quantity of the matrix load. In the process of this sort of assault, the assaulter obtains a piece of information from a particular node, then changes the information and then delivers it to other nodes. The solution to this assault is that matrix administrator can define a limit of the distance between the sending and receiving nodes. If the distance between the sending and receiving nodes exceeds the maximum defined limit then it means it is suspected to have an assault.

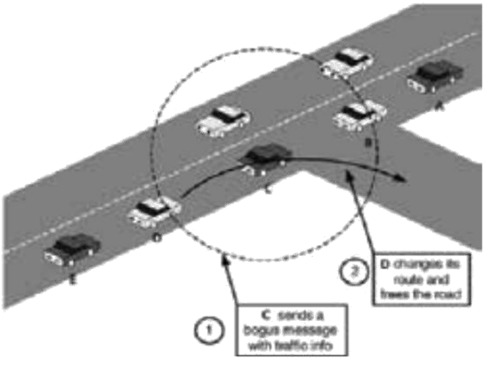
A
B
C
D
E
2
D changes its route and frees the road
1
C sends a bogus message with traffic info

Fig.7 Wormhole attack

Table. I Some Other Solutions On Attacks

S. No.	Solution	Attacks Covered	Technology used	Security Req .
1.	ARAN	1. Replay Attack 2. Impersonation 3.False Warning	1. Cryptographic Certificate	1. Authentication 2. Message Integrity 3. Non-Repudiation
2.	SMT	1. Information Disclosure	1. MAC (Message Authentication Code)	1. Authentication
3.	SEAD	1. DoS 2. Routing Attack 3. Resource Consumption	1. One Way Hash Function	1. Availability 2. Authentication
4.	NDM	1. Information Disclosure 2. Location Tracking	1. Asymmetric Cryptography	1. Privacy
5.	ARIADNE	1. DoS 2. Routing Attack 3. Replay Attack	1. Symmetric Cryptography 2. MAC	1. Authentication

3. CONCLUSION

Safety measurements and methods that are applied on the guided matrices are not applicable on the VANET because the properties and feature of VANET are quite different for the guided matrices. The purpose of this study is to discuss the issues and problems of VANET, the type of assaults in the very matrix and proposed procedures and solutions. The assaults and the structure and reasons of the assaults are clearly discussed. This discussion represents the assaulters always try to utilize the matrix of moving nodes and the operation of how the matrix work. And the solutions to these attacks and procedure along with the advantages and disadvantages to stop these assaults are discussed in details. Whenever we move in an open matrix like VANET which is connected to the internet, chances of being assaulted by any attacker increases due to the very nature of the matrix. The intention of the assaulter is to hack the useful and personal information of the user and deliver the false information among the nodes in the matrix and to diminish the matrix. He or she can be attacked in many ways like the ones eh have discussed in this paper. However they can be made stop by some suitable approaches to stop the assaults or to minimize the chances of the assaults. Conclusively, assault or to find the unusual behavior of the nodes in VANET is very complicated and difficult study and methods and procedures for the safety of such assaults is even more complicated and a difficult task to perform. Computational intelligence-based procedures are suitable methods that might be traversed in coming time research for making the VANET safer.

4. REFERENCES

[1] J. Wan, J. Liu, Z. Shao, A. Vasilakos, M. Imran, and K. Zhou, "Mobile Crowd Sensing for Traffic Prediction in Internet of Vehicles," Sensors, vol. 16, no. 1, p. 88, Jan. 2016.

[2] A. Kapadia, N. Triandopoulos, C. Cornelius, D. Peebles, and D. Kotz, "AnonySense: Opportunistic and Privacy-Preserving Context Collection," in Pervasive Computing, vol. 5013, J. Indulska, D. J. Patterson, T. Rodden, and M. Ott, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 280–297.

[3] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," Computer Communications, vol. 44, pp. 1–13, May 2014.

[4] T. Moore, M. Raya, J. Clulow, P. Papadimitratos, R. Anderson, and J.-P. Hubaux, "Fast exclusion of errant devices from vehicular networks," in 2008 5th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2008, pp. 135–143.

[5] Deena M. Barakah , Muhammad Ammad-uddin , "A Survey of Challenges and Applications of Wireless Body Area Network (WBAN) and Role of A Virtual Doctor Server in Existing Architecture," 2012.

[6] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," Journal of Parallel and Distributed Computing, vol. 73, no. 6, pp. 746–756, Jun. 2013.

[7] US Dept. Transp, Vehicle Safety Communications Project Task 3 Final Report, 2005.

[8] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP-Sybil Attacks Detection in Vehicular Ad Hoc Networks," IEEE Journal on Selected Areas in Communications, vol. 29, no. 3, pp. 582–594, Mar. 2011.

[9] M. Kadam and S. Limkar, "Performance Investigation of DMV (Detecting Malicious Vehicle) and D&PMV (Detection and Prevention of Misbehave/Malicious Vehicles): Future Road Map," in Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), 2013, pp. 379–387.

[10] S. Ruj, M. A. Cavenaghi, Z. Huang, A. Nayak, and I. Stojmenovic, "On data-centric misbehavior detection in VANETs," in Vehicular technology conference (VTC Fall), 2011 IEEE, 2011, pp. 1–5.

[11] H. Sedjelmaci and S. M. Senouci, "An accurate and efficient collaborative intrusion detection framework to secure vehicular networks," Computers & Electrical Engineering, vol. 43, pp. 33–47, 2015.

[12] O. A. Wahab, A. Mourad, H. Otrok, and J. Bentahar, "CEAP: SVM-based intelligent detection model for clustered vehicular ad hoc networks," Expert Systems with Applications, vol. 50, pp. 40–54, 2016.

[13] J. Grover, N. K. Prajapati, V. Laxmi, and M. S. Gaur, "Machine learning approach for multiple misbehavior detection in VANET," in International Conference on Advances in Computing and Communications, 2011, pp. 644–653.

[14] A. Studer, M. Luk, and A. Perrig, "Efficient mechanisms to provide convoy member and vehicle sequence authentication in VANETs," in Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007, pp. 422–432.

[15] R. K. Schmidt, T. Leinmüller, E. Schoch, A. Held, and G. Schäfer, "Vehicle behavior analysis to enhance security in vanets," in Proceedings of the 4thIEEEVehicle-to-Vehicle Communications Workshop (V2VCOM2008), 2008.

[16] S. Park, B. Aslam, D. Turgut, and C. C. Zou, “Defense against sybil attack in vehicular ad hoc network based on roadside unit support,” in MILCOM 2009-2009 IEEE Military Communications Conference, 2009, pp. 1–7.

[17] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, “Privacy-preserving detection of sybil attacks in vehicular ad hoc networks,” in Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, 2007, pp. 1–8.

[18] M. Raya and J.-P. Hubaux, “Securing vehicular ad hoc networks,” Journal of Computer Security, vol. 15, no. 1, pp. 39–68, 2007.